NOTICIAS

AGERS

INFORMACION Y ESTUDIOS DE REFERENCIA DE RIESGOS

EPOCA II NUMERO XXII MAYO 1.998

SUMARIO

EDITORIAL

En lo que va de año, cabe destacar, las siguientes actividades:

Junta Directivas:
- 21 de Enero 1998
- 04 de Marzo 1998
- 07 de Mayo 1998

Asamblea General Ordinaria:
- 31 de Marzo de 1998

Comisión de Modificación de Estatutos:
- 21 de Abril de 1998
- 19 de Mayo de 1998

Congreso Cegers:
- 30 y 31 de Marzo 1998, en el Hotel Holiday Inn, sobre "Riesgos Informáticos y Panorama actual de otros grandes Riesgos".

Jornadas:
- Jornada técnica sobre "El Aseguramiento de los Riesgos Ambientales", organizada por el Instituto de Educación Continua - Universidad Pompeu Fabra, con la colaboración de la Generalitat de Cataluña y AGERS, contando con la participación de los Sres. Torner y Aymerich, del Grupo Nestlé, Empresa Asociada a AGERS.

- Jornada en Sicur sobre "La Responsabilidad de la Empresa ante los Riesgos Laborales", organizada por AGERS en colaboración con Cepreven, fueron conferenciantes los Sres.: Iturmendi, Abogado, López-Fando, Fiscal del Tribunal Supremo, González Escandón, Asepeyo, moderador: Sr. Sáez, El Corte Inglés.

- Participación del Presidente de la Asociación en la Mesa Redonda, celebrada igualmente dentro del marco de Sicur, sobre "El Incendio y sus consecuencias: un riesgo básico a evaluar".
- Seminario "Cuenta Atrás: 85 semanas", organizado por Marsh & McLennan, brindando a los asociados la posibilidad de asistir, por medio de gestiones realizas con los organizadores.

Futuras Jornadas:

- La Asociación está trabajando en la actualidad, en la organización de una Mesa Redonda sobre "Riesgos Informáticos" como continuación a la buena acogida que se reflejo en el CEGERS de este año, a celebrar en Madrid.

- Jornada sobre "La Gerencia de Riesgos en Entidades Públicas y Privadas", a celebrar en Alicante.

Junta Consultiva de Seguros

- Celebrada el pasado 27 de Febrero, con el siguiente Orden del Día:

  1. aprobación del Acta de la última sesión celebrada el 20/10/97.
  2. Proyecto de Real Decreto por el que se aprueba el Reglamento sobre R.C. y seguro en la Circulación de Vehículos a Motor.
  3. Ruegos y preguntas.

Otros:

- Reunión el día 2 de Febrero 1988 con Maurizio Castelli, Secretario General de FERMA, sobre los cambios a producir y futuro de la Federación.

- Asistencia de AGERS a la celebración de los 25 años de Actualidad Aseguradora, el 5 de Febrero 1998.

- Asistencia de AGERS a la presentación de Generali Global, el pasado 10 de Marzo 1998.

- Invitación de la D.G.S. al Día de Seguro, el 26 de Mayo 1998.

- Adquirida para la biblioteca la "Guía Nacional de Seguros 1998".

RIESGOS INFORMATICOS Y PANORAMA ACTUAL DE OTROS GRANDES RIESGOS

INTRODUCCIÓN

Como todos los años, hemos celebrado una edición más del CEGERS y, al igual que en otras ocasiones, se ha elegido un tema monográfico de interés para los gerentes de riesgos y las empresas en general. La espina dorsal de los temas tratados este año han sido los riesgos informáticos: pero al hablar de éstos hay que hablar de una variedad de riesgos que tienen un nexo común - los sistemas de información - pero muy divergentes por su origen y por los efectos. Así, por ejemplo, cabe dentro de este ámbito el riesgo de pérdida de información en soporte informático, pero también la adaptabilidad al Euro de las empresas cuando están obligadas a soportar bajo esa moneda sus operaciones, al igual que la responsabilidad administrativa debida al manejo inadecuado o ilegal de los datos de clientes.

Es evidente la cada vez mayor dependencia que tenemos en nuestras empresas de los sistemas informáticos, y con la misma se incrementan los riesgos que derivan directa o indirectamente de la informática. Hace poco toda la prensa reflejo la noticia de que un banco español corrió el riesgo de un importante quebranto económico debido a unas inundaciones que afectaron a las dependencias donde estaba instalado su ordenador central. Las consecuencias del Y2K es otro buen ejemplo de los importantes riesgos que pueden sufrir las empresas, y que pueden implicar su desaparición si no se toman las medidas oportunas.

La gerencia de los riesgos informáticos implica, como en otros casos, su identificación, su estudio, análisis y diagnostico, la prevención y el estudio de su posible transferencia, entre otros. El CEGERS se ha centrado fundamentalmente en los aspectos de análisis y diagnóstico de los riesgos informáticos que más preocupan y al estudio de su posible transferencia.

Para ello hemos contado con una serie de especialistas que nos han dado su visión sobre los distintos temas tratados: sirva como ejemplo las intervenciones de: Juan Andrés Pro, Informático, que trato el importante tema de la continuidad de los negocios y la informática utilizada en la comercialización y distribución; los abogados Javier Sigüenza, que nos habló de los aspectos jurídicos de la confidencialidad y Gonzalo Iturmendi, José Antonio Cobeña por parte de la Administración y los aseguradores Christian Mehl y Pietro Cossu.

Enrique de Carlos Boutet
Responsable de Seguros
Dpto. Asesoría Jurídica
CONTINENTE

DECIMO CONGRESO DE GERENCIA DE RIESGOS Y SEGUROS

Al cumplirse la décima edición de este Congreso hemos querido hacerlo de una manera significativa, buscando un contenido importante que sirviera de celebración de la efeméride, con unos temas que reflejaran las inquietudes presentes en el momento de su realización.

El Congreso "CEGERS/98" está organizado conjuntamente por AGERS (Asociación Española de Gerencia de Riesgos y Seguros) e INESE (Instituto de Estudios Superiores Financieros y de Seguros. El titulo correspondiente a este año ha sido "**RIESGOS INFORMATICOS Y PANORAMICA ACTUAL DE OTROS GRANDES RIESGOS**".

¿Qué tema más actual, complejo y fuente de tal cantidad de riesgos, que el de la Informática, en su múltiple sentido de fenómenos tan importantes como su enorme divulgación en todos las esferas de la vida, desde el punto de vista individual, doméstico y fundamentalmente empresarial?

La informática aisladamente. La teletransmisión a través de los modems es un fenómeno habitual. El consultar, y manejarse a través de Internet, realizar operaciones, algo absolutamente normal y al alcance de los más básicos sistemas.

Hasta hace poco tiempo, los riesgos informáticos, desde el punto de vista de la Gerencia de Riesgos, consistían en tener debidamente identificados los riesgos de los centros de cálculo, los equipos, y la información en sus más diversos aspectos. Las configuraciones en este sentido eran fácilmente protegidas mediante sistemas de prevención y protección. Mas adelante, la financiación del riesgo mediante pólizas de "todo riesgo" era una realización al alcance de cualquiera.

En el espectro de nuevos riesgos se ofrecen panorámicas como las del "Efecto 2.000". El denominado "Milénium", es decir, el funcionar con cuatro dígitos por año, está siendo fuente de enorme esfuerzo tecnológico para la transformación de los actuales programas, pero, quizás no abordado por la generalidad de los usuarios. Se decía recientemente por los mas destacados Consultores de Dirección, que salvo la Banca y el Sector Asegurador, se estaba haciendo bastante más despacio de lo que sería necesaria a la altura del momento que nos encontramos.

La magnitud de los riesgos que pueden derivarse de esta inercia, es tan enorme, que algunos reaseguradores de Responsabilidad Civil, en la cobertura de Responsabilidad Civl de Consejeros y Directores han excluido de sus coberturas las producidas por la imprevisión de corregir sus efectos.

Por otro lado, las consecuencias derivadas de la transmisión de datos a través de las redes telefónicas, pueden convertirse en reiterada fuente de siniestros.

Si hablamos de la transformación monetaria para actuar de operaciones en pesetas a operaciones en "euros", añadimos un factor importante a una cuestión manejada necesariamente, mediante instrumentos informáticos. ¿Qué riesgos puede añadir esta operación, a los ya existentes en la profesión de los Gerentes de Riesgos? La respuesta tiene que ser necesariamente que: infinitos.

Esta fue la propuesta de exposición y debate a lo largo del primer día del Congreso.
Para el segundo, la panorámica que deseábamos sirviera de base de exposición y debate fue la del fenómeno de la "Globalización" y de la concentración que en forma de fusión, absorción, etc. se están produciendo en el mundo de la financiación del riesgo, con bastante frecuencia en los últimos tiempos, tanto en Sociedades Reaseguradores, como en Grupos Aseguradores, como en Corredores, Consultores o en Despachos de Peritación ¿Hasta donde puede llegar estas concentraciones? ¿Qué puede esperar el Gerente de Riesgos de semejantes fenómenos?

Más aún: a los instrumentos de Financiación de los Riesgos se han añadido desde hace tiempo las Sociedades Cautivas de Reaseguro, utilizadas por los Asegurados en las tácticas internas de retención de riesgos y de optimización de los programas "máster" internacionales y, especialmente el reaseguro financiero denominado habitualmente "ART" (ALTERNATIVE RISK TRANSFER), que se corresponden con planteamientos de soluciones financieras a largo plazo y, en cierto sentido, como auténticos "trajes a medida".

En el Congreso participan Gerentes de Riesgos, Aseguradores, Reaseguradores, Corredores de Seguros, Peritos ajustadores de Pérdidas, Consultores de Riesgos, Consultores de Prevención y Seguridad, etc. Y si decimos que "participan" es porque las reuniones se producen en un clima totalmente abierto de autentico debate y de intercambio de experiencias, moderado por los que designa el Congreso y que siempre coinciden con Gerentes de Riesgos de reconocida experiencia, concretamente en este Congreso fueron Enrique de Carlos Boutet, Responsable de Seguros de C. C. Continente, en el primero de los días e Ignacio Martínez de Baroja y Ruiz de Ojeda, Jefe de Identificación y Evaluación. Departamento de Gerencia de Riesgos de Telefónica, que afrontaría esta difícil papeleta a partir de su segundo.

La ponencia inaugural se desarrolló por CHRISTIAN MELH, Ingeniero en Electrónica, con amplia experiencia en seguros y reaseguro de riesgos informáticos obtenida en Tela Vesicheriung, A.G.. Munich, donde al final trabajó como Gerente del Departamento de Apoyo a la Venta y actualmente en TESCON, Munich (TELA Electronic Security Consultants), como Director Senior.

Su exposición se centró en las coberturas tradicionales que los mercados han otorgado a estos riesgos, basándose fundamentalmente en fórmulas " todo riesgo" de instalaciones de hardware, de pérdida de información y por los riesgos de paralización debidos al fallo de una instalación. La creciente interconexión de los ordenadores y la dependencia de

servicios externos generan nuevos riesgos y, como consecuencia de ello, a "lagunas de coberturas".

Planteó cuestiones como "el concepto de redes de comunicaciones y de información" especialmente de redes de alta capacidad ("autopistas de información") que pueden ser utilizadas para la transmisión de muchos datos o bien para varias aplicaciones a la vez, para definir conceptos de riesgo como el de responsabilidad de los propietarios de la infraestructura básica de la red (carrier, compañía de telecomunicaciones).

Otra de las figuras importantes en la teletransmisión de datos se refiere a los proveedores de servicios de telecomunicación (service provider), también denominados operadores de red, proveedores de servicio (service provider), VANS, redes de servicio de valor añadido.

El papel del asegurador de daños electrónicos, concretamente de daños materiales en componentes electrónicos de la red puede deberse a:

* Carrier (infraestructura básica de la red. PED)
* Proveedor de servicio(PED)
* Proveedor de información (PEDE, equipos de multimedia)
* Usuarios (terminales)

Desde la óptica del seguro de software o del seguro de portadores de datos, los clientes son idénticos a los mencionados:

* Carrier (SW de red, eventualmente datos de facturación)
* Proveedor de servicio (SW de red, datos de facturación, datos, datos de los usuarios)
* Proveedor de información (SW de red, datos de facturación, datos)
* Usuarios (SW de red, datos)

En la actualidad, la mayoría de los seguros electrónicos ofrecen esta gama de productos. En el área de coberturas de pérdidas consecuenciales por siniestros en el ramo del seguro electrónico se ofrecen bajo el concepto de SPB (Seguro de Pérdida de Beneficios) y el SICO (Seguro de Incremento del Coste de Operación). Normalmente se suele otorgar esta cobertura a los "usuarios", ya que hay algunas dificultades importantes para emitirla al "proveedor", porque se presentan cuestiones generales relacionadas con aspectos jurídicos de responsabilidad y de tipo técnico del riesgo, que la impiden.

Los aseguradores están trabajando a fin de ver de desarrollar una solución para los usuarios de proveedores de servicios, en caso ideal con inclusión de daños en las vías de transmisión, o sea en los "carriers"- con lo cual se dispondría en el mercado de un producto con perspectivas óptimas de suscripción.

Por la propia esencia, en el manejo de la informática por medios de teletransmisión se produce una situación de flujos numerosos, internos y externos, a menudo por vías de uso público, que la sitúan en una posición de vulnerabilidad ante los intentos de usos indebidos con ánimo de lucro o alteración de su funcionamiento.

Destacó que la función de Gerencia de Riesgos impone adaptar determinadas precauciones para prevenir la ocurrencia de siniestros, como son: La utilización de la seguridad criptográfica. Seguridad en los accesos, mediante la identificación del usuario/terminal, para evitar la intrusión no deseada.

La identificación de los mensajes, a fin de evitar la alteración de los mismos, que es la técnica más sencilla, segura y clásica de la criminalidad informática, etc.

Como conclusión, vino a decir que el uso no autorizado de servicios, las consecuencias de transmisiones defectuosas y los subsiguientes derechos a indemnización son riesgos adicionales que no pueden ser atendidos actualmente por la industria del seguro en forma de productos específicos.

La siguiente ponencia estuvo a cargo de D. FRANCISCO JAVIER SIGUENZA, que es Abogado y Economista por ICADE, con experiencia en distintas Compañías de Consultoría Informática y que actualmente dirige el Departamento de Derecho Informático del despacho Batalla, Larrauri & López-Ante, es también Profesor en Icade y Coordinador del Curso de Derecho Informático del Colegio Universitario de Segovia. El titulo de la misma fue "ASPECTOS JURIDICOS DE LA CONFIDENCIALIDAD".

Tras de una introducción al complejo tema de la confidencialidad en los riesgos informáticos, con sus diferentes aspectos habló de la Confidencialidad Legal apoyándose en la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (Ley 5/1992) y sus Desarrollos. De la Directiva sobre el Tratamiento de los Datos Personales y la Protección de la Intimidad en el sector de las Telecomunicaciones (97/66/CEE), del Texto Refundido de la Ley de Propiedad Intelectual (RDL 1/1996) y en otra normativa a propósito.

Sobre la Ley 5/92, expuso que se trata de una Ley pionera, que desarrolla el mandato constitucional contenido en el art. 18-4 CE, que ha tenido múltiples desarrollos desde su publicación como son el R.D. 1.332/94, el R.D. 428/93. Estatuto A.P.D.. modificado por R.D. 156/96 e Instrucciones, que concibe la seguridad como suma de cuatro conceptos más precisos:

* Confidencialidad
* Veracidad
* Integridad
* Disponibilidad.

Exige que los datos sean de "calidad" (art. 4) en el sentido de que sean:

* Datos adecuados.
* Datos puestos al día.
* Datos exactos y veraces.
* Derecho de acceso.
* Propio de utilización no abusiva.
* Propio de Lealtad.

Datos especialmente protegidos (art. 7)
Art. 9:

- Aborda con mayor detalle los requerimientos de seguridad.
- Se remite a desarrollos reglamentarios.

El responsable de los ficheros debe garantizar la seguridad: física, lógica, Organizativo-administrativa y establece los principios generales de protección y de las medidas a tomar.

Secreto profesional del responsable del fichero que trasciende a su vida laboral (art. 10)
Derechos a favor del afectado: Información (art. 5), de acceso(art. 14) de rectificación (art.15). de cancelación (art. 15) y de indemnización (art. 17).

Dejó muy claro cuales son las consecuencias del incumplimiento de la normativa, las particularidades de los ficheros privados, la cesión de datos, con mención especial a la cesión internacional así como a la Agencia de Protección de Datos, su potestad sancionadora, recomendaciones e instrucciones, registro y jurisprudencia.
En este apartado Fco. Javier Sigüenza hizo hincapié en conceptos fundamentales como son:

* Concepto de programa de ordenador.
* Titularidad de los derechos.
* Contenido y limites de los derechos de explotación. Protección especial del código fuente
* Sistemas de seguridad informática necesarios para evitar vulneración de los derechos de autor. Prohibiciones legales.
* Empleador como responsable civil subsidiario.
* Presentación y limitación de la línea llamante y conectada.
* Desvío automático de llamada.
* Llamadas no solicitadas

Siguió analizando los aspectos de la confidencialidad contractual, con figuras tales como la contratación de software estardar, contratación de desarrollos a medida y de la contratación electrónica.

Aquí F Javier Sigüenza desarrolló los importantes aspectos a que nos referimos a continuación.:

* Contratación de SW estándar: Obra científica sometida a L:P:I: Garantizar la titularidad del Proveedor. Prever consecuencias. Confidencialidad unidireccional. Piratería como riesgo básico. Garantizar por seguridad, servicio de mantenimiento preventivo, correctivo y evolutivo.

* Contratación de desarrollos a medida: Confidencialidad bidireccional. Transcendental establecer titularidad del desarrollo. Garantizar mantenimiento. Mayor control sobre el personal. Cláusula sobre confidencialidad recíproca. Evitar usos ilegítimos de otro SW.

* Contratación electrónica: Validez de la forma de celebración.

Otra normativa:

* Normativa civil y mercantil: Empleo de procedimientos informáticos para la llevanza de Libros y su conservación. Regulación pactos contractuales con fuerza de ley. Ley reguladora de la Responsabilidad Civil por los daños causados.
* Normativa laboral: Obras desarrolladas en atención a una relación laboral. Cumplimiento de obligaciones sociales.

* Normativa administrativa:

Como cuarto concepto se ocupó de la confidencialidad en Internet, relacionada con la obtención no consentida de información así como de la confidencialidad y secreto profesional.

Ante la magnitud del fenómeno, la ponencia destacó cuatro aspectos fundamentales:
Obtención consentida de información: los COOKIES: Relevancia del consentimiento.

El error. Funcionamiento de los "cookies" Finalidad que se persigue con el "cookie".

* Consentimiento implícito del usuario o previo aviso de la existencia de "cookies".

* Confidencialidad y secreto profesional: Confidencialidad reciproca. Elementos sobre los que existe deber de secreto en casos de asesoramiento por INTERNET. Seguridad técnica o asunción de riesgo por el afectado.

* Confidencialidad y seguridad. Obligaciones de los ISP. Las "nuevas vulneraciones" y su importancia en la seguridad. "hyperlinking, framing, metatags.

A lo largo de la conferencia se fue manifestando una larga experiencia de casos y contenciosos experimentados que clarificaron la enorme complejidad del tema, pero, al tiempo tan habitual en la gestión del riesgo informático y, en consecuencia, tan del día a día del Gerente de Riesgos.

Complementando los dos temas anteriores y en sintonía con el riesgo informático, la siguiente conferencia se desarrolló bajo el titulo de "CONTEMPLACION DE LAS DISTINTAS RESPONSABILIDADES (CIVILES, PENALES, ADMINISTRATIVAS, PROFESIONALES, ETC) que le fue encomendado a D.GONZALO ITURMENDI MORALES, que es Abogado, Director y propietario de su propio Despacho, especializado en Derecho del Seguro. Es Profesor de Derecho del Seguro, Responsabilidad Civil y Gerencia de Riesgos en ICEA, INESE Y CENTRO UNIVERSITARIO MAPFRE DE ESTUDIOS DEL SEGURO. Se trata de un Miembro de nuestra Asociación AGERS y participe asiduo de nuestros Foros.

Algunos de los temas que afectaban a esta ponencia tenían una proximidad con la conferencia anterior, si bien, la experiencia de Gonzalo Iturmendi, las soslayó complementándola de la forma, habitual en él, dejar claros asuntos tan complejos como son las responsabilidades.

El resumen de su exposición consistió en:

1-Delitos informáticos contra la intimidad.
2-Delitos informáticos contra el patrimonio y el orden socioeconómico.
3-La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.
4-Responsabilidad Civil en materia informática.

Ampliando, Gonzalo Iturmendi, resaltó la importancia de la responsabilidad, comenzó con el análisis de la informática en el nuevo Código Penal, de 23/11/1995, con los artículos 197 y 198 referidos a Delitos informáticos contra la intimidad. Continuó con el tema de los Delitos informáticos contra el patrimonio y el orden socioeconómico: Robo con fuerza en las cosas (art. 239) De la estafa (art. 248.2). De los Daños (art. 264.2) De la Propiedad Intelectual (art. 270 a 272) De la Responsabilidad Civil derivada de los delitos relativos a la Propiedad Intelectual (art. 133 a 135 del Texto refundido de la Ley de Propiedad Intelectual, aprobado por R.D. legislativo de 12/4/1996). De la Propiedad Industrial (art. 273 C. Penal). Del espionaje industrial, (art. 278 a 280 C. Penal).

En relación con la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD), pasó un poco más ligero, ya que había sido ampliamente desarrollada por F. J. Sigüenza. No obstante, destacó algunos aspectos fundamentalmente en orden a su significación relacionado con el tema de "responsabilidades".

A continuación desarrolló el tema "estrella" de su conferencia: la Responsabilidad Civil en el contexto informático, donde no existe una normativa específica, por lo que hay que recurrir a las normas generales contenidas en el Código Civil sobre responsabilidad civil contractual y extracontractual; a las normas sobre responsabilidad civil derivada de la comisión de delitos o faltas que se recogen en los art.109 a 122 del Código Penal, así como a la normativa que regula la R.C. derivada de productos defectuosos, Ley 22/1.994, la R.C. derivada de la prestación de servicios que recoge la Ley 26/1.984, de Defensa de Consumidores y Usuarios y la responsabilidad derivada de la violación del derecho de Propiedad Intelectual contenida en el Texto Refundido de la Ley de la Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1.996.

Se detuvo para reflexionar en relación con la R.C. derivada de actuaciones profesionales, en cuanto a la obligación del profesional, no de obtener un resultado, sino de cumplir su obligación de medios, consistente en actuar de acuerdo con el estado de la ciencia y la habilidad normal exigida en cada caso (lex artis).

Responsabilidad civil por actuaciones contrarias a la LORTAD y "ex delicto", fue comentada a continuación, deteniéndose especialmente en su art. 139. Principios de responsabilidad, el 140 Responsabilidad concurrente de las Administraciones Públicas, el 141 Indemnización, el 142 Procedimientos de Responsabilidad patrimonial, el 143. Procedimiento abreviado. En cuanto a la R.C. emanada de lo penal tiende a resarcir al perjudicado por el delito de cualquier orden, producidos por la infracción punible, así como los producidos por los dolores físicos y morales que acarrean todo padecimiento y los gastos que la curación de las lesiones implique. Apoyándose en la doctrina reiterada

de la Sala Segunda del Tribunal Supremo, pasó a aclarar algunos conceptos fundamentales: ¿Quién debe responder?, ¿En que medida se debe responder cuando existan varios autores de delitos o faltas?, ¿Cómo responden los autores, cómplices y otros partipantes?.Posicion de los Aseguradores de responsabilidad civil en el proceso penal. Responsabilidad civil "ex delicto" en caso de exención de la responsabilidad criminal. Responsabilidades civiles "ex delicto" de las Administraciones Públicas y sus dependientes.
Concretando en la Responsabilidad civil por productos informáticos defectuosos, tanto los producidos por el hardware como por el software, a consecuencia de mal funcionamiento resulta aplicable la Ley 22/1.964, de Responsabilidad Civil por los daños causados por Productos Defectuosos. Esta Ley ha optado por un sistema de responsabilidad objetiva, aunque no absoluta, permitiendo al fabricante del producto exonerarse de responsabilidad en los supuestos que enumera la Ley.

En relación con la responsabilidad civil por servicios informáticos, es decir de la Responsabilidad Civil Profesional, Gonzalo Iturmendi, vino a decir que la misma requiere del elemento de culpabilidad. Es decir, no hay responsabilidad sin culpa por parte del profesional de la informática causante del daño.

El asunto INTERNET ocupó la última parte de su ponencia, en sus más variadas manifestaciones de riesgo y, de una manera más destacada, debemos señalar los siguientes aspectos:

Responsabilidad por la intromisión en el derecho al honor, la intimidad y la propia imagen. Al igual que en el caso de la R.C. informática, no existe una normativa especifica que regule la responsabilidad civil de la telemática, por lo que, una vez más, hay que recurrir a la normativa general. El enorme desarrollo presente y, especialmente, futuro del Internet, flujo incesante de información, de opinión y comunicación, aparece la necesidad de proteger derechos de la persona ya existentes, fundamentalmente la intimidad y la propia imagen, pero también las libertades del sujeto y el honor. El Tribunal Supremo así lo entiende, en la sentencia 254/1.993, la cual determina que estamos ante un instituto de garantía de otros derechos.

Resulta obligado establecer los criterios para dirimir la posible colisión entre el derecho al honor y la libertad de información, para lo cual es necesario acudir a la aplicación jurisprudencial de estos derechos constitucionales que pueden entrar en colisión. El derecho al honor puede verse atacado, lesionado o vulnerado por la divulgación, a través de los medios de comunicación, especialmente los de muy alta audiencia pública, de actos, hechos, noticias, etc. Relativas a personas tanto físicas como sociales, que puedan afectar tanto a su propia estimación, como a su esfera familiar y a su consideración socio-profesional. En la línea de Fernando GALINDO, Profesor Titular de Filosofía del Derecho, de la Universidad de Zaragoza, seria necesaria una regulación de INTERNET, desde la doble perspectiva de una directiva EUROPEA y Leyes estatales complementarias.

Hasta aquí, se había desarrollado un planteamiento teórico, desde el punto de vista de riesgos informáticos y coberturas aseguradoras y dos de carácter técnico jurídico, que nos permitían entrar en los siguientes tres casos prácticos.

El primero de ellos: "GERENCIA DE RIESGOS EN LOS SISTEMAS Y TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN EN EL SERVICIO ANDALUZ DE LA SALUD".

Para un tema tan especial, tan sensible, cual es la salud en un colectivo importantisimo, pero, al tiempo, tan delicado en cuanto se refiere a la imprescindible e inexcusable confidencialidad, se eligió a un miembro de la Junta Directiva de AGERS, a fin de que su exposición tuviera la calidad que, tan especial, asunto requería. Fue desarrollado, por D. JOSE ANTONIO COBEÑA, que es Licenciado en Psicología y Antropología. Profesor Titular de la Escuela Universitaria. Director de la Escuela de Trabajo Social, de Huelva. Director del Area de Salud, de la Diputación Provincial de Huelva. Gerente Provincial del Instituto Andaluz de la Salud Mental, de Huelva. Jefe del Servicio de Evaluación y Control del Servicio Andaluz de Salud. Director de la Oficina de Ordenación Administrativa y Subdirector General de Ordenación Administrativa del Servicio Andaluz de Salud, de la Consejería de Salud de la Junta de Andalucía. En la vertiente del riesgo, es el Director de Programas de la Gerencia de Riesgos del Servicio Andaluz de la Salud.

Comenzó J. A. Cobeña exponiendo una certeza, cual es, que la próxima década será testigo de casos de abusos de los derechos de propiedad intelectual y de invasión de nuestra intimidad. Habrá vandalismo digital, piratería del software y robo de información.

Como señas de identidad del Servicio Andaluz de la Salud:

7.000.000 de usuarios/clientes potenciales.
75.000 trabajadores.
690.000 millones de pesetas de presupuesto en 1.998.
30 hospitales.
53 Distritos.
6 centros de transfusión.
3 áreas sanitarias.
1.508 edificios operativos 24/365.

Ante semejante panorama el Sistema de Gestión de Información y Gestión Global de los Servicios Sanitarios en Andalucía están gestionados conforme a:
INSTRUMENTOS Y FINES:

1. Rediseñar el esquema de trabajo para vincular todos los procesos con las Tecnologías de la Información.
2.Vincular los proyectos y servicios orientándolos directamente hacia los destinatarios: usuarios y profesionales.
3.Atender tanto los aspectos tangibles de la gestión de la innovación (instalaciones, costes, tecnologías...) como los intangibles (satisfacción, implicación, valor...)

GESTION DE SISTEMAS DE INFORMACION Y GESTION GLOBAL DE LOS SERVICIOS SANITARIOS DE ANDALUCIA:

4.Desarrollar un proceso de innovación continua versus un plan (entendido como proceso estático e inerte)
5.¿Para qué? Para consolidar un nuevo modelo de servicios públicos, cuya estabilidad reside sobre todo en la satisfacción de sus usuarios (antes, incluso, que en el equilibrio financiero).

LINEAS ESTRATEGICAS DEL PLAN ESTRATEGICO DEL SERVICIO ANDALUZ DE LA SALUD:

1.Orientar los servicios a la mejora de la salud.
2.Incrementar receptividad a la demanda de los usuarios.
3.Eficiencia y efectividad desde la interrelación entre los usuarios y los profesionales.
4.Asegurar la equidad y solidaridad.

El estado general del planteamiento, está, en estos momentos, en un alto cumplimiento de los objetivos.

Para el conocimiento de la situación la estrategia informática en el Servicio Andaluz de la Salud, consiste en un conjunto de planes, medidas y acciones, entre otras, de la protección y seguridad de datos y recursos informáticos de las comunicaciones. Por ejemplo en INTRANET CORPORATIVA, se ofrece mas beneficios que perjuicios a los usuarios generales, internos y externos, así como escasas limitaciones, siendo de las más importantes, la seguridad y confidencialidad en las transmisiones y transacciones internas y externas (firewall, túneles y encriptación). Se garantiza la autenticidad, integridad, conservación y recepción de los documentos.

En cuanto se refiere al programa de Gerencia de los Riesgos, José Antonio Cobeña expuso:

Vertiente de transferencia:
Aseguramiento de la responsabilidad civil, general, profesional sanitaria y no sanitaria
Proyecto del impacto y gestión del efecto milenio.
Proyecto de contratación de asesoría, desarrollo, implantación y administración de la gerencia de riesgos.

En cuanto a la LORTAD: Implantación rigurosa de lo dispuesto en la Ley orgánica reguladora del tratamiento automatizado de datos de carácter personal. , basado en los principios de: Formación e información selectivas acerca de la Ley, divulgación del contenido de la libertad informática, de la autodeterminación informativa y del "habeas data".

Como PUNTOS DE ENCUENTRO, se definen dos grandes áreas de actuación:
Seguridad lógica,
y

Seguridad física.

Para abordar estas cuestiones bajo la óptica de la Gerencia de Riesgos, se define que no es posible una gerencia de riesgos en los sistemas y tecnologías de la información y comunicación, sin antes analizar los riesgos, con objeto de implantar las medidas proporcionadas a estos riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas).

La metodología a utilizar va a consistir en la denominada MAGERIT, que permitirá investigar los riesgos que soportan las tecnologías de la información y la comunicación y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. Esta tecnología, como es sabido, utiliza una estructura de submodelos: de Elementos, de Eventos y de Procesos, que conjuntamente con la Planificación, el Análisis de Riesgos y la Gestión de los mismos permiten una selección de salvaguardas.

El siguiente interviniente planteó un nuevo caso de Gerencia de Riesgos dirigido a permitir conocer, desde la perspectiva del mayor Centro Comercial de España, su casuística compleja y apasionante, bajo el titulo de "LA INFORMATICA UTILIZADA EN LA DISTRIBUCION Y COMERCIALIZACION", que desarrollo D. JUAN ANDRES PRO DIOS, Licenciado en Ciencias Matemáticas, especialidad Investigación Operativa y Estadística Matemática, comenzó a trabajar en el Centro de Calculo de El Corte Inglés, para pasar en 1.995 a dirigir la División de Soluciones y Servicios Profesionales de Informática de El Corte Ingles.

Comenzó afirmando que la informática y las demás tecnologías afines han invadido tanto la vida empresarial y económica como la vida privada. Estamos asistiendo, dijo, a un nuevo modelo de negocio, mucho más competitivo, que requiere una integración más estrecha entre las Tecnologías de la Información y los procesos de trabajo y, que como consecuencia de ello, el papel de los Departamentos de Informática en las organizaciones está cambiando.

Bajo su punto de vista, la emergencia de los riesgos informáticos, manifestada desde el principio de esta década, tiene su origen en los siguientes hechos:
Los sistemas de información y control de las empresas están cada da más integrados y automatizados.

Las aplicaciones informáticas incorporan cada vez más inteligencia del negocio.

El desarrollo de las tecnologías de las Comunicaciones hace que los sistemas informáticos tiendan a estar interconectados en tiempo real, tanto intrínseca como extrínsecamente a cada organización.

La evolución vertiginosa de las tecnologías de la información y su incorporación rápida al mercado para amortizar las costosas inversiones en I+D que se ven obligados a realizar todos los fabricantes, provoca el uso de técnicas poco maduras, no dominadas totalmente ni en el fondo ni en la forma.

Además, este hecho se ve agravado porque la experiencia del pasado vale poco para el futuro.

Tanto el hardware como el software siguen siendo costosos y, además, su complejidad técnica aumenta.

La información es uno de los activos más importantes de todas las organizaciones. Para un gran porcentaje de ellas tiene, incluso, un valor monetario precisamente tasado.

Debido a su carácter estratégico, la informática puede ser objeto de hechos vandálicos y terroristas, como medio de perjudicar los intereses empresariales. Estos pueden ser cometidos por agentes internos o externos a la organización en beneficio de individuos aislados o de colectividades.

En muchas organizaciones la informática todavía es, por desgracia, un mundo aparte en donde los intereses de los profesionales pueden no estar alineados con los objetivos del negocio. Este hecho puede provocar diferencias en el análisis multidisciplinar preciso para evaluar las consecuencias que toda acción, tanto originado por los técnicos como por los usuarios, pueda tener de cara a prever los riesgos que conlleva.

El aseguramiento de la calidad en los procesos de desarrollo y de producción de sistemas de información es todavía muy incipiente. En una actividad con un alto componente tecnológico, las labores de diseño y construcción del software son, aun hoy, muy artesanales. La calidad del sistema sigue estando directamente relacionada con la calidad de sus diseñadores y usuarios; el riesgo del error todavía es grande...! Y sus consecuencias no bien analizadas!

Si verificamos las causas que han dado lugar a los siniestros, a nivel mundial, se puede afirmar que:

Solamente un 13 por ciento están originados por equipos (9%) y software (4%)
Un 78 por ciento tienen su origen en acciones malintencionadas y sabotajes.
El 9 por ciento restante tiene su origen en fallos habidos en otro equipamiento de la empresa (7%) y en otras causas no clasificables dentro de los puntos anteriores.

Analizando más en detalle, las causas de siniestros, y partiendo de las conclusiones de un informe realizado en 1.994, en el Reino Unido por el National Computing Center (NCC), se obtiene la siguiente información:

El 33 por ciento son debidas a acciones fraudulentas.
El 13 por ciento de las pérdidas son debidas a fallos en los sistemas de ordenador.
El 13 por ciento a robos.
El 12 por ciento a fallos en el suministro de corriente eléctrica.
El 9 por ciento a la contaminación por algún tipo de virus de los sistemas microinformáticos.
El 7 por ciento de las pérdidas es imputable a siniestros provocados por inundaciones y/o avenidas de agua.
El 3 por ciento a incendios.
El 2 por ciento es imputable a los daños ocasionados por sabotaje.
Otro 2 por ciento es imputable a fallos en la red de comunicaciones.

Una cantidad similar de pérdidas, en porcentaje, a las anteriores es imputable a las descargas eléctricas provocadas por fenómenos atmosféricos de carácter tormentoso. ¡Solamente el 1 por cien de las pérdidas es imputable a causas relacionadas con el mal uso del sistema!

El 3 por ciento restante se pueden clasificar en el apartado de otras causas no citadas anteriormente.

Esta estadística puede dar datos muy diferentes en otro lugar o en otro momento, tal como veíamos anteriormente y hay que considerar que el porcentaje de casos no se corresponde con el porcentaje de las pérdidas. Así, por ejemplo, los casos existentes de contaminación por virus con muy elevados, pero su repercusión económica es muy baja. Mientras que casos como fuego o sabotaje, con poca ocurrencia representan unas perdidas elevadísimas.

Continuó con el importantísimo tema de "la disponibilidad de los sistemas de información" en el sentido de que el nivel de servicio es la medida por la que se valora la función informática en cualquier compañía. El departamento de informática, no es solo el garante de la consistencia, integridad y confidencialidad de la información, sino también del rendimiento de los sistemas de información y de la disponibilidad de esta última para el usuario.

Por ello, los aspectos de seguridad, tanto físicos, como lógicos, de una instalación y de la necesidad de la garantía de la confidencialidad de la información en ella contenida y manipulada, son aspectos en los que hay que poner un esfuerzo de prevención, de prevención y de seguridad importante.

El proceso de mejora que permitan un alto porcentaje de disponibilidad, puede clasificarse en cuatro niveles, a saber:

Nivel básico, que puede ser obtenido con un sistema único y unos procedimientos primarios de gestión. La selección de un software y hardware fiables pueden ayudar a mejorar la disponibilidad.

Nivel mejorado: Basado también, en un sistema único se dota de mayor robustez mediante la aplicación o redundancia de algún componente del mismo (discos espejados, discos sustituibles en caliente, fuentes de alimentación continua, log. De datos/transacciones, etc.)

Alta disponibilidad: En este nivel se intenta dotar a la instalación de los sistemas de hardware y software necesarios para suministrar un servicio continuo dentro de una ventana temporal determinada. Generalmente se requiere un alto grado de redundancia en los componentes del sistema de cara a protegerles de cualquier fallo. Deberá utilizarse una correcta tecnología para automatizar los procesos de recuperación y minimizar los requerimientos de tiempo necesario para ejecutarlos.

Disponibilidad continua: En este nivel, el Sistema debe ofrecer servicios de forma permanente, incluso ante cambios de procesos y de recuperación de errores. La redundancia de todos los componentes del sistema es vital para conseguir este nivel.

.La clase de eventos que pueden provocar la falta de disponibilidad en un Centro de Cálculo se categorizan en tres grandes grupos:

Mantenimiento preventivo.
Contingencias resolubles a nivel local.
Desastres. Todas aquellas contingencias no resolubles a nivel local. Este tipo de contingencia esta relacionado con eventos de carácter violento o inesperado que inhabilitan los recursos informáticos de la organización durante un largo periodo de tiempo.

Precisamente la recuperación ante desastres para la reanudación del estado de normalidad, implica tanto a las unidades de soporte al proceso de datos como a todas las unidades de la entidad que utilizan para su trabajo las aplicaciones informáticas que se procesan en la instalación siniestrada.

Estas últimas deben contar, en función de la previsión de recuperación del servicio, con: Los procedimientos de gestión alternativos que deberán emplear hasta que el servicio informático se restaure.

Los procedimientos de recuperación de datos ante eventuales pérdidas de información, resultantes del intervalo de tiempo transcurrido desde el momento en que se obtuvo la última copia de seguridad válida para proceder a la recuperación del servicio, y el momento del siniestro. Por supuesto, que hay varias soluciones para proteger los recursos informáticos críticos. Estas incluyen un rango muy amplio de costes y de tiempo necesario para el proceso de recuperación.

Por último propuso el planteamiento de "plan de recuperación de negocio versus recuperación de desastres" que, en general pueden estructurarse de la siguiente manera:

1°. GESTION DE RIESGOS:

Identificar riesgo.
Minimizar riesgo.
Prevenir fallos evitables.

2°. GESTION DE RECUPERACION:

Información crítica.
Activos críticos.
Protección.

3°. CAPACIDAD DE RECUPERACION:

Facilidades técnicas.
Servicios externos necesarios.
Diseño, desarrollo, prueba de implantación del Plan de contingencia y recuperación.

4° . PLAN DE RECUPERACION:

Diseño, desarrollo, prueba de implantación del Plan de contigencias y recuperación.

5º. CONTINUIDAD DE NEGOCIO:

Requerimientos.
Servicios externos requeridos.

La siguiente Ponencia se desarrolló bajo el titulo de "LA INFORMATICA UTILIZADA EN LOS SERVICIOS FINANCIEROS (BANCA Y SEGUROS) , siendo expuesta por D. PIETRO COSSU, cuya formación se corresponde con Financiera, Jurídica y Bancaria, con experiencia de cinco años en Seguros de Crédito, tres en Banca Internacional, ocho en seguros (Estrategia y Seguro de Empresa), siendo actualmente Director del Departamento de Riesgos Financieros y Bancarios, de la Aseguradora AGF en su Sede de París.

El planteamiento de la Conferencia fue expuesto en base al desarrollo de las siguientes cuestiones:

1º Especifidades de la informática en servicios financieros.
2º Aspectos de riesgos focalizados sobre el fraude, el sabotaje, la conversión al Euro y el año 2.000.
3º Como analizar y tratar el riesgo. Como asegurarlo.
4º Soluciones de financiamiento tradicionales y alternativas.

En relación con la primera de las cuestiones pasó a destacar que las industrias de servicios financieros y de tratamiento de flujos de dinero, se diferencia de otras actividades por:

La materia prima es la información. Todos los procesos están basados en la Informática, ya que es como el sistema nervioso del banco y del contacto con el exterior.
Flujos de Datos en gran parte flujos de fondos.
Fondos gestionados por cuenta de terceros.
Sistemas abiertos al exterior con muchas puertas(Gestión de Cuentas, de Créditos, de Tesorería). Mercados Financieros, Cuentas Interbancarias, mediante Sistemas de Tarjeta, Sistemas de Clientes on-line, Relaciones Banco central, etc.
En relación con la relación Flujos de Datos en mayor parte flujos de fondos determinó como especifidades:
Flujos de dinero/Saldos de cuentas
Moneda electrónica.
Desmaterialización de Títulos.

Lógicamente la exposición aumenta con la masa de transacciones electrónicas.

Pietro Cossu continuó con otros aspectos de la especifidad al tratar de los:
Fondos gestionados por cuenta de Terceros, refiriéndose concretamente al dinero en depósito en el banco (o Seguro de Vida), a valores que no pertenecen al banco en que

hay que poner, sin duda, una mayor atención a su seguridad y, de una manera especialmente significativa, a la gestión patrimonial.

En relación con los sistemas abiertos al exterior "con muchas puertas" se destaca la interconexión con INTERNET, con Sistemas de Gestión, con otros Bancos (Cámaras de Compensación) con Particulares (on-line) y con Empresas. En todos los casos se tratan de sistemas complejos, que administran más actividades ligadas entre ellas y que refuerzan la exposición a riesgos recurrentes (Fraude y Sabotaje) o más puntuales (Conversión al Euro y al año 2.000).

Efectos en la gestión del riesgo:

La exposición del riesgo directo sobre los datos puede ser más grande que los efectos indirectos.
La exposición es la del banco y de sus clientes: un tratamiento global indispensable.
Punto de vista de la protección aseguradora:
Exposición a riesgo de daños y de riesgos de daños de responsabilidad civil profesional.
En el segundo de los temas de su conferencia, el fraude, conversión al euro y al año 2.000, Pietro Cossu, expuso claramente cuales pueden ser los efectos de riesgo, tanto en el "computer crime", como en el Euro: una conversión a riesgo y el fenómeno "milenium" como un riesgo potencialmente catastrófico.
En relación con el fraude, dio unas cifras, que reflejan el preocupante aspecto de la cuestión:

En 10 años el fraude informático ha aumentado en un 131 %.
En el mismo periodo los ataques "lógicos" (piratería) han conocido un incremento del 242 %.

Los mecanismos identificados son: Internos, Externos e Internet.

En relación con los problemas de la conversión al Euro, se identifican los enormes problemas de actualizar los procesos (movimientos y saldos de cuentas en moneda local y en Euro) y los de poner al día todos los programas de gestión de cuentas añadiendo una divisa.

Por lo que se refiere al fenómeno 2.000 las necesidades urgentes desembocan en: poner al día todos ("todos") los programas que administran las fechas. A realizar: un inventario exhaustivo de todas las cadenas relacionadas o no. Atender el problema de los pequeños, o medianos o grandes, programas periféricos.

Las consecuencias posibles:

Euro: Responsabilidad Civil Profesional por Errores u omisiones
Año 2.000: Principalmente Responsabilidad Civil Profesional (por las industrias de servicios las consecuencias en daños existen más con efecto menor en comparación con la industria).

De cómo analizar y tratar el riesgo, Pietro Cossu, reflexionó sobre las medidas de:

Prevención:

Controles previos (físicos, lógicos, humanos, organizativos), integración de "fire-walls". Contraseñas, control de empleados (situación vacaciones)...etc.
Controles a posteriori: Sistemas de "huellas", auditorias (internas y externas) test de penetración.
Seguro.

De cómo analizar y tratar el riesgo del Euro y del "milenium" habló en relación a la prevención con énfasis especial en la revisión de los sistemas, proyecto y presupuesto asumido por la Dirección General. Dedicación primordial del personal informático en relación con ambos problemas, la aportación de empresas externas, las relaciones con los proveedores, con especial énfasis en buscar protección en el campo jurídico (responsabilidad de los mismos)

Seguro: En relación con el Euro, soluciones tradicionales y en relación con el 2.000 soluciones alternativas.

La financiación de riesgos aludida en el párrafo anterior, se produce bajo el punto de vista de soluciones tradicionales, lo habitual es asegurarlas en el caso de "computer Crime" en coberturas de fraude/sabotaje continentales o "computer Crime" anglosajonas. Y por cuanto respecta al Euro: Pólizas de responsabilidad civil profesional de instituciones financieras.

Como soluciones "alternativas", precisó que, pueden ser estructuradas para todo de riesgo siendo las más frecuentes los programas "Finitos" y los "Multiline-Multiyear Blended" que combinan una parte de financiación y una parte de transferencia.

Con esta ponencia concluía el primer ida del Congreso que se había dirigido específicamente a los riesgos de naturaleza informática, en todo su conjunto y desde los más diversos puntos de vista.

La participación de los congresistas en los diversos coloquios fue importante y la moderación de Enrique de Carlos propició una magnifica consecución del "intercambio de experiencias", que es uno de los objetivos fundamentales de los Congresos "CEGERS".

Los temas elegidos para el segundo día cambiaban el escenario de una manera fundamental, aspectos de la Financiación de Riesgos, distintos a los tradicionales de conducir la misma a través de los mercados aseguradores y las consecuencias de una concentración de los clásicos interlocutores, lo ponían apasionante

.El día comenzó con la conferencia de SANDRA PAJAROLA, norteamericana de nacimiento, graduada en Empresariales por la Universidad de Wisconsin, con experiencia de trabajos en Bancos Suizos a lo largo de cinco años, para pasar al Grupo Zurich, primero en reaseguro de Crédito y Caución para el mercado hispanoamericano, y desde 1.995 en CENTRE RE, Grupo Zurich, como Responsable de Soluciones no tradicionales, primordialmente para el mercado español. Su ponencia: ART."ALTERNATIVE RISK TRANSFER. PLANTEAMIENTO DE SOLUCIONES

FINANCIERAS" es de una enorme dificultad por cuanto todo lo que se refiere al "finite risk", constituye una confusión, empezando por su denominación. En los últimos tiempos, tres Mesas Redondas organizadas por AGERS han pretendido aclarar, lo más posible, no solo la terminología sino el complejo mundo en que se desarrolla esta técnica. Cabe decir que estas alternativas de transferencia de riesgo, englobadas bajo la sigla "ART", no se corresponden en absoluto con las tradicionales filosofías y practicas del reaseguro tradicional.

Sandra PAJAROLA, lo quiso hacer un poco más fácil, mediante la ayuda de un prestidigitador argentino, que fue haciendo juegos malabares, al tiempo que ella desarrollaba el contenido de la ponencia. Con toda la seguridad que hubo unanimidad en dos cosas, que el artista invitado era "un figura" y que el "ART", seguirá siendo, en cierto modo, una formula casi "mágica".

Básicamente "ART" pretende ofrecer lo mismo que cualquier tipo de seguro: protección y liquidez, diferenciándose, en cambio, en la manera de ofrecerlo y en el deseo de proveer de algo más.

A modo de ejemplo citó el caso de unas enormes inundaciones que, en 1.987, afectaron a Inglaterra, Francia y Holanda, que dieron lugar a importantísimas pérdidas en "property". Las Sociedades afectadas seguramente encontraron respuesta mediante sus seguros, con los límites que pudieran corresponder a sus franquicias o carencias. También en 1.987, concretamente el día 19 de octubre, sucedió el derrumbamiento de la bolsa. Se habló de pérdidas entre un 20 y un 25 % en un solo día. Seguramente muy pocas compañías tuvieron algún tipo de protección para estas pérdidas, para este tipo de riesgo.

Viéndolo desde el punto de vista tradicional, las compañías compraron protección mediante el seguro de "property" ¿porque no se preguntaron que acontecimientos podrían causar una pérdida mayor del 10 % de su capital?. Teniendo en cuenta el doble fenómeno de las inundaciones y de la caída de la bolsa, sin duda que se nos ofrece el panorama, no solo de proteger los bienes que figuran en los "Activos" del Balance, sino también cuestiones como la protección del Capital, que figura en el "Pasivo" de dicho Balance.

Al contrario de lo que ocurre con los seguros tradicionales que se suscriben por un año, aun cuando se vayan prorrogando sucesivamente, el "ART", para que sea realmente eficaz, deberá ser suscrito por varios años, con lo cual, la experiencia siniestral de los años sucedidos, permiten ajustes a los límites, produciéndose unas primas estables, y, dependiendo de la siniestralidad, del participar de beneficios, en relación con posibles resultados positivos para el reasegurador.

En resumen, el asegurado en el caso del "doble gatillo" tendrá protección y liquidez, pero con mucho valor añadido. Está comprando la cobertura que necesita y, si no ocurren siniestros, recibirá una participación en beneficios. todo ello a un precio razonable gracias al empleo de diferentes métodos técnicos.

Lógicamente la relación debe de ser consecuencia del mutuo conocimiento, más aún, de la mutua confianza de las partes, es decir de la Sociedad que pretende ser asegurada y del Asegurador/Reasegurador que va a otorgar el instrumento financiero.

Con ello quedaba concluida la parte destinada a conferencias, con sus habituales debates coloquiales, para pasar a una Mesa Redonda, en la que, los organizadores, teníamos puestas enormes ilusiones.

Bajo el título de "LA GLOBALIZACION ECONOMICA Y EL FENOMENO DE CONCENTRACION EN LOS TRADICIONALES SUMINISTRADORES DE FINANCIACION DE RIESGOS(ASEGURADORES, REASEGURADORES Y BROKERS) participaron en la misma Jose Angel Yarritu Lafuente, General Risk Manager Accounts, de AON, Agustín Martín Martín, Sudirector General de ALLIANZ-RAS y Eduardo Romero Villafranca, Gerente de Riesgos del Grupo de Empresas de CORPORACCION DRAGADOS.

El primero en intervenir, lógicamente, fue el Gerente de Riesgos, es decir Eduardo Romero, que hizo un planteamiento perfecto del marco relacional y de las enormes transformaciones que se están produciendo, a lo largo de los últimos años, pero especialmente a lo largo del pasado año.

Afirmó que dentro del mundo del seguro todos los fenómenos de la globalización están teniendo una incidencia notable, que la situación del mercado "blando" que atravesamos desde hace tiempo, ha provocado que algunas grandes empresas se hayan reconvertido hacia la intermediación y, que tanto corredores como aseguradores, se hayan lanzado hacia una carrera frenética de adquisiciones, quizás con el deseo de conseguir un mayor control del mercado. En cuando a concentración de empresas aseguradoras citó los casos de Royal-Sun Alliance. AXA-UAP, Allianz y Generali con AGF-Athena, Hermes, etc. En el caso de las Corredurías: MML con JONHSON & HIGGINS, CECAR, etc y AON con ALEXANDER, LEBLANC, GIL Y CARVAJAL; SEDGWICK-NIKOLS, etc.

Todo ello configura un escenario cuyo denominador común es la incertidumbre, ya que lo que hasta hace algunos años podía considerarse como un marco relativamente estable en el que las empresas podían planificarse a medio y largo plazo, sin esperar grandes sobresaltos, ha sufrido una alteración radical.

Los interrogantes que planteó a la Mesa fueron:

¿cómo será el Mercado de mañana?
¿va a conseguir el proceso de concentración un control del mercado por los grandes corredores y las mega-aseguradoras?
¿hasta cuando va a durar el marcado soft?
¿qué hacer para proteger mejor a nuestras empresas de los riesgos emergentes, incluso de los especulatívos?
¿cómo combinar los nuevos productos financieros –Programas Finitos de Reaseguro, ART, etc. Con las protecciones tradicionales del seguro?
¿qué rol habría que asignar hoy a una Compañía Cautiva de reaseguros?
¿apostamos por la estabilidad de las coberturas o explotamos a fondo las condiciones actuales del mercado?

¿en que situación se encontraran el día de mañana las compañías que colaboran en la protección de nuestros riesgos el día de hoy.
Terminaba Eduardo Romero esperando que sus reflexiones y preguntas suscitaran más interrogantes que respuestas pero que, en cualquier caso, sirvieran para animar el debate posterior.

Efectivamente, la intervención de Agustín Martín, apoyó, lógicamente posicionamientos propios de la naturalidad de la concentración en base a los valores añadidos que, pensaba, podrían otorgarse a los clientes como consecuencia de las sinergias, que se derivarían, sin duda, de estos fenómenos.

Entre otras cosas, Agustín Martín, afirmó que estas dinámicas podrían derivar en:

* Desaparición de mercados locales.
* Areas económicas supranacionales.
* Presencia del Euro y Globalización.
* Razones estratégicas de tamaño y "masa crítica".
* Ofensiva/defensiva para posicionamiento.
* Oferta más amplia para atender a sus suscriptores.

Know how.
Conjugación de oferta de seguros tradicionales + Servicios Financieros.
Más capacidad de retención.
Una mayor capacidad de atención a Clientes domésticos y de clientes internacionales.
Como resumen una mayor atención al cliente.

A continuación intervino José Angel YARRITU, que en el mismo orden de justificación, adujo los siguientes razonamientos:

Obviar la ineficiencia de la mediación.
Una mayor respuesta a las necesidades del cliente.
Un mayor control del mercado

El coloquio, en esta ocasión moderado por Ignacio Martínez de Baroja comenzó con largo preámbulo de intentar llevar el coloquio, que a la luz de lo expuesto, se consideraba apasionante, en el debate que intentara proporcionar una realidad de lo que, aparente, se estaba posicionando, a unos términos de clarificación, cosa que, sin la menor de las dudas, obtuvo cumplidamente.

Efectivamente a lo largo de más de una hora los congresistas expusieron razonamientos en pro, y, especialmente, en contra de los argumentos razonados por los Aseguradores/Corredores, desde todos los puntos de vista y a la luz de los más diversos intereses del auditorio.

Al final hay que convenir que la globalización de la economía y a la información se percibe en todos los sectores de la economía y del negocio, por lo cual no puede ser ajeno a este fenómeno el sector asegurador, a fin de evitar, lo que parece una amenaza para la supervivencia de las empresas y, a la vez, como una vía para encontrar nuevos horizontes.

Es evidente que la reforma debe imponerse, por múltiples razones, entre otras las manifestadas por el asegurador y el broker, en sentido de buscar dinámicas positivas para el consumidor del seguro industrial. Como ejemplo de la oportunidad de nuevas dinámicas está el resultado, e, incluso, la propia supervivencia de los aseguradores, véase Diario "Expansión" del 7.5.98, en que afirma que el beneficio bruto del sector asegurador cayó el 26 % en 1.997, hasta 165.960 millones de pesetas. Bien es cierto que se explica el fenómeno por varios factores, especialmente caída de los tipos de interés del destino de una gran parte de sus inversiones, por la sobredotación de reservas de vida, debido precisamente a la caída del tipo de interés, por el rescate de seguros de vida para su conducción hacia fondos de inversión, y por los malos resultados de algunas ramos, especialmente el de automóvil.

En el sentido aludido, en la revista "Gerencia de Riesgos", de la Fundación Mapfre Estudios, en su número 61, del primer trimestre de 1998, en articulo firmado por Jean ARVIS, de la Federation Francaise des Societes D¨Assurances, invoca varias razones en orden a la reestructuración:
-Necesidad de acabar con las reestructuraciones en curso.
-Aprovechar la apertura de los mercados.
-Adaptarse a las necesidades de los asegurados.
-Buscar el mejor equilibrio posible entre la rentabilidad y la solvencia.
-Utilizar de forma óptima las posibilidades ofrecidas por la integración de los mercados de capitales y por la llegada del Euro (Caso Europa)
-Reforzar la experiencia en la gestión de los riesgos a largo plazo y en la segmentación de los mercados.

Su conclusión es que el riesgo es uno de los motores del progreso. El control de los riesgos es un requisito para el éxito económico y social.

Aún cuando se trata de opinión, de parte interesada en los campos de la financiación de los riesgos, su lectura debe ser atendida por el mundo de los gestores de los riesgos a fin de adecuar los comportamientos, a las mejores dinámicas para la cobertura de los riesgos en que esta implicado su ámbito de gestión de los riesgos de su empresa.

Si se quiere un resumen breve de la principal enseñanza del Congreso, pasa por recomendar una vez más, la esencia de la Gerencia de Riesgos: IDENTIFICACION, PROTECCION. Buscando luego lo óptimo en la idónea FINANCIACION del riesgo no asumible en órden a la capacidad financiera de la empresa para asumir riesgos.

TOMAS ROMANILLOS DOMINGUEZ
Licenciado en Ciencias Empresariales (ICADE)
Ex - Presidente de AGERS
Ex – Gerente de Riesgos del Grupo CEMENTOS DEL MAR, S.A.

AGERS. Asociación Española de Gerencia de Riesgos y Seguros.
Balbina Valverde, 23.
28.002 MADRID.

EL SEGURO DE EQUIPOS ELECTRÓNICOS PARA REDES DE INFORMACIÓN - HOY Y MAÑANA

Desde hace muchos años, el Seguro de Equipos Electrónicos - antes conocido en Alemania bajo la denominación "Seguro de Instalaciones de Corriente Débil - viene ofreciendo una cobertura especial para la técnica de información y comunicación. Basándose en la cobertura a todo riesgo - se refiere al seguro de hardware, de pérdida de información y de los riesgos por paralización debidos al fallo de una instalación. La creciente interconexión de los ordenadores y la dependencia de servicios externos generan nuevos riesgos y con ello posibles lagunas de cobertura.

El artículo primeramente da una visión global del mercado de las redes de información y trata sobre los diferentes participantes en el mercado que, desde la óptica del seguro, constituyen un grupo objetivo potencial; y las interdependencias existentes entre los participantes del mercado que se suelen definir en contratos de servicio. A continuación se investiga el grado actual de cobertura que obtiene el cliente mediante el Seguro de Equipos Electrónicos existente. La última parte del artículo trata de las carencias de cobertura en los conceptos actuales y las ofertas adicionales, en su caso también de los ramos de responsabilidad civil y de fraude.

El concepto de "redes de comunicación y de información".

En el pasado, se ha usado el concepto de "red" en forma muy restrictiva definiendo a menudo su empleo. Así p. ej. existían y siguen existiendo redes telefónicas, redes de telex, redes de radio móvil, redes de datos y redes de cables TV. En modo creciente se suele entender bajo el concepto de red algo más general y amplio: la red se ha convertido en un vehículo de transporte de informaciones. Existen informaciones digitales, p. ej. en forma de datos informáticos, texto, texto/faximil no codificado, correo electrónico o dibujos. Pero también las informaciones analógicas como voz, imágenes, valores de medición, TV y vídeo suelen ser digitalizadas cada vez más antes de su transmisión; así se convierten igualmente en "datos".

Cuando se trata exclusivamente de la transmisión de datos, el empleo concreto de ellos va perdiendo importancia para la red; en estos casos las redes son de uso universal. La realización técnica de la línea de transmisión como por ej. por cable de cobre, conductores de fibra óptica, radio terrestre o satélite pierde igualmente importancia; tiene solamente efectos diferenciadores en la capacidad de transmisión o su coste.

Si la red tiene suficiente capacidad ("autopista de información"), puede ser usada para la transmisión de muchos datos o bien para varias aplicaciones a la vez. En este contexto surge el concepto de "multimedia" entendido aquí en el sentido de aplicaciones múltiples.

Contemplando las centrales de conmutación, todas las redes modernas son redes de datos y con ello redes informáticas. En la actualidad, esto ya es aplicable en cuanto a las redes digitales de la radio móvil y, en un futuro próximo, para la clásica red telefónica hasta la última "central urbana". Es por esta razón que el presente texto no contempla el aspecto técnico que sólo resultaría de interés para una inspección individual de riesgo, por ej. en el caso del seguro de daños materiales de una infraestructura de red.

Para el asegurador en este ramo son más importantes los participantes en el "negocio de red", o sea los grupos objetivos. La misma cuestión surge también en relación con los aspectos de responsabilidad.

Los propietarios de la infraestructura básica de la red (carrier=compañia de telecomunicaciones).

Debido al monopolio en las vías de transmisión, que existía en Alemania hasta finales de 1997, la propiedad de la infraestructura de red (inglés: carrier) está - con pocas excepciones - en manos de la compañía Telekom.

En virtud de regímenes especiales existen también algunos otros propietarios como Deutsche Bahn AG (Ferrocarriles Alemanes), empresas suministradoras de energía y municipios, que disponen de infraestructuras propias y que empiezan a ofrecer sus redes a terceros.

Los oferentes de infraestructuras alternativas conseguirán el acceso al mercado mediante licencias especiales. La competencia se da principalmente en el área de las comunicaciones a larga distancia en las llamadas "autopistas de datos"; en el sector de las líneas individuales, Telekom dispone de una ventaja casi inalcanzable.

Los consorcios mencionados ya se han preparado con grandes inversiones en la organización y el montaje de infraestructuras de red ATM de banda ancha con base en conductores de fibra óptica, ATM significa "asynchronous transfer mode = modo de transferencia asíncrona" y corresponde a la técnica de transmisión altamente flexible del futuro.

Los proveedores de servicio de telecomunicación (service provider)

En el futuro, no se ganará el "fortunón" en la infraestructura básica sino con los productos y servicios. Actualmente existen en Alemania ya más de 600 proveedores de servicio de telecomunicación autorizados por el Ministerio Federal de Correos y Telecomunicación.

Según oferta y ramo se utilizan también los siguientes sinónimos: operadores de red, proveedores de red (no confundir con propietarios de red), proveedores de servicio, service provider, proveedores de servicios añadidos o VANS (value added network services) redes de servicio de valor añadido.

Junto a los consorcios empresariales, de mucha capacidad financiera, con su punto de concentración en el área de red, es un mercado idóneo para numerosos proveedores de servicios especiales.

El participante de mercado más importante sigue siendo Telekom y su filial DeTe-System GmbH, particularmente en el segmento de los servicios de gestión de redes.

Desde el comienzo de la reforma de correos en 1989, se ha registrado un boom en el mercado de los competidores autorizados. Las líneas de datos ("servicios de datos") pueden ser alquiladas tanto de DeTe-System como también de Meganet GmbH o Info AG. Estas tres empresas y todos los demás suministradores de estos servicios se caracterizan por una cosa: no son los propietarios de la infraestructura básica sino, a su vez, tienen que alquilar las líneas de Telekom.

En el ejemplo citado la línea no es decisiva para el mercado sino que lo que tiene valor es su "perfeccionamiento" a través de servicios complementarios, por ej. garantías de disponibilidad y, naturalmente, el precio. El concepto de VAN o servicio de valor añadido describe precisamente este perfeccionamiento.

Los demás participantes del mercado

Los proveedores de información se presentan como otro grupo diferenciado. Pueden, pero no tienen por que ser idénticos a los proveedores de servicio.

En cuanto a su número, son los usuarios de servicios de telecomunicación los que juegan el papel más importante en el mercado. La gama se extiende desde los abonados particulares a través del hogar privado, que demanda otro tipo de servicio, por ej. de telebanco, hasta las empresas que requieren la gama completa de servicios. Con respecto a los daños consecuenciales, pueden ser de interés para el ramo de los seguros de interrupción.

Desde la óptica jurídica de responsabilidad hay que incluir también en estas consideraciones los eventuales clientes de los usuarios que pueden sufrir daños consecuenciales por problemas en la red.

Un ejemplo conocido demuestra el efecto multiplicador. Muchas agencias de viaje (usuarios) son clientes del sistema de reserva START (proveedor de servicio). Si la agencia de viaje necesita una reserva de vuelo, es comunicado en la red, por ej. con Lufthansa (proveedor de información). Por la infraestructura de la red, o sea las líneas y su disponibilidad, tiene que responder la compañía de telecomunicación (carrier). Cada eslabón de la cadena dispone, a su vez, de componentes de hard y software propios por los que responden otras empresas. Finalmente, está el cliente de la agencia de viaje que compra el billete de avión. Cuando se produce una avería en la red, por ej. una interrupción del servicio o una reserva defectuosa, éste, teóricamente, puede sufrir también un daño.

El papel del asegurador de daños electrónicos - hoy y mañana

¿Donde está posicionado el asegurador de los daños electrónicos en este mercado gigante de crecimiento rápido? ¿Cuáles son los productos que ya se ofrecen? Y ¿con qué éxito? ¿Cuáles son los productos que demandará el mercado en el futuro?.

Desde la óptica del seguro de daños materiales en equipos electrónicos se distinguen los siguientes grupos que pueden sufrir daños materiales en componentes electrónicos de la red:

Carrier	(infraestructura básica de red, PED)
Proveedor de servicio	(PED)
Proveedor de información	(PED, equipos de multimedia)
Usuarios	(terminales)

Desde la óptica del seguro de software o del seguro de portadores de datos, los clientes son idénticos a los mencionados.

Carrier	(SW de red, eventualmente datos de facturación)
Proveedor de servicio	(SW de red, datos de facturación, datos, datos de usuarios)
Proveedor de información	(SW de red, datos de facturación, datos, programas-información)
Usuarios	(SW de red, datos)

En la actualidad, la mayoría de los seguros de equipos electrónicos ofrecen principalmente esta gama de productos; más tarde se tratarán determinados problemas. La creación de numerosas empresas nuevas y la creciente densidad de instalación supondrá un potencial de crecimiento. Por otro lado, es conocido que la bajada de los precios del hardware está limitando en crecimiento.

La rentabilidad del seguro de daños materiales para terminales a menudo está limitada por los reducidos valores. Un ejemplo evidente son los teléfonos móviles que hoy en día ya no requieren cobertura alguna.

En el año 1989, TELA Versicherung AG ofreció por primera vez el seguro de software en el mercado alemán. El concepto de cobertura va más allá del seguro clásico de portadores de datos, ya que el seguro material para el portador de datos no era más una condición previa para la obligación a indemnizar. Junto a muchos otros riesgos se asegura también la pérdida de información debido a negligencia, virus informáticos, intrusos y por averías en la teletransmisión de los datos y con ello está posicionado claramente en el área de PED interconectado en redes.

En la actualidad falta mucho para llegar a una saturación del mercado. Pero el reducido grado de conocimiento y la necesidad de una explicación del producto impiden un aprovechamiento completo del potencial.

Hasta ahora, no existe la demanda de un seguro de software para los "contenidos de programa" - se trata de los de proveedores de información, por ej. un catálogo electrónico de una casa de venta por correo o una película de TV de pago - pero en principio es imaginable.

En el área de las coberturas de pérdidas consecuenciales por siniestros en el ramo del seguro electrónico se ofrecen el SPB electrónico (Seguro de Pérdida de Beneficio) y el SICO (Seguro de Incremento en el Coste de Operación). El potencial de clientes en el mercado de redes coincide otra vez con él del seguro de daños materiales y de software.

Carrier	(Infraestructura básica de red, PED)
Proveedores de servicio	(PED)
Proveedores de contenidos	(PED, equipos multimedia)
Usuarios	(terminales)

Aquí son los usuarios los que constituyen un grupo muy importante. Si se produce por ej. un problema en la mencionada red START, las agencias de viaje no pueden trabajar, lo que se reflejará seguramente en su cifra de ventas.

Este ejemplo aclara a la vez una dificultad fundamental en este mercado. El tomador del seguro PB suele disponer de equipos informáticos de los que responde únicamente él y que están destinados a la obtención de ingresos de venta.

La agencia de viaje START no depende de sus terminales propios que, en caso de siniestro, podría reemplazar sin problema alguno. El verdadero riesgo de pérdida viene a ser determinado por Telekom (carrier), el centro de cálculo de START (proveedor de servicio) y por ej. el centro de cálculo de Lufthansa (proveedor de información). Un daño en cualquier eslabón de esta cadena que no puede ser influenciado directamente por el asegurado ni por el asegurador, puede tener como resultado que en la agencia de viaje "el monitor se quede oscuro" sin que se pueda mejorar la situación mediante el reemplazo del mismo.

La misma situación se da en los centros de cálculo de servicio, que - en el sentido de este artículo - son también participantes en el mercado , a saber, proveedores de servicio. Un siniestro en el centro de cálculo puede paralizar la actividad comercial de todos los usuarios, es decir, los clientes del proveedor de servicio. Estos usuarios son empresas que, en muchos casos, han dejado de manejar su propio centro de cálculo por completo mediante la delegación de estos trabajos a servicios externos (outsourcing).

En este contexto se presentan cuestiones generales relacionadas con aspectos jurídicos de responsabilidad y de tipo técnico del riesgo.

Normalmente, el proveedor de servicio no responde frente a sus usuarios en casos de "fuerza mayor". Son muy pocos los proveedores que tienen un plan de emergencia que garantice alternativas en caso de siniestro. Una planificación de emergencia causa gastos adicionales de puesta a disposición que se reflejarán en los precios del proveedor de servicios y que debilitarán su posición en el mercado puesto que los usuarios no lo valoran o bien presuponen automáticamente su existencia.

Ahora bien, si se señala al proveedor de servicio que un seguro de pérdida de beneficio le permitirá responder frente a los usuarios y que obtendrá así una ventaja competitiva en el mercado, en primer plano seguramente mostrará interés en el producto. Probablemente se eche atrás cuando se hable de la prima necesaria. Esto es comprensible teniendo en cuenta que en un caso como este, la prima de un seguro PB superará en probablemente los gastos de una planificación de emergencia.

Por los motivos expuestos, resulta más interesante ofrecer este seguro al propio usuario. Él entenderá rápidamente que se le puede producir una interrupción del servicio debido a un daño en su proveedor de servicio o su operador de red y de cuyas consecuencias no responderá nadie. Como ejemplo se pueden citar otra vez las agencias de viaje.

En este contexto no hay que dejar de mencionar nuevamente el aspecto técnico del riesgo. El usuario no tiene influencia alguna con respecto a las medidas de seguridad de su proveedor de servicio, normalmente las desconoce por completo. ¿Cómo calcula el asegurador el riesgo y, sobre todo, las posibles opciones de reducción del daño mediante redundancias?. En caso de siniestro no podrá obligar al proveedor de servicio a tomar medidas de minimización del daño por no tratarse de su parte contratante.

Y aún peor: en caso de un fallo en la red, el asegurador probablemente no tendría la posibilidad de verificar, por ej. con el carrier responsable, si la causa del fallo está cubierta conforme a las condiciones del seguro (condiciones generales del seguro de equipos electrónicos/pérdida de beneficios).

Debido a la tendencia del outsourcing de los centros de cálculo, se cuenta para el futuro una creciente necesidad de conceptos de seguro de este tipo.

Si los aseguradores lograran desarrollar una solución para los usuarios de proveedores de servicio - en caso ideal con inclusión de daños en las vías de transmisión, o sea en los carriers - se dispondría de un producto con perspectivas óptimas en el mercado.

Este mismo producto también sería de interés para los usuarios de otros servicios de telecomunicación, por ej. los clientes de bancos de datos económicos, situándose la cifra de fallo en estos casos a menudo por debajo del 100% (la cifra de fallo indica la dependencia económica del tomador de seguro del funcionamiento de la instalación asegurada).

Otras ideas innovativas de este tipo podrían conducir a que el asegurador extendiera la definición del concepto de daño material en el sentido de una "cobertura de red a todo riesgo". Un producto semejante, que también indemnizara por ej. en caso de fallo de la red por "problemas de software", tendría una salida de venta extremadamente buena - para el asegurador, sin embargo, supondría un riesgo considerable. Si cada fallo en la red, que haya superado un determinado tiempo mínimo, condujera a la obligación de indemnización, la renuncia a la verificación del daño, por ej. con el carrier, resultaría fácil.

Otras posibilidades con respecto a daños consecuenciales

El último apartado trata formas de cobertura que se sitúan fuera del ámbito clásico del seguro de equipos electrónicos. Todas tienen en común que hasta la actualidad no se ofrecen en el mercado y que en realidad se acercan a los ramos del seguro de fraude o de responsabilidad civil. Su problemática se comentará sólo brevemente.

Seguro de "Tarifas de comunicación"

El usuario paga a su proveedor de servicio una tarifa de uso, convenida contractualmente, que a menudo depende - como es el caso en telefonía - de la intensidad y duración del uso. Pero, ¿qué pasa si el usuario no ha utilizado este servicio?.

El riesgo, de que la facturación contenga errores siendo así inválida, aún sería mínimo. Las sentencias dictadas por los tribunales sobre facturas de Telekom en el negocio de clientes particulares demuestran las dificultades de comprobación para ambas partes.

Más importancia reviste el riesgo del uso no autorizado de los servicios de proveedores a cargo de un usuario legal cuya palabra clave se ha descubierto. En este caso y desde la óptica del proveedor, es correcta la facturación.

Para el caso particular del servicio de telefonía existe ya un nuevo concepto de cobertura en el mercado estadounidense: el asegurador indemnizará la pérdida patrimonial que ha sufrido la empresa (tomador de seguro) debido al uso no autorizado de su instalación telefónica por "intrusos o hacker telefónicos", llamados "Phreaker". Las instalaciones telefónicas modernas pueden ser manipuladas desde el exterior, igual que las computadoras. Esto permite que externos puedan efectuar llamadas telefónicas a terceros vía el sistema, cargando la facturación de las tarifas acumuladas al título del sistema. Otras posibilidades semejantes de abuso existen - a pesar de medidas técnicas de protección - en los teléfonos celulares y las tarjetas "calling cards".

Una situación similar se da en caso de los ordenadores. Cualquier computadora, con la que se adquieren servicios a través de la red, está sujeta a manipulaciones por personas no autorizadas. Con este riesgo corre siempre el usuario, o sea el propietario legítimo. Los seguros de daños por fraude y sus coberturas derivadas, el seguro de ordenadores y de abuso de datos, sólo ofrecen posibilidades muy limitadas para transferir el riesgo a un asegurador.

Daños consecuenciales por "transmisión defectuosa".

Tanto los proveedores de servicio como sus usuarios y también los clientes de estos, pueden sufrir daños patrimoniales a consecuencia de las siguientes situaciones:

Ninguna transmisión (avería en la red)
Cuando se presentan averías en la red, los usuarios no pueden trabajar o bien sólo en forma limitada, con efectos negativos en las actividades comerciales o, peor todavía, causando una interrupción de los servicios. El tema ya se ha tratado en relación con las coberturas de daños por fallos.

Transmisión alterada (error de transmisión)
En la mayoría de las transmisiones se detectan automáticamente los eventuales errores con sistemas muy complicados y se corrigen mediante repetición. Si se presenta un fallo en estos mecanismos, es posible que los datos modificados de producción causen producciones equivocadas y, por consiguiente, un daño patrimonial al usuario. Si, debido a esta situación, el usuario no puede cumplir con sus compromisos, también quedarán afectados sus clientes.

Transmisión falsificada (dolo/manipulación)
Más probable que un error son las manipulaciones conscientes en la vía de transmisión, sea por motivos de sabotaje o enriquecimiento. El escenario de los datos modificados de producción puede ser citado también en el caso de actos de sabotaje. A las manipulaciones por motivos de enriquecimiento están particularmente expuestos los datos de transacciones financieras.

Transmisión "interceptada" (espionaje industrial)
A menudo, la escucha crea la condición previa para una penetración de la red por delincuentes con intenciones de manipulación. Esto no es imposible ya que se transmiten también los códigos de acceso, por ej. palabras de paso. Para los espías industriales la misma escucha de las informaciones puede resultar tan interesante como el fotocopiado de datos secretos de investigación. El afectado sufre un daño patrimonial cuando la competencia comercializa sus ideas de producto.

Es importante señalar que prácticamente cada usuario de equipos informáticos está sometido a este riesgo. En un ordenador no conectado en red se puede producir también un fallo, un procesamiento defectuoso de datos o una manipulación o escucha por terceros. La interconexión en red, sin embargo, multiplica esta probabilidad de daño en forma considerable. La red constituye un sistema altamente complejo y de difícil orientación y con ello es más susceptible a perturbaciones técnicas de todo tipo. Las líneas, los equipos y el mismo software de transmisión constituyen riesgos de fallo no existentes en caso de equipos informáticos sin interconexión en red. Para efectuar manipulaciones o espionaje en un ordenador aislado, el delincuente tiene que formar parte del personal o bien acceder físicamente a la localidad, es decir, entrar violentamente en la empresa. Si es posible acceder al ordenador a través de la red, puede utilizar su propio PC y el riesgo de ser descubierto se reduce considerablemente.

Riesgos de Responsabilidad Civil

Con respecto a los daños consecuenciales de una transmisión defectuosa aún no está muy claro hasta qué punto tienen que responder el carrier, el proveedor de servicio y el usuario entre sí y frente a terceros, por ej. los clientes del usuario. ¿Quién se responsabiliza de la protección contra escuchas?, ¿el carrier cuyas líneas probablemente son "permeables", o el proveedor de servicio que es el responsable de la codificación de los datos transmitidos, o

bien el usuario que debería elegir una palabra de acceso "razonable" y cambiarla regularmente?.

Los escenarios que posiblemente darán lugar a derechos de responsabilidad civil son idénticos a los mencionados:
- ninguna transmisión (PB de la red)
- transmisión alterada (error de transmisión)
- transmisión falsificada (dolo/manipulación)
- transmisión "interceptada"

Conclusión

Las redes de información, o sea la conexión de ordenadores a estructuras altamente complejas, parcialmente en estructuras de distribución internacional, implican nuevos riesgos para todos los participantes en el mercado. En particular, son los usuarios de servicios de telecomunicación los que quedan afectados de forma especial. Hace diez años, estos riesgos aún no existían en su envergadura actual.

En aquel tiempo se había concebido el seguro de equipos electrónicos (seguro de daños materiales, de soportes de datos o de software, seguro de incremento en los costes y de pérdida de beneficios) para instalaciones individuales y no para redes. Para las redes actuales de información se sigue ofreciendo todavía una cobertura básica suficiente del hardware (seguro de daños materiales) y de la información (seguro de software).

Pero ya en el caso de las coberturas por interrupción se aprecia claramente que existe una necesidad de ampliación para el futuro. Los conceptos actuales se basan en el hecho que el mismo tomador de seguro puede determinar su situación de riesgo y que depende solamente del funcionamiento de su propio equipo informático. Sólo existe una obligación de indemnización si la causa de la interrupción es un daño material cubierto. La dependencia de proveedores de servicio, carrier y eventualmente de proveedores de información, así como la posibilidad de una producción de averías independiente de daños materiales ya no se deberían descuidar más si no se quieren tener lagunas de cobertura que, en algunos casos, pueden amenazar la existencia de la empresa.

El uso no autorizado de servicios, las consecuencias de transmisiones defectuosas y los subsiguientes derechos a indemnización son riesgos adicionales que no pueden ser atendidos actualmente por la industria del seguro en forma de productos específicos.

Una vista general resumida de los servicios proporciona una mejor idea del mercado:

- Servicios de conmutación

transmisión en ráfagas, por satélite, de radio móvil, de datos, radiocomunicación, servicios de telefax, de buzón de correo, proveedores de internet, EDI (electronic data interchange = intercambio electrónico de datos), correo electrónico.

– Servicios de gestión de red
por ej. servicios de datos, redes corporativas

– Servicios de información
bancos de datos

– Servicios de transacción
por ej. sistemas de reserva
(aquí por eje. START)

– Servicios de procesamiento
por ej. Datev, debis, EDS, Info AG

– Servicios de telecontrol
Mando, control y mantenimiento remoto

La agrupación de posibles proveedores de información refleja a la vez los campos de empleo para autopistas de datos y multimedia:

Empresas turísticas, agencias de viaje, líneas aéreas, ferrocarriles, periódicos, editoriales, servicios regionales de información, bancos de datos.

Negocios, casas de venta por correo, otros prestadores de servicio, restaurantes (teleshopping)

Bancos (telebanco) aseguradores (venta directa)

Proveedores de TV (TV estándar, TV interactivo, vídeo-a-demanda, pay-per-view), telejuegos.

Proveedores de información (tele-entrenamiento, telelearning, teleteaching).

Proveedores de vídeoconferencias.

Teletrabajo (teleworking), telecooperación.

Christian Mehl
Director & Senior Consulting
de TESCON-TELA.

RIESGOS INFORMÁTICOS: ASEGURANDO LA CONTINUIDAD DE LOS NEGOCIOS

En el mundo cambiante en que vivimos, la informática se ha convertido en fuente de ventaja competitiva para las empresas, pero también en fuente de problemas. Desde el punto de vista de la gerencia de riesgos es lícito afirmar que hay causas de siniestros propias de la aplicación de las Tecnologías de la información a la vida socio-económica; sin ellas no se hubiera producido o, al menos, no con la misma amplitud y repercusión.

En esta ponencia se describen los riesgos informáticos que amenazan la continuidad de los negocios, sus causas finales, su impacto sectorial y las soluciones de que disponen las organizaciones para prevenirlos.

A finales del siglo XX vivimos en un mundo caracterizado por la rápida aparición de nuevas tecnologías, con ciclos de vida cada vez más cortos tanto en su desarrollo y comercialización como en su aplicación a la vida social y económica.

Parece claro que una fuente de ventaja competitiva para todas las empresas es el conocimiento y el uso y aplicación que de él se hace. Estamos viviendo una nueva revolución en la historia de la humanidad; estamos ante una nueva Era, la Era del Conocimiento. Y las tecnologías de la información no son ajenas a ello; más bien se han convertido en su instigador.

La informática y las demás tecnologías afines han invadido tanto la vida económica como la privada.

La seguridad de la información, tanto desde el punto de vista de la confidencialidad como de la integridad, consistencia y disponibilidad de la misma, es una necesidad de primer orden; las implicaciones sobrepasan al plano socio económico y alcanzan a la propia ética.

Voy a centrar esta exposición en el mundo empresarial. Estamos asistiendo al nacimiento de un nuevo modelo de negocio, mucho más competitivo, que requiere una integración más estrecha entre las Tecnologías de la Información y los procesos de trabajo. Como consecuencia de ello, el papel de los departamentos de informática en las organizaciones está cambiando.

La informática ya no es una mera herramienta de soporte a los procesos administrativos y operaciones repetitivas, sino que se ha convertido en un mecanismo de transformación organizativa e, incluso, de rediseño del propio negocio.

La variedad creciente de sistemas de información, la distribución de los mismos y el uso intensivo que de ellos se hace en el mundo empresarial ha hecho de las Tecnologías de la Información una herramienta estratégica para la sostenibilidad del negocio. Y como tal, no sólo sujeta a los riesgos a los que cualquier bien empresarial está expuesto (daños materiales, robo, gastos suplantarios, ...) sino también a otros relacionados con las consecuencias que de un mal uso o funcionamiento de la misma se puedan derivar para la vida económica de la empresa.

Todos los profesionales del sector asegurador tienen una larga experiencia en medir las probabilidades de un siniestro y en el nivel de las consecuencias que se pueden derivar de éste, pero cuando estamos hablando de riesgos informáticos que pueden poner en serio peligro la continuidad de las actividades de la empresa es cuando el papel del Gestor de Riesgos cobra un protagonismo especial. El avance tecnológico supone para éste último la identificación constante de nuevos riesgos, su evolución previsible, la planificación del control de los mismos y los planes de monitorización de los sucesos potenciales. Y todo ello en unos escenarios de carácter multiforme, con una gran complejidad operativa, con multiplicidad de arquitecturas y sin base documental de mejores prácticas.

La emergencia de los riesgos informáticos, manifestaba desde principios de esta década, tiene su origen en los siguientes hechos:

A. Los sistemas de información y control de las empresas están cada vez más automatizadas e integrados entre sí.
B. Las aplicaciones informáticas incorporan cada vez más inteligencia del negocio.
C. El desarrollo de las Tecnologías de las Comunicaciones hace que los sistemas informáticos tienden a estar interconectados en tiempo real, tanto intrínseca como extrínsecamente a cada organización.
D. La evolución vertiginosa de las Tecnologías de la Información y su incorporación rápida al mercado para amortizar las costosas inversiones en I+D que se ven obligados a hacer todos los fabricantes, provoca el uso de técnicas poco maduras, no dominadas totalmente ni en el fondo ni en la forma. Además, este hecho se ve agravado porque la experiencia del pasado vale poco para el futuro.
E. Tanto el hardware como el software siguen siendo costosos y, además, su complejidad técnica aumenta.
F. La información es uno de los activos más importantes de todas las organizaciones. Para un gran porcentaje de ellas tiene, incluso, un valor monetario precisamente tasado.
G. Debido a su carácter estratégico dentro de todas las compañías, la informática puede ser objeto de hechos vandálicos y terroristas como medio de perjudicar los intereses empresariales. Estos pueden ser cometidos por agentes internos o externos a la organización en beneficio de individuos aislados o de colectividades.

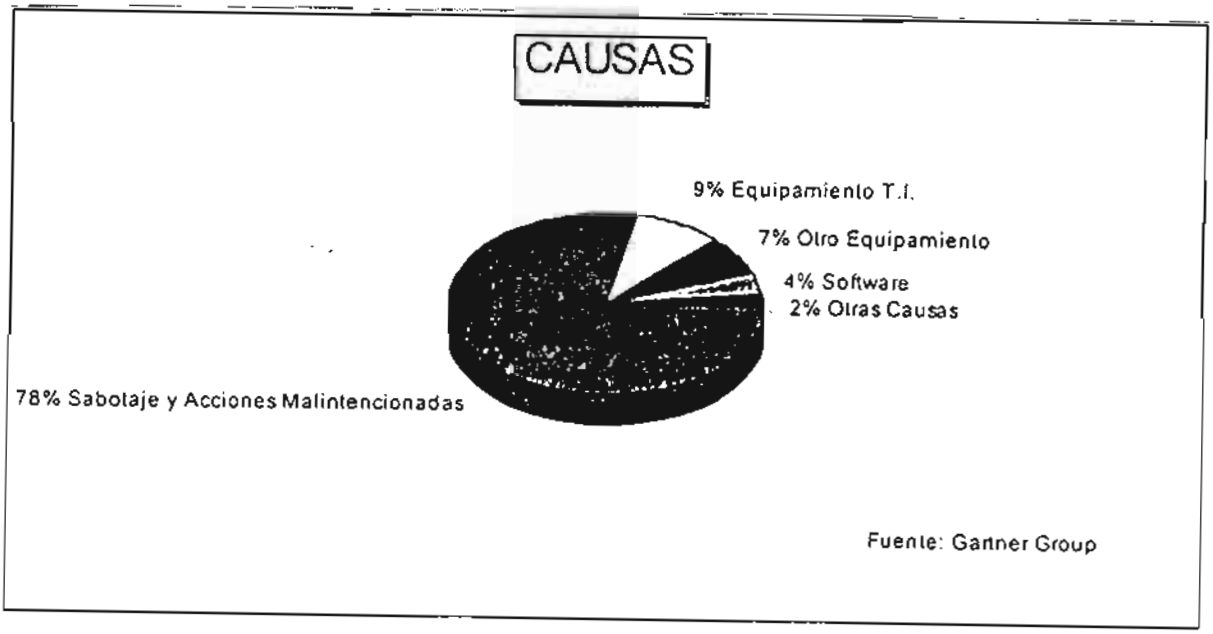
H. En muchas organizaciones la informática todavía es, por desgracia, un mundo aparte en donde los intereses de sus profesionales pueden no estar alineados con los objetivos del negocio. Este hecho puede provocar diferencias en el análisis multidisciplinar preciso para evaluar las consecuencias que toda acción, tanto originada por los técnicos como por los usuarios, puede tener de cara a prever los riesgos que conlleva.
I. El aseguramiento de la calidad en los procesos de desarrollo y de producción de sistemas de información es todavía muy incipiente. En una actividad con un alto componente tecnológico, las labores de diseño y construcción de software son, aún hoy, muy artesanales. La calidad del sistema sigue estando directamente relacionada con la calidad de sus diseñadores y usuarios; el riesgo de error todavía es grande...¡ Y sus consecuencias no bien analizadas!.

Seguramente hay algunos hechos más, no detallados aquí, que agravan el problema. Pero hay uno que, sin lugar a dudas, puede interesar a los gestores de riesgos: la informática desempeña el papel de amplificar de los siniestros. Cualquier organización, cualquier proceso de trabajo ve modificados sus mecanismos de prevención y de protección cuando se aplican las Tecnologías de la Información a los mismos. A día de hoy es lícito afirmar que hay causas de siniestros propias de la aplicación de la Informática a la vida socio económica; sin ella no se hubiera producido o, al menos, no con la misma amplitud y repercusión.

CAUSAS FINALES DE LOS RIESGOS INFORMÁTICOS

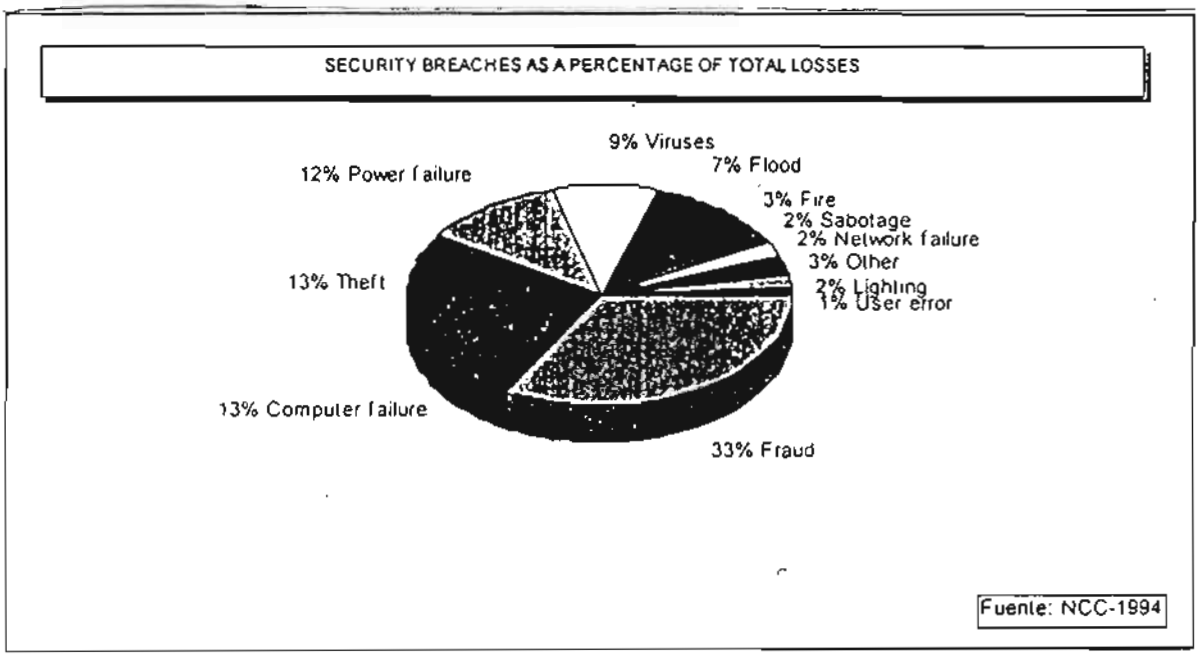
Si analizamos las causas que han originado los siniestros habidos a nivel mundial y, pese a la dificultad que entraña obtener estadísticas de este tipo, podemos aventurar que:

* Solamente un 13 por cien están originados por equipos (9%) y software (4%).
* Un 78 por cien tienen su origen en acciones malintencionadas y sabotajes cometidos tanto por elementos ajenos a las organizaciones como por personal de las mismas.
* El 9 por cien restante tiene su origen en fallos habidos en otro equipamiento de la empresa (7%) y en otras causas no clasificables dentro de los puntos anteriores.



TIPOS DE SINIESTROS, PÉRDIDAS ECONÓMICAS Y FRECUENCIAS

A partir de las conclusiones derivadas de la encuesta realizadas en 1994 en el Reino Unido por el National Computing Center (NCC) puede construirse el siguiente gráfico:



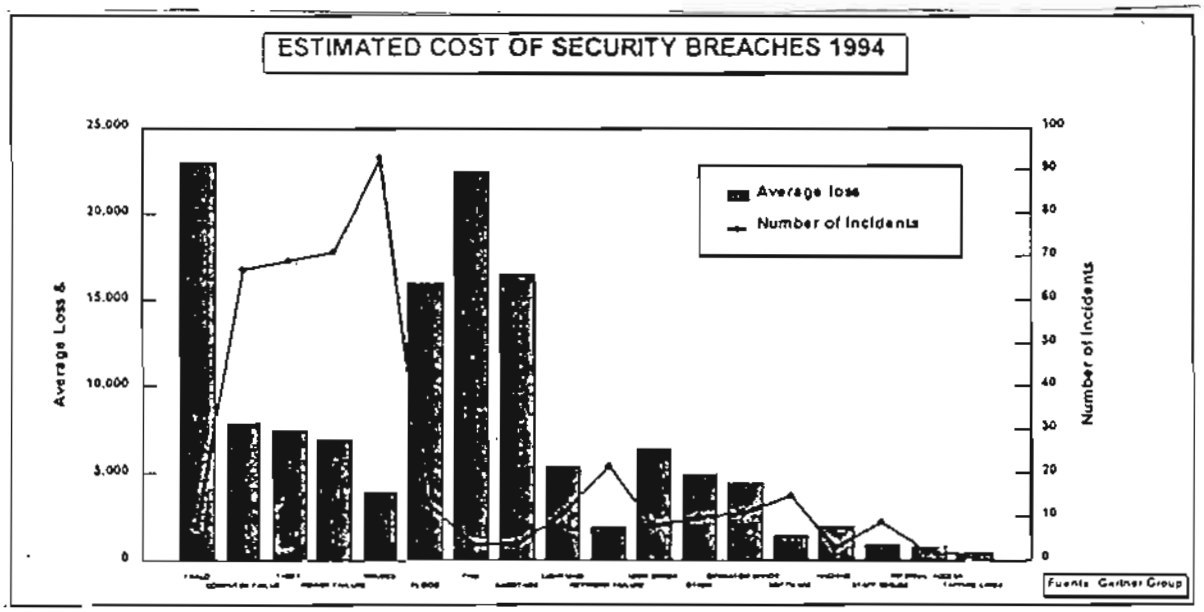
Siempre con la precaución de que la estadística que mostramos está basada en la información que, voluntariamente, los damnificados por los siniestros han reportado al NCC y que puede haber hechos no registrados en el cómputo, se concluye que del total de pérdidas por siniestros informáticos:

* el 33 por cien son debidas a acciones fraudulentas.
* el 13 por cien de las pérdidas son debidas a fallos en los sistemas de ordenador.
* el 13 por cien a robos.
* el 12 por cien a fallos en el suministro de corriente eléctrica.
* el 9 por cien a la contaminación por algún tipo de virus de los sistemas microinformáticos.
* el 7 por cien de las pérdidas es imputable a siniestros provocados por inundaciones y/o avenidas de agua.
* el 3 por cien a incendios.
* el 2 por cien es imputable a los daños ocasionados por sabotaje.
* Otro 2 por cien es imputable a fallos en la red de comunicaciones.
* Una cantidad de pérdidas similar, en porcentaje, a las anteriores es imputable a las descargas eléctricas provocadas por fenómenos atmosféricos de carácter tormentoso.
* ¡Solamente por fortuna, un 1 por cien de las pérdidas es imputable a causas relacionadas con el mal uso del sistema!.
* Y el 3 por cien restante de las pérdidas se pueden clasificar en el apartado de otras causas no contempladas en las anteriores.

Si consideramos sobre la misma base estadística el número de casos registrados, podemos concluir que no existe una relación directa entre el número de siniestros y el valor medio al que asciende la pérdida económica que de ellos se deriva.

Así, por ejemplo, los casos existentes de contaminación por virus son muy elevados y, sin embargo su repercusión económica es francamente pequeña. En el polo opuesto se encuentran casos como el fuego o el sabotaje, con pocas ocurrencias pero con una repercusión económica elevadísima.

En el siguiente gráfico puede consultarse el número de siniestros habidos frente a la perdida económica media que se deriva de ellos, siempre según el estudio realizado por el NCC.



No obstante, esta estadística puede ser significativamente distinta entre unas zonas geográficas y otras.

Es evidente que un factor importante a considerar es el riesgo de exposición a desastres naturales - terremotos huracanes y tornados, ... - de la región donde se ubica el Centro de Proceso de Datos de cada empresa. También deben considerarse otros factores más relacionados con la situación política y de clima social, a la hora de evaluar los riesgos potenciales.

LA DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN

La gran cuestión a la que deben dar respuesta los departamentos de informática de todas las organizaciones ante los riesgos que, como hemos expuesto anteriormente, el uso y aplicación de Tecnologías de la Información al mundo empresarial conlleva el ¿Cómo garantizo el cumplimiento del nivel de servicio a toda mi organización?.

El nivel de servicio es la medida, universal y objetiva, por la que se valora la función informática en cualquier compañía. El departamento de informática es, no sólo el garante de la consistencia, integridad y confidencialidad de la información, sino también del rendimiento de los sistemas de información y de la disponibilidad de ésta última para el usuario.

Y todo estos aspectos influyen decisivamente en el nivel de riesgos que una instalación informática presenta.

Los aspectos de seguridad, tanto física como lógica, de una instalación y de la confidencialidad de la información en ella contenida y manipulada son aspectos muy trillados - incluso alguno de ellos sometidos a la legislación -, comprendidos y soportados por lo que no haremos más que mención de ellos en esta exposición.

Otro tanto ocurre con los aspectos relacionados con el rendimiento de los sistemas de información. Los diseñadores y programadores de éstos cada día están más concienciados de que sus trabajos no solamente debe ir orientados a conseguir la funcionalidad requerida por el usuario, sino que también deben contemplar las características de la instalación en donde las aplicaciones que construyen deben ejecutarse, con el fin de que los diseños físicos de las mismas aprovechen al máximo sus capacidades, pero siempre minimizando los recursos requeridos. Los técnicos de sistemas, por otra parte, siempre han orientado sus esfuerzos a gestionar de manera óptima los recursos físicos disponibles en la instalación en relación con el uso de que ellos se demanda.

Ahora bien, el concepto de disponibilidad, y la problemática que le rodea, es mucho más disperso, menos conocido y menos comprendido, incluso por los profesionales del sector.

La disponibilidad absoluta de cualquier sistema de información no existe, de la misma manera que el ser humano no puede controlar la naturaleza o las acciones de otros semejantes suyos; lo que si puede hacer es prever los riesgos que le acechan y dotarse de los medios necesarios para alcanzar ciertos niveles de seguridad en relación a esos riesgos y amenazas. Y en el mundo de la tecnología pasa exactamente igual.

Entendemos por disponibilidad del sistema de información la cantidad de tiempo que éste está funcionando respecto del nivel de servicio comprometido con el usuario. Este término está mediatizado por dos conceptos:

* El mantenimiento preventivo y planificado de los recursos informáticos, a nivel de hardware, software y de otros.
* Los fallos o contingencias imprevistas en cualquiera de sus componentes.

Una mala estrategia de mantenimiento puede derivar en un incremento del riesgo de contingencias para la instalación. Y, evidentemente, éstas últimas pueden ir desde el nivel de un pequeño problema que afecta a cualquiera de los componentes del sistema de información, subsanable en pocos minutos, hasta un desastre general en el Centro de Cálculo que lo inhabilite durante días, semanas o, incluso, meses.

¿Nos hemos preguntado que ocurriría en cualquier empresa con un alto grado de información de sus procesos si esto último ocurriera? Evidentemente repercutiría de una manera grave en su negocio y no sería extraño que, incluso, pudiera comprometer su supervivencia. Es evidente la necesidad que manifiestan todas las organizaciones de disponer de una estrategia de prevención y de recuperación ante desastres.. Hablamos más adelante de ello.

La clase de eventos que pueden provocar falta de disponibilidad en un Centro de Cáculo se categorizan en tres grandes grupos:

* Mantenimiento preventivo.
* Contingencias resolubles a nivel local.
* Desastres.

En el grupo del mantenimiento preventivo se incluyen todas aquellas actividades necesarias para realizar pruebas, modificaciones u operaciones de salvaguarda de información, necesarias para evitar la rotura de componentes. Se pueden incluir aquí otro tipo de actividades encaminadas a dotar a la instalación de los medios y procedimientos necesarios para recuperar la información en caso de anomalía.

A día de hoy existen métodos y tecnología suficientes cómo para garantizar la disponibilidad del sistema, aun cuando estas operaciones se realicen en instalaciones con niveles de servicio comprometido 24 x 7 (veinticuatro horas durante los siete días de la semana, es decir, todo el año sin parar).

En el grupo de las contingencias resolubles a nivel local distinguimos, a su vez, dos subcategorías:

* Punto de fallo
* Frecuencia de fallo

Desde el punto de vista del punto de fallo, se consideran:

* Cortes en el fluido eléctrico
* Averías en elementos anejos al sistema

* Fallos del hardware, tanto del sistema de ordenador como de su periferia.
* Fallos de las comunicaciones.
* Fallos en el sistema operativo y en los subsistemas.
* Fallos en las aplicaciones, bien sean éstas de desarrollo propio, paquetes estándar o desarrolladas a medida por terceros.

Desde el punto de vista de la frecuencia de fallo podemos considerar los siguientes:

* Fallos recurrentes por error de un componente del sistema, cualquiera que sea éste.
* Fallos puntuales motivados por la baja calidad del componente afectado.

En el grupo de Desastres encuadramos todas aquellas contingencias no resolubles a nivel local. Este tipo de contingencia está relacionado con eventos de carácter violento e inesperado que inhabilitan los recursos informáticos de la organización durante un largo período de tiempo.

MEJORA DE LA DISPONIBILIDAD DE LOS SISTEMAS

¿Cómo podemos protegernos para minimizar los efectos de cualquiera de los siniestros anteriormente descritos?.

Evidentemente diseñando los procedimientos y métodos de trabajo adecuados, las arquitecturas de sistemas idóneas e invirtiendo las cantidades económicas necesarias para dotar a la instalación de las tecnologías y recursos humanos requeridos para garantizar los niveles de disponibilidad objetivo.

Existen cuatro niveles de protección que mejoran la disponibilidad, minimizando el impacto de las contingencias resolubles a nivel local.

* Nivel básico.

Puede ser obtenido con un sistema único y unos procedimientos primarios de gestión. La selección de un software y hardware fiables puede ayudar a mejorar la disponibilidad.

* Nivel mejorado.

Basada, también, en un sistema único se dota de mayor robustez mediante la aplicación o redundancia de algún componente del mismo (discos espejados, discos substituibles en caliente, fuentes de alimentación continúa, log de datos/transacciones, etc...). Es evidente que para alcanzar este nivel es necesario disponer de una rigurosa gestión del sistema.

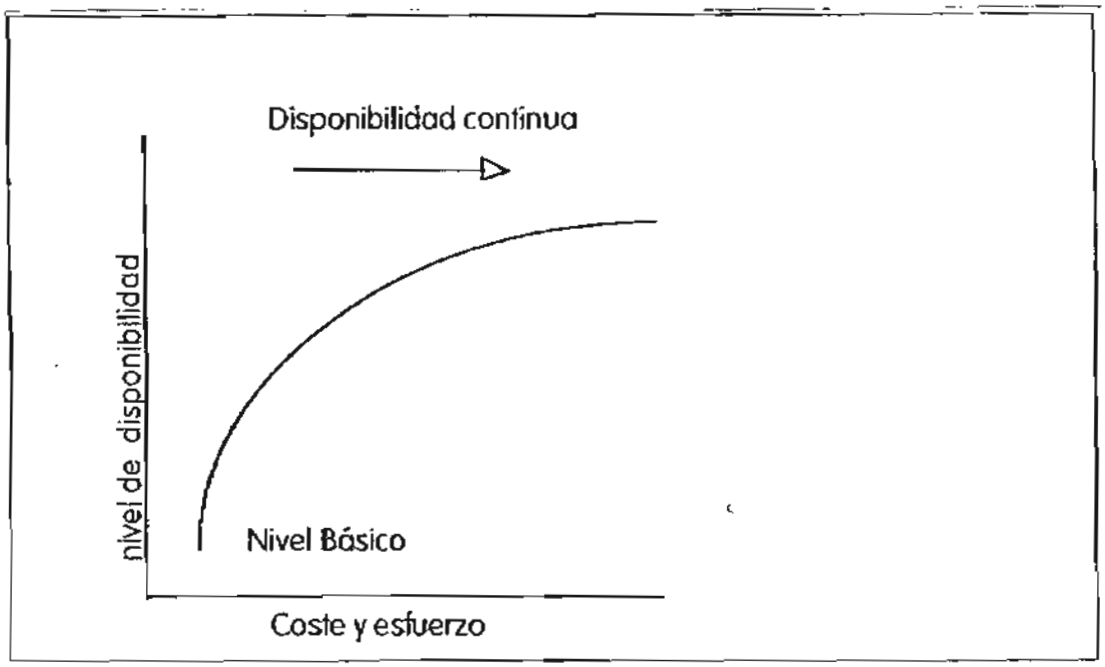
* Alta disponibilidad

En este nivel se intenta dotar a la instalación de los sistemas hardware y software necesarios para suministrar un servicio continuo dentro de una ventana temporal determinada. Generalmente se requiere un alto grado de redundancia en los componentes del sistema de cara a protegerlos de cualquier fallo. Deberá utilizarse una correcta tecnología para automatizar los procesos de recuperación y minimizar los requerimientos de tiempo necesario para ejecutarlos.

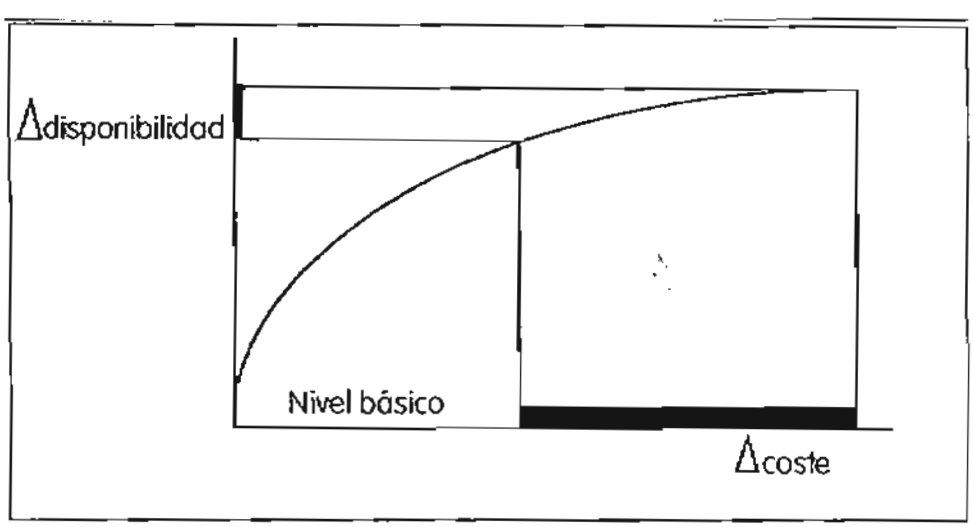
* Disponibilidad continua.

En este nivel, el Sistema debe ofrecer servicios de forma permanente, incluso ante casos de cambio de procesos y de recuperación de errores. La redundancia de todos los componentes del sistema es vital para conseguir este nivel.

Ante todo este programa, la disponibilidad se ve como una función continua definida por los valores "coste y esfuerzo" (eje de abcisas) y su contraprestación del nivel de disponibilidad alcanzando (eje de ordenadas).



Con relativamente pocas inversiones pueden conseguirse mejoras importantes en la disponibilidad del sistema. A medida que tendemos a la disponibilidad continua el coste crece exponencialmente.



LA RECUPERACION ANTE DESASTRES

A lo largo de la exposición anterior hemos visto como los Centros de Cálculo son en la actualidad componentes críticos para el funcionamiento de cualquier organización, sea cual sea el sector en el que desarrolla su actividad. En consecuencia, la recuperación de sus operaciones en caso de fallo no resoluble a nivel local, constituye una actividad crítica para el negocio.

La recuperación de desastres implica un conjunto de procedimientos, políticas y productos que permitan la reanudación en un tiempo limitado de los elementos informáticos asociados a los procesos de negocio de la empresa, tras una interrupción significativa del servicio.

La presunción fundamental que existe detrás de todo plan de recuperación de los procedimientos habituales de gestión implica tanto a las unidades de soporte al proceso de datos como a todas las unidades de la entidad que utilizan para su trabajo las aplicaciones informáticas que se procesan en la instalación siniestrada.

Estas últimas deben contar, en función de las previsiones de recuperación del servicio con:

* Los procedimientos de gestión alternativos que deberán emplear hasta que el servicio informático se restaure.
* Los procedimientos de recuperación de datos ante eventuales pérdidas de información, resultantes del intervalo de tiempo transcurrido desde el momento en que se obtuvo la última copia de seguridad válida para proceder a la recuperación del servicio, y el momento del siniestro.

Por otra parte, las unidades de soporte al proceso de datos deben disponer de un conjunto de procedimientos que permitan recuperar las bases de datos y que garanticen la posibilidad de reanudación de los procesos.

Hay varias soluciones para proteger los recursos informáticos críticos. Esas incluyen un rango muy amplio de costes y de tiempo necesarios para el proceso de recuperación.

* Espera caliente

El medio ambiente de esta solución es una instalación cuya utilización está exclusivamente dedicada a la recuperación después de un desastre. No tiene ningún otro uso. Esta instalación puede tener una imagen duplicada del sistema de información completo o, solamente, una parte de éste con la funcionalidad más crítica.

* Sombra de la base de datos

En este caso, la información nueva se manda sobre una red local a una copia remota tan pronto como sea posible. Esta acción es asíncrona respecto a la actualización en el sistema primario, por lo que puede haber inconsistencias entre las bases de datos en el momento del siniestro.

* Espejo de la base de datos

En un sistema con espejo de la base de datos, la información nueva se actualiza de manera síncrona en los sistemas primario y secundario. Puede, por tanto, tener un impacto significativo en el rendimiento del sistema principal, pero garantiza que su copia es exacta en caso de desastre.

* Almacenaje y edición del sistema operativo

En esta solución se mantiene una imagen del sistema operativo de producción en un disco del sitio remoto dedicado a la recuperación de desastres. Después de un siniestro, se utiliza esta imagen para iniciar el sistema de la "espera caliente". Este método es más rápido que el proceso de restaurar la imagen de las cintas de reserva.

* Traslado electrónico de grandes paquetes de datos

Este traslado consiste en mandar, a través de la red de comunicaciones, las copias de los datos críticos de la instalación al sitio remoto. Evidentemente este proceso optimiza los tiempos necesarios para el transporte de la información y elimina el trasiego de cintas entre las instalaciones.

* Sitio caliente/Sitio frío

Los sitios calientes/fríos son facilidades de proceso de datos alternativos, donde se puede reconfigurar el medio ambiente del sistema primario si ocurre un desastre. El tiempo necesario para recuperar el sistema es variable, en función de la complejidad de la instalación siniestrada.

Ahora bien, ante tanta opción, el dilema que se plantea a los profesionales de las tecnologías de la información es escoger aquella solución que mejor se adapte a las necesidades de su empresa y que, garantizando la recuperación de los sistemas, minimice el coste total de propiedad de éstos últimos.

Para ello, lo primero que debe hacer es preguntarse.

1. ¿Qué características de servicio al cliente presenta mi negocio?.
2. ¿Cuáles son los sistemas de información críticos en la organización?.
3. ¿Cuánto tiempo es posible operar sin sistemas de información hasta que el servicio pueda ser restablecido?.
4. Una vez restablecido el servicio, ¿Cuál es el tiempo máximo que la empresa puede soportar con una situación de contingencia en su proceso de datos?.

Seguramente con estas respuestas en la mano y con el conocimiento profundo de las distintas soluciones que la tecnología ofrece a día de hoy, podrá aproximar su mejor opción. No obstante, antes de tomar una decisión definitiva, sobre la solución escogida debería constatar:

* La integridad de la información que provee.
* El nivel de automatización de los procesos de notificación de fallos y de toma de control por una segunda máquina en caso de que estos ocurran.
* El tiempo de demora necesario para la restauración del servicio.
* La distancia máxima admisible para la ubicación de un centro de respaldo.
* La escalabilidad del sistema.
* La relación coste del tiempo perdido a causa del siniestro, comparado con los costes de instalación y mantenimiento del sistema de salvaguarda.
* La eficacia y eficiencia de la solución en el proceso de restauración del servicio.

UNA VISIÓN SECTORIAL

Los distintos sectores de actividad económica presentan diferentes grados de necesidad para adoptar una solución de recuperación ante desastres.

Pese a que no existe una legislación específica que regule tales salvaguardas, si existen ciertas características de los negocios que ejercen una presión considerable sobre la dirección de las empresas a la hora de diseñar, desarrollar, probar e implantar una solución de recuperación.

* La banca de negocios tiene la presión de los auditores y de los bancos centrales para operar de manera continua.
* Además de ello, la banca de particulares necesita de continuidad en las ventas, tanto directas como a través de medios electrónicos.
* El mundo del Seguro también necesita de continuidad en las ventas.
* Para el sector de fabricación es vital asegurar el control de los stocks para garantizar el "Just in Time" de su producción así como el asegurar la distribución de los bienes fabricados.
* Para el comercio, el aseguramiento de su cadena logística es vital para la continuidad de su negocio. Esto incluye desde el aprovisionamiento hasta la venta.
* El sector transporte necesita la continuidad en las operaciones de venta de billetaje y en la logística de materiales de mantenimiento, como parte fundamental de la seguridad de los viajeros.

Como consecuencia de las características y presiones anteriores, a nivel mundial, las distintas industrias presentan grados de necesidad diferentes a la hora de considerar la recuperación ante desastres:

* Banca, Seguros y Comercio encabezan el ranking de "sectores más necesitados".
* Transportes y Fabricación presentan menores índices de necesidad.

Sin embargo, solamente la banca - tanto la de particulares como la de negocios - está preparada para la recuperación ante desastres en la misma que los requerimientos y características de su actividad empresarial manifiestan.

También hablando en términos generales, podemos tipificar las soluciones técnicas utilizadas en cada uno de los sectores.

* El mundo de la Banca de negocios necesita restaurar rápidamente sus operaciones, aunque no hasta el punto inmediatamente anterior al siniestro. Por lo general, aplican soluciones de sitio caliente/sitio frío.

* Tanto el mundo de la Banca de particulares como el Comercio necesitan restaurar rápidamente (en menos de 2 horas) sus operaciones hasta el punto inmediatamente anterior al siniestro. Por lo general, una solución mixta de segundo centro de proceso, con bases de datos espejo y sistema en "espera cliente" es la que típicamente aplican.
* El sector asegurador, por contra, no tiene especiales necesidades de velocidad de recuperación de la contingencia, aunque si de restaurar los sistemas hasta el momento en el que el siniestro de produce. Es usual la aplicación de técnicas de salvaguarda de los datos en cinta o disco para su restauración en caso de siniestro y de espejo de las bases de datos.

Este panorama tiene su correspondiente reflejo económico. Mientras, según datos de Giga Group, la media del gasto anual en recuperación de desastres de todos los sectores económicos es de un 3 ó 4 por cien del Total de gastos en informática, en la banca esta cantidad llega a elevarse hasta el 7 por cien.

Si analizamos en detalle estos datos, podemos concluir que el incremento de gastos viene motivado, entre otras cosas, por el uso intensivo que de los sistemas de telecomunicación ha de hacer la Banca para alcanzar sus garantías de respaldo ante desastres.

PLAN DE RECUPERACIÓN DEL NEGOCIO VERSUS RECUPERACIÓN DE DESASTRES

El Plan de Recuperación de Desastres encaja dentro del un Contexto más amplio de reanudación completa del negocio. Tradicionalmente, el primero de ellos se centra en la recuperación de los sistemas de información; el segundo se deriva de la conciencia, cada vez mayor, de la necesidad imperativa de continuar la operación de los negocios de empresa.

Este modelo de continuidad del negocio pretende asegurar que una interrupción inevitable del mismo sea transparente a los elementos clave de la compañía, incluyendo clientes, proveedores, accionistas y empleados.

Así, el modelo completo de continuidad del negocio, puede estructurarse de la siguiente manera:

Las diferencias entre la recuperación de desastres y la continuidad del negocio estriban, más que en el "Qué hay que hacer", en el "Quien es el responsable de hacerlo".

La continuidad del negocio afecta a toda la compañía, no sólo al Centro de Cálculo y a los responsables de los sistemas de información; pone énfasis en la capacidad de recuperar la funcionalidad, no sólo en las aplicaciones informáticas; implica un proceso para establecer prioridades de negocio, no de salvaguarda de los sistemas informáticos exclusivamente en los aspectos tecnológicos y de relación entre los técnicos y los usuarios finales.

D. Juan Andrés Pro
División de Sistemas y Servicios
Director
Informática El Corte Inglés

AÑO 2000: ASPECTOS RELACIONADOS CON LOS SEGUROS

Recientemente tuve la oportunidad de preparar un análisis sobre el problema de referencia relacionado con los seguros. Aunque está redactado desde el punto de vista estadounidense, creo que puede serles útil para definir sus propias cuestiones.

Objeto

Este documento servirá para proporcionar un panorama general sobre la manera en que las coberturas de seguro existentes y propuestas pueden relacionarse con el problema Año 2000.

Resumen

- **El Seguro de Responsabilidad Civil para Directores y Ejecutivos (D&O)** proveerá cobertura para la responsabilidad civil proveniente de alegaciones de conducta negligente, incurrida por directores y ejecutivos a título individual. Ni el seguro D&O ni los seguros en general cubren las responsabilidades que puedan surgir de actos delictivos intencionados ni las sanciones relacionadas con los mismos. (Es importante advertir que los ejecutivos de una empresa pueden prestar servicios como directores de otras entidades, a solicitud de su propia empresa. Dado que estas otras entidades también pueden tener problemas relacionados con el Año 2000, tanto los ejecutivos como la empresa están potencialmente expuestos).

- **Nuevas coberturas para Excesos de Pérdidas/Pérdidas Catastróficas.** El año pasado se crearon nuevas coberturas para Excesos de Pérdidas/Pérdidas Catastróficas que, entre otras cosas, pueden proveer a los directores y ejecutivos cobertura para excesos de pérdidas con relación al Año 2000.

- **Cobertura corporativa de responsabilidad profesional y de errores y omisiones.** Como se indica anteriormente, el seguro D&O responde en caso de acciones judiciales entabladas contra personas físicas, pero no contra la corporación. Algunas empresas adquieren un seguro de responsabilidad profesional para cubrir las pérdidas que puedan surgir de alegaciones contra la propia empresa por errores y omisiones cometidos en el curso de la prestación de servicios. Si se tiene, esta cobertura podría aplicarse a las acciones judiciales contra la corporación relacionadas con el Año 2000. (Muchas empresas consideran que este seguro no es rentable como seguro primario, y por lo tanto no lo adquieren).

- **Seguro contra interrupción de negocios.** El seguro contra la interrupción de los negocios constituye una extensión de la cobertura contra daños materiales. Los daños materiales constituyen el factor esencial que activa la cobertura. Si no hay daños materiales, este seguro no cubriría una interrupción de negocios causada por el problema Año 2000.

- **Cobertura Combinada de Responsabilidad Civil General y Complementaria**, que se aplica a la responsabilidad civil incurrida cuando el asegurado, actuando con negligencia, es causa de que un tercero sufra daños corporales, daños materiales o daños personales, p.ej.: difamación, calumnia. La cobertura se aplica a sucesos definidos como accidentes inesperados. Esta cobertura potencialmente puede aplicarse a daños corporales y materiales resultantes del mal funcionamiento de una computadora en la medida en que dicho mal funcionamiento no pudo haber sido previsto. Esta cobertura también puede estar incluida en la sección "Productos u Operaciones Terminadas". No obstante, las aseguradoras en la actualidad están promulgando restricciones a esta cobertura.

- **Coberturas de seguros recientemente creadas**, cuyo objetivo específico es cubrir las exposiciones a riesgo relacionadas con el problema Año 2000, están siendo anunciadas por las principales corredurias. Las coberturas ofrecidas, que comentaremos en detalle, cubren la responsabilidad corporativa y personal, la Interrupción de Negocios sufrida por la propia empresa y la interrupción contingente de los negocios de un tercero del que dependa la empresa.

ANÁLISIS

Seguro de responsabilidad civil para Directores y Ejecutivos

Antes de atender en concreto el problema Año 2000, es necesario analizar el carácter de este insólito tipo de seguro. Normalmente, una póliza de seguro D&O ofrece dos coberturas distintas. Esto se deriva del hecho de que la mayor parte de las responsabilidades que pueden ser incurridas por los directores y ejecutivos a título individual en el desempeño de sus funciones son indemnizables por la empresa. No obstante, bajo ciertas, circunstancias, tales como una acción judicial secundaria iniciada por accionistas, se impide a la empresa que indemnice en última instancia a directores y ejecutivos específicos, si se determina que los mismos son responsables. Por estas razones, la cobertura responde sobre dos bases distintas. Si la empresa puede indemnizar, la aseguradora responde por la cantidad indemnizable por la empresa, sujeta a un deducible. Si la empresa no puede indemnizar, la aseguradora responde por la pérdida incurrida directamente por los directores o ejecutivos, por lo general sin que se aplique ningún deducible. En el segundo caso, el seguro constituye la única fuente de fondos disponible que no sean los bienes personales de los directores o ejecutivos.

La póliza D&O cubre la responsabilidad civil incurrida como consecuencia de la comisión de actos erróneos, que se definen normalmente como sigue:

> "Todo incumplimiento de obligación, negligencia, error, declaración errónea, declaración engañosa, omisión u otro acto perjudicialmente cometido o intentando por los Asegurados, o toda alegación de un demandante de que los asegurados han cometido uno de los anteriores actos, o toda demanda presentada contra los asegurados únicamente por el hecho de ser éstos Directores y Ejecutivos de la compañía".

Esta cobertura se centra en la negligencia y sería aplicable a muchas de las responsabilidades individuales identificadas por los asesores jurídicos, tales como el incumplimiento del deber fiduciario.

No obstante, esta cobertura no responde contra responsabilidades que pueden surgir de las acciones ilícitas intencionadas, p.ej.: la negociación bursátil utilizando información confidencial (insider trading), consistente en la venta de un número considerable de acciones con anterioridad al 1ro. de enero del año 2000, realizada por directores o ejecutivos que tengan información sobre un problema que no sea de dominio público.

La sección de la póliza que ofrece cobertura individual contiene normalmente la siguiente exclusión:

> "La aseguradora no será responsable de efectuar pagos relacionados con reclamaciones presentadas contra los Asegurados basadas en o atribuibles a que los mismos obtengan, de hecho, cualquier beneficio o ventaja personal a los que no tengan derecho legalmente".

Aunque la sección del contrato de seguro que ofrece cobertura corporativa puede no contener esta exclusión específica, por lo general se considera contrario a la normativa el que un seguro cubra actividades ilícitas intencionadas. En este sentido, ambas secciones de la póliza expresamente excluyen de la cobertura lo siguiente:

> "...multas o sanciones impuestas por la ley u otros casos que puedan considerarse no asegurables de acuerdo con la ley bajo la cual se interprete esta póliza".

Con respecto a la posibilidad de que los directores y ejecutivos especulen con los títulos valores de la empresa p.ej.: compraventas a corto plazo, la póliza normalmente contiene una exclusión similar a la siguiente:

> "La aseguradora no será responsable de efectuar pagos relacionados con reclamaciones presentadas contra los Asegurados para que den cuenta de los beneficios efectivamente obtenidos de la compra o venta de títulos valores de la Compañía por parte de los Asegurados... Según el Artículo 16(b) de la Ley del Mercado de Valores de 1934, según enmendada, o disposiciones similares de cualquier ley estatal estatutaria".

(Algunas empresas de hecho mantienen un seguro que cubre ciertos tipos de pérdidas que pueden surgir de los actos ímprobos y delictivos cometidos por empleados y otras personas. No obstante, estas coberturas tienen poca aplicabilidad al problema Año 2000).

Con respecto a la divulgación del problema Año 2000 a la aseguradora, las empresas aseguradas presentan periódicamente solicitudes actualizadas que incluyen informes financieros, p.e.:, la memoria anual, los informes 10K y 10Q, etc. Las aseguradoras son plenamente conscientes del problema Año 2000 como lo demuestran su afán en crear nuevos productos para resolver el problema.

La membresía en el directorio de otras empresas también puede representar una considerable exposición a riesgo. Muchos ejecutivos prestan servicios como directores de otras empresas. Según las condiciones de cobertura que figuren en la póliza de la empresa, si tal servicio se presta a petición por escrito de la empresa, pueden ser aplicables tanto la indemnización de la empresa como el seguro D&O, además de la indemnización y el seguro de la otra empresa. Quizás algunas de estas otras empresas no dispongan de los recursos necesarios para hacer frente al problema Año 2000 por encima de un cierto nivel. Se debe alertar sobre esta cuestión a los ejecutivos y directores que presten servicios como directores de estas empresas.

Aunque han circulado algunos rumores sobre posibles exclusiones del problema Año 2000 en las pólizas D&O, las coberturas D&O contratadas por un plazo de 3 años, y por lo tanto válidas más allá del año 2000, están siendo renovadas normalmente. Es dudoso que en estos momentos puedan sugerirse estas posibles exclusiones, dado que las aseguradoras son conscientes de que el problema Año 2000 es un hecho o circunstancia que plausiblemente puede dar lugar a una reclamación que esté cubierta por la póliza D&O. Si las exclusiones fueran realmente inminentes, sería prudente dar inmediatamente aviso oficial a la aseguradora. (Aunque el seguro D&O está ideado principalmente para responder en caso de reclamaciones contra personas físicas, en estos últimos años ha sido posible incluir cobertura para personas jurídicas con respecto a ciertos tipos de reclamaciones).

Nueva Cobertura contra Excesos de Pérdidas/Pérdidas Catastróficas

El año pasado se creó una nueva cobertura contra Excesos de Pérdidas/Pérdidas Catastróficas que cubre diversos riesgos, varios de los cuales anteriormente no eran asegurables.

Estos programas, con límites de 400 millones de dólares o más, se aplican por encima de una retención considerable o por encima del límite de un seguro subyacente, constituyendo una verdadera transferencia de riesgo.

Las coberturas incluyen: seguro contra pérdidas que pueden surgir de actos no autorizados, entre ellos la compraventa bursátil no autorizada, la responsabilidad profesional corporativa, la cobertura complementaria de responsabilidad civil para Directores y Ejecutivos y el seguro complementario contra delitos penales. Aunque tales pólizas contienen exclusiones generales con respecto al problema Año 2000, también estipulan que dicha cobertura complementaria no puede ser nunca más restrictiva que la póliza subyacente. Por lo tanto, si la póliza D&O subyacente no contiene exclusiones con respecto al problema Año 2000, el programa de cobertura complementaria contra excesos de pérdidas/pérdidas catastróficas proporciona cobertura complementaria de responsabilidad civil para Directores y Ejecutivos.

Seguro contra Interrupción de Negocios

El Seguro contra la Interrupción de Negocios/Gastos Extraordinarios se deriva del seguro contra incendio. Históricamente, si un fabricante era víctima de un incendio que interrumpía la producción, dicho fabricante asegurado podía reclamar tanto por los daños directos causados a sus bienes muebles e inmuebles como por las pérdidas resultantes de la interrupción de los negocios (pérdida de ingresos netos) y de los gastos extraordinarios (gastos adicionales incurridos para reanudar los negocios, p.ej.:, el arriendo de otros equipos, otro local, etc). Esta cobertura se ofrece en la actualidad a toda clase de empresas.

A lo largo de los años se ha ido extendiendo la cobertura para incluir interrupciones contingentes de los negocios, p.ej.:, las pérdidas sufridas por un asegurado a consecuencia de daños materiales sufridos por uno de sus principales abastecedores o empresas de servicios públicos. Debido a que esta cobertura sólo se ofrece como extensión de la póliza de seguro de daños materiales, el factor que activa la cobertura es la existencia de un daño material. La cobertura no se aplica a una interrupción de negocio causada por una falla de software o hardware en donde no exista daño material. Hasta la fecha, lo más que han hecho ciertas aseguradoras para extender esta cobertura ha sido reconocer que la destrucción de datos causada por un virus informático puede ser considerada como "daño material". Sin embargo, la ocurrencia de un virus sigue siendo un caso fortuito desde el punto de vista del asegurado.

Existe la posibilidad de que un daño material pueda provenir de, o se permita que ocurra debido a, fallos de sistemas causados por el problema Año 2000, v.g., la pérdida de un sistema de protección contra incendios. Por esta razón, las aseguradoras en el Reino Unido y en U.S.A. están redactando exclusiones a esta cobertura. Se dice que la Association of British Insurers (ABI) (Asociación de Aseguradoras Británicas) ya ha recomendado un texto que excluye todos los daños directos e indirectos que puedan surgir de fallas informáticas. La ABI considera este texto una clarificación y no una nueva limitación.

Cobertura combinada de responsabilidad civil general y complementaria
Esta cobertura se aplica a la responsabilidad civil potencial ante terceros, que hayan sufrido por causa del asegurado daños corporales/daños materiales o daños personales (difamación, calumnia, arresto ilegal, detención ilegal): Estos casos de responsabilidad civil deben surgir de un "suceso" según definido en la póliza. Este seguro generalmente incluye la cobertura de responsabilidad contractual, sin embargo, sólo se aplica a la responsabilidad por daños corporales y materiales asumida bajo un contrato.

La cobertura exigiría, como mínimo, la existencia de daños corporales o daños materiales propiamente dichos. En la medida en que los datos de algún tercero podrían ser borrados debido a un proceso de interfaz, una empresa puede intentar argumentar que ha ocurrido daño material a un tercero. En el pasado, la destrucción de datos informáticos a veces ha sido considerada como daño material si el medio en que estaban almacenados tales datos también había quedado destruido. Sin embargo, los datos informáticos en sí no pueden ser considerados como propiedad tangible. Asimismo, la póliza responde sólo por "sucesos" definidos como "accidentes". Por último, la cobertura contra daños materiales excluye específicamente los daños materiales anticipados por el asegurado.

Al igual que sucede con respecto a los daños físicos, es posible que una falla de sistemas relacionada con el Año 2000 pueda resultar en daños corporales y materiales, p.ej.:, el mal funcionamiento de un ascensor. Claramente, existe un considerable riesgo relacionado con productos u operaciones terminadas, p.ej.:, para el fabricante de la computadora que controla un sistema de navegación aérea. Por una parte, puede argumentarse que los problemas relacionados con el Año 2000 pueden preverse y por lo tanto no son accidentes ni están cubiertos. Por otra parte, también puede argumentarse que una empresa ya había hecho todo lo que creía posible para resolver el problema y que, a pesar de ello, por error u omisión (negligencia) se produjo un daño corporal y/o material cubierto por la póliza. Al igual que en el caso arriba mencionado, Insurance Services Offices (ISO) (Oficinas de Servicios de Seguros) desea textos que excluyan estos siniestros y clarificaciones sobre la cobertura.

Nuevas coberturas
Nuevas coberturas, específicamente ideadas para los riesgos relacionados con el problema Año 2000, están siendo desarrolladas actualmente por las principales corredurías de seguros.

En un primer tiempo, la AIG desarrolló una propuesta que era principalmente un método de autoseguro o riesgo limitado; hasta ahora ésta no ha despertado mucho interés. Más recientemente, se han formulado métodos de transferencia efectiva del riesgo.

La firma J&H Marsh & McLennan recientemente anunció que está ofreciendo un proyecto de cobertura liderado por Lloyds. El límite de la cobertura que inicialmente se está discutiendo es de 200 millones de dólares; no obstante, también se ofrece por cantidades mayores. El deducible dependerá de la cuantía y clasificación del riesgo. Por ejemplo, las indicaciones iniciales para un banco en una capital financiera mencionan una retención de riesgo de aproximadamente 10 millones de dólares. La tasa de la prima sobre la línea del seguro oscilará entre un 2 y un 10 por ciento, y se anticipa que las primas de las instituciones financieras, por ejemplo, se sitúen en el nivel más alto de la escala, p.ej.:, el 10 por ciento sobre una línea de seguro con un límite de 200 millones. Esto podría resultar en una prima única de 20 millones de dólares.

La cobertura se aplicaría a la responsabilidad civil proveniente de alegados actos ilícitos, la interrupción de los negocios de la propia empresa asegurada y la interrupción contingente de los negocios sufrida por otra empresa de la que dependa la empresa asegurada, ambas resultantes de un problema Año 2000. Con respecto a la interrupción contingente de los negocios, los terceros de quienes dependa la empresa tendrán que ser identificados y examinados antes de ser expresamente incluidos en la póliza.

AON informa que ha formulado una propuesta parecida. La oferta de AON es liderada por American Re, con 100 millones de dólares; sin embargo, AON informa que se ha identificado una capacidad adicional de 900 millones de dólares en el mercado. Las coberturas esencialmente son las mismas que las ofrecidas en la propuesta de J&H Marsh pero, a diferencia del método utilizado por J&H Marsh, la interrupción contingente de los negocios no será específica sino que será considerada como parte del proceso global de debida diligencia inicial. La estructura de los deducibles también será similar, con una retención mínima de 5 millones de dólares y algún componente de coaseguro. La tasa de la prima sobre la línea del seguro para los primeros 100 millones de dólares oscila entre el 5 y el 8 por ciento, aplicándose porcentajes inferiores a niveles más elevados de cobertura.

Willis Corroon informa que también está desarrollando un programa que será anunciado en un futuro próximo.

Estas nuevas ofertas de seguros obviamente serán objeto de extensas negociaciones en un entorno sumamente competitivo.

Conclusión

Con excepción del seguro de responsabilidad civil para Directores y Ejecutivos, ninguno de los seguros existentes proporciona mucho alivio, especialmente en vista de las anticipadas restricciones y exclusiones. Afortunadamente, ciertos segmentos del sector de seguros está intentando actuar de una manera proactiva creando nuevas alternativas de cobertura. Las negociaciones que actualmente están llevando a cabo las diversas empresas determinarán si estas coberturas proyectadas van o no a resultar interesantes.

Confío en que esta discusión haya servido para identificar y explicar el problema Año 2000 en lo que se refiere a los seguros. El objeto de estos comentarios es proporcionar información y orientación general. La cobertura real de cada empresa dependerá de las disposiciones específicas que contengan sus respectivas pólizas. Deben consultar con profesionales de gestión de seguros y riesgos de su empresa tanto para determinar los detalles del seguro como para obtener asistencia para adaptar las nuevas coberturas ofrecidas a necesidades específicas.

William J. Kelly
Expresidente de IFRIMA,
actual Chairman.
Vicepresidente de
J.P. Morgan

...scan parte de Madrid

...bajada de bandera fue en la Avenida de Aster y concluyó en la Plaza de Castilla. Al pasar por el Tribunal de Defensa la Competencia, en Pío XII, los profesionales presentaron una denuncia, en la que exigen mejoras laborales en el sector.

...dos de los socios de la firma, fundada en 1988, y que ocurrió en septiembre del año pasado. Uno de los abogados que se fueron era quien prestaba su nombre al bufete, Alfonso Caldevilla.

Debido a esto, durante medio año ha habido dos despachos abiertos en Madrid con el apellido Caldevilla. Sierra, Luis López Herrera, Carlos Sánchez-Ocaña, María Echevarría, José Luis Sierra e Iván López-Chicheri) han optado por una firma de asesoramiento jurídico integral a la empresa; es decir, en un despacho multidisciplinar, que cubre diversas áreas jurídicas, como la mercantil, la laboral, la fiscal, la admi... ...europea Logos, una agrupación europea de interés económico fundada en 1989 y con asociados en 12 países de la UE.

Desde la ruptura hace medio año entre los socios de Caldevilla & Asociados, Alfonso Caldevilla ha preferido concentrarse en organizar un despacho especializado exclusivamente en derecho laboral.

...s de Oro'

...staca
...a
...citario

...e San Sebas-
... LAUS, o los
...IAP.
...sentación del
...or reflexionó
...ntajas e inco-
...e anunciarse
...o de prensa o
...sivo.
...rer los anun-
...visión tienen
...tos básicos: la
...la contrapro-
...la telebasura
... "El proble-
...ando se pre-
...actar a un
...tivo concreto,
...do, la prensa
...tal, porque la
... los lectores
...una credibili-
...ontenidos del
...ndicó Ferrer.

...e sociedad

...ce
...ial'

... incluirán en

...lia, el 40% de
...a tiene algu-
...dad, ha inten-
...lizarse en in-
...ocial, recordó
...ga, su director
...on *Línea So-*
...de recalcar la
... de este cam-
...vo

La multinacional informática Digital previene ante el relajamiento de miles de empresas

Dos de cada tres empresas descuidan la amenaza del 2000

Hoy faltan 673 días para que explote en los sistemas informáticos la bomba de relojería del 2000. En ese momento se descubrirá a las empresas previsoras frente a las que están condenadas a desaparecer. Y todo por culpa de una sencilla, pero laboriosa, actualización del calendario informático de millones de ordenadores, cuyo coste se estima en torno a los 90 billones de pesetas, más del PIB español de ese año.

ANTONIO LORENZO
DUBLÍN

"No se puede perder un segundo". La advertencia proviene del director para Europa de Digital, Cliff Murphy, en la presentación de dos productos específicos para atemperar la "maldición del cambio de milenio". Según sus cálculos, sólo el 37% de las grandes compañías se han tomado en serio el problema, frente al 42% que acumula retrasos en la adaptación del calendario de sus sistemas informáticos; el 21% apenas da importancia a la prevención. Dos de cada tres empresas se despreocupan de la amenaza.

Sólo sobrevivirá el 20% de los sistemas informáticos sin actualizar, frente al 80% que paralizará el sistema nervioso de los agentes productivos del mundo.

La responsable del caos es la imprevisión de los programadores. Para resumir al máximo la información, los programadores identificaron el año con dos dígitos. Por tanto, cualquier ordenador "entenderá" que tras el 31 de diciembre de 1999 comienza ¡el 1 de enero de 1900!. Un segundo significará un siglo de retraso.

Los directivos de Dig... ...capacidad para visuali... ...zar los cambios a realizar, pudiendo éste revisar en la estrategia de resolución del problema. 'Corre' en Digital Unix.

Navig 8 2000 completa las necesidades que no cubre el anterior al permutu el chequeo y cambio de los programas elaborados con Cobol, Fortram, C, Basic, cualquier otro

NEGOCIOS

Las empresas que ya se están adaptando, exigirán a sus proveedores un esfuerzo similar.

Remedios informáticos

Digital encomendó la tarea de crear aplicaciones eficaces de cara al 2000 a 6.100 profesionales, que elaboraron:

Piercom 2000 responde a la necesidad de cambiar automáticamente los lenguajes de programación digital, como Cobol, y ampliará su oferta con sistemas en Fortram y Pascal. Es-

...tal advirtieron ayer a las empresas que nunca se sientan sorprendidas ante una actualización de fechas que requiere más trabajo y tiempo de lo que se piensa.

Digital se ha aplicado su medicina y ha 'vacunado' el 90% de sus aparatos y aplicaciones.

Entre las grandes compañías que esperan el 2000 sin miedo están el Banco de Irlanda, British Gas, British Aerospace y decenas de empresas de Europa y EEUU. Éstas, a su vez, exigirán a sus proveedores un esfuerzo similar.

BARLOW LYDE & GILBERT

BRIEFING NOTE

12 February 1998

Implications of Y2K for Reinsurers

A separate complementary Briefing Note discusses the implications of Y2K for insurers.

CONTENTS

Introduction

Y2K has been described as the most serious issue which is now facing the international insurance and reinsurance markets. This conclusion is not surprising when estimates of the costs of litigation in the United States associated with Y2K between 1997 and 2005 amount to the staggering sum of US $1 trillion. Damages and punitive awards arising from this litigation are projected to be in the region of US $100 billion. These estimates are larger than the combined cost of asbestos-related, breast implant and pollution claims and compare with Hurricane Andrew, the most expensive single event in US insurance history, which cost US $16.5 billion. These figures are based upon worst case scenarios, but it is reasonable to assume that there will be significant world-wide claims arising from Y2K problems. Despite enormous Y2K publicity some companies have still not taken active steps to address their Y2K problems. According to research conducted by the Cologne Re, during the summer of 1997, 60 per cent of German companies had not yet explored the possible effects of Y2K and one third had taken no precautionary measures whatsoever. In this country, Unilever has warned that up to a

fifth of its small and medium-sized suppliers may not be Y2K compliant by 1 January 2000. In Australia, PA Consulting has warned that 38 per cent of Australian organisations will fail to re-programme their systems in time.

Y2K problems have already started to emerge. For example:

- In Kansas, a 104 year old woman recently received a letter telling her to register for kindergarten!
- In Washington, a Pentagon supplier with a contract for delivery of goods in 2003 received a warning that it was 94 years behind schedule.

In the United States there are already reports of Y2K litigation and regulatory action:

- A New York computer re-seller has filed a Y2K class action against a Californian software company, alleging that the software which was provided is not Y2K compliant, and it will cost more than US $50 million to upgrade customers using non-compliant versions to a Y2K compliant version.
- Cease and desist orders were recently issued against several Georgia banks and their parent company for alleged "unsafe and unsound" practices in failing to institute a Y2K compliance plan.

The nature of the problem

The Y2K problem is the result of computer programmers trying to save precious computer memory. Programmers used two digit abbreviations for date fields. Instead of a database programme having to hold, for example, a full date 5-07-1947, the programme was written to understand 5-07-47. The Y2K problem principally results from the inability of computers to distinguish between "00" meaning 2000 or 1900. Processes which involve dates may, therefore, no longer function or may produce incorrect results. The Y2K problem is not limited to computer programmes; many products contain micro-processor chips which also made use of the above convention. The result of the use of such chips is that we are now faced with the possibility of lifts, security systems, cars, planes, and even traffic lights failing before or at the commencement of the year 2000.

There are other dates in addition to 1 January 2000, for example 9 September 1999 [illegible] problems may be encountered with computerised systems. References in this note to Y2K apply to all these potential electronic date related problems. Another specific potential problem arises from the fact that the year 2000 is a leap year, whereas 1900 was not. Systems may be, therefore, further affected by the need to recognise the date 29 February 2000. Leap year problems were experienced in 1996. For instance, the Brussels Stock Exchange had to close for three hours at a cost of US $1 million; in New Zealand, an aluminium smelting plant shut itself down and a few hours later in Tasmania another plant controlled by the same software followed suit.

Reinsurance implications

In our Briefing Note concerning the insurance implications of Y2K we conclude that there are potential exposures for London and international insurers from Y2K claims. These exposures arise from a wide variety of classes of direct business such as property, business interruption, directors and officers, professional indemnity, marine and aviation. An example of a Y2K insurance claim which could arise is:

- a control system installed on an off-shore oil platform fails to operate at the commencement of the year 2000 due to a non-Y2K compliant embedded chip;
- the oil platform is damaged by a fire because the control system which operates the sprinkler system fails to work;
- the insured oil company makes substantial property and business interruption insurance claims;
- the insurers might then present reinsurance claims to their rig account reinsurers.

Particular issues of interest to reinsurers

It is not the intention of this Briefing Note to discuss all of the possible reinsurance issues which could arise in connection with Y2K claims. The following are believed, from the English law perspective, to be of particular interest to reinsurers:

- governing law and jurisdiction;
- trigger of cover;
- reinsurers' liability for non-indemnity payments — particularly declaratory judgment

- aggregation,
- follow the settlements.

• Governing law and jurisdiction

The business which reinsurers have written or may write in the future which could be affected by Y2K claims will be governed by the laws of a number of different jurisdictions including England, because Y2K is a global problem. For instance, if the London market has written supporting lines on the reinsurance of a US carrier, which is led in the USA, the reinsurance is likely to be governed by the law of a particular US state. On the other hand, reinsurance of London market cedants and retrocessions led in the London market will normally be governed by English law. The law governing the reinsurance or retrocession in question and the jurisdiction where it is agreed disputes are to be decided will have a vital bearing upon the outcome of any Y2K dispute under the reinsurance or retrocession concerned.

A further important consideration will be whether the parties have agreed to arbitrate their disputes. The Arbitration Act 1996 ("the Act") will apply to all Y2K reinsurance arbitrations commenced after 31 January 1997. The Act contains a number of changes to English arbitration law and procedure. The Act gives legal recognition to honourable engagement clauses which are sometimes included in reinsurance contracts. These clauses aim to allow an arbitration panel the right to determine a dispute in accordance with market principles and in the spirit of good faith and equity. Although the inclusion of an honourable engagement clause in a reinsurance contract gives the arbitration panel a degree of flexibility concerning the interpretation of the contract, it adds a further element of uncertainty regarding the result of an arbitration. For example, it is possible that an arbitration panel which is asked to interpret a Y2K exclusion clause in a reinsurance contract, which is subject to an honourable engagement arbitration provision, may interpret the exclusion more leniently i.e. in favour of the reinsured. Further, under English law, there is a limited right to appeal from an arbitral award to the courts on points of law. The position in the USA is even more restricted because under the US Federal Arbitration Act there is no appeal to the courts except in exceptional circumstances such as fraud.

Recommendations

- Ensure that the reinsurance contract contains a jurisdiction, arbitration and choice of law clause.
- Consider carefully before including honourable engagement provisions in arbitration clauses.

• Trigger of cover — reinsurance and retrocession contracts not governed by English law

Inwards excess of loss reinsurance business participated in by the London market is normally written on a losses occurring during the period ("LOD") basis. The date of the reinsurance loss will normally be the date(s) of the loss(es) under the original policies which will be established by the law governing the original policy. In US jurisdictions, for example, there are several theories relating to the trigger of cover (such as "exposure", "manifestation", "injury in fact" and "continuous"). In asbestos-related and pollution insurance coverage disputes heard in US jurisdictions the US courts have, in many instances, chosen the trigger of cover which gave the maximum policy coverage for the particular insured. If those courts take a similar approach to Y2K insurance claims, the trigger of cover could depend in many cases upon what is the most favourable coverage profile for the insured concerned. In some cases the "continuous trigger" theory could give the insured the maximum policy coverage. In this situation the initial trigger could be the date of the installation of the defective software, component or hardware and the trigger could continue until the date of the manifestation of the loss or damage caused by the non-compliant Y2K software.

• Trigger of cover — reinsurance and retrocession contracts governed by English law

There is no reported English case dealing with the trigger of coverage for LOD excess of loss reinsurance, but some guidance about this issue can be drawn from the Court of Appeal's decision in Kelly v. Norwich Union (1989). In this case, the policy provided that the insurer would indemnify the insured "in respect of events occurring during the period of the insurance". The Court of Appeal held that the "events" referred to insured events i.e. the cause of the loss rather than

the manifestation of the damage. If a similar approach was applied to Y2K claims concerning excess of loss contracts written on LOD basis, probably the date of the installation of the defective software or component or hardware would be the trigger for coverage under the reinsurance.

The question of which reinsurance policies may be subject to Y2K claims is of considerable importance with regard to establishing IBNR reserves for the appropriate underwriting years of account.

Recommendation

- Consider impact of the trigger of cover for Y2K claims with respect to reserving.

● Reinsurers' potential liability for non-indemnity payments

Potential exposure for cedants' costs could be the most serious issue for reinsurers of US cedants. Very substantial legal costs were incurred in the defence of declaratory judgment actions in connection with asbestos-related claims between US insureds and US insurers. It is predicted that significant costs could be incurred in defending Y2K insurance coverage disputes.

The question whether defence costs are covered by the relevant reinsurance will depend upon the precise wording of the reinsurance policy which is in issue. If the chosen trigger of cover points to an old reinsurance, it is possible that the wording or slip policy may be silent about this issue. The case of Baker v. Black Sea and Baltic (1996) will then be relevant; the issue was whether Black Sea was liable for legal expenses incurred by Lloyd's Syndicates in the course of investigating, settling and defending claims by their insureds/ reinsureds.

The court held that:

- the contract of reinsurance in question was for an indemnity against a specified liability to the reinsured under the policy and it was not apt to include an indemnity for costs incurred in resisting the insured claim;
- it was not prepared to imply a term into the reinsurance as a matter of business efficacy to the effect that reinsurers should be obliged to pay the legal expenses; and
- there was insufficient evidence of a custom of the market that reinsurers agree to pay defence costs; the fact that reinsurers often or usually paid a proportion of reinsureds' legal expenses did not establish such practice as universal.

This decision has been appealed to the House of Lords. The appeal will be heard during the course of this year.

There is, at present, no English decision as to whether declaratory judgment costs are recoverable from reinsurers pursuant to the usual Ultimate Net Loss clause wording contained in excess of loss policies issued in the London market:

> "The term 'Ultimate Net Loss' shall mean the sum actually paid by the reassured in settlement of losses or liability and shall include all adjustment expenses arising from the settlement of claims ..."

There are conflicting views as to whether such costs are recoverable as "sum(s) paid ... in settlement of losses" or "adjustment expenses arising from the settlement of claims" — respectable arguments can be advanced on both sides of this dispute. It is, therefore, necessary to await a definitive court decision about this issue.

US reinsureds are potentially exposed to punitive damage or bad faith claims arising from Y2K insured claims. To protect themselves from such claims reinsurers should consider including extra-contractual damages exclusion clauses in their reinsurance contracts.

Recommendations

- If the reinsurance contract is not intended to cover defence and/or declaratory judgment costs it is recommended that these are expressly excluded.
- Include an extra-contractual damages exclusion clause in reinsurances covering US business.

● Are the reinsured's Y2K loss settlements binding on reinsurers?

If the reinsurance contract does not contain a "follow the settlements" or "follow the fortunes" clause it will be necessary for the reinsured to establish that the Y2K loss being claimed falls within the terms of the original policy and the

reinsurance policy.

There are a number of forms of follow the settlements or follow the fortune clauses which are used in the London market. The extent to which, if at all, the reinsured will be required to prove that the Y2K loss falls within the terms of the original policy will depend upon the requirements stipulated in the wording of the relevant clause.

In the case of Hill v. M&G Re (1996) the House of Lords considered one of the forms of follow the settlements clauses used in the London market:

> "All loss settlements by the reassured including compromise settlements and the establishment of funds for the settlement of losses shall be binding upon the reinsurers, provided such settlements are within the terms and conditions of the original policies and/or contracts and within the terms and conditions of this reinsurance."

In the course of his judgment, Lord Mustill said that there are two obvious general rules which have to be satisfied before a reinsurer can be legally liable to its reinsured under any reinsurance contract:

- the reinsurer cannot be held liable unless the loss falls both within the cover of the original policy and within the relevant reinsurance policy;

- the parties are free to agree on ways of proving whether these requirements are satisfied.

Having regard to the above general principles, the House of Lords decided that the follow the settlements clause in question entitled the reinsurers to question the legal basis of the inwards settlement concluded by the reinsureds.

If, therefore, the relevant clause stipulates that the loss settlement must be within the terms of the original policy and the reinsurance, reinsurers do not automatically have to follow a Y2K loss settlement but would be entitled to question whether as a matter of law the original Y2K loss properly fell within the terms and conditions of the original policy. This is an important protection for reinsurers because, as discussed in our companion Briefing Note concerning the Insurance Implications of Y2K, there are a number of potentially valid policy defences to Y2K claims which should be relied upon by reinsureds, such as whether the loss in question is fortuitous.

The recent case of Commercial Union Plc & Others v. NRG Victory (August 1997) could be relevant to Y2K claims arising from the reinsurance of US business. In this case, the reinsurer (NRG Victory) disputed its liability to indemnify the reinsureds (Commercial Union and others) for sums which the reinsureds had paid to Exxon following the grounding of the Exxon Valdez. The payment was made in settlement of Texas proceedings commenced against them by Exxon. NRG Victory argued that the original policies were governed by English law and that the reinsureds were not, under English law, liable to Exxon. NRG Victory claimed, accordingly, that the settlement of the Texas action was not binding on it under the principles established in **Hill v. M&G Re**. The court found that the reinsureds had proved that they had entered into a sensible settlement of a claim arising in a court of competent jurisdiction.

This case has a wider significance for Y2K and other reinsurance claims. Whenever a reinsured's liability to its original insured is determined by a court of competent jurisdiction in a way in which an English court might not have determined it (and notwithstanding that England may have been an equally competent jurisdiction in the circumstances of the case), the reinsurer will be liable to indemnify the reinsured under a contract which is governed by English law. An insurance policy which is governed by English law could contain an absolute Y2K exclusion clause excluding all liabilities of the insurer for Y2K claims; if, however, a court of competent jurisdiction other than in England decided that the Y2K exclusion was ineffective, then, in the absence of a Y2K exclusion in the reinsurance, reinsurers would under English law be liable to indemnify the reinsured under the relevant reinsurance.

Some follow the settlement clauses which are used in the London market provide that reinsurers agree to pay *"ex gratia"* settlements. Reinsurers may wish to consider declining to agree this extension of liability for business which may be exposed to Y2K claims.

Recommendations

- Review the wording of your follow the settlements clauses included in your reinsurance contracts. Reinsurers might consider including in these clauses the qualification that loss must fall within the terms and conditions of the original policy as well as the reinsurance policy; reinsureds ought to try to bind reinsurers unconditionally to their settlements.
- Reinsurers should try to avoid including in follow the settlement clauses an agreement to pay *"ex gratia"* settlements; reinsureds should attempt to keep such agreements in place to give them flexibility in the negotiation of inwards losses.

Aggregation of claims

We anticipate there are likely to be a number of disputes regarding the extent to which reinsureds can properly aggregate Y2K claims and make a single or multiple claims presentation(s) to their reinsurers. Many excess of loss reinsurance contracts written in the London market are issued on an "event" basis. A typical event clause defines "each and every loss" in the following terms:

> "Each and every loss and/or occurrence and/or catastrophe and/or disaster and/or calamity and/or series of losses and/or occurrences and/or catastrophes and/or disasters and/or calamities arising out of one event."

The meaning of the word "event" has been considered in a number of reinsurance arbitrations, which usually remain confidential to the parties. The leading English legal authority on the meaning of the word "event" is the Court of Appeal's decision in **Caudle v. Sharp (1995)**. This case arose out of insurance claims paid by the professional indemnity underwriters of certain Lloyd's managing agencies and members' agents. These claims related to allegations by Lloyd's Names that Mr. Outhwaite, a Lloyd's underwriter, had negligently written 32 run-off contracts which were exposed to long-tail liability losses arising particularly from asbestos-related claims. The issue for the court was whether the professional indemnity underwriters could aggregate the claims when presenting them to their reinsurers on the basis that all of the claims arose from "one event".

Evans LJ, who delivered the principal judgment of the Court of Appeal, identified three requirements which must be fulfilled before there can be said to be an event in the sense relevant to the clause quoted above:

- there must be a common factor which can be properly described as an event;
- a test of causation must be satisfied; and
- the event must not be too remote for the purpose of the definition of "each and every loss" i.e. it must be something which both the reinsured and the reinsurer would have contemplated as a reasonable basis for the aggregation of claims.

It is implicit in Evans LJ's reasoning that in order to qualify as an event, the common factor must be limited in time and space and it must also be capable of producing legally relevant consequences.

The right of reinsureds to aggregate Y2K reinsurance claims will depend on the particular facts of each case and the precise wording of the event-based or other aggregation clause contained in the relevant reinsurance contract. We expect that the principal points of disagreement between reinsureds and their reinsurers will be whether the test of causation can be satisfied and whether the relevant event is or is not too remote.

Event-based wordings are not the only type of aggregation provision used in the London market; cause-based reinsuring clauses are sometimes used. The House of Lords in **Axa Reinsurance (UK) Plc v. Field (1996)** considered whether there was any distinction between the expressions "originating cause" and "event". Lord Mustill, who gave the leading judgment in the House of Lords, considered that the expressions "originating cause" and "event" were not at all the same. He considered that an "event" is something which happens at a particular time, at a particular place and in a particular way. A "cause" is something less constricted and could include a continuing state of affairs, or the absence of something happening. The effect of this decision, so far as Y2K reinsurance claims are concerned, is that if the relevant reinsurance contract contains a cause-based clause, the reinsured will have a better prospect of aggregating Y2K claims

than would be the case if the contract contained an event based clause.

Y2K compliance for reinsurers

The reinsurance industry has embraced information technology to the extent that it is now one of the essential tools for running its business. Reinsurers are, therefore, particularly vulnerable to problems caused by Y2K non-compliance in their own and their trading partners' systems. In a survey carried out in the USA during the summer of 1996, 89 of 100 insurance executives responding to a survey about the Y2K problem believed their systems were exposed to the Y2K problem, but only 17 per cent were looking for outside support to help them become Y2K compliant. The costs of reprogramming systems to ensure Y2K compliance can be enormous and, therefore, as part of the Y2K auditing process consideration should be given to carrying out a legal review of the relevant supplier or software contracts to establish whether any claim can be made against a potentially responsible party. Care should be taken to investigate this aspect promptly because there is the risk that legal time limits for pursuing such claims could expire before the year 2000. Under English law, the six year general time limit for claims in contract commences from the date of the breach of contract, which could, for example, be when the software was supplied, and not the later date when the problem manifests itself. The contract, however, could be subject to a system of law with a shorter limitation period.

Recommendations

- Consider commissioning a legal review of all software and hardware supplier contracts to establish what rights you have against your suppliers of any software or hardware which is non-Y2K compliant.
- Ensure that steps are taken to prevent any claims against your suppliers from becoming time-barred.

What can reinsurers do to mitigate their exposure to Y2K claims?

- Y2K exclusion clauses

In the light of the possibly substantial number and value of Y2K reinsurance claims reinsurers may consider that they wish to exclude absolutely all direct and indirect losses arising from Y2K claims. It is important that reinsurance contracts potentially exposed to Y2K claims contain a choice of law clause because the interpretation and effectiveness of a Y2K exclusion will be significantly affected by the express or implied law governing the contract. The wording of any Y2K exclusion clause which is included in a policy must be clear and unambiguous. It should cover all direct and indirect losses arising from non-compliance with Y2K, including the fact that losses must not arise from the lack of recognition that the year 2000 is a leap year and also other electronic date-related problems.

Under English law a clearly-worded Y2K exclusion clause will usually protect reinsurers from Y2K claims. A reinsurer who is seeking to rely upon a Y2K exclusion clause will, however, have the onus of proving that the claim is excluded by virtue of the exclusion. There is a presumption that words are to be interpreted in their ordinary and popular sense although expressions which have a particular accepted meaning in the reinsurance market will be given their market meaning. If the court decides that the Y2K exclusion is ambiguous, the clause will be construed against reinsurers. The position with respect to reinsurance contracts which are not governed by English law may be different. Particular care needs to be taken with the wording of Y2K exclusion clauses which are included in contracts which are subject to the jurisdiction and law of any US state. There have been, from the English lawyers' perspective, some surprising decisions in the USA regarding the interpretation of the "sudden and accidental" and "absolute" pollution exclusion clauses. It is possible that in some US jurisdictions, an "absolute" or "qualified" Y2K exclusion clause in a reinsurance policy may not be held to apply in all circumstances to Y2K claims.

The ABI has published a number of model Y2K exclusion clauses for various classes of insurance business. There are, at present, no model exclusion clauses which have been recommended by LIRMA or Lloyd's with respect to reinsurance business but working parties have been established to examine the implications of Y2K for reinsurers. A number of reinsurance companies and Lloyd's Syndicates have, however, drafted their own Y2K exclusions. It is important to ensure that any model exclusion which may be recommended for use by reinsurers in the London market is consistent with the other terms and conditions used in the relevant reinsurance wording. Market organisations and groups of

underwriters who are considering recommending Y2K exclusions clauses for use in respect of US reinsurance business should consider with their US legal advisers the potential implications of Federal and US state anti-trust legislation.

Recommendations

- Consider including absolute or qualified Y2K exclusion clauses in your reinsurance contracts.
- Ensure wording of Y2K exclusion is clear, unambiguous and consistent with the other provisions contained in your reinsurance contracts and in particular consistent with the law chosen to govern the contract.

Other measures

- Questionnaires

Reinsurers may wish to consider including in their standard questionnaires specific queries concerning the reinsured's potential exposure to Y2K claims. Y2K reinsurance questionnaires are likely to be of limited value to reinsurers but a carefully worded questionnaire should be designed, at least, to ensure that the reinsured is asking its insureds the appropriate questions about the steps being taken to ensure Y2K compliance. Questions concerning Y2K should be carefully drafted because of the potential risk that if there is a subsequent disputed claim the reinsured may argue that the reinsurer has waived his right in certain respects to require full disclosure of all material information relating to Y2K issues. The quality and completeness of the information which reinsureds will be able to provide about their potential exposure to Y2K claims will, of course, depend upon the information which they are receiving from their insureds. Insurers are unlikely to be provided with a complete picture of their insureds' readiness for the year 2000 because most insureds will, at present, be unable to confirm that their computer systems are Y2K compliant. Insureds should be able, however, to explain satisfactorily what steps they have taken and will be taking to ensure that their systems will be Y2K compliant at the appropriate time, which may be before the year 2000.

Recommendation

- Consider including questions concerning reinsureds' exposure to Y2K claims in your reinsurance questionnaires.

- Warranties

Some reinsurers may be considering including Y2K warranties in their slips and policy wordings. These are likely to be resisted by reinsureds because many insureds will be unable to warrant to their insurers that their computer systems are, at present, Y2K compliant. A further difficulty is that any warranty which may be required to be given by the reinsured is likely to be limited to the information and knowledge of the reinsured at the time when the warranty is given. In view of the on-going nature of work which will usually be required to be carried out by insureds to ensure that their systems are Y2K compliant, it is recommended that a duty should be imposed upon reinsureds as a term of the slip/policy to keep reinsurers informed of material developments regarding Y2K compliance issues which affect the accounts which are protected by the relevant reinsurance.

Recommendation

- Ensure reinsurance wording imposes duty on reinsured to keep reinsurer informed of material Y2K issues affecting specific or whole accounts.

Conclusions

Despite the world-wide publicity given to the need to ensure that computer systems are Y2K compliant, it is predicted by systems specialists that a significant number of companies will not have taken the appropriate steps in time to ensure their systems are Y2K compliant. Reinsurers are potentially exposed to significant Y2K claims and, accordingly, they need to analyse their potential exposures to enable them to decide, with the assistance of their legal advisers, what action they wish to take, to respond positively to this new challenge. Reinsureds need to be satisfied that their reinsurance protections will cover them for exposures relating to Y2K insurance claims ●

Y2K Checklist of issues and recommendations

- Ensure your reinsurance contracts contain jurisdiction and choice of law clauses.
- Consider how disputes are to be decided i.e. by an arbitration panel or by a particular court (e.g. English High Court).
- Reinsurers should consider carefully before including honourable engagement provisions in arbitration clauses. Reinsureds may wish to consider including honourable engagement provisions in arbitration clauses.
- Consider impact of the trigger of cover for Y2K with respect to reserving.
- If the reinsurance contract is not intended to cover defence and/or declaratory judgment costs it is recommended that these are expressly excluded; if they are intended to be included expressly include.
- Consider including an extra-contractual damages exclusion clause.
- Review your standard follow the settlement clause(s). For reinsurers: consider including in the clauses the qualification that the loss must fall within the terms and conditions of the original policy as well as the reinsurance policy. For reinsureds: consider whether it is possible to negotiate the inclusion of provisions which bind reinsurers unconditionally to your settlements.
- Consider the impact of including in your follow the settlement clauses an agreement to pay *ex gratia* settlements.
- Basis for aggregating claims: the mechanism which the reinsured is entitled to use as the aggregating factor for Y2K claims will be crucially important. For example, "cause-based" clauses generally provide a greater scope for aggregation than "event-based" wordings.
- Consider commissioning a legal review of all software and hardware supplier contracts to establish strengths of your rights against your software/hardware suppliers.
- Ensure steps are taken to prevent any claims against your suppliers from becoming time-barred.
- Do you want to include an absolute or qualified Y2K exclusion clause?
- Ensure wording of Y2K exclusion contained in your reinsurance contracts is clear and unambiguous.
- Consider including questions concerning reinsureds' exposure to Y2K claims in your reinsurance questionnaires.
- Ensure reinsurance wording imposes duty on reinsured to keep the reinsurer informed of material Y2K issues affecting specific or general accounts.

"Professional Service Provider of the Year"

At the 1997 Review Worldwide Reinsurance Awards, Barlow Lyde & Gilbert became the first law firm to be named "Professional Service Provider of the Year" by an international panel of judges drawn from distinguished members of the reinsurance industry.

The panel was presented with a short list of "some of the world's most committed and technically supreme industry service providers". The judges felt that in the light of the tough competition "to simply do the job for which you are paid is not enough". The judges alluded to this firm's "unquestioned professionalism and success in litigation". We were praised for our considerable contribution to the continuing education of the reinsurance market and our "proactive approach" to the provision of information to the industry which were of "great value". The panel also singled out the fact that we are often involved in technical developments, such as the recent restructuring of St Paul Re's catastrophe capacity.

The judges concluded by recognising the firm's "great efforts in the marketplace and its consistency over a number of years".

The recipients of The Review Worldwide Reinsurance Awards pictured at the Awards Ceremony at the Dorchester Hotel: (from left to right) BLG's Colin Croly; Thomas Hess of Swiss Re; Richard Hinchcliff of General Re; John Major of Guy Carpenter; David Spiller of Greig Fester; Andreas Jaggi of Swiss Re; Jin Darong of PICC Re; Dennis Mahoney of Aon (for Patrick Ryan); and Nick Walsh of AIG (for Maurice Greenberg).

BLG Publications

Copies of all our BLG publications are available from Philippa Perry on 0171 415 8881 or via our main switchboard. The following publications are issued on a regular basis:

- BLG Insurance Law Quarterly
- BLG Pollution and Environmental Risk Digest
- BLG Directors' and Officers' Liability Review
- BLG Employment Law Review
- BLG Accountants' Liability Briefing
- BLG Construction Law Briefing
- BLG Banking Law Briefing

BLG Programme for Lloyd's, Chartered Insurance Institute and Law Society Continuing Professional Education

Lloyd's Continuing Professional Education Programme and The Chartered Insurance Institute's Continuing Professional Development Scheme have been widely supported by all concerned as a way to ensure continuing professionalism within the market.

At BLG we are pleased to be able to play our part in this initiative by offering, for the fourth year, a continuing professional education programme for those within the Lloyd's and companies markets. Commencing in February 1998, our programme is offered to all members of the London and international insurance and reinsurance markets. Our programme has been approved by Lloyd's for its Continuing Professional Education Programme and by The Chartered Insurance Institute for the purpose of its Continuing Professional Development Scheme. Our courses are also Law Society CPD accredited. Seven modules in our current programme remain to be held; details are set out below. Each of the seminars will commence at 4.30 pm and finish at 6.30 pm, thus giving two hours' Lloyd's CPE credit. The timing of the seminars has been fixed to cause least disruption to the working day of attendees. The seminars will involve lectures, question and answer sessions and, where appropriate, case studies. Seminars will be followed by refreshments to allow for informal discussion of the issues covered in the presentations. As part of our continuing commitment to the market, we are making no charge for attendance at these seminars.

Our programme is as follows:

Professional Indemnity and Financial Institutions — *17 February 1998*

This seminar will look at the future of claims against professionals, including auditors, solicitors and brokers. It will also examine banks' exposures.

Arbitration Workshop — *3 March 1998*

An examination of the current trends in arbitration, particularly following the implementation of the Act and with particular reference to construction, marine and reinsurance arbitrations.

How Evidence is Used — *21 April 1998*

A seminar on preparing to give evidence including a focus on witness statements and experts' reports.

Pollution – 20th Century Problems : 21st Century Solutions — *28 April 1998*

This seminar will examine the differences in environmental liability law and the way in which environmental impairment is being handled in the US, the UK and the rest of Europe.

Deposition Training Workshop — *19 May 1998*

An inter-active session showing how one should give evidence and prepare for depositions. We will use edited highlights from actual depositions in role playing exercises.

Product Liability in Europe — *2 June 1998*

A review of the existing state of product liability law in Europe, including recent developments and a consideration of likely future trends.

The Year 2000 – An Opportunity or Potential Disaster for the Insurance Industry? — *16 June 1998*

What is the Year 2000 problem? What liability issues arise; what scope is there for insurance and new insurance products to assist in remedying these problems?

If you would like to attend any of the seminars, please contact Jo Seaman at BLG on 0171 782 8004 or via our main switchboard.

WHO WE ARE AND HOW WE CAN HELP

If you would like any further information or advice about Y2K reinsurance issues please contact either any member of our Y2K Reinsurance Team, whose members are Colin Croly, Michael Mendelowitz and Michael Graham, or any of our other partners in our Reinsurance Division:

John Hanson (0171 782 8478: jhanson@blg.co.uk)
Tim Hardy (0171 782 8479: thardy@blg.co.uk)
Clive O'Connell (0171 782 8477: coconnel@blg.co.uk)
Paul Howick (0171 782 8546: phowick@blg.co.uk)
Andrew Crouchman (0171 782 8063: acrouchm@blg.co.uk)
Janet Lambert (0171 782 8534: jlambert@blg.co.uk)
Andrew Deighton (0171 782 8532: adeighto@blg.co.uk)

Colin Croly
0171 782 8657
ccroly@blg.co.uk

Michael Mendelowitz
0171 782 8595
mmendelo@blg.co.uk

Michael Graham
0171 782 8557
mgraham@blg.co.uk

If you would like advice about the implications of Y2K with respect to your suppliers or software contractors please contact David Strang or Andrew Horrocks.

David Strang
0171 415 8937
dstrang@blg.co.uk

Andrew Horrocks
0171 782 8082
ahorrock@blg.co.uk

If you would like to be sent a copy of our Briefing Note concerning the Implications of Y2K for Insurers, please request a copy from Michael Graham at our London office.

London Offices:
Barlow Lyde & Gilbert
Beaufort House
15 St. Botolph Street
London EC3A 7NJ
Telephone: 0171 247 2277
Fax: 0171 782 8500
DX 155
and at Lloyd's

Hong Kong Office:
Barlow Lyde & Gilbert
4010 Jardine House
1 Connaught Place
Central
Hong Kong
Telephone: 25264202
Fax: 28105994
(Contact Cameron Scott)

European web site http://www.blg.co.uk
North American web site http://blg2.com

BRIEFING NOTE

12 February 1998

Implications of Y2K for Insurers

The purpose of this Briefing Note is to outline the potential exposures of international insurers to claims arising from non-millennium compliant systems and what steps can be taken now to try to mitigate the "Y2K" problem. A separate complementary Briefing Note discusses the implications of Y2K for reinsurers.

Introduction

Y2K has been described as the most serious issue which is now facing the international insurance and reinsurance markets. This conclusion is not surprising when estimates of the costs of litigation in the United States associated with Y2K between 1997 and 2005 amount to the staggering sum of US $1 trillion. Damages and punitive awards arising from this litigation are projected to be in the region of US $100 billion. These estimates are larger than the combined cost of asbestos-related, breast implant and pollution claims and compare with Hurricane Andrew, the most expensive single event in US insurance history, which cost US $16.5 billion. These figures are based upon worst case scenarios, but it is reasonable to assume that there will be significant world-wide claims arising from Y2K problems.

Despite enormous Y2K publicity which has appeared in the press some companies have still not taken active steps to address their Y2K problems. According to research conducted by the Cologne Re, during the summer of 1997, 60 per cent of German companies had not yet explored the possible effects of Y2K and one third had taken no precautionary measures whatsoever. In this country, Unilever has warned that up to a fifth of its small and medium-sized suppliers may not be Y2K compliant by 1 January 2000. In Australia PA Consulting has warned that 38 per cent of Australian organisations will fail to re-programme their systems in time.

Y2K problems have already started to emerge. For example:

- In Kansas, a 104 year old woman recently received a letter telling her to register for kindergarten!
- In Washington, a Pentagon supplier with a contract for delivery of goods in 2003 received a warning that it was 94 years behind schedule.

In the United States there are already reports of Y2K litigation and regulatory action:

- A New York computer re-seller has filed a Y2K class action against a Californian software company, alleging that the software which was provided is not Y2K compliant, and it will cost more than US $50 million to upgrade customers using non-compliant versions to a Y2K compliant version.
- Cease and desist orders were recently issued against several Georgia banks and their parent company for alleged "unsafe and unsound" practices in failing to institute a Y2K compliance plan.

The nature of the problem

The Y2K problem is the result of computer programmers trying to save precious computer memory. Programmers used two digit abbreviations for date fields. Instead of a database programme having to hold, for example, a full date 5-07-1947, the programme was written to understand 5-07-47. The Y2K problem results from the inability of computers to distinguish between "00" meaning 2000 or 1900. Processes which involve dates may no longer function or may produce incorrect results. The Y2K problem is not limited to computer programmes; many products contain micro-processor chips which also made use of the above convention. The result of the use of such chips is that we are now faced

with the possibility of lifts, security systems, cars, planes, and even traffic lights failing before or at the commencement of the year 2000.

There are other dates in addition to 1 January 2000, for example, 9 September 1999, where problems may be encountered with computerised systems. References in this note to Y2K apply to all these potential electronic date related problems. Another specific potential problem arises from the fact that the year 2000 is a leap year, whereas 1900 was not. Systems may be, therefore, further affected by the need to recognise the date 29 February 2000. Leap year problems were experienced in 1996. For instance, the Brussels Stock Exchange had to close for three hours at a cost of US $1 million; in New Zealand, an aluminium smelting plant shut itself down and a few hours later in Tasmania another plant controlled by the same software followed suit.

Insurance implications

It is apparent from the above comments that there is likely to be a large number of claims arising from non-Y2K compliant systems. It is highly likely that insureds will try to recover their losses from the insurance market particularly in those jurisdictions where insurers are perceived to have "deep pockets". Insurers' first line of defence to such claims will be that the losses are not fortuitous and are, thus, not covered. We discuss the merits of this general defence in the next section of our note.

Will Y2K losses be fortuitous?

Although there is no statutory or exhaustive judicial definition of insurance, it is clear that one of its hallmarks is that the happening of the relevant event must be one involving uncertainty — "There must be either uncertainty whether the event will happen or not, or if the event is one which must happen at some time, there must be uncertainty as to the time at which it will happen." (Prudential Insurance Company v. Inland Revenue Commissioners (1904).)

It is inevitable that there will be disruption if companies do not reprogramme their software such that it is Y2K compliant. The disruption will be caused as soon as dates beyond 31 December 1999 start to be generated by software. Although there is an inevitability about the disruption its exact timing may not be clear. For example, two years ago a number of supermarkets encountered problems with corned beef. Corned beef has an exceedingly long shelf-life and, thus, the "use by" dates printed on tins can be a number of years in the future. Consignments of corned beef were placed on shelves but their "use by" and "sell by" dates were after 31 December 1999. The supermarkets' computer stock control and point of sale systems wrongly concluded that the corned beef was actually 95 or 96 years old and, as such, was, of course, not fit to be sold.

If the only consequence of non-Y2K compliant software is the corruption of data in a computer, this may be inevitable and, thus, not fortuitous. If, on the other hand, the result of non-compliance is damage or loss to other property, such as for instance, when a security system shuts down and there is a theft of property, such loss is unlikely to be inevitable.

A further general consideration is that a loss will not be considered to be fortuitous if it was caused by the wilful misconduct of the insured occurring at any time during the insurance period. Wilful misconduct is not the same as negligence. If a company negligently carries out a Y2K audit, and then takes all the steps recommended in the audit, it would not be guilty of wilful misconduct. On the other hand, an insured would be guilty of wilful misconduct if it carries out a Y2K audit and deliberately decides not to take any action because the steps that are necessary to make its business systems Y2K compliant are perceived to be just too costly.

Particular classes of insurance business

● All risks property and business interruption insurances

The principal concern for most businesses will be the impact of computer failure due to non-Y2K compliance on their ongoing business operations. In the event of a catastrophic failure of computer systems, this could have a very significant impact on the normal business of a company. In such circumstances, the company is likely to wish to make claims under its all risks property and, in particular, its business interruption policies. Apart from the issues of whether such losses are fortuitous and whether there has been any non-disclosure by the insured, two further general

issues will arise for consideration by insurers in respect of such claims. These are whether the losses which are claimed relate to "property" which is insured and whether "damage" has been sustained to the "property". The property which is insured may be specifically described in the policy or its schedule. Many policies, however, simply state that the policy covers loss and damage to the property without identifying particular types of property which are insured and, thereafter, excludes certain classes of property. Policies vary as to whether they cover computer hardware. Tangible property such as computer hardware and probably computer chips are likely to be included in the meaning of the word "property" if it is undefined in the policy. There is currently no guidance from the courts regarding the question whether software can be considered to be property in the context of a property insurance, when the policy does not contain a definition of the insured property. Some limited assistance about this question can be obtained from two non-insurance cases. The first case is **St Albans City & District Council v. ICL (Court of Appeal, 1996)**. The Court of Appeal commented that computer programmes did not come within the specific definition of "goods" contained in the Sale of Goods Act 1979 which refers to "all personal chattels other than things in action or money". A different approach was taken in a criminal case, **Regina v. Whiteley (1993)**, when the court had to consider whether there had been any criminal damage caused by computer hacking. The court found that the defendant had altered magnetic particles on computer disks in such a way as to impair the value or usefulness of the disk to their owners, and accordingly criminal damage to property had been caused. The fact that the alteration could only be perceived by operating the computer did not make the damage any less real. The question whether a business interruption claim would be covered will largely depend upon whether it can be established that the claim is as a result of a material damage claim.

● **Directors' and officers' liability insurance**

Directors' and officers' insurance usually covers the insureds for "wrongful acts" which are generally broadly defined. Claims against directors and officers in this country are, at present, not common. It is anticipated that a number of companies will sustain substantial financial losses from non-Y2K compliant systems and some could become insolvent. Some companies could suffer significant disruption to their business as a result of their suppliers or other third parties failing to make their systems compliant. Liquidators of insolvent companies and shareholders may consider instituting proceedings against the directors of companies who suffer from major or fatal Y2K problems. The position in the United States is likely to be very different with a real risk of claims arising.

● **Professional indemnity insurance**

Significant claims are likely to be made under professional indemnity policies insuring "professionals" such as computer consultants, auditors, solicitors and insurance brokers. Professional indemnity is usually written on a "claims made" basis. Claims made policies usually exclude the consequences of any circumstances known to the insured at the inception of the insurance which might reasonably have expected to produce a claim. The Y2K problem has been well publicised for some time and, therefore, insurers may contend that any claim is excluded by virtue of this provision. The insured may seek to rebut this contention by arguing that the above "circumstances" are insufficient and what is required is actual knowledge that the insured's computer systems are not Y2K compliant and that such knowledge can only be acquired, for example, after a Y2K compliance audit reveals that the system is not Y2K compliant. A further defence, which insurers may seek to rely upon is that insureds have failed to notify promptly "circumstances" which may give rise to a claim. Insureds who are concerned about their notification obligations may decide to make either blanket notifications to their professional indemnity insurers or prepare a "laundry list" of notifications of "circumstances" which might give rise to a claim. Insurers will have to consider carefully whether such blanket notifications comply with the insured's notification obligations under the policy. A further potential defence which might be available to professional indemnity insurers at the time of a renewal is that the insured has failed to disclose all material information relating to Y2K problems.

● Employers' liability, public liability and product liability insurances

It is possible that Y2K problems could result in death and/or injuries to third parties. This could particularly arise from non-compliant embedded chips which malfunction in machinery, lifts, sprinkler systems, and even traffic lights. Liability policies often include an exclusion to the effect that the policy will not cover deliberate acts or omissions of the insured which could reasonably have been expected by the insured to have resulted in liability. This is obviously a difficult factual matter to prove but depending upon the particular facts of the case may be applicable to a loss submitted under a liability policy, when, for example, the insured has deliberately ignored a known Y2K problem.

● Bankers and financial institutions insurances

There is clearly a significant exposure for banks and financial institutions which could arise from non-compliant Y2K systems. For instance, interest due to customers could be incorrectly calculated, pensions not paid on time and inter-bank money transfer payments not made promptly.

● Credit insurance

It is anticipated that insolvencies will either directly arise from companies failing to take adequate steps to ensure that their systems are Y2K compliant or alternatively there could be a knock-on effect of third parties whose systems are not Y2K compliant. For instance, if a supplier is unable to deliver a component for a machine which is being manufactured and must be delivered to the buyer by a specific date.

● Marine, aviation and transport insurance

All these classes of insurance are potentially exposed to Y2K claims. For example, navigational aids which are fitted to ships and aircraft may have Y2K non-compliant embedded software which could malfunction and which could then result in potential first and third party insured losses.

Y2K compliance for insurers

The insurance industry has embraced information technology such that it is one of its essential tools for running its business. Insurers are, therefore, particularly vulnerable to problems caused by Y2K non-compliance in their own and their trading partners' systems. In a survey carried out in the USA during the summer of 1996 89 of 100 insurance executives responding to the survey about the Y2K problem believed their systems were exposed to the Y2K problem, but only 17 per cent were looking for outside support to help them become Y2K compliant. The costs of reprogramming systems to ensure Y2K compliance can be enormous and, therefore, as part of the Y2K auditing process consideration should be given to carrying out a legal review of the relevant supplier or software contracts to establish whether any claim can be made against any potentially responsible party. Care should be taken to investigate this aspect promptly because there is the risk that legal time limits for pursuing such claims could expire before the year 2000 because the general time limit for claims in contract is six years, which commences from the date of the breach of the relevant contract. Time limits could commence, for example, from the date of the installation of the non-Y2K compliant software, and not the later date when the problem manifests itself. The contract, however, could be subject to a system of law with a shorter limitation period.

What can insurers do to mitigate their exposure to Y2K claims?

● Y2K exclusion clauses

We have highlighted in this Briefing Note certain classes of insurance which may be potentially exposed to Y2K claims. In the light of the possibly substantial number and value of Y2K claims insurers may consider that they wish to exclude absolutely all direct and indirect losses arising from Y2K claims. The wording of any Y2K exclusion clause which is included in a policy must be clear and unambiguous such that it covers all direct and indirect losses arising from non-compliance with Y2K including the fact that losses must not arise from the lack of recognition that the year 2000 is a leapyear.

Under English law a clearly worded Y2K exclusion clause will usually protect insurers from Y2K claims. An insurer seeking to rely upon a Y2K exclusion clause will have the onus of proving that the claim is excluded by virtue of the exclusion There is a presumption that words are to be

interpreted in their ordinary and popular sense although expressions which have a particular accepted meaning in the insurance market will be given their market meaning. If the court decides that the Y2K exclusion is ambiguous the clause will be construed against insurers. There are limited exceptions to the freedom of insurers to exclude Y2K liabilities such as insurance contracts covering consumers, which must satisfy the test of reasonableness and certain specific classes of insurance.

The ABI has published a number of model Y2K exclusion clauses for various classes of insurance business. It is important that any model clause which is applied to a particular policy is reviewed to ensure that its wording is consistent with the other terms and conditions used in the policy wording in question. Market organisations and/or groups of underwriters who are considering recommending Y2K exclusions clauses for use in respect of US insurance business should consider with their US legal advisers the potential implications of Federal and US state anti-trust legislation.

Other measures

● Questionnaires and proposal forms

An appropriately worded Y2K questionnaire can be an important source of information for the underwriter when he is assessing a prospective insured's potential exposure to Y2K problems. Y2K questionnaires should be carefully drafted because of the potential risk that if there is a subsequent disputed claim the insured may argue that the insurer has waived his right in certain respects to require full disclosure of all material information relating to Y2K issues. Although questionnaires will undoubtedly be helpful to underwriters they are unlikely to provide a complete picture of the insured's readiness for the year 2000 because most insureds will, at present, be unable to confirm that their computer systems are Y2K compliant. Insureds should be able, however, to explain satisfactorily what steps they have taken and will be taking to ensure that their systems will be Y2K compliant at the appropriate time, which may be before the year 2000.

● Warranties

Some insurers may be considering including warranties in their proposal forms. Warranties may be of limited value to insurers because, as discussed above, many insureds will be unable to warrant that their computer systems are, at present, Y2K compliant. The information contained in any proposal form and any warranty which may be required to be given by the insured is likely to be limited to the information and knowledge of the insured at the time of the completion of the proposal form and the date when the warranty is given. In view of the on-going nature of work which will usually be required to be carried out by an insured to ensure that its systems are Y2K compliant it is recommended that a duty should be imposed upon insureds as a term of the policy to keep insurers informed of material developments regarding Y2K compliance issues.

Conclusions

Despite the world-wide publicity given to the need to ensure that computer systems are Y2K compliant it is predicted by systems specialists that a significant number of companies will not have taken the appropriate steps in time to ensure their systems are Y2K compliant. Insurers are potentially exposed to significant Y2K claims and, accordingly, they need to analyse their potential exposures to enable them to decide, with the assistance of their legal advisers, what action they wish to take to respond positively to this new challenge ●

WHO WE ARE AND HOW WE CAN HELP

Barlow Lyde & Gilbert is one of the largest insurance and reinsurance practices in the world. The firm was chosen as the Professional Service Provider of the Year at the 1997 Review Worldwide Reinsurance Awards; the first time the award has been given to any legal practice.

If you would like any further information or advice about Y2K insurance issues please contact any member of our Y2K insurance team which consists of partners Ian Jenkins (Senior Partner), Colin Croly, Michael Mendelowitz, Francis Kean and Michael Graham.

Ian Jenkins
0171 782 8455
ijenkins@blg.co.uk

Colin Croly
0171 782 8657
ccroly@blg.co.uk

Michael Mendelowitz
0171 782 8595
mmendelo@blg.co.uk

Francis Kean
0171 782 8586
fkean@blg.co.uk

Michael Graham
0171 782 8557
mgraham@blg.co.uk

If you would like advice about the implications of Y2K with respect to your suppliers or software contractors please contact our partners David Strang and Andrew Horrocks.

David Strang
0171 415 8937
dstrang@blg.co.uk

Andrew Horrocks
0171 782 8082
ahorrock@blg.co.uk

If you would like to be sent a copy of our Briefing Note concerning the Implications of Y2K for Reinsurers, please request a copy from Michael Graham at our London office.

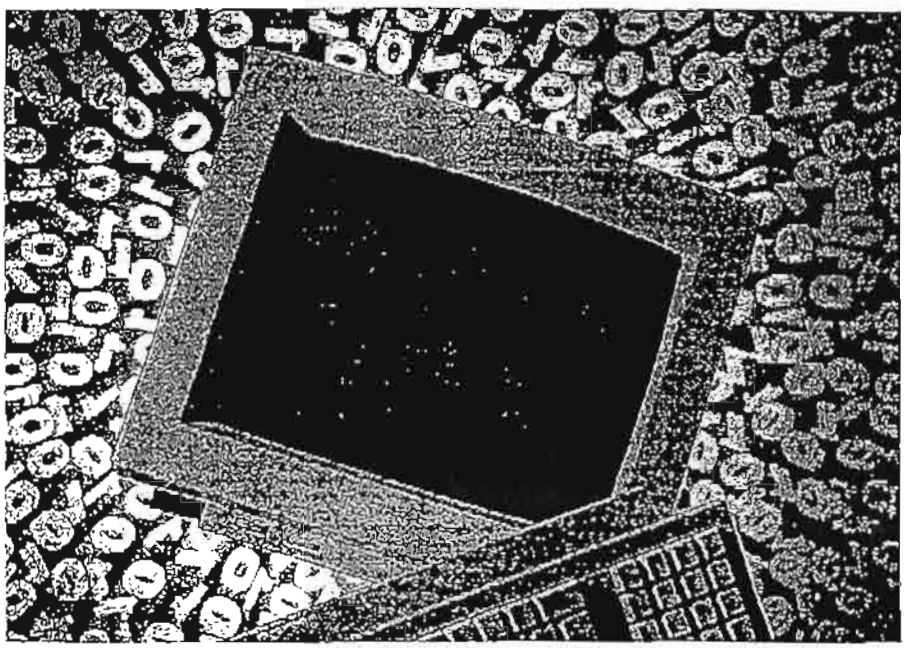
London Offices:
Barlow Lyde & Gilbert
Beaufort House
15 St. Botolph Street
London EC3A 7NJ
Telephone: 0171 247 2277
Fax: 0171 782 8500
DX 155
and at Lloyd's

Hong Kong Office:
Barlow Lyde & Gilbert
4010 Jardine House
1 Connaught Place
Central
Hong Kong
Telephone: 25264202
Fax: 28105994
(Contact Cameron Scott)

European web site http://www.blg.co.uk
North American web site http://blg2.com

Computer problems 2000

The millennium muddle



Many companies are facing an enormous hurdle that they do not even know about yet. A time bomb is ticking away in mainframes, personal computers, processing chips and traffic control systems. Its effects could be devastating. Why? To save expensive and precious memory in the first generation of computers, years were recorded as two-digit numbers, for example 65 instead of 1965. Only at the beginning of the 1990s did computer programmers realise the chaos that this could cause at the turn of the century. Although a technical solution to the millennium problem is actually quite simple, the added costs and follow-up charges caused by it are considerable. The "millennium-bug" is certain to be a major concern for the insurance industry. In the meantime, the following rule of thumb holds true for the computer date dilemma: "burning buildings" are not insurable.

Monday, 3 January 2000. Eric B. Head of the Logistics department with a pharmaceutical firm, joins a group of bewildered colleagues at the company gates. An employee from an external security firm is handing out new passes for entry to the premises and distributing circulars to all employees. They read "...unfortunately we realised only on 1 January 2000 that our security system is not yet equipped with year-2000-compatible card readers."

It gradually begins to dawn on Eric. The computer systems have gone haywire! The year-2000 problem had been the number one joke at the New Year's Eve party, but Eric had not really taken it seriously. And he certainly had not thought that it would affect his own firm. After all, the pharmaceutical firm had taken precautions. An internal working group had been set up two years ago. And whenever they made an announcement, it was, "No problem. Everything's under control."

The secretary is waiting impatiently for Eric with a fax. A hospital is in desperate need of medicine Z for burn victims. A defective traffic light on New Year's Eve caused two buses to collide and burst into flames. Many of the injured will only survive if medicine Z is supplied by the company within two days.

The manager of the high-rack storage warehouse has already tried to retrieve medicine Z, but first he had to switch the lift to manual operation, since an error had shut down the automatic system. In addition, the computer record showed several power cuts on New Year's Eve.

These inconsistencies prompt Eric to check the updated list of products which is automatically produced on the first day of the month. His heart skips a beat: medicine Z has been disposed of! The disposal process is computer-controlled and is carried out according to product expiry date. The computer deletes the relevant location from the warehouse shelving and sends the product to be disposed of. Medicine Z has been incinerated.

Eric stands rooted to the spot. The supplier of the high-rack storage warehouse had offered to adapt the system's software two years ago to help to prevent problems, but the pharmaceutical firm had turned down the offer. The budget was tight and no-one had imagined that such serious consequences could be caused by the new millennium.

The true gravity of the situation slowly becomes clear: several victims in the hospital would probably die and others would have to live with severe after-effects. In their contract, the pharmaceutical firm guarantees delivery to the hospital within two days. It is impossible for the company to keep its side of the agreement because its entire stock has been incinerated and a new batch would take at least a week to produce. The hospital would have the option of taking legal action against the firm; there could be liability claims from the burn victims or their families. It would be difficult to hide the incident from the media; and the negative publicity would have an immediate impact on the company's share price.

Many computer programs only record years as two-digit numbers in data fields, for example 150397 for 15 March 1997. When the year becomes 00 in the year 2000 this may have far-reaching consequences because many systems are unable to interpret the two digits unambiguously. For example, the machine could interpret the date 010400 as either 1 April 1900 or 1 April 2000. This ambiguity will cause the miscalculation of periods of time. 2001 minus 1997 leaves 4; 01 minus 97 leaves -96 or even 96. The computer will then use these figures to produce incorrect results, or the system will fail altogether.

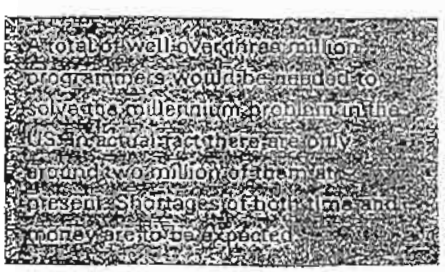
The roots of these problems lie in the origins of the computer age. Spare memory on punch-cards was an expensive luxury in the 1950s and 1960s. Saving only the last two digits of the year thus became quite commonplace, programmers did not question the lifespan of the programs, micro-processors or chips. The practice was only slightly modified at the beginning of the 1990s, when the first warning signs started to appear.

The year-2000 problem could affect all of us, either directly or indirectly: privately, with health insurance or pensions, as drivers or passengers, as electricity consumers, as owners of a malfunctioning car navigation system, etc. Even a firm which has managed to eradicate the millennium bug for itself is not guaranteed immunity. Economics departments or controllers everywhere work with imported data. In addition, certain errors will not be immediately recognisable and for the time being will work their way unnoticed into statistics, individual calculations or controls.

The internationally renowned consultancy Gartner Group estimates the costs of adapting computer programs at USD 600 billion worldwide. In many places, particularly the US, large claims for compensation will also be lodged. In the worst case, courts will face a barrage of legal action.

The countdown has begun

A comparison of the millennium problem in the US and in the EU shows that time may be running out for many companies, particularly in Europe. There is a distinct



lack of qualified specialists still able to understand the early programming languages. Many firms specialising in eradicating the millennium bug are already fully booked.

The effects of the millennium bug

Area	Possible effects	Type
Warehouse/ logistics	– Orders are carried out on the wrong day or not at all – Erroneous expiry date causes the rejection of intact goods – Customer data is deleted	1, 2, 3, 4
Patent Office	– Patent specifications are released too soon	1, 3, 4
Lifts, production systems	– Processors provide incorrect dates – Systems may shut down or fail completely	1, 3, 4
Traffic control systems	– Incorrect dates lead to blockages (potential traffic chaos, accidents, etc)	1, 4
Power stations	– Plant shut-downs because individual sub-systems fail, possibly resulting in electricity shortages	1, 3, 4
Access control systems	– Buildings and industrial complexes will remain closed as individual components fail	1, 3, 4
Building control systems	– Buildings will not be heated (for example causing business interruption and frozen heating systems) – Cold-storage depots will not be operational (spoilt goods which will then have to be disposed of)	1, 3, 4
Telephone switchboards	– Incorrect price calculations and business interruption	1, 2, 3, 4
Hospitals	– Life-support machines fail – Patient data is lost, incorrect treatment is the result	1, 3, 4
Consultants/ engineers	– Incorrect processing dates lead to large interruption in business for customers (for example industrial plants)	1, 2, 3, 4, 5
Financing/ banking	– Payments and orders are not carried out – Mortgage interest lost because dates have been saved incorrectly	1, 2, 3, 4, 5
Accounting	– Customer data is processed incorrectly or lost	1, 4
Life insurance	– Statistical data is selected incorrectly – Incorrect results lead to errors of judgement	1, 2, 3, 4, 5
Marine transport	– Control and steering systems will be disrupted	1, 2
Aviation	– In the global reservations network, erroneous dates will be read in through individual interfaces, causing incorrect passenger bookings	1, 2, 3, 4
Archives	– Results of statistical analyses could be calculated incorrectly	1, 2, 3, 4, 5

Causes

Type 1:
Incorrect century if the prefix is always assumed to be 19. Problems occur if this is ignored when entering or updating data. This results in incorrect data, calculations or days of the week. It should also be borne in mind that the year 2000 is a leap year.

Type 2
Special figures such as 99 or 00 have been used in two-digit entries for specific codes such as "no extension" or "year unknown". In 1999 and 2000 this will lead to miscalculations or total system collapses.

Type 3:
Arithmetical calculations for two-digit years pose a particular risk because the programs may carry out further calculations using meaningless or erroneous results. The computer would calculate someone born on 3 April 1980 as being either -80 (00-80) or, ignoring the first two digits, 80 in the year 2000. It may then be that this person is suddenly classed as a pensioner. In many cases, this data would then be exported to other companies.

Type 4:
If data sequences are sorted on the basis of their two-digit year then statistics will contain incorrect values because the year 2000 (represented by 00) will be classified before and not after 1999 (99). As a result data may be deleted or products destroyed because their selection age is too high, or the expiry date is assumed to have passed.

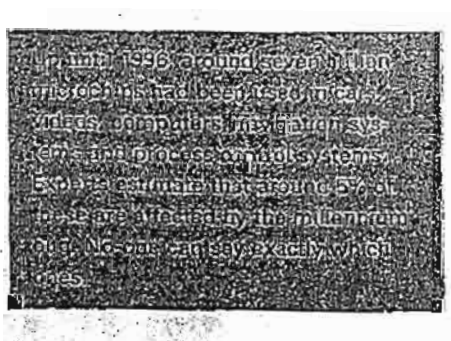
Type 5:
Two-digit years also falsify historical data because no differentiation can be made between the year 2000 and 1900, and later decades.

The millennium muddle is not simply a technical problem. It represents a challenge for management in general. In addition to the technical aspects, administrative, legal and economic factors also play a significant role. Another important factor is time.

Technically the solution is quite simple, but it can require considerable amounts of money and manpower. Basically, companies can approach the millennium problem in one of four ways:

1. Do nothing, and wait and see what happens when the computer or the plant is switched on at the beginning of January 2000. This alternative is particularly appealing to small and medium-sized companies, but may plunge the company unprepared into a potentially dangerous situation.

2. Replace everything and make all systems year-2000-compatible in one go. This option may be worth considering for smaller companies which do



not have large amounts of stored data. The expenditure on new machines and software is thus relatively low.

3. Carry out simple improvements. For many software packages, alterations are easy. Normally, data is affected only slightly, if at all, but it must still be analysed.

4. Carry out a thorough analysis and establish compatibility. This is by far the most comprehensive approach, but also causes the most expenditure. It includes analysis, transition to a correct date format, testing the relevant plants and applications and drawing up emergency plans.

A comprehensive approach

If a company chooses the comprehensive approach to tackling the millennium problem, it must first assess its exposure and analyse all aspects which could pose a threat to the company. The process may be split into three phases as follows:

- Internal: internal IT, production plants, access control systems, logistics, in short anything with an embedded computer chip, should be examined for compatibility with the year 2000.
- Business relations and interfaces with other companies (customers, suppliers): the company must assess how customers and suppliers may be affected by the problem and how any difficulties which may arise will affect the company itself.
- Dependencies on (public) infrastructure: the potential effects of the turn of the century on the company itself should be analysed. What would happen, for example, if there was disruption to the electricity supply or telephone network?

A company is only able to develop a methodological and comprehensive procedure if it uses an identical approach to each of the three phases. The cost of stocktaking can sometimes be considerable. Companies would do better to concentrate their efforts on components which are critical to the firm's activities. For most companies, an access control system is not as critical as the telecommunications network or a computer-controlled warehouse. External interfaces are also important. Coherent communication with partners can be effective in overcoming the millennium problem

Once stock has been taken, the actual exposure must be analysed. Only then can the modification of the programs begin. Here, it necessary to ensure that the correct software tools are used. This can noticeably accelerate the conversion process, thus creating drastic time advantages. Again, manpower requirements should not be underestimated.

The next step is testing, which plays a key role in the entire process. According to different estimates, testing the converted components can contribute around 40% to 60% of the total cost. On completion of the tests, a year-2000-compatibility certificate should be requested. Use of the correct software tools can also save large amounts of time and money during testing.

Creating acceptance

The key aspect in overcoming the millennium problem is clearly good project management. One of the major responsibilities of management must be to ensure that communication is continuous and transparent from the outset. If this is not the case, the project may overlook some important aspects. Each stage of the process should be adequately communicated; this will ensure that the entire process is accepted amongst employees.

The communication process may incorporate the following:

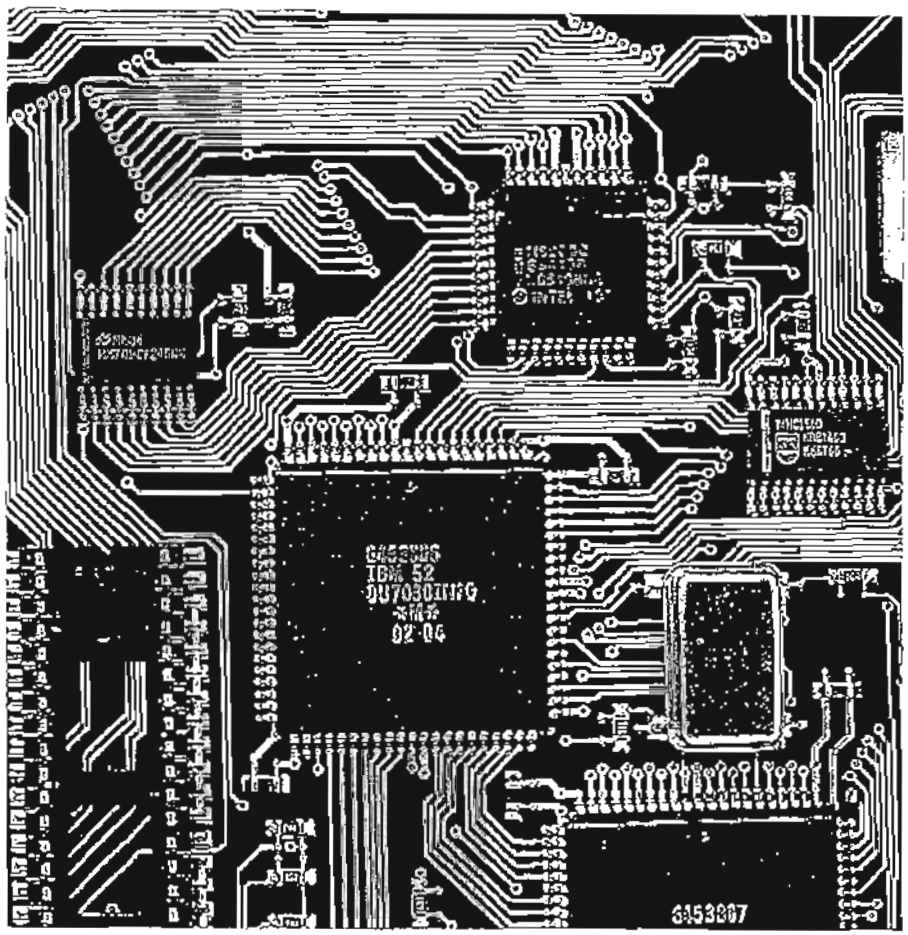
- Creating awareness amongst those affected (presenting the problem, informing employees what is expected of them, defining technical standards).
- Preparing the process (defining procedure including all company relations, determining strategies regarding legal obligations, insurances, etc)
- Identifying communication channels and ensuring communication throughout the process.
- Carrying out the conversion (monitoring tests, ensuring timely completion of the project, drawing up emergency-plans, and assessing the risk remaining for the company)

Orders carried out incorrectly, mis-sorted goods and deleted customer data; will the millennium muddle cause chaos in the warehouse?

Viewed economically, losses resulting from the millennium problem and their prevention can be extremely costly. It is too early at present to predict to what extent the insurance industry will be affected.

In line with the principle "burning buildings" are uninsurable, it is possible to exclude known loss situations by observing prudent underwriting policy. A "non-fortuitous event" or "knowledge of the deficiency or harmfulness of goods or services" are regularly excluded from cover. We know today that the millennium problem can cause losses, which means that although the building is not yet on fire the matches are lying around. Since many policies commit policyholders to carrying out loss prevention measures, it is the responsibility of the insurance industry to contribute to clarification and to point out the possible consequences of passivity.

In all probability, the insurance industry will face claims for compensation arising from the millennium muddle. These will focus on liability, property and certain types of engineering insurance, as well as marine, hull and aviation. The different cover descriptions in each branch and the varying legal situations in each country make an accurate estimate of claims difficult.



Electronics – an essential part of everyday life

Pure economic loss covers are exposed

The problems associated with the millennium change will focus particularly on the additional financial outlay involved. Most policies are limited to compensation for property damage and/or bodily injury and do not normally extend to pure economic losses. However, poorly-worded covers and specific covers for pure economic losses may well be exposed.

In liability insurance business, policies which cover pure economic losses (professional indemnity, directors & officers and certain product liability policies) are most likely to be affected by claims for compensation. Professional liability policies provide liability coverage for bodily injury and/or property damage. In general, the legal variety and the differing formulations of insurance conditions make liability insurance complicated, for example different definitions of the trigger of coverage depending on the country and line of liability insurance.

In the property insurance field, fire, marine and engineering policies may be affected. This may be the case if the millennium meltdown triggers a highly improbable fire or explosion, ie a "hot" loss, or if goods are no longer traceable or the ship or steering computers crash. If a "cold" property loss occurs (for example machinery breakdown, water damage), it depends largely on the circumstances and formulation of cover as to whether the policies must pay up. Avoidable losses or those caused purely by "program error" should actually be excluded; all-risk policies sometimes contain such extensive and vague wordings that there is likely to be a large amount of uncertainty. Larger potential losses may also be incurred from business interruption following property damage. Whether these are insured or not depends on the same principles that apply to the property losses which caused them.

Even traffic control systems are not safe from the millennium bug

Since it is barely possible to quantify the potential loss, the insurance industry must take a differentiated approach to the problem. Procedures and measures must be adapted to suit the extent of cover. The table on page eight shows the options available to insurers when renewing existing policies, writing new business or reviewing their portfolios.

New insurance products

Many losses resulting from the millennium muddle will not be covered under classic insurance policies if steps towards prevention have not been taken. Neither is it the responsibility of the insurance industry to reimburse through insurance the obvious expenditure of a company in overcoming its millennium problem.

Even if a company has taken all reasonable precautions to counter the problem, it is not possible to rule out financial loss caused by business interruption when the new century dawns. A number of insurers have been developing specific products with brokers to insure this residual risk, the main emphasis being:

- Guaranteeing cover requires a detailed risk analysis. This creates the environment for effective loss prevention and thus insurability.
- The lack of loss experience for this one-off event makes it difficult to set adequate premiums. The increased risk must be reflected in a relatively high premium level and limited cover. Risk financing may be a genuine alternative to traditional products.

Swiss Re Zurich's mainframe computer runs 5000 computer programs, approximately 1500 of which have a millennium problem. Swiss Re reacted quickly to the problem and commissioned a team of experts to find a solution. All programs should be year-2000-compatible by the end of March 1998 and the subsequent test phase can begin. The total cost will be approximately six million Swiss francs.

Within the insurance industry, the direct insurers carry the main responsibility for the financial consequences of the millennium problem. Reinsurers are supporting insurers in their efforts to implement correctly the basic principles of insurance. However, specific reinsurance covers must be established for insurance products aimed at coping with the residual risk, since these do not fall under traditional reinsurance treaties.

Possible ways of dealing with the millennium problem in exposed insurance covers:

Policy			Measures
New business	Renewal	Portfolio	
+	+	+	Sensitise the insured to the millennium problem (bulletins)
+	+	+	Perform risk analysis to assess the insured's exposure (questionnaire, visit,
+	+	+	Provide loss prevention advice
	+	+	Commit the insured to eliminating threatening circumstances (insured must inform recipient of products/services and examine own computer systems)
		+	Amend policy wordings in agreement with both parties
+	+		Record in writing the level of the insured's exposure (duty to disclose the extent of the millennium problem in the application for insurance cover)
+	+		Introduce specific obligations
+	+		Introduce specific exclusion clauses for highly exposed insurance covers

Telephone: +41 1 285 21 21
Fax: +41 1 285 20 23
E-mail: publications@swissre.com
Internet: http://www.swissre.com

Authors:
René Favre,
Daniel Gantner,
Robert Wiest

Translation by Swiss Re Language Services

Produced by:
Product Management department
Knowledge Transfer section

Photographs:
Fotostudio H.R. Bramaz, Zurich, pp 1, 5, 6
swissecontrol, Berne, p 7

PM, RD, EN 11/97 3000e