Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Cyber Risk Insurance

The discussion presented offers insight to the implications of insurance and cyber crime coverage and to raise the awareness of the uncertain ties within cyber insurance. The insurance industry is attempting to understand the nature of cyber crime issues and how to more accurately design insurance policies for the future. In an effort to protect against unlawful electronic or physical activity, organizations are now taking a closer look at how their implementations are performing and what is needed to protect confident...

Copyright SANS Institute
Author Retains Full Rights

AD

Cyber Risk Insurance

A Discourse and Preparatory Guide

Denis Drouin

February 9, 2004

GIAC Security Essentials Certification

Practical Assignment Version 1.4a, option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Abstract.....3
Insurer's Issues.....3
Insured's Issues.....6
Breaches: For the Taking.....7
Insurance Policy Coverage.....8
Industry Threat Statistics.....10
Privacy Legislation.....12
The Law.....16
Infrastructure Preparation.....18
Final Thoughts.....26
References.....27

© SANS Institute 2004, Author retains full rights.

Abstract

Technology has continued to astound the world's electronic culture by reacting with the use of mechanisms to defend and protect against the unknown. Cyber insurance has been one of those phenomenons that has experienced many challenges and at the same time mutated into a more complex tool to protect companies. It has perplexed those who had thought that with protection from the cyber zone they would be safe from engaging foes. The discussion presented offers insight to the implications of insurance and cyber crime coverage and to raise the awareness of the uncertain ties within cyber insurance.

The insurance industry is attempting to understand the nature of cyber crime issues and how to more accurately design insurance policies for the future. In an effort to protect against unlawful electronic or physical activity, organizations are now taking a closer look at how their implementations are performing and what is needed to protect confidential assets. The ill effects or inabilities have proven costly to the insurance industry and has triggered a sense of desire to define more efficient controls to mitigate the burden of settlement. With recent national and international regulations, organizations face even greater challenges to ensure that information assets and those environments that house critical information are proactively protected against unauthorized breaches. Insurance companies are realizing the need to implement greater assessment capabilities to determine the state of an organizations security infrastructure when examining an organizations request for coverage.

We will examine what technology based insurance policies are available to the insured, what protection is likely required, the liabilities organizations face, and remedies that will lessen the impact of cyber crime. Technology is changing and the effects it will have on organizations over time will change how insurance awards or denies reparation. Liability is a very complex term when it comes to insurance related matters. In many instances liability is tested through the lengthy process of suit and a final ruling of judgment, or is it simply a matter of the mere definition of clauses that fill the page. Let's take a look.

Insurer's Issues

Since 1995 e-Commerce has emerged as a viable method of doing business yet increasing the ability of undesirables to create true Cyber Risk as we now know it. Over this period, insurers began to manage insurance claims they had never contemplated using polices that were founded upon a very confusing medium. Consequently, e-commerce data exclusions (no direct statement of data protection either logical or physical) are now common practice in the development of insurance policy. Insurance underwriters now must scrutinize policy applications and recommend to clients that they educate themselves. Organizations should become aware of the ever increasing onus upon their infrastructures to engage in the education of technological risks that affect their environments and the options to deal with these risks. Organizations in the non-Fortune 1000 layer are less likely to acquire coverage for exposures either due to the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

minimal infrastructure that is required by the underwriter's standards, or that costs are out of reach.

Geography plays a significant role in what insurance options are available to organizations. In the US for example, a greater selection of insurance options are accessible to insured's than those that are offered in Canada. Some of the major insurance companies in the US have good e-commerce/cyber risk products. In Canada, many of these same policies may not be available, largely due to the fact that insurance premium base that is available to cover cyber-risk exposures is too small. This is slowly changing.

Any technology related business should prepare and conduct a thorough cost-benefit analysis before the organization leaps into any new security technologies or plan a security strategy. If your company does business on computer systems or web sites, you may need cyber liability protection. The technology insurance application is intended to act, in part, as a perfunctory assessment of your organizations current technology stance. This evaluation is a strategic tool used to determine whether your company is granted coverage. There will be questions posed to the organization as to whether it has suffered any prior incidents involving their network(s) and electronic environments. If the organization fails to reveal any details relating to a prior incident, the insurer may decline processing the application due to improperly disclosing application details. Insurers must grapple with two distinct results of financial impact to an organization, financial fraud and theft of proprietary information. Identity theft is on the rise and one of the most profitable unlawful money generators in the technology world. If an organization is found liable, theft of client information could ultimately sink the organization, destroying partnerships, and credibility. Even if not found liable, this exposure could still very easily damage the integrity of the business entity.

Fraud is a very hot issue in the insurance industry, in earlier years an investigations most effective method to detect illegal activity had simply been a matter of accidentally discovering fraud. Originally, most technology-based fraud detection capability was designed into hard-coded programs which flagged known suspect circumstances; for example, a financial institution might flag account withdrawals of $10,000.00 cash for personal chequing accounts. Eventually, fraud artists would learn that multiple withdrawals of $9999.99 or less would not trigger an alert. Multiple withdrawals of this size became quite lucrative.

Later, relational databases and analytical tools allowed insurer's to detect and defuse fraud affecting organizations. This process employed query languages using 'if, then, else' tests allowing the carriers to process large volumes of data. This assisted with the identification of patterns and trends to better predict potential areas of fraud. Nevertheless, this process required the insurer to look for the known triggers, identify them, and use this process to confirm their suspicions. Even when fraud patterns were detected, the time and effort it took to make the necessary system changes would often leave the insurer fixing a problem long after the fraud perpetrator had moved on to uncover a new opportunity. These methodologies were often not worth the effort even if

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

a fraud was uncovered. The value of the policyholder relationship often proved to be a detriment and not worth the cost of damaging the insured's confidence as the insurer would scrutinize the legitimate claimant's position while being closely examined.

Fraud technology has gained greater ground in the past couple of years by offering toolsets and software with advanced computational techniques. These techniques have allowed investigators to learn from experience and to advance their ability to better understand fraud detection and pattern identification. Artificial intelligence will allow software to examine more finite details of fraud tactics and assist reviewers in detecting fraud faster. These techniques will shift the burden of detection from the human element and reduce the number of false positives that need to be examined. But, the perpetrators will continue to refine their fraud capabilities and find new ways to infiltrate organization's information systems. Combining the early generation of fraud-fighting tools with these new advanced predictive analytics and adaptive optimization techniques (such as, rough sets, classifier systems, and revolutionary programming) gives the insurance industry the opportunity to gain ground in the fraud race. This may allow the insurers to come closer to tracking this form of crime but not necessarily keep pace with the wrong side of the law.

Today, the risks of cyber fraud are ever increasing. They can include stealthy espionage challenges to drive-by attacks that include denial-of-service and web defacements. Insurer's have realized that the General Liability policies of past do not meet the requirements of today's standards [1] Insurers Rethinking IT Coverage For 2002" (http://www.informationweek.com/story/IWK20020102S0004). Insurer's are suggesting that organizations acquire "'stand-alone" polices specifically designed for specific occurrences of disruption, such as a hacking events [2] "Firms' hacking-related insurance costs soar" http://www.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm. This of course will require more funding to protect against the unidentified. If it is decided to limit protection, organizations may find that when it comes to fending off legal action from clients and business partnerships they may be on their own. Virus and worm coverage is a form of insurance that has not matured due to the nature the more powerful strains of viral forms yet to surface.

Brokers represent organizations by way of developing technology policies that match the organizations protection requirements. They can tailor policies in such a way that will more closely meet an organization's insurance protection needs in order to limit liability exposures. Anytime an organization is pursuing a broker to represent its interests, the organization should take the time to request and review a copy of the brokers proposed submission so that the requirements are clearly detailed and understood. Otherwise, the organization may be left with policies that do not serve their immediate protection to reduce and mitigate exposures. Performing a self-assessment allows and organization to systematically identify and consider computer security issues. There is great importance that must be given to the process of self-assessment discovery as it becomes the vehicle that will divulge how the business functions and what is needed to ensure that it continues to function after a disruption of services.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Insured's Issues

There is no panacea. In recent years, organizations have recognized the level of importance associated with the risk of doing business electronically and the security requirements required to establish a safe and competitive presence. Recent regulations and standards have also forced many organizations to rethink they way they do business. They appreciate that there are threats that could disable their ability to continue participating as an electronic business. Organizations are able to acquire coverage even if they have merely met the minimum standards established by the insurance industry. This attitude towards a stable security stance can become the devils sickle. If an organization fails to implement a strategy that is adequate to industry standards as well as to conform to an ongoing security stance, clients will not have establish the confidence in their provider, and will have little assurance that their personal information is not at risk. Electronic users are beginning to realize that their information is important to them, although many are still willing to allow their personal information to be manipulated unknowingly. This may be the result of confusing wording presented by a provider that the user does not understand or could not be bothered to read. Many times this is related to the lack of education and awareness of the user.

It is necessary to identify the two inter-related aspects of computer incidents, that is, accidental and intentional. Computer-related activities such as loss of data from power blackouts may be characterized as accidental. The other form is intentional, for example, an attacker breaches a network's defenses and infiltrates internal servers and networking devices. The latter of these could also affect critical infrastructures that support general populations, potentially catastrophic situation. As technology improves, so does the ability to move information more swiftly, process data at higher speeds, and reduce the size and number of machines required to perform calculations that once took five times the equipment and manpower. Therefore it is necessary for organizations ensure that they are keeping pace with technology and continue to be vigilant with updating procedures, training, and maintaining an awareness of the perils of the Internet.

Other concerns that face insurance companies include the wording of their insurance policies and how the courts will test cyber liability with respect to the physical theft of electronic data. It has yet to be established how the courts will decide whether data stored on a harddrive that was stolen, damaged/destroyed, or written over mistakenly, be determined as actual physical property. Most courts have ruled that data is not considered physical property as tested against the "Direct Physical Loss" legislation. The insurance industry does not consider loss of confidential information as property. Physical security and cyber/logical controls, such as facility planning and equipment theft prevention disciplines, will become more interrelated as infrastructure demands increase. This is a topic that has been misread over the years, but we are now seeing these two dimensions come together. It is also unclear whether the insurance industry and the courts will, at some time, find that information assets are indeed real property.

It is important to outline the meaning of "property insurance". This coverage is designed for the purposes of business interruption, where an organization incurs a direct loss.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

This type of coverage is designed for losses against physical assets and physical peril, not for information assets and electronic risk. Other risks include intellectual property that which is stored electronically is deemed as “data”. It is important to note that policy coverage is not worldwide. Each organization must determine its reach to its clients and the potential risks associated with multiple jurisdictions. Insurance policies have become more restrictive. In order to acquire the right coverage an organization may have to purchase multiple policies in order to ensure reasonable coverage, whereas in previous years it was more likely that a single policy may fit all its needs. Organizations implementing a website or a computer network may require a number of policies such as, intellectual property, privacy, network security, and data integrity insurance.

Insurance related risks may include organizations having underdeveloped policy and procedures that fail to satisfy insurance coverage or establish a firm line of conduct within the infrastructure. In many cases, policies that have been implemented exclude processes that are critical to day-to-day support. For example, simple back up and restore procedures are non existent for support personnel and even if they do exist would fail to provide the administrator or support personnel with steps to assist with a quick recovery. A worst case scenario, the administrator is not available to respond; the individual who is restoring the backup media has little or no experience in an emergency situation. The recovery process could be further delayed or possibly equipment or software effected beyond recovery. How will insurance cover this form of incident, if at all? Were procedures available to guide the recovery process to a normal state of operation? These considerations must be examined thoroughly.

Breaches: For the Taking

The wiley hacker, it seems, has more to gain these days, or does she. Until recently, the hackers have had great opportunity and substantial ease of breaking into networks of varying size and complexity and having their way. Today, industry is experiencing new legislation that imposes strict standards and expectations upon its networking environments. Law enforcement has also stepped up to the bar and now is being given greater ability to locate, seize, arrest and prosecute illegal entry. The law enforcement community has developed far reaching relationships and is now coming together as extended families encouraging cross-informational communication to track down occurrences of cyber wrong doing. All the while, the hacking community becomes more sophisticated with technology and its ability to infiltrate and traverse the sensors that attempt to track their movements. In any case, organizations can recoup a variety of costs with insurance. For example, it could help companies that are sued for downstream liability, in cases where one company's systems are used to attack another’s servers. Insurance can also cover downtime for a company that was attacked. Organizations need to ensure security budgets are sufficient to support current needs, but also to establish a long-range plan as technology shifts into high gear. [3] “Corporate security spending not in line with real-world requirements” http://www.nwfusion.com/news/2003/0505nemertes.html.

This appears to be an indicator as to why many insurance companies are no longer offering technology insurance due to the complexity of determining how to develop a

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

specific policy and what constitutes a cyber incident or service disruption. The other reality is that the surmounting costs of this form of insurance can, in some cases, out weigh the necessity and risk associated with cyber incidents.

Insurance Policy Coverage

Insurance companies offer numerous variations of coverage which has, to say the least, perplexed organizations more so now than in past. Organizations have similar yet disparate business requirements in terms of the level of protection required to protect against losses. This presents a situation where each organization must take the initiative to fully comprehend its existing level of protection requirements before it engages in the insurance application process. The insurer may not necessarily request a security assessment report, but it may need to see some proof of infrastructure preparation before the application is processed. For example, if an organization provides website services and purports to have a firewall which protects all clients' information, yet the organization is not regularly monitoring the firewall, applying patches regularly, and monitoring the technology, this would reflect a risk to the enterprise. This deficiency of IT management could leave the organization with questionable coverage or a lengthy litigation process if systems were damaged, hacked or destroyed. Part of the assessment exercise is to determine whether the organization has adequate controls and procedures in place to-maintain a constant vigilance within the environment. Otherwise, if damage is incurred, the organization may not have the ability to recover or protect itself from technical damage and potential litigation.

If, for example, an organization simply carries a CGL (Commercial General Liability) policy, it would be a long shot to expect that this form of insurance would provide sufficient protection from a website hacking incident or other relative disaster. Generally, organizations should carry at least three typical technology policies in its portfolio, these being E&O (Errors and Omissions), D&O (Directors and Officers) liability, and EPL (Employment Practices Liability) insurance. If you're an organization who is providing, for example, online web services, development or hosting services, and possibly other services or combinations thereof, then this is the time to ensure that the organization has a complete understanding of its business critical mass. This message must resonate throughout the organization. There shouldn't be issues of unfounded information regarding who was supposed to do what and why it wasn't done. Point of interest relating to Canadian technology insurance statistic [4] "Insurance. What's going on?" http://www.yorktech.ca/events/10-30Presentation2.pdf.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The table below lists policy structures that are typical of cyber associated insurance coverage available on the market today.

Insurance Policy Coverage Options **(These policy descriptions will vary – these are not exhaustive)**	
Option	**Description**
General Internet Crime Liability	Addresses the first- and third-party risks associated with e-business, the Internet, networks and informational assets. Limitations exist with this level of coverage. It is key to review your business activities to ensure appropriate coverage.
Property	Protection against damage to hard assets caused via the internet, machinery taken down, or equipment programmed to operate erratically. Typically, this policy does not acknowledge "data" as property.
Errors and Omissions (see Professional Liability)	E&O liability protects your organization from claims if your client holds you responsible for programming errors, software performance, or the failure of your work to perform as promised in your contract.
Professional Liability (see Errors & Omissions)	Provides protection against claims that the policyholder becomes legally obligated to pay as a result of an error or omission in his/her professional work. Also known as Errors and Omissions insurance, this type of professional liability insurance is critical to your business. E&O insurance responds to claims of professional liability in the delivery of your technical services.
Directors and Officers Liability	Required by a board of directors to protect them in the event they are sued in conjunction with their duties.
Employment Practices Liability	Protects employers against claims made by employees for discrimination (age, sex, race, disability, etc.), wrongful termination, and sexual harassment.
Business Interruption	Physical damage is not the only consideration when determining potential disaster scenarios. An organization should also include death, disability or kidnapping of key personnel; Defection of key personnel to a competitor; Theft of Trade Secrets; Image Management (public perception).
Kidnap/Ransom & Extortion Coverage (see Business Interruption)	Provides coverage for kidnappings and other events through a combination of financial indemnification and expert crisis management.
Group Personal Liability	Coverage for key personnel, managers, and employees.
Key Person Life Coverage	This coverage is designed to protect your business upon the loss of a key employee. The tax-free proceeds from this policy can be used to find, hire and train a replacement, compensate for lost business during the transition, or finance any number of timely business transactions (typically found in US policy structure).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Media Liability Coverage	Protects you against claims arising out of the gathering and communication of information. Media Liability Insurance provides very valuable coverage against defamation and invasion of privacy claims as well as copyright and/or Trademark infringement. (investigate and clarify the level of privacy coverage before acquisition).
Fidelity or Crime Liability	Protects organizations from loss of money, securities, or inventory resulting from crime.
Network Security Coverage	Protects you from losses associated with unauthorized access to or theft of your data or e-business activities, computer viruses, denial of service attacks, as well as alleged unauthorized e-commerce transactions.
Intellectual Property	Protects companies for copyright, trademark or patent infringement claims arising out of the company's operation. Items such as all working papers, records, trade secrets, data, methodologies, drawings, software, documents or other writings created, developed or acquired the company. This includes any documents, records, trade secrets, data, drawings, software or other writings created by or supplied to or made available the company.
Patent Coverage	A policy which reimburses the insured for defense expenses and damages paid by the insured resulting from allegations that the insured has infringed on a patent, copyright or trademark of a third party.
Workplace Violence coverage (see Business Interruption)	Protection against the expenses that a company can face resulting from incidences of workplace violence, including the cost to hire independent security consultants and public relations experts, as well as payment of death benefits and business interruption expenses.

It is imperative that any insurance acquisitions be investigated thoroughly before any decisions are made. If the incorrect insurance is obtained, the organization may be left vulnerable to liability even if they think they are covered appropriately.

Industry Threat Statistics

In 2003, the CSI/FBI released its 2003 Computer Crime and Security Survey [5] http://www.gocsi.com/ referencing respondent's insights into cyber crime incidents and the financial effects on their organizations. There were 530 security practitioners who offered their responses from industries such as, U.S. corporations, government agencies, financial, health, and educational institutions. This survey suggests that even though there continued to be steady activity in the cyber warfare community, the financial effects of those deeds had showed a reduction in losses from the previous year. Cyber attacks continued at a high level of activity which only means that even due to the efforts of security practitioners to implement protective measures illegal behavior continued to occur. The survey suggests that most attacks occurred from an external source. The primary response to these incidents was to patch known vulnerable machines. Still, many organizations are not reporting incidents of this nature in an effort to avoid negative public relations, weakened marketing position, and competition seeing

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

opportunity with the negative position of the organization. Some regulatory associations are beginning to require that organizations impacted by uncontrolled incidents, must report these disruptions.

Noted, are a few excerpts from the CSI/FBI survey relating to the number of incidents and the direction in which they were identified (first three tables listed on page 7, and fourth table listed on page 12 of survey):

How Many Incidents?						
By percentage (%)	**1 to 5**	**6 to 10**	**11 to 30**	**31 to 60**	**Over 60**	**Don't Know**
2003	38	20	More:16	0	0	26
2002	42	20	8	2	5	23
2001	33	24	5	1	5	31
2000	33	23	5	2	6	31
1999	34	22	7	2	5	29

2003: 356 Respondents/67%, 2002: 321 Respondents/64%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%

How Many from Outside?						
By percentage (%)	**1 to 5**	**6 to 10**	**11 to 30**	**31 to 60**	**Over 60**	**Don't Know**
2003	46	10	13	0	0	31
2002	49	14	5	0	4	27
2001	41	14	3	1	3	39
2000	39	11	2	2	4	22
1999	43	8	5	1	3	39

2003: 336 Respondents/63%, 2002: 301 Respondents/60%, 2001: 316 Respondents/59%, 2000: 341 Respondents/53%, 1999: 280 Respondents/54%

How Many from Inside?						
By percentage (%)	1 to 5	6 to 10	11 to 30	31 to 60	Over 60	Don't Know
2003*	45	11	12	0	0	33
2002	42	13	6	2	1	35
2001	40	12	3	0	4	41
2000	38	16	5	1	3	37
1999	37	16	9	1	2	35

2003: 328 Respondents/62%, 2002: 289 Respondents/57%, 2001: 348 Respondents/65%, 2000: 392 Respondents/61%, 1999: 327 Respondents/63%

Dollar Amount of Losses by Type	
Incident	**Financial Impact**
Unauthorized and Insider Access	$ 406,300
Financial Fraud	$ 10,186,400
Telecom Fraud	$ 701,500
* Theft of Proprietary Information	$ 70,195,900

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Virus	$ 27,382,340
Laptop Theft	$ 6,380,500
Insider Net Abuse	$ 11,767,200
* Denial of Service	$ 65,643,300
Sabotage	$ 5,148,500
System Penetration	$ 2,754,400
Telecom Eavesdropping	$ 76,000
Active Wire Tapping	$ 705,000

CSI/FBI 2003 Computer Crime and Security Survey / Source: Computer Security Institute 2003: 251 Respondents/47% R d / %

In May of 2003 the AusCERT (Australian Computer Emergency Response Team) presented a survey [6] "Australian Computer Crime and Security Survey" http://www.auscert.org.au/render.html?it=2001 outlining a number of issues relating to cyber crime and organizational impacts suffered as result. This survey is built upon the CIS/FBI Computer Crime and Security Survey.

Privacy Legislation

Privacy has become one of the latest players in the arsenal of federal, provincial and state controls to ensure that organizations are kept responsible for the handling and manipulation of personal information. As seen in the last few years, with the number of incidents causing massive damage to business confidence and financial destruction of personal asset, something had to be done. In an effort to establish a mechanism to monitor and protect the best interests of the 'individuals' electronic information, international bodies created legislation that influences how organizations are to administer personal data. These enactments have provided the insurance industry a leg up to possibly reduce the surmounting financial losses incurred due to cyber risks. This is not the defining rod but may offer insurance vendors a window to refine the design of cyber policy. Other concerns may become systemic involving lobby groups or watch-dog associations who intentionally attempt to disrupt, for example, anti-fraud regulation, federal law enforcement monitoring, or even privacy legislation. This may not necessarily be a bad thing. Pressure to find common ground is needed to maintain a reasonable level of consciousness at all levels of industry, government, and the community at large.

In Canada, the Privacy Act took effect July 1, 1983. The Act imposes obligations on a number of federal government departments and agencies. Its premise is based upon the necessity to respect the privacy rights of Canadians by placing limits on the collection, use and disclosure of personal information. The Act gives Canadians the right to access and correct personal information about them held by these federal government branches. The January 1, 2001 enactment of PIPED (Personal Information Protection and Electronic Documents Act) established rules for how private sector

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

organizations may collect, use or disclose personal information in the course of commercial activities. The Act includes the protection of information sold across provincial and territorial boundaries. As of January 1, 2002, the personal health information collected, used or disclosed by these organizations was put into force. As of January 1, 2004, the Act now covers the collection, use or disclosure of personal information in the course of any commercial activity within a province, including provincially regulated organizations. The latter stage of enactment included the introduction of two provincial privacy acts brought into force concurrently to the federal act.

The province of Quebec has maintained a distinct privacy act since 1994. The federal Privacy Commissioner has reviewed and determined that the Quebec version is notably similar to the federal Act. In essence, the effect of organizations in the Province of Quebec Exemption is observed in Part 1 of the Personal Information Protection and Electronic Documents (PIPED - Federal) Act [7] The Canadian Federal Privacy Act known as PIPED (Personal Information Protection and Electronics Documents Act) http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6TOCE.html stating that it will not apply to those organizations in the province of Quebec that are subject to the private sector privacy legislation. The effect of the Act is specifically relating to the collections, uses and disclosures of personal information within the province. PIPED will only continue to apply to federal works and trans border collections, uses and disclosures of personal information relating to commercial activity. Along with Quebec, Alberta and British Columbia have enacted their own versions of PIPED as of January 1, 2004. Each of these acts displays some ambiguity between the federal and provincial protection acts in so far as the federal act implies a more explicit ideal in guidance. The federal and provincial versions of the privacy act and its three commissioners will continue to eliminate the confusion regarding jurisdiction. In time, once these acts are tested in the judicial sand box industry will then have experienced the effects of litigation through the enforcement of privacy compliance legislation.

Similar to the United States, industry specific privacy legislation may begin to appear within other provincial jurisdictions. Without a basis to argue what is right or wrong in relation to privacy, we have only the limits of history to determine the possible risks of insurance coverage. The insurance industry has a substantial amount of hesitation when attempting to establish a method to design cyber coverage. Underwriters have spent the last few years developing multiple cyber risk policies to address various issues that have plagued business technology. The cyber risk based policies that are available on the market today do not offer any impression of privacy protection coverage in the event of challenges raised in court relating to privacy infractions. Largely, this is due to the uncharted territory that privacy legislation has yet to uncover. Once the courts begin to lay judgment on cyber related insurance claims, issues of privacy may arise in conjunction with insurance related cyber suits. This undoubtedly may set the tone of extremely costly legal battles and the potential implosion of corporate electronic scrutiny. To say the least, mistakes will happen and individual's personal information will be revealed knowingly or not. The extent of the volume of information will also be uncertain.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The North American and European legislated privacy requirements, such as the Personal Information Protection and Electronic Documents (PIPED), Health Insurance Portability and Accountability (HIPAA), the Gramm-Leach-Bliley Financial Modernization Act, the Sarbanes-Oxley Act, Directive 95/46/EC of the European Parliament and of the Council and ongoing federal security initiatives, represent a significant concern for companies currently under going re-alignment of technology and business structures. Do these laws only affect companies currently under going re-alignment of technology and business structures? These Acts may, in turn, prove to be the momentum security personnel have longed for in support of their efforts to establish and secure budgets for much needed security funding.

In the US where specific industry acts have been legislated, there still is no federal regulation-specific technology standards or guidelines that organizations can adopt to ensure compliance with respect to these requirements. What organizations are left with is, a simple yet complex matter of, if you say you are doing it then you must do it.

The Financial Modernization Act, also known as the "Gramm-Leach-Bliley Act" of 1999 [8] http://www.ftc.gov/privacy/glbact/index.html, was established to protect individual's personal financial data preserved by financial institutions. It requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information. The privacy requirements outline three principal components (a) the Financial Privacy Rule, (b) Safeguards Rule and (c) pretexting provisions. Eight federal agencies have been given authority by The GLB Act and positioned to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers.

The Health Information Portability and Accountability Act [9] http://aspe.hhs.gov/admnsimp/pl104191.htm of 1996 enforces new privacy and security standards on the healthcare industry. Specifically, the purpose is to (a) combat waste, fraud, and abuse in health insurance, (b) provide sound health care delivery, (c) promote the use of medical savings accounts, (d) improve access to long-term care services and coverage, (e) simplify the administration of health insurance, and other forms of health care initiatives. As one of the more crucial phases of HIPAA, by 2005 all network-accessible data must be encrypted. A couple of issues that may pose concern with regard to establishing an agreed standard of encryption are a suitable algorithm. Secondly, the movement of data through networks particularly information packaged as image generations, transmission of data, and storage of data in a secure manner. Extensive network and systems implementation and management will pose technical and financial challenges those within the health sector who have limited capabilities.

The Sarbanes-Oxley Act of 2002 [10] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf purpose has mandated that corporation's establish strict controls over business conduct and how

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

they manage their finance and accounting processes. The Act applies in general to publicly held companies and their audit firms. Key technical components include data center operations, system software maintenance, application development and maintenance, business continuity, and application software integrity. Business requirements are controlled by the Audit Committee who is responsible for reporting and certifying the organizations statements of corporate information and internal controls of information technology. If these specifics are not adhered to and the organization is found negligent in reference to fraud, then those implicated or found in violation of the Corporate and Fraud Accountability Act of 2002 may face severe fines and possible imprisonment of up to ten to twenty years.

Until recently, trans border communications have been without serious consequence relevant to privacy related legislation. Legal issues have been experienced primarily within the boundaries of home territories. These days organizations within certain jurisdictions are under strict expectations pursuant to the methods and mechanisms that are used to move data between certain countries. For example, the European Directive has specific guidelines as to "who", being certain countries under the basis of Article 25(6) of directive 95/46/EC [11] European Parliament and of the Council (1995)
http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf
will be able to handle data without instituting additional safeguards. This restriction has been mandated to fifteen specified countries of which include Canada and the United States. [12] "The Commissions decisions on the adequacy of the protection of personal data in third countries"
http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm. The effect of such a decision is that personal data is allowed to flow from the fifteen EU MS and three EEA member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard necessary. The Commission has so far recognized Switzerland, Hungary, the US Department of Commerce's Safe harbor Privacy Principles, Canada and Argentina as providing adequate protection. Insurance policies do not include trans border cyber coverage if implications arise from data being mishandled or intervened with by unauthorized entities.

Excerpt from the European Union Directive 95/46/EC (the "Directive"): "The Act states that
users must 'unambiguously' give consent for personal data to be collected after being informed about the purposes of the collection. The Directive also expressly forbids the collection of 'sensitive data' such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sexual preference. Finally, the Directive forbids the transfer of personal data to a country that does not provide a level of protection similar to its own." As indicated in Article 25(6) of the directive, only specific countries have been granted the ability to move personal data with respect to that data falling under explicit criterion, listed above, in third countries.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Directive 58/EC of the European Parliament and of the Council (2002) [13] http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett aim is to take account of technological changes and to make the provisions as technology-neutral as possible concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The Law

Global connectivity has made the Internet an opportunistic venue for both e-commerce to allow information to flow more easily, and for computer crime to fester and evolve into a billion dollar industry. International boundaries have made this phenomenon a real threat. Many countries, until most recently, have only begun to realize the capability of the Internet, and at the same time they have not understood the damaging risks resulting in weak laws or a complete absence of laws regarding cyber crime and electronic commerce. This causes great obstacles to international cooperation with respect to jurisdiction and geographies. More importantly, how will legitimate consumers be protected if transactions or information is found to be unsatisfactory or fabricated? Which legal system will assist business or the consumer to correct an incident?

Spamming is a hot issue these days with the proliferation of marketing and other nefarious groups taking full advantage of the Internet and email. Organizations are having to deal with the effects of mass mailings that cause disruptions to communication services and the annoyance of managing the receipt of thousands of junk mail items, some coming in the form of pornography. Recently, a case in California was brought to court and ultimately found in favor of the plaintiff. [14] “California wins anti-spam case” http://news.bbc.co.uk/2/hi/americas/3213161.stm. A marketing firm and its owner were charged under the 1998 state anti-spam law with sending out millions of e-mails including advertising guides on how to spam. The violation was founded on the basis of unsolicited e-mails being sent out without a free call number for recipients to contact the marketing firm to cease any further solicitations. As of January 1, the state’s anti-spam laws will become more demanding and will allow private persons to pursue suit with spammers and possibly win judgments of up to $1,000 per e-mail. Insurance policies relating to spamming events would provide coverage under some form of denial of impairment. It is expected that there will be limitations to the scope and power of the legislation. The scope of limitation may be that of the legal systems ability to determine what and who is in violation and to what extent of that violation has been made in reference to the anti-spam act.

Intellectual property has become a critical concern to many organizations who continue to strive to control and protect their proprietary products and research and development. As seen in the press over the last number years, espionage and proprietary theft are on the rise and generate large revenues for those who successfully acquire the intellectual property of others. This has been accomplished by way of well thought out plans to appropriate highly significant proprietary details through the use of technically savvy individuals or persuading internal personnel with money to turn over corporate property or data. In other cases, social engineering tactics have been used by corporate

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

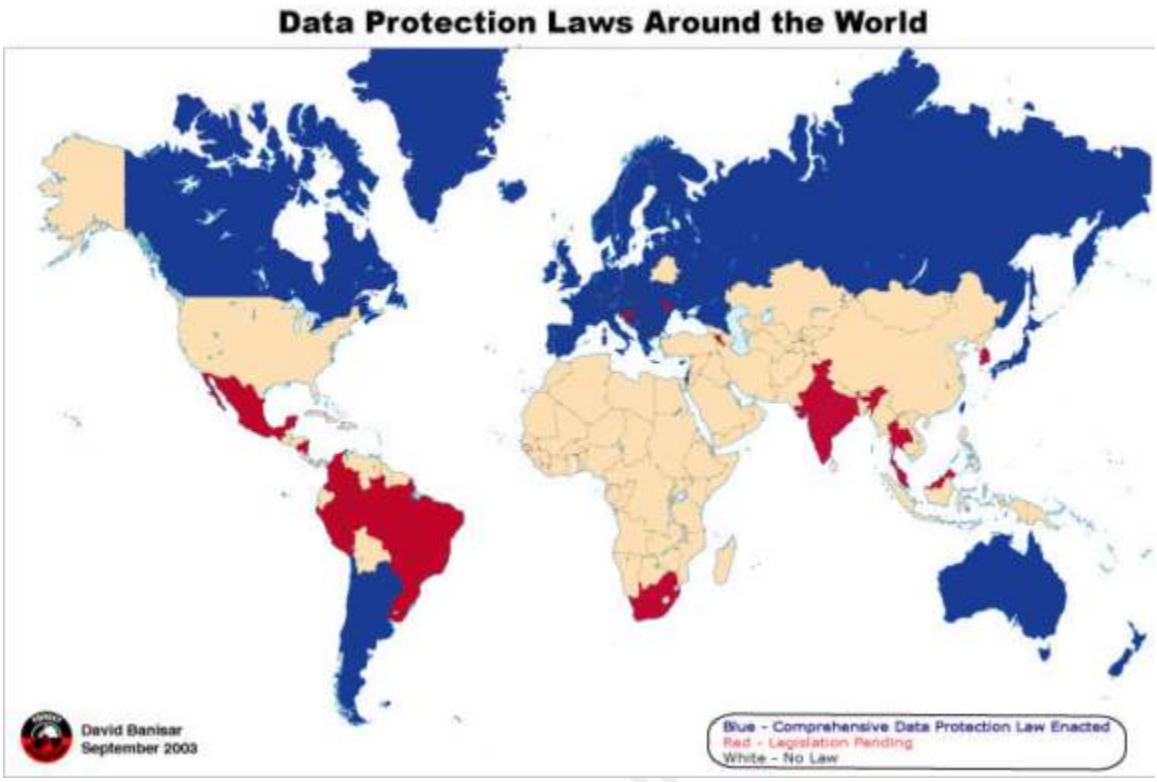
personnel posting research details on message boards. [15] “Raytheon Company v. John Does 1-21, Commonwealth of Massachusetts, Middlesex Superior Court, Civil Action Number 99-816” http://www.netlitigation.com/netlitigation/cases/raytheon.html (1 Feb 1999). This particular case was based upon an issue of privacy. It also concerns intellectual property issues of corporate affairs even after personnel, under hiring requirements, signed employment contracts specifically stating the protection of trade secrets. IP insurance protects against such items as copyright, trademark, working papers, trade secrets, data, methodologies, and so on. This form of insurance is and has been proven, if discovered, to protect against such financial and proprietary losses.

Technology suits will be played out in the courts as the legal system tests the boundaries of new legislation. Jurisdiction will be sliced into a playing field which will be pared down and potentially remodel how the laws are currently written with respect to trans border movement of data. Industry should expect to experience litigation being initiated by large corporations to individuals pursuing the need to protect their personal assets. Small to midsized organizations should not assume that they are exempt from potential litigation and that this scenario will only affect large corporations.

Noticeably the United States is reportedly driving organizations in every sector of its economy to obtain cyber security insurance. In Canada there appears to be no such public guidance coming from the political powers. Perhaps in the future cyber insurance will become as common place as home insurance policies. In terms of cyber law and its treatment within the courts, the judges who must apply the law to fit legal disputes on the Internet will have to use preexisting legal foundations in order to establish precedent. In its current state, legal principles that govern conduct and ecommerce over the Internet are and will experience reformation as judgments are disposed.

The map below from [16] Privacy International http://www.privacyinternational.org/survey/dpmap.jpg. provides a compass of jurisdictional data protection laws worldwide. The blue indicates those countries who have implemented significant laws, those in red have drafted a form of legislation, and those in white have no pending laws. With the exception of the United States who have implemented industry specific regulations, yet no all encompassing legislation.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.



Infrastructure Preparation

The insurance industry has evolved from a one dimensional technical policy provider to a diversified entity that is now able to more closely understand the potential risks that cause injury to organizations. As the landscape of insurance coverage evolves, a benefit of this cycle may be derived from organizations who seek software development services. The organizations providing development services will need to build secure code from the ground up, rather than building security in as an after thought or not at all. As part of the application process, insurers may request an organization to provide details of what applications they utilize, whether they were developed in-house or by a software developer. If the latter is indicated then the insurer will want to know who the developer is and the details of the service contract. This may have a direct effect on the insured's policy premiums as they may fluctuate depending on the products that are being used.

As organizations seek out insurance policy coverage, they should be aware of a very important clause within technology policies. If an organization happens to be drawn into suit with a client, depending upon the policy structure, there may be limitations to what the insurer will defend in terms of claims. If, for example, you are insured with a CGL (Commercial General Liability) policy you may be in for a surprise. It is important for the insured to select an appropriate policy that is suited to its requirements. When reviewing a policy with a legal defense component, the insured needs to take the time to discuss who has the right to choose counsel. It is imperative that this aspect of the policy is

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

discussed very clearly with the insurer as many hours can be expended on this issue, it could even make or break the negotiations.

The technology industry has provided users of technology with standards that are designed to evaluate the state of an organizations security position. These standards are used by security practitioners to establish a condition of preparedness and to assist in the ongoing development and continuity of the infrastructure. One of these standards that are highly recognized is ISO/IEC 17799:2000 (formerly the British Standard 7799) International Organization for Standardization [17] http://www.iso.org/iso/en/CatalogueListPage.CatalogueList. It covers many aspects of a sound security infrastructure but not every control will be relevant to every situation. Other tools acknowledged in industry are CobiT (Control Objectives for Information and Related Technology) developed by ISACA (Information System Audit Control Association) [18] http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981). This standard is an IT audit methodology that is used to measure the security and control practices for a corporate infrastructure. This methodology is also not restricted to large environments. Other industry standards have been developed upon the basis of a specific sector which may support your infrastructure, for example, finance relating to the security of transactions over the Internet. If an organization can show that it has performed due diligence in measuring its corporate structure, it will appease the insurer and ease the application process. The insurer has no other way of making an educated conclusion that a company is fit and capable of sustaining and or reducing the impact of a cyber event occurring without a formal assessment. Sound security practices and safety of information on/offline is best practice.

The basis for a 'best practice' strategy includes numerous criteria. A few of the requirements used to establish appropriate controls in organizations should include: ensuring strong authorization and authentication measures, establishing sound logical and physical access controls, creating boundaries over internal and external user activities, and, specific attention to the archiving of records and all information. Organizations must ensure network and system capacity will sustain business standards for client use. In support of a sustainable environment, a clear business continuity and disaster recovery program should be in place and tested at regular intervals. As a component of this strategy an incident response capability with a communication strategy should complement the corporate recovery program. As a monitoring mechanism, regular audit cycles will ensure that the credibility and reliability of the corporate infrastructure is measured against industry standards and regulations.

This table will provide a limited overview of a number of the standard security requirements and limited business requirements needed to be considered when establishing a security strategy position for insurance coverage. In the table are a series of questions that would require a response on most insurance applications. Not all questions may appear on every application, but be prepared if you may be requested to provide information listed in the table. Listed in the table are subsections pertaining to

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the type of business technology realm. The “Enterprise Exploration” column pertains to the various technical and business requirements of the organization. The “Exposure/State” column provides a query of the condition of the technology or business activity. The “Percentage % of Business Activity” column represents the amount of business associated with the exposure. The “Level of Priority” column identifies the level of assumed risk against the exposure. The “Status” column offers a statement of position with respect to the exposure. For example, the exposure may be a deployment of a firewall at the network perimeter, the status may state “implemented, but not tested, no procedures developed.” Many questions in varying nature will be asked on an application in order to begin processing the insurance coverage submission. If you have regular security or audit assessments conducted at your site, the reports generated from the findings should answer most questions posed on these applications. In some cases, dependant upon the size of the organization, various areas and levels of management may be queried to provide further information relating to the specific business sections of the application.

Insurance Cyber-Risk Self-Assessment **(This is a general review listing. Comprehensive details should be attained through an insurance underwriter/broker)**					
Enterprise Exploration	**Exposure/State**	**Yes/ No**	**Percentage % of Business Activity**	**Level of Priority** **1 – 2 – 3 – 4 – 5 (1 high > 5 low N/A – not applicable**	**Status**
Market Sectors & Media					
1	What is the business reach into market sectors (financial, government, Health care, commercial, other), list all?				
2	Is original content provided?				
3	Are subscriber services provided on your website?				
4	What number of subscribers are supported and is capacity adequate to accommodate subscribers?				
5	Are bulletin/chat room service supported on your website?				
6	Do you analyze, edit or censor the material on your website or Internet service in any way?				
7	At what frequency is web site or Internet service content updated?				
8	Do you provide content for client web sites?				
9	Does the client approve content before it is posted to the Internet?				
10	Are your contract liabilities limited for any breaches of your				

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	professional services?				
11	Do you make guarantees or warranties in your contracts regarding professional services?				
12	Are materials on you website designed to be downloaded and are they scanned for viruses?				
13	Do you sell product or services on your web site or Internet service?				
14	Are credit card transactions conducted on your website over the Internet?				
15	Is there a process in place to screen content?				
16	If yes, has a qualified attorney reviewed the content of your website?				
17	Are there established procedures for deleting, modifying, and removing controversial, offensive or infringing material from your website or Internet service?				
18	Are materials of other entities used in any electronic form, including on your website or electronic database?				
19	Do you own the intellectual property rights to the content/material and business methods of your website in contract agreements?				
20	Has a clearly stated privacy statement been established on your website and has it been reviewed by legal council?				
Business Impact					
1	How would your revenues be affected, if a breach of security were experienced?				
2	How would service related business partners be affected by a security breach, what is your liability?				
3	If you are a service provider, what service interruption procedures do you have in place, are they documented (copy of procedures and contract/SLA)?				
4	Are you responsible for the property of others (credit card, money, securities, data assets)?				
5	Are credit and criminal background checks performed on all existing/new employees, and consultants?				
6	Upon hiring or contracting, do you				

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	provide each personnel with a copy of your security policy and orientation?				
7	Are corporate awareness training sessions provided to assist personnel with the understanding of security issues (how often)?				
8	Are all employees required to sign a Non-Disclosure or Confidentiality agreement upon hiring (copy of document)?				
9	What are the total number of consultant and contract employees performing Internet, network and computer system, and application services for your organization?				
10	Are external contractors/consultants required to maintain liability insurance (list coverage expectations)?				
11	How many fulltime, part-time, or contract personnel have access to sensitive areas? (accounting, research and development, online transaction processing, engineering, security and systems administration, or other sensitive areas?				
12	Do any non-personnel (service providers, etc.) have access to sensitive areas (how many)?				
13	Who is responsible for managing and monitoring infrastructure access (list management)?				
14	What web based applications are being used for Internet based services (list all applications)?				
15	Are any of the web based applications designed by or for you (list applications and designer)?				
16	Have these applications been tested for security vulnerabilities, if so what was uncovered, and what action was taken?				
Software Development					
1	Do your technical services personnel follow an SDLC (software development life cycle) process?				
2	What percentage of your product/service (hardware or software) is made to specification of others?				
3	What percentage of your product/service (hardware or				

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	software) is made to specification of your own?				
4	What testing procedures do you have in place for all personnel and non-personnel (attach documentation)?				
5	What Change Management procedures are in place for all personnel and non-personnel (attach documentation)?				
6	Do you have recovery procedures documented for production and non-production environments in the event of a service disruption (attach documentation – see "Network Security" Item #11)?				
7	What procedures have been established to manage bugs or anomalies with software products?				
Physical Security					
1	Has a full and complete inventory of all corporate computer related equipment been catalogued and recorded (attach inventory listing)?				
2	Are critical servers secured within a climactically controlled environment?				
3	What access controls are in place to protect critical servers? Who has access?				
4	Are removable media stored securely? Where and how are media stored and under what controls?				
5	Who has access to removable media areas?				
6	How are accesses to critical areas recorded and controlled?				
7	What mechanisms are used to identify personnel and visitors in critical areas?				
8	What surveillance monitoring devices are used to protect sensitive areas?				
9	What support services are installed to sustain disruptions to systems?				
10	What procedures have been established for the evacuation of people in the event of an emergency?				
11	How are sensitive materials disposed of (media, documents, etc.)?				
12	What policies have been				

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	established to respond to off-site emergencies?				
13	Are users provided security awareness training surroundings awareness and emergency procedures?				
14	Have emergency procedures been distributed to all personnel?				
Network Security					
1	Are firewalls in place to avert unauthorized access to internally protected networks from external sources, what technology is used?				
2	Are authentication vehicles used to allow connections from remote users into internal networks, what form is used?				
3	Are desktops and critical servers protected by firewalls, intrusion prevention, and anti-virus mechanisms?				
4	How often are firewalls, intrusion prevention, and anti-virus safeguards updated with vendor patches, or product revisions (list process and frequency per product)?				
5	Are general backup and recovery procedures documented?				
6	Are back up and recovery procedure specifically documented for critical systems, web sites, firewalls, and corporate data?				
7	Are corporate backup procedures conducted by internal personnel or outsourced?				
8	If outsourcing is utilized, provide a copy of the contract or SLA.				
9	How are privileges for primary back up system administration personnel managed?				
10	Are Business Continuity Plans (BCP) in place for all mission critical processes?				
11	In the event of a corporate or service disaster, what recovery procedures have been established (attach documentation)?				
12	In the event of a security breach, do you have a CIRT (Computer Incident Response Team) in place to respond to incidents?				
13	If you have a CIRT, in the event of a successful security breach, do you				

© SANS Institute 2004, Author retains full rights.

	have procedures to respond to a breach (supply documentation)?				
14	What is your back up media archive cycles and where is the media stored?				
15	Have short and long-range plans been designed?				
16	What is the maximum business outage duration anticipated to be (hours)?				
17	If this business process is being outsourced, indicate who the services provider is and whether a contract/SLA has been established (contract copy)?				
18	Do you have system and network monitoring in place?				
19	If monitoring is outsourced, indicate the service provider name and a copy of the contract/SLA.				
20	Has an internal network and Internet use security policy been established (copy)?				
21	Has a corporate privacy policy been establish and implemented (copy)?				
22	Has the corporate privacy policy been extended to all business related partnerships?				
23	Are authentication applications utilized with e-commerce products/services (indicate products/processes)?				
24	Do you outsource and part of your corporate infrastructure, such as, Internet services, network or computer systems to others, products, or equipments?				
25	List all outsourced service providers, services supported, and a copy of the contract/SLA.				
26	Are you activity receiving or participating in computer emergency response advisories, bulletins or other notifications (indicate source)?				
27	Have there been any changes in ownership or senior management (including CIO) in the past year?				
28	Is there a fulltime Chief Information Security Officer or equivalent?				
29	Are procedures in place to detect and identify network and systems security weaknesses?				

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Security Solution Implementation					
1	Have any of the following security solutions been implemented or will be implemented (list product and status of implementation)?				
(a)	:Security Management Software				
(b)	:VPN (Virtual Private Networking)				
(c)	:Access Control utilities (hardware or software based)				
(d)	:Data Integrity Programs				
(e)	:PKI (Public Key Infrastructure)				
(f)	:FES (File Encryption Software)				
(g)	:Firewalls				
(h)	:Intrusion Prevention (IDS – Intrusion Detection System, IPS – Intrusion Prevention System)				
(i)	:Routing and switching technology				
(j)	:Mobile security software (laptops, notebooks, PDA, cellular)				
(k)	:Communications (PBX – Private Branch Exchange, VOIP – Voice Over IP)				

As part of the application process, the insurer may request that a security analysis by an independent security consulting firm who are approved by the insurer be performed as part of the security risk survey. The risk assessment should be conducted by a reputable security assessment provider, discuss the selection process with the insurer before accepting the insurer's recommended consulting service provider. Note that any security assessment is based upon a "point-in-time" review. If you are submitting an application with an assessment that was performed six months ago and subsequent development has taken place since, then the disclosure of information on the insurance application may not be accurate and complete.

Final Thoughts

Generally, cyber risk insurance policies are, in part, key in the protection of an organizations investment and responsibility to its clients to the extent of financing the defense costs if litigation were pursued by a plaintiff. If an organization were drawn into a legal battle over the protection of information assets, or lack thereof, having insurance coverage would reduce the burden of cost for litigation. Until loss experience hardens, premiums will be in a state of flux and protection could be challenged. Risk management and mitigation is paramount to ensure that the corporate infrastructure maintains a high level of self preservation.

The stage is set. In coming years we will experience a new breed of cyber warfare with greater complexity. This will drive industry to respond to protection mechanisms that will change how we trust the competition, business relationships, and endure the unlawful side of cyber space. This will also change how organizations control and manipulate personal information in response to changes in privacy and other federal legislation.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The cost of piece of mind is and will continue to be a large factor in the protection landscape. Organizations will have to develop corporate governance and enterprise risk management infrastructures in order to protect their interests and the interests of their client(s). As technology progresses business entities doing business with each other will begin requesting that any company that does business with itself must have cyber insurance. This expresses the importance of responsible business practices. Enron and Worldcom will not be the last to see executives or security officers defending the corporation and potentially looking at jail time if found at the negative end of a judgment. Many organizations may even see this as an epiphany. Finally, industry does not have a clear perspective as to what the implications will be in relation to changing regulation, federal laws governing technology and the use of the Internet. How they will be decided will be lessoned in the courts, and will be a test of time. Insurance can reduce the financial severity of liability and provide adequate levels of responsibility.

References

[1] Swanson, Sandra "Insurers Rethinking IT Coverage For 2002" URL: (http://www.informationweek.com/story/IWK20020102S0004) (2 Jan 2002)

[2] Swartz, Jon "Firms' hacking-related insurance costs soar" URL: http://www.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm (2 Sep 2003)

[3] Dubie, Denise "Corporate security spending not in line with real-world requirements" URL: http://www.nwfusion.com/news/2003/0505nemertes.html (5 May 2003)

[4] Steen, Andrew "Insurance. What's going on?" URL: http://www.yorktech.ca/events/10-30Presentation2.pdf (2002)

[5] Richardson, Robert "CSI/FBI 2003 Computer Crime and Security Survey" Computer Security Institute/Federal Bureau of Investigation URL: http://www.gocsi.com/ (29 May 2003)

[6] Ghosh, Ajoy/Hourigan, Phillip/Price, Rowan/Ford, Stephen/Gaskell, Gary/NSW Police "Australian Computer Crime and Security Survey 2003" AusCERT (Australian Computer Emergency Response Team) URL: http://www.auscert.org.au/render.html?it=2001 (May 2003)

[7] [CAN00] The Canadian Federal Privacy Act known as PIPEDA (Personal Information Protection and Electronics Documents Act) URL: http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6TOCE.html (13 April 2000)

[8] [GLB99] Gramm-Leach-Bliley Financial Modernization Act (1999) URL: http://www.ftc.gov/privacy/glbact/index.html (1999)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[9] [HIPAA96] Health Insurance Portability and Accountability Act (1996) URL: http://aspe.hhs.gov/admnsimp/pl104191.htm (21 Aug 1996)

[10] [SOA02] Sarbanes-Oxley URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf (30 Jul 2002)

[11] [EU95] Directive 95/46/EC of the European Parliament and of the Council (1995) URL: http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf (24 Oct 1995)

[12] Commission decisions on the adequacy of the protection of personal data in third countries http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.
[14] Shiels, Maggie "California wins anti-spam case" URL: http://news.bbc.co.uk/2/hi/americas/3213161.stm (25 Oct 2003)

[13] [EU58] Directive 2002/58/EC of the European Parliament and of the Council URL: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett (12 Jul 2002)

[14] "California wins anti-spam case" http://news.bbc.co.uk/2/hi/americas/3213161.stm (25 Oct 2003)

[15] Raytheon Company v. John Does 1-21, Commonwealth of Massachusetts, Middlesex Superior Court, Civil Action Number 99-816 URL: http://www.netlitigation.com/netlitigation/cases/raytheon.html (1 Feb 1999).

[16] Privacy International: Map http://www.privacyinternational.org/survey/dpmap.jpg

[17] ISO/IEC 17799:2000 (formerly the British Standard 7799) International Organization for Standardization http://www.iso.org/iso/en/CatalogueListPage.CatalogueList

[18] COBIT (Control Objectives for Information and Related Technology) developed by ISACA (Information System Audit Control Association) http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced