New Risks in a Networked World

Security takes on a different meaning in the open, networked world. Securing information systems is a complex process that involves several factors:

- Continuous technological advancements
- Strategic shifts such as IT outsourcing
- Security vulnerabilities in hardware and software products
- Acquisitions requiring integration of different systems in a secure way
- Security and privacy laws and regulations
- The changing nature of the electronic threat profile

The threat profile expands in a networked environment. Attackers not only have easier access to financial assets, but richer and better opportunities for information theft, sabotage, industrial espionage, disruption and information warfare. Dependence on information systems drives business growth, but dependencies and interdependencies create dangerous vulnerabilities.

Information age attackers have new advantages as well. Internet-dependent communication allows attackers to:

- Hide their identities
- Avoid physical risk by acting from remote locations
- Exploit vulnerabilities before their existence is known to security defenders
- Use newly discovered vulnerabilities and associated exploits developed by other hackers that are often communicated in the hacker underground
- Take advantage of interdependencies inherent in most networks
- Use insecure systems of unrelated parties as attack tools

Technology is a great equalizer. Unfortunately, it gives a single attacker with a computer and internet access the tools to attack even the most well defended and distant target.
Technology is a great equalizer. Unfortunately, it gives a single attacker with a computer and internet access the tools to attack even the most well defended and distant target. The wave of very fast spreading worms is a recent example. In a post-9/11 world, a whole new front has opened up for terrorists and foreign governments – cyber terrorism, state-sponsored espionage and information warfare. As part of the nation’s critical infrastructure, financial institutions face a growing and dangerous threat.

Two Surveys Help Fill the Information Gap and Dispel the Myths Surrounding Cyber Risk Insurance

Much of the information evaluating Cyber risk exposures has been prepared with the security or privacy professional in mind or on a level that is inaccessible to those without technical expertise. Assessing the new risk environment and the role that Cyber risk insurance ought to play in a financial institution’s insurance program has been difficult. However, two recent surveys provide information that can assist risk managers in gaining insight into a number of fundamental questions about exposure that might aid in evaluating the option of Cyber risk insurance. The studies are:

- **2004 Global Security Survey** by Deloitte Touche Tohmatsu (“Deloitte”), which focuses on financial institutions and bases its conclusions on responses by 64 financial institutions from around the world (32 percent from the US). (Click below or paste link into your browser to read survey in full. http://www.deloitte.com/dtt/article/0%2C2297%2Csid%25253D3057%2526cid%252D48286%2C00.html)

- **2004 E-Crime Watch Survey** conducted by Carnegie Mellon Software Engineering Institute/CERT Coordination Center, CSO Magazine and The United States Secret Service. The E-Crime Watch Survey Summary of Findings (“E-Crime”) based its conclusions on 500 respondents and a panel of advisors including Bear Stearns. Of the survey base of 500 organizations, 13 percent were in banking and finance and three percent were in insurance. (Click below or paste the link into your browser to read survey in full http://www.csoonline.com/releases/ecrimewatch04.pdf)

Another valuable industry survey is the CSI/FBI Computer Crime and Security Survey, now in its ninth year. The surveys referenced here were chosen due to their approach and their focus on financial institutions.

The surveys provide useful and much needed fact-based guidance, which allows for some benchmarking opportunities. These surveys are complex documents that deserve careful reading to ensure a balanced view of both improving and problematic areas in information security and the budgetary and regulatory forces that can hugely impact security decisions. Here, we look at some typical risk management questions in the light of some of the key survey results. The questions assume a traditional insurance program that has typical gaps in Cyber coverage, meaning risks involving computer attacks (intrusions such as unauthorized access or use) against a network or information resources by either outside hackers or malicious employees. At issue are:

- Attacks that result in the theft, destruction or alteration of personal or confidential information or other information held or used by the organization
- Disruption of service to third parties
- Unavailability of the network to the organization
- Attacks against third-party systems by users of the organization’s network or hackers that compromise it
- Extortion against data or systems

Gaps in Traditional Insurance Coverage Line Up With Key Cyber Risk Exposures

Financial institutions generally have insurance protection against direct financial fraud by use of computers as well as some protection against viruses and hacker damage related to attempts at direct financial fraud, though these may be limited. Also, many have coverage for negligence in providing covered banking services and related services. However, most traditional insurance programs do not cover several types of risk:
• Liability for theft of private or confidential information which includes the rising wave of identity theft
• Business interruption income loss or extra expense due to hacker or virus attacks that disrupt operations (including intrusion by insiders and denial of service (DoS) attacks)
• Liability for attacks against third parties using the financial institution’s information network
• Theft of passwords by non-electronic means

Assessing the potential impact on the organization of such gaps in insurance coverage is vital. If the gaps represent serious exposures, this information can be of use in technical security planning, risk analysis in business decisions and choices about Cyber risk insurance or other risk financing.

Key Questions About Cyber Risk

How serious is the Cyber risk threat to a financial institution?

The increase in patches – which is code to fix vulnerability in an application – has been dramatic (with)... the number of reported vulnerabilities increasing from 171 in 1995 to 4,129 in 2002.

According to the Deloitte survey, respondents are worried that attacks against their networks are becoming more sophisticated. Significantly, 83 percent of the respondents – up from 39 percent the year before – reported that their systems had been breached. A substantial cause of the increase was due to very fast moving worms. Of US respondents, 24 percent reported that their security had been compromised in the past 12 months. Viruses and worms were responsible for a large part of the increase. Of the virus and worm attack, 21 percent were externally based, 13 percent from internal sources and 49 percent combined internal and external attacks. In the E-Crimes survey, 45 percent of respondents reported more than 10 cyber crimes or intrusions in 2003, with 20 percent reporting more than 100 incidents.

Even with the growing threat, US respondents to the Deloitte survey indicated that they were willing to take higher risks and lead in the adoption of new technologies.

Deloitte respondents noted that the growth of e-commerce, which requires them to connect electronically to customers and partners, increases the threat of financial fraud and the theft of customer information from inside and outside the organization. In the 2003 survey, organized crime was singled out as a major source of such attacks. Respondents to the 2004 survey ranked the top threats as viruses/worms, loss of customer data and being flooded with patches, characterized as inadequate patch management. The increase in patches – which is code to fix vulnerability in an application – has been dramatic over the past several years. According to CERT (one of the sponsors of the E-Crime Survey and the group responsible for logging and issuing advisories on application vulnerabilities), the number of reported vulnerabilities increased from 171 in 1995 to 4,129 in 2002. Vulnerability reports average more than 10 per day.

E-Crime respondents reported a 43 percent increase in the number of electronic crimes and intrusions involving networks, systems or data in 2003 versus 2002. The greatest Cyber security threat in 2003 was hackers (40 percent), current employees (22 percent) and former employees (6 percent).

Isn’t my organization’s information security risk management sufficient?

Deloitte respondents reported varying degrees of confidence in how well their network was protected from Cyber attacks. Eight percent were not very confident about internal protection and one percent about external protection. Most were somewhat confident (48 percent internal and 37 percent external). Almost as many were very confident (43 percent internal and 53 percent external). A small number (two percent internal and nine percent external) were extremely confident.
Another relevant issue the Deloitte survey addressed was risk management approach. Forty-four percent characterized their risk management as “efficient and effective.” Thirty percent said their risk management covered all but “necessary risk only” whereas 13 percent saw their risk management as “world class and bullet proof.”

Outsourcing IT functions and business process was found in the Deloitte survey to have grown considerably in the past 18 months. Often, off-shore locations are chosen as outsourcing sites. Outsourced functions are an important dimension in security risk management as risks generally follow the function. Although, no similar questions were contained in the 2004 survey, the 2003 Deloitte survey found that only 38 percent conducted their own rigorous assessment of third-party security measures. Only 44 percent receive regular information from third parties that allows ongoing assessment of their security. The 2004 Deloitte survey also found that outsourcing certain security functions was more likely to be done by larger organizations. Respondents indicated concern over customer privacy and outsourced operations.

The Deloitte survey revealed that 91 percent of the organizations have IT disaster recovery or business continuity plans. However, only 54 percent (while a significant improvement from 43 percent last year), were very confident that their backups worked or met policy requirements for off-site storage.

It is worth noting that some Cyber risk insurance policies require the insured to have and follow a regular (daily or weekly) data backup and off-site storage policy.

What claims or losses have occurred that would justify adding a Cyber risk insurance policy to my portfolio?

The E-Crime survey went rather deeply into this issue despite the fact that the base responding to these questions often fell significantly from the base of 500 participating in the survey. Disclosing losses is a sensitive issue especially in Cyber risk where the degradation of one’s reputation as a trusted party for electronic commerce is often seen as too important to risk.

Three percent of the E-Crime respondents had losses over $10 million and five percent had losses between $1 million and $10 million. However, 50 percent track their losses, but were unable to quantify them.

Some type of financial loss due to electronic crime was experienced by 83 of E-Crime respondents. Of these crimes, 56 percent were operational and 25 percent financial. The E-Crime survey reported the top electronic crimes.

- Virus or other malicious code (77 percent)
- Denial of service attacks (44 percent)
- Illegal generation of SPAM email (38 percent)
- Unauthorized access by an insider (36 percent)
- Unauthorized access by outsider (27 percent)

The top adverse consequences from insider intrusion reported in the E-Crime survey were:

- Critical disruption to the organization (25 percent)
- Harm to organization’s reputation (15 percent)
- Critical disruption affecting customers and business partners (seven percent)
- Loss of current and future revenue (seven percent).

In the matter of insider intrusion, the E-Crime survey revealed that legal action was not taken out of fear of negative publicity (27 percent), concern that competitors would take advantage of the situation (11 percent) and prior negative experience with law enforcement (seven percent).

It appears likely that the general reticence about Cyber losses together with problems quantifying such losses at some organizations has caused the actual level of losses to be underreported. Therefore, basing a risk management or insurance decision heavily on available loss information would be inadequate and undervalue other important risk information revealed in these surveys.
Do Cyber risk insurance products address the gaps in traditional policies?

The answer is yes. Generally, Cyber risk insurance policies provide coverage for computer attacks by insiders (employees) and outsiders (hackers), viruses and malicious code, denial of service attacks and theft of passwords by non-electronic means. Computer attacks are generally defined as unauthorized access or use of covered networks and include:

- Liability for theft of private or confidential information including identity theft
- Inability of authorized users to access the network
- Loss of data
- Downstream liability, or attacks launched against other computers or networks from the covered network if it is compromised by an attacker via:
  - Hacking into other systems
  - Denial of service (DoS) attacks
  - Virus

Some Cyber risk policies offer first party coverage as well. Again the basis of cover is computer attacks against the covered network. Disruption of the network or the alteration or destruction of data caused by a hacker, insider, virus or DoS attack would be covered for business interruption to provide for lost income and extra expense to restore network service and data.

Cyber risk policies also cover systems and IT functions outsourced to third parties. This was an area of concern identified in the Deloitte survey. Here Cyber risk insurance can play an important role since most outsourced IT service providers are subject to the same attacks and usually limit their liability to the value of the outsource contract as well as disclaim consequential damages for business interruption.

Are other financial institutions buying Cyber risk insurance?

Deloitte’s 2003 survey found that 24 percent of the respondents have Cyber risk insurance. Of the remainder, five percent more were planning to buy such coverage. This question did not appear on the 2004 survey, though there is no reason to suggest the trend has changed. These results are similar to the 28 percent obtained by the 2004 CSI/FBI Computer Crime and Security Survey, the second year this question appeared in the survey.

The Deloitte survey did not address limits of insurance purchased or whether the coverage was third party, first party or both. Hopefully, a future survey will address these important questions.

Conclusion

Cyber risk policies line up with the coverage gaps in traditional insurance policies. As the Deloitte and E-Crime surveys show, Cyber risk policies do address key exposures that are generally not otherwise covered by insurance and pose a significant risk to financial institutions. Reliance only on information security risk management appears to be inadequate even in the eyes of many survey respondents. Given the networked business model and the dependence on information systems, it would appear prudent to explore the value provided by Cyber risk insurance. An organization’s chief security office (CSO) or chief information security office (CISO) can be a valuable partner in this process. With many financial institutions purchasing Cyber risk coverage it is important for risk managers to provide the Cyber coverage option to senior management or review the adequacy of the scope of current Cyber risk coverage and limits of insurance. This task is especially crucial in light of the growing threat to financial institutions from attacks on their networks — attacks that threaten the basis of trust that is essential to their dealings with customers and business partners.

Geoffrey K. Allen, Senior Vice President, is the e-risk and E&O Product Leader at Willis North America. For additional information about areas mentioned in this article or anything else related to Cyber risks, you can contact Geoff by phone at 212 837 0745 or via email at allen_gk@willis.com. For information on any topic related to Financial Institutions, please contact John Bayeux, head of our Financial Institutions Practice by phone at 212 770 0739 or via email at john.bayeux@willis.com.