Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security

By Carol A. Siegel, Ty R. Sagalow, & Paul Serritella[1]

Introduction

Traditional approaches to security architecture and design have attempted to achieve the goal of the elimination of risk factors – the complete prevention of system compromise through technical and procedural means. Insurance-based solutions to risk long ago admitted that a complete elimination of risk is impossible and, instead, have focused more on reducing the impact of harm through financial avenues – providing policies that indemnify the policy holder in the event of harm.

It is becoming increasingly clear that early models of computer security, which focused exclusively on the risk-elimination model, are not sufficient in the increasingly complex world of the Internet. There is simply no magic bullet for computer security; no amount of time or money can create a perfectly hardened system. However, insurance alone cannot act alone as a risk mitigation tool – the front line of defense must always be a complete information security program and the implementation of security tools and products. It is only through leveraging both approaches in a complementary fashion that an organization can reach the greatest degree of risk reduction and control. Thus, today, the optimal model requires a program of understanding, mitigating and transferring risk

[1] The views and policy interpretations expressed in this work by the authors are their own and do not necessarily represent those of American International Group, Inc. or any of its subsidiaries, business units or affiliates.

through the use of integrating technology, processes and insurance – i.e. a Risk Management approach.

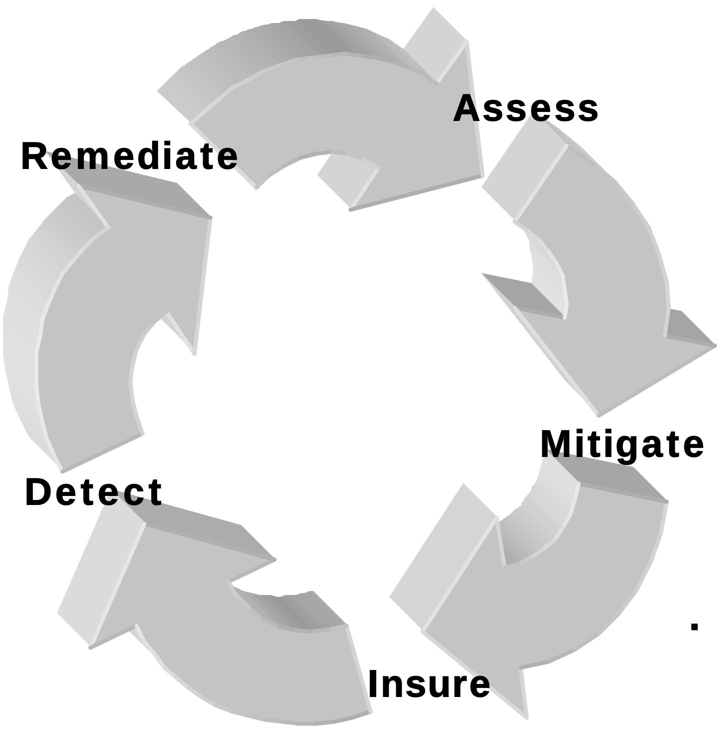
The Risk Management approach starts with a complete understanding of the risk factors facing an organization. Risk assessments allow for security teams to design appropriate control systems and leverage the necessary technical tools; they also are required for insurance companies to properly draft and price policies for the remediation of harm. Complete risk assessments must take into account not only the known risks to a system, but also the possible exploits which may be developed in the future. The completeness of Cyber-Risk management and assessment is the backbone of any secure computing environment.

After a risk assessment and mitigation effort has been completed, insurance needs to be procured from a specialized insurance carrier of top financial strength and global reach. The purpose of the insurance is three fold: Assistance in the evaluation of the risk through products and services available from the insurer, transfer of the financial costs of a successful computer attack or threat to the carrier, and the provision of important post-incident support funds to reduce the potential reputation damage after an attack.

The Risk Management Approach

As depicted in "Figure 1 – Risk Management Cycle," risk management requires a continuous cycle of assessment, mitigation, insurance, detection and remediation:

Figure 1 – Risk Management Cycle



REMEDIATE

- Understand the report that the assessment yields
- Determine areas of vulnerability that need immediate attention
- Establish a recurring procedure to address these vulnerabilities
- Recover lost data from backup systems
- Execute alternative hot-site until primary site is available

ASSESS

- Evaluate the organization's security framework, including penetration testing and interviews with key personnel.
- Use standard methodology and guidelines for assessment (e.g. ISO17799, INFOSEC etc.)

MITIGATE

- Creating and implementing policies & procedures that ensure high levels of security
- Implementing financial risk mitigation and transfer mechanisms
- Should be reviewed periodically to ensure maintenance of security posture

DETECT

- Monitor assets to discover any unusual activity
- Implement a 24x7 monitoring system, that includes intrusion detection, anti-virus etc, to immediately identify and stop any potential intrusion
- Analyze logs to determine any past events that were missed

INSURE

- Choosing the right insurance carrier based on expertise, financial strength and global reach
- Choosing the right policy including both first party and third party coverage
- Implementing insurance as a risk transfer solution and risk evaluation tool that complements technology based security solutions
- Working with the carrier, determine potential

Assess

An assessment means conducting a comprehensive evaluation of the security in an organization. It usually covers diverse aspects ranging from physical security to network vulnerabilities. Assessments should include penetration testing of key enterprise systems and interviews with security and IT management staff. As there are many different assessment formats, an enterprise should use a method that conforms to a recognized standard (e.g. ISO17799, INFOSEC – see appendix A.). Regardless of the model used, however, the assessment should evaluate people, processes, technology and financial management. The completed assessment should then be used to determine what technology and processes should be used to mitigate the risks exposed by the assessment. They should be done periodically in order to determine new vulnerabilities, and to develop a baseline for future analysis to create consistency and objectivity.

Mitigate

Mitigation is the series of actions taken in order to reduce risk, minimize chances of an incident occurring, or limit the impact of any breach that does occur. Mitigation includes creating and implementing policies that ensure high levels of security. Security policies, once created, require procedures that ensure compliance. Mitigation also includes determining and using the right set of technologies to address the threats that the organization faces, and implementing financial risk mitigation and transfer mechanisms.

Insure

Insurance is a key risk transfer mechanism that allows organizations to be protected financially in the event of loss or damage. A quality insurance program can also provide superior loss prevention and analysis recommendations often providing premium discounts for the purchase of certain security products and services from companies known to the insurer which serve dovetail into a company's own risk assessment program. Initially, determining potential loss and business impact due to a security breach allows organizations to choose the right policy for their specific needs. The insurance component then complements the technical solutions and policy procedures. A vital step is choosing the right insurance carrier by seeking companies with specific underwriting and claims units with expertise in the area of information security, top financial ratings and global reach. The right carrier should offer a suite of policies for companies to choose from which can provide adequate coverage.

Detect

Detection implies constant monitoring of assets to discover any unusual activity. Usually this is done by implementing a 24x7 monitoring system that includes intrusion detection to immediately identify and stop any potential intrusion. Additionally, anti-virus solutions allow companies to detect new viruses or worms as they appear. Detection also includes analyzing logs to determine any past events that were missed and specification of action to prevent future misses. Part of detection is the appointment of a team in charge of incident response.

Remediate

Remediation is the tactical response to vulnerabilities that assessments discover. This involves understanding the report that the assessment yields and prioritizing the areas of vulnerability that need immediate attention. The right tactic and solution for the most efficient closing of these holes, has to be chosen and implemented. Remediation should follow an established recurring procedure to address these vulnerabilities periodically.

In the cycle above, most of the phases focus on the assessment and implementation of technical controls. However, no amount of time or money spent on technology will eliminate risk. Therefore, insurance plays a key role in any risk management strategy. When properly placed, the insurance policy will transfer the financial risk of unavoidable security exposures from the balance sheet of the company to that of the insurer. As part of this basic control, companies need to have methods of detection (such as Intrusion Detection Systems, or IDS) in place to catch the cyber-attack when it takes place. Post incident, the insurer will then remediate any damage done, including financial and reputation. The remediation function includes recovery of data, insurance recoveries and potential claims against third parties. Finally, the whole process starts again with an assessment of the company's vulnerabilities, including an understanding of a previously unknown threat.

Types of Security Risks

The CSI "2001 Computer Crime and Security Survey[2]" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting. According to the survey, eighty-five percent of respondents detected computer security breaches within the last twelve months and the total amount of financial loss reported by those who could quantify the loss amounted to $377,828,700, over $2,000,000 per event.

One logical method for categorizing financial loss is to separate loss into three general areas of risk:

- **First Party Financial Risk:** direct financial loss not arising from a third party claim (called First Party Security Risks),
- **Third Party Financial Risk**: a company’s legal liabilities to others, called Third Party Security Risks, and
- **Reputation Risk:** the less quantifiable damages such as those arising from a loss of reputation and brand identity. These risks, in turn, arise from the particular cyber-activities. Cyber-activities can include: having a web site presence, email, Internet professional services such as web design or hosting, network data storage and e-commerce (i.e. purchase or sale of goods/services over the internet).

First Party Security Risks include financial loss arising from damage, destruction or corruption of a company’s information assets, i.e. data. Information Assets whether in

[2] See http://www.gocsi.com for additional information

the form of customer lists and privacy information, business strategies, competitor information, product formulas or other trade secrets vital to the success of a business are the real assets of the 21st century. Their proper protection and quantification is key to a successful company. Malicious code transmissions and computer viruses whether launched by a disgruntled employee, over zealous competitor, cyber-criminal or prankster can result in enormous costs of recollection and recovery.

A second type of First Party Security Risk is the risk of loss of revenue arises from a successful Denial-of-Service attack. In February 2000, a distributed DOS attack was launched against some of the most sophisticated web sites including Yahoo, Buy.com, CNN and others resulting in $1.2B in loss revenue and related damages according to the Yankee Group. Finally, First Party Security Risk can arise from the theft of trade secrets.

Third Party Security Risk can manifest itself in a number of different types of legal liability claims against a company, its directors and officers or employees. Examples of these risks can arise from the company's presence on the web, its rendering of professional services, the transmission of malicious code or a denial-of-service attack (whether or not intentional) and theft of the company's customer information.

The very content of a company's web site can result in allegations of copyright and trademark infringement, libel or invasion of privacy claims. The claims need not even arise from the visual part of a web page but can, and often do, arise out of the content of a site's meta-tags, the invisible part of a web page used by search engines.

If a company renders internet-related professional services to others, this too can be a source of liability. Customers or others who allege that such services, such as web design or hosting, were rendered in a negligent manner or in violation of a contractual agreement may find relief in the court system.

Third party claims are imaginable directly arising from a failure of security. A company which negligently or through the actions of a disgruntled employee transmits a computer virus to its customers or other email recipients may be open to allegations of negligent security practices. The accidental transmission of a denial-of-service attack can pose similar legal liabilities. In addition, if a company has made itself legally obligated to maintain its web site open on a 24/7 basis to its customers, a denial-of-service attack shutting down the web site could result in claims by its customers. A wise legal department will make sure that the company's customer agreements specifically permit the company to shut down its web site for any reason at any time without incurring legal liability.

Other potential third party claims can arise from the theft of customer information such as credit card information, financial information, health information or other personal data. For example, theft of credit card information could result in a variety of potential lawsuits whether from the card issuing companies who must undergo the expense of reissuing, the card holders themselves or even the web merchants who later become the victims of the fraudulent use of the stolen credit cards. As discussed later, certain industries such as financial institutions and health care companies have specific regulatory obligations to guard their customer data.

Directors and officers ("D&Os") face unique, and potentially personal, liabilities arising out of their fiduciary duties. In addition to case law or common law obligations, D&Os can have obligations under various statutory laws such as the Securities Act of 1933 and the Securities & Exchange Act of 1934. Certain industries may also have specific statutory obligations such as those imposed on financial institutions under the Gramm-Leach-Bliley Act (GLBA), discussed in detail later.

Perhaps the most difficult and yet one of the most important risks to understand is the intangible risk of damage to the company's reputation. Will customers give a company their credit card numbers once they read in the paper that a company's database of credit card numbers was hacked into? Will top employees remain at a company so damaged? And, what will the reaction of the company's shareholders? Again, the best way to analyze reputation risk is to attempt to quantify it. What is the expected loss of future business revenue? What is the expected loss of market capitalization? Can shareholder class or derivative actions be foreseen and, if so, what can the expected financial cost of those actions be in terms of lawyer fees and potential settlement amounts?

The risks just discussed are summarized in Table 1 below:

Table 1: First/Third Party Risks

Activity	First Party Risk	Third Party Risk
Web site presence	Damage or theft of data (assumes database is connected to network) via hacking.	Allegations of trademark, copyright, libel, invasion of privacy and other “web content” liabilities.
Email	Damage or theft of data (assumes database in connected to network) via computer virus; Shut down of network via denial-of-service attack.	Transmission of malicious code (e.g. NIMDA) or DOS alleging due to negligent network security. Denial-of-service customer claims if site is shut down due to DOS attack.
eCommerce	Loss of revenue due to successful DOS attack.	Customer suits.
Internet Professional Services		Customer suits alleging negligent performance of professional services.
Any		Claims against directors and officers for mismanagement.

Threats

These risks defined above do not exist in a vacuum. They are the product of specific threats, operating in an environment featuring specific vulnerabilities which allow those threats to proceed uninhibited. Threats may be any person or object, from a disgruntled employee to an act of nature, which may lead to damage or value loss for an enterprise. While insurance may be used to minimize the costs of a destructive event, it is not a substitute for controls on the threats themselves.

Threats may arise from external or internal entities, and may be the product of intentional or unintentional action. External entities comprise the well-known sources – hackers, virus writers – as well as less obvious ones such as government regulators or law enforcement entities. Attackers may attempt to penetrate IT systems through various means, including exploits at the system, server, or application layers. Whether the intent is to interrupt business operations, or to directly acquire confidential data or access to trusted systems, the cost in system downtime, lost revenue, and system repair and redesign can be crippling to any enterprise. The collapse of the British Internet Service Provider (ISP) Cloud-Nine in January 2002, due to irreparable damage caused by distributed denial-of-service attacks launched against its infrastructure, is only the most recent example of the enterprise costs of cyber-attacks[3].

[3] Coverage provided in ISPreview, ZDNet

Viruses and other malicious code frequently use the same exploits as human attackers in order to gain access to systems; however, as viruses can replicate and spread themselves without human intervention, they have the potential to cause widespread damage across an internal network, or the Internet as a whole.

Risks may arise from non-human factors as well. For example, system outages through failures at the ISP level, power outages, or natural disasters may create the same loss of service and revenue as attackers conducting denial of service attacks; therefore, technical controls should be put in place to minimize those risks. These risks are diagrammed in "Figure 2 – Enterprise Resource Threats".

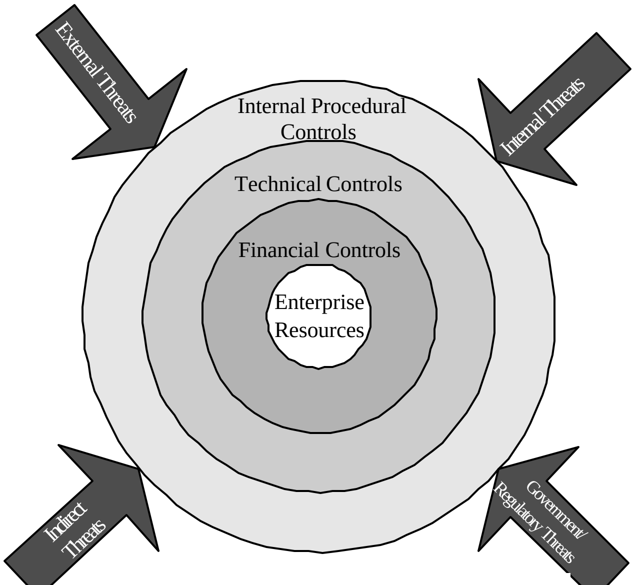


Figure 2 – Enterprise Resource Threats

Threats which originate from within an organization can be particularly difficult to track. This may entail threats from disgruntled employees (or ex-employees), or mistakes made by well-meaning employees as well. Many standard technical controls – firewalls, anti-virus software, or intrusion detection – assume that the internal users are working actively to support the security infrastructure. However, such controls are hardly sufficient against insiders working actively to subvert a system. Other types of risks, for example, first party risks of intellectual property violations may be created by internal entities without their knowledge. "Table 2: Threat Matrix" describes various threats by type:

Table 2: Threat Matrix

Threat		Description	Security Risk	Controls
External	*System Penetration (External Source)*	Attempts by external parties to penetrate corporate resources to modify or delete data or application systems.	Moderate	Strong authentication Strong access control Ongoing system support and tracking.
	Regulatory Action	Regulatory action or investigation based on corporate non-compliance with privacy and security guidelines.	Low-Moderate	Data protection Risk assessment and management programs User training Contractual controls
	Virus Penetration	Malicious code designed to self-replicate and	Moderate	Technological: Anti-Virus Controls
	Power Loss/ Connectivity Loss	Loss of Internet connectivity, power, cooling system. May result in large-scale system outages.	Low	Redundant Power & Connectivity. Contractual controls with ISP/Hosting Facilities

Internal	*Intellectual Property Violation*	Illicit use of third party intellectual property – images, text, code – without appropriate license arrangements	Low-Moderate	Procedural/Personnel Controls Financial controls mitigating risk
	System Penetration (Internal Source)	Malicious insiders attempting to access restricted	Moderate	Strong Authentication Strong Access control Use of internal firewalls to segregate critical systems.

As noted above, threats are comprised of motive, access, and opportunity – outsiders must be provided with a desire to cause damage as well as a means of affecting the target system. While an organization's exposure to risk can never be completely eliminated, all steps should be taken to minimize exposure and limit the scope of damage. Such vulnerabilities may take a number of forms.

Technical vulnerabilities include exploits against systems at the operating system, network, or application level. Given the complexity and scope of many commercial applications, vulnerabilities within code become increasingly difficult to detect and eradicate during the testing and quality assurance (QA) processes. Examples range from the original 'Internet Worm' to recently documented vulnerabilities in commercial instant messaging clients and web servers. Such weaknesses are an increasing risk in today's highly interconnected environments.

Weaknesses within operating procedures may expose an enterprise to risk not controlled by technology. Proper change management processes, security administration processes, and human resources controls and oversight, for example, are necessary. They may also prove disruptive in highly regulated environments, such as financial services or health care, in which regulatory agencies require complete sets of documentation as part of periodic auditing requirements.

GLBA/HIPAA

Title V of the Gramm-Leach-Bliley Act (GLBA) has imposed new requirements on the ways in which consumer data is handled by financial services companies. The primary focus of Title V, and the area which has received the most attention, is the sharing of personal data between organizations and their non-affiliated business partners and agencies. Consumers must be given notice of the ways in which their data is used, and must be given notice of their right to 'opt-out' of any data sharing plan.

However, Title V also requires financial services organizations to provide adequate security for systems which handle customer data. Security guidelines require the creation and documentation of detailed data security programs addressing both physical and logical access to data, risk assessment and mitigation programs, and employee training in the new security controls. Third party contractors of financial services firms are also bound to comply with the GLBA regulations.

On February 1, 2001, the Department of the Treasury, Federal Reserve System and Federal Deposit Insurance Corporation issued interagency regulations in part, requiring financial institutions to:

- Develop and execute an Information Security Program.
- Conduct regular tests of key controls of the Information Security Program. These tests should be conducted by an independent 3rd party or staff independent of those that develop or maintain the program.
- Protect against destruction, loss or damage to customer information, including encrypting customer information while in transit or storage on networks).
- Involve the Board of Directors, or appropriate committee of the Board, to oversee and execute all of the above.

Since, the responsibility for developing specific guidelines for compliance was delegated to the various federal and state agencies which oversee commercial and financial services and some are still in the process of being issued, it is possible that different guidelines for GLBA compliance will develop between different states and different financial services industries (banking, investments, insurance, etc.).

The Health Insurance Portability and Accountability Act (HIPAA) will force similar controls on data privacy and security within the health care industry. As part of HIPAA regulations, health care providers, health plans, and clearinghouses are responsible for protecting the security of client health information. As with GLBA, customer medical data is subject to controls on distribution and usage, and controls must be established to protect the privacy of customer data. Data must also be classified according to a standard classification system to allow greater portability of health data between providers and health plans. Specific guidelines on security controls for medical information have not been issued yet. HIPAA regulations are enforced through the Department of Health and Human Services.

As GLBA and HIPAA regulations are finalized and enforced, regulators will be auditing those organizations who handle medical or financial data to confirm compliance with their security programs. Failure to comply can be classified as an unfair trade practice, and may result in fines or criminal action. Furthermore, firms which do not comply with privacy regulations may leave themselves vulnerable to class action law suits from clients or third-party partners. These regulations represent an entirely new type of exposure for certain types of organizations as they increase the scope of their IT operations.

Cyber-terrorism

The potential for cyber-terrorism deserves special mention. After the attacks of 9/11/01, it is clear that no area of the world is protected from a potential terrorist act. The internet plays a critical role in the economic stability of our national infrastructure. Financial transactions, running of utilities and manufacturing plants and much more are dependent upon a working Internet. Fortunately, companies are coming together in newly formed entities such as ISACs (Information Sharing and Analysis Centers) to determine their interdependency vulnerabilities and plan for the worse. It is also fortunate that the weapons used by a cyber-terrorist do not differ much from those of a cyber-criminal or other hacker. Thus, the same risk management formula that discussed above should be implemented for the risk of cyber-terrorism.

Insurance for Cyber-risks

Insurance, when property placed, can serve two important purposes. First, it can provide positive reinforcement for good behavior by adjusting the availability and affordability of insurance depending upon the quality of an insured's Internet security program. It can also condition the continuation of such insurance on the maintenance of that quality. Second, insurance will transfer the financial risk of a covered event from a company's balance sheet to that of the insurer.

The logical first step in evaluating potential insurance solutions is to review the company's traditional insurance program including its Property (including Business Interruption) Insurance, Comprehensive General Liability (CGL), Directors and Officers insurance, Professional Liability Insurance and Crime policies. These policies should be examined in connection with a company's particular risks (see above) to determine whether any gap exists. Given that these policies were written for a world that no longer exists, it is not surprising that traditional insurance policies are almost always found to be inadequate to address today's cyber-needs. This is not due to any *defect* in these time-honored policies but simply due to the fact that with the advert of the new economy risks, there develops a need for specialized insurance to meet those new risks.

One of the main reasons why traditional policies such as Property and CGL do not provide much coverage for cyber-risks is their approach that “property” means *tangible* property and not data. Property policies also focus on *physical* perils such as fire and windstorm. Business Interruption insurance is sold as part of a Property policy and covers, for example, lost revenue when your business burns down in a fire. It will not, however, cover eRevenue loss due to a denial-of-service attack. Even “computer crime” policies usually do not cover loss other than for money, securities and other *tangible* property. This is not to say that traditional insurance can *never* be helpful with respect to cyber-risks. A mismanagement claim against a company’s directors and officers arising from cyber-events will generally be covered under the company’s directors and officers insurance policy to the same extent as a non-cyber claim. For companies who render professional services to others for a fee, such as financial institutions, those which fail to reasonably render those services due to a cyber risk may find customer claims to be covered under their Professional Liability policy. (Internet professional companies should still seek to purchase a specific Internet professional liability insurance policy.)

Specific Cyber-Liability and Property Loss Policies

The inquiry detailed above, however, does illustrate the extreme dangers associated with relying upon traditional insurance policies to provide broad coverage for 21st century cyber-risks. Regrettably, at present there are only a few specific policies providing expressed coverage for all the risks of cyber-space listed at the beginning of this article. One should be counseled against buying an insurance product simply because it has the name “internet” or “cyber” in it. So-called Internet Insurance policies vary widely with some providing relatively little real coverage. A properly crafted internet-risk program should contain multiple products within a *suite concept* permitting a company to choose which risks to cover depending upon where it is in its internet maturity curve.[4] A suite should provide at least 6 coverages:

Table 3: First/ Third Party Coverage

	First Party Coverage	Third Party Coverage
Media		Web Content Liability
E&O		Professional Liability
Network Security	Cyber-attack caused damage, destruction and corruption of Data, theft of trade secrets or eRevenue business interruption	Transmission of a computer virus or DOS Liability; Theft of Customer Information Liability; DOS Customer Liability
Cyber-extortion	Payment of cyber-investigator	Payment of extortion amount where appropriate
Reputation	Payment of public relations fees up to $50,000	
Criminal Reward	Payment of criminal reward fund up to $50,000	

These coverages may be summarized as follows:

[4] One carrier’s example of this concept can be found at www.aignetadvantage.com.

Web Content Liability provides coverage for claims arising out of the content of your web site (including the invisible meta-tags content) such as libel, slander, copyright and trademark infringement.

Internet Professional Liability provides coverage for claims arising out of the performing of professional services. Coverage usually includes both web publishing activities as well as pure Internet services such as being an ISP, host or web designer. Any professional service conducted over the Internet can usually be added to the policy.

Network Security Coverage comes in two basic types:

- <u>Third Party Coverage</u> provides liability coverage arising from a failure of the insured's security to prevent unauthorized use or access of its network. This important coverage would apply, subject to the policy's full terms, to claims arising from the transmission of a computer virus (such as the Love Bug or NIMDA Virus), theft of a customer's information (most notably including credit card information) and so-called Denial of Service liability. In the last year alone there has been reported countless cases of this type of misconduct.
- <u>First Party Coverage</u> provides, upon a covered event, reimbursement for loss arising out of the altering, copying, misappropriating, corrupting, destroying, disrupting, deleting, damaging or theft of information assets, whether or not criminal. Typically the policy will cover the cost of replacing, reproducing, recreating, restoring or recollecting. In case of theft of a trade secret (a broadly defined term), the policy will either pay

or be capped at the endorsed negotiated amount.

First Party Coverage also provides reimbursement for lost eRevenue as a result of a covered event. Here the policy will provide coverage for the Period of Recovery plus an extended business interruption period. Some policies also provide coverage for Dependent Business interruption, meaning loss of eRevenue as a result of a computer attack on a third party business (such as a supplier) upon which the insured's business depends.

Cyber-extortion provides reimbursement of investigation costs, and sometimes the extortion demand itself, in the event of a covered cyber-extortion threat. These threats which usually take the form of a demand for "consulting fees" to prevent the release of hacked information or to prevent the extortion from carrying out a threat to shut down the victims' web site are all too common.

Public Relations or Crisis-communication coverage provides reimbursement up to $50,000 for use of public relation firms to re-build an enterprise's reputation with customers, employees and shareholders following a computer attack.

Criminal Reward funds coverage provides reimbursement up to $50,000 for information leading to the arrest and conviction of a cyber-criminal. Given that many cyber-criminals hack into sites for "bragging rights", this unique insurance provision may create a most-welcomed chilling effect.

Loss Prevention Services

Another important feature of a quality cyber-risk insurance program is its loss prevention services. Typically these services could include anything from free on-line self-assessment program and free educational CDs, to a full-fledged on-site security assessment, usually based on ISO 17799. Some insurers may also add other services such as an internal or external network scan or other services. The good news is that these services are valuable costing up to $50,000. The bad news is that the insurance applicant usually has to pay for the services, sometimes regardless of whether it ends up buying the policy! Beginning in 2001, one carrier has arranged to pay for these services themselves as part of the application process. This is welcomed news. It can only be hoped that more insurers follow this lead.

Finding the Right Insurer

As important as finding the right insurance product is finding the right insurer. Financial strength, experience and claims philosophy are all important. In evaluating insurers, buyers should take into consideration:

Table 4: Finding the Right Insurer

Quality	Preferred or Minimum Threshold
Financial Strength	Triple-A from Standard & Poor
Experience	At least 2 years in dedicated, specialized unit composed of underwriters, claims, technologists and legal professionals

Capacity	Defined as amount of limits single carrier can offer, minimum acceptable: $25,000,000
Territory	Global presence with employees and law firm contacts throughout the U.S., Europe, Asia, Middle East, South America.
Underwriting	Flexible, Knowledgeable,
Claims Philosophy	Customer focused. Willing to meet with client both before and after claim.
Policy Form	Suite permitting insured to choose right coverage including 8 cover ages described above.
Loss Prevention	Array of services most importantly including FREE on-site security assessments conducted by well established third party (worldwide) security assessment firms.

In summary traditional insurance is not up the task of dealing with today's cyber-risks. To obtain the full benefits insurance program should provide a purchase combination of traditional insurance and specific cyber-risk insurance should be implemented.

Technical Controls

Beyond insurance, standard technical controls must be put in place to manage risks. First of all, the basic physical infrastructure of the IT data center should be secured against service disruptions caused by environmental threats. Organizations that plan to build and manage their own data center should implement fully redundant and modular systems for power, internet access, and cooling. For example, data centers should consider backup generators in case of area-wide power failure, and Internet connectivity from multiple ISPs in case of service outages from one provider.

In cases where the customer does not wish to directly manage their data center, the above controls should be verified before contracting with an ASP or ISP. These controls should be guaranteed contractually, as should failover controls and minimum uptime requirements.

Physical Access Control

Access control is an additional necessity for a complete data center infrastructure. Physical access control is more than simply securing entrances and exits with conventional locks and security guards. Secure data centers should rely on alarm systems and approved locks for access to the most secure areas, and motion detectors throughout. More complex security systems, such as biometric[5] or dual-factor authentication (authentication requiring more than one proof of identity; e.g., card and biometric), should be considered for highly secure areas. Employee auditing and tracking for

[5] Biometrics authentication comprises many different measures, including fingerprint scans, retinal or iris scans, handwriting dynamics, and facial recognition.

entrances and exits should be put in place wherever possible, and visitor and guest access should be limited. A summary of potential controls is provided in "Table 5 – Physical Controls" below.

If it is feasible to do so, outside expertise in physical security, just like logical security, should be leveraged wherever possible. Independent security audits may provide insight regarding areas of physical security which are not covered by existing controls. Furthermore, security reports may be required by auditors, regulators, and other third parties. Audit reports and other security documentation should be kept current and retained in a secure fashion.

Again, if an organization uses outsourced facilities for application hosting and management, it should look for multi-level physical access control. Third-party audit reports should be made available as part of the vendor search process; security controls should be made part of the evaluation criteria. As with environmental controls, access controls should also be addressed within the final service agreement, such that major modifications to the existing access control infrastructure require advance knowledge and approval of the contractees. Organizations should insist on periodic audits or third-party reviews to ensure compliance.

Table 5: Physical Controls

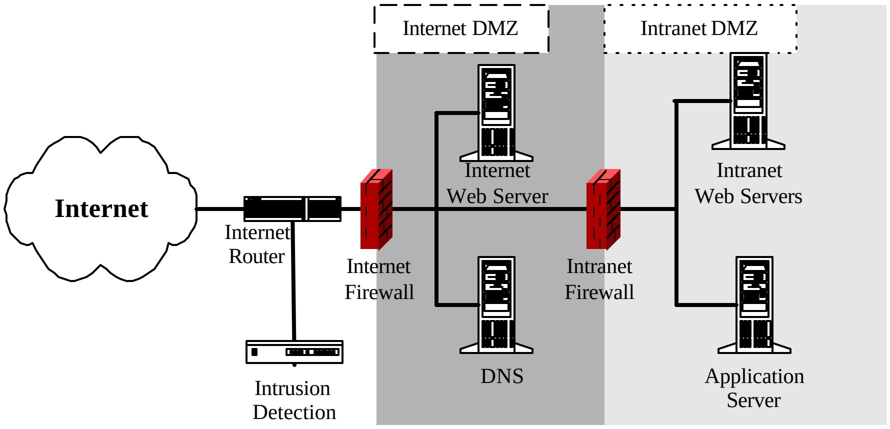
Physical Control	Description	Role
Access Control	Grants access to physical resources through possession of	Securing data center access in general, as well as access to core resources such as server rooms.

	keys, cards, biometric indicators, or key combinations. Multi-factor authentication may be used to increase authentication strength. Access control system which require multiple-party authentication provide higher levels of access control	Media – disks, CD-ROMS, tapes – should be secured using appropriate means as well. Organization s should model their access control requirements on the overall sensitivity of their data and applications
Intrusion Detection	Detection of attempted intrusion through motion sensors, contact sensors, and sensors at standard access points (doors, windows, etc.)	At all perimeter access points to the data center, as well as in critical areas.
24/7 Monitoring	Any data center infrastructure should rely on round-the-clock monitoring, through on-premises personnel and/or off-site monitoring.	Validation to existing alarm and access control systems.

Network Security Controls

A secure network is the first layer of defense against risk within an eBusiness system. Network level controls are instrumental in preventing unauthorized access from within and without, and tracking sessions internally to detect and alert administrators in the case of system penetration. "Figure 3 – Demilitarized Zone Architecture" depicts conceptually the overall architecture of an eBusiness data center.

Figure 3 –Demilitarized Zone Architecture



Common network security controls include:

Firewalls – firewalls are critical components of any internet-facing system. Firewalls filter network traffic based on protocol, destination port, or packet content. As firewall systems have become more advanced, the range of different attack types which can be recognized by the firewall has continued to grow. Firewalls may also be upgraded to filter questionable content, or scan incoming traffic for attack signatures or illicit content.

For any infrastructure which requires access to business data, a multiple firewall configuration should be used. An Internet Demilitarized Zone ("DMZ") should be created for all web-accessible systems – web servers or DNS servers – while an Intranet DMZ, separated from the internet, contains application and database servers. This architecture prevents external entities from directly accessing application logic or business data.

Network Intrusion Detection Systems – Networked IDS systems track internal sessions at major network nodes and look for attack signatures – a sequence of instructions corresponding to a known attack. These systems generally also are tied into monitoring systems which can alert system administrators in the case of detected penetration. More advanced IDS systems look for only 'correct' sequences of packets, and use real-time monitoring capabilities to identify suspicious but unknown sequences.

Anti-Virus Software – Anti-virus gateway products can provide a powerful second level of defense against worms, viruses, and other malicious code. Anti-virus gateway products, provided by vendors such as Network Associates, Trend Micro, and Symantec, can scan incoming HTTP, SMTP, and FTP traffic for known virus 'signatures' and block the virus before it infects critical systems.

As described in “Table 6: Secure Network Design Principles”, the following design principles should be observed in building a stable and secure network. “Table 7: Network Security Controls” provides a summary of the controls in question.

Table 6: Secure Network Design Principles

Redundancy	Firewall systems, routers, and critical components such as directory servers should be fully redundant to reduce the impact of a single failure.
Currency	Critical network tools must be kept up-to-date with respect to patch level and core system operations. Vulnerabilities are discovered frequently, even within network security devices such as firewalls or routers.
Scalability	An enterprise’s network security infrastructure should be able to grow as business needs require. Service outages caused by insufficient bandwidth provided by an ISP or server outages due to system maintenance can be fatal for growing applications. The financial restitution provided by Cyber-risk coverage might cover business lost during the service outage, but cannot address the greater issues of loss of business, consumer goodwill, or reputation.
Simplicity	Complexity of systems, rules, and components can create unexpected vulnerabilities in commercial systems. Where possible, Internet-facing infrastructures should be modularized and simplified such that each component is not called upon to perform multiple services. For example, an organization with a complex eBusiness infrastructure should separate that network environment from its own internal testing and development networks, with only limited points of access between the two environments. A more audited and restricted set of rules may be enforced in the former without affecting the productivity of the latter.

Table 7: Network Security Controls

Network Control	Description	Role
Firewall	Blocks connections to internal resources by protocol, port, and address. Also provides stateful packet inspection	Behind Internet routers. Also within corporate networks to segregate systems into DMZs
IDS	Detects 'signature' of known attacks at the network level	At high-throughput nodes within networks, and at perimeter of network (at firewall level)
Anti-Virus	Detects malicious code at network nodes	At Internet HTTP and SMTP gateways

Increasingly, organizations are moving towards managed network services rather than supporting the systems internally. Such a solution saves the organization from having to build staff for managing security devices, or to maintain a 24-7 administration center for monitoring critical systems. Such a buy (or, in this case, hire) –vs.-build decision should be considered very strongly in planning your overall risk management framework. Organizations looking to outsource security functions can certainly save money, resources, and time; however, organizations should look closely into the financial as well as technical soundness of any such vendors.

Application Security Controls

A successful network security strategy is only useful as a backbone to support the development of secure applications. These controls entail security at the operating system level for enterprise systems, as well as trust management, encryption, data security, and audit controls at the application level.

Operating systems should be treated as one of the most vulnerable components of any application framework. Too often, application developers create strong security controls within an application, but have no control over the lower level exploits. Furthermore, system maintenance and administration over time is frequently overlooked as a necessary component of security. Therefore, the following controls should be observed:

1. Most major OS suppliers – Microsoft, Sun, Hewlett Packard, etc. – provide guidelines for operating system hardening. Implement those guidelines on all production systems.
2. Any non-essential software should be removed from production systems.
3. Administer critical servers from the system console wherever possible. Remote administration should be disabled; if this is not possible, secure login shells should be used in place of less secure protocols such as Telnet.

~~3.System-level administration should be enabled from the console only whenever possible.~~

4. Host-based intrusion detection software should be installed on all critical systems. Host-based IDS is similar to the network-based variety, except it only scans traffic intended for the target server. Known attack signatures may be detected and blocked before reaching the target application, such as a web or application server.

Application level security is based on maintaining the integrity and confidentiality of the system itself, as well as the data managed by the system. A web server which provides promotional content and brochures to the public, for example, has little need to provide controls on confidentiality. However, a compromise of that system resulting in vandalism or server downtime could prove costly; therefore, system and data integrity should be closely controlled. Partially, these controls are provided by secur ity and the operating system and network levels as noted above; additional controls, however, should be provided within the application itself.

Authentication and authorization are necessary components of application level security. Known users must be identified and allowed access to the system, and system functions must be categorized such that users are only presented with access to data and procedures which correspond to their defined privilege level.

The technical controls around authentication and authorization are only as useful as the procedural controls around user management. The enrollment of new users, management of personal user information and usage profiles, password management, and the removal of defunct users from the system are required for an authentication engine to provide real risk mitigation.

“Table 8: Application Security Controls” provides a summary of these technologies and procedures.

Table 8: Application Security Controls

Application Control	Description	Role
System Hardening	Processes, procedures, and products to harden operating system against exploitation of network services or	Should be performed for all critical servers and internal systems
Host Based Intrusion Detection	Monitors connections to servers and detects malicious code or attack signatures	On all critical servers and internal systems.
Authentication	Allows for identification and management of system users through identities and passwords	For any critical systems. Authentication systems may be leveraged across multiple applications to provide single sign-on for enterprise
Access Control	Maps users, by identity or by role, to system resources and functions	For any critical application.
Encryption	Critical business data or non-public client information should be encrypted, that is, obscured, while in transit over public networks	For all Internet-based transactional connectivity. Encryption should also be considered for securing highly sensitive data in storage.

Data Backup and Archival

In addition to technologies to prevent or detect unauthorized system penetration, controls should be put in place to restore data in the event of loss. System backups – onto tape, or permanent media - should be in place for any business-critical application.

Backups should be made regularly – as often as daily depending on the requirements of the business – and should be stored off-site to prevent loss or damage. Test restores should be performed regularly as well, in order to ensure the continued viability of the backup copies. Backup retention should extend to at least a month; with one backup per week retained for a year, and monthly backups retained for several years. Backup data should always be created and stored in a highly secure fashion.

Lastly, in order to ensure system availability, enterprise applications should plan on at least one tier of redundancy for all critical systems and components. Redundant systems can increase the load bearing capacity of a system, as well as providing increased stability. The use of enterprise-class, multi-processor machines is one solution; multiple systems can also be consolidated into server 'farms'. Network devices such as firewalls and routers can also be made redundant through load balancers. Businesses may also wish to consider maintaining 'standby' systems in event of critical data center failure. Standby systems, like backups, should be housed in a separate storage facility, and should be tested periodically to ensure stability. These backup systems should be able to be brought online within 48 hours of a disaster, and should be restored with the most recently available system backups as well.

Conclusion

The optimal model to address the risks of internet security must combine technology, process and insurance. This Risk Management approach permits companies to address successfully a range of different risk exposures, from direct attack on system resources to unintentional acts of copyright infringement. In some cases, technical controls have been devised which help address these threats; in others, procedural and audit controls must be implemented. Because these threats cannot be completely removed, however, Cyber-Risk insurance coverage represents an essential tool in providing such non-technical controls and a major innovation in the conception of risk management in general. A comprehensive policy backed by a specialized insurer with top financial marks and global reach allows organizations to lessen the damage caused by a successful exploit, and better manage costs related to loss of business and reputation. It is only though merging the two types of controls that an organization can best minimize it security threats and mitigate its IT risks.

Appendix A – The Eleven Domains of Risk Assessment

1) Security Policy

During the assessment, the existence and quality of the organization's security policy is evaluated. Security policies should establish guidelines, standards and procedures to be followed by the entire organization. These need to have been updated frequently.

2) Organizational Security

One of the key areas that any assessment looks at is the organizational aspects of security. This means ensuring that adequate staff has been assigned to security functions, that there are hierarchies in place for security related issues, and that people with the right skill sets and job responsibilities are in place

3) Asset Classification and control

Any business will be impacted if the software and hardware assets it has are compromised. In evaluating the security of the organization, the existence of an inventory management system and risk classification system have to be verified.

4) Personnel security

The hiring process of the organization needs to be evaluated to ensure that adequate background checks and legal safeguards are in place. Also, employee awareness of security and usage policies should be determined

5) Physical and environmental security

Ease of access to the physical premises need to be tested, making sure that adequate controls are in place to allow only authorized personnel access. Also, the availability of redundant power supplies and other essential services have to be ensured.

6) Communication and Operations Management

Operational procedures need to be verified to ensure that information processing occurs in a safe and protected manner. These should cover standard operating procedures for routine tasks as well as procedures for change control for software, hardware and communication assets

7) Access Control

This domain demands that access to systems and data be determined by a set of criteria based on business requirement, job responsibility and time period. Access control needs to be constantly verified to ensure that it is available only of a need to know basis with strong justification

8) Systems Development and Maintenance

If a company is involved in development activity, the assessment to determine if security considerations are a key part at all stages of the development lifecycle.

9) Business Continuity Management

Determining the existence of a business continuity plan that minimizes or eliminates the impact of business interruption is a part of the assessment

10) Compliance

The assessment has to determine if the organization is in compliance with all regulatory, contractual and legal requirements.

11) Financial Considerations

The assessment should include a review to determine if adequate safeguards have to be implemented to ensure that any security breach results in minimal financial impact. This is implemented through risk transfer mechanisms; primarily insurance that covers the specific needs of the organization.