

# Network Risk Insurance: A Layman's Overview

October 2004

*Kevin Kalinich*

*kevin\_kalinich@ars.aon.com*

*+1.312.381.4203*

*Mark Greisiger*

*mark.greisiger@netdiligence.com*

*+1.610.568.0913*

## What Is It?

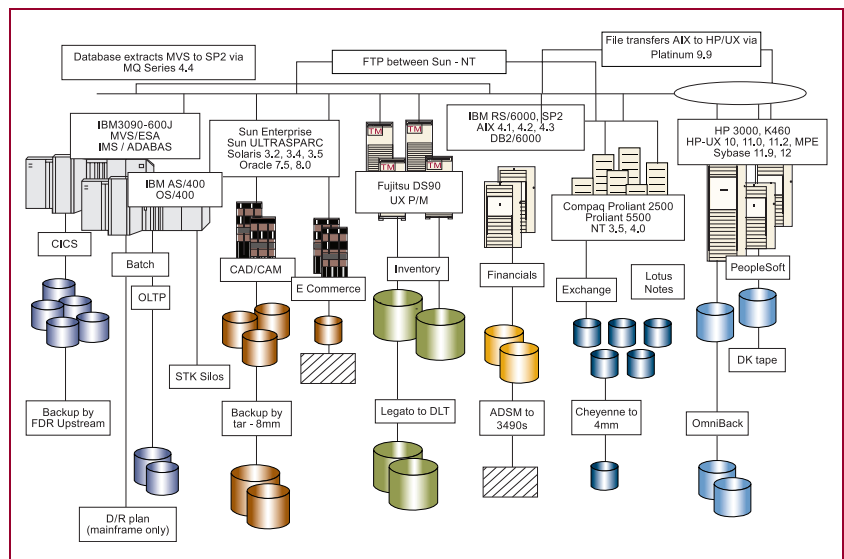
Network Risk Insurance is coverage to address the unique ‘e-risk’ exposures associated with electronic processes, interactions and digital assets arising from computer-dependent business activities that may effect an entity’s financial statements.

*First-party* insurance policies may provide coverage for business interruption losses arising from the interruption, suspension or degradation of an entity’s own computer network, including business income, extra expense and contingent dependent business interruption. For example, it has been widely reported that a distributed denial-of-service attack disrupted Web-based systems at credit card payment processing firm Authorize.Net Corp. recently. Its lost revenue and extra expense to repair the damage could be covered by Network Risk Insurance. In addition, the value of an entity’s digital assets may be protected involving data, computer system resources and information assets, such as customer data, proprietary information, trade secrets, order fulfillment and credit card or other sensitive data and e-records. Cyber extortion, cyber terrorism, crisis communication and forensic investigative services may also be added by endorsement.

*Third-party liability* coverage provides damage and defense costs suffered by others due to a failure of the insured’s computer network, systems and software applications. According to published sources, Authorize.Net’s customers have suffered millions in losses, which could be covered under the liability portion of the payment processor’s Network Risk Insurance. This includes liability caused by transmission of a computer virus, unauthorized access, denial-of-service, disclosure of confidential information and identity theft. Such insurance may also cover content-based injuries such as libel, slander, defamation, copyright, trademark infringement and invasion of privacy from the display of material on an entity’s website. If an entity provides professional services in connection with networks, then those services may be covered also, such as xSP’s, technology consultants and software developers.

## Who Needs It?

Nearly every entity in operation today relies on electronic networks (including the information, data and the e-records within these computer networks), regardless of whether it sells products from a website. Such entities are judged by Wall Street, shareholders, customers and spheres of influence not only on the quality of their products and services, but also on their ability to deliver consistent and predictable earnings. A critical factor in increasing earnings predictability is adequate management of network exposures. These exposures extend far beyond those specific to a corporate Web site. If an entity uses email, computerized accounting, electronic procurement, electronic fulfillment, RFID, or stores electronic data, it has network exposures.



Many entities are underinsured against network risks and they either do not realize it or do not understand the potential impact of such risks. Precedent setting court decisions in 2003 definitively decided that typical general liability and property policies exclude coverage for many “intangible property” related exposures. Recent Insurance Services Office (“ISO”) policy form changes and insurance carrier exclusions coincided with such decisions.

Corporate governance initiatives, such as Sarbanes-Oxley Act of 2002, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), California Security Breach Information Act and the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, all encourage, if not mandate, network risk management. Increasingly, well-informed customers, suppliers, distributors and partners require network risk insurance.

## What Should You Do?

The first step is to identify and prioritize primary network risk concerns. Does your entity have important intangible property, the damage, theft or loss of which could negatively impact your entity financially? Does your entity rely upon technology systems [i.e., records management systems], of which degradation in performance could negatively impact your entity financially? Does your entity have revenue streams that are dependent on the availability of your electronic supply chains, distribution systems, websites, networks, applications or data? Do you have revenue streams that are dependent upon the availability of your customers'/partners' networks?

Companies working to improve their network management have found that the efforts resulted in fewer incidents of unauthorized computer use and a decline in damages. The Computer Security Institute/FBI 2004 survey found that damages related to network attacks declined, reaching about \$290,000 per company versus \$400,000 per company a year ago. Yet the first party losses from viruses has exceeded billions of dollars and third party liability claims for failure to deliver adequate network services and damages caused to another's network from email, networks, systems, etc. are increasing. Given that over 70% of the market capitalization of Fortune 500 companies is attributed to information assets, 1.4 billion emails are sent every day, and there was over \$1 trillion in 2003 online B2B sales, it is no wonder that entities are expected to spend \$14 billion by 2005 fending off network intruders.

Upon completion of a *network risk assessment*, an entity should first eliminate and mitigate the exposures identified to the extent feasible. Network risk mitigation may include physical security measures, documented corporate policies, third party assessments, employee awareness programs and technological safeguards. Demonstration of such mitigation efforts will be required in order to obtain network risk insurance and will improve an entity's risk management in the event insurance is not purchased.

For the remaining e-risk, an entity may choose to review and evaluate available insurance options which address network risk exposures. One may find the pricing of these cyber risk insurance policies is often inconsistent because underwriters do not have a history of claims data upon which to base their pricing. It is recommended that quotations be obtained from several insurers, as differences in pricing as well as terms and conditions can be dramatic. Some insurance carriers offer policies with combined programs of Errors and Omissions and Network Risk with a shared limit of coverage, while some will also offer standalone Network Risk protection. In addition, some carriers will only write such policies if a major insurance relationship exists with the insured. Some carriers offer modular options for specific risks and liabilities.

# How Do Network Risk Underwriters Quantify the Risk?

Unlike more established lines of business insurance there is not yet a set standard for a good network risk underwriting submission [although there are some emerging baseline requirements often sought by the leading insurers]. Presenting your company in the most favorable light requires a bit of effort, pulling together information from various disciplines within your company including risk management, legal (contracts, dispute resolution process and litigation), privacy officer, systems/information technology, sales and marketing, product development, and human resources. If prudent measures are in place in each of these areas, appropriate processes are implemented to coordinate such efforts and this work is well documented in your underwriting submission, your company may be eligible for significant rate credits as well as higher limits and/or lower self-insured retentions.

So what are network risk underwriters looking for?

## 1. Financial Stability and Lack of Losses

Self-explanatory, but cannot be overemphasized. Some industries are more prone to complaints and incidents than others. The insurance carriers realize this fact and will price your risk accordingly. But how do you educate the underwriter that your entity is a better risk than your peers? How is your entity different?

*Key documentation: financial statements and loss runs.*

## 2. Sales Practices and Contract Procedures

Underwriters examine your sales practices to verify mutual expectations of you and your customers. Limitation of liability clauses, exculpation of warranty provisions and consistent contract review procedures are critical.

*Key documentation: standard contracts and guidelines to amend standard clauses.*

## 3. Dispute Procedures

More important than whether you win litigation is how do you avoid litigation? Escalation of dispute procedures .

*Key documentation: complaint and dispute guidelines (i.e., when, how and who gets involved to what extent at each escalation threshold?).*

## 4. Formal Management Responsibility and Standards

First and foremost, companies must successfully demonstrate that the responsibility to maintain a secure network environment is 'owned' by a senior individual within the organization. The presence of ongoing vigilance and a 'security mentality' is paramount. This might be a Chief Security Officer or Chief Technology Officer for a large organization, or a COO or systems administrator for a smaller company. Regardless, unless responsibility is formally assigned to a senior individual, network security will never be considered a priority. Network security policies and procedures should be published and communicated to all staff, and the responsible individual or team should have a budget that allows them to meet policy goals. Finally, Assessments and testing benchmarking to industry standards such as ISO 17799 that include network scanning [and possibly 'ethical Hacking'] should be completed at least twice a year by either an internal team or a trusted and competent third party

*Key documentation: written network security policies and procedures, security audit schedules, security audit reports.*

## 5. Physical Network Security Safeguard Controls

As maintaining a proper network security posture has more to do with process than anything else, the company needs to be able to demonstrate that the physical environment is robust enough to keep the bad guys out. Along with the basics such as magnetic access cards for employees and closed circuit television, key IT facilities such as data centers and server rooms should be accessible only by the IT staff tasked to work in them. Physical security (as with logical) should be 'layered', and staff should know who to call in the event of suspicious activity.

*Key documentation: physical security policies and guidelines, lists of perimeter and internal security elements in place.*

## 6. Logical Network Security Controls

The presence of a written network security, privacy and acceptable usage policies (AUP)\_ which govern the constellation of baseline safeguard controls designed to protect the integrity and security of the organization's computer network should be documented and demonstrated. At a minimum, this should include proxies, filters and firewalls to keep unauthorized intruders from accessing the network from the Internet or other private networks, antivirus software to keep viruses, worms, Trojan horses and other malicious code at bay, and intrusion detection software (IDS) to identify potential network trespassers. In the event that medical, financial or other non-public personally identifiable information (PII) is transmitted via the Internet or stored in a marketing database, Triple DES and/or 128 bit minimum data encryption standards should be enforced. For networks with a large number of users, password management software can automatically ensure that users create alphanumeric passwords that are not easily broken (i.e., guessable), and that are changed periodically. Systems and security logs should also be activated on key servers and networking equipment to assist in future audits and investigations.

Having these security tools in place is necessary, but properly installing, updating and managing them is of equal importance. Servers and firewalls should be 'hardened' upon installation, with default settings reviewed and unneeded services/functionality disabled. Fresh virus definition files should be downloaded from antivirus software vendors at least twice a week, and system and security logs should be manually reviewed periodically for suspicious activity.

*Key documentation: network architecture diagrams, firewall and IDS make and model information, antivirus vendor information, and a copy of the policies and procedures in place to ensure that new equipment is properly configured before it is connected to the network.*

## 7. Change Management Controls

A 'softer' security function requiring consistent communication between the human resources and IT departments, proper change management controls include policies and procedures to ensure that network access rights for ex-employees (and sub-contractors) which have resigned or have been terminated are revoked, and token authentication (SecureID and similar) and facility access cards are revoked during exit interviews. Also, there must be fluid processes to ensure that security precautions are again factored into any request for a system/application/network modification.

*Key documentation: written employee resignation and termination guidelines in network security planning document.*

## 8. Internet Content Controls

A critical area of network liability risk involving the broadcasting of content over the Internet by companies that may not have publishing experience, companies must be able to document written controls over the posting of information to Internet-facing websites. These include legal reviews to ensure that any third party content posted has gone through a formal clearing process, rule sets around the use of Internet deep-links and the use of framing technology, and the proper management of BBS's, chat rooms, discussion boards, and other interactive areas of company sites.

*Key documentation: written rules, including legal reviews, surrounding the posting of content on company sites*

## 9. Disaster Recovery and Business Continuity Planning

This is a critical component of any network risk submission, especially where contractually guaranteed network availability (via a SLA) is offered to customers or network interruption coverage is required by the applicant. Companies with larger networks should be prepared to demonstrate that formal DR/BCP plans are in place not only to protect critical data, but also to ensure that network availability is maintained in the event of a natural disaster, malicious code outbreak, or Denial of Service attack. Elements include data backup and recovery testing, redundant/mirrored applications and connections, hot or warm sites contracted for and periodically tested, and personnel plans to ensure that the human element is covered as well.

*Key documentation: DR/BCP planning reports and outlines, contracts for redundant mirror/hot sites.*

While each insurer maintains its own underwriting requirements, companies with high availability networks or large Internet footprints (visibility) — or companies that simply require higher insured limits — will need to prove that the importance of each of these areas is understood and that network risk exposures have been sufficiently addressed through the preparation of plans and guidelines, the purchase of appropriate hardware and software tools, and ongoing testing, assessments and audits.

The bottom line: network risk insurance underwriters want to know that the applicant takes network security seriously, that the parties responsible for security are adequately trained and funded, and that loss prevention practices — including baseline information security controls — are built into the company's everyday policies and procedures. This ranges from new employee training through the policies and procedures surrounding the handling of sensitive customer data along with the installation of new equipment onto the corporate network, and touches nearly every corporate function. While the insurance coverage applications — for the better network risk programs — include questions in each of these areas, the more documentation that a company can provide proving that they 'walk the walk' can result in significant premium discounts and broader network risk coverage options.

## Conclusion

Technology exposures continue to evolve in an unprecedented manner due to the unique aspects of e-business — 24x7x365 availability, worldwide distribution, dynamic content, etc. Court decisions provide conflicting legal precedence and insurers have minimal historical claims event data. Entities may be left with potentially catastrophic gaps in coverage, which can decimate their bottom line. Maximum financial statement stability related to critical electronic processes and interactions may be achieved through a proactive, comprehensive mitigation initiative combined with network risk specific insurance coverage. Recent case law suggests a trend toward a different treatment for electronic perils.

## About Us:

Aon Technology & Professional Risks Group [www.aon.com](http://www.aon.com) is part of Aon Corporation, which is one of the world's largest insurance brokerage and consulting companies, and conducts business in three segments: insurance brokerage, consulting, and insurance underwriting. Aon Technology & Professional Risks Group has taken a leadership role in the identification, education, mitigation, and transfer of risks posed by an increasingly networked, digital economy.

NetDiligence, [www.netdiligence.com](http://www.netdiligence.com) provides cyber risk and network security assessment and testing services to allow our corporate and financial institution clients to better protect their computer network resources and information assets in order to mitigate potential network liability risk and demonstrate compliance. NetDiligence loss prevention services are endorsed by the cyber-risk insurance industry.

Risk Services

