

CYBER RISKS

How to protect your business
in the Digital Age

Business Insurance
WHITE PAPER

ENTIRE CONTENTS COPYRIGHT © CRAIN COMMUNICATIONS INC. ALL RIGHTS RESERVED.

INTRODUCTION

While cyber risks long have been associated with e-commerce firms, any firm that holds confidential information in an electronic format is exposed to the threat of data loss and breaching state and federal privacy laws.

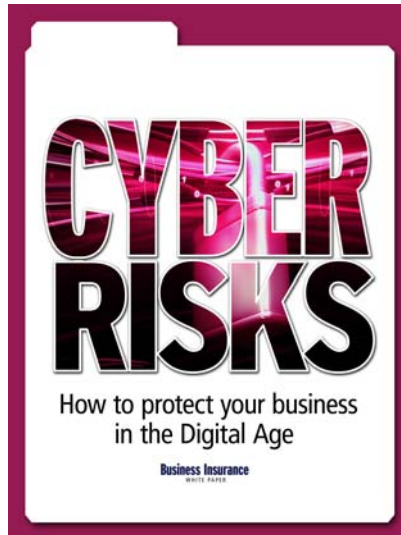
As numerous well-publicized data breaches have shown, organizations from banks to hospitals to government departments face significant cyber-related exposures.

Data breaches, whether they stem from the work of an outside hacker or innocent errors made by staff, can cause huge disruptions for the companies whose information is leaked. And the cost of fixing the breaches and compensating individuals whose private information was released can be substantial.

The executive summary of the latest white paper from Business Insurance, cyber risk and insurance expert Mark Greisiger outlines the exposures that companies face, steps they can take to mitigate those risks, and the insurance coverage available to transfer cyber risks.

As president of NetDiligence, Mr. Greisiger provides cyber risk assessment services for chief financial officers and risk managers to help them better understand whether their organizations deploy reasonable and prudent safeguards to mitigate data breach losses and liability risks.

For more information on how to identify and manage all the cyber risks that organizations face, including detailed opinions from security, legal and insurance experts and a comprehensive directory of cyber insurers, download the complete 33 page white paper at www.businessinsurance.com/whitepapers.



CONTENTS

DATA BREACHES BECOME FACT OF BUSINESS LIFE	3
FIRMS MUST ACT FAST TO STOP FLOW OF DATA	4
SPECIALTY COVERAGE FOR A SPECIALTY RISK	5
DEVELOPING LAYERED SAFEGUARD CONTROLS	6

Visit www.BusinessInsurance.com

DATA BREACHES BECOME FACT OF BUSINESS LIFE

PREPARATION KEY FOR MITIGATION EFFORTS

By Mark Greisiger
mark.greisiger@netdiligence.com

With data and information serving as the lifeblood of most companies, it's not the Apple iPhone that competitors covet, but the design and innovation behind the product. Yet these most valuable assets are threatened by a growing threat: cyber risk or e-risk. Studies such as the annual CSI Computer Crime and Security Survey and Verizon Communications Inc.'s 2010 Data Breach Investigations Report have shown that approximately 80% of all companies will suffer one or more network breach incidents each year.

RISKY BUSINESS

Typical business activities that create cyber risk include:

- E-commerce business websites
- Credit card data collection and online payment processing
- Data storage (online and traditional shipping of paper records or back-up tapes)
- Housing private customer data on laptops
- Business partners, contractors that touch customer data
- Providing online content or media
- Cloud computing and outsourced computing
- Social media sites (Facebook, MySpace, Twitter) that collect and display private information

Privacy is a front-line consumer rights issue. In the United States, the risk of a system breach involving nonpublic sensitive information that affects people (or customers) can lead to a massive class action liability lawsuit, and that's a growing concern for CEOs, chief financial officers and risk managers.

Various privacy regulations require that businesses protect certain sensitive data no matter where it resides: on the network; on stand-alone systems such as tax collection, billing, medical, and marketing databases; on remote devices, such as laptops; and on paper.

Moreover, there are industry standards, such as the PCI Security Standards Council L.L.C.'s PCI Data Security Standard, that can result in multimillion-dollar fines for noncompliance. These regulations and standards also are being used by plaintiffs attorneys as a benchmark standard of care for reasonable and prudent information security practices.

As the value of critical data grows, an organization's cyber risk exposure also increases. But the good news is that companies can protect themselves. With new network-emanaing risks come new forms of loss prevention—and insurance products.

This white paper examines the threats from hackers, thieves, third-party contractors and employees, all of which make it imperative for organizations to implement industry-

recommended security safeguards. We shall also examine the legal ramifications of cyber risk and key strategies for risk managers.

Data breaches are not only a reality in today's risk management landscape, they're also a near-certainty for just about any business. Unfortunately, even the most compliance- and security-focused organization can be victimized by a data breach.

The truth is that a bigger operation often is more complex, with more moving parts and more dependencies on other vendors or partners—and greater visibility.

Nobody is immune from the threat of data breaches, no matter the size of the war chest or the level of technical sophistication.

"Cyber risk" is loosely defined as the chance of injury, damage or loss from an electronic exposure that can result in an adverse impact on a business. To many organizations, this may mean the disclosure, modification/destruction or theft of information, or the unavailability of their transaction website, system or network.

For many organizations, the type of data most at risk includes financial and medical information as well as other personally identifiable information and nonpublic information.

Many risk managers quickly are becoming educated about their own cyber risks, including their duty to safeguard PII data types that their

business may collect, store, use, transact and share with industry-accepted practices. Part of this process is recognizing that cyber risks can come from third-party business partners—and the unknown quality of data security within those trusted organizations.

Today's highly computer-networked business environments often are porous, exposing companies of all types and sizes to cyber security risks and growing legal liability.

Many risks can lead to costly investigations and remedial measures, tarnished reputations, class action lawsuits and lower earnings.

If an average network outage that a company incurs is tantamount to a "snow day" in which no one is working, a data breach can magnify that disruption many times over.

Despite the world's dependence on data/information, networks and business application software, the external audits and studies by leading consulting firms continue to disclose serious informational security weaknesses across all sectors.

Studies show that risk increases when sensitive personal information traverses an online business application or nonpublic personal identification data is stored in an SQL database with access given to numerous internal personnel or external partners.

Poor business practices, such as allowing employees to download a full customer list and e-mail this data (unfiltered or scanned) to the world are still fairly common.

Cyber damage encompasses the loss and damage that results from hacker attacks, employee mistakes and other types of risks to a company's information systems. The extent of cyber damage can range from a nuisance to a catastrophe that seriously erodes data integrity, confidentiality and system availability. In the latter case, the very future of the business can be jeopardized.

The destruction of critical data, paralysis of service and interruption of business transactions can mean financial disaster for any company.

The consequences of a cyber

THREATS

- Hacking (with access to private data)
- Denial-of-service attacks (against a network or the cloud the company leases)
- Information extortion
- Employee or partner mistakes
- Software glitches
- Outright privacy policy violations
- Lost or stolen laptops
- Rogue insiders or contractors
- Improper disposal of paper records
- Lost or stolen backup tape

attack can be financially crippling. According to an annual FBI Computer Security Institute cyber crime study, the theft of personal information cost organizations an average of about \$710,000 per incident.

ACT FAST TO STOP THE FLOW OF DATA

Typically, organizations learn about a breach from a credit card company, bank, business partner, the victims or a lawyer rather than discovering it on their own. The organization must react immediately, carefully following its breach incident response plan and determining the nature of the problem. Outside forensic computer investigators and lawyers should be alerted and told to await further instructions. The network will need to be restored in a timely manner, as revenue may be hemorrhaging with each hour of lost network operations.

Meanwhile, additional support, such as a public relations specialist should be on standby, waiting to help with news media inquiries triggered by customer complaints.

Any failure to take the necessary and industry-recognized measures to secure personal data with prudent and reasonable safeguards—or to mitigate the future chance of harm to victims in a timely manner after the bad event occurs—can result in significant financial costs.

There are many federal and state regulations that govern and often require organizations to deploy

reasonable data security and privacy measures to safeguard nonpublic information.

State or federal agencies are constantly responding to the evolving risk environment, with proposed legislation that potentially governs how personal information should be protected and how victims should be alerted, making it difficult for organizations to keep up with legal standards and compliance duties. Meanwhile, many of these laws are being cited as a standard of care by plaintiff counsel in class-action litigation.

SPECIALTY COVERAGE FOR A SPECIALTY RISK

MOST PROPERTY/CASUALTY POLICIES OFFER LITTLE PROTECTION

The regulatory environment for safeguarding privacy is evolving as industries rely more on electronic networks and data, making cyber risk insurance a vital need for companies.

In a recent survey of middle-market company senior executives who are responsible for insurance about their interest and awareness of coverage for cyber risks, Betterley Risk Consultants Inc. found that approximately one-third already buy cyber risk and privacy insurance and another 25% plan to buy it in the next 18 months.

However, risk managers often were unaware of all the insurers that offer such coverage. For a list of major cyber risk insurers and their product offerings and contact information, purchase the full version of the this white paper at www.BusinessInsurance.com/whitepapers.

Too often, entities that are judged by Wall Street, shareholders and customers are underinsured against network risks and pay attention only after a breach. Compounding this problem is misinformation: Many organizations think their property, commercial general liability, errors and omissions, fidelity/crime and employment practices liability insurance also covers their cyber risks. However, this typically is not the case.

Cyber risk insurance addresses the unique risk exposures associated with electronic processes, privacy policies and interactions with data arising from computer-dependent business activities. One may argue that almost every business, regardless of the product or service it provides, has some exposure to cyber risks, such as unauthorized access to data from internal or external sources, computer viruses, denial-of-service attacks, staff mistakes and poor network management.

When considering whether to buy cyber risk insurance, keep in mind that privacy liability insurance underwriters may not put much merit in a one-time “clean” network vulnerability scan or a past payment card industry audit if there is no formal plan, policy and evidence of

ongoing efforts to ensure the consistency and safety of data. Regular updates of the software that runs and protects computer systems is essential to keep hackers at bay.

The cyber risk insurance underwriters want to know that the applicant has a corporate culture that takes data security and privacy 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, from new employee training to handling sensitive customer data.

The more documentation a company can provide to prove they “walk the walk,” the more significant premium discounts and broader network risk coverage options they will have.

When considering applications, insurers examine whether an organization’s data security and privacy practices are prudent and reasonable. This typically is demonstrated by a third-party cyber risk assessment, which serves as a loss-control process. The goal is for the organization to demonstrate that they have the capabilities to broadly protect data confidentiality, data integrity and system availability.

Cyber risk assessments also can serve another key purpose: When a data breach occurs, a company may find itself faced with a class action lawsuit due to perceived negligence in safeguarding customer information. When dealing with a plaintiffs lawyer, judge and jury, it can be helpful to demonstrate that the organization used due care to proactively protect its customers’ sensitive information—and that it had reasonable security measures in place at the time of the breach.

In the end, a cyber risk assessment should enable an organization to identify and address security flaws and then showcase its proactive security and privacy posture, which can bolster a future legal defense.

DEVELOPING LAYERED SAFEGUARD CONTROLS

MEDIEVAL THINKING CAN HELP PROTECT MODERN TECHNOLOGY

Because there's no way to completely prevent a security breach, preparation for a future event can be a vital part of a business' cyber risk management strategy.

Consider the medieval castle, which used moats, decoys, tall walls, hidden passages, and so on to keep intruders at bay—a "layered security" approach. Security practitioners use the moat metaphor to describe ways to protect corporate network-based assets. Today we use human and technical controls such as firewalls, unique network topographical designs, passwords, intrusion detection, mirror sites, backup servers, security and event logs, virus protection and encryption. In this way, modern practitioners use layered security to partition, add redundancy and disguise network resources and information.

Keep in mind that most companies are not necessarily "risk-averse" but "loss-averse." There always will be residual risk. It's a matter of whether your company can afford to absorb the resulting cost. Even with layered controls, solid people and generous security budgets, even the best companies get hit. Included are some weak spots that are common across many organizations, regardless of size or sector.

Cyber damage has characteristics similar to environmental pollution damage: It's rife with latent impact and hidden dynamics of cause and effect, and the long-term exposure can be devastating.

For this reason, insurance companies and insured enterprises must take proactive steps to clarify the extent of cyber insurance coverage. They also must track network incidents continuously. When the insured files a

claim, there must be a process for investigation and remediation using state-of-the-art forensics.

Claims submitted for network and data losses will require risk managers and claims departments to use the services of a forensic computer specialist to help remediate damage and confirm facts surrounding a "loss." Essentially, this is the technical expert who can help claims adjusters or legal counsel ascertain the specific who, what, when, where and how of a claim.

Some forensic service vendors also can assist with data recovery and restoration. Computer forensics involves preserving, identifying, extracting and documenting computer evidence stored in the form of magnetically encoded information or data. These specialists investigate and examine computer hardware and software, including e-mail trails, using legal procedures to obtain evidence that proves or disproves allegations, which include a cyber-based insurance claim. Part of the investigation is an audit involving forensic analysis, backward tracing, attack route hypothesis and possibly attack re-creation.

In this risk-centric climate, organizations are thinking hard about how to prepare for data breaches and all of their attendant risks. The best preparation starts by acknowledging the complexity of these events and organizing legal resources, applying safeguard controls and choosing insurance protection accordingly.

If there is any certainty in this arena, it's that no two cyber claims are the same: In every case, on the attacker side we see different skills, motives and exploits; on the organization side, we see a unique cross section of safeguards (or lack thereof), affected systems and data loss.



NetDiligence
Cyber Risk Management & Information Security Services

www.netdiligence.com

Mark Greisiger is president of Network Standard Corp., which does business as NetDiligence, a Philadelphia-based firm that provides cyber risk assessment services for chief financial officers and risk managers to help assess whether their organizations deploy reasonable and prudent safeguards to mitigate data breach losses and liability risk. Since 2001, NetDiligence services have been used by insurers in the United States and the United Kingdom that offer data and privacy risk insurance products, providing loss control services to their insured business clients. Prior to starting NetDiligence, Mr. Greisiger worked for more than a decade directly in the insurance industry where he developed and underwrote a 'hacker insurance' product.

Elisa Ludwig, a freelance writer based in Philadelphia, helped write this white paper.

The full 33 page version of the this white paper is available for purchase at www.BusinessInsurance.com/whitepapers