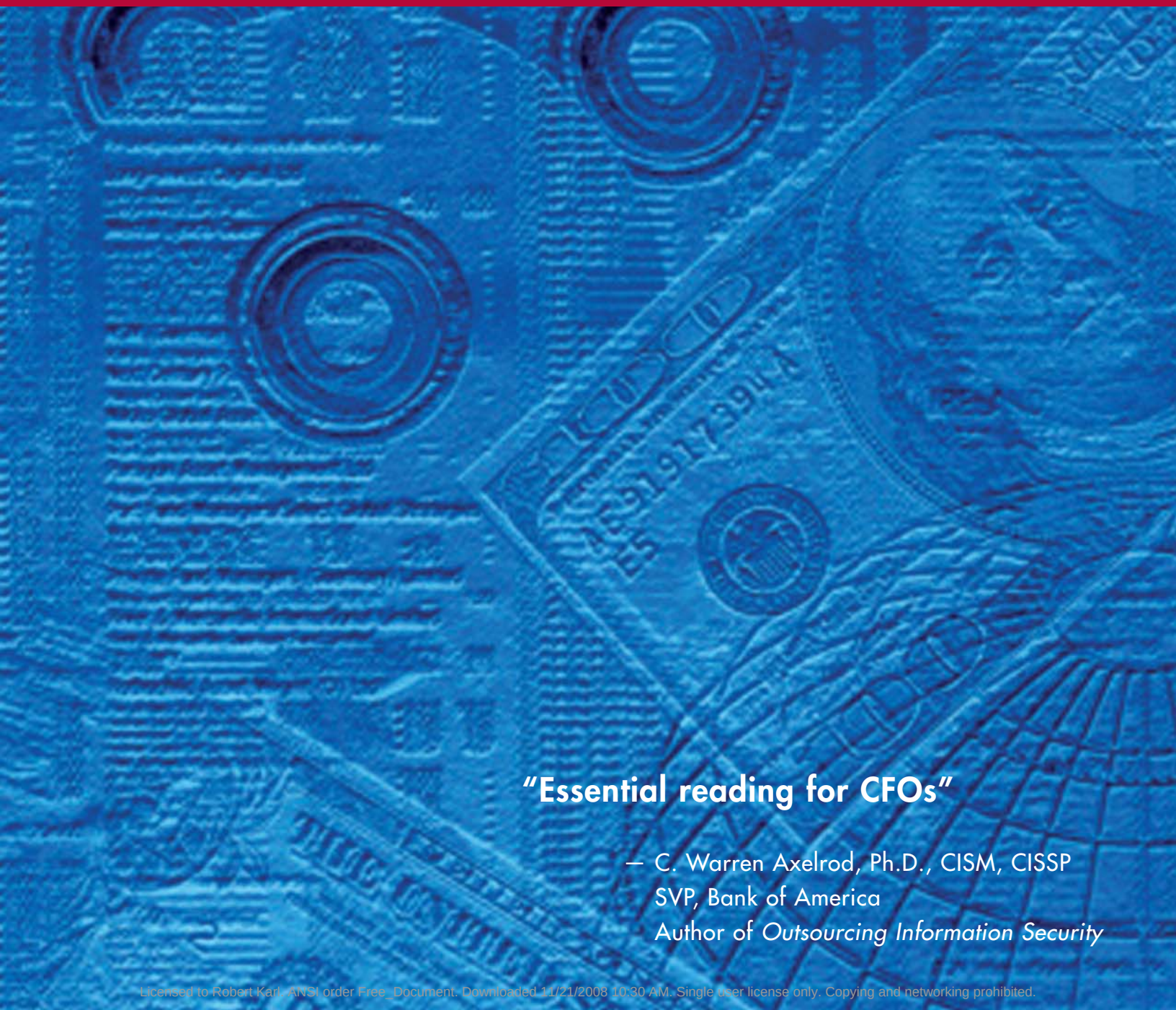
ANSI
American National Standards Institute

INTERNET SECURITY ALLIANCE

THE FINANCIAL IMPACT OF CYBER RISK

50 QUESTIONS EVERY CFO SHOULD ASK



"Essential reading for CFOs"

— C. Warren Axelrod, Ph.D., CISM, CISSP
SVP, Bank of America
Author of *Outsourcing Information Security*

Material in this publication is for educational purposes. Neither the publisher nor the authors assume any liability for any errors or omissions or for how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. For legal advice or any other, please consult your personal lawyer or the appropriate professional.

The views expressed by the individuals in this publication do not necessarily reflect the views shared by the companies they are employed by (or the companies mentioned in this publication). The employment status and affiliations of authors with the companies referenced are subject to change.

TABLE OF CONTENTS

APPENDICES

ACKNOWLEDGEMENTS

The following professionals participated in one or more of the ANSI-ISA sponsored workshop meetings. The views expressed in this document are those of the individual Workshop participants and do not necessarily reflect the views of the companies and organizations listed.

American International Group	Richard Billson*, Nancy Callahan*, Paul de Graaff*, Robert Roche*, Ty R. Sagalow†
American National Standards Institute	Jessica Carl*, Matt Deane*
Aon	Patrick Donnelly*
Beazley Group plc	Bob Wice*
Booz Allen Hamilton	Will Robinson*
CNA Insurance	John Wurzler*
Carnegie Mellon University — Software Engineering Institute	David White
Crimson Security	Narender Mangalam
Direct Computer Resources, Inc.	Ed Stull*
Ernst & Young LLP	Jennifer Celender*, Seth Rosensweig*
Guy Carpenter	Harry Oellrich*
Hunton & Williams	Lon Berk*
IBM Tivoli Software	Eric McNeil*
ID Experts	Christine Arevalo*, Rick Kam*, Jason Porter
Internet Security Alliance	Barry Foer*, Larry Clinton*
KPMG LLP	Neil Bryden, Cole Emerson*
Lockheed Martin Corporation	Ben Halpert*
Marsh, USA	Nadia Hoyte*, Robert Parisi*
Moody's Risk Services	Edward Leppert*
New York Metro InfraGard	Joseph Concannon*, Phil Froehlich*, Vincent Orrico*
Quality Plus Engineering	Greg Hutchins*
Reed Elsevier	Arnold Felberbaum*
Robinson Lerer & Montgomery	Anne Granfield*, Michael Gross*
State Farm Insurance	Bob Hillmer*
U.S. Cyber Consequences Unit	Scott Borg*
U.S. Department of Commerce	Michael Castagna*
U.S. Department of Justice	Martin Burkhouse*
U.S. Department of Homeland Security	
Office of Infrastructure Protection	Chris Watson*
Science & Technology Directorate	Peter Shebell*
University of California, Berkeley	Aaron Burstein*
Willis	Tom Srail*

* Task Group Participant † Workshop Leader

Thanks and acknowledgement are given for the support and participation of all the organizations that supplied experts to this initiative. Without the contributions from these individuals and their collective expertise, particularly those that participated on the Workshop task groups, this final deliverable would not have been possible.

- Special acknowledgement and appreciation is given to **Ty R. Sagalow** of **American International Group** (AIG) for being the Workshop Leader of this initiative. Mr. Sagalow's leadership and dedication in helping to shape the initiative, lead its proceedings, and build consensus for the final deliverable was instrumental in reaching a successful outcome. Thanks also to **Richard Billson** of AIG for his added support in this regard.

- Appreciation is given to the **American National Standards Institute** (ANSI) and the **Internet Security Alliance** (ISA) for the effective project management that kept this initiative on track and allowed for a successful delivery of the final publication in a timely manner, particularly **Matt Deane** and **Jessica Carl** of ANSI and **Larry Clinton** and **Barry Foer** of ISA.

- Special acknowledgement is given to **American International Group** (AIG) for hosting and sponsoring the first two Workshop meetings, the **American National Standards Institute** (ANSI) for hosting the final meeting, and to **Direct Computer Resources, Inc.** for sponsoring the final meeting.

- Thank you to the following special advisors for their review and insightful comments on the advance proof copy which contributed to the final version presented here.

  Regan Adams, Vice President and Assistant General Counsel in the Contracts, Privacy & IP Legal group, Goldman Sachs
  C. Warren Axelrod, SVP, Privacy and Security, Bank of America
  Lawrence Berk, President and CEO, Baron Group, USA
  Joe Buonomo, President and CEO, Direct Computer Resources, Inc.
  George Carruthers, Chief Financial Officer, LoneStar National Bank
  Phillip Chappo, First Vice President and Acting CFO, Credit Industriel et Commercial
  Richard Davis, Chief Financial Officer, The George Washington University Hospital
  Robert Gardner, Founding Partner, New World Technology Partners

- Thank you to **Ed Stull**, sponsored by Direct Computer Resources, Inc., for leading this special advisor review effort and for providing the consolidated and insightful feedback to the Workshop leaders.

- Finally, thank you to **U.S. Department of Homeland Security Assistant Secretary for Cyber Security and Communications Greg Garcia** for his support in framing this Workshop and for the continued efforts of his program in furthering cyber security preparedness within our nation.

INTRODUCTION

Cyber security[1] is vital to America's economic well-being. Its importance was underscored in 2008 by U.S. Homeland Security Secretary Michael Chertoff, who named it one of the nation's four priority security issues, alongside border security.

Corporations use cyber systems to accomplish real-time tracking of supply chains, manage inventory, improve employee efficiency, generate on-line commerce, and more. Virtually every corporation has, by now, calculated the positive aspects of digitalization into its immediate and long-term business plans.

Unfortunately, corporations have often failed to properly account for the financial downside resulting from the risks of cyber systems.

Corporate America cannot be completely faulted for this deficiency, since to date there has not been any *agreed upon* methodology for understanding and mitigating the potential *financial losses* associated with network security and cyber risk. The classic financial risk management discipline that Chief Financial Officers and Risk Managers use to deal with brick-and-mortar risks has not been systematically applied to digital risks. While there is a substantial body of work dealing with the *technical* standards of network, internet and computer system security and plenty of attention has been paid to important issues such as data encryption and best-in-class security technologies, *classic financial risk management*— as it pertains to cyber security exposures—has been largely overlooked.

The purpose of this work is to correct that deficiency by providing guidance in both the identification and quantification of the financial risk due to issues related to information security.[2]

Thanks to the joint effort organized by the American National Standards Institute's (ANSI) Homeland Security Standards Panel (HSSP) and the Internet Security Alliance (ISA), with input provided by the many industry and public sector professionals who contributed their time and energy, the work represents an Action Guide that private sector enterprises can undertake to assess and address the financial exposure of cyber security from all angles. It is a tool the CFO — and often other executives — can use to build a framework for analyzing, managing and transferring the Net Financial Risk (defined below) of cyber security. As opposed to focusing on technological standards or even best practices, this guide is presented to further advance the understanding of financial management.

1 Cyber security might be defined as the protection of any computer system, software program and data against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. Cyber security attacks can come from internal networks, the internet or other private or public systems.

2 Throughout this work, the terms "cyber security," "network security" or "information security" may be used interchangeably.

A frightening fact every CFO must face is that the financial consequences of cyber security, or more pointedly, of cyber security "events" can be substantial. The total average costs of a data breach grew to $197 per record compromised in 2007.[3] Since January 2005, the Privacy Rights Clearinghouse has identified more than 230 million records of U.S. residents that have been exposed due to security breaches.[4] Costs have increased in terms of lost business, legal defense and public relations.[5] An organization that is unprepared to avert or manage a data breach can suffer severe financial losses and irreparable damage to its reputation and customer base. Conversely, when an organization is prepared and responds skillfully to a cyber threat, the crisis can go down in history as an event that cements customer loyalty and a positive brand image.

The key to understanding the financial risks of cyber security is to fully embrace its multi-disciplinary nature. Cyber risk is not just a "technical problem" to be solved by the company's Chief Technology Officer. Nor is it just a "legal problem" to be handed over to the company's Chief Legal Counsel; a "customer relationship problem" to be solved by the company's communications director; a "compliance issue" for the regulatory guru; or a "crisis management" problem. Rather, it is all of these and more.

To successfully analyze and manage financial risk requires a dialogue, sparked by a series of pointed questions directed at the major stakeholders in all corporate domains: the Chief Legal Counsel, Chief Technology Officer, Chief Risk Officer, heads of Corporate Communications, Investor Relations and Customer Service. Each of these individuals should be "in the room" with a surprised CFO finding that individuals with different positions in the company giving very different, sometimes contrary, advice to the same question. Of course, the foregoing list is not intended to be exhaustive and, depending on the enterprise in question, may need to include other stakeholders. For example, the head of Human Resources might be given a seat in the room given the correlation between the management and training of employees and the potential for internal cyber attacks.[6]

This Action Guide provides a practical, immediately actionable guide on how to bring the multiple stakeholders in cyber security together and give them, in the form of strategic questions, a roadmap for developing a multi-disciplinary risk management approach to analyze, manage and mitigate the financial risks of cyber security. The answers to these questions will better enable a company's CFO to determine the company's "Net Financial Risk."

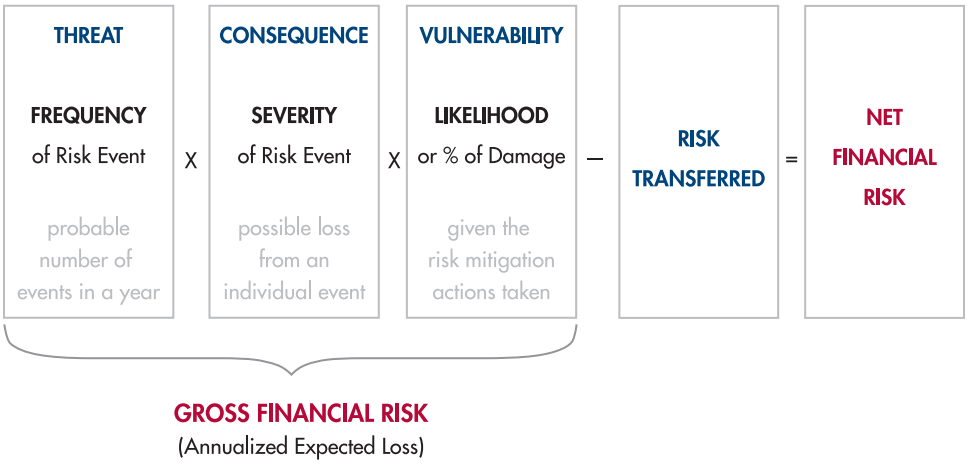
3 2007 Annual Study: U.S. Cost of a Data Breach. Benchmark research conducted by Ponemon Institute, LLC ("Ponemon Study").

4 Organization such as the Privacy Rights Clearinghouse and Attrition track and publish information on data breaches. For more information visit www.privacyrights.org and www.attrition.org.

5 Ponemon Study, pages 2-3.

6 The term "cyber attack" is meant to be broadly understood to include both external and internal attacks whether launched intentionally or unintentionally. Recent studies continue to indicate that internal attacks are generally more frequent than external ones.

Net Financial Risk can be expressed as follows:



As companies go through the questions posed in this work, they will find the answers can be plugged into the above formula, enabling them to better quantify their own net cyber risk. However, it is important to understand that the quantitative evaluation of these factors (Threat, Consequences, and Vulnerability) must be qualified by the degree of *confidence* the organization has in the accuracy of each factor. In other words, in addition to the probability of loss, there is the probability of the estimate of the probability of loss being accurate. Once the risk equation has been qualified by the degree of confidence, it provides a sound basis for guiding all risk management decisions.

In addition, several useful charts are included in the Appendices that can be customized to help measure the Net Financial Risk of a company, together with lists of helpful web sites and technical standards.

In each of the chapters that follow, it is generally the CFO who is envisioned to be asking the questions. Yet this Action Guide is also of direct benefit to all of the aforementioned stakeholders, all of whom should be "in the room" when the questions are asked … to provide the answers, to listen to the answers, and to act on them.

For each enterprise, individual answers may be different. Routes will vary, yet the destination for all private sector enterprises embarking on this cyber risk management methodology is a common one: an immediately actionable understanding of the Net Financial Risk of cyber security through which the CFO, with the executive team, can make informed decisions about which "risk management actions" (if any) are to be implemented.

Let the process, and the preparation, wait no longer.

Gather the stakeholders.

Let the questions begin.

CHAPTER 1
KEY QUESTIONS FOR YOUR CHIEF LEGAL COUNSEL

A company's cyber risk can result in numerous legal and regulatory problems. Companies generally have legal responsibilities arising from business and contractual relationships and regulatory oversight. Such responsibilities can in some circumstances result in civil and criminal claims as well as regulatory investigations and sanctions.

Analyzing legal exposures for cyber security requires a multi-jurisdictional review of the company's obligations with care taken to evaluate the impact of different jurisdictions in which the company does business. Both the regulatory environment and the data privacy rules that apply to cyber communications must be examined in each jurisdiction in which the company does business. Exposures that should be considered include potential liabilities relating to the loss of trade secrets, intellectual property, breach of contract, as well as violations of privacy. If companies do not properly manage these exposures, they may find themselves facing the high costs of criminal and civil investigations, as well as civil class actions.

At the same time, appropriate steps can mitigate financial risk relating to cyber security. Companies modify their vendor contracts, for example, to obtain indemnification rights and to require vendors to purchase specific cyber insurance. Additionally, law enforcement and other governmental authorities may provide support, and contacts with relevant agencies should be part of a company's legal review of its cyber exposures.

To flesh out such issues, the following questions should be put to the company's Chief Legal Counsel:

1.1 Have we analyzed our cyber liabilities?

There are numerous aspects of liability that can arise from breaches of cyber security. Failure to maintain adequate network security can lead to allegations of violations of contractual responsibilities, negligence or violation of regulatory requirements. Loss of data and denial of service, for instance, may lead to claims by customers and business partners. Ultimately, such failures could also lead to mismanagement claims by shareholders or other company stakeholders.

1.2 What legal rules apply to the information that we maintain or that is kept by vendors, partners and other third parties?

With the wealth of personally identifiable information (PII) kept by companies regarding its employees, customers and others, companies need to take adequate steps to protect it from disclosure. Companies doing business in multiple jurisdictions may be subject to competing regulations from different authorities. Information such as social security numbers, health insurance, driver's license identifiers and contact information are

KEY RESULTS

Understand your exposure to civil litigation as well as regulatory investigations.

Protect intellectual property and customer/employee personal information.

Comply with the laws and regulations in all countries in which your company operates.

Understand how to transfer the risks of cyber liability using customer and vendor contracts and insurance.

protected by different rules and regulations, and different authorities. Nearly every state requires companies to notify individuals who are identifiable through this data if it is obtained by unauthorized parties—often without regard to whether the company accidentally disclosed the data or suffered a deliberate cyber attack. Notification itself is costly and, if not executed properly, may lead to class action lawsuits and government investigations.

Cyber security breaches may need to be reported for other reasons as well. If a publicly-traded company suffers a breach that has a material impact on the company's financial position, the company may be required under federal securities laws to report it. Some key U.S. statutes impacting cyber liabilities include:

- Communications Act of 1934, updated 1996
- Computer Fraud & Abuse Act of 1984
- Computer Security Act of 1987
- Economic Espionage Act of 1996
- Electronic Communications Privacy Act of 1986
- Federal Privacy Act of 1974
- Gramm-Leach-Bliley Act of 1999 (Financial Institutions)
- Health Insurance Portability & Accountability Act (Healthcare Organizations) of 1996
- National Information Infrastructure Protection Act of 1996
- U.S.A. Patriot Act of 2001

1.3 Have we assessed the potential that we might be named in class action lawsuits?

Release of PII not protected by reasonable security can cause high-risk litigation. Although individual damage claims may be small or difficult to prove, consolidation of multiple claims through national class actions can expose a company to substantial risks and legal expenses. Federal e-discovery rules (which govern the discovery in such cases) can make defending these suits especially costly.

1.4 Have we assessed the potential for shareholder suits?

Failures of network security—whether leading to breakdown of computer systems needed to conduct business operations or the release of electronically-stored information, including trade secrets and intellectual property—could lead to shareholder actions alleging mismanagement. Drops in stock price can trigger non-disclosure allegations and shareholder class actions. Such actions can be among the most expensive litigation faced by publicly-traded companies. Even privately-held companies can suffer lawsuits from their shareholders. A wide variety of laws—Sarbanes-Oxley, for example, as well as sector-specific laws (HIPAA, Gramm-Leach-Bliley, Fair Credit Reporting Act, etc.) and associated regulations—require companies to take "reasonable" or "appropriate" steps to protect PII. These laws generally do not provide more specific requirements, but becoming familiar with industry practices and seeking additional guidance from the relevant regulatory agencies can give more specific meaning to these broad standards.

1.5 Have we assessed our legal exposure to governmental investigations?

The inadvertent release of confidential, electronically-stored information can result in expensive governmental investigations—both civil and criminal. Certain agencies, such as the Federal Trade Commission (FTC), have authority to investigate whether PII is adequately protected by companies in certain businesses and whether those practices are consistent with privacy policies or terms of service. In addition to fines, the costs of legal counsel, expert consultants and diverting employees from their primary responsibilities must be considered as part of the cost of a government investigation. Outside the area of data theft, specific industries, such as financial institutions and healthcare, have specific, security-related regulatory obligations.

1.6 Have we assessed our exposure to suits by our customers and suppliers?

Cyber attacks can cause short- and long-term business interruptions. Even if a "denial of service" attack renders a company's website or other online resources useless for only moments, it may result in a long-term loss of customers and interfere with contractual obligations to business partners. Outside of a network shutdown, cyber attacks can result in the theft or inadvertent disclosure of trade secrets and other confidential business information. In addition to seriously harming an enterprise's ability to compete and the loss of reputation and trust, suppliers and customers may rely upon the company to maintain and protect such data. Accordingly, contracts with business partners, as well as agreements with customers, should be examined to determine the company's rights and responsibilities under these circumstances.

1.7 Have we protected our company in contracts with vendors?

Contracts with vendors and other third parties can impose obligations on those parties to protect such information and provide the company with recourse in the event of a breach. Vendors may be required to warrant that company data is appropriately protected and to indemnify the company for losses arising from cyber security events that are the fault of the vendor. Furthermore, vendor contracts may contain requirements to purchase network security insurance, which typically indicates that a third party has thoroughly evaluated the vendor's systems and funds damages the vendor may owe the company.

1.8 What laws apply in different states and countries in which we conduct business?

Different nations impose different requirements on a company's business activities. Jurisdictions vary even in what they consider acceptable web content. With respect to data protection, jurisdictional differences may be dramatic. European Union countries, for example, generally have stricter data privacy standards than the United States; data transfers to and from these jurisdictions may be affected. Conversely, some nations have more active data monitoring than others. The People's Republic of China, for instance, may very well monitor intensively the internet traffic passing through its borders. Border searches of laptop computers and PDAs pose another threat. Companies that transfer trade secrets across borders via networks or physical devices may find those secrets in government hands, not only risking their ability to earn future profits but also subjecting themselves and their directors to shareholder suits.

Within the United States, state laws vary in their definitions of the events that trigger an obligation to report a data security breach, the required reporting method and the penalties for failing to give notice.

1.9 Have we assessed our exposure to theft of our trade secrets?

Some of a company's most important assets are its trade secrets. Trade secrets are often held in electronic or digital form and are subject to misappropriation through a cyber attack. Unlike theft of physical assets, a theft of digital assets leaves behind the asset stolen. It is more fairly considered a copying of the asset, which makes the theft that much more difficult to discover.

1.10 What can we do to mitigate our legal exposure and how often do we conduct an analysis of it?

Taking affirmative steps to bring a company's information systems into compliance with applicable laws and regulations can reduce the risk of legally-actionable security breaches.

- Conduct a comprehensive review of the laws and regulations applicable to the company's business operations.
- Ensure that procedures and processes are in place to quickly advise customers and other third parties of a theft of PII consistent with state and foreign law.
- Review the company's contracts with customers and suppliers to reduce the legal exposure to these third parties in the event of a breach, including use of liquidated damage clauses, where appropriate.
- Review company contracts with vendors to determine whether greater protection from these business partners, such as indemnification in the event of a breach, is advisable. In addition, these contracts may require the third party to purchase a specific level of cyber security insurance.
- Review procedures designed to minimize e-discovery costs if litigation does occur.
- Review the company's privacy policy to ensure that it is consistent with applicable law and that procedures are in place to adhere to its obligations.
- Bear in mind that, like the threats a company faces, cyber security laws and regulations change constantly. It is important to stay abreast of (and in compliance with) state, national, and international developments, which requires coordination among different parts of the company. Doing so not only mitigates exposure to potentially serious legal risks but also may make the company aware of legal rights and remedies that can reduce its financial risk.

CHAPTER 2
KEY QUESTIONS FOR YOUR COMPLIANCE OFFICER

Cyber security events have a direct and indirect financial, strategic and operational impact as companies deal with how to effectively identify, manage and lower their risk profile and cyber threats amidst a growing number of regulations. First and foremost, a company must have a complete understanding of all applicable regulations. Second, a company needs to understand and have in place the security measures and protections required by those regulations. A company cannot claim that it was unaware it had to comply with applicable regulations. A responsible business will have a clear understanding of the appropriate regulations, have identified where the applicable data resides, a security plan in place to protect the data and the network as a whole, and appropriate monitoring to ensure compliance.

As a follow-up to the questions in preceding section, the following key questions should be put to the company's Chief Compliance Officer or Chief Privacy Officer:

2.1 Have we inventoried what regulations we must comply with?

Companies must be thinking both locally and globally with regard to regulations. The inventory of regulations that the company needs to comply with forms the framework of a risk-based action plan to help make decisions on what to do with regulated data. The company needs to consider where business is transacted, where data is stored and where regulated data may travel.

2.2 Do we understand what regulated data we have, where it exists and in what format?

A risk-based approach is a prudent first step. Based on the company profile, lines of business (e.g., health companies with personally identifiable information (PII)), and regulated product lines, companies should, in combination with the inventory referred to in 2.1, assess where data resides and who has the ability to access this data.

2.3 Are there valid business reasons for collecting the data, if not required by regulations?

In some cases, companies collect PII for business reasons that have nothing to do with compliance requirements. There is, of course, nothing wrong with this. However, it is imperative that the company understand these reasons and formulate a strategy to either keep and protect, or destroy the data. For example, if the cost of keeping and securing the data far outweighs the business reason for keeping it, a company might rethink whether it wishes to keep the data.

2.4 How do we track and monitor compliance on an ongoing basis?

If an incident happens, it is important that a company can demonstrate that it had policies and procedures for not only protecting data but for monitoring and tracking compliance.

KEY RESULTS

Maintain a "living" inventory of all applicable regulations.

Establish controls to protect data and test the controls regularly.

Put appropriate monitoring in place.

Particularly important are identity and access management for individuals and business processes, as well as visible audit trails and self-reporting of control effectiveness. Without a program, a company leaves itself open to further regulatory scrutiny. Additionally, a company should have a program in place to track new regulatory requirements and changes to existing ones.

2.5 Do we have regulatory risk with vendors / companies we do business with?

All vendors need to be considered when thinking through regulatory risk as more and more companies outsource key processes and data. A vendor risk program should be implemented.

2.6 Are all of our procedures and policies with respect to our regulatory obligations documented?

A company must know the operating procedures to be followed in the aftermath of a cyber security event and employees must be trained to handle such conditions. In a regulatory investigation, interested parties would first look to see documented procedures.

2.7 Are there (regulatory) requirements we can or have considered opting out of?

In extreme cases it might make sense to terminate a business or change a business model in order to "opt out" of a regulation if the benefits of the business are outweighed by the costs of compliance. In recent times, for example, some public companies have decided to go private in order to release themselves from the securities and disclosure regulations required of publicly-traded companies.

2.8 Are there processes and procedures in place regarding data retention and data destruction?

Data retention is a risk that businesses face, as in some cases data is not retained for an appropriate length of time, and in others it is retained for longer than is required by law. Care should be taken to ensure that any data which is required to be destroyed is in fact removed from all systems in which the data resides.

2.9 Does the organization have processes to review and update privacy policies and disclaimers to customers?

It is important that the company consider having processes in place to accommodate "opt-in/out" and "do not call" requirements. Companies put themselves at risk when they are not continuously reviewing, updating and monitoring their privacy policies. Not being compliant can lead to significant direct cost to the company.

2.10 Are we complying with what our privacy policy says?

Privacy policies are often the main way that companies tell customers about how they retain and use PII. In recent years the FTC and state attorneys general have brought a number of actions for unfair or deceptive practices against companies that collected PII in a manner inconsistent with their stated policies, or that failed to provide reasonable protection for customers' PII. Many of these actions have resulted in fines, agency oversight, or both.

CHAPTER 3

KEY QUESTIONS FOR YOUR BUSINESS OPERATIONS AND TECHNOLOGY TEAMS

The machinery of modern industry is business operations, including the technology, security and recovery processes. For things to function properly, gauges, mechanics and planned alternatives are still needed when things go wrong. These requirements are often addressed to the Chief Technology Officer (CTO), Chief Security Officer (CSO), Chief Information Security Officer (CISO) and the Disaster Planning/Business Continuity Planning (DR/BCP) groups.

The CSO/CISO and/or the CTO should be able to address the issues below. However, prior to asking these questions, it is important to know which aspects of the business (confidentiality of data, availability of systems, and integrity of data) are important to the bottom line. Once this is understood, the questions can be asked with the understanding that answers may need further research and may require more detailed questions to be asked of the technical staff in order to provide a full response.

KEY RESULTS

Analyze the confidentiality, integrity and availability of your data and systems.

Assess physical security and vendor/service provider risk exposure.

Re-evaluate, constantly and consistently, technical exposures.

3.1 What is our biggest single vulnerability from a technology or security point of view?

Consider what is the worst thing that can actually go wrong. Given the kind of attackers of concern, and their probable skill levels, determine how likely they are to succeed and, if successful, what type of damage will be caused. In reality, most corporations will not have a single vulnerability of major concern, but many. However, no data about the numbers of cyber attacks or their success rates are meaningful, unless the kinds of attacks and the skill levels of the attackers are known. The key is to apply the appropriate metrics to estimate how well a company is doing from a security standpoint. For example, the number of hours per year a company's systems are down due to cyber attacks may be the wrong measurement, since many kinds of destruction can only be carried out when systems are up and running.

3.2 How vulnerable are we to attack on the *confidentiality*, *integrity* and *availability* of our data and systems?

There is usually *confidential* information that a company does not want in the hands of its competitors or the public, from secret sauces and internal culture to private data of executives and employees. Without proper controls, a company's competitive advantage or at least the trust of its customers and employees is likely at risk.

Often the importance of the *integrity*, (i.e. the accuracy) of a company's data is overlooked. Purchase orders must be accurate, customer lists and, of course, financial data must be accurate. If controls are not in place, malicious or accidental changes could be problematic and could be very costly in terms of product recalls, safety issues, fraud, class action suits or other regulatory/industry impacts.

Availability of systems is critical. If a company's systems are unavailable, the impact to its customers, employees, business partners and providers could be immense. While business continuity plans are an essential part of the response, they are a reactive measure. Taking a pro-active approach will reduce a company's risks of needing to activate its DR/BCP plans and increase the chances of a recovery.

3.3 If our system goes down, how long until we are back up and running and are there circumstances where we do NOT want to be back up quickly?

A company should attempt to estimate how many hours or days it would take until its operations would be back to normal under the different attack scenarios and how this downtime would impact the business. Understanding the duration of cyber attack effects can be trickier than understanding their immediate nature and costs, yet it is equally important. A modest loss of market share, due to a cyber attack, could be extremely expensive if it becomes a permanent loss. Achieving the goal of minimum downtime is an important measurement of security. However, equally important is the understanding that simply "getting the system back on" is not in many cases the correct action. If data or computer networks are compromised, putting the system back in production will almost always cause more harm than good.

3.4 Where do we stand with respect to any information security/technology frameworks or standards that apply to us? (See also Appendix E)

It is most likely that applicable frameworks or standards exist for every company. These frameworks and standards are effective in providing valuable information about where a company is positioned and where its risks are. A company needs to assess where it is and then determine its acceptance of that position and take action if needed. This process needs to be repeated periodically as technology and the global context are always evolving.

3.5 Do we have the proper staffing to reasonably maintain and safeguard our most important assets and processes?

A company should assess the appropriate staffing level and timeframe that should be dedicated to these efforts. There are strong strategic returns on these investments that are often overlooked.

3.6 What is the assessment of physical security controls at each of our sites (data center, home office, field offices, and other sites?)

Physical security assessments are often not performed frequently enough or not at ALL locations. Many risks of loss are easy to spot and address. Common sense approaches with regards to physical security can reap a huge reduction in risks to business operations and risks of data breach. These assessments must be done regularly with an implementation of lessons learned.

3.7. How prepared are our incident response and business continuity plans?

The consequences of a cyber attack can be greatly affected by the way the business consequences are managed after the cyber attack begins. Business continuity plans are vital to continued revenue and reputation. The plans should be formalized, tested and ready in case of a network security breach.

3.8 What is our risk exposure of technology or business operations failures at our vendors and service providers?

A company's security is only as good as that of the vendors and service providers on which they rely. Ideally, each of a company's service providers would go through a similar exercise as documented in this Action Guide, at least addressing the question about applicable security/technology frameworks and their maturity level. However, any assessment is better than nothing and having some visibility into these "extended" elements of a company's business operations is highly advisable. A company can never outsource responsibility to its customers.

3.9 What is the maturity of our information classification and management program?

Information management is a complex issue; often data is not classified, handled or disposed of when it is no longer needed. Poor information management is another key contributor to the largest breach events to date. Often the biggest challenge with data lifecycle is related to people and process rather than technology. Of particular importance are identity and access management for individuals and business processes, as well as visible audit trails and self-reporting of control effectiveness. Without proper awareness and education empowering a "human firewall," any technology solutions will be insufficient.

3.10 How often are we re-evaluating our technical exposures?

Just discovering the vulnerabilities in information systems that a company needs to know about at any one point in time is insufficient long-term protection. A company must also have a process which permits it to discover new vulnerabilities in an acceptable timeframe. The key factor is how much time a company has before a given kind of vulnerability is likely to be exploited. Some vulnerabilities are typically exploited within hours after they are posted on the internet. Others are not usually exploited for months. It is also important to know how often a company is overlooking or losing track of vulnerability. In a corporate environment of complex networks with many kinds of software, there is always going to be some system that is missing an upgrade, or has a known incompatibility, or is running in a default configuration when it should not be. Thus, prioritizing and monitoring the most vital systems become essential.

CHAPTER 4

KEY QUESTIONS FOR YOUR EXTERNAL COMMUNICATIONS AND CRISIS MANAGEMENT TEAMS

Cyber security events can significantly impact a company's relationship with a variety of stakeholders, including customers, employees, business partners and investors, as well as regulators and law enforcement officials. With today's 24-hour news cycle, where news of an event adverse to a company's reputation can appear on a cable news channel footer or a well-trafficked web site in moments, careful planning and expert execution is no longer a luxury. In the wake of a cyber security event, an effective communications strategy can materially minimize potential damage to a company's reputation, customer loyalty, employee morale, and, ultimately, shareholder value. A responsible business will have a formally documented communications plan in place to notify stakeholders and the media when appropriate, since the unfortunate reality is that even the best-protected companies cannot eliminate the real risk of a successful cyber attack resulting in a "crisis" to be managed.

A CFO should address the following questions to the heads of marketing, communications, public relations, investor relations, customer service, security, legal and compliance to assess an organization's ability to communicate effectively after a cyber security event.

4.1 Do we fully understand the overall financial impact of mishandling communications with our key stakeholders following a cyber security event?

Customers, employees, investors, business partners, regulators and other key stakeholders will lose confidence in an organization that does not communicate effectively in a crisis. This can have a direct impact on the bottom line – from lost revenues (and increased marketing expenses to recapture those revenues) to additional legal, compliance and public relations expenses, among others.

Conversely, a well-executed communications plan not only minimizes harm and potential legal liability but can actually enhance a company's overall reputation. For example, it is widely held that Johnson & Johnson's expert handling of the Tylenol scare, and the positive perception of Choicepoint's aggressive response when criminals accessed sensitive personal information, enhanced their respective reputations.

4.2 Have we evaluated the appropriate communication responses to our key stakeholders?

Different types of cyber security events require different types of communications responses – e.g., the theft of important confidential corporate information by a former employee would likely be handled quite differently than the loss or theft of thousands of employees' Social Security numbers.

In addition, certain types of events that impact individual safety or national security will demand timely outreach to law enforcement and others.

KEY RESULTS

Ensure a written crisis management plan is in place at all times and "road tested" regularly.

Identify all internal and external resources required to respond to key stakeholders following a cyber security event.

Budget in advance for the communications and crisis expenses required which are in addition to the usually anticipated legal and technical expenses associated with cyber security events.

In most scenarios, a critical communications task will be crafting and delivering messages about *how* the incident happened, *what steps are being taken* to help individuals or others affected, and *what is being done* to prevent a re-occurrence. This all must be carefully coordinated with, and vetted by, legal counsel.

4.3 Do we have a documented, proactive crisis communications plan?

A robust communications plan requires thoughtful consideration of who should be notified and how, and whether or not the company should offer a compensating benefit to the affected individuals or businesses to offset any inconvenience or damage caused by the event.

Notification to key regulatory bodies is mandated in some circumstances (unless it might impede a criminal investigation), and is an important courtesy in others.

The communications plan should anticipate the potential for aggressive media attention 24/7. It should prepare for responding to media inquiries in a manner that delivers a clear message to parties affected directly or indirectly, as well as to other key stakeholders.

The plan should also anticipate providing services to help those who have been affected to obtain additional information and recommendations to minimize potential harm.

A crisis communications plan is NOT an incident response plan. The former is crafted by a company's communications and crisis management experts while the latter is crafted by the company's business continuity and network security experts.

4.4 Have we identified and trained all of the internal resources required to execute the communications plan?

Considerable internal resources will be required to reduce the financial impact of a cyber security event, perhaps for a significant period of time, triggering incremental costs and potentially distracting management attention from running the business.

In addition to a careful outlining of roles and responsibilities, decision-making authority should be explicitly assigned to avoid potential delay, confusion or conflict. All company personnel who are part of the response team should be adequately prepared (for example, by media training) to communicate effectively.

The company spokesperson should be as knowledgeable as possible about security issues. Legal counsel should be prepared to carefully review the method and content of any communications in order to identify any potential issues.

4.5 Do we have a template timeline for executing the communications plan?

A timeline, and a process for establishing it, is a critical tool for managing the conflicting and pressing demands of law enforcement, regulators, consumers, business partners and media, as well as internal functions such as marketing, customer services, IT and physical security, legal and compliance.

It is important to anticipate the needs and manage the expectations of each group, which is very difficult to do without a realistic and comprehensive timeline.

4.6 Do we have contacts at specialist crisis communications firms if we need their services?

In addition to identifying the internal response team, some companies have planned for cyber security events by pre-selecting external service providers for legal, public relations and notification activities, as well as pre-selecting compensatory packages for affected populations.

This makes sense for a number of reasons, for example:

- there may be a need to communicate simultaneously with multiple populations; or
- some communications may be better handled by an independent third party.

Attributes of an appropriate crisis communications firm would include deep knowledge of the relevant industry, experience in handling the type of events and constituents anticipated by the plan, and the ability to speak to the media on the company's behalf, as necessary.

4.7 In the case of a cyber security event involving personally identifiable information (PII), do we have a system in place to quickly determine who should be notified, and how?

Because many state, federal and foreign regulators require prompt notification, it is important to determine in advance how individuals will be contacted. Immediately after an event occurs, steps should include identifying:

- the size of the affected population;
- all data elements exposed;
- risk to the affected constituents from such exposure; and
- predicted response of the affected constituents.

Speed and accuracy are both important. Some constituents and regulators will react negatively to any delay that they perceive to be unreasonable. Consumers expect timely and clear notification delivered in a manner appropriate to their needs.

4.8 Have we considered that, depending on the situation, we may need to craft different messages for different types or levels of clients or employees?

It may be appropriate to have a different message and method of delivery for the company's most important relationships, such as highest-value customers or most-senior employees, or for categories of individuals that may be particularly sensitive, such as the elderly, the disabled and minors. Most organizations realize too late or in the heat of notification that there are subsets of the population that require specific communication. Such special communication needs may be caused by particularities of a geographic region, unique characteristics of the population, etc.

4.9 Have we implemented improvements as a result of an actual execution (real or mock) of the plan?

An organization should carefully analyze past events and responses to improve its communications plan and minimize the likelihood of future events. Regardless, conducting mock "fire drills" is an essential part of testing a crisis management plan. Ideally, plans should be tested regularly and at different times during the year, and updated as necessary to remediate any deficiencies.

4.10 Have we budgeted for a cyber security event?

Responding to a cyber security event is often an unexpected and unbudgeted expense. The heat of crisis is not a good time to make financial decisions of this magnitude, especially when the legal timelines regulating notification preclude lengthy debate over finances. The average cost of basic notification for a large data breach can be $1-$2 per customer record; this may reach $3-$6 if call center services are required. Services to affected individuals to minimize the impact and reduce the chance of customer defections or lawsuits – such as credit monitoring services, fraud resolution, and/or ID theft insurance – can cumulatively cost between $10 and $120 per individual per year. Many organizations have privacy insurance to cover the costs associated with the communications plan and incident response, including hiring a crisis public relations firm, notifying regulators and affected parties, and providing monitoring and identity theft remediation services to affected individuals.

CHAPTER 5

KEY QUESTIONS FOR YOUR RISK MANAGER FOR CORPORATE INSURANCE

Cyber security events can, and often do, result in substantial short-term direct costs such as lost income, business interruption and significant legal expenses and liabilities, among others, which can severely strain the financial resources of a company. Even when managed properly, a company remains at substantial risk from unknown or worse than anticipated loss events. Each company has to decide how it wishes to handle that residual risk, how much to accept and how much, if any, to transfer through insurance. Since the late 1990s, insurance companies have developed, and specialized brokers have emerged with respect to, a range of products which allow an entity to transfer many of these financial risks. Commonly known as "cyber risk" or network security and privacy insurance, these policies are specifically designed to cover a host of cyber risks including legal expenses, settlements, judgments, business loss and "extra expenses."

The questions below are those which would typically be asked of the Risk Manager for Corporate Insurance or individual responsible for the purchase of insurance to transfer the cost of recovering from a cyber security event.

5.1 Doesn't the company already have insurance coverage for this?

Unfortunately, traditional insurance policies, written well before the arrival of the internet, do not generally cover cyber-related risks. For example, general liability policies purchased by companies today typically cover bodily injury and tangible property damage claims. They do not normally cover damage or theft to digital property or litigation arising from most cyber events. Similarly, property policies as a general matter only cover tangible property loss arising from physical perils such as flood or fire.

5.2 What does cyber risk insurance cover?

Because cyber insurance policies have been around only since the late 1990s, there is no universally-accepted insurance form in the marketplace. Nevertheless, regardless of the particular language (which can be very important), superior cyber risk policies should provide the following coverage:

- third party litigation and regulatory investigations (especially those arising from theft of personally identifiable information (PII) of customers) including legal expenses, judgments and settlements;
- first party losses an insured company may suffer from business interruption, and "extra expenses" incurred due to a covered cyber security event; and
- with respect to PII theft events, enhanced coverage for "crisis management" expenses, state notification expenses and other remediation costs.

Exclusions vary from carrier to carrier but generally include no coverage if the insured: a) fails to meet the minimum security standards; b) fails to provide notice of a material

KEY RESULTS

Even if managed properly, a cyber security event will lead to residual financial loss.

Specifically-designed cyber insurance can be a useful tool in transfers of unwanted residual risk.

Sometimes a company qualified for insurance can use this as a positive fact in regulatory negotiations and civil lawsuit settlements.

change to the information provided in their application; or c) breaches representations and warranties made in the application. There is usually an overall policy aggregate limit and a per loss deductible or "self-insured retention."

5.3 What types of cyber security events are covered by this insurance and how are our insured losses measured?

If there is a failure of security and a successful breach occurs compromising a company's system or unauthorized access to sensitive information is gained, civil lawsuits from customers, suppliers and others could arise, resulting in substantial legal defense costs and potential expensive settlements costs or adverse judgments. In addition, investigations by regulatory bodies including the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC) or state attorney generals could arise resulting in company costs to investigate and defend. Business interruption and related expenses associated with reduced network availability can also affect the bottom line and reduce profitability. Over the short- or long-term, such events can lead to reputation damage. The quantifiable measurement of third party litigation is, of course, the cost of mounting a legal defense, payment of any settlement or cost of an adverse judgment. Business interruption can be quantified in terms of numbers of transactions, dollars or contracts per time period measured on a typical business day. The cost of re-constructing intangible assets may include forensic investigation, recompiling data or transcribing information.

5.4 Does the policy specifically cover identity theft issues?

Many cyber/information risk insurance policies explicitly respond to events that could lead to identity theft, including release of PII. Coverage may include reimbursement for the cost of notifying affected individuals and providing identity theft risk management services such as credit monitoring. Furthermore, many identity theft risk management services include personal identity theft insurance as a component of the service.

5.5 Is there a Directors' & Officers' exposure if we do not purchase the cover?

In theory, if a company suffers a large uninsured financial loss where reasonable insurance was available in the market, failure to obtain insurance may be ground for a management liability suit by aggrieved shareholder(s). Furthermore, most D&O policies have an exclusion for a "failure to obtain insurance" claim.

5.6 Where do we find an insurance broker who can assist in evaluating whether we need this type of insurance?

Any insurance broker with a "P&C" (Property and Casualty) license can help with purchase of this coverage. Almost all large insurance brokers in the United States have developed information security and privacy expertise. Many "middle-tier" or "regional" broking houses have also developed, or are in the process of developing, internal resources dedicated to this coverage as brokerage revenues from information security and privacy insurance continue to grow year to year. Finally, there are specialist wholesalers who serve as dedicated resources to retail brokers who have

no in-house expertise. The essential lesson here is that this type of coverage is fairly new and can be complex, requiring the use of a brokerage firm schooled in the area.

5.7 How do we know what insurance carrier to consider with respects to this insurance?

A growing number of insurers either currently offer or are gearing up to offer some form of cyber risk coverage. Key considerations for selecting an insurance company include:

- the insurer's ratings from the insurance rating agency A.M. Best as well as financial rating agencies such as Standard & Poor's, Moody's etc.;
- the length of time the carrier has been providing this specific coverage;
- the maximum limits the carrier can offer on any one policy (known as the carrier's "capacity");
- the scope of coverage being sought/offered;
- price; and
- claims handling practices and reputation in "specialty" lines.

5.8 Have there been losses in this area?

On average, one new cyber-security incident has been reported almost every day since 2006. In recent years, PII theft events have frequently appeared in the media. Less public but occurring nevertheless are computer attacks against both public and private entities that result in data destruction, downtime, etc.

5.9 What does a policy cost?

The cost of this policy will be comparable to that of many other corporate insurance policies. The actual cost of insurance depends on coverage, limits and retention. For a very small company, this insurance may cost less than $1,000 dollars per year. For a very large company, the cost may be over a million dollars per year.

5.10 What are the other benefits of our purchasing a specific cyber risk insurance policy?

In addition to the obvious benefit of legal and first party expense reimbursement, the purchase of a specific cyber risk policy has a number of other indirect benefits, including the ability to obtain an objective, usually free, review of a company's network security by a third party (i.e. the insurer or its agent), a better ability to understand the company's risk level compared to its peers (by examining the differences in premium) and better quantification of net financial risk. Finally, the demonstration of the successful ability to purchase insurance could be a favorable factor with the company's regulators, or even in litigation.

APPENDICES

APPENDIX A

PROBABILITY OF FINANCIAL LOSS BASED ON MITIGATING ACTIONS

The following model provides a simple method to look at current and expected probabilities of financial risk. By estimating the financial improvement if certain risk mitigating actions are taken, a CFO can better determine the company's ROI arising from suggested steps to mitigate the company's overall Net Financial Risk.

Risk Mitigation Actions (RMA) vary based on the business of the company. Typical RMAs might include:

- Additional technology
- Additional staff
- Purchase of insurance or additional insurance
- Change in contract language in vendor or customer agreements
- Change in business activity
- Change in business continuity plan
- Change or implementation of crisis management plan

This Action Guide contains these and many other possible activities.

In the chart at right, the number in each cell represents the overall likelihood of incurring a financial loss equal to the amount indicated in Column 1. Column 1 figures should be changed to reflect the risk tolerance range of the company. Numbers are illustrative only. To calculate the overall number, each area (legal, compliance, crisis management, etc.) would be asked to recommend a mitigating action based on the estimated loss.

As the contributions to mitigating the risk are not necessarily cumulative in specific steps, the example shows what might occur as one approaches risk management with an holistic view, adding value to the process as each contribution is added.

The number of columns depends on the number of actions, which depends on the justification of the mitigation for the risk in question. One should not send a dollar after a dime.

The number of rows depends on the steps and corresponding dollar levels an organization wishes to use for analysis.

Financial Loss Estimate	Current	RMA 1	RMA 2	RMA 3	RMA 4
$1,000	100	100	100	100	100
$25,000	90	85	80	80	70
$50,000	85	80	75	85	65
$100,000	80	75	70	80	60
$250,000	75	70	60	75	55
$1,000,000	70	65	50	45	50
$5,000,000	50	45	50	40	50
$10,000,000	20	15	20	10	20
$25,000,000	10	5	10	5	10
$50,000,000	2	1	2	.05	2
$100,000,000	1	.05	1	.005	1
"Out of business"	.000005	.000005	.000005	.000005	.00005

APPENDIX B

PROBABILITY (FREQUENCY) OF FINANCIAL LOSS FOR CERTAIN RISK EVENTS

The following model provides a simple method to look at current and expected probabilities of financial risk due to certain events. The methodology illustrated by this chart is a simple H(igh), M(edium) and L(ow). Then this probability is then modified, or not, after taking into consideration certain Risk Mitigation Actions (RMAs). (For examples of RMAs, see Appendix A). By estimating the financial risk probability of certain risk events, a CFO can better determine the company's ROI arising from suggested steps to mitigate the company's overall Net Financial Risk. The loss events are company-specific and the model below is for illustrative purposes only, but in all cases loss events should include all risk areas of the company (legal, compliance, crisis management, etc.).

As the contributions to mitigating the risk are not necessarily cumulative in specific steps, the example shows what might occur as one approaches risk management with an holistic view, adding value to the process as each contribution is added.

The number of columns depends on the number of actions, which depends on the justification of the mitigation for the risk in question. One should not send a dollar after a dime.

The number of rows depends on the types of Loss Events or expenditures an organization wishes to use for analysis.

Loss Event	Current	RMA 1	RMA 2	RMA 3	RMA 4
Individual Litigation	H	M	M	H	L
Class Litigation	M	M	L	L	L
Regulatory Investigation	H	M	H	M	L
Contract Dispute	H	H	M	M	L
Loss of Customers	M	L	M	L	L
Reputation Damage	H	H	M	M	L
Data Theft	H	M	M	L	L
Denial of Service	M	M	L	M	L
Cyber-Terrorism	M	M	M	L	L
Cyber-Extortion	M	L	L	M	L
Fraud	H	H	M	L	L

APPENDIX C

SEVERITY OF FINANCIAL LOSS FOR CERTAIN RISK EVENTS

Similar to Appendix B, the following model provides a simple method to look at current and expected severity of financial risk due to certain events. The methodology illustrated by this chart is a simple H(igh), M(edium) and L(ow). Then this severity estimate is then modified, or not, after taking into consideration certain Risk Mitigation Actions (RMAs). (For examples of RMAs, see Appendix A). By estimating the financial risk severity of certain risk events, a CFO can better determine the company's ROI arising from suggested steps to mitigate the company's overall Net Financial Risk. The loss events are company-specific and the model below is for illustrative purposes only, but in all cases loss events should include all risk areas of the company (legal, compliance, crisis management, etc.).

As the contributions to mitigating the risk are not necessarily cumulative in specific steps, the example shows what might occur as one approaches risk management with an holistic view, adding value to the process as each contribution is added.

The number of columns depends on the number of actions, which depends on the justification of the mitigation for the risk in question. One should not send a dollar after a dime.

The number of rows depends on the types of Loss Events or expenditures that an organization wishes to use for analysis.

Loss Event	Current	RMA 1	RMA 2	RMA 3	RMA 4
Individual Litigation	H	M	M	H	L
Class Litigation	M	M	L	L	L
Regulatory Investigation	H	M	H	M	L
Contract Dispute	H	H	M	M	L
Loss of Customers	M	L	M	L	L
Reputation Damage	H	H	M	M	L
Data Theft	H	M	M	L	L
Denial of Service	M	M	L	M	L
Cyber-Terrorism	M	M	M	L	L
Cyber-Extortion	M	L	L	M	L
Fraud	H	H	M	L	L

Note: A similar method can be used with respect to a vulnerability analysis.

APPENDIX D

GLOSSARY OF ACRONYMS

Acronyms commonly used within this publication include:

ANSI	American National Standards Institute
BCP	Business Continuity Planning
CERT	U.S. Computer Emergency Readiness Team
CISO	Chief Information Security Officer
CobiT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations
CRO	Chief Risk Officer
CSO	Chief Security Officer
CTO	Chief Technology Officer
DHS	U.S. Department of Homeland Security
DR	Disaster Recovery
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
GLB	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HSSP	ANSI Homeland Security Standards Panel
IEC	International Electrotechnical Commission
ISA	Internet Security Alliance
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
RMA	Risk Mitigation Actions
SBU	Sensitive But Unclassified Information
SEC	U.S. Securities and Exchange Commission

APPENDIX E

APPLICABLE STANDARDS, FRAMEWORKS AND GUIDANCE DOCUMENTS

The following list of standards and reference documents is excerpted from *Recommendation for Creating a Comprehensive Framework for Risk Management and Compliance in the Financial Services and Insurance Industries,*[7] a document published by the InterNational Committee for Information Technology Standards (INCITS).

For the reader's convenience, information and links for access to the standards and documents identified below can be found online at **webstore.ansi.org/cybersecurity**.

Standard | Reference Work Title
ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems – Requirements*
ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*
ISO/IEC 2nd FCD 27004, *Information Security Management Measurement*
ISO/IEC 2nd FCD 27005, *Information technology — Security techniques — Information security risk management*
ISO/IEC FDIS 21827, *Information technology — Security techniques — Systems security engineering — Capability maturity model (SSE-CMM®) to address cyber threats*
NIST 800-53, Recommended Security Controls For Federal Information Systems
NIST 800-30, Risk Management Guide For Information Technology Systems
NIST 800-55r1, Performance Measurement Guide For Information Security
NIST SP 800-100, Information Security Handbook — A Guide For Managers
Control Objectives for Information Technology (CobiT®)
Enterprise Risk Management — COSO
OCTAVE Allegro, Improving the Information Security Risk Assessment Process
FFIEC IT Examination Handbook
Security Operations Maturity Architecture (SOMA)
Information Security Management Maturity Model (ISM3)
An Introduction to Factor Analysis of Information Risk (FAIR)

7 Full text available online at www.incits.org/tc_home/sbp/sbp070049.pdf.

Recommendation for Creating a Comprehensive Framework for Risk Management and Compliance in the Financial Services and Insurance Industries identifies numerous information resources; it does not prescribe to be an exhaustive list or inventory of every applicable standard and guidance document in this area.

Additional documents identified during the development of this Action Guide include:

Standard | Reference Work Title
ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*
ISO/IEC 15408 (Parts 1-3):2005, *Information technology — Security techniques — Evaluation criteria for IT security*
Internet Security Alliance (ISA), Common Sense Guide for Senior Managers — Top Ten Recommended Information Security Practices
The US-CCU Cyber-Security Check List (2007)
Federal Information Security Management Act (FISMA) Implementation Project
NFPA 1600 – *Standard on Disaster/Emergency Management and Business Continuity Programs* (2007)
CERT Resiliency Engineering Framework (REF)
CERT Insider Threat Research
ANSI-Better Business Bureau Identity Theft Prevention and Identity Management Standards Panel (IDSP) Report (2008)

APPENDIX F

SUMMARY LIST — 50 QUESTIONS EVERY CFO SHOULD ASK

Chapter 1 Key Questions for Your Chief Legal Counsel

1.1 Have we analyzed our cyber liabilities?
1.2 What legal rules apply to the information that we maintain or that is kept by vendors, partners and other third parties?
1.3 Have we assessed the potential that we might be named in class action lawsuits?
1.4 Have we assessed the potential for shareholder suits?
1.5 Have we assessed our legal exposure to governmental investigations?
1.6 Have we assessed our exposure to suits by our customers and suppliers?
1.7 Have we protected our company in contracts with vendors?
1.8 What laws apply in different states and countries in which we conduct business?
1.9 Have we assessed our exposure to theft of our trade secrets?
1.10 What can we do to mitigate our legal exposure and how often do we conduct an analysis of it?

Chapter 2 Key Questions for Your Compliance Officer

2.1 Have we inventoried what regulations we must comply with?
2.2 Do we understand what regulated data we have, where it exists and in what format?
2.3 Are there valid business reasons for collecting the data, if not required by regulations?
2.4 How do we track and monitor compliance on an ongoing basis?
2.5 Do we have regulatory risk with vendors/companies we do business with?
2.6 Are all of our procedures and policies with respect to our regulatory obligations documented?
2.7 Are there (regulatory) requirements we can or have considered opting out of?
2.8 Are there processes and procedures in place regarding data retention and destruction?
2.9 Does the organization have processes to review and update privacy policies and disclaimers to customers?
2.10 Are we complying with what our privacy policy says?

Chapter 3 Key Questions for Your Business Operations and Technology Teams

3.1 What is our biggest single vulnerability from a technology or security point of view?
3.2 How vulnerable are we to attack on the *confidentiality*, *integrity* and *availability* of our data and systems?
3.3 If our system goes down, how long until we are back up and running and are there circumstances where we do NOT want to be back up quickly?
3.4 Where do we stand with respect to any information security/technology frameworks or standards that apply to us? (see also: Appendix E)
3.5 Do we have the proper staffing to reasonably maintain and safeguard our most important assets and processes?

3.6 What is the assessment of physical security controls at each of our sites (data center, home office, field offices and other sites)?
3.7 How prepared are our incident response and business continuity plans?
3.8 What is our risk exposure of technology or business operations failures at our vendors and service providers?
3.9 What is the maturity of our information classification and management program?
3.10 How often are we re-evaluating our technical exposures?

Chapter 4 Key Questions for Your External Communications and Crisis Management Teams

4.1 Do we fully understand the overall financial impact of mishandling communications with our key stakeholders following a cyber security event?
4.2 Have we evaluated the appropriate communications response to our key stakeholders?
4.3 Do we have a documented, proactive crisis communications plan?
4.4 Have we identified and trained all of the internal resources required to execute the communications plan?
4.5 Do we have a template timeline for executing the communications plan?
4.6 Do we have contacts at specialist crisis communications firms if we need their services?
4.7 In the case of a cyber security event involving personally identifiable information (PII), do we have a system in place to quickly determine who should be notified, and how?
4.8 Have we considered that, depending on the situation, we may need to craft different messages for different types or levels of clients or employees?
4.9 Have we implemented improvements as a result of an actual execution (real or mock) of the plan?
4.10 Have we budgeted for a cyber security event?

Chapter 5 Key Questions for Your Risk Manager for Corporate Insurance

5.1 Doesn't the company already have insurance coverage for this?
5.2 What does cyber risk insurance cover?
5.3 What types of cyber security events are covered by this insurance and how are our insured losses measured?
5.4 Does the policy specifically cover identity theft issues?
5.5 Is there a Directors' & Officers' exposure if we do not purchase the cover?
5.6 Where do we find an insurance broker who can assist in evaluating whether we need this type of insurance?
5.7 How do we know what insurance carrier to consider with regard to this insurance?
5.8 Have there been losses in this area?
5.9 What does a policy cost?
5.10 What are the other benefits of our purchasing a specific cyber risk insurance policy?

The **American National Standards Institute** (ANSI) is a private non-profit organization whose mission is to enhance U.S. global competitiveness and the American quality of life by promoting, facilitating, and safeguarding the integrity of the voluntary standards and conformity assessment system. Its membership is comprised of businesses, professional societies and trade associations, standards developers, government agencies, and consumer and labor organizations. The Institute represents the diverse interests of more than 125,000 companies and organizations and 3.5 million professionals worldwide.

The Institute is the official U.S. representative to the International Organization for Standardization (ISO) and, via the U.S. National Committee, the International Electrotechnical Commission (IEC), and is a U.S. representative to the International Accreditation Forum (IAF).

www.ansi.org

The **ANSI Homeland Security Standards Panel** (ANSI-HSSP) was launched in 2003 to assist DHS and those sectors requesting assistance to accelerate the development and adoption of consensus standards critical to homeland security.

www.ansi.org/hssp

The **Internet Security Alliance** (ISA) is a non-profit collaboration between the Electronic Industries Alliance (EIA) and Carnegie Mellon's CyLab and works closely with the CERT Coordination Center (CERT/CC), a leading, recognized center of Internet security expertise. The non-profit helps law firms and companies in the aerospace, defense, entertainment, financial, food service, manufacturing and telecommunications sectors by standardizing best practices in Internet security and network survivability and by working with legislators and regulators to ensure that market incentives are at the forefront of public policy.

www.isalliance.org

ANSI Homeland Security Standards Panel
25 West 43rd Street — Fourth Floor, New York, NY 10036
T: 212.642.4900 | F: 212.398.0023 | E: hssp@ansi.org
www.ansi.org or **www.ansi.org/hssp**

Internet Security Alliance
2500 Wilson Boulevard, Arlington, VA 22201
T: 703.907.7799 | F: 703.907.7093 | E: info@isalliance.org
www.isalliance.org

An electronic edition of this text is available online at **webstore.ansi.org/cybersecurity**

"*The Financial Impact of Cyber Risk* report is excellent and recommended reading for all CFOs. I found the report to be informative and very helpful."

— George Carruthers, EVP & Chief Financial Officer
LoneStar National Bank

"The realization of your organization's status and potential financial implications related to cyber attack preparedness will be eye-opening for every CFO."

— Richard Davis, Chief Financial Officer
The George Washington University Hospital

"This study is instrumental in demonstrating that cyber risk is not just a technology issue but a core business issue."

— Phillip Chappo, First Vice President
Credit Industriel et Commercial

"An astute analysis that clearly spells out the financial impact of poor enterprise risk and controls on the balance sheet. This study offers both real and practical insight to effectively hedging those risks."

— E. Regan Adams , Esq.,
Legal and Regulatory Data Risk and Retention
Goldman Sachs

"Fiduciaries must quantify consequences of cyber risk as share holder currency. This document shifts the paradigm from technology issues to enterprise financial requirements."

— Robert K. Gardner, Founding Partner
New World Technology Partners

"This document sensitizes the reader to the complex multi-disciplinary issues of cyber security and reduces them to financial considerations that every enterprise must address."

— Lawrence Berk, President and CEO
Baron Group, USA

"As an information protection software supplier, the explicit identification in this document of the multidisciplinary roles for cyber security from a CFO's perspective provides us with a pragmatic set of requirements through which we can satisfy the broad range of needs of our customers."

— Joe Buonomo, President and CEO
Direct Computer Resources, Inc.

"One must account for technical, legal, compliance, crisis management and customer relations issues in order to fully evaluate the financial risks of cyber security. This book not only makes a strong case for such a multi-disciplinary approach, but also provides the reader with a detailed method for achieving it."

— Dr. C. Warren Axelrod, SVP, Privacy and Security
Bank of America