Cooperative Systems
forward thinking IT

What every CEO should understand about security

This whitepaper is a top-level review of key aspects of cyber resilience: information-sharing, planning, skill and the economics of cyber security. We offer a number of recommendations for the private and public sector, urging both to engage in discussion of corporate responsibility and balanced policy to strengthen their business and global cyber resilience.

NOAH
information technology services

80 Lamberton Rd., Windsor, CT 06095 • 860.523.1000
67 South Bedford St., Suite 400 West, Burlington, MA 01803 • 781.496.3075
noahsales@coopsys.com
www.coopsys.com

Introduction

Cooperative Systems has acquired over 20 years of experience working with banks, credit unions, healthcare organizations, large retailers, and a number of other business sectors all rightfully concerned about data protection. In that time, we have accumulated a significant amount of knowledge about implementable practical measures. Unfortunately, most organizations with unsophisticated security programs view security as a checklist and fail to integrate as they invest in new applications, technology, or infrastructure. The "hope" is that the vendor will "take care of it" when it comes to implementing secure systems. But all too often, software and hardware products and their installation standards fall far too short of the real threats posed by today's cyber criminals. In addition, personal habits and corporate preferences contribute to the lack of sophistication and easy penetration by even amateur actors utilizing powerful and effective hacking tools.

This whitepaper is based in part on a public initiative called RE: CYBER which was designed to help business leaders that may lack the tools and resources to protect against the ever changing cyber-threat landscape. Jointly developed by the National Cyber Security Alliance (NCSA) and Business Executives for National Security (BENS), both nonpartisan nonprofit organizations, the ultimate goal of the initiative is the inclusion of cybersecurity in enterprise risk management at the CEO and board level. By managing cybersecurity risk, CEOs and board members can do their part to protect their companies, protect our nation's economic future and support our national defense establishment.

We intend to bring this discussion to the attention of business owners and executive management to foster an intelligent discussion on the priorities of a cyber risk program for your organization.

An Obvious Statement

Let's begin with the following claim: ***A major cyber breach could result in the loss of information that would cause you to lose a bid on a contract, lose key intellectual property, and potentially lose millions of dollars because of an operational shut-down.***

…and you are not paying attention? Cyber risk is a major business risk and must be managed from the top. With the frequency and severity of cybersecurity incidents involving business on the rise, it is an especially critical time for CEOs and boards to focus on understanding and proactively managing cyber risk.

Consider just a select few of the long list of cyber incidents reported in recent years:

- **Operation Shady Rat** - For at least five years starting in 2006, hackers infiltrated the computer systems of more than 70 national governments, global corporations and nonprofits in 14 countries. The hackers stole sensitive property including government secrets, email archives, contracts and intellectual property. This hacking campaign, dubbed Operation Shady Rat by McAfee, is widely assumed to have been perpetrated by, or to have been funded by, the People's Republic of China. More information. (Alperovitch, Dimitri, McAfee. *Revealed: Operation Shady RAT*. August 2011.)

- **VTech** – Over 4.8 million parent accounts and 6.3 million child-related profile were affected by a breach of the database for their online store. General user information was accessed, as well as data related to password retrieval, IP addresses, and physical mailing addresses. Furthermore, names and birthdates of children were included in the leak of information.
- **Anthem –** This particular breach, which occurred in early 2015, was the largest healthcare data breach to date. It resulted in theft of over 78 million patient records, in addition to over 10 million non-patient records that featured highly sensitive identifying information.
- **Otto Pizza –** Data breaches are hitting international-level enterprises, but we are also keenly aware that simultaneously small and midsize businesses are being treated as easy targets more than ever before. This Maine-based pizza company, for example, experienced a breach that leaked over 900 customers' credit and debit card numbers from multiple locations. This was a Point-Of-Sale attack that spanned months and flew under the radar while collecting data since there was no immediate fraud reported on consumers' accounts.

As highlighted by the examples above, consequences of a cyber incident can include but are certainly not limited to:

- **Financial loss** due to operational shutdowns, loss of customers and sales, loss of financing or lawsuits.
- **Long-term loss of competitive position** because of the loss of intellectual property, business plans and **loss of trust**.
- **Add Damage to Brand or Reputation**

The Internal Cybersecurity Threat

Quite often, we think of a cybersecurity threat as a hacker or adversary attempting to penetrate our computer systems from outside our network; these threats do exist, but what about the internal cybersecurity threat? In many data breach instances, the breach of data happens inside the network and inside the company's four walls. Below are several key examples:

- For example, many employees' home networks are not secure. An employee could unknowingly bring in a USB memory stick that has malware on it. When the employee plugs the USB stick into their corporate computer, the malware is transferred, resulting in data being gathered and then being sent outside the corporate network. This increases the possibility of malware being transferred from home network to corporate network via laptops, tablets and other electronic devices.
- Another example could be an employee losing his or her laptop during the security screening process at the airport. Most laptops do not have full-disk encryption enabled or remote wipe configured, so an enormous amount sensitive data is lost every day as hundreds of computers are stolen.
- Many companies are now using cloud-based services such as Dropbox to store sensitive data. Unfortunately, these consumer-based services typically do not have the kind of security controls and protocols that a corporate

environment would have. Whether users have weak passwords or the settings aren't configured properly, corporate data can be at risk with these types of services.

- Another potential internal cyber risk is a disgruntled employee. It is not uncommon for someone who is disgruntled with an organization to transfer sensitive information to a USB memory stick and walk out the front door. Also, if an employee sets up his or her own WiFi router on the corporate network for convenience. With a weak password or no password enabled, this type of device can have serious security consequences.
- Finally, security experts are seeing a rapid increase of extremely sophisticated socially-engineered attacks in which hackers gain access by using other methods of intelligence. For example, there have been many cases in which hackers have called IT help desks and impersonated employees. With social media and the resources available on the Internet, it is not difficult to gain enough knowledge on an individual to be able to convince an IT department to reset a password over the phone.

There is no question that the external cybersecurity threat is of great magnitude. But we also must pay attention to the internal threat. Good, solid technology, training, policies and procedures can greatly reduce businesses' internal threats. A related whitepaper titled, *Creating A Culture Of Security Awareness Inside Your Organization* addresses the specific needs of IT staff and how they can play a key role in the overall security health of your organization.

Reputation Risk

Reputation risk is driven by a wide range of other business risks that must all be actively managed. Atop the list are risks related to ethics and integrity, such as fraud, bribery, and corruption. Next is security risk, including both physical and cyber breaches — followed closely by product and service risks, such as those related to safety, health, and the environment. Third-party relationships are another rapidly emerging risk area, with companies increasingly being held accountable for the actions of their suppliers and vendors.

According to a study by World Economics, on average more than 25% of a company's market value is directly attributable to its reputation. And in a highly connected world where customers, operations, supply chains, and internal and external stakeholders are scattered across the planet — and where reputations can be globally attacked with just a few keystrokes — that number is likely even higher today.

A company's reputation is affected by its business decisions and performance across a wide range of areas:

- **Financial performance**. Shareholders, investors, lenders, and many other stakeholders consider financial performance when assessing a firm's reputation.
- **Quality**. An organization's willingness to adhere to quality standards goes a long way to enhancing its reputation. Product defects and recalls have an adverse impact.
- **Innovation**. Firms that differentiate themselves from their competitors through innovative processes and unique/niche products tend to have strong name recognition and high reputation value.
- **Ethics and integrity**. Firms with strong ethical policies are more trustworthy in the eyes of stakeholders.

- **Crisis response**. Stakeholders keep a close eye on how a company responds to difficult situations. Any action during a crisis can ultimately affect the company's reputation.
- **Safety**. Strong safety policies affirm that safety and risk management are top strategic priorities for the company, building trust, and value creation.
- **Corporate social responsibility**. Actively promoting sound environmental management and social responsibility programs helps create a reputation "safety net" that reduces risk.
- **Security**. Strong infrastructure to defend against physical and cybersecurity threats helps avoid security breaches that could damage a company's reputation.

Asking the right (and tough) questions

Companies must protect themselves against a number of cyberattacks, whether the perpetrator is a nation state, cyber criminal or disgruntled employee. In some companies, cybersecurity has historically been treated as a technology issue. However, cyber risk must be managed at the most senior level in the same manner as other major corporate risks. To properly manage cyber risk, the CEO must fully understand the company's cyber risks, the company's plan to manage these risks, and the company's response plan when the inevitable breach occurs. CEOs also must consider the risk to the company's reputation and the legal exposure that could result from a cyber incident.

A good starting point for a CEO is a list of cyber security questions for CEOs created by the Department of Homeland Security. Some of the key questions a CEO should ask the chief information security officer or outside information technology consultants are:

1. How is our executive leadership informed about the current level and business impact of cyber risks to our company?
2. What are the current level and business impact of cyber risks to our company?
3. How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying executive leadership?
4. What is our plan to address identified risks? How do we preserve the integrity of data resident on our network?
5. How are industry standards and best practices reflected in our cybersecurity program?
6. How comprehensive is our cyber incident response plan? How often is it tested? If we were breached tomorrow, who would we call?
7. Do we have cyber security insurance that covers data breaches?

Cyber Risk Assessment and Management

Proper cyber security risk management is more than a technology solution. A company, led by its CEO, must integrate cyber risk management into day-to-day operations. Additionally, a company must be prepared to respond to the inevitable cyber incident, restore normal operations and ensure that company assets and the company's reputation are protected.

Cyber Assessments

1. **Understand what information you need to protect: identify the corporate "crown jewels."**
   The first step in assessing an organization's cyber risk is to understand what company assets you are trying to protect and why. Ask yourself, what are your most critical assets? Identify your most important information, assets, and legally protected information.

2. **Identify Threats to Crown Jewels**

   - How do you store the information?
   - Who has access to the information?
   - How do you protect your data?
   - What steps are you taking to secure your computers, network, email and other tools?

3. **Forecast the consequences of a successful attack**
   If you have an information technology staff or chief information security officer, ask them to walk you through the above analysis. Ask them to quantify the risk. Also ask them to explain what could happen as a result of a fully successful cyber-attack against your company.

Cyber Risk Mitigation – Implement a Cybersecurity Plan

Most experts recommend that businesses have a strategic approach to cybersecurity. The Federal Communications Commission created the Small Biz Cyber Planner to help businesses evaluate their current cybersecurity posture and create a plan. See the full report.

A comprehensive cybersecurity plan needs to focus on three key areas:

1. **Prevention:** Solutions, policies and procedures need to be put in place to reduce the risk of attacks.

2. **Resolution:** In the event of a computer security breach, plans and procedures need to be in place to determine the resources that will be used to remedy a threat.

3. **Restitution:** Companies need to be prepared to address the repercussions of a security threat with their employees and customers to ensure that any loss of trust or business is minimal and short-lived.

Cyber Insurance – Risk Transfer

The cyber insurance market has evolved significantly since the first policies were introduced in the late 1990's. Today, there are more than 25 carriers in the market providing up to $300M in limits. Coverage extensions have developed to include both the third-party liability and first-party cost and expenses associated with a data breach or cyber attack. Insuring agreements vary by insurance company. Options may include:

- **Security & Privacy Liability** – defense and indemnity for failure to keep information private, failure of third-party affiliates to keep information private and failure of systems to prevent a network security failure (including transmission of a virus). Information includes corporate confidential information (CCI), personally identifiable information (PII) or protected health information (PHI) and can be in electronic or tangible form.
- **Crisis Management** – expenses incurred by the insured stemming from a security failure. Covered expenses include costs to respond to adverse publicity, comply with regulatory requirements and voluntarily and proactively provide notification and credit monitoring services to affected parties.
- **Regulatory Proceedings** – covers defense of a proceeding or action brought by a privacy regulator (Federal Trade Commission, Health Insurance Portability and Accountability Act (HIPAA), State Attorney General) or fines for breach of a privacy regulation. Limited coverage for "PCI" fines is available.
- **Business Interruption** – costs incurred by the insured stemming from a material business interruption directly caused by a security failure.
- **Data Recovery** – costs incurred by the insured to restore, recreate or recollect electronic data stored on the insured's computer system that becomes corrupted or destroyed due to a computer attack; including disaster recovery and computer forensic investigation services.
- **Cyber Extortion** – costs incurred, and extortion monies paid, due to a threat related to the interruption of the insured's computer system, or the release or destruction of private information.

With the increasing frequency and costs associated with cyber attacks, your company's risk management strategy should include cyber insurance to help mitigate financial loss and protect your company's balance sheet.

Evaluation

A designated team or individual should follow-up to ensure that the cyber security plan has been implemented and that the plan is protecting the company's assets. The CEO and board of directors should engage in evaluating the company's cyber security plan. Here are some great resources that can help with an assessment and action plan - all the way to the point of implementation and maintenance.

- **Advisory Services**
  While many IT security product and service firms exist to support the CIO and his staff, they are less likely to address the needs of the CEO and board. This may change with time.

- **Legal Options**
  Performing risk management responsibilities may inherently reveal sensitive information about the firm's risk posture. Most firms are concerned with such information being discoverable in a lawsuit that results from a security breach and thus working against the firm whether the risks were caused intentionally or accidentally. For this reason, it is advisable to work through internal or external counsel so the data may be controlled under attorney-client privilege.

- **Managed Services and Cloud Providers**
  Scaling cyber defenses to the same level as large businesses is typically out of reach for smaller companies. One way of achieving the scale and scope of a large business is through the use of managed security services. Managed security service providers (MSSPs) provide perspective across many customers and can see attack patterns more clearly and quickly, allowing them to design more comprehensive incident response and ongoing remediation roadmaps. Moving systems to the cloud can also allow SMBs to leverage scaled security resources. In choosing among MSSPs and cloud providers, the company should balance benefits versus the risk of single points of failure among providers and pay attention to service level agreements (SLAs), jurisdictions and geographic locations in which data and services will be implemented.

4 Ways to Address Privacy Today

While privacy and security are two different things, awareness about privacy is directly linked to a greater awareness of security and will only strengthen your overall security posture against breaches, theft, and accidental data loss. From a recent blog post on our website, here are four ways you can address the majority of privacy concerns right now.

- **Change your settings -** Look over your privacy settings on your browser, social media profiles and other online accounts and make sure you're providing as little information as possible by turning off your location and cookies and opting out of other online trackers.
- **Use ad blockers or privacy add-ons -** Tools like Privacy Badger from the Electronic Frontier Foundation can help you turn off creepy trackers running in the background on some sites, as well as those ever-present social media icons on websites you visit.
- **Log out every time -** For an extra layer of privacy, log out of your social media accounts when browsing the web to avoid trackers from sending information to social media channels.
- **Consider using pro privacy alternatives -** As a result of the data mining, concerned users turn to alternative tools, such as browsers, VPN services and social media services that help to hide their online footprints.

Recommended CEO Actions

In summary, here are the things every CEO should know about Cyber Security along with guidance about how they can get it done. It's an evolving process that requires consistency and follow-through and it really does start at the top.

- Establish a team to create a cyber security plan and evaluation process.
- Get involved in cyber risk management discussions, including an evaluation of your company's specific cyber risks and cyber incident response plans.
- Confirm that cyber risk is addressed in existing risk management and governance processes.
- Discuss with your IT staff or IT consultant how to raise cyber security awareness in your company.
- Begin best practices in privacy immediately to make a small but powerful impact.
- Budget for an annual cyber risk assessment or update your current risk assessment report.
- Discuss cyber insurance policies and options with a knowledgeable broker.

Conclusion

Today, cyber risk is not just a function of the IT department. Technology permeates every aspect of your business and your exposure to breaches far surpasses the capabilities of your IT department to handle it. Rely on a team approach that brings in outside resources, coupled with internal resources, to form an alliance committed to minimizing cyber risk and making it difficult for external hackers to penetrate and for internal employees to become educated and vigilant. Let smart guys work for you and help them through your overall knowledge, appropriate budget and resource commitment, and follow through.

For More Information

- Multi-State Information Sharing and Analysis Center; NYS Office of Cyber Security. Cyber Security: Risk Management, A Non-Technical Guide. 2012. http://www.dhses.ny.gov/ocs/local-government/documents/Risk-Management-Guide-2012.pdf
- World Economic Forum; Deloitte. Risk and Responsibility in a Hyperconnected World, Pathways to Global Cyber Resilience. June 2012. http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience

- U.S. Chamber of Commerce. Internet Security Essentials for Business 2.0. 2012. https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf
- Department of Homeland Security. Cyber Security Evaluation Tool (CSET®). http://ics-cert.us-cert.gov/Assessments
    - Questions for CEOs https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf
- National Cyber Security Alliance. Implement A Cybersecurity Plan. 2013. http://www.staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan/
- Council on CyberSecurity. Critical Controls for Effective Cyber Defense. 2013. http://www.counciloncybersecurity.org/images/downloads/Critical%20Controls%20v4.1.pdf
- Mark Stollery. “Cyber security – the best weapon remains good information security hygiene.” Computer Weekly. March 2013. http://www.computerweekly.com/news/2240178473/Cyber-security-the-best-weapon-remains-good-information-security-hygiene
- McGuire Woods. Buyer’s Guide to Cyber Insurance. October 2013. http://www.mcguirewoods.com/Client-Resources/Alerts/2013/10/Buyers-Guide-to-Cyber-Insurance.aspx
- Review Cooperative Systems’ Cyber Liability webinar.

Cooperative Systems has provided information technology solutions to the SMB market since 1993 when it was established. Our relationships with partners such as Microsoft, HP, Dell, VMware, and Cisco have allowed us the ability to design, scale and implement effective infrastructure solutions for our diverse client base. Our Solution Stack includes custom designed Cyber Security Solutions, Voice over IP (VOIP) Solutions and Phone Systems, Structured Voice and Data Cabling, Mobile and Wireless, Physical Security Solutions, Website Design, Local and Wide-Area Networking, as well as Managed Services. As a Certified Microsoft Partner, our core competencies include Server Administration, Networking Infrastructure, and Managed Services Solutions.

We specialize in educating you in the Information Technology options available to ease your business' IT concerns in the 21st century. Our professional scope ranges from engineering and implementing Telecommunications Systems and Local and Wide Area Networking Solutions, to architecting and designing custom Voice and Data Cabling Solutions to address your specific business needs. Cooperative Systems Network and Technical Engineers' combined experience allow us the ability to successfully provide custom, affordable solutions to our valued Clients.

Our technical expertise enables us to provide Network Design and Support, as well as Communication Design for Office Automation, and Structured Voice and Data Design; utilizing technologies such as Broadband Internet, Dedicated Connectivity, Point-To-Point Tunneling Protocol, and Virtual Private Networking. These technologies provide the ability to securely design and structure your equipment, optimizing communication, productivity and overall business progress.

By coordinating and managing your technical solutions and vendors, we can proactively manage your network and you would see benefits that come with your ability to completely focus on running your organization.