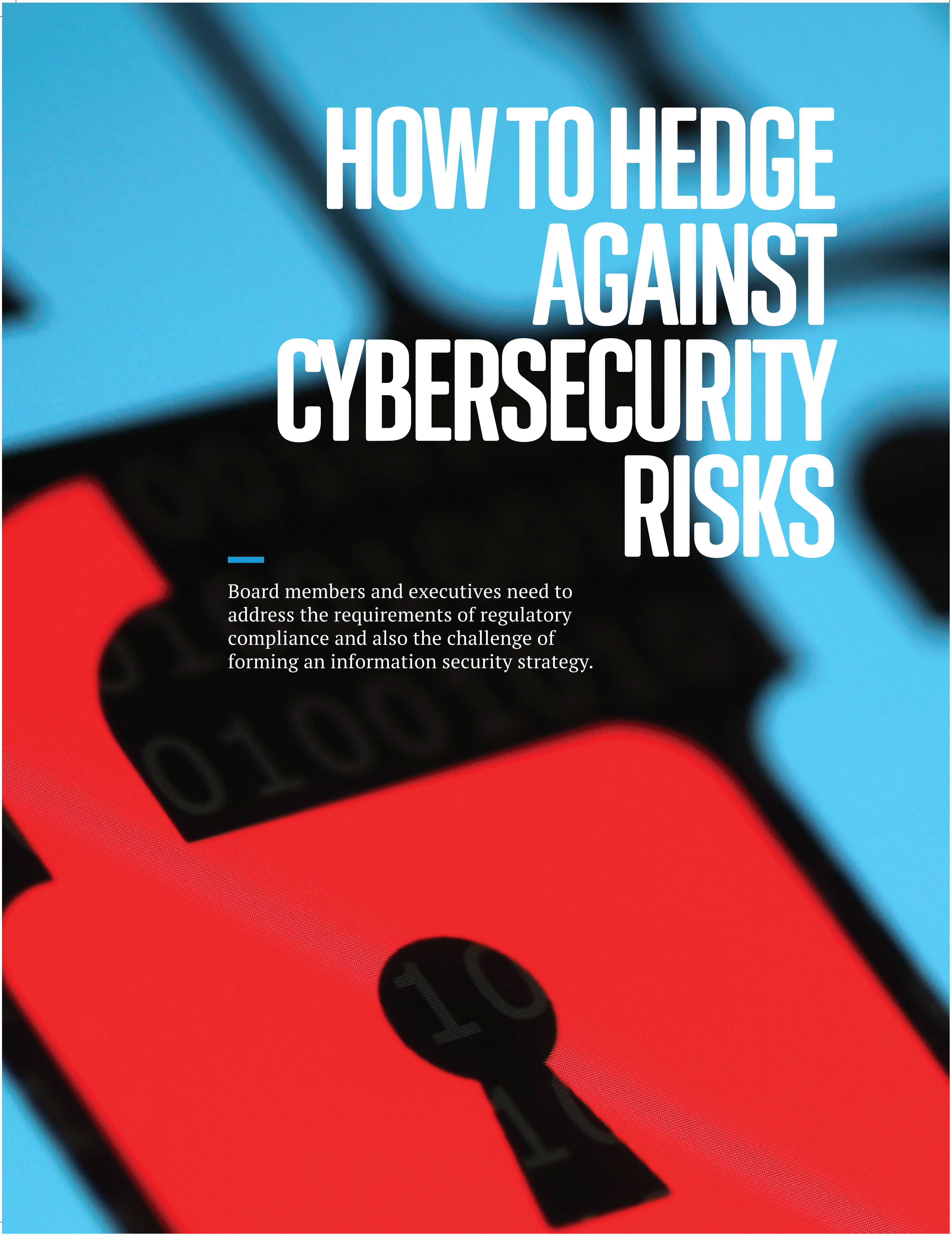
HOW TO HEDGE AGAINST CYBERSECURITY RISKS

Board members and executives need to address the requirements of regulatory compliance and also the challenge of forming an information security strategy.



COMPANIES ARE UNDER ATTACK. News headlines warn about hijacked email, ransomware, and hacked databases,[1] while regulators, laws and professional standards make it increasingly clear that businesses must protect their critical information and operations, with executives responsible for any breaches. The risks are real. Unfortunately, many organizations lack the expertise to implement an effective security program. In particular, many board members and senior executives lack familiarity with the key issues to supervise a security strategy. This paper presents several elements of information and cyber security, including how Chief Information Security Officers (CISOs) and virtual CISOs can provide advisory expertise to companies.

Regulations, Guidelines, and Risks

Business requirements for information and cybersecurity are changing rapidly. Regulations; international, U.S., and state laws; and accepted best practice security standards all demand attention. As examples of these new requirements, in 2017 both the Securities and Exchange Commission (SEC) and the National Association of Corporate Directors (NACD) issued enhanced guidelines for information and cybersecurity.

SECURITIES AND EXCHANGE COMMISSION

SEC rules and guidelines drive management controls for public companies and the securities industry. In September 2017, SEC Chairman Jay Clayton stated, "The scope and severity of risks that cyber threats present have increased dramatically, and constant vigilance is required to protect against intrusions."[2] The SEC specifies that cybersecurity efforts cover assessment, prevention, mitigation, resilience, and recovery, and that in cases of a breach, companies may be required to disclose an attack, including its costs and other business impacts.[3]

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

The NACD sets standards for board behavior and responsibilities, and their 2017 *Handbook on Cyber-Risk Oversight*[4] emphasizes the direct responsibilities of board members to review, approve, and monitor their company's cybersecurity strategy. Boards are required to have direct access to information and cybersecurity expertise, and are being held responsible for the effectiveness of their organizations' information and cybersecurity programs.

RISKS

There are many threats to protect against, all of which are trying to gain unauthorized access to companies' information or systems. In addition to revenue hits, short-term costs to a security breach include immediate management distraction, lost or damaged data and systems, and degraded operational effectiveness with urgent system recoveries and upgrades. Long-term impacts include lawsuits, reputation damage, possible losses of customers, and potential job losses for some employees, executives, and board members.

[1] Larry Ponemon, "2017 Ponemon Institute Cost of a Data Breach Study," *IBM - Security Intelligence*, July 26, 2017.
[2] Jay Clayton, "Statement on Cybersecurity," SEC, September 20, 2017.
[3] SEC Statement, "CF Disclosure Guidance: Topic N. 2, Cybersecurity," SEC Division of Corporation Finance, October 13, 2011.
[4] *NACD Director's Handbook on Cyber-Risk Oversight*, NACD, 2017.

Faced with these risks, companies need to develop and implement a security program appropriate for their business, balancing regulations (which need to be followed), professional standards (which should be followed), and effective protections against expected threats.

What Must We Do?

Companies need to identify and support their business priorities through the protections of their security program. Through choice or inaction, some companies wait for audit findings or a breach to drive their security improvements. Other companies want to be proactive but lack an expert to lead their program. The good news is that while security expertise is necessary, the core elements of an effective security program build on general management skills.

RISK ASSESSMENT

A risk assessment is an early task in any security process, encompassing all current operations and outsourced relationships. Organizations can and should do internal assessments, but regulators and auditors place higher value on (and sometimes require) independent external risk evaluations.

> The FBI reports that some **90%** of company security exploits result from employees clicking on an email link or opening a web page with embedded malware.[5] All it takes is one click and a firm's systems can be attacked from the inside.

Risk assessments usually start by conducting or verifying an inventory of all hardware devices, systems infrastructure, applications, and data. If you do not know what you have, you cannot know what to protect or what threats to protect against.

Next, these assets are linked to critical business functions, identifying those which are most important and most vulnerable. This linking of assets, business activities, and business priorities allows risk assessments and security plans to focus on what most needs protection.

A risk assessment broadly covers these steps:

- Identify what needs to be protected, plausible threats, and known vulnerabilities
- Estimate the business risks if vulnerabilities are exploited (considering probability and potential severity)
- Prioritize these risks and identified protective gaps
- Document and agree to a plan to address these gaps
- Track progress of the plan, with executive and board updates
- Monitor the effectiveness of these protections
- Periodically and regularly repeat the above steps

Although specific threats and vulnerabilities may be unfamiliar to executives, the security process applies general management actions: prioritizing critical business functions, deciding which risks to accept or mitigate, allocating resources, delegating responsibility, approving plans, monitoring effectiveness, and intervening when necessary.

PENETRATION TESTS

A penetration test is a controlled attempt to break into an organization's systems or data. These tests often identify misconfigured infrastructure, manufacturer default passwords still in use, and software that allows unfiltered database access. Penetration tests also may target employees or subcontractors (e.g., social engineering), or physical security protections. Specialist firms generally conduct these reviews, leveraging their knowledge of frequent configuration mistakes, common software and organizational risks, and popular attack vectors.[6] Penetration test results are documented, and prioritized and become part of the risk assessment and plan.

VENDOR REVIEWS

Operationally, many business functions and services that used to be done in-house now are outsourced. Systems once built by internal information technology (IT) departments now are purchased, leased, or used as software services, with data and systems in a remote and vendor-controlled cloud.

These externally developed or provided systems still must be checked for appropriate security standards, and should be validated through vendor statements or third-party certificates such as SSAE18 or ISO audits, which are designed for service-providing organizations.

[5] FBI, "Business Email Compromise: Cyber-Enabled Financial Fraud on the Rise Globally," February 27, 2017.
[6] The Open Web Application Security Project publishes a list of the top web application security risks and protections at https://www.owasp.org.

Companies should conduct annual due diligence reviews of their critical vendors and should expect to provide statements to their own customers.

WRITTEN POLICIES

There are two approaches to documenting security policies and standards. One is to research and document best practices, making those the official policy and using the policy to force organizational changes: an "idealist" approach. The other, an "incrementalist" approach, is to document current practices, testing for protection effectiveness, and prioritizing and targeting required changes, thus, making improvements over time. An organization's resources, business priorities, current protections, and risk tolerance will guide where it belongs on this spectrum. A reality check is that regulators and many customers require firms to test and verify that their documented policies are followed, so regulated or service-providing organizations without policies need to move quickly to establish them.

TRAINING PROGRAMS

Many employees analyze customer or financial data on spreadsheets, removing that data from a controlled systems environment if it is copied to a laptop or work is done from home. This is an example of basic activities with risks that all employees should understand. More important, these are as much human and behavioral issues as they are technological. Information security awareness training programs are a common way to educate people to better recognize security risks and to modify their behavior to be safer.

Some firms focus on "Do Not" policies rather than recognizing that many potentially risky behaviors reflect people's work habits. Studies suggest that the best way to change a behavior is to change expectations around that behavior. With information security awareness training, if people believe they will bring malware into their organization by clicking on links, then eventually they will stop clicking on links – though habits can be slow to change. Experienced Chief Information Security Officers (CISOs) often can identify ways to mitigate risks to a manageable level so that people can get their jobs done with limited modifications or constraints.

Returning to the spreadsheet example, password-protecting spreadsheets containing critical data, providing secure remote access to files, and automatically encrypting laptop hard drives could provide sufficient data protection while supporting a mobile or distributed workforce.

Security training for technologists is also essential. System builders and operators have special responsibilities for safety, but too often security is handled by a separate team or considered an afterthought. As an example of early consideration, defensive programming is the technique of designing, building, and testing systems with the assumption that unexpected events will happen, including security attacks. All developers should be familiar with the inherent vulnerabilities of the languages they use as well as the common risks in specific functions (such as database queries). Security has been appropriately considered before new systems or procedures are implemented. Security should be considered a core design or purchase requirement, and proper training teaches how and why security can be applied throughout the life cycle of a system.

> Information and cybersecurity professionals have a saying, "There are two types of companies: those that have been hacked and those that know they've been hacked."

INCIDENT RESPONSE PLAN

Organizations need to monitor if their protections have been broken. This includes setting warnings on firewalls, reviewing activity logs and investigating unusual events. Unusual events include those when customers or vendors may have detected a problem at your business, as about half of breaches are reported from outside and not discovered internally. It is difficult to plan during an emergency, so companies should have pre-established incident response plans (IRPs) for how to respond to and recover from different breaches. These plans can be viewed as an extension of other business continuity or disaster recovery preparations.

A general IRP will include steps to detect, investigate, respond/mitigate, recover, and remediate. If a computer crime has been committed, care is needed to avoid destroying or contaminating evidence. Thus, a good plan has pre-identified experts to assist as needed, who also can coordinate with the police, FBI, or Secret Service, and who can require vendors to preserve incident-related data.

A written IRP is a fundamental business and security requirement, as is having a pre-established incident response team to carry out that plan.[7]

According to the Ponemon Institute, in 2016 it took firms an average of 191 days to discover a security breach and then another 66 days to contain it.[8]

Important Questions and Considerations

BEST PRACTICES VERSUS GOOD ENOUGH

Security standards such as NIST[9] and ISO[10] specify best practice protections. These standards evolve over time and reflect the cumulative experience of security leaders from around the world. Standards are an excellent starting point for a security program, and they all offer some flexibility to be adapted as appropriate. Companies can decide that best practice protections are not necessary or even appropriate for parts of their business. Limited controls often are acceptable for systems or data that are not business-critical. An effective risk policy can state, "We understand there are risks to not doing xxx, but have decided to accept these risks and instead will protect and monitor that protection by yyy and zzz."

> "I didn't know" is not an acceptable response to a security failure. "You should have known" is the requirement for boards and executives.

Expert guidance on the prevalence and severity of different risks can guide efficient decisions on the benefits, cost, effort, and complexity of different protections.

SECURITY TECHNOLOGY SOLUTIONS

A traditional view of cybersecurity was to build a network wall (firewall) to keep dangers out and then assume all was safe within the protected environment. Among other challenges with this approach, the distinction between 'outside' and 'inside' can be blurry. Technology is part of many people's jobs, and mobile devices, remote access, and web interfaces makes perimeters hard to define and therefore harder to protect, especially because vendors and clients also may be connected. As a result, effective security is better achieved through multiple layers of protection and compartmentalization. Users, systems, and data should be tightly managed for those who need access, and technologies should be implemented to help monitor for and protect against unusual or risky activities.

There are thousands of vendors selling security-related hardware, software, and services. Products include network management, anti-virus, encryption, and other tools. Services include code evaluation and security operations centers. However, integrating security tools into an operational business can be complicated, and poorly chosen or poorly implemented technologies can hide or even create security problems. Well-integrated tools will help make safer behavior a default (e.g., restricting and/or checking software installations for malware, and flagging the CEO's email request for an urgent vendor payment as actually coming from an external email system). An experienced CISO can evaluate security technology products and guide an organization toward those that are most effective and appropriate. Effective security requires an understanding of how to identify and manage risks and secure behavior. Tools help, but they are not the solution.

FOR BOARDS AND SENIOR EXECUTIVES

Recent standards set by the NACD[11] include an update that the association's affiliated boards are required to have direct access to information and cybersecurity expertise, as they are now being held responsible for the effectiveness of information and cybersecurity programs and strategy. These responsibilities include board review of identified information and cyber risks, – including legal implications, board approval of an enterprise-wide security strategy, ensuring that responsibilities and resources are appropriately allocated, and monitoring the effectiveness of these programs, including timely updates on critical incidents.

There is no such thing as perfect protection, so boards and executives need to identify which risks they are willing to accept and which they want to mitigate or avoid, a decision process that combines

[7] One source for incident response guidance is CERT, https://www.cert.org/incident-management/.
[8] Larry Ponemon, "2016 Ponemon Institute Cost of a Data Breach Study," *IBM – Security Intelligence*, June 15, 2016.
[9] NIST - Computer Security Resource Center, https://csrc.nist.gov/.
[10] ISO/IEC 27000 family - Information security management systems, https://www.iso.org/isoiec-27001-information-security.html.
[11] For additional information, see *NACD Director's Handbook on Cyber-Risk Oversight*, NACD, 2017.

business, legal, operational, technical, and security knowledge. Unfortunately, there is a significant gap in security expertise at the executive and board level in most organizations. There are not enough CISOs to go around.

CISOS AND VIRTUAL CISOS

A Chief Information Security Officer (CISO) is a senior-level executive responsible for establishing the information and cybersecurity strategy for an organization.

This individual has access and responsibilities to the board and senior executives, works closely with senior managers in all departments, and has the responsibility to integrate security considerations and protections throughout the company. Note, while a CISO can establish, lead, and supervise a security program, it requires the entire organization to execute it.

Regulations may require a company to designate a CISO; however, some individuals are assigned these responsibilities without the necessary experience and skills, which usually take 10-plus years to acquire. Hiring and keeping an expert may also be difficult, as there is a global shortage of qualified CISOs.

There is currently a shortage of qualified CISOs. The Rand Corporation reported global demand as 10x to 30x higher than the estimated 1,000 top-level security experts,[12] with over 100,000 unfilled information security positions in the United States.[13]

For companies and boards facing this expertise gap there is an alternative, which is to contract or outsource the CISO function on a part-time or advisory basis while retaining executive responsibilities within the firm. These part-time advisors are known as virtual CISOs, and they help companies leverage a combination of business, regulatory, technology, and security expertise. The NACD explicitly recognizes the benefits of virtual CISOs.[14] Experienced virtual CISOs can provide a range of supporting roles, including:

- Advising boards and senior executives on their information and cybersecurity responsibilities, presenting security risks and choices in a prioritized business context, and supporting the development, implementation, and monitoring of an enterprise security strategy.
- Mentoring internal security officers, accelerating their professional development, and providing guidance on priorities, projects, and purchases
- Advising or leading specific projects such as vendor selections, purchase decisions, and reviews of security plans, or prioritizing audit findings and coordinating their remediation (as it is sometimes easier for an outside expert to bridge internal hierarchies).
- While most of the above work can be scheduled in advance, virtual CISOs also can provide emergency support, such as for breach evaluation and recovery efforts. Ideally your organization has a ransomware plan already prepared, but getting external advice in a crisis still helps.

SECURITY PROCEDURES COME FROM THE TOP

As cyber risks increase, organizations that understand and implement effective security will be in stronger positions to protect their operations, data and customers against potential breaches, while meeting regulatory and best practice standards.

As with any corporate priority, security strategy needs to be set and supported from the top of the organization. With expert CISO or virtual CISO advice, board members and executives can appropriately incorporate security into their company's activities. For those that don't, the lack of preparation could be catastrophic.

This article was adapted from the white paper "Information and Cyber Security for the Futures Industry," published in October 2017 by VSEC, LLC, an information technology and cybersecurity advisory firm.

John Falck, MBA, MSc
Co-Founder, VSEC, LLC
+1.773.494.5292
john.falck@vsecllc.com

Michael Phillips, MBA, C|CISO, CISSP, ITIL, IAM, CISA
Co-Founder, VSEC, LLC
+1.312.504.3596
michael.phillips@vsecllc.com

[12] Martin Libicki, et al., "Hackers Wanted: An Examination of the Cybersecurity Labor Market," Rand Corporation, 2014.
[13] Steve Morgan, "Top U.S. Cybercrime Job Doesn't Pay," *Forbes*, February 10, 2016.
[14] NACD Resource Center: Cyber-Risk Oversight, https://www.nacdonline.org/cybercenter.