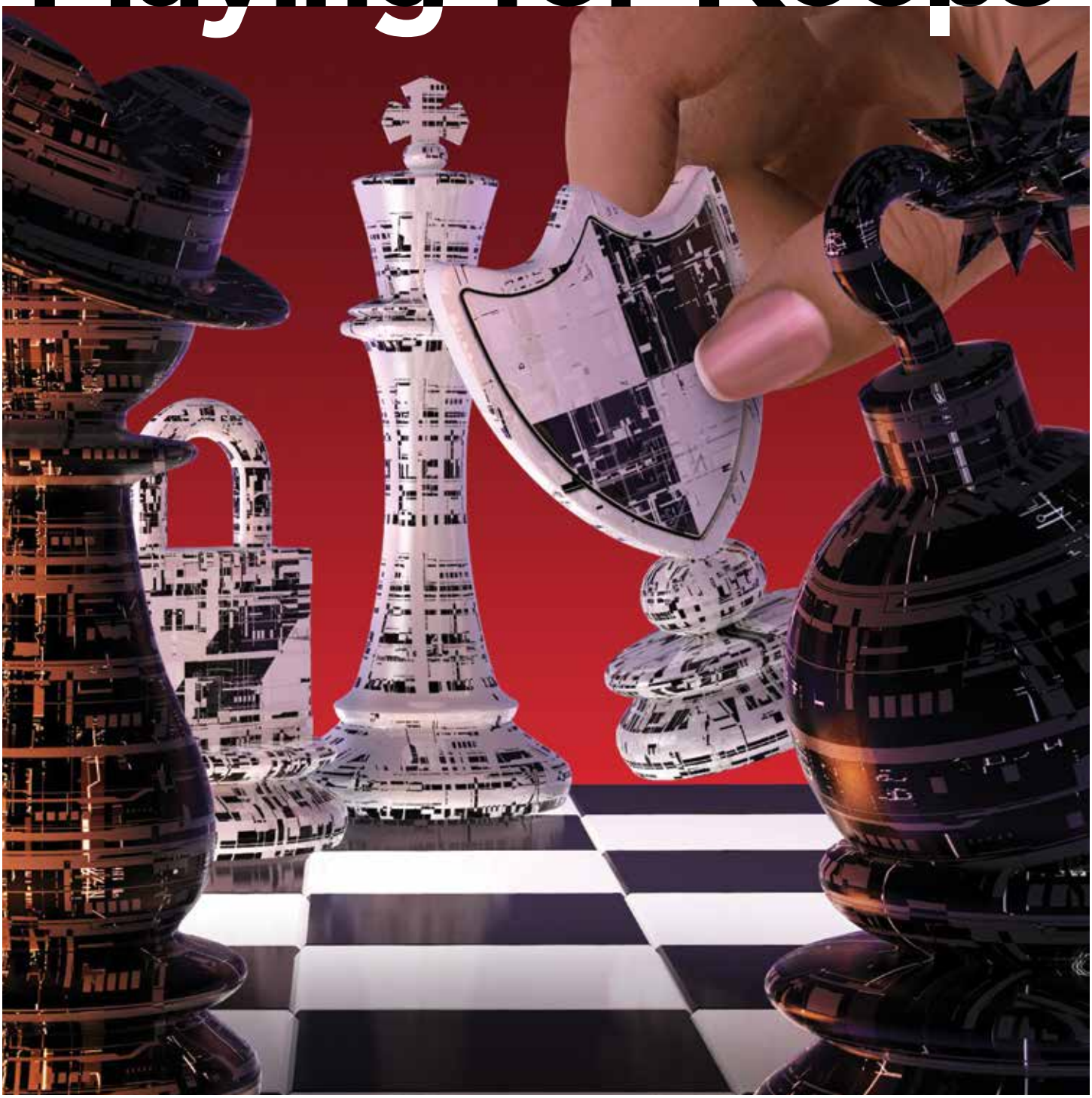
Playing for Keeps



Now that corporate directors have grasped the seriousness and perpetuity of cyber risks, they are seeking learning experiences to deepen their oversight knowledge and better understand the consequences of their failure to do so. Increasingly, the battle is being waged on two levels. The first is one of strategic gamesmanship: protecting a corporation's most valuable assets against human error or formidable armies of hackers motivated by greed, politics, or personal revenge. The second is being played mostly on the federal level, as various regulators and law enforcement agencies seek to identify the implications and consequenes of disclosure—specifically, how much a corporation should publicly reveal about their cyber vulnerabilities or the intrusions into their systems, to whom, and when. Is more transparency better?

Keeping cyber issues in check.

By Judy Warner

One source of such knowledge continues to be the Securities and Exchange Commission (SEC). As the type, frequency, and targets of cyberattacks have grown—recently labeled a "cyber pandemic" by one prominent law firm—the SEC has been working to determine whether greater disclosure is needed. SEC Chair Mary Jo White has sought input into how to provide investors with more accurate information about public companies' abilities to withstand cyberattacks without revealing or compromising their methods. In an SEC-hosted roundtable on cybersecurity in March, White called on the public and private sectors to be "riveted, in lockstep, in addressing these threats."

In April, the agency's Office of Compliance Inspections and Examinations (OCIE) issued a cybersecurity risk alert underscoring the importance being placed on cybersecurity preparedness. The alert contained a questionnaire designed in general to assess cybersecurity systems in the public markets. More specifically, it "intended to empower compliance professionals in the industry with questions and tools they can use to assess their firms' level of preparedness, regardless of whether they are included in OCIE examinations." The SEC has begun to examine the cyber "resilience" of more than 50 broker-dealers and investment advisors, advising other companies to evaluate their own resiliency by using the risk alert.

While each day brings new reminders of how difficult it is to make computer systems uncorruptible, there are signs that greater cooperation between the public and private sectors is yielding promising results. As this issue was going to press, for instance, the Department of Homeland Security (DHS) and the Secret Service issued a joint statement advising businesses that an investigation of the point-of-sale malware hack that had infected Target cash registers in 2013 has since infected more than 1,000 U.S. businesses "of all sizes."

While the scope of the infection is hardly reassuring, the fact that the malware was identified and other retailers warned highlights the importance of reporting incidents of cybercrime to law enforcement. The malware finding also shows that Target, the victim of a large and costly data breach in December 2013 in which more than 40 million customer records were compromised, is hardly alone in its vulnerability. (This is something Target investors seemed to realize when they voted the entire Target board back last proxy season despite a campaign by Institutional Shareholder Services to deny seven directors their seats.)

These recent federal actions build on a 2013 executive order from President Barack Obama that instructed the National Institute of Standards and Technology (NIST) to create a federal framework for organizations, regulators, and customers "to create, guide, assess, or improve comprehensive cybersecurity programs." The NIST "Framework for Improving Critical Infrastructure Cybersecurity," issued on Feb. 12, is intended to be used more broadly than the aforementioned OCIE questionnaire. The framework provides organizations with recommendations on how to determine their current level of cybersecurity preparedness, set goals for cybersecurity that align with their business environments, and establish a plan for improving or maintaining their cybersecurity.

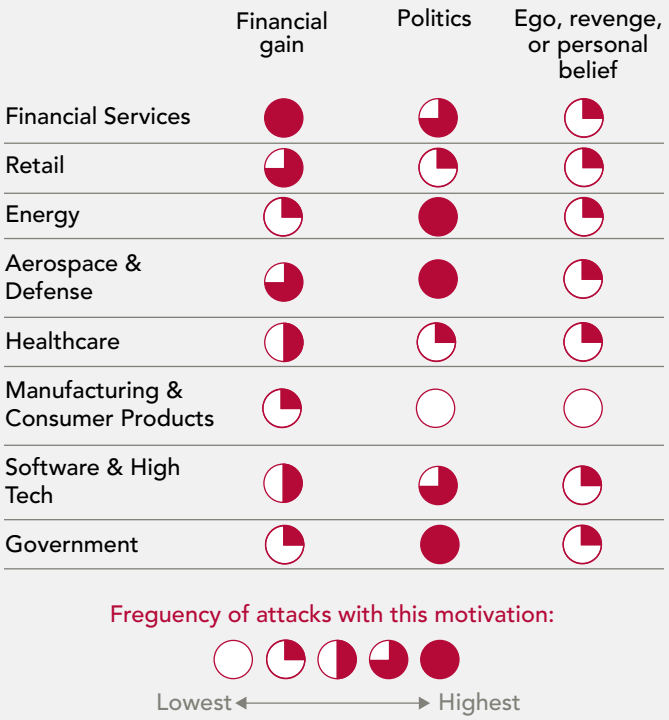
Even so, the debate over how and when to disclose cyber breaches continues to escalate. Cyber-specific disclosure guidance was first provided by the SEC in 2011, well before White was sworn in as the 31st chairman of the agency in 2013. That guidance, issued by the agency's Division of Corporate Finance on Oct. 13, 2011, stipulated that public companies "dependent on digital technologies" are obligated to report cybersecurity risks and material incidents with the caveat that such disclosures not be so detailed as to compromise security efforts. The non-binding guidance left it up to the individual company to determine materiality and how much detail to provide. In introductory remarks before the SEC's cyber

roundtable, White said the guidance "makes clear that material information regarding cybersecurity risks and cyber incidents is required to be disclosed."

Halfway through this year, 1,516 companies traded on either the NYSE or Nasdaq stock markets had included the words "cybersecurity," "cyberattacks," "hacking," or "data breach" in their securities filings, according to an analysis conducted and reported by *The Wall Street Journal*. That was up from 1,288 in all of 2013 and 879 in 2012. Disclosures range from providing some detail to boilerplate *(see samples, opposite page)*. Directors take note: there is plenty to be gleaned and learned from those who have gone before you. One of the more riveting disclosures, not surprisingly, was from Target, which has been fighting mightily to regain customer confidence since a 2013 data theft. In its most recent quarterly filing, the retailer disclosed that for the six-month period ending Aug. 2, data breach-related costs after an expected insurance payout of $46 million would reach $129 million. The retailer had previously reported that cumulative expenses related to the breach totaled $236 million, offset by insurance of $90 million.

Why Would They Attack Us?

Some businesses believe that because they are small or don't hold substantial amounts of sensitive or personal consumer data, such as credit card numbers or medical information, that they are unlikely to be the victims of cybercrime, writes Larry Clinton, president and CEO of the Internet Security Alliance, and author of the *NACD Cyber-Risk Oversight* handbook. Yet any Internet-connected business may be vulnerable. What motivates attacks? A recent report by PwC and the IRRC Institute charts the preponderance of motivation by industry.



Source: "What Investors Need to Know About Cybersecurity: How to Evaluate Investment Risks," PwC IRRCi, June 2014

What Also Bears Watching

In addition to keeping an eye on cyber-related developments on the regulatory front, the legislature bears watching. So far, 47 states plus the territories have enacted breach-notification laws, according to the National Conference of State Legislatures. These laws typically stipulate what firms or government agencies must comply, types of personal information, what constitutes a breach, and methods of notification.

The latest read from Capitol Hill is that federal legislation—at least in the near term—is unlikely. Should the size and scope of data breaches continue to dominate the headlines, however, there is little doubt that legislators will heed the cry for some kind of fix. DHS Director Jeh C. Johnson says his agency has reached the extent of its capabilities and requires action to "codify" its power to facilitate the work of public-private initiatives. "Some private companies can and do resist sharing information with DHS about cyberattacks on their systems, for fear of potential liability," Johnson wrote in a recent op-ed published by The Hill.com.

That fear is well founded. The plaintiffs' bar is circling, according to Stanford Law Prof. Joseph A. Grundfest: "We are beginning to see litigation activity directed at boards of companies that have experienced cyber breaches. These lawsuits manifest themselves in the form of derivative litigation, alleging that the board was derelict in its duties of oversight and care, or in the form of class action securities fraud litigation, if the company's stock price suffers as a result of the breach and plaintiffs can allege some form of omission or misrepresentation by the company."

The takeaway from all of this activity? Back to the SEC's springtime roundtable. Participant Peter Beshar, general counsel at Marsh & McLennan, while noting that sales of cyber-specific insurance policies are on the upswing, advised that public, private, and nonprofit sectors continue to work together toward cybersecurity solutions. Noting that the the NIST framework is "inherently flexible," he added, "What's clear is that government, business, and the non-profit world need to partner together to figure out what's the best way to respond because we surely know that our adversaries are adjusting their tactics as we speak."

Samples of Cyber-Risk Disclosures

JPMORGAN CHASE & CO.

"The Firm is working with appropriate government agencies and other businesses, including the firm's third-party service providers, to continue to enhance defenses and improve resiliency to cybersecurity threats."

Source: JPMorgan Form 10-Q filed with the SEC, August 4, 2014

WELLS FARGO

"To date we have not experienced any material losses relating to cyber attacks or other information security breaches, but there can be no assurance that we will not suffer such losses in the future. Our risk and exposure to these matters remains heightened because of, among other things, the evolving nature of these threats, the prominent size and scale of Wells Fargo and its role in the financial services industry, our plans to continue to implement our Internet banking and mobile banking channel strategies and develop additional remote connectivity solutions to serve our customers when and how they want to be served, our expanded geographic footprint and international presence, the outsourcing of some of our business operations, and the current global economic and political environment."

Source: Wells Fargo & Co. Form 10-K filed with the SEC, Feb. 26, 2014

GOLDMAN SACHS

"A failure in our operational systems or infrastructure, or those of third parties, could impair our liquidity, disrupt our businesses, result in the disclosure of confidential information, damage our reputation, and cause losses."

Source: Goldman Sachs Form 10-K filed with the SEC, Feb. 27, 2014

FACEBOOK

"Computer malware, viruses, hacking and phishing attacks, and spamming could harm our business and results of operations."

Source: Facebook Form 10-K filed with the SEC, Jan. 31, 2014

TWITTER

"Computer malware, viruses, hacking and phishing attacks, and spamming could harm our business and results of operations."

Source: Twitter Form 10-K filed with the SEC, March 6, 2014

CVS CAREMARK

"The failure or disruption of our information technology systems, our information security systems and our infrastructure to support our business and to protect the privacy and security of sensitive customer and business information."

Source: CVS Caremark Form 10-K filed with the SEC, Feb. 10, 2014

GOOGLE

"If our security measures are breached, or if our services are subject to attacks that degrade or deny the ability of users to access our products and services, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.…We experience cyber-attacks of varying degrees on a regular basis, and as a result, unauthorized parties have obtained, and may in the future obtain, access to our data or our users' or customers' data. Our security measures may also be breached due to employee error, malfeasance, or otherwise. Additionally, outside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information in order to gain access to our data or our users' or customers' data. Any such breach or unauthorized access could result in significant legal and financial exposure, damage to our reputation, and a loss of confidence in the security of our products and services that could potentially have an adverse effect on our business. Because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and often are not recognized until launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose users and customers."

Source: Google Form 10-K filed with the SEC, Feb. 11, 2014

NEIMAN MARCUS GROUP

"A material disruption in our information systems could adversely affect our business or results of operations.…We rely on our information systems to process transactions, summarize our operating results and manage our business. Our information systems are subject to damage or interruption from power outages, computer and telecommunications failures, computer viruses, cyber-attack or other security breaches and catastrophic events such as fires, floods, earthquakes, tornadoes, hurricanes and acts of war or terrorism."

Source: Neiman Marcus Group Form 10-K filed with the SEC, Sept. 25, 2013

Thinking Strategically About Cyber Risk

Safety and resilience will be transformational for today's companies that view Internet security not as an expense but an investment, says the former Secretary of Homeland Security, Tom Ridge.

By Adam J. Epstein

The Hon. Tom Ridge is the CEO of Ridge Global, a firm that helps businesses and governments address a range of needs throughout their organizations, including risk management, global trade security, emergency preparedness and response, strategic growth, infrastructure protection, technology integration, and crisis management. With former White House cybersecurity czar Howard A. Schmidt, he also co-founded Ridge-Schmidt Cyber, a consulting firm that provides insight, threat intelligence, and strategic advice to C-suite and board-level executives on 21st-century cybersecurity challenges.

Following the tragic events of 9/11, Ridge became the president's first assistant for homeland security and, on Jan. 24, 2003, became the first secretary of the U.S. Department of Homeland Security. The creation of the country's 15th cabinet department marked the largest reorganization of government since the Truman administration. During his tenure as secretary, Ridge worked with more than 180,000 employees from a combined 22 agencies to create an agency that facilitated the flow of people and goods; instituted layered security at air, land, and seaports; developed a unified national response and recovery plan; protected critical infrastructure; integrated new technology; and improved information sharing worldwide.

Previously, Ridge was twice elected governor of Pennsylvania, serving as the state's 43rd governor from 1995 to 2001. Prior to his gubernatorial tenure, he was elected to Congress in 1982. He was one of the first Vietnam combat veterans to serve in the U.S. House of Representatives—Ridge served as an infantry staff sergeant in Vietnam, earning the Bronze Star for Valor, the Combat Infantry Badge, and the Vietnamese Cross of Gallantry—and was re-elected for five successive terms.

Ridge also has served on the boards of several companies, including The Hershey Co., and has received numerous honors including the Woodrow Wilson Award, the Veterans of Foreign Wars' Dwight D. Eisenhower Award, the John F. Kennedy National Award, the Ellis Island Medal of Honor, the American Bar Association's John Marshall Award, and the National Guard's Harry S. Truman Award.

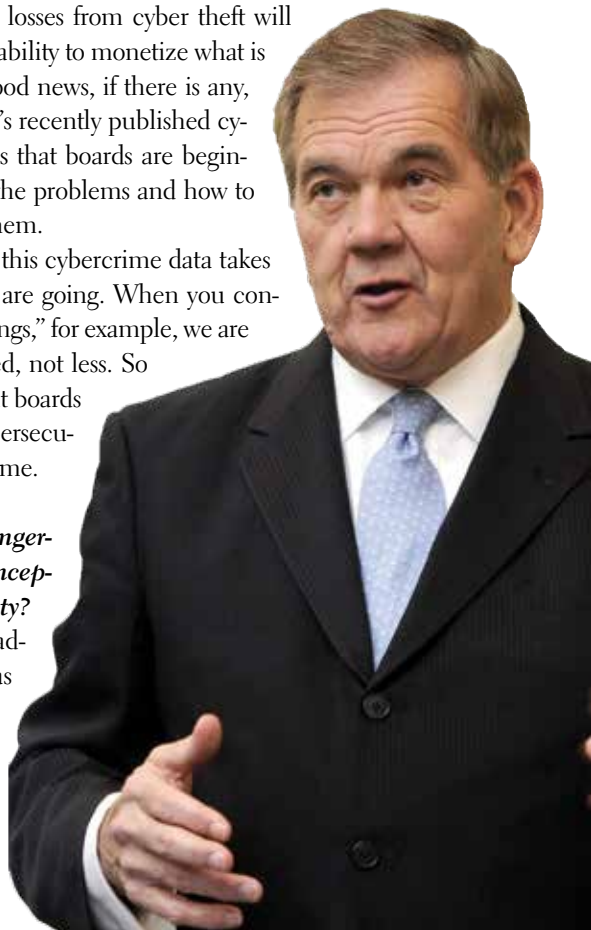
We hear daily about the need for cybersecurity, but would you help directors better understand the scope of the problem they are facing?

I saw some statistics from a study by the Center for Strategic and International Studies [CSIS] in June 2014 that every director should be aware of: at least 3,000 U.S. companies were the victims of some kind of hack last year and the global cost of cybercrime is estimated to exceed $400 billion. [*See related sidebar, page 34.*] The bad news is that these numbers could actually be quite a bit higher, since some of these costs are very hard to measure. The CSIS report also made what I thought was an instructive observation, especially for small public companies and soon-to-be public companies. That is, cybercrime is in essence "innovation cannibalism." Their point, I think, was that cyber theft is in some sense a tax on innovation, meaning that losses from cyber theft will continue to grow as the ability to monetize what is stolen advances. The good news, if there is any, as evidenced by NACD's recently published cybersecurity handbook, is that boards are beginning to really focus on the problems and how to constructively address them.

All that said, none of this cybercrime data takes into account where we are going. When you consider the "Internet of things," for example, we are growing more connected, not less. So I think it's safe to say that boards will be focusing on cybersecurity for a long time to come.

What are the most dangerous, widely held misconceptions about cybersecurity?

First, far too many leaders view cybersecurity as just an information technology [IT] or technology problem.



ASSOCIATED PRESS

That approach is simplistic and destined to fail. There is a context of security within organizations that must be created and led. Technology exists in that context; it is not the context itself.

What do you mean by that?

Cybersecurity is the responsibility of senior leaders who are responsible for creating an enterprise-wide culture of security. It is about aligning IT with business competencies. It is about a well-informed board and C-suite that make security decisions not based on the musings of a business show talking head but from utilizing an informed, risk-based approach.

Ask yourself this question: What business today, large or small, does not have its most important communications and information, intellectual property [IP], strategies, plans, customer, employee, and transactional data traversing its networks? So forget about cybersecurity only being a responsibility for the IT department. Ask the last CEO at Target if that strategy works.

Second, some C-suite leaders and board members are under the impression that somehow you can build an electronic fence around your entire operation to keep the "bad guys" out. This oversimplifies the challenge and really frustrates the technical staff who are combatting threats that are not just external—such as hackers, criminal organizations, and nation-states—but possibly internal, such as employees either accidentally or intentionally enabling a breach, as well as former employees, contractors, or vendors with access. You cannot eliminate cyber risk but you can manage it. You can become more secure and resilient, but it requires leadership across an organization. This requires a new level of understanding, and board members need to be better educated about cyber issues in order to perform their duties.

Most small and mid-sized companies understandably lack the time and resources to study their adversaries in terms of their motivations, skills, and resources to conduct malicious cyber activities. But corporate leaders of any size organization need to consider what information adversaries seek and why—whether it's intellectual property, customer data, negotiation strategies, or something else. By clearly understanding adversary motivations, corporate leaders can more easily identify vital assets and information and make more effective cybersecurity investment decisions.

Your firm has had the benefit of advising heads of state and Fortune 50 companies on cybersecurity. What can directors learn from their actions or omissions?

Company leaders, regardless of the size of the business, must learn to ask the right questions. Whether you run a global company or a local family business, at the end of the day, the CEO will be held accountable by your customers, shareholders, and the public. They may not know the names of the people in the information security office, but they know the names of those who manage the brand. Company leaders have to ask themselves if they have done what they can to minimize cyber risk. Have they identified the company's "crown jewels" and understand how they may be at risk according to the company's cyber profile? Do corporate policies and governance complement security technology? If a breach does occur, are you prepared to deal with its wide-ranging implications? Do you have a response plan? How will you determine the source of the breach? Who will help you fix it? Internally, who will be in charge of the various aspects of the response? Who will provide information to your employees, your customers, and to the press? Do government officials need to be notified? Are there legal and regulatory compliance implications for your business? Have your IT, security, human resources, communications, and legal teams met jointly or conducted exercises to explore these matters?

If you consider even this small universe of questions, you see that you cannot view cybersecurity just as a technology issue but as a business imperative.

As reported in a June 8 story in* The New York Times, *cyber insurance hasn't been terribly effective to date in mitigating cyber risk. What changes are likely in that regard, and what do boards need to know?

Looking into the near future, I see cyber insurance playing a larger role in helping companies—especially small- and mid-cap—mitigate risk. Small companies can affordably look for an assessment process that will help make them aware of their cyber and reputational vulnerabilities. This can be achieved in conjunction with either the insurance review or the risk review process. The fact is, insurance is important for closing or strengthening the "value chain" of cybersecurity; for protecting against cyber theft that most assuredly will happen. Insurance can be not just a "policy" written by an agent but a true focal point for assessing, correcting, and even predicting the cyber world and its impacts on your business.

Boards also should be aware of the voluntary NIST Cybersecurity Framework, released in February 2014, which will likely become a *de facto* standard of care in legal proceedings stemming from cyber events. At this time, NIST is talking with major insurance companies about utilizing the framework during the policy issuance process to more clearly ascertain corporate cyber-risk positions.

High Costs of Cybercrime

- The annual cost of cybercrime to the global economy is estimated to be in excess of $445 billion.
- In 2013 alone, cybercrime likely cost more than $200 billion in the United States, China, Japan, and Germany.
- The cost of individual identification theft is estimated to be approximately $160 billion annually.
- Some 40 million people have had their information stolen by hackers in the United States.
- Approximately 3,000 U.S. companies were hacked in 2013.
- Annual GDP losses due to cybercrime are estimated at 0.5% to 0.8%.
- Cybercrime could translate into more than 200,000 lost U.S. jobs.

Source: Center for Strategic and International Studies, June 2014

The valuable intellectual property of tomorrow resides today in pre-IPO and small-cap companies, yet these companies have the least resources to protect against cyber theft. Where does that realistically leave directors of these companies in effectively overseeing cyber-risk management?

You just touched on it—oversight. Oversight is not simply asking the CIO if the company is secure and taking their word for it. For anyone trying to protect IP, cybersecurity must be a priority because in many cases the IP *is* the business. Proper oversight requires directors not only to educate themselves about the threats to the business and to learn to ask the right questions but to work with the technical staff to ensure that cybersecurity spending is prioritized to protect the crown jewels. This is particularly important when budgets are limited.

Board members are usually focused on business metrics, so we must apply a similar level of scrutiny to the cybersecurity spend, as well as to the broader enterprise risk management practice. This is not a challenge that will be going away anytime soon. I call it the "digital forevermore." For board members, cybersecurity oversight is a critical part of fulfilling their fiduciary responsibilities.

It is remarkable to me that companies will comb through the numbers on the business side of the house looking for an extra one or two percent of growth. Meanwhile, they are losing that much each year due to inadequate risk management practices. Too many businesses simply view cybersecurity—and security in general—as an expense. It must be viewed as investment. Just as Deming's quality revolution was transformational in the 20th century, business security and resilience will be transformational in the 21st. Companies that understand this, especially those with a global footprint or supply chain, will have a competitive edge as we see an increasing number of potentially disruptive events.

All board members can't be expected to have deep technical knowledge, but they must have an understanding of cyber risk and key adversaries in order to make informed investment decisions for corporate IT systems. To meet this requirement, all boards should complete continuing education programs to develop deeper knowledge on embedding cybersecurity within conventional risk oversight responsibilities.

Homeland Security Secretary Tom Ridge speaks in front of New York City Mayor Michael Bloomberg (left) and New York Gov. George Pataki in 2003.

ASSOCIATED PRESS

In the early days of the Internet, every intellectual property and technology lawyer refashioned themselves as an expert in Internet law. Similarly, many IT firms are now suddenly cybersecurity experts. What should boards be looking for when selecting individuals or firms to advise them regarding cybersecurity?

It is critical to have advisors with a true enterprise perspective. In our cyber consultancy work at Ridge-Schmidt Cyber, we see companies that have hired some of the best forensics firms or leading-edge technology companies, but the functions are not effectively coordinated. This can produce costly overlaps or, of greater concern, leave critical gaps in an IT security program. And we have to remember that some cybersecurity breaches can be enabled by physical security failures, so IT security must be part of a comprehensive enterprise security and resilience program. Company leaders should not be distracted by the hottest new technology or specialty firm. The primary focus needs to be on managing a solid, risk-based program. Then you can effectively leverage the right technology and specialty firms to implement the enterprise strategy.

Companies have come to us in post-breach situations, and what we have found is that they address

cyber and physical security separately, and it's to their detriment. We have seen physical security deficiencies such as poor access control lead to cybersecurity breaches. If a company lacks appropriate policies and procedures for employees, vendors, and contractors who have access to or work near pertinent corporate IT infrastructure, your risk will be higher. And it's the simplest of errors that can be the costliest. Firms should engage third-party consultants that understand both the interplay between cyber and physical security risks and the most effective ways to mitigate these risks in a coordinated fashion.

Another reason boards, and small-cap boards in particular, should do their best to engage third-party advisors is the existing talent gap and supply-demand imbalance with information security professionals. It's difficult to fill corporate IT security openings with highly qualified candidates with deeply relevant past experience, certifications, and other credentials, as many of these candidates already work for consultancies and larger corporations in well-compensated positions.

What can directors learn from the way your firm undertakes proactive cybersecurity assessments and audits?

You have to be proactive in both how you organize and how you manage cyber risk. Most executives weren't taught this kind of risk management in business school. Yes, cybersecurity is about IT's ones and zeros, but it's also your bottom-line ones and zeros. Your business is on your networks and systems, so cybersecurity must be treated as the business imperative that it is.

The cyber and IT leadership needs to be properly situated both on the org chart and in practice. The seniority of a CIO or similarly accountable official often tells us how seriously an organization manages cybersecurity. The C-suite and board should be coordinating with those leaders regularly, not just when there is a crisis. Communication is critical.

Budgets should provide for regular cyber audits and assessments, just as you would for financial risk management and oversight. This will help you be proactive, to protect your systems as the threat environment quickly evolves and bad actors develop new tactics.

It is also important to note that while corporations spend millions conducting financial due diligence on companies or products they are looking to acquire, few conduct cyber due diligence. When you buy a company, you also are buying their networks—gaps, liabilities, and all. That risk needs to be evaluated. Too many companies are willing to take the risk that the "bad guys" won't get into their system and cause a business-interrupting breach. News flash: They may already be there.

Protecting Your Board Books

By Jeff Hilk and Jeffry Powell

Secure communication is essential to keeping organizations running smoothly without disruption. This is especially true for a company's board, which is privy to sensitive, confidential, and market-moving information. Ensuring that board members are well educated and aware of cybersecurity risks is the first step to protecting a company's board materials.

For companies that regularly communicate highly confidential and sensitive information, board portal technology provides a way to grant secure access to the critical documents needed by directors and officers to fulfill their duties without sacrificing the flexibility provided by mobile devices. Today's portal technology far outpaces the static access of paper-based communications and limited security of file-sharing and annotation software.

Board members should embrace communication through a portal as a means to strengthen existing security processes. Information must be fully password protected with a unique set of keys for each user, and the data must be encrypted at rest, in transit, and on the users' devices. Nothing material should ever be communicated via e-mail in order to prevent inadvertent oversharing and ensure confidential information remains in the control of the company.

Public cloud-based file-sharing services should also be avoided, with reliance instead on privately hosted solutions. While public cloud solutions can offer easy uploading and downloading of files as well as security features such as encryption and authentication, many have been successfully hacked, compromising private files and e-mail addresses.

A secure board portal is hosted privately, meaning clients' data is on secure, dedicated hardware and servers, not hosted in the third-party or virtualized environments that characterize the public cloud. Board portals also allow companies to control logical access to their data based on the nature of their business and the overall threat level.

To face the ever-complex and digital corporate landscape, board members must educate themselves on cybersecurity. Understanding the risks and awareness of protective measures are two simple, yet effective, ways to defend a company against potential cyberattacks.

Jeff Hilk is executive vice president and director of client services, and Jeffry Powell is executive vice president, Americas, for Diligent Board Member Services.