Wharton
University of Pennsylvania

SULLIVAN & CROMWELL LLP | RANE Risk Assistance Network + Exchange | KNOWLEDGE@WHARTON

DECEMBER 2015

CORPORATE GOVERNANCE IN THE AGE OF CYBER RISKS

Corporate Governance in the Age of Cyber Risks

CORPORATE BOARDROOMS ARE WAKING UP TO THE ENCROACHING, SYSTEMIC THREAT OF CYBERSECURITY RISKS. But while awareness is growing — more than 80% of boards now discuss cybersecurity at most, if not all, of their meetings — many directors simply are not sure if they have the information and tools at their disposal to provide effective oversight of top management to handle today's hacking dangers, especially intrusions sponsored by nation-states.

Information and expertise in this area are scarce. Companies have demonstrated a reluctance to disclose data breaches and have been cautious in contacting authorities. The government has made some efforts to encourage public-private cooperation but at the same time has sought to hold the private sector responsible for data breaches. These and other factors, including concerns over costs and uneven levels of technological expertise, have contributed to the information and expertise deficit. At the recent "Cyber Risks in the Boardroom" conference in New York City, leading experts in the public and private sectors shared their perspectives for directors as they navigate these uncharted waters.

> "Regulators and policymakers increasingly expect that board members and senior managers have a sufficient grasp of cybersecurity core principles."
>
> — Simon McDougall, Promontory Financial Group

It is clear that cybersecurity is no longer chiefly the domain of CIOs, CISOs and IT departments, but rather a companywide and nationwide concern that demands oversight and direction from the boardroom and the broader community. "Nonspecialist executives and board directors all play a role in determining whether a company's dedicated cybersecurity professionals have prepared the firm for the cybersecurity risks it faces," said Simon McDougall, managing director and head of the cybersecurity practice at Promontory Financial Group. "Regulators and policymakers increasingly expect that board members and senior managers have a sufficient grasp of cybersecurity core principles and can collaborate with and challenge a firm's cybersecurity specialists."

McDougall said the principles of good operational risk management also apply. And engaged directors and executives should ask questions about the type of scenarios the firm must plan for — whether the range of identified risks is complete, how resources are prioritized, what lessons one might learn from incidents and near misses, and whether the cybersecurity risk management function is competent and has sufficient resources.

Investors are increasingly aware of the dangers breaches pose to companies and should be expected to hold boards and CEOs responsible if companies do not manage cyber risks effectively, including dealing with cyber intrusions, which virtually all conference participants agreed are inevitable.

And the threat is escalating: The widespread use of mobile devices, social media, and cloud computing, as well as potential vast digital expansion with the so-called Internet of Things (IoT), have ushered in several asymmetric

or unconventional threats. These range from the lone hacktivist to organized crime and nation-states. It is now clear that traditional corporate firewalls do not offer adequate protection, according to speakers at the cybersecurity conference, which was organized by Sullivan & Cromwell, RANE (Risk Assistance Network + Exchange) and Knowledge@Wharton, in collaboration with AIG, Spencer Stuart and the John Jay College of Criminal Justice. This report was also informed by subsequent strategic conversations with a wide range of experts due to the evolving threat environment around cybersecurity.

Moreover, the frequency and diversity of cyber attacks have increased. In 2015, prominent breaches included Iran's hacking of email and social media accounts of Obama administration officials, attacks on the Ashley Madison adultery website, several Trump Hotels, CIA Director John Brennan's personal email account, U.K. telecom giant Vodafone and two breaches of the U.S. Office of Personnel Management — in which personal and security clearance records of at least 21.5 million government employees, contractors, applicants and their family members were stolen. The OPM hack is thought to be one of most far-reaching breaches of government security in history, and it ultimately cost the agency's director her job.

"The cyber threat is one of the most significant economic and national security risks we face, and the inability to effectively address this threat will have long-lasting implications," said Shawn Henry, president of CrowdStrike Services and CSO of CrowdStrike Inc. "Adversaries including organized crime groups, terrorists, and nation-states, are constantly seeking to access organizations' most sensitive and valuable information through remote-access attacks. Boards of directors and the C-suite must acknowledge and recognize this business risk, and work to detect and respond to them quickly to mitigate the consequences. The leadership must set the pace for the rest of the organization, and it starts with awareness of the threat and a sense of urgency to respond. Anything less is unacceptable."

Cyber thieves have become more brazen, too. This year, hackers demanded a ransom after stealing the personal information of customers of TalkTalk, one of the largest communications companies in Britain. And in the past two years, the Carbanak hacking group has stolen an estimated $1 billion from more than 100 banks in 30 countries. In 2014, there were 800 tracked U.S. data breaches, speakers said, and data on half of the U.S. adult population was exposed as well in just the last 12 months. "The cyber battlefield has expanded dramatically," one national security expert noted.

A 2015 survey by the NYSE Governance Services and Veracode shows the extent to which boardrooms are unprepared to deal with cyber attacks. While more than 80% of directors say they discuss cybersecurity at most if not every meeting, 66% still lack confidence in their company's ability to protect itself against hacking. Their biggest fear — noted by 41% of respondents — is brand damage due to loss of customers. Other concerns include the cost of responding to the breach, the loss of competitive advantage as a result of corporate espionage, and regulatory and compliance violations. When it comes to accountability in the event of a major breach, directors place the responsibility first on the CEO, CIO and the entire executive team before the CISO, and themselves.

"The leadership must set the pace for the rest of the organization, and it starts with awareness of the threat and a sense of urgency to respond. Anything less is unacceptable."

— Shawn Henry, CrowdStrike Inc.

CALL FOR CLOSE PUBLIC AND PRIVATE SECTOR COORDINATION

Cybersecurity, including a hacking response plan, is a must-have for enterprises of all sizes. Conventional wisdom dictates that companies in the defense industry, or those controlling critical infrastructure and essential services face the biggest cyber threats, while larger corporations operating in less critical areas such as retail are thought to face medium-level risks and small businesses have the least exposure. But such thinking is too simplistic. "If you happen to have something the attack team is looking for, or happen to be in the wrong place at the wrong time, then you're going to get attacked," said one Fortune 500 company executive. "It doesn't matter if you're big, little, important or not important."

Andrea Little Limbago, principal social scientist at Endgame, holds the same view. "Many organizations still underestimate the threat if they are not in the defense or financial sectors. Even those in some critical infrastructure industries have yet to truly grasp the possibility that they are targets," she said. "Many still view the threatscape as solely comprised of targeted attacks at high-profile corporations and the public sector.

This myopic view of the threatscape fails to consider the range of opportunistic actors that attack based more so on a combination of ease of access (vulnerabilities) with the potential return. Opportunistic malicious actors seek a high return on investment, constantly perusing the landscape for opportunities for easy breaches with high rewards. Because of this, every organization must prioritize and focus defensive efforts on their most essential data and applications instead of spreading their resources too thin."

The Target data breach, for instance, was carried out by hackers who stole network credentials from a small heating and cooling subcontractor plugged into the retailer's systems. A major enterprise in Washington was hacked through a thermostat in a remote building that was wirelessly connected to its main network, one speaker said. These types of cyber attacks are fluid and ongoing. "We are in a race against time," another speaker said.

> **"Many organizations still underestimate the threat if they are not in the defense or financial sectors."**
>
> — Andrea Little Limbago, Endgame

"Cybersecurity is a complex and multi-dimensional issue. The technology and tools available today are extremely advanced and do a great deal to prevent and detect intrusions," added Dan Wachtler, CEO of IPSA International, a root9B Technologies Inc. company. "However, the more we look at the challenge, the more we realize the largest gap in our cybersecurity posture relates to the human element. Insider and training issues will continue to be a problem, but it is also critical to understand that behind every hack is a hacker, in other words, a human being. You cannot build an automated solution to stop a determined human, you must think like the adversary and execute your plan based on a combination of technology and manned information security strategies."

But companies should not be discouraged from mounting a proper defense, even if cybersecurity problems seem to be overwhelming. While businesses cannot completely eliminate cyber risks, they can manage them just like other risks and do so without overspending. "That means making investments to power down the risk without bankrupting yourself," one speaker said. "Driving down the risk is worth doing."

Consider this: If not managed properly, the fallout from a breach could be far worse in terms of damage to company reputations, decreased revenue and declines in market value. It is also simplistic to think that China and Russia, thought to be the origin of many hacks, among other countries, would not damage the global economy in which they play major roles. For one, the Chinese have a "different calculus about the importance to them when it comes to protecting their monopoly of power," one speaker said.

H. Rodgin Cohen, senior chairman of Sullivan & Cromwell, a leading global law firm, said in his keynote address that these hacking attacks represent "one of the truly existential threats to a wide swath of American industry." He noted that bank systems closed down by hackers could spur a run on money and create a crisis of confidence, while a hacked utility company could mean no heating for millions of homes in the dead of winter.

Cohen also called for closer collaboration between businesses and the government to fight these threats, even advocating an "effective retaliation policy" on nations if an attack could be traced to their territory, citizens or residents. The interconnectedness of today's global economy underscores the seriousness of such hacks because one compromised link could infect the whole system. "We really are all in this together," Cohen said. "The enemy is not us. It is them."

(In a 2015 opinion piece for Knowledge@Wharton, RANE founder David Lawrence and other distinguished authors laid out a plan for business and government to work together effectively in their fight against cyber attacks.)

IMPERATIVES AND REALITIES FOR DIRECTORS

It is critical for boards and senior management to be realistic about what they can and cannot do. "Unless you're an extremely large company that can spend a lot of money on new technology, re-engineering your environment, hiring a large and comprehensive cyber security team … you have to move to the cloud or seek some external service partnerships," said a top executive for a major company.

Businesses could consider using the corporate, not personal, cloud services of tech giants such as Google, Amazon and Microsoft to keep their data and systems secure. "You look at the thousands of high-end security engineers maintaining the Google corporate cloud — I don't know how you can think you can better protect yourself when you have that apparatus to use," he said. While companies do take on some level of risk by moving

their data to the cloud, the benefits more than offset the disadvantages.

Companies that want to take a more active role in their cyber defenses should organize efforts under five themes: awareness, governance, systems, process and strategy. One speaker said businesses must be aware of the types of cyber threats they face, where they are vulnerable — such as connections to third-party vendors — and whether the firm is systemically relevant. Defense companies know they are prime targets, but smaller financial institutions and retail companies do not gauge their value to hackers often enough, though the level of awareness is rising following hacks on Target, Sony and JPMorganChase. Moreover, businesses must determine their level of risk tolerance and the extent of their cybersecurity budget.

"A proactive cyber offense is critical in today's environment. It's not enough to just invest in the right tools or have a strong defense in place. In order for an organization to truly embark on the pathway toward cyber resilience it's also necessary to proactively hunt for cyber criminals who might already be lurking in an organization's network," said Erin Nealy Cox, executive managing director at Stroz Friedberg. "Cyber risk is an enterprise risk issue and requires the active inclusion of all board members in the cyber risk discussion. Organizations should establish a cyber-risk committee with a charter that mandates cyber education for its board. Once boards are properly educated about cybercrime, a proactive cyber offense will be a natural outcome."

Under principles of corporate governance, companies must analyze whether their organizational structures are set up to deal with cybersecurity issues because it clearly is an enterprise-wide problem, not just a technology issue, according to conference speakers. Directors should ask the right questions about security and have an ongoing dialogue with their CIOs and CISOs. They should also consider adding a director with a technical or security background to the board or bringing in consultants.

As for systems, businesses must look at how they approach data protection, insider threat monitoring, layers of defense, and building of redundancy and response around critical areas of vulnerability. Of significant importance is the process for addressing a hack or other intrusion. Finally, because resources are limited, companies must think strategically in the way they measure the risks and assess countermeasures.

Speakers urged companies to prepare as follows for a cyber attack:

Risk assessment. Companies should identify the key assets they wish to protect — such as customers' personal information, intellectual property, sensitive financial data and the like. "As you inventory your assets, you can begin to segment your network and understand what needs to be relatively open and what needs to be tightly closed," one speaker said. "Who should have access? Who is given administrator privileges? What kinds of ID do they need? Will it have single-factor or multi-factor authentication? How often do you monitor your network?" Moreover, find a way to contain breaches that could be introduced by third-party vendors.

"The largest gap in our cybersecurity posture relates to the human element. … behind every hack is a hacker, in other words, a human being."

— Dan Wachtler, IPSA International

Incident response team. To have an effective response, it is critical to have a team in place ahead of an incident. This team should include, at a minimum, top executives from operations, IT, HR and compliance, communication and the general counsel. Companies should also have contacts within the FBI and other law enforcement so they can tap government resources as they work together to contain the breach and find the perpetrators. The government has established various contacts around the globe to help companies address attacks from inside and outside the U.S. It can also fight hackers directly — something companies are advised not to do (and for the most part, not allowed to do) themselves.

Share information. Consider joining ISACs, Information Sharing and Analysis Centers, or ISAOs, Information Sharing and Analysis Organizations. ISACs are organized around sectors and companies that do not fall neatly into a sector can opt to join an ISAO. Members share information about the their breaches and responses. However, one security chief's concern is that companies are reluctant to share exactly how they were compromised because they do not want to divulge points of vulnerability. "When something bad happens, let's talk about how to close that vulnerability, not just share who the attacker was, what the malware was and where the attack came from," he said.

Another resource is the National Cyber-Forensics & Training Alliance in Pittsburgh, which helps with

information sharing among businesses, law enforcement and academia. Soltra, a joint venture of the Financial Services Information Sharing and Analysis Center and The Depository Trust and Clearing Corp., offers a software automation service that collects and distributes intelligence on threats to guard against cyber attacks.

Speakers said law enforcement agencies detect malicious activity when it is on its way out of a network, not as it goes into a system, so it is difficult to warn companies ahead of time. But they assured companies that they should not be worried about calling the FBI or other government security agency for fear of opening themselves to an investigation. In a time of crisis, law enforcement's main goal is to catch perpetrators.

> **"It's not enough to just invest in the right tools or have a strong defense in place ... it's also necessary to proactively hunt for cyber criminals who might already be lurking in an organization's network."**
>
> — Erin Nealy Cox, Stroz Friedberg

Test the response plan. Participants advised companies to create an instant response plan and put it in practice regularly. A mistake many companies make is to develop a plan and then let is sit on a shelf. So when an attack occurs, they are caught unprepared and may have to execute a stale plan, whose chief architects may have since left the firm. A plan should have a practical and flexible strategy of communicating internally as well as with customers, regulators, law enforcement, analysts, reporters and investors. One speaker recommended testing the plan once or twice a year for six to eight hours at a time. The plan should then be updated to reflect the results of the testing, including responses for different scenarios, lists of people to mobilize, potential press statements, lists of potential legal obligations and mandatory and advisable disclosures.

Fulfill legal obligations. In general, most states have passed statutes requiring that, if a customer's personal information is accessed and unencrypted, companies must disclose the breach to affected individuals as well as regulators, one speaker said. But the current rules vary widely from state to state, and some regulators have broad, non-specific requirements for disclosures, leaving companies to chart their own path. The SEC, for example, wants companies to disclose breaches as they see fit, in a timely and robust way. Even so, it is hard to avoid civilian lawsuits over breaches. Cohen said it only takes a handful of significant legal victories for many law firms to jump on the bandwagon and sue companies that suffer a hacking. Taking out cyber risk insurance is one way of hedging the financial fallout.

However, the market capacity for cyber insurance is still evolving and not yet large enough to adequately cover all of the related risks and damages, according to AIG. The amount of cyber liability coverage currently being offered by insurance carriers will only cover a fraction of the damages that occur during and after a data breach. For example, cyber coverage pales in comparison to the amount of capacity that is available for a complex chemical plant, refinery or offshore oil platform.

Nonetheless, the cyber insurance market continues to evolve. In fact, it is one of the fastest growing products in both the standard, as well as excess and surplus markets. The amount of coverage available for cyber policies is predicted to increase over time — and quickly. The willingness of insurers and others in the industry to provide greater capacity will increase with greater comfort in response to the maturity of the countermeasures.

U.S. GOVERNMENT'S RESPONSE

President Obama has signed a series of executive orders to beef up the government's response to cyber attacks, including the building and promotion of a cybersecurity framework for preparedness and risk mitigation, boosting information sharing and setting standards to work across sectors as well as incident reporting.

One order stands out as a potential "cornerstone of a new financial battle plan" against hackers targeting the U.S., one speaker said. In April 2015, President Obama signed the executive order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." Invoking the International Emergency Economic Powers Act, he ordered the freezing of assets or blocking of transactions of hackers as well as entities linked to such activities. Cyber warfare now faces sanctions similar to those covering terrorist acts, nuclear proliferation and other national threats. Meanwhile, the government continues its discussions with nations thought to sponsor hackers in hopes of ending such attacks.

But conference speakers also said the government should be declassifying more information and giving out more clearances to those managing critical infrastructure in order to help the business community better understand

cyber threats. Moreover, Cohen called for the creation of a central cyber office at the federal level — even the appointment of a Cabinet-level cyber secretary — to boost effectiveness and collaboration. At present, at least six U.S. government agencies monitor cybersecurity: CIA, NSA, FBI, U.S. Department of Homeland Security, the U.S. Treasury and the Air Force. In addition, a slew of state and local authorities are tackling the matter.

Cohen said the government should mitigate civil liability and antitrust concerns of businesses as they cooperate in cybersecurity. Companies should have immunity for a wide range of actions they might take to prevent or deal with cyber attacks and the sharing of information among them. While it may not be politically possible to get unqualified immunity, some is better than none. "Perhaps the best to hope for is explicit standards of liability," he said.

Cohen also suggested seeking business review letters from the U.S. Justice Department that would give companies immunity from antitrust concerns when it comes to cyber security issues. On a positive note, he said, cyber reform is a bipartisan issue in Congress. There are bills on cyber risk being circulated in both houses dealing with four topics: information sharing, private sector active defense, data security obligations and breach notification requirements.

Legislation to give immunity to companies sharing threat information has received positive headwinds of late. Recently, the U.S. Senate overwhelmingly passed the Cybersecurity Information Sharing Act, which would give companies legal immunity from sharing data about hackings with the government, which would then warn other companies. A similar bill is making its way in the House. The measures have White House support.

One conference speaker raised the possibility of a "cyber privateering" approach to dealing with hackers. He pointed to a portion of Article 1, Section 8 of the U.S. Constitution that called for the granting of "letters of marque and reprisal" used during a time of maritime upheaval in the early 19th century. Such letters gave privateers the right to attack enemy ships if they were harmed and exact equal value to their loss.

Applying it to cyberspace, the letters would give companies the right to fight back against hackers and profit from any victories. "Why not think more creatively about applying a cyber-privateering model, which has clear constraints and controls?" he said. However, another speaker said U.S. businesses with interests in nations that are the source of hacks might balk at taking such an aggressive approach.

Hacking attacks represent "one of the truly existential threats to a wide swath of American industry."

— H. Rodgin Cohen, senior chairman of Sullivan & Cromwell

As for resetting the Internet, one panelist said there is no appetite for it. However, businesses are increasingly building "defensible architecture," redesigning their systems to be more resilient to hacking. Another speaker brought up the idea of slowing down on digitizing devices in the Internet of Things. "Why does everything have to be connected?" Such interconnections merely give hackers a bigger playground for their activities.

Speakers also called upon companies to collect less data on customers. "You don't need to hold that much data about a person to validate them," one panelist said. Perhaps there need to be levels of consent given by consumers for access to their information. But all agreed the time to act is now, before there is a cyber 9/11. "Do we have to wait for a catastrophic attack on our national system of some sort to actually react?" one speaker said. "I hope that's not the case."

SULLIVAN & CROMWELL LLP | RANE Risk Assistance Network + Exchange | KNOWLEDGE@WHARTON

CORPORATE GOVERNANCE IN THE AGE OF CYBER RISKS

ABOUT KNOWLEDGE@WHARTON

Knowledge@Wharton is the online business analysis journal of the Wharton School of the University of Pennsylvania. The site, which is free, captures relevant knowledge generated at Wharton and beyond by offering articles and videos based on research, conferences, speakers, books and interviews with faculty and other experts on global business topics.

For more information, please visit knowledge.wharton.upenn.edu

ABOUT RANE

RANE (Risk Assistance Network and Exchange) is an information services company created to help enterprises and individuals manage complex risk more effectively through collaboration. We connect the leading risk management experts and service providers with subscriber members seeking solutions to the most pressing and evolving challenges. We provide members unbiased access to:

- Experts from around the world, selected and credentialed by RANE
- Collaboration tools to work with peers and experts
- Curated and original content
- Briefings and events for sharing knowledge, resources, and best practices

RANE was founded on the premise that our collective resources afford far greater protections than any individual approach. We serve both private and public interests, with the firm belief that shared risks require shared solutions.

AIG

CROWDSTRIKE

ENDGAME.

IPSA International
A root9B Technologies company

PROMONTORY

SpencerStuart

STROZ FRIEDBERG

JOHN JAY COLLEGE OF CRIMINAL JUSTICE