zoomlens

September 2012

Note to Corporate America: Cybersecurity Matters More Than Ever

Note to Corporate America: Cybersecurity Matters More Than Ever

On September 19, Senator John D. Rockefeller IV (D-WV) sent a letter to each of the US Fortune 500 companies, a group that contributes 78% of the US Gross Domestic Product,[1] soliciting their views on a number of cybersecurity issues, including current cybersecurity practices and development processes. The letter also asks companies to identify concerns with various proposals outlined in the Cybersecurity Act of 2012, specifically public-private collaboration on standards, US government-directed cyber risk assessments, and the identification of critical cyber-infrastructure.[2]

Rockefeller's letter was sent after a Senate procedural vote on the Cybersecurity Act of 2012 failed to get the necessary support to move the bill forward last month. According to Rockefeller, the Senate's failed procedural vote was attributable to "opposition from a handful of business lobbying groups and trade associations, most notably the United States Chamber of Commerce." Rockefeller says he sent the letter to hear directly from the chief executives of business "without the filter of beltway lobbyists."

In the letter, Rockefeller says he believes that most business executives recognize the gravity of the cybersecurity threat and that "their companies would benefit from a greater collaboration with government." Toward proving that point, Rockefeller asks companies to respond to a series of eight questions set forth in the letter and says he would be surprised to learn that companies are as "intransigently opposed to our cybersecurity legislative efforts as the Chamber of Commerce has indicated they are."

While your company may or may not have been a recipient of Senator Rockefeller's letter, it is important to understand that cybersecurity is a high priority issue for many policy makers and, although Congress did not pass comprehensive cybersecurity legislation before adjourning, government efforts in this area are expected to continue. Both Senator Rockefeller, as mentioned in his letter, and Cybersecurity Act of 2012 sponsor Senator Joe Lieberman (I-CT) sent letters to President Obama urging him to direct various agencies to implement cybersecurity protections.

[1] The 2011 Fortune 500 Gross Revenues were $11.7 billion versus $15 billion in GDP.
[2] Gorman, Siobhan. (September 19, 2012). Senator Presses on Cybersecurity. The Wall Street Journal. (accessed September 20, 2012).

pwc

President Obama is expected to issue an Executive Order (EO) in this area that would direct various federal agencies to develop voluntary cybersecurity guidelines for owners of power, water, and other critical infrastructure facilities. Additionally, the Securities and Exchange Commission (SEC) has focused on company disclosure of cybersecurity risks and cyber incidents, issuing follow-up letters to companies not appearing to follow staff guidance on the issue.

The message to business leaders: An effective cybersecurity protection strategy is imperative from a business perspective, and it is one that may be mandated by the US government in the future. If your organization views cybersecurity as merely an interesting policy debate, it's time to reorient your thinking.

What it means to you

Our view, based on what we know from our Global CEO Survey, Global Economic Crime Survey, and Global Information Security Survey (GISS), is that senior executives recognize that attention to cybersecurity can make or break your business.

There's still room for improvement, though, in putting cybersecurity risk management strategies into practice. Our Global CEO Survey shows that CEOs today view cybersecurity risks as a top five issue. In our November 2011 Global Economic Crime Survey, 61% of US respondents believed their risk of cybercrime had increased, while only 37% of C-suite/senior executives had reviewed their cybercrime risks at least annually.

Our GISS Survey shows that cybersecurity practices lag the CEOs' new recognition and expectations regarding information security. We believe there will be increasing focus and expenditure to close the gap in the next two to five years.

Protecting information assets is a matter of business strategy and business survival. The right cybersecurity strategy can, in the long run, give you an advantage in the global competitive marketplace. We present eight enlightening cybersecurity questions we believe you should be able to answer.

Take charge of your cybersecurity.

1. Who is responsible for the security of your organization?
   - While cybersecurity programs are executed by the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or Chief Security Officer (CSO), the executive leadership team must be committed to cybersecurity as a business imperative. Companies that embed security into strategic decision-making across the business are better able to recognize current and future security risks, navigate the threat landscape in pursuit of business opportunities, and allocate security resources more effectively.

2. Can you explain your cybersecurity strategy to your shareholders? Your investors? Your employees? Your regulators?
   - You must not only have a clear vision of how cybersecurity increases your company's value, but you also must be able to share that vision with your stakeholders.

Know what you need to know.

3. Do you know how an adversary looks at your organization?
   - The cyberthreat landscape changes daily. Know what your cyberthreat profile is. The threats your business faces can include foreign nation states, terrorists, hacktivists, competitors, or malicious employees. It's affected by where you do business, how you conduct business, and who you do business with.

4. Do you know what your cybersecurity strategy is protecting?
   - Too many companies try to protect everything, with little success. Understanding both your threat landscape and your critical corporate assets is essential to a strong and resilient cybersecurity strategy. Effective cybersecurity requires a culture shift. Everyone in the organization needs to know what they are protecting, why they are protecting it, and what their role is in protecting it.

5. Do you have a secure enterprise ecosystem?
    - Corporate assets — and corporate vulnerabilities — no longer reside behind a company fence, or even a company firewall. Understand that your supply chain, your service providers and strategic partners, your employees and customers, are all interconnected. Effective cybersecurity strategies account for both the risks and the opportunities these interconnected relationships represent.

Have a resilient action plan.

6. Do you have a threat-based, asset-based cybersecurity plan?
    - Sound security resource investments are predicated on informed risk assessments, rather than compliance requirements alone. Companies that do this right have a business that's competitive in the marketplace. Companies that do this wrong — or don't do anything — may not have a business to worry about.

7. Is an integrated security strategy a pivotal part of your business model?
    - Many firms look at security as a technology-focused cost center, and it's often bolted on after business strategies are enacted. Competitive firms leverage their security model at all levels of business. They also consider the full scope of security — cyber, physical, personnel, technical and non-technical — in creating and protecting business.

8. Do you have a public-private partnership strategy?
    - The increased government focus on corporate cybersecurity is a challenge, but we believe it's also an opportunity. Strong private sector organizations seek out the right opportunities to collaborate with government agencies. They also recognize that information sharing is not a one-way street. Successful companies implement a security information sharing plan that encompasses enterprise ecosystems, industry peers, cross-industry groups, and government agencies.

Organizations that can answer these eight questions will be able to:

- Prioritize corporate resources and protect those things that are valuable to both you and your adversary.
- Proactively implement cybersecurity practices that not only protect their business, but also put them ahead of the pack in the global marketplace.
- Effectively engage with policy makers and be prepared to answer inquiries concerning current and future cybersecurity initiatives, whether originating from Congress or the executive branch.

Where will you play? How will you fare?

A crowd is gathering in critical chorus against cybercrime, and issues of cybersecurity have reached new levels of concern with no sign of slowing. Ignoring this issue is not an option. Companies face cyber assaults daily from foreign intelligence services, corrupt competitors, transnational criminal enterprises, malicious insiders, and outside hackers, all of whom know how to hide evidence of attacks for months or even years.[3] These adversaries, as well as cyber actors who are not knowingly trying to harm you, will negatively impact your business performance, reputation, and ability to compete successfully over the long haul. Cybersecurity is critical to protecting the interests of every business, and every business — from the Fortune 500 to mom-and-pop technology startups — must act in the interest of its shareholders. The time to answer the crucial questions we raise here and figure out how your organization can play proactively and effectively in this space is now.

An In-Depth Look at the Cybersecurity Debate

Renewed Government Resolve

While it appears that Congress may not act on cybersecurity legislation until 2013, White House action and federal agency regulations may affect US companies in the near term. Businesses should pay close attention and stand poised to plan for action.

In early September, reports of a draft Executive Order (EO) began to surface, indicating a strong White House interest in moving forward with the Administration's cybersecurity agenda before election.[4]

---

[3] 2011 Global Economic Crime Survey, citing 10Minutes on Information Security, PwC, November 2010.
[4] Strohm, C., & Engleman, E. (September 8, 2012). Obama Weighs Executive Order to Defend Against Cyber Attacks. Businessweek. (accessed September 20, 2012).

The EO would direct agencies to create voluntary standards that would help companies protect themselves against cyber attacks, according to White House officials. It would also establish a special interagency council, led by the Department of Homeland Security (DHS), to identify threats that could compromise critical sectors. The Office of the Director of National Intelligence (ODNI) would sit on the council, as would the Departments of Commerce, Energy, Defense, Treasury, and Justice. Media accounts suggest that the council would use intelligence to develop cybersecurity standards for industry.[5]

The EO likely will not mandate that the private sector undertake specific steps, but it fuels continued debate about how to address unprecedented cyber threats and could refocus congressional efforts on cybersecurity legislation.

The voluntary approach outlined in the EO is not a panacea, according to an Administration official, who said, "We still think it should be mandated," but added "It's better than sitting around and waiting for legislation."[6]

Senator Rockefeller was more direct, telling CEOs that he views an EO as progress, but that legislation along the lines of the Cybersecurity Act of 2012, remains a necessity.[7]

SEC sharpens disclosure requests

In October 2011, the Securities and Exchange Commission (SEC) issued staff guidance on disclosure obligations related to cybersecurity risks and cyber incidents. Although not legally binding, the guidance encouraged publicly traded firms to report cyber risks in their quarterly filings. By the end of the first quarter of 2012, it was clear from the corporate filings that firms were not eagerly following the Guidance.

The SEC began sending letters in March to firms with publicly-reported cyber incidents and data breaches that had gone unreported in their quarterly disclosures. The firms were encouraged to consider or reconsider including the incidents in their SEC reports. At least six have since announced plans to adhere to the Guidance.[8]

More public-private partnerships on the horizon

Public-private collaboration is a cornerstone of many cybersecurity initiatives. Security-focused information sharing with the federal government has become increasingly important, but gaps remain between what the government shares and what the private sector believes it needs to do to protect itself.

Some public-private approaches work well…

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is often praised for bringing the financial services industry and government agencies together with respect to security. It recently revised its cyber threat level from elevated to high, pointing to recent credible intelligence on sophisticated distributed denial of service (DDOS) and other cyber attacks against financial institutions.[9] The alert didn't cite specific incidents, but reports indicate that several major US banks suffered unexplained network disruptions the week of September 17; and, on September 18, a group calling itself the 'Cyber Fighters of Izz ad-din Al Qassim' warned of a network attack against Bank of America and the New York Stock Exchange.[10]

---

[5] Nakashima, E. (September 7, 2012). White House Drafting Standards to Protect US Against Cyber Attack, Officials Say. The Washington Post. (accessed September 20, 2012).

[6] Ibid.

[7] Democratic Press Office. (2012 19 Sep). Rockefeller Calls on Fortune 500 Companies to Prioritize Cybersecurity. US Senate Committee on Commerce, Science and Transportation. (http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=18db690c-c237-4358-9097-3d53f4762cc0&ContentType_id=77eb43da-aa94-497d-a73f-5c951ff72372&Group_id=4b968841-f3e8-49da-a529-7b18e32fd69d. Accessed 21 Sep 2012).
R. (2012, 19 September). An Open Letter to Sen. Rockefeller. Forbes Online. (http://www.forbes.com/sites/richardstiennon/2012/09/19/an-open-letter-to-senator-rockefeller/ (accessed September 20, 2012).

[8] Sandler, L. (August 29, 2012). SEC Guidance on Cyber Disclosure Becomes Rule for Google. Businessweek Online. (http://www.businessweek.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google. (accessed September 20, 2012).

[9] Cyber Threat Level for the Financial Sector. (September 19, 2012). FS-ISAC.COM. (http://www.fsisac.com/ (accessed September 20, 2012).

[10] Vijayan, J. (September 20, 2012). US Banks on High Alert Against Cyberattacks. ComputerWorld. (http://www.computerworld.com/s/article/9231515/U.S._banks_on_high_alert_against_cyberattacks. (accessed September 23, 2012).

Among other efforts to engage CEOs in the public-private sector cyber dialogue, is the Enduring Security Framework (ESF), launched in 2008. The ESF briefings "scare the bejeezus out of them," according to a US government participant.[11] Practically speaking, the ESF offers CEOs from leading defense and technology companies classified briefings on cyberwarfare capabilities and how they can be used against US companies.

...but many efforts are uncoordinated and duplicative...

It can be a time-consuming challenge to navigate the maze of public-private partnerships, particularly for small and mid-size companies with limited security resources. While nearly every US government agency has an industry outreach program, and business leaders can participate in numerous public-private information-sharing groups, including Infragard, Sector Coordinating Councils (SCCs), and DIBNet, they're often unable to determine what government agencies to engage and what to expect from them.

...and both sides remain unsatisfied with the level of sharing.

DHS Secretary Napolitano has been lobbying heavily for faster, more collaborative information sharing, pointing out that time is of the essence in cybersecruity matters and calling upon companies to share information with the DHS in the event of a cyber attack.[12] Many in industry, however, believe the government has most of the vital information —particularly identifying signatures — and consistently ask for an increased flow of information from the government to the private sector.

No One-Size-Fits-All Solution

A common theme in the cyber policy debate is that government sees an opportunity to connect with the private sector more broadly as an ally in the cybersecurity battle. At a New York panel on cybersecurity in April, National Counterintelligence Executive (NCIX) Frank Montoya told the audience that, unlike in World War II, when the US military protected civilian infrastructure, "We're an information-based society now. Information is everything. That makes you, as company executives, the front line — not the support mechanism, the front line — in what comes."[13]

But companies don't have the same objectives or resources as the government. As an Internet security expert told National Public Radio, "The legally mandated role of the government is to provide for the common defense, and they're willing to spend pretty much whatever it takes to do that. If you're in a private organization, your legally mandated responsibility is to maximize shareholder value. You can't spend just anything on the cyberthreat."[14]

This may create a market for cybersecurity insurance. Underwriters would then confirm that firms had met new industry standards before issuing policies. This is important from an investment perspective, as insurers would have to place a value on corporate intellectual property (IP). Firms could use that estimate — along with a strong understanding of their threat landscape — to make decisions about how much to spend on security to protect such critical assets.

The bottom line for businesses: You won't find a one-size-fits-all approach to cybersecurity. An effective strategy will address a firm's own unique risk profile, resources, and business objectives.

---

[11] Gjelton, T. (Mary 9, 2012). Cyber Briefings Scare the Bejeezus out of CEOs. National Public Radio. (http://www.npr.org/2012/05/09/152296621/cyber-briefings-scare-the-bejeezus-out-of-ceos.) (accessed September 20, 2012).

[12] ASIS made Secretary Napolitano's speech available via a link on www.asisonline.com: http://www.youtube.com/watch?v=MsBtwYXYVkE&feature=youtu.be (accessed September 20, 2012)

[13] Amerding, T. (May 14, 2012). Public V. Private Cyber Attack Responsibility Debate Heats Up. Network World. (http://m.networkworld.com/news/2012/051412-public-vs-private-cyberattack-responsibility-259259.html?page=2. (accessed September 20, 2012).

[14] Gjelton, T. (May 9, 2012). Cyber Briefings Scare the Bejeezus out of CEOs. National Public Radio. (http://www.npr.org/2012/05/09/152296621/cyber-briefings-scare-the-bejeezus-out-of-ceos. (accessed September 20, 2012). (Quoting Larry Clinton, Internet Security Alliance).

Eight questions from Senator Rockefeller:

1. Has your company adopted a set of best practices to address its own cybersecurity needs?
2. If so, how were these cybersecurity practices developed?
3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.
4. When were these cybersecurity practices developed? How frequently have they been updated? Does your company's board of directors or audit committee keep abreast of developments regarding the development and implementation of these practices?
5. Has the federal government played any role, whether advisory or otherwise, in the development of these cybersecurity practices?
6. What are your concerns, if any, with a voluntary program that enables the federal government and the private sector to develop, in coordination, best cybersecurity practices for companies to adopt as they so choose, as outlined in the Cybersecurity Act of 2012?
7. What are your concerns, if any, with the federal government conducting risk assessments, in coordination with the private sector, to best understand where our nation's cyber vulnerabilities are, as outlined in the Cybersecurity Act of 2012?
8. What are your concerns, if any, with the federal government determining, in coordination with the private sector, the country's most critical cyber infrastructure, as outlined in the Cybersecurity Act of 2012?

About the authors

David Burg

Mr. Burg is a Principal in PwC's Advisory Practice, where he is the US leader of the Forensic Technology Solutions practice. He has assisted clients in reactive and proactive consulting capacities involving the deployment of information technology solutions and their use. Mr. Burg has assisted corporate clients, law firms, and the US Government in matters involving cybercrime investigations, complex data correlation/analysis, and various business transformation or operational initiatives. He also led a variety of engagements in recent years, addressing a number of significant data breaches for clients in numerous industries; working with a global company to assess and improve its information security program; investigating a very large system outage to assess causative factors; performing a risk assessment in connection with an international litigation matter with the potential for billions of dollars in liability; and leading a forensic analysis team that responded to an international bank's infrastructure hack that led to nearly $10 million in unauthorized ATM use.

703 918 1067
david.b.burg@us.pwc.com

Michael D. Compton

Mr. Compton is a Principal in PwC's Advisory Practice, serving as our operations leader for the US security consulting practice, advising clients on a wide array of technology issues. A partner who has been with PwC for over 22 years, he specializes in information security consulting, where he has extensive experience in assessing, designing, and implementing information security solutions. Mr. Compton, is responsible for our identity management solution offering, and serves as the engagement partner on our largest security implementation projects. He is also the firm relationship partner for high-profile clients in the automotive industry.

313 394 3535
michael.d.compton@us.pwc.com

Laurie Schive

Laurie Schive is a Director in PwC's Forensic Services practice. She came to PwC in 2012 with more than 24 years of experience in the field of intelligence operations. Her specialties include counterintelligence and security strategy, threat and vulnerability assessments, and cybersecurity training and awareness. Prior to joining PwC, Ms. Schive most recently served as the Director of Outreach for the Office of the National Counterintelligence Executive (ONCIX), advising private sector entities on counterintelligence and security leading practices, insider threat detection, cybersecurity, and supply chain risk management. During an 18-year stint with the CIA, she focused on economic security and weapons proliferation issues.

703 350 9445
laurie.a.schive@us.pwc.com

Kimberly K. Peretti

Kimberly Kiefer Peretti, J.D., LL.M., CISSP, is a Director in PwC's Forensic Services practice. A former senior litigator for the Department of Justice's (DOJ) Computer Crime and Intellectual Property Section, she joined PwC in May 2010 and focuses on the prevention, response, and remediation of privacy breaches and cyber intrusions. She also services a wide range of clients in matters of cyber investigations, cyber security, privacy, financial crime, fraud, and regulation, payment systems compliance and risk mitigation, economic espionage, and intellectual property theft. Ms. Peretti is a Board Advisor to the Financial Services Information Sharing and Advisory Center. While at the DOJ, she led several benchmark cybercrime investigations and prosecutions, including the prosecution of infamous hacker Albert Gonzalez, who is serving 20 years in prison for his role in the largest hacking and identity theft case the DOJ ever prosecuted, in which over 170 million credit and debit card numbers were stolen from over 14 major US retailers.

703 918 1500
kimberly.k.peretti@us.pwc.com

About the authors

Neal A. Pollard

Neal A. Pollard is a Director in PwC's Forensic Technology Solutions practice. He has conducted large, complex forensic investigations of cybercrime and economic espionage, and assisted US industry in establishing insider threat management programs. He also has developed operational requirements and test metrics for advanced technology research to detect and counter insider threats for the US Defense Advanced Research Projects Agency. A member of the Council on Foreign Relations Independent Task Force on US Policy in the Digital Age, he also has served as a member of the United Nations Experts Group on Use of the Internet for Terrorist Purposes. Prior to joining PwC, Mr. Pollard was a senior officer in the US intelligence community, serving in multiple assignments for the CIA, the National Counterterrorism Center, and the Office of the Director of National Intelligence, including a staff detail as Director for Counterterrorism for the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism.

703 918 3781

neal.a.pollard@us.pwc.com