Cybersecurity Roundtable Meeting

Thursday, April 2nd
11am – 12:15pm
JW Marriot Desert Ridge Resort & Spa
Phoenix, AZ

Discussion Leads:

Heidi Roth, SVP, CAO & Controller, Kilroy Realty Corporation
Anthony Buffomante, Principal, KPMG LLP
Kurt Manske, VP-Compliance & Corporate Information Technology, QTS Realty Trust, Inc.

NAREIT's Law, Accounting & Finance Conference

JW Marriott Desert Ridge Resort & Spa
Phoenix, AZ

Cyber Security

March 31-April 2, 2015

Agenda

1

State of the Union for Cyber Security

- New Vectors of Threats
- Dynamic World of Change
- Real Estate Cyber Security Risks
- Common Cyber Security Mistakes

2

Planning Your Response

- 5 steps to minimize your exposure
- Assess your Readiness
- Lessons learned from Law Enforcement

3

Appendix Materials

- Cyber Maturity Assessment Areas of Focus

New “Vectors” of Threats are Accelerating the Concern

Yesterday…

Bad “Actors”

- Isolated criminals
- “Script Kiddies”

“Target of Opportunity”

Targets

- Identity Theft
- Self Promotion Opportunities
- Theft of Services

Today…

Bad “Actors”

- Organized criminals
- Foreign States
- Hactivists
- Insiders

“Target of Choice”

Targets

- Intellectual Property
- Financial Information
- Strategic Access

Dynamic World of Change

Business Delivery "Stack"	Areas of Dynamic Change
BUSINESS LAYER Industry Leading Practices Geopolitical Drivers Business Process Corporate Objectives	- Driving Growth & Profitability - New Products/Services - Mergers/Acquisitions - Globalization - Strategic Sourcing - Competitive Differentiation - Increased Regulatory Scrutiny
ENABLEMENT LAYER Application Data	- Mobile & Cloud Deployments - "Big Data," BI & Analytics - Self service & Consumerization
INFRASTRUCTURE LAYER Servers/Hosts Networks Physical Environment	- Virtualization & Cloud Platforms - Internetworking/VPNs - New Operating Systems - Low cost computing models - Changing DataCenter models

Traditional Approach

KPMG Approach

Real Estate Cyber Security Risks

- Cash – wire transfer fraud
- Employee personal information
- Application data (tax returns, financial information, etc.)
- Tenant information – residential / senior living (HIPAA)
- Third-party vendor risks
- Building automation

The Five Most Common Cyber Security Mistakes

Mistake #1:

"We have to achieve 100 percent security."

Reality:

100 percent security is neither feasible nor the appropriate goal.

The Five Most Common Cyber Security Mistakes

Mistake #2:

"When we invest in best-in-class technical tools, we are safe."

Reality:

Effective Cyber Security is less dependent on technology than you think.

The Five Most Common Cyber Security Mistakes

Mistake #3:

"Our weapons have to be better than those of our attackers."

Reality:

The security policy should primarily be determined by your goals, not those of your attackers.

The Five Most Common Cyber Security Mistakes

Mistake #4:

"Cyber Security compliance is all about effective monitoring."

Reality:

The ability to learn is just as important as the ability to monitor.

The Five Most Common Cyber Security Mistakes

Mistake #5:

"We need to recruit the best professionals to defend ourselves against cyber crime."

Reality:

Cyber Security is not a department, but an attitude.

Planning Your Response
Example Cyber Security Framework

Planning Your Response
Five Steps to Minimize Your Exposure

1	Assess your Readiness to Respond	Perform a cyber maturity assessment to look at areas such as Leadership and Governance, Human Factors, Information Risk Management, Business Continuity and Crisis Management.
2	Hone in on your critical assets	Identify your critical assets but remember that what you consider to be of no value, may be considered valuable to an attacker. Take a look at the lifecycle of your critical information assets from creation all the way to destruction.
3	**Select your defense**	Based on your assessment and your critical assets, select your defenses. Know what threats you are going to defend against – trying to prevent them all it gets very expensive
4	**Boost your security awareness and education**	Everyone in the organization – from the boardroom to the mailroom – must understand the value and sensitivity of the information they possess and, more importantly, how to protect it.
5	Enhance Monitoring & Incident Response	Being able to adequately respond to a security incident through established tested processes should not be taken lightly. Supported by a security monitoring platform and good threat intelligence, you can get a better grip on monitoring and responding to cyber crime.

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

LEGAL AND COMPLIANCE

Regulatory and international certification standards as relevant

LEADERSHIP AND GOVERNANCE

Board demonstrating due diligence, ownership and effective management of risk

OPERATIONS AND TECHNOLOGY

The level of control measures implemented to address identified risks and minimize the impact of compromise

HUMAN FACTORS

The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge

BUSINESS CONTINUITY AND CRISIS MANAGEMENT

Preparations for a security event and ability to prevent or minimize the impact through successful crisis and stakeholder management

INFORMATION RISK MANAGEMENT

The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

Leadership and Governance
Board demonstrating due diligence, ownership and effective management of risk

Topics
Understanding of Cyber
Board Involvement
Third-Party Supplier Relationships
Identification of Critical Data
Ownership and Governance for Data Protection
Program Management

Human Factors
The level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge

Topics
Training and Awareness
Culture
Personnel Security Measures
Talent Management
Organizational Roles and Responsibilities

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

Information Risk Management
The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners

Topics
Risk Management Approach and Policies
Risk Tolerance Identification
Risk Assessment and Measures
Asset Management
Information Sharing
Third Party Accreditation
Ability to Detect Attacks & Integrate Improvements

Business Continuity and Crisis Management
Preparations for a security event and ability to prevent or minimize the impact through successful crisis and stakeholder Management

Topics
Ability to Manage Cyber Events
Financial Ramifications & Budget
Resources Required & Training
Robust Plans
Communications
Testing

Planning Your Response
Assess Your Readiness – Cyber Maturity Assessment

Operations and Technology
The level of control measures implemented to address identified risks and minimize the impact of compromise

Topics
Threat and Vulnerability Management
Logical Security Controls
Physical Security Controls
Security Monitoring
Incident Response
Integration with IT Service Management

Legal and Compliance
Regulatory and international certification standards as relevant

Topics
Inventory of compliance requirements
Compliance program components
Role of the Audit Committee
Litigation inventory
Cyber insurance

Tony Buffomante
KPMG LLP
Principal, Information Protection Services

200 E. Randolph
Chicago, IL 60601

abuffomante@kpmg.com
312-665-1748

Homeland Security

Cybersecurity Questions for CEOs

Cyber threats constantly evolve with increasing intensity and complexity. The ability to achieve mission objectives and deliver business functions is increasingly reliant on information systems and the Internet, resulting in increased cyber risks that could cause severe disruption to a company's business functions or operational supply chain, impact reputation, or compromise sensitive customer data and intellectual property.

Organizations will face a host of cyber threats, some with severe impacts that will require security measures that go beyond compliance. For example, according to a 2011 Ponemon Institute study, the average cost of a compromised record in the U.S. was $194 per record and the loss of customer business due to a cyber breach was estimated at $3 million.

This document provides key questions to guide leadership discussions about cybersecurity risk management for your company, along with key cyber risk management concepts.

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Key Cyber Risk Management Concepts

Incorporate cyber risks into existing risk management and governance processes.

Cybersecurity is NOT implementing a checklist of requirements; rather it is managing cyber risks to an acceptable level. Managing cybersecurity risk as part of an organization's governance, risk management, and business continuity frameworks provides the strategic framework for managing cybersecurity risk throughout the enterprise.

Elevate cyber risk management discussions to the CEO.

CEO engagement in defining the risk strategy and levels of acceptable risk enables more cost effective management of cyber risks that is aligned with the business needs of the organization. Regular communication between the CEO and those held accountable for managing cyber risks provides awareness of current risks affecting their organization and associated business impact.

Implement industry standards and best practices, don't rely on compliance.

A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current threats and enable timely response and recovery. Compliance requirements help to establish a good cybersecurity baseline to address known vulnerabilities, but do not adequately address new and dynamic threats, or counter sophisticated adversaries. Using a risk based approach to apply cybersecurity standards and practices allows for more comprehensive and cost effective management of cyber risks than compliance activities alone.

Cybersecurity Questions for CEOs

Evaluate and manage your organization's specific cyber risks.

Identifying critical assets and associated impacts from cyber threats are critical to understanding a company's specific risk exposure– whether financial, competitive, reputational, or regulatory. Risk assessment results are a key input to identify and prioritize specific protective measures, allocate resources, inform long-term investments, and develop policies and strategies to manage cyber risks to an acceptable level.

Provide oversight and review.

Executives are responsible to manage and oversee enterprise risk management. Cyber oversight activities include the regular evaluation of cybersecurity budgets, IT acquisition plans, IT outsourcing, cloud services, incident reports, risk assessment results, and top-level policies.

Develop and test incident response plans and procedures.

Even a well-defended organization will experience a cyber incident at some point. When network defenses are penetrated, a CEO should be prepared to answer, "What is our Plan B?" Documented cyber incident response plans that are exercised regularly help to enable timely response and minimize impacts.

Coordinate cyber incident response planning across the enterprise.

Early response actions can limit or even prevent possible damage. A key component of cyber incident response preparation is planning in conjunction with the Chief Information Officer/Chief Information Security Officer, business leaders, continuity planners, system operators, general counsel, and public affairs. This includes integrating cyber incident response policies and procedures with existing disaster recovery and business continuity plans.

Maintain situational awareness of cyber threats.

Situational awareness of an organization's cyber risk environment involves timely detection of cyber incidents, along with the awareness of current threats and vulnerabilities specific to that organization and associated business impacts. Analyzing, aggregating, and integrating risk data from various sources and participating in threat information sharing with partners helps organizations identify and respond to incidents quickly and ensure protective efforts are commensurate with risk.

A network operations center can provide real-time and trend data on cyber events. Business-line managers can help identify strategic risks, such as risks to the supply chain created through third-party vendors or cyber interdependencies. Sector Information-Sharing and Analysis Centers, government and intelligence agencies, academic institutions, and research firms also serve as valuable sources of threat and vulnerability information that can be used to enhance situational awareness.

About DHS

The Department of Homeland Security (DHS) is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity.

For more information, please visit: www.dhs.gov/cyber.

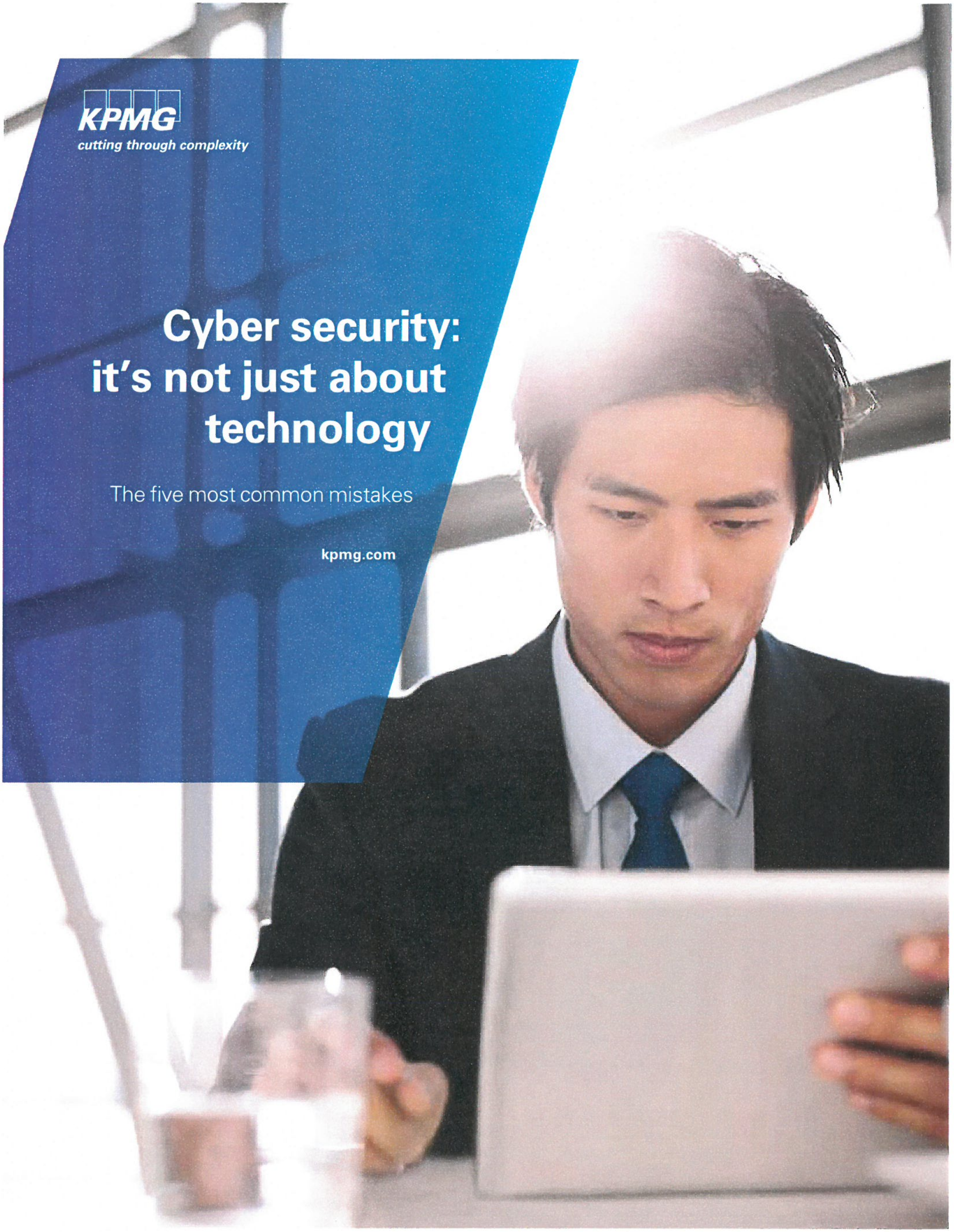
To report a cyber incident: https://forms.us-cert.gov/report/ or (888) 282-0870

KPMG
cutting through complexity

Cyber security: it's not just about technology

The five most common mistakes

kpmg.com



Contents

Preface

Cyber security is an important concern for every organization. Daily occurrences demonstrate the risk posed by cyber attackers—from individual, opportunistic hackers, to professional and organized groups of cyber criminals with strategies for systematically stealing intellectual property and disrupting business.

The management of any organization faces the task of ensuring that its organization understands the risks and sets the right priorities. This is no easy task in light of the technical jargon involved and the pace of change.

Focusing on technology alone to address these issues is not enough. Effectively managing cyber risk means putting in place the right governance and the right supporting processes, along with the right enabling technology.

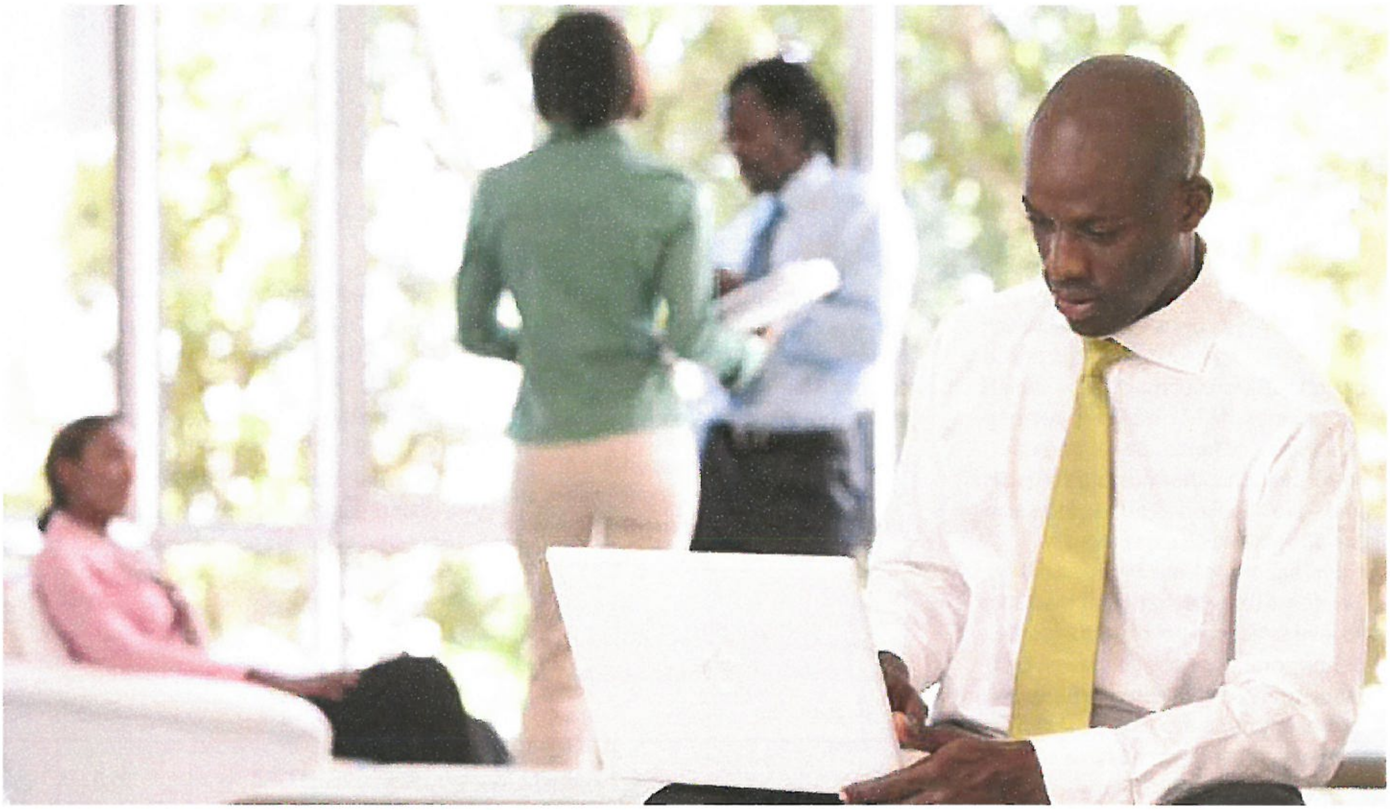
This complexity, however, cannot be an excuse for company management to divest responsibility to technical "experts." It is essential that leaders take control of allocating resources to deal with cyber security, actively manage governance and decision making over cyber security, and build an informed and knowledgeable organizational culture.

This white paper provides essential insights for management to get the basics right. We'll cover the world of cyber crime today, explore five common cyber security mistakes, explain the importance of customizing cyber security policies, outline the critical dimensions of a strong cyber security model, and look at key questions to help you navigate the "new normal" of cyber security.

Steve Barlock
Principal, Advisory
Information Protection and Business Resilience
T: 415-963-7025
E: sbarlock@kpmg.com

Tony Buffomante
Principal, Advisory
Information Protection and Business Resilience
T: 312-665-1748
E: abuffomante@kpmg.com

Fred Rica
Principal, Advisory
Information Protection and Business Resilience
T: 973-912-4524
E: frica@kpmg.com



What is cyber crime and who is carrying it out?

Cyber crime is a range of illegal digital activities targeted at organizations in order to cause harm. The term applies to a wide range of targets and attack methods.

Understanding the "actor," i.e. the person or organization that is sponsoring or conducting the attacks, is essential for effective defense.

Actors can be divided into four categories:

1. An individual hacker, generally acting alone and motivated by being able to show what he/she can do
2. The activist, focused on raising the profile of an ideology or political viewpoint, often by creating fear and disruption
3. Organized crime, focused solely on financial gain through a variety of mechanisms, from phishing to selling stolen company data
4. Governments, focused on improving their geopolitical position and/or commercial interests

Attacks by these different actors have a number of different characteristics, such as the type of target, the attack methods and scale of impact.

01

Understanding the cyber risk

The amount of data continues to grow exponentially, as does the rate at which organizations share data through online networks. Billions of machines – tablets, smartphones, ATM machines, security installations, oil fields, environmental control systems, thermostats and much more – are all linked together, increasing inter-dependencies exponentially. Organizations increasingly open their IT systems to a wide range of machines and lose direct control of data security. Furthermore, business continuity, both in society and within companies, is increasingly dependent on IT. Disruption to these core processes can have a major impact on service availability.

Cyber criminals are very aware of these vulnerabilities. Driven by a wide range of motivations – from pure financial gain, to raising the profile of an ideology, to espionage or terrorism – individual hackers, activists, organized criminals and governments are attacking government and company networks within increasing volume and severity.

But while the cyber threat is very real and its impact can be debilitating, the media often sketches an alarmist picture of cyber security, creating a culture of disproportionate fear. Not all organizations are necessarily easy targets for cyber criminals. For example, a small or midsized company has a very different risk profile than a multinational organization.

What is true for any government or organization is that cyber crime risks can be controlled. Cyber criminals are not invincible geniuses, and while they can cause real damage to your business, you can take steps to protect yourself against them. You may not be able to achieve 100 percent security, but by treating cyber security as "business as usual" and balancing investment between risks and potential impacts, your organization will be well prepared to combat cyber crime.

Organizations can reduce the risks to their business by building up capabilities in three critical areas – prevention, detection and response.

Prevention

Prevention begins with governance and organization. It is about installing fundamental measures, including placing responsibility for dealing with cyber crime within the organization and developing awareness training for key staff.

Detection

Through monitoring of critical events and incidents, an organization can strengthen its technological detection measures. Monitoring and data mining together form an excellent instrument to detect strange patterns in data traffic, to find the location on which the attacks focus and to observe system performance.

Response

Response refers to activating a well-rehearsed plan as soon as evidence of a possible attack occurs. During an attack, the organization should be able to directly deactivate all technology affected. When developing a response and recovery plan, an organization should perceive cyber security as a continuous process and not as a one-off solution.

	Prevention	Detection	Response
Management and organization	Appointing cyber crime responsibilities	Ensuring a 24/7 stand-by (crisis) organization	Using forensic analysis skills
Processes	Cyber crime response tests (simulations) Periodic scans and penetration tests	Procedures for follow-up of incidents	Cyber crime response plan
Technology	Ensuring adequate desktop security Ensuring network segmentation	Implementing logging of critical processes Implementing central monitoring of security incidents	Deactivating or discontinuing IT services under attack

02

The five most common cyber security mistakes

To many, cyber security is a bit of a mystery. This lack of understanding has created many misconceptions among management about how to approach cyber security. From our years of experience, we have seen the following five cyber security mistakes repeated over and over – often with drastic results.

1

Mistake: **"We have to achieve 100 percent security"**

Reality: **100 percent security is neither feasible nor the appropriate goal**

Almost every airline company claims that flight safety is its highest priority while recognizing that there is an inherent risk in flying. The same applies to cyber security. Whether it remains private or is made public, almost every large, well-known organization will unfortunately experience information theft.

Developing the awareness that 100 percent protection against cyber crime is neither a feasible nor an appropriate goal is already an important step towards a more effective policy, because it allows you to make choices about your defensive posture. A good defensive posture is based on understanding the threat (i.e., the criminal) relative to organizational vulnerability (prevention), establishing mechanisms to detect an imminent or actual breach (detection) and establishing a capability that immediately deals with incidents (response) to minimize loss.

In practice, the emphasis is often skewed towards prevention – the equivalent to building impenetrable walls to keep the intruders out. Once you understand that perfect security is an illusion and that cyber security is "business as usual," you also understand that more emphasis must be placed on detection and response. After a cyber crime incident, which may vary from theft of information to a disruptive attack on core systems, an organization must be able to minimize losses and resolve vulnerabilities.

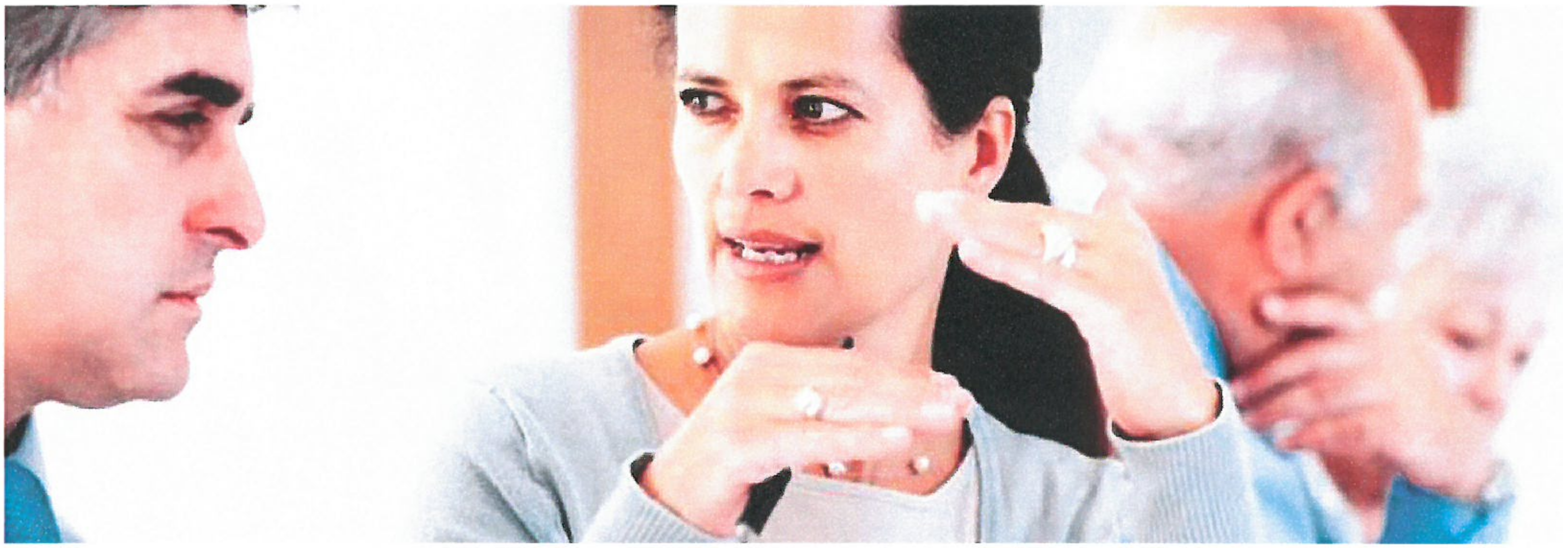
2

Mistake: **"When we invest in best-of-class technical tools, we are safe"**

Reality: **Effective cyber security is less dependent on technology than you think**

The world of cyber security is dominated by specialist suppliers that sell technical products, such as products that enable rapid detection of intruders. These tools are essential for basic security, and must be integrated into the technology architecture, but they are not the basis of a holistic and robust cyber security policy and strategy. The investment in technical tools should be the output, not the driver, of cyber security strategy. Good security starts with developing a robust cyber defense capability. Although this is generally led by the IT department, the knowledge and awareness of the end user is critical. The human factor is and remains, for both IT professionals and the end user, the weakest link in relation to security. Investment in the best tools will only deliver the return when people understand their responsibilities to keep their networks safe. Social engineering, in which hackers manipulate employees to gain access to systems, is still one of the main risks that organizations face.

Technology cannot help in this regard and it is essential that managers take ownership of dealing with this challenge. They have to show genuine interest and be willing to study how best to engage with the workforce to educate staff and build awareness of the threat from cyber attack. This is often about changing the culture such that employees are alert to the risks and are proactive in raising concerns with supervisors.



3

Mistake: **"Our weapons have to be better than those of the hackers"**

Reality: **The security policy should primarily be determined by your goals, not those of your attackers**

The fight against cyber crime is an example of an unwinnable race. The attackers keep developing new methods and technology and the defense is always one step behind. So is it useful to keep investing in increasingly sophisticated tools to prevent attack?

While it is important to keep up to date and to obtain insights into the intention of attackers and their methods, it is critical for managers to adopt a flexible, proactive and strategic approach to cyber security. Given the immeasurable value of a company's information assets, and the severe implication of any loss on the core business, cyber security policies need to prioritize investment into critical asset protection, rather the latest technology or system to detect every niche threat.

First and foremost, managers need to understand what kinds of attackers their business attracts and why. An organization may perceive the value of its assets differently than a criminal. How willing are you to accept risks to certain assets over others? Which systems and people store your key assets, keeping in mind that business and technology have developed as chains and are therefore codependent on each other's security?

4

Mistake: **"Cyber security compliance is all about effective monitoring"**

Reality: **The ability to learn is just as important as the ability to monitor**

Reality shows that cyber security is very much driven by compliance. This is understandable, because many organizations have to accommodate a range of laws and legislation. However, it is counterproductive to view compliance as the ultimate goal of cyber security policy.

Only an organization that is capable of understanding external developments and incident trends and using this insight to inform policy and strategy will be successful in combating cyber crime in the long term. Therefore, effective cyber security policy and strategy should be based on continuous learning and improvement.

- Organizations need to understand how threats evolve and how to anticipate them. This approach is ultimately more cost-effective in the long term than developing ever-higher security "walls." This goes beyond the monitoring of infrastructure: it is about smart analysis of external and internal patterns in order to understand the reality of the threat and the short-, medium- and long-term risk implications. This insight should enable organizations to make sensible security investment choices, including investing to save. Unfortunately, in practice, many organizations do not take a strategic approach and do not collect and use the internal data available to them.
- Organizations need to ensure that incidents are evaluated in such a way that lessons can be learned. In practice, however, actions are driven by real-time incidents and often are not recorded or evaluated. This destroys the ability of the organization to learn and put better security arrangements in place in the future.

- The same applies to monitoring attacks. In many cases, organizations have certain monitoring capabilities, but the findings are not shared with the wider organization. No lessons, or insufficient lessons, are learned from the information received. Furthermore, monitoring needs to be underpinned by an intelligence requirement. Only if you understand what you want to monitor does monitoring become an effective tool to detect attacks.
- Organizations need to develop an enterprise-wide method for assessing and reporting cyber security risks. This requires protocols to determine risk levels and escalations, and methods for equipping the board with insight into strategic cyber risks and the impacts to core business.

5

Mistake: **"We need to recruit the best professionals to defend ourselves from cyber crime"**

Reality: **Cyber security is not a department, but an attitude**

Cyber security is often seen as the responsibility of a department of specialist professionals. This mindset may result in a false sense of security and lead to the wider organization not taking responsibility.

The real challenge is to make cyber security a mainstream approach. This means, for example, that cyber security should become part of HR policy, even in some cases linked to remuneration. It also means that cyber security should have a central place when developing new IT systems, and not, as is often the case, be given attention only at the end of such projects.

03
The key is customization

The risks of cyber crime for a local entrepreneur compared to a globally operating multinational are vast. The former may not have the resources or expertise to adequately detect or prevent cyber crime. But the latter is a more attractive target to criminals: it is more visible, more dependent on IT, and has far more valuable assets.

It is clear that both businesses need to adopt a customized approach to cyber security, based on the character of the organization, its risk appetite and the knowledge available. Consider how a jeweler arrives at the proper level of security through a strategic, realistic and customized approach to protecting its assets. Then compare it to the current common corporate approach to cyber security.

Jeweler's perspective on theft security	Corporate perspective on cyber security
I know which assets to protect and have set up the appropriate measures.	I take measures without a having a clear idea of the assets it is essential to protect.
I perceive theft as a risk in the business and know that realistically I can't be in business if I want 100 percent security.	I see cyber crime as something exotic and strive to achieve 100 percent security.
I focus on measures that prevent a person from leaving with valuable goods.	I focus on measures that prevent a person from entering and forget to take measures that prevent a person from taking away information.
I do not let security suppliers spook me and I make my own purchasing decisions.	My security policy depends on the tools available in the marketplace, without knowing exactly what I need.
When it goes wrong or almost goes wrong, I learn a lesson.	When it goes wrong or almost goes wrong, I panic.
I train employees in how to reduce the risk of theft and talk to them when they make mistakes.	I view cyber security as mainly a matter for specialist professionals and don't want to burden the rest of the organization with it.
I invest in tools because they assist the continuity of my business.	I invest in tools because it is mandatory and because the media reports on incidents every day.

04

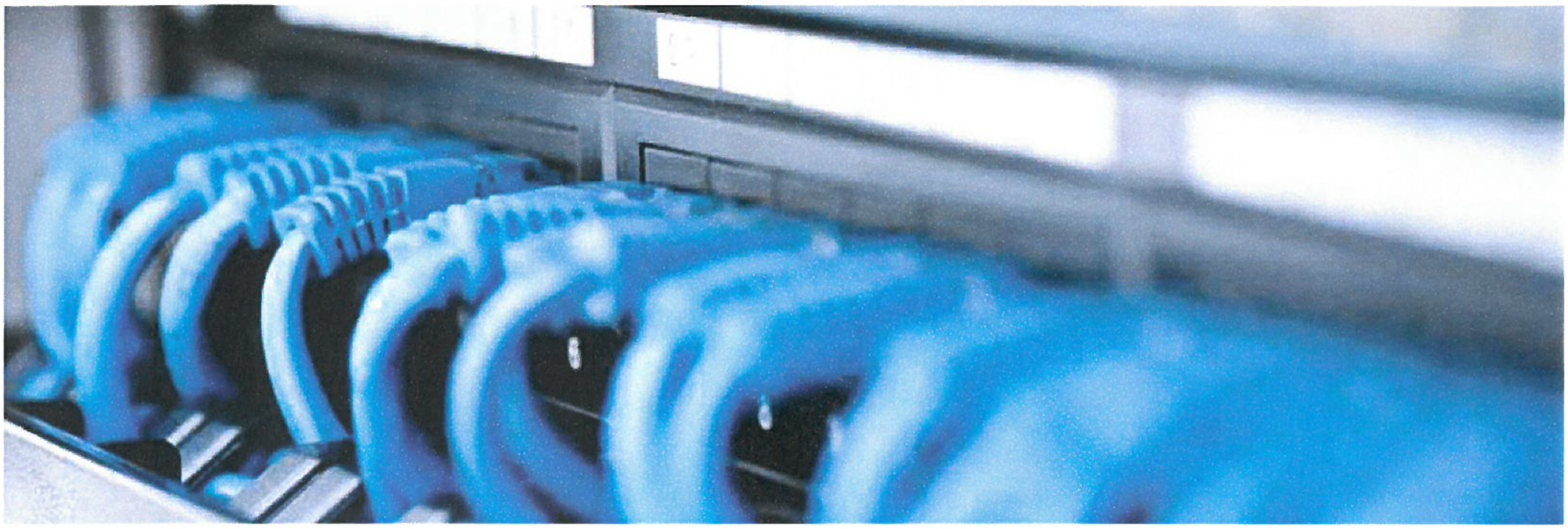
The six dimensions of cyber maturity

As management, you want to know whether your organization has an adequate approach to cyber security. At KPMG LLP (KPMG), we consider six key dimensions that together provide a comprehensive and in-depth view of an organization's cyber maturity.

Leadership and Governance
Is the board demonstrating due diligence, ownership and effective management of risk?

Human Factors
What is the level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge?

Information Risk Management
How robust is the approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners?



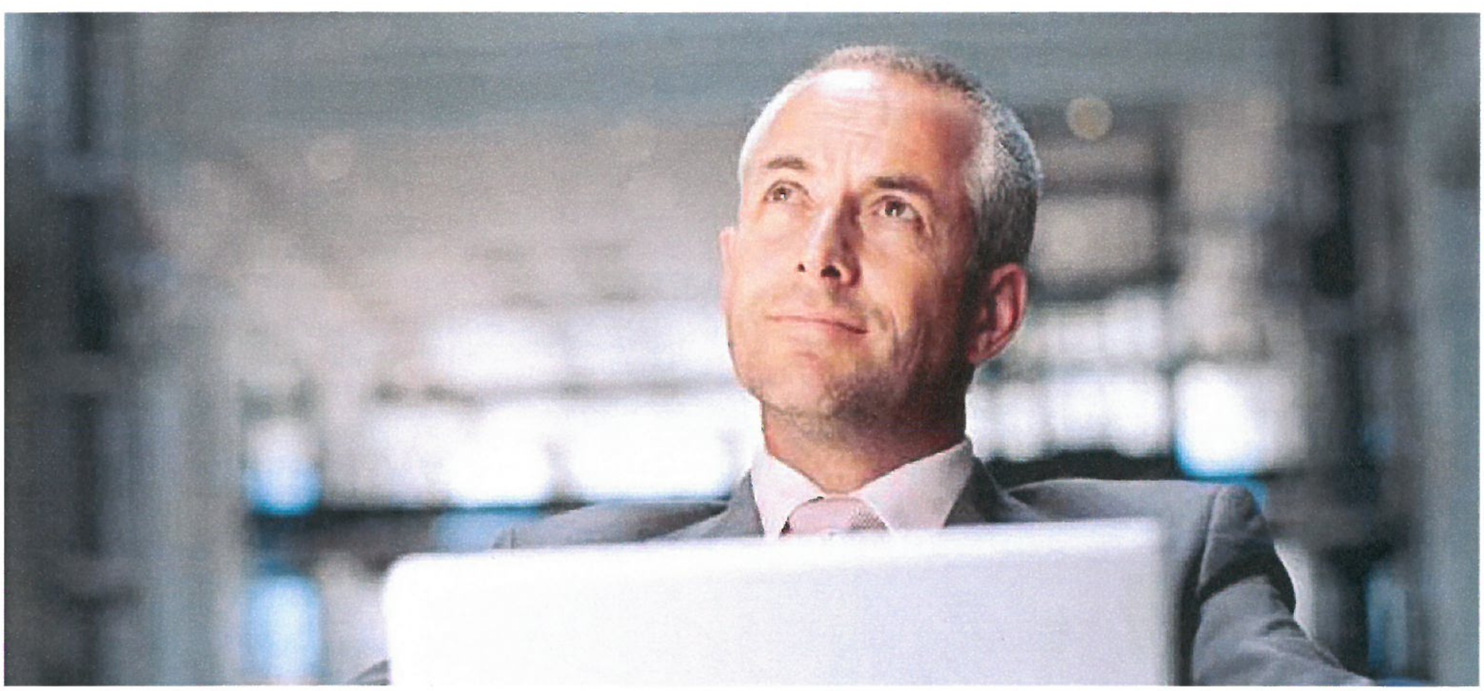
Business Continuity
Have we made preparations for a security event and the ability to prevent or minimize the impact through successful crisis and stakeholder management?

Operations and Technology
What is the level of control measures implemented to address identified risks and minimize the impact of compromise?

Legal and Compliance
Are we complying with relevant regulatory and international certification standards?

Addressing all six of these key dimensions can lead to a holistic cyber security model, providing the following advantages to any organization:

- Minimizing the risk of an attack on an organization by an outside cyber criminal, as well as limiting the impact of successful attacks
- Better information on cyber crime trends and incidents to facilitate decision making
- Clearer communication on the theme of cyber security, enabling everyone to know his or her responsibilities and what needs to be done when an incident has occurred or is suspected
- Improved reputation, as an organization that is well prepared and has given careful consideration to its cyber security is better placed to reassure its stakeholders
- Increased knowledge of competence in relation to cyber security
- Benchmarking the organization in relation to peers in the field of cyber security
-



05

Are you ready for action?

Cyber security must be on your agenda. Your management, boards, shareholders and clients all expect you to pay sufficient attention to this problem.

But just because you recognize the problem doesn't mean you are ready for action.

Developing a strategic, customized and comprehensive cyber security program, driven from the top, will help you avoid five common cyber security mistakes:

1. "We have to achieve 100 percent security"
2. "When we invest in best-of-class technical tools, we are safe"
3. "Our weapons have to be better than those of the hackers"
4. "Cyber security compliance is all about effective monitoring"
5. "We need to recruit the best professionals to defend ourselves from cyber crime"

If you have taken a holistic view of cyber security and can answer the following questions about your approach, **you are ready for action!**

1. How big is the risk for your organization and the organizations you do business with?

- How attractive is your organization to potential cyber criminals?
- How dependent is your organization on the services of partners, suppliers and other organizations, and how integrated are the corresponding IT processes?
- Do you know which processes and/or systems represent the greatest assets from a cyber security perspective?
- Have you considered how much risk you are willing to take in relation to these processes and/or systems, since there is no such thing as 100 percent security?
- Do your partners have the same risk appetite and cyber security measures as you do?
- Have you developed clear business cases for your cyber security investments?

2. Do governance processes and the organizational culture enable effective risk management?

- Do you know how the culture of your organization contributes to (or hampers) good cyber security?
- When was the last time your board communicated something about the importance of cyber security?
- Are you prepared to act in the event of a crisis or incident? Do you know how you should communicate and who should do it?
- Can you provide assurance to stakeholders on your cyber security policy?

3. How large should your cyber security budget be and how should you spend it?

Depending on the risk profile of your organization, the budget for cyber security should probably be in the range of three percent to five percent of your total IT budget. Currently, a significant part of such budgets is often spent on implementing technological solutions and solving problems from the past. The key question you need to answer is:

- Is at least three to five percent of the total IT budget dedicated to cyber security?
- How much of your cyber security budget is spent on solving past problems?
- How much is spent on structural investments in better security systems?
- How much is spent on systems and tools?
- How much is spent on awareness and culture change?

For more information on the cyber maturity assessment, incident response or KPMG's cyber security services, please visit us at www.kpmg.com/US/informationprotection or contact one of our Information Protection and Business Resilience team leaders:

Steve Barlock
Principal, Advisory
Information Protection and Business Resilience
T: 415-963-7025
E: sbarlock@kpmg.com

Tony Buffomante
Principal, Advisory
Information Protection and Business Resilience
T: 312-665-1748
E: abuffomante@kpmg.com

Fred Rica
Principal, Advisory
Information Protection and Business Resilience
T: 973-912-4524
E: frica@kpmg.com

kpmg.com

Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus

Commissioner Luis A. Aguilar

"Cyber Risks and the Boardroom" Conference
New York Stock Exchange
New York, NY

June 10, 2014

Good afternoon. Thank you for that kind introduction. I am glad to be back at the New York Stock Exchange. In anticipating today's conference, I thought back to an earlier trip to the NYSE where in April 2009, I had the opportunity to ring the closing bell. Before I begin my remarks, let me issue the standard disclaimer that the views I express today are my own, and do not necessarily reflect the views of the U.S. Securities and Exchange Commission ("SEC" or "Commission"), my fellow Commissioners, or members of the staff.

I am pleased to be here and to have the opportunity to speak about cyber-risks and the boardroom, a topic that is both timely and extremely important. Over just a relatively short period of time, cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators.[1] I suspect that not too long ago, we would have been hard-pressed to find many individuals who had even heard of cybersecurity, let alone known what it meant. Yet, in the past few years, there can be no doubt that the focus on this issue has dramatically increased.[2]

Cybersecurity has become an important topic in both the private and public sectors, and for good reason. Law enforcement and financial regulators have stated publicly that cyber-attacks are becoming both more frequent and more sophisticated.[3] Indeed, according to one survey, U.S. companies experienced a 42% increase between 2011 and 2012 in the number of successful cyber-attacks they experienced per week.[4] As I am sure you have heard, recently there have also been a series of well-publicized cyber-attacks that have generated considerable media attention and raised public awareness of this issue. A few of the more well-known examples include:

- The October 2013 cyber-attack on the software company Adobe Systems, Inc., in which data from more than 38 million customer accounts was obtained improperly;[5]
- The December 2013 cyber-attack on Target Corporation, in which the payment card data of approximately 40 million Target customers and the personal data of up to 70 million Target customers was accessed without authorization;[6]
- The January 2014 cyber-attack on Snapchat, a mobile messaging service, in which a reported 4.6 million user names and phone numbers were exposed;[7]
- The sustained and repeated cyber-attacks against several large U.S. banks, in which their public websites have been knocked offline for hours at a time;[8] and

- The numerous cyber-attacks on the infrastructure underlying the capital markets, including quite a few on securities exchanges.[9]

In addition to becoming more frequent, there are reports indicating that cyber-attacks have become increasingly costly to companies that are attacked. According to one 2013 survey, the average annualized cost of cyber-crime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009.[10] In addition, the aftermath of the 2013 Target data breach demonstrates that the impact of cyber-attacks may extend far beyond the direct costs associated with the immediate response to an attack.[11] Beyond the unacceptable damage to consumers, these secondary effects include reputational harm that significantly affects a company's bottom line. In sum, the capital markets and their critical participants, including public companies, are under a continuous and serious threat of cyber-attack, and this threat cannot be ignored.[12]

As an SEC Commissioner, the threats are a particular concern because of the widespread and severe impact that cyber-attacks could have on the integrity of the capital markets infrastructure and on public companies and investors.[13] The concern is not new. For example, in 2011, staff in the SEC's Division of Corporation Finance issued guidance to public companies regarding their disclosure obligations with respect to cybersecurity risks and cyber-incidents.[14] More recently, because of the escalation of cyber-attacks, I helped organize the Commission's March 26, 2014 roundtable to discuss the cyber-risks facing public companies and critical market participants like exchanges, broker-dealers, and transfer agents.[15]

Today, I would like to focus my remarks on what boards of directors can, and should, do to ensure that their organizations are appropriately considering and addressing cyber-risks. Effective board oversight of management's efforts to address these issues is critical to preventing and effectively responding to successful cyber-attacks and, ultimately, to protecting companies and their consumers, as well as protecting investors and the integrity of the capital markets.

The Role of the Boards of Directors in Overseeing Cyber-Risk Management

Background on the Role of Boards of Directors

When considering the board's role in addressing cybersecurity issues, it is useful to keep in mind the broad duties that the board owes to the corporation and, more specifically, the board's role in corporate governance and overseeing risk management. It has long been the accepted model, both here and around the world, that corporations are managed under the direction of their boards of directors.[16] This model arises from a central tenet of the modern corporation — the separation of ownership and control of the corporation. Under this structure, those who manage a corporation must answer to the true owners of the company — the shareholders.

It would be neither possible nor desirable, however, for the many, widely-dispersed shareholders of any public company to come together and manage, or direct the management of, that company's business and affairs. Clearly, effective full-time management is essential for public companies to function. But management without accountability can lead to self-interested decision-making that may not benefit the company or its shareholders. As a result, shareholders elect a board of directors to represent their interests, and, in turn, the board of directors, through effective corporate governance, makes sure that management effectively serves the corporation and its shareholders.[17]

Corporate Boards and Risk Management Generally

Although boards have long been responsible for overseeing multiple aspects of management's activities, since the financial crisis, there has been an increased focus on what boards of directors are doing to address risk management.[18] Indeed, many have noted that, leading up to the financial crisis, boards of directors may not have been doing enough to oversee risk management within their companies, and that this failure contributed to the unreasonably risky behavior that resulted in the destruction of untold billions in shareholder value and plunged the country and the global economy into recession.[19] Although primary responsibility for risk management has historically belonged to management, the boards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs.[20]

The importance of this oversight was highlighted when, in 2009, the Commission amended its rules to require disclosure about, among other things, the board's role in risk oversight, including a description of whether and how the board administers its oversight function, such as through the whole board, a separate risk committee, or the audit committee.[21] The Commission did not mandate any particular structure, but noted that "risk oversight is a key competence of the board" and that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."[22]

The evidence suggests that boards of directors have begun to assume greater responsibility for overseeing the risk management efforts of their companies.[23] For example, according to a recent survey of 2013 proxy filings by companies comprising the S&P 200, the full boards of these companies are increasingly, and nearly universally, taking responsibility for the risk oversight of the company.[24]

Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk[25] — and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight. The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.[26]

What Boards of Directors Can and Should Be Doing to Oversee Cyber-Risk

Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities. [27]

In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and lasting reputational harm, there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats.[28] Perhaps unsurprisingly, there has recently been a series of derivative lawsuits brought against companies and their officers and directors relating to data breaches resulting from cyber-attacks.[29] Thus, boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.

Given the known risks posed by cyber-attacks, one would expect that corporate boards and senior management universally would be proactively taking steps to confront these cyber-risks. Yet, evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks. Some have noted that boards are not spending enough time or devoting sufficient corporate resources to addressing cybersecurity issues.[30] According to one survey, boards were not undertaking key oversight activities related to cyber-risks, such as reviewing annual budgets for privacy and IT security programs, assigning roles and responsibilities for privacy and security, and receiving regular reports on breaches and IT risks.[31] Even when boards do pay attention to these risks, some have questioned the extent to which boards rely too much on the very personnel who implement those measures.[32] In light of these observations, directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management.

NIST Cybersecurity Framework

In considering where to begin to assess a company's possible cybersecurity measures, one conceptual roadmap boards should consider is the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology ("NIST") in February 2014. The NIST Cybersecurity Framework is intended to provide companies with a set of industry standards and best practices for managing their cybersecurity risks.[33] In essence, the Framework encourages companies to be proactive and to think about these difficult issues in advance of the occurrence of a possibly devastating cyber-event. While the Framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes.[34] At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed.

Board Structural Changes to Focus on Appropriate Cyber-Risk Management

The NIST Cybersecurity Framework, however, is a bible without a preacher if there is no one at the company who is able to translate its concepts into action plans. Frequently, the board's risk oversight function lies either with the full board or is delegated to the board's audit committee. Unfortunately, many boards lack the technical expertise necessary to be able to evaluate whether management is taking appropriate steps to address cybersecurity issues. Moreover, the board's audit committee may not have the expertise, support, or skills necessary to add oversight of a company's cyber-risk management to their already full agenda.[35] As a result, some have recommended mandatory cyber-risk education for directors.[36] Others have suggested that boards be at least adequately represented by members with a good understanding of information technology issues that pose risks to the company.[37]

Another way that has been identified to help curtail the knowledge gap and focus director attention on known cyber-risks is to create a separate enterprise risk committee on the board. It is believed that such committees can foster a “big picture” approach to company-wide risk that not only may result in improved risk reporting and monitoring for both management and the board, but also can provide a greater focus — at the board level — on the adequacy of resources and overall support provided to company executives responsible for risk management.[38] The Dodd-Frank Act already requires large financial institutions to establish independent risk committees on their boards.[39] Beyond the financial institutions required to do so, some public companies have chosen to proactively create such risk committees on their boards.[40] Research suggests that 48% of corporations currently have board-level risk committees that are responsible for privacy and security risks, which represents a dramatic increase from the 8% that reported having such a committee in 2008.[41]

Clearly, there are various mechanisms that boards can employ to close the gap in addressing cybersecurity concerns — but it is equally clear that boards need to be proactive in doing so. Put simply, boards that lack an adequate understanding of cyber-risks are unlikely to be able to effectively oversee cyber-risk management.

I commend the boards that are proactively addressing these new risks of the 21st Century. However, while enhancing board knowledge and board involvement is a good business practice, it is not necessarily a panacea to comprehensive cybersecurity oversight.

Internal Roles and Responsibilities Focused on Cyber-Risk

In addition to proactive boards, a company must also have the appropriate personnel to carry out effective cyber-risk management and to provide regular reports to the board. One 2012 survey reported that less than two-thirds of responding companies had full-time personnel in key roles responsible for privacy and security, in a manner that was consistent with internationally accepted best practices and standards.[42] In addition, a 2013 survey found that the companies that detected more security incidents and reported lower average financial losses per incident shared key attributes, including that they employed a full-time chief information security officer (or equivalent) who reported directly to senior management.[43]

At a minimum, boards should have a clear understanding of who at the company has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company’s cyber-risk management practices.[44] In addition, as the evidence shows, devoting full-time personnel to cybersecurity issues may help prevent and mitigate the effects of cyber-attacks.

Board Preparedness

Although different companies may choose different paths, ultimately, the goal is the same: to prepare the company for the inevitable cyber-attack and the resulting fallout from such an event. As it has been noted, the primary distinction between a cyber-attack and other crises that a company may face is the speed with which the company must respond to contain the rapid spread of damage.[45] Companies need to be prepared to respond within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done, and prepare a response to the event.[46]

While there is no "one-size-fits-all" way to properly prepare for the various ways a cyber-attack can unfold, and what responses may be appropriate, it can be just as damaging to have a poorly-implemented response to a cyber-event. As others have observed, an "ill-thought-out response can be far more damaging than the attack itself."[47] Accordingly, boards should put time and resources into making sure that management has developed a well-constructed and deliberate response plan that is consistent with best practices for a company in the same industry.

These plans should include, among other things, whether, and how, the cyber-attack will need to be disclosed internally and externally (both to customers and to investors).[48] In deciding the nature and extent of the disclosures, I would encourage companies to go beyond the impact on the company and to also consider the impact on others. It is possible that a cyber-attack may not have a direct material adverse impact on the company itself, but that a loss of customers' personal and financial data could have devastating effects on the lives of the company's customers and many Americans. In such cases, the right thing to do is to give these victims a heads-up so that they can protect themselves.[49]

Conclusion

Let me conclude my remarks by reaffirming the significance of the role of good corporate governance. Corporate governance performed properly, results in the protection of shareholder assets. Fortunately, many boards take on this difficult and challenging role and perform it well. They do so by, among other things, being active, informed, independent, involved, and focused on the interests of shareholders.

Good boards also recognize the need to adapt to new circumstances — such as the increasing risks of cyber-attacks. To that end, board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks.

Those of you who have taken the time and effort to be here today clearly recognize the risks, and I commend you for being proactive in dealing with the issue.

Thank you for inviting me to speak to you today.

[1] For example, the Director of the Federal Bureau of Investigation (FBI), James Comey, said last November that "resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats." *See,* Testimony of James B. Comey, Jr., Director, FBI, U.S. Department of Justice, before the Senate Committee on Homeland Security and Governmental Affairs (Nov. 14, 2013), *available at* http://www.hsgac.senate.gov/hearings/threats-to-the-homeland. *See also,* Testimony of Jeh C. Johnson, Secretary, U.S. Department of Homeland Security, before the House Committee on Homeland Security (Feb. 26, 2014) ("DHS must continue efforts to address the growing cyber threat to the private sector and the '.gov' networks, illustrated by the real, pervasive, and ongoing series of attacks on public and private infrastructure."), *available at* http://docs.house.gov/meetings/HM/HM00/20140226/101722/HHRG-113-HM00-Wstate-

JohnsonJ-20140226.pdf; Testimony of Ari Baranoff, Assistant Special Agent in Charge, United States Secret Service Criminal Investigative Division, before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (Apr. 16, 2014), *available at* http://docs.house.gov/meetings/HM/HM08/20140416/102141/HHRG-113-HM08-Wstate-BaranoffA-20140416.pdf ("Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cybercrimes targeting private industry and critical infrastructure."); Remarks by Secretary of Defense Leon E. Panetta to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 ("As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East. And the cyber threats facing this country are growing.").

[2] *See, e.g.*, Martin Lipton, *et al.*, *Risk Management and the Board of Directors — An Update for 2014*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Apr. 22, 2014), *available at* http://blogs.law.harvard.edu/corpgov/2014/04/22/risk-management-and-the-board-of-directors-an-update-for-2014/ (noting that cybersecurity is a risk management issue that "merits special attention" from the board of directors in 2014); PwC 2012 Annual Corporate Directors Survey, *Insights from the Boardroom 2012: Board evolution: Progress made yet challenges persist*, *available at* http://www.pwc.com/en_US/us/corporate-governance/annual-corporate-directors-survey/assets/pdf/pwc-annual-corporate-directors-survey.pdf (finding that 72% of directors are engaged with overseeing and understanding data security issues and risks related to compromising customer data); Michael A. Gold, *Cyber Risk and the Board of Directors–Closing the Gap*, Bloomberg BNA (Oct. 18, 2013) *available at* http://www.bna.com/cyber-risk-and-the-board-of-directors-closing-the-gap// ("The responsibility of corporate directors to address cyber security is commanding more attention and is obviously a significant issue."); Deloitte Development LLC, *Hot Topics: Cybersecurity … Continued in the boardroom*, Corporate Governance Monthly (Aug. 2013), *available at* http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Deloitte%20Periodicals/Hot%20Topics/Hot%20Topics%20-%20Cybersecurity%20%20%20Continued%20in%20the%20boardroom%20-August%202013%20-Final.pdf ("Not long ago, the term 'cybersecurity' was not frequently heard or addressed in the boardroom. Cybersecurity was often referred to as an information technology risk, and management and oversight were the responsibility of the chief information or technology officer, not the board. With the rapid advancement of technology, cybersecurity has become an increasingly challenging risk that boards may need to address."); Holly J. Gregory, *Board Oversight of Cybersecurity Risks*, Thomson Reuters Practical Law (Mar. 1, 2014), *available at* http://us.practicallaw.com/5-558-2825 ("The risk of cybersecurity breaches (and the harm that these breaches pose) is one of increasing significance for most companies and therefore an area for heightened board focus.").

[3] For example, on December 9, 2013, the Financial Stability Oversight Council held a meeting to discuss cybersecurity threats to the financial system. *See*, U.S. Department of the Treasury Press Release, "Financial Stability Oversight Council to Meet December 9," *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl2228.aspx. During that meeting, Assistant Treasury Secretary Cyrus-Amir-Mokri said that "[o]ur experience over the last couple of years shows that cyber-threats to financial institutions and markets are growing in both frequency and sophistication." *See,* Remarks of Assistant Secretary Cyrus Amir-Mokri on Cybersecurity at a Meeting of the Financial Stability Oversight Council (Dec. 9, 2013), *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl2234.aspx. In addition, in testimony before the House Financial Services Committee in 2011, the Assistant Director of the FBI's Cyber Division stated that the number and sophistication of malicious incidents involving financial institutions has increased dramatically over the past several years and offered numerous examples of such attacks, which included fraudulent monetary transfers, unauthorized financial transactions from compromised bank and brokerage accounts, denial of service attacks on U.S. stock exchanges, and hacking incidents in which confidential information was misappropriated. *See,* Testimony of Gordon M. Snow, Assistant Director, Cyber Division, FBI, U.S. Department of Justice, before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit (Sept. 14, 2011), *available at* http://financialservices.house.gov/uploadedfiles/091411snow.pdf.

[4] *2012 Cost of Cyber Crime Study: United States*, Ponemon Institute LLC and HP Enterprise Security (Oct. 2012), *available at* http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[5] *See, e.g.,* Jim Finkle, *Adobe says customer data, source code accessed in cyber attack*, Reuters (Oct. 3, 2013), *available at* http://www.reuters.com/article/2013/10/03/us-adobe-cyberattack-idUSBRE99212Y20131003; Jim Finkle, *Adobe data breach more extensive than previously disclosed*, Reuters (Oct. 29, 2013), *available at* http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029; Danny Yadron, *Hacker Attack on Adobe Sends Ripples Across Web*, Wall Street Journal (Nov. 11, 2013), *available at* http://online.wsj.com/news/articles/SB10001424052702304644104579192393329283358.

[6] *See,* Testimony of John Mulligan, Executive Vice President and Chief Financial Officer of Target, before the Senate Judiciary Committee (Feb. 4, 2014), *available at* http://www.judiciary.senate.gov/imo/media/doc/02-04-14MulliganTestimony.pdf; Target Press Release, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores" (Dec. 19, 2013), *available at* http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.

[7] *See, e.g.,* Andrea Chang and Salvador Rodriguez, *Snapchat becomes target of widespread cyberattack*, L.A. Times (Jan. 2, 2014), *available at* http://articles.latimes.com/2014/jan/02/business/la-fi-snapchat-hack-20140103; Brian Fung, *A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix?* Washington Post (Jan. 1, 2014), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/.

[8] *See, e.g.,* Joseph Menn, *Cyber attacks against banks more severe than most realize*, Reuters (May 18, 2013), *available at* http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518; Bob Sullivan, *Bank Website Attacks Reach New Highs*, CNBC (Apr. 3, 2013), *available at* http://www.cnbc.com/id/100613270.

[9] For example, according to a 2012 global survey of securities exchanges, 53% reported experiencing a cyber-attack in the previous year. *See,* Rohini Tendulkar, *Cyber-crime, securities markets, and systemic risk*, Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges (July 16, 2013), *available at* http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf. Forty-six securities exchanges responded to the survey.

[10] *See*, HP Press Release, *HP Reveals Cost of Cybercrime Escalates 70 Percent, Time to Resolve Attacks More Than Doubles* (Oct. 8, 2013), *available at* http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128.

[11] *See*, Target Financial News Release, *Target Reports Fourth Quarter and Full-Year 2013 Earnings* (Feb. 26, 2014), *available at* http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight (including a statement from then-Chairman, President and CEO Gregg Steinhafel that Target's fourth quarter results "softened meaningfully following our December announcement of a data breach."); Elizabeth A. Harris, *Data Breach Hurts Profit at Target*, N.Y. Times (Feb. 26, 2014), *available at* http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html?_r=0 (noting that "[t]he widespread theft of Target customer data had a significant impact on the company's profit, which fell more than 40 percent in the fourth quarter" of 2013).

[12] I also want to note that at the Investment Company Institute's ("ICI") general membership meeting, held just last month, the issue of cybersecurity was front and center. Among the issues raised during the meeting was the "huge risk to brand" for a firm if they have a security failure in the event of a cyber-attack. A separate panel at the ICI conference devoted to cybersecurity also discussed the shift in focus from building "hard walls" to protect against risks from outside the company to cybersecurity focused on "inside" risks, such as ensuring that individuals with mobile applications or other types of flexible applications don't introduce, intentionally or unintentionally, malware or other kinds of security breaches that could lead to a cyber-attack on the company. *See, e.g.,* Jackie Noblett, *Cyber Breach a "Huge Risk to Brand,"* Ignites (May 29, 2014), *available at* http://ignites.com/c/897654/86334/cyber_breach_huge_risk_brand?referrer_module=emailMorningNews&module_order=7.

[13] *See,* Commissioner Luis A. Aguilar, *The Commission's Role in Addressing the Growing Cyber-Threat* (Mar. 26, 2014), *available at* http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184.

[14] On October 13, 2011, staff in the Commission's Division of Corporation Finance (Corp Fin) issued guidance on issuers' disclosure obligations relating to cyber security risks and cyber incidents. *See,* SEC's Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2—Cybersecurity* ("SEC Guidance") (Oct. 31, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Among other things,

this guidance notes that securities laws are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision, and cybersecurity risks and events are not exempt from these requirements. The guidance identifies six areas where cybersecurity disclosures may be necessary under Regulation S-K: (1) Risk Factors; (2) Management's Discussion and Analysis of Financial Condition and Results of Operation (MD&A); (3) Description of Business; (4) Legal Proceedings; (5) Financial Statement Disclosures; and (6) Disclosure Controls and Procedures. The SEC Guidance further recommends that material cybersecurity risks should be disclosed and adequately described as Risk Factors. Where cybersecurity risks and incidents that represent a material event, trend or uncertainty reasonably likely to have a material impact on the organization's operations, liquidity, or financial condition — it should be addressed in the MD&A. If cybersecurity risks materially affect the organization's products, services, relationships with customers or suppliers, or competitive conditions, the organization should disclose such risks in its description of business. Data breaches or other incidents can result in regulatory investigations or private actions that are material and should be discussed in the Legal Proceedings section. Cybersecurity risks and incidents that represent substantial costs in prevention or response should be included in Financial Statement Disclosures where the financial impact is material. Finally, where a cybersecurity risk or incident impairs the organization's ability to record or report information that must be disclosed, Disclosure Controls and Procedures that fail to address cybersecurity concerns may be ineffective and subject to disclosure. Some have suggested that such disclosures fail to fully inform investors about the true costs and benefits of companies' cybersecurity practices, and argue that the Commission (and not the staff) should issue further guidance regarding issuers' disclosure obligations. *See,* Letter from U.S. Senator John D. Rockefeller IV to Chair White (Apr. 9, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51.

[15] *See* SEC Press Release, *SEC Announces Agenda, Panelists for Cybersecurity Roundtable* (Mar. 24, 2014), *available at* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541253749; *Cybersecurity Roundtable Webcast* (Mar. 26, 2014), *available at* http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml. In addition, the SEC's National Exam Program has included cybersecurity among its areas of focus in its National Examination Priorities for 2014. *See,* SEC's National Exam Priorities for 2014, *available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf. In addition, it was recently announced that SEC examiners will review whether asset managers have policies to prevent and detect cyber-attacks and are properly safeguarding against security risks that could arise from vendors having access to their systems. *See,* Sarah N. Lynch, *SEC examiners to review how asset managers fend off cyber attacks*, Reuters (Jan. 30, 2014), *available at* http://www.reuters.com/article/2014/01/30/us-sec-cyber-assetmanagers-idUSBREA0T1PJ20140130. FINRA has also identified cybersecurity as one of its examination priorities for 2014. *See,* FINRA's 2014 Regulatory and Examination Priorities Letter (Jan. 2, 2014), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p419710.pdf.

To continue the discussion and to allow the public to weigh in on this important topic, the SEC set up a public comment file associated with the Cybersecurity Roundtable. To date, we have received ten comment letters from academics, software companies, and other interested parties, *available at* http://www.sec.gov/comments/4-673/4-673.shtml. *See, e.g.*, Jodie Kelly, Senior Vice President and General Counsel, BSA| The Software Alliance comment letter (Apr. 30, 2014) (highlighting the importance of strong internal controls related to software assets as a first line of defense against cyber-attacks, and noting that verifying legal use of software is a critical first step in deterring cyber-attacks because the "existence and availability of pirated and counterfeit software exposes corporate information technology networks to significant risks in many ways."); Tom C.W. Lin, Associate Professor of Law, Temple University Beasley School of Law comment letter (Apr. 29, 2014) (expressing support for the roundtable and the Commission's attention to cybersecurity and highlighting four broad issues for the Commission's consideration: (1) cybersecurity threats to the high-speed, electronically connected modern capital markets can create systemic risks; (2) due to technological advances, financial choices are made by both people and machines, which does not comport congruently with many traditional modes of securities regulation; (3) incentives, in addition to penalties, should be designed to encourage firms to upgrade their cybersecurity capabilities; and (4) private regulation of cybersecurity should be vigorously enhanced and leveraged to better complement government regulation); Dave Parsonage, CEO, MitoSystems, Inc. comment letter (Apr. 3, 2014); Gail P. Ricketts, Senior IT Compliance and Risk Analyst, ON Semiconductor comment letter (Mar. 26, 2014) (suggesting future roundtables include speakers from outside the financial services industry, such as manufacturing); Michael Utzig, IT Director, Hefren Tillotson, Inc. comment letter (Mar. 26, 2014) (noting that readily available technologies that can protect email communications are not widely used despite universal understanding that cybersecurity is a high-priority); Cathy Santoro comment letter (Mar. 26, 2014) (raising questions about the interactions between banks and service providers and the measures being undertaken regarding mobile payment cybersecurity risks); Duane Kuroda, Senior Threat Researcher, NetCitadel comment letter (Mar. 25, 2014) (noting that the panel discussion should focus on the process and people involved in responding to breaches and not just their detection); William Pfister, Jr. comment letter (Mar. 25, 2014) (requesting that one of the panels address the potential conflicts between national security and required disclosure). Many of these letters are generally supportive of the Commission's efforts and focus in this area, and some identify issues and concerns that were not discussed in detail during the roundtable and warrant further attention. For example, one commenter highlighted the need for companies to adopt sound internal controls over the legal use of software, noting that pirated and counterfeit software can expose companies to heightened risk of cyber-attacks and recommending that registrants report on the status of such internal controls.[15] *See, e.g.*, Jodie Kelly, Senior Vice President and General Counsel, BSA| The Software Alliance comment letter (Apr. 30, 2014) (noting, among other things, that unlicensed software eliminates the opportunity for security updates and patches from legitimate vendors when security breaches are identified, and that malware and viruses may be contained within pirated software itself or reside on the networks from which it is downloaded. BSA recommends that registrants report on the status of their internal controls in the area of licensing and legal use of software, and that such controls should, at a minimum, ensure that software is only purchased from authorized vendors and that companies should have procedures to conduct periodic software inventories and limit exposure to malware and viruses brought into their systems by linkage of employees' personal devices to corporate systems). I encourage others to comment and provide valuable input on this critical issue.

[16] *See, e.g.*, Model Bus. Corp. Act § 8.01 (2002); Del. Gen. Corp. Law § 141(a).

[17] For additional thoughts on the importance of effective corporate governance, *see* Commissioner Luis A. Aguilar, *Looking at Corporate Governance from the Investor's Perspective*, *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370541547078.

[18] *See, e.g.*, Committee of Sponsoring Organizations of the Treadway Commission, *Effective Enterprise Risk Oversight: The Role of the Board of Directors* (2009), *available at* http://www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf ("Clearly, one result of the financial crisis is an increased focus on the effectiveness of board risk oversight practices."); Committee of Sponsoring Organizations of the Treadway Commission, *Board Risk Oversight: A Progress Report — Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities* (Dec. 2010), *available at* http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf ("Risk oversight is a high priority on the agenda of most boards of directors. Recently, the importance of this responsibility has become more evident in the wake of an historic global financial crisis, which disclosed perceived risk management weaknesses across financial services and other organizations worldwide. Based on numerous legislative and regulatory actions in the United States and other countries as well as initiatives in the private sector, it is clear that expectations for more effective risk oversight are being raised not just for financial services companies, but broadly across all types of businesses."); David A. Katz, *Boards Play A Leading Role in Risk Management Oversight*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Oct. 8, 2009), *available at* http://blogs.law.harvard.edu/corpgov/2009/10/08/boards-play-a-leading-role-in-risk-management-oversight/ ("Just as the Enron and other high-profile corporate scandals were seen as resulting from a lack of ethics and oversight, the credit market meltdown and resulting financial crisis have been blamed in large part on inadequate risk management by corporations and their boards of directors. As a result, along with the task of implementing corporate governance procedures and guidelines, a company's board of directors is expected to take a leading role in overseeing risk management structures and policies.").

[19] Nicola Faith Sharpe, *Informational Autonomy in the Boardroom*, 201 U. Ill. L. Rev. 1089 (2013) ("The financial crisis of 2007-2008 was one of the worst in U.S. history. In a single quarter, the blue chip company Lehman Brothers (who eventually went bankrupt) lost $2.8 billion. While commentators have identified multiple reasons why the crisis occurred, many posit that boards mismanaged risk and failed in their oversight duties, which directly contributed to their firms failing."); Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. Marshall J. Computer & Info. L. 313 (Spring 2011) ("With accusations that boards of directors of financial institutions were asleep at the wheel while their companies engaged in risky behavior that erased millions of dollars of shareholder value and plunged the country into recession, increasing pressure is now being placed on public company boards to shoulder the burden of risk oversight for the companies they serve."); William B. Asher, Jr., Michael T. Gass, Erik Skramstad, and Michele Edwards, *The Role of Board of Directors in Risk Oversight in a Post-Crisis Economy*, Bloomberg

Law Reports-Corporate Law Vol. 4, No. 13, *available at* http://www.choate.com/uploads/113/doc/Asher,%20Gass%20-The%20Role%20of%20Board%20of%20Directors%20in%20Risk%20Oversight%20in%20a%20Post-Crisis%20Economy.pdf ("Senior management and corporate directors face renewed criticism surrounding risk management practices and apparent failures in oversight that are considered, at least in part, to be at the root of the recent crisis.").

[20] *See, e.g.,* Stephen M. Bainbridge, *Caremark and Enterprise Risk Management*, 34 Iowa J. Corp. L. 967 (2009) ("Although primary responsibility for risk management rests with the corporation's top management team, the board of directors is responsible for ensuring that the corporation has established appropriate risk management programs and for overseeing management's implementation of such programs."); Martin Lipton, *Risk Management and the Board of Directors–An Update for 2014*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Apr. 22, 2014), *available at* http://blogs.law.harvard.edu/corpgov/2014/04/22/risk-management-and-the-board-of-directors-an-update-for-2014/ (". . . the board cannot and should not be involved in actual day-to day risk *management*. Directors should instead, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization. The board should establish that the CEO and the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risks that underlie its risk oversight. Through its oversight role, the board can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is instead an integral component of strategy, culture and business operations.").

[21] *Proxy Disclosure Enhancements*, SEC Rel. No. 33-9089 (Dec. 16, 2009), 74 Fed. Reg. 68334, *available at* http://www.sec.gov/rules/final/2009/33-9089.pdf.

[22] *Id.* That amendment also required disclosure of a company's compensation policies and practices as they relate to a company's risk management in order to help investors identify whether the company has established a system of incentives that could lead to excessive or inappropriate risk taking by its employees.

[23] *Supra* note 19, William B. Asher, Jr. *et al.*, *The Role of Board of Directors in Risk Oversight in a Post-Crisis Economy* ("We know today, however, that risk management has indeed forced its way into the boardroom and that there has been a substantial change in the relationship between the overseers of public companies and their shareholders.").

[24] *Risk Intelligent Proxy Disclosures — 2013: Trending upward*, Deloitte (2013), *available at* http://deloitte.wsj.com/riskandcompliance/files/2014/01/Risk_Intelligent_Proxy_Disclosures_2013.pdf (noting that 91% of the issuers of proxy disclosures noted that "the full board is responsible for risk.").

[25] See, *Proxy Disclosure Enhancements*, *supra* note 21.

[26] Paul Ziobro, *Target Shareholders Should Oust Directors, ISS Says*, Wall St. Journal (May 28, 2014), *available at* http://online.wsj.com/article/BT-CO-20140528-709863.html; Bruce Carton, *ISS Recommends Ouster of Seven Target Directors for Data Breach Failures*, ComplianceWeek (May 29, 2014), *available at* http://www.complianceweek.com/iss-recommends-ouster-of-seven-target-directors-for-data-breach-failures/article/348954/?DCMP=EMC-CW-WeekendEdition.

[27] *See, e.g.*, *Risk Management and the Board of Directors–An Update for* 2014, *supra* note 2 (noting that cybersecurity is a risk management issue that "merits special attention" from the board of directors in 2014); Alice Hsu, Tracy Crum, Francine E. Friedman, and Karol A. Kepchar, *Cybersecurity Update: Are Data Breach Disclosure Requirements On Target?*, The Metropolitan Corporate Counsel (Jan. 24, 2014), *available at* http://www.metrocorpcounsel.com/articles/27148/cybersecurity-update-are-data-breach-disclosure-requirements-target ("As part of a board's risk management oversight function, directors should assess the adequacy of their company's data security measures. Among other things, boards should have a clear understanding of the company's cybersecurity risk profile and who has primary responsibility for cybersecurity risk oversight and should ensure the adequacy of the company's cyber risk management practices, as well as the company's insurance coverage for losses and costs associate with data breaches.").

[28] Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 Rich. J.L. & Tech. 12 (2013), *available at* http://jolt.richmond.edu/v19i4/article12.pdf. (indicating that "[t]he principles thus enunciated raise the specter of potential liability if officers and directors utterly fail to ensure the adequacy of information systems."); J. Wylie Donald and Jennifer Black Strutt, *Cybersecurity: Moving Toward a Standard of Care for the Board,* Bloomberg BNA (Nov. 4, 2013), *available at* http://www.bna.com/cybersecurity-moving-toward-a-standard-of-care-for-the-board/ (quoting from a Delaware Chancery Court decision stating that directors may be liable if "(a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.").

[29] *See, e.g., Collier v. Steinhafel et al.* (D.C. Minn. Jan. 2014), case number 0:14-cv-00266 (alleging that Target's board and top executives harmed the company financially by failing to take adequate steps to prevent the cyber-attack then by subsequently providing customers with misleading information about the extent of the data theft.); *Dennis Palkon et al. v. Stephen P. Holmes et al*. (D.C.N.J. May 2014), case number 2:14-cv-01234 (alleging that Wyndham's board and top executives harmed the company financially by failing to take adequate steps to safeguard customers' personal and financial information.).

[30] Steven P. Blonder, *How closely is the board paying attention to cyber risks?*, Inside Counsel (formerly Corporate Legal Times) (Apr. 9, 2014), *available at* http://www.insidecounsel.com/2014/04/09/how-closely-is-the-board-paying-attention-to-cyber. (Indicating that "[i]n all likelihood, absent an incident, it is likely that board members are not spending sufficient time evaluating or analyzing the risks inherent in new technologies, as well as their related cybersecurity risks.").

[31] Jody R. Westby, *Governance of Enterprise Security: CyLab 2012 Report — How Boards & Senior Executives Are Managing Cyber Risks*, Carnegie Mellon University CyLab (May 16, 2012), at 5. (Hereinafter "CyLab 2012 Report.").

[32] *Supra note 30,* Steven P. Blonder, *How Closely is the Board Paying Attention to Cyber Risks?* (stating that "[f]urther, even if a board has evaluated these risks, to what extent is such an evaluation dependent on a company's IT department — the same group implementing the existing technology protocols?").

[33] The National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) (the "NIST Cybersecurity Framework"), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, was released in response to President Obama's issued Executive Order 13636, titled "Improving Critical Infrastructure Cybersecuity," dated February 12, 2013. The NIST Cybersecurity Framework sets out five core functions and categories of activities for companies to implement that relate generally to cyber-risk management and oversight, which the NIST helpfully boiled down to five terms: Identify, Protect, Detect, Respond and Recover. This core fundamentally means the following: companies should (i) *identify* known cybersecurity risks to their infrastructure; (ii) develop safeguards to *protect* the delivery and maintenance of infrastructure services; (iii) implement methods to *detect* the occurrence of a cybersecurity event; (iv) develop methods to *respond* to a detected cybersecurity event; and (v) develop plans to *recover* and restore the companies' capabilities that were impaired as a result of a cybersecurity event. *See also,* Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*, The Metropolitan Corporate Counsel (Mar. 17, 2014), *available at* http://www.sheppardmullin.com/media/article/1280_MCC-Cybersecurity-Breaching%20The%20Boardroom.pdf.

[34] *Supra note* 2*,* Holly J. Gregory, *Board Oversight of Cybersecurity Risks; supra note* 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom* (stating that "[w]hile adoption of the Cybersecurity Framework is voluntary, it will likely become a key reference for regulators, insurance companies and the plaintiffs' bar in assessing whether a company took steps reasonably designed to reduce and manage cybersecurity risks.").

[35] Matteo Tonello, *Should Your Board Have a Separate Risk Committee?*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Feb. 12, 2012), *available at* https://blogs.law.harvard.edu/corpgov/2012/02/12/should-your-board-have-a-separate-risk-committee/ (asking "[d]oes the audit committee have the time, the skills, and the support to do the job, given everything else it is required to do?").

[36] *See, e.g.*, Katie W. Johnson, *Publicly Traded Companies Should Prepare To Disclose Cybersecurity Risks, Incidents*, Bloomberg BNA (Mar. 17, 2014), *available at* http://www.bna.com/publicly-traded-companies-n17179885721/ (citing Mary Ellen Callahan, Chair of the Privacy and Information Governance Practice at Jenner & Block, LLP at the International Association of Privacy Professionals Global Privacy Summit, held in March 2014); Michael A. Gold, *Cyber Risk and the Board of Directors — Closing the Gap*, Bloomberg BNA (Oct. 18, 2013), *available at* http://www.bna.com/cyber-risk-and-the-board-of-directors-closing-the-gap// (suggesting that companies would do well to have "[m]andatory cyber risk education for directors," among other things.); *see also, The Comprehensive National*

Cybersecurity Initiative, initially launched by then-President George W. Bush in 2008, referencing "Initiative #8. Expand cyber education," and *available at* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[37] *Supra* note 19, Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*.

[38] *Supra* note 35, Matteo Tonello, *Should Your Board Have a Separate Risk Committee?*; *supra* note 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*.

[39] Dodd-Frank Act Section 165(h).

[40] *Supra* note 19, Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*.

[41] Deloitte Audit Committee Brief, *Cybersecurity and the audit committee* (Aug. 2013), at 2, *available at* http://deloitte.wsj.com/cfo/files/2013/08/ACBrief_August2013.pdf.

[42] *See*, *supra* note 31, CyLab 2012 Report, at 27.

[43] PricewaterhouseCoopers LLP, *The Global State of Information Security Survey 2014*, at 4, *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml (the "PwC IS Survey"). The PwC IS Survey also noted other shared attributes, such as having (i) an overall information security strategy; (ii) measured and reviewed the effectiveness of their security measures within the past year; and (iii) an understanding as to exactly what type of security events have occurred in the past year. *See also*, *supra* note 2, Holly Gregory, *Board Oversight of Cybersecurity Risks*.

[44] *Supra* note 27, Alice Hsu, *et al.*, *Cybersecurity Update: Are Data Breach Disclosure Requirements on Target?*.

[45] *See, e.g.,* Roland L. Trope and Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid,* 40 Wm. Mitchell L. Rev. 647 (2014), at 656 (stating that "unlike other corporate crises, boards and management must be ready to address severe cyber incidents with response and recovery plans that activate upon discovery of an intrusion and with little or no time for deliberation.") Some observers have even suggested that companies conduct "cyberwar games" organized around hypothetical business scenarios in order to reenact how a company might respond in a real cybersecurity situation in order to fix what vulnerabilities are teased out from the simulated scenario. Tucker Bailey, James Kaplan, and Allen Weinberg, *Playing war games to prepare for a cyberattack*, McKinsey & Company Insights & Publications (July 2012). Other observers have suggested that companies implement a response plan that takes into consideration a number of factors, such as (i) how much risk the company can accept if systems or services have to shut down; (ii) for how long the company can sustain operations using limited or backup technology; and (iii) how quickly the company can restore full operations. *See, Former FBI Agent Mary Galligan on Preparing for a Cyber Attack,* CIO Journal, Deloitte Insights (Mar. 3, 2104), *available at* http://deloitte.wsj.com/cio/2014/03/03/former-fbi-agent-mary-galligan-on-preparing-for-a-cyber-attack/.

[46] *See, e.g., id.*, Roland L. Trope and Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid*, at 656.

[47] *Supra* note 45, Tucker Bailey, James Kaplan, and Allen Weinberg, *Playing War Games to Prepare for a Cyberattack*.

[48] *Supra* note 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*, Metropolitan Corporate Counsel (stating that "Boards should prepare for worst-case scenario cybersecurity breaches and help management develop immediate response plans, including public disclosure procedures and economic recovery strategies, to mitigate potential damages." In addition, "[b]oards should consider disclosing cybersecurity risks and protective measures on relevant SEC filings, as such disclosures can generate confidence in investors rather than fear.") The U.S. Department of Commerce also has suggested that a company's cybersecurity preparedness could include cybersecurity insurance, which is specifically designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. *Cybersecurity Insurance*, U.S. Department of Homeland Security, *available at* http://www.dhs.gov/publication/cybersecurity-insurance*.* Despite the increased threats of cyber-attacks, the cybersecurity insurance market has been slow to develop, and many companies have chosen to forego available policies, citing their perceived high cost, a lack of awareness about what they cover, and their confidence (or ignorance) about their actual risk of a cyber-attack. *Id.* Moreover, despite the fact that cyber incidents are not covered by general liability policies, one survey noted that 57% of respondents indicated that their boards are not reviewing their existing policies for cyber-related risks. *See*, *supra* note 31, CyLab 2012 Report, at 15.

[49] The Department of Justice recently unsealed indictments against five Chinese military officials who allegedly conspired to steal information from U.S. companies across different industries. In connection with this indictment, it was recently reported that three U.S. public companies identified as victims of this conspiracy failed to report the theft of trade secrets and other data to their investors, despite the Commission's disclosure guidance on this topic. Two of the companies, Alcoa Inc. and Allegheny Technologies Inc., said that the thefts were not "material," and therefore did not have to be disclosed to investors. *See,* Chris Strohm, Dave Michaels and Sonja Elmquist, *U.S. Companies Hacked by Chinese Didn't Tell Investors*, Bloomberg (May 21, 2014), *available at* http://www.bloomberg.com/news/2014-05-21/u-s-companies-hacked-by-chinese-didn-t-tell-investors.html*; See also, supra note 14.*

Last modified: June 10, 2014