The current cyber risk landscape

Overview

- The frequency and severity of cyber attacks are increasing at an alarming rate.
- Cybersecurity is no longer just an "IT issue" or a matter that results only in information loss.
  - It now impacts an entity's reputation and has resulted in theft of protected or sensitive information (e.g., intellectual property, credit card information, personally identifiable information (PII)) and disruption of computer-controller operations or access to online systems, and can require significant financial costs to remediate the breach.
- It is now a much broader business issue affecting most corporations.
- As these attacks continue to evolve, so will their impact on the organization as a whole.
- While many of the recent, highly publicized attacks/breaches do not appear to have been directly targeted at financial systems, the access gained by the attackers provided them the ability to:
  - Manipulate or modify financial records, such as billing/cost/interest rates
  - Modify key automated business rules
  - Modify automated controls relied upon by management
The current cyber risk landscape

Overview

► Attackers are beginning to realize the potential benefits of targeting systems containing financial data to support their motivation (e.g., financial gain, corporate espionage).
► August 2015 – SEC charged 32 defendants in a scheme to trade on hacked corporate earnings announcements.  
► November 2015 – US prosecutors charged three individuals accused of hacking major US financial institutions.

"It is no longer hacking for a quick payout … this was hacking as a business model."

"The conduct alleged in this case may also signal the next frontier for securities fraud — sophisticated hacking to steal nonpublic information."

— Preet Bharara, U.S. Attorney for the Southern District of New York


The current cyber risk landscape

Evolution of cyber threats

<table>
<thead>
<tr>
<th>Risk</th>
<th>Attacker resources and sophistication</th>
<th>Motivations and common attackers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsophisticated attackers (script kiddies)</td>
<td>You are attacked because you are on the internet and have a vulnerability.</td>
<td>Common attackers: Companies that manufacture/produce products that leverage certain IP to maximize their advantage in the marketplace (e.g., aerospace and defense, drug manufacturing, companies negotiating M&amp;A transactions).</td>
</tr>
<tr>
<td>Sophisticated attackers (hackers)</td>
<td>You are attacked because you are on the internet and have information of value.</td>
<td>Common attackers: State-sponsored, organized crime.</td>
</tr>
<tr>
<td>Corporate espionage (malicious insiders)</td>
<td>Your current or former employee seeks financial gain from stealing and selling your intellectual property (IP).</td>
<td>Common attackers: State-sponsored, organized crime.</td>
</tr>
<tr>
<td>State-sponsored attacks and advanced persistent threat (APT)</td>
<td>You are targeted because of who you are, what you do or the value of your IP.</td>
<td>Common attackers: State-sponsored, organized crime.</td>
</tr>
<tr>
<td>Organized crime (criminal gangs)</td>
<td>You are attacked because you have money or something else of value that can be sold.</td>
<td>Common attackers: State-sponsored, organized crime.</td>
</tr>
<tr>
<td>Script kiddies</td>
<td>Amusement, experimentation, nuisance, notoriety</td>
<td>Common attackers: State-sponsored, organized crime.</td>
</tr>
<tr>
<td>Hackers Malicious insiders</td>
<td>Comic relief, personal gain, stock price manipulation</td>
<td>Common attackers: State-sponsored, organized crime.</td>
</tr>
<tr>
<td>Criminal gangs</td>
<td>Cash, embarrassment, political, social or environmental causes</td>
<td>Common attackers: State-sponsored, organized crime.</td>
</tr>
</tbody>
</table>

The current cyber risk landscape

Motivations and common attackers

<table>
<thead>
<tr>
<th>Motivations</th>
<th>Common attackers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial gain through the theft of IP and/or proprietary information</td>
<td>Companies that manufacture/produce products that leverage certain IP to maximize their advantage in the marketplace (e.g., aerospace and defense, drug manufacturing, companies negotiating M&amp;A transactions).</td>
</tr>
<tr>
<td>Sales and economic growth</td>
<td>Companies that manufacture/produce products that leverage certain IP to maximize their advantage in the marketplace (e.g., aerospace and defense, drug manufacturing, companies negotiating M&amp;A transactions).</td>
</tr>
<tr>
<td>Financial gain through access to non-monetary assets (e.g., PII) that can be sold to others</td>
<td>Companies that manufacture/produce products that leverage certain IP to maximize their advantage in the marketplace (e.g., aerospace and defense, drug manufacturing, companies negotiating M&amp;A transactions).</td>
</tr>
<tr>
<td>Political disruption, terrorism, service disruption</td>
<td>Financial services, power generation and distribution facilities, oil and gas exploration and distribution facilities.</td>
</tr>
<tr>
<td>Manipulation of stock price</td>
<td>Companies competing in emerging or expanding markets.</td>
</tr>
</tbody>
</table>
The current cyber risk landscape
What can a targeted cyber attack look like?

Intelligence gathering
Initial exploitation
Command and control
Privilege escalation
Data exfiltration
Enable persistence
Conduct enterprise reconnaissance
Move laterally to new systems
Escalate privileges
Gather and encrypt data of interest
Maintain persistent presence
Exfiltrate data from victim systems
Conduct background research
Execute initial attack
Establish foothold

Initial exploitation
Point where most targets are notified of the attack (generally by third party)
Point where third parties are aware of the attack
Accelerating attack detection
Degrading security posture or health as the attack life cycle progresses

Market insights: What are we seeing?

36%
of respondents say it is unlikely they would be able to detect a sophisticated attack

57%
of respondents say the lack of skilled resources is challenging Information Security’s contribution and value to the organization

59%
of respondents see criminal syndicates as the most likely source of an attack today

The cost of a data breach
A survey of 68 US cyber breaches in 2015 found the cost ranged from $1.9m to $65m.

- Ponemon Institute: 2015 Cost of Cyber Crime Study

Market insights: What are we seeing?
Current threats and vulnerabilities

Responses to EY GISS question: Which threats* and vulnerabilities** have most increased your risk exposure over the last 12 months?

Top vulnerabilities
- 44% feel vulnerable to careless or unaware employees
- 34% feel vulnerable to outdated information security controls or architecture

Top threats
- 44% see phishing as a top threat
- 27% say end-user phishing led to their most significant cyber breach
- Phishing attacks are getting more sophisticated as hackers are targeting social media information to “personalize” the attack emails
- 43% see malware as a top threat
Market insights: What are we seeing? How can you manage the attacks?

Your organization will suffer cyber incidents. This is an often unspoken truth when operating in the digital world.

The starting point for evaluating your cyber risk is to understand what you look like to a cyber attacker.

► Have you identified your most critical information assets and where they are located?
► Do you know what it is the attackers are targeting?
► How will they gain access and how would this damage you and your critical assets?
► Do you fully understand your organization’s ability to respond, contain and recover from an attack?

Applying risk management principles to cyber risk is a useful way to think about cybersecurity.

Factoring cybersecurity into your planning and risk appetite

- Focus on what matters most
- Measure and report
- Comprehensible in nature
- Allocation of risk appetite
- Integrates with business planning

<table>
<thead>
<tr>
<th>Key risk management principles</th>
<th>Applied to cyber risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus on what matters most</td>
<td>Know your critical information assets</td>
</tr>
<tr>
<td>Measure and report</td>
<td>Make cyber risk more tangible</td>
</tr>
<tr>
<td>Comprehensible in nature</td>
<td>Align with existing risk frameworks</td>
</tr>
<tr>
<td>Allocation of risk appetite</td>
<td>Make cyber risk relevant to the business</td>
</tr>
<tr>
<td>Integrates with business planning</td>
<td>Enable risk appetite in investment decisions</td>
</tr>
</tbody>
</table>

Marketplace response to growing cyber risk

- Various interested parties are concerned about entities’ abilities to appropriately deal with cyber attacks and breaches:
  - Audit committees/boards
  - PCAOB
  - AICPA
  - Various federal and state-level regulators
  - SEC

- PCAOB – information-gathering activities during its current assessment cycle
- AICPA – The AICPA Trust Information Integrity Task Force is developing a suggested approach to cybersecurity attestation reporting; this is anticipated to be exposed for comment in 2016 (see page 24)
- Various federal and state-level regulators
- SEC – Continues to highlight the importance of the issue in speeches and comments:
  - “Firms must adopt written policies to protect their clients’ private information and they need to anticipate potential cybersecurity events and have their procedures in place rather than waiting to react once a breach occurs.” (September 2015)
Marketplace response to growing cyber risk

- Various interested parties are concerned about entities' abilities to appropriately deal with cyber attacks and breaches (cont'd.):
  - House and Senate – Evaluating cyber threat information-sharing legislation and data breach notification standards
  - National Association of Corporate Directors – Publisher of general articles/handbooks for boards seeking guidance on cyber preparedness
  - Significant investors and customers/consumers – Asking for more transparency into an entity's cyber risks and processes as well as privacy and how PII is handled

Board and audit committee oversight of cyber risk

- The increase in the volume and severity of attacks, coupled with the increased scrutiny by regulators, has significantly elevated its importance.
- Members are now expected to have an appropriate understanding of (1) cyber risk concepts and (2) the business implications of these risks on the entity to enable them to evaluate:
  - The suitability of the governance structure implemented by management
  - The appropriateness of the cyber risk management program implemented by management
  - The appropriateness of the cyber risk disclosures required per SEC guidance
  - How insider threats should be managed (i.e., CISO reporting directly to the board, efficacy of the CISO)

Board and audit committee oversight of cyber risk
Challenges faced by boards and audit committees

- Boards play a critical role in overseeing cyber and cyber risk and promoting cultural awareness of cybersecurity risk in the entity.
- However, the complexity and technical nature of cybersecurity can create a barrier to effective board oversight.

Board and audit committee oversight of cyber risk

Boards should consider if the following challenges exist:
- Cybersecurity expertise – However capable boards are, it can be challenging to have specialist knowledge in many important areas and to stay current with a topic that is shifting constantly in terms of threat vectors.
- Capacity – Boards are dealing with a significant number of other issues and may not have full capacity to focus sufficient attention on this emerging topic.

Potential solutions to consider:
- Supplement technical knowledge via external sources and/or periodic board training
- Inclusion of board members with expertise in cybersecurity
- Establishment of a separate committee to oversee cyber risk
Board and audit committee oversight of cyber risk

What are boards and audit committees looking for?

- Regular (e.g., quarterly) updates from the CISO/CIO on information security and cyber threat intelligence that is both meaningful and actionable
- Reporting should address the following:
  - Identification. Which are the top three to five threats that are most relevant to the organization?
  - Protection. Summarize the actions taken to manage these threats. Summarize what other actions management considered, but elected not to pursue.
  - Detection. What mechanisms are being used to detect incidents? How does management evaluate and categorize incidents identified and determine which to elevate to senior leadership? What activity has been seen since the last report?
  - Response and recovery. How did the company respond to higher-risk incidents?
  - Industry scorecard. How does the company compare against its peer group or when compared with general benchmarks against industries with leading cybersecurity practices, such as financial services?

Cybersecurity dashboard

- To provide effective oversight, boards, audit committees (and senior management) need insight into appropriate cyber risk and security-related performance metrics.
- Dashboards should focus on metrics that quantify the business impact of cyber risk mitigation efforts and measure progress.

Example dashboard information:
- Type of attacks experienced
- Severity of attacks (e.g., How far did attackers get into the system?)
- Response to attacks (e.g., How quickly did management react?)
- Analysis of where the entity ranks when compared with benchmarks or emerging standards
- Threat assessments that could possibly predict future attacks
- Competitive/industry benchmarks
- ROI to help assess the effect as cybersecurity spend increases

- Boards can also hire external specialists to assess the entity’s cybersecurity efforts and benchmark against comparable companies.

Review incident response plan

* Bridging the gap between technology and response
  - Boards should evaluate the entity’s incident response plan and determine whether it includes all functions of the entity, not just top management and IT
  - Roles should also be defined for the board, general counsel and public relations

* Crisis management
  - Responsibilities should be defined for issuing statements in the event of an attack
  - Slow response can be damaging

* Rehearsal
  - Boards should encourage management to rehearse its incident response capabilities to identify and close gaps
Common areas exploited in recent cyber attacks

In evaluating the root cause/attack vectors being used by attackers in a number of recent highly publicized attacks, some common themes were identified:

<table>
<thead>
<tr>
<th>Common themes</th>
<th>Cyber risk area</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged accounts were not adequately protected (especially system accounts)</td>
<td>Privileged account access</td>
<td>Facilitated the attacker’s ability to deepen and broaden the breach</td>
</tr>
<tr>
<td>Exposure to social engineering attacks</td>
<td>Security awareness program</td>
<td>Isolated attackers to gain a foothold in a target’s system</td>
</tr>
<tr>
<td>Depth and quality of event monitoring did not keep pace with existing attack vectors</td>
<td>Security monitoringincident management program</td>
<td>Attacker’s structured their attacks to avoid detection via historical controls (e.g., inspection).</td>
</tr>
<tr>
<td>Quality of threat and vulnerability management programs not keeping pace with evolving risks</td>
<td>Threat and vulnerability management program</td>
<td>Lack of effective response to address new/evolving threats</td>
</tr>
<tr>
<td>Lack of timely, comprehensive patching of technologies</td>
<td>Patch management program</td>
<td>Issues are being exploited (weakest link).</td>
</tr>
<tr>
<td>Inadequate evaluation and testing of vendor access to client systems</td>
<td>Vendor risk management program</td>
<td>Unauthorized vendor access is being exploited (weakest link).</td>
</tr>
<tr>
<td>General lack of clarity and prioritization around the higher-risk areas of the entity and the level of protection needed</td>
<td>Data classification program</td>
<td>Critical information was not being adequately protected</td>
</tr>
</tbody>
</table>

Common areas exploited in recent cyber attacks
Understanding the action taken by management

<table>
<thead>
<tr>
<th>Cyber risk area</th>
<th>Example considerations when assessing the actions taken by management to address the cyber risk areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged account access</td>
<td>▶ Determine the controls for account provisioning (system and human accounts)</td>
</tr>
<tr>
<td></td>
<td>▶ Determine how management assesses ongoing appropriateness (system and human accounts)</td>
</tr>
<tr>
<td></td>
<td>▶ Define adequate access for managing whether an account has been hijacked (e.g., running behavior)</td>
</tr>
<tr>
<td></td>
<td>▶ Define access with privileged access has been hijacked (e.g., running behavior)</td>
</tr>
<tr>
<td></td>
<td>▶ Remediate access with privileged access has been hijacked (system and human accounts)</td>
</tr>
<tr>
<td>Governance/ risk management program</td>
<td>▶ Determine how management periodically assesses and evaluates its cybersecurity program for effectiveness</td>
</tr>
<tr>
<td></td>
<td>▶ Determine whether management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
<tr>
<td>Security monitoringincident management program</td>
<td>▶ Determine whether management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
<tr>
<td>Security awareness program</td>
<td>▶ Determine whether management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
</tbody>
</table>

Common areas exploited in recent cyber attacks
Understanding the action taken by management

<table>
<thead>
<tr>
<th>Cyber risk area</th>
<th>Example considerations when assessing the actions taken by management to address the cyber risk areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch management program</td>
<td>▶ Determine how management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
<tr>
<td></td>
<td>▶ Determine how management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
<tr>
<td>Vector risk management program</td>
<td>▶ Determine how management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
<tr>
<td>Data classification program</td>
<td>▶ Determine how management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
<tr>
<td>Threat and vulnerability management program</td>
<td>▶ Determine how management polices and procedures for the management of vulnerabilities and impacts are in place</td>
</tr>
</tbody>
</table>
Cybersecurity breaches and auditor actions

Auditor responsibilities when a breach comes to our attention
► When a known or suspected breach comes to our attention with the potential to materially impact the financial statements, we:
  ► Gain an understanding of management’s approach to investigating the breach
  ► Evaluate the actions taken by management in response to the investigation
  ► Assess the effect of the breach on our audit

Notification of cybersecurity breaches
► Establish protocols to provide auditors with timely notification of a cybersecurity breach with potential material implications to the financial statements
► Consider updating the incident response plan to include a step to notify auditors and disclosure committees responsible for public filing

What represents a breach that may be significant to the entity’s financial statements?
► Not all breaches are significant to the entity. A breach that results in one or more of the following may potentially be significant:
  1. Extraction of protected or sensitive information
     ► Could result in impairment of assets; fines, penalties and lawsuits requiring the recording of material liabilities and/or commitment and contingency disclosures in the financial statements
     ► Examples: intellectual property, credit card information, personally identifiable information, customer data
  2. Modification of financial applications or information
     ► Could affect the accuracy and/or integrity of processing financial information
     ► Examples: changes to key business rules, automated controls or billing, cost or interest rates

Looking forward: what to expect

Future considerations

Audit considerations
► Potential increased focus on cybersecurity programs and controls on audits
► Cyber risks will continue to evolve as attacks become more frequent and complex
  ► Entities’ cyber programs must keep up with the increased risks
  ► Our audit procedures will also evolve in response to these risks

Cyber attestation reporting
► To help address the needs of regulators, investors, directors, etc., for additional transparency into an entity’s cyber risk management activities, the AICPA has initiated a project to develop/identify criteria for performing cybersecurity attestation engagements
  ► Practitioner guidance for performing such engagements is expected in 2016
  ► The appropriate framework is under development but may leverage reporting structures and frameworks recognized by the market
  ► SOC 2 reporting (report on controls over information handling)
  ► “Cybersecurity Framework” issued by the National Institute of Standards and Technology
  ► Scoping is expected to include areas that have not previously been subjected to extensive auditing. Control gaps may be identified – evaluate cyber control environment now
Looking forward: what to expect

Cyber attestation reporting overview

Proposed cybersecurity attestation reporting options

- **Entity-level** (expected Q2 2016)
  - To address the needs of regulators, investors, boards, etc., for greater transparency into their overall control environment
  - Scope: the enterprise-wide operations of the entity

- **Service provider-level** (expected Q3 2016)
  - To address vendor risk management needs of companies
  - Scope: the operations supporting the services being outsourced

- **Supply chain-level** (expected Q4 2016)
  - To address supply chain needs of companies (i.e., entities that supply goods to those who are part of the critical infrastructure)
  - Scope: the operations supporting the goods being produced and distributed to others

Summary

Key learning points

- Cybersecurity is no longer just an “IT issue”; it is now a much broader business issue
- Apply a cyber-risk lens to everything you do
- There is significant interest in the marketplace about entities’ abilities to appropriately deal with cyber attacks and breaches
- Apply key risk management principles: place the most attention, prevention and countermeasures around your areas of most value and highest risk
- Board and audit committee oversight is critical; consider expertise and capacity of board members to assess cyber risks and evaluate cybersecurity programs
- Act now to prepare for potential cyber attestation standards
- Stay informed about potential regulatory actions that will have an effect
- Organizations are making progress in responding to cyber threats and attacks, but there is a need for considerable improvement as the world becomes more digital and attackers increase in sophistication and persistence

Cybersecurity resources

- EY’s Global Information Security Survey 2015: Creating trust in the digital world
- EY Center for Board Matters: Taking charge – How Boards can activate, admit and adapt now to get ahead of cybersecurity risk
- The CFO agenda video series: cybersecurity

- View more of EY’s insights on cybersecurity: ey.com/cybersecurity
- For further GRC thought leadership, please refer to our insights on governance, risk and compliance series: ey.com/GRCInsights
THANK YOU!

Damian Klute, Principal, EY Advisory Services
804-344-4658
damian.klute@ey.com

Ben Moreland, Manager, EY Advisory Services
410-783-3703
ben.moreland@ey.com