Evolving Cybersecurity Risks

Results on EY's Global Information Security Survey

EY
Building a better working world

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

EY

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.[1]
  - 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."

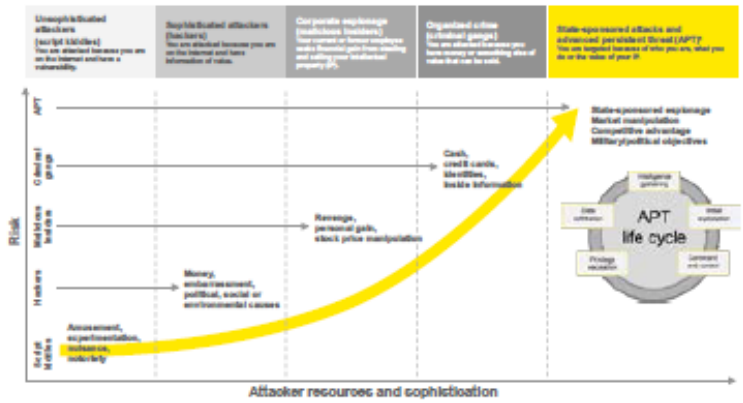
    "The conduct alleged in this case may also signal the next frontier for securities fraud — sophisticated hacking to steal nonpublic information."

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

[1] "SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases," U.S. Securities and Exchange Commission, http://www.sec.gov/news/pressrelease/2015-163.html, 11 August 2015.

EY

The current cyber risk landscape
Evolution of cyber threats



† An advanced persistent threat (APT) is a set of sophisticated, stealthy and continuous computer attacks often targeting a specific entity with business or political motives. The processes involve a high degree of covertness over a long period of time and sophisticated techniques to exploit vulnerabilities in systems.

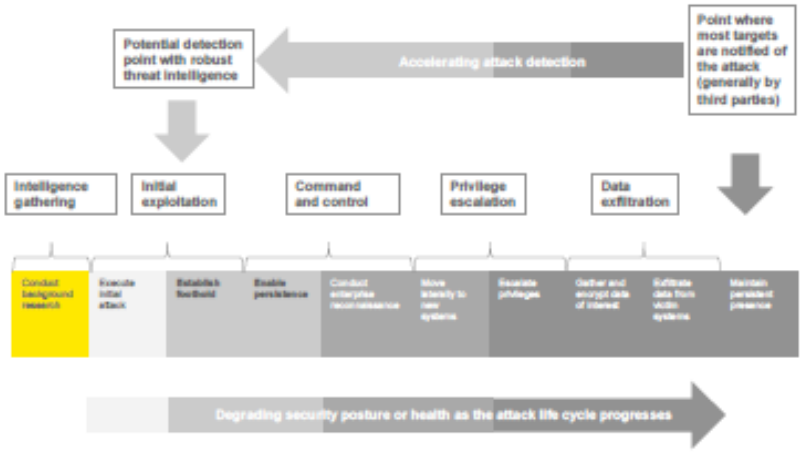
EY

The current cyber risk landscape
Motivations and common attackers

Motivations	Common targets	Common attackers
Financial gain through the theft of IP and/or proprietary information ▸ Accelerate company or country research and development ▸ Competitive advantage ▸ Sales and economic growth	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&A transactions)	▸ State-sponsored ▸ Organized crime
Financial gain through access to non-monetary assets (e.g., PII) that can be sold to others	Companies with credit card information and/or other PII of a target audience	▸ Organized crime ▸ Employees/contractors
Financial gain through direct access to monetary assets and/or financially relevant information	Banks, insurance companies, trading firms	▸ Competitors ▸ Organized crime ▸ Employees/contractors
Political disruption, terrorism, service disruption	Financial markets, power generation and distribution facilities, oil and gas exploration and distribution facilities	▸ State-sponsored ▸ Organized crime ▸ "Hacktivists"
Manipulation of stock price	Companies competing in emerging or expanding markets	▸ State-sponsored ▸ Organized crime

EY

The current cyber risk landscape
What can a targeted cyber attack look like?



EY

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 58 US cyber breaches in 2015 found the cost ranged from $1.9m to $65m.
- Ponemon Institute: 2015 Cost of Cyber Crime Study

Source: EY 2015 Global Information Security Survey

EY

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

* Threat is defined as the potential for a hostile action from actors in the external environment.
** Vulnerability is defined as exposure to the possibility of being attacked or harmed.

Source: EY 2015 Global Information Security Survey

EY

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.

EY

Factoring cybersecurity into your planning and risk appetite

Key risk management principles …	… applied to cyber risk
Focus on what matters most Must align to your unique business and risk culture	**Know your critical information assets** Identify critical business assets most vulnerable to cyber attack
Measure and report Include qualitative statements and quantitative measures	**Make cyber risk more tangible** Clearly define cyber risk and underlying metrics
Comprehensive in nature Should cover all risk types, current and forward-looking	**Align with existing risk frameworks** Financial, operational, regulatory, customer reputational, etc.
Allocation of risk appetite Allocation of appetite to business units and risk types	**Make cyber risk relevant to the business** Link organizational-level risks to individual BUs and their information assets
Integrate with business planning Regulators are increasingly looking for evidence	**Embed risk appetite in investment decisions** Prioritize investment where critical, empower businesses to make informed local decisions

EY

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** – Expected to have an appropriate understanding of the business implications of cyber risks
  - **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** – Issuing guidance to help improve cyber preparedness (e.g., FFIEC, FISMA, FedRAMP, NERC, SEC, NY DFS[2])
  - **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 clear procedures in place rather than waiting to react once a breach occurs." (September 2015)[3]

[2] "Potential New NYDFS Cyber Security Regulation Requirements," New York State Department of Financial Services, http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf, 9 November 2015.
[3] "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach," U.S. Securities and Exchange Commission, http://www.sec.gov/news/pressrelease/2015-202.html, 22 September 2015.

EY

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

EY

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)

EY

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.

Boards should consider if the following challenges exist:

- **Cybersecurity expertise** – however capable boards are, it can be challenging to have specialist knowledge on 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

EY

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?

Board and audit committee oversight of cyber risk
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:
- Types of attacks experienced
- Severity of attacks (e.g., How far did attackers get into the system?)
- Responses 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.

Board and audit committee oversight of cyber risk
Review incident response plan

Bridging the gap between technology and response

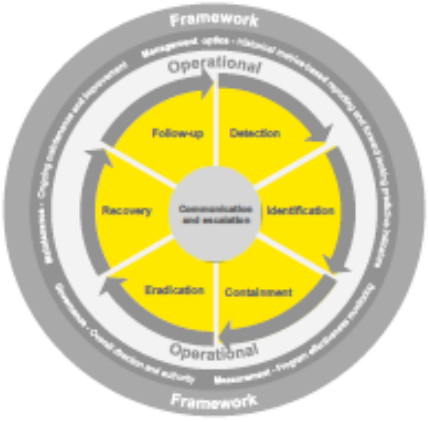
- Boards should evaluate the entity's incident response plan and determine whether it includes all functions of the entity, not just top management and IT
- Roles should also be defined for the board, general counsel and public relations

Crisis management

- Responsibilities should be defined for issuing statements in the event of an attack
- Slow responses can be damaging

Rehearsal

- Boards should encourage management to rehearse its incident response capabilities to identify and close gaps



EY

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:

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

EY

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

Cyber risk area	Example considerations when assessing the actions taken by management to address the cyber risk areas

Privileged account access	▸ Determine the controls for account provisioning (system and human accounts)
	▸ Determine how management assesses ongoing appropriateness (system and human accounts)
	▸ Determine management's process for identifying whether:
	  ▸ An account with privileged access has been hijacked (e.g., monitoring behavior)
	  ▸ Fictitious accounts with privileged access have been established (system and human accounts)

Governance/risk management program	▸ Determine how management periodically assesses and evaluates its cybersecurity program for effectiveness ▸ Determine whether management engages third parties to perform attack and penetration or other cyber assessments and understand how management evaluates and responds to results
Security monitoring/incident management program	▸ Determine how management would know if the entity were under a cyber attack, if a breach of audit significance had occurred, and if a user's account had been hijacked ▸ Determine whether a security incident response plan has been developed and tested
Security awareness program	▸ Understand what programs are in place (audience, frequency, topics, trainings, etc.)

EY

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

Cyber risk area	Example considerations when assessing the actions taken by management to address the cyber risk areas
Patch management program	▸ Determine how management identifies, evaluates, prioritizes and implements software patches issued by software vendors ▸ Determine how management monitors the patch status of key technologies to work toward consistent deployment
Vendor risk management program	▸ Determine how vendors connected to the IT environment are identified ▸ Determine how the risk associated with each vendor connected to the IT environment is assessed
Data classification program	▸ Determine how data classified as "most critical" to the entity is protected ▸ Determine how management would know if information critical to operating its business and/or maximizing its advantage in the marketplace were accessed, stolen or destroyed
Threat and vulnerability management program	▸ Determine how new and evolving threats to the IT environment are identified ▸ Determine the adequacy of the response procedures to those threats deemed credible ▸ Understand what processes exist to classify and remediate vulnerabilities

EY

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

EY

Cybersecurity breaches and auditor actions

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

EY

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

EY

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

EY

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

EY