Cybersecurity – retail and consumer products (RCP)
Looking at the current situation

April 2015
Cyber threats represent real risk to the business

The rapid-fire pace of technology (r)evolution will only accelerate in the years to come – as will the cyber risks. Not considering them until they arise gives cyber attackers the advantage. In fact, chances are, they’re already in!

Security breaches can derail key objectives; undermine the confidence of shareholders, analysts and consumers; damage your brand reputation; and cause significant financial harm.

Executives need to stop simply looking at the costs of information security and instead view it as an opportunity that can truly benefit the company and its customers.

In a cyber breach, who pays, banks or retailers?
- The Wall Street Journal, January 12, 2014

FBI warns retailers of more cyber attacks
- USA Today, January 24, 2014

U.S. retailers face pressure to raise cybersecurity spending
- Reuters, February 5, 2014

Calif. attorney general focuses on retailers’ data theft
- USA Today, February 27, 2014

Holder Targets Retailers in Data Thefts
- ABC News, February 24, 2014

Cybercriminals continue to target retail sector
- FireEye Blog, March 11, 2014
The challenge of evolving security threats

Cybersecurity threats are constantly evolving, and global corporations are being targeted

- Attackers are patient, persistent and sophisticated.
- Challenges have caused a paradigm shift in information security processes.
- Organizations must alter their mindset on how they think about cyber threats, risks and capabilities.
- The gap between threats and information security advances is widening, i.e., the challenge for global, leading companies is outpacing progress.

Unsophisticated attackers (script kiddies)
- Experimentation
- You are attacked because you are on the internet and have a vulnerability.

Sophisticated attackers (hackers)
- Monetization
- You are attacked because you are on the internet and have information of value.

Corporate espionage (insiders)
- Your current or former employee seeks financial gain from selling your intellectual property.

State-sponsored attacks (Advanced Persistent Threat (APT)), Hacktivism, identity thefts
- You are targeted because of who you are, what you do, or the value of your intellectual property.
- Cyber attacks occur to promote political ends.
- Theft of Personally Identifiable Information (PII) increases.

Risk

1980s/1990s 2014+
Retailers were cited as one of two industries having the highest estimated probability for a security breach, most likely as a result of the amount of confidential and sensitive customer information they collect.*

*Source: 2014 Cost of Data Breach Study: United States (Ponemon Institute LLP)
While breaches like Target’s have historically been rare, their costs and other long-term implications can be significant.

Financial implications
- Approximately $300m in costs associated with breach
- Decline in profit of 46%
- 8% decrease in stock price
- $53.7m income the hackers made from the sale of 2 million cards stolen

Other implications
- Impact to brand/reputation
- Customer churn and decreased customer lifetime value
- Decreased employee morale
- Potential turnover of key executives or those deemed responsible
- Potential increased scrutiny from security regulatory bodies, e.g., the Payment Card Industry (PCI)

“They’re really in a difficult place. It’s going to take them a long time to build the trust of the shopper and get them to where they were prior to December 2013.”

“I don’t see how they’re getting out of this for under a billion, over time,” he said, adding, “$150 million in a quarter seems almost like a bargain.”

### Additional cost of a breach

The cost of a breach, broken out for three sample companies

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Company A: Low-profile breach in a non-regulated industry</th>
<th>Company B: Low-profile breach in a regulated industry</th>
<th>Company C: High-profile breach in a highly regulated industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery, notification and response</td>
<td>Outside legal counsel, mail notification, calls, call center and discounted product offers</td>
<td>$50</td>
<td>$50</td>
<td>$50</td>
</tr>
<tr>
<td>Lost employee productivity</td>
<td>Employees diverted from other tasks</td>
<td>$20</td>
<td>$25</td>
<td>$30</td>
</tr>
<tr>
<td>Opportunity cost</td>
<td>Customer churn and difficulty in getting new customers</td>
<td>$20</td>
<td>$50</td>
<td>$100</td>
</tr>
<tr>
<td>Regulatory fines</td>
<td>FTC, PCI, SOX</td>
<td>$0</td>
<td>$25</td>
<td>$60</td>
</tr>
<tr>
<td>Restitution</td>
<td>Civil courts may ask to put this money aside in case breaches are discovered</td>
<td>$0</td>
<td>$0</td>
<td>$30</td>
</tr>
<tr>
<td>Additional security and audit requirements</td>
<td>The security and audit requirements levied as a result of a breach</td>
<td>$0</td>
<td>$5</td>
<td>$10</td>
</tr>
<tr>
<td>Other liabilities</td>
<td>Credit card replacement costs; civil penalties if specific fraud can be traced to the breach</td>
<td>$0</td>
<td>$0</td>
<td>$25</td>
</tr>
<tr>
<td><strong>Total cost per record</strong></td>
<td></td>
<td><strong>$90</strong></td>
<td><strong>$155</strong></td>
<td><strong>$305</strong></td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.
What does it mean to you?

► A cyber attack not only can damage your brand/reputation, it also can result in loss of competitive advantage, legal/regulatory noncompliance (e.g., PCI) and steep financial consequences.

► The cost of a breach to an organization increases the longer a breach goes undetected; further, the value of the data to an attacker decreases dramatically after a breach is detected and reported. Therefore, promptly identifying and reporting the breach reduces your costs as well as the incentive of attackers to target you.
What does a targeted attack look like?
A cybersecurity game changer

- Background research
- Initial attack
- Establish foothold
- Privilege escalation
- Move laterally
- Leverage privileges
- Enumerate PCI/POS
- Deploy malware
- PCI focused attacks
- Gather data
- Steal data
- Data exfiltration

External network/trusted business partner
Corporate Network
PCI environment
Point-of-sale (POS) systems

Intel gathering
Initial exploit
Privilege escalation
PCI focused attacks
Data exfiltration
What leading retail and consumer products companies should be focused on

**Identify the real risks**
- Define the organization's overall risk appetite and how information risk fits
- Identify the most important information and applications, where they reside and who has/needs access
- Assess the threat landscape and develop predictive models highlighting your real exposures

**Protect what matters most**
- Develop a security strategy focused on business drivers and protecting high-value data
- Assume breaches will occur - improve processes that plan, protect, detect and respond
- Balance fundamentals with emerging threat management
- Establish and rationalize access control models for applications and information

**Enable business performance**
- Make security everyone's responsibility
- Don't restrict newer technologies; use the forces of change to enable them
- Broaden program to adopt enterprise-wide information risk management concepts

**Optimize for business performance**
- Align all aspects of security (information, privacy, physical and business continuity) with the business
- Spend wisely in controls and technology - invest more in people and processes
- Selectively consider outsourcing operational security program areas

**Sustain an enterprise program**
- Get governance right - make security a board-level priority
- Allow good security to drive compliance, not vice versa
- Measure leading indicators to catch problems while they are still small
- Accept manageable risks that improve performance

---

Cybersecurity – RCP: looking at the current situation | March 2015
How to begin preparing?

Organizations should begin by asking the following questions:

► Are we focused on protecting “what matters most” (e.g., revenue-generating assets, customer information)?
► How do we measure the effectiveness of our information security program?
► How has the information security program kept pace with the evolving IT landscape (e.g., cloud, mobile, social, bring your own device)?
► Is the information security organization appropriately organized, trained, staffed, equipped and funded?
► Do we have the ability to detect if we’ve been breached?
► Do we know if we’ve been breached?
  ► Do we know who might attack us; how, when, and why?
  ► Do we have a response plan in place?
  ► Have we developed countermeasures to enact when something like this occurs?
► Do our various control audits (PCI, financial audit) address these risks?

Cybersecurity now – the new normal

New outlook: The network is already compromised or soon will be.

New approach: Develop a strategy to:
What protection measures are needed

Improve
► Current state for many organizations – defenses against cyber attacks remain reactive, addressing known threats only; knowing that an attack will occur sparks improvements

Expand
► Leading organizations – proactive in determining both the known and unknown risks within their security programs.

Innovate
► Innovators – continuously review, rethink and potentially redesign their entire information security framework to fortify against both known and unknown cyber risks
## How can EY help

<table>
<thead>
<tr>
<th>Service Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Breach compromise assessment</strong></td>
<td>EY can leverage a network-based, malware detection solution(s) that identifies systems compromised by an external threat actor or infected with malware. EY can also assist with the investigative process to determine scope and nature of a potential intrusion.</td>
</tr>
<tr>
<td><strong>Evaluate incident response capabilities</strong></td>
<td>EY can review your existing plan and provide leading practices for any gaps where necessary to help your plan mature. If no program or plan exists, EY can help develop the plan, provide training and then perform a readiness exercise.</td>
</tr>
<tr>
<td><strong>Attack and penetration testing</strong></td>
<td>EY can perform a simulated attack of your cyber environment to assess any current vulnerable exploits. Scoping can include one or more of the following attack paths: internet, intranet, web application, wireless and social engineering. EY can also perform a simulated attack through a specific scenario (red team).</td>
</tr>
<tr>
<td><strong>Evaluate overall security program maturity</strong></td>
<td>EY can assess your capabilities against all key security-related domains, including a quantitative maturity assessment of each domain and a benchmark comparison of the company’s maturity score against the company’s peer group. We can also develop a strategic roadmap to close assessment gaps and improve maturity.</td>
</tr>
<tr>
<td><strong>Investigation services</strong></td>
<td>EY can conduct forensic investigations involving cyber breaches and cybercrimes. We also can follow behind the company’s cyber incident response investigators and cyber forensics examiners to validate their observations and findings to help make certain the who, what, when, where, why and how are understood.</td>
</tr>
<tr>
<td><strong>POS assessment</strong></td>
<td>EY can identify/model threat vectors and attack techniques that may be used. We can also review data flows and POS system architecture to identify potential weaknesses and related controls.</td>
</tr>
</tbody>
</table>
More Information about EY Information Security Advisory Services
EY is a global leader in information security consulting services

Forrester considers EY the top-ranked information security consulting provider for its strategy.

► EY’s overall Forrester score, which led to the top-ranking, was 4.28 out of 5.00

► Also, EY had the highest score (4.90 out of 5.00) of all of the consulting providers in the evaluation for its strategy which includes its value proposition and future direction

The Forrester Wave™: Information Security Consulting Services, Q1 2013, Forrester Research, Inc.

The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester’s call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.
# EY Cyber Security and Threat Services

## Accelerators

- **Business and industry sector focus**
- **Technical research through advanced security centers**
- **Diverse personnel who drive fact-based, creative business improvement**
- **Proprietary frameworks, tools and thought leadership**
- **Most globally aligned of the Big Four with an award-winning people culture**

## Client outcomes

- Transformed security program, driving business performance
- Integrated information security and IT risk approach across enterprise
- Identified and evaluated threats
- Consistent and reliable response to incidents
- Optimized measures to mitigate threats
- Understand who has or needs access to important data and applications
- Sustainable, compliant and efficient access processes
- Protect information that matters
- Regulatory and industry compliance
- Globalization of data protection strategies
- Build, test, and improve mechanisms to protect against catastrophic risks
- Establish culture to better respond to volatility and velocity

## Accelerators

<table>
<thead>
<tr>
<th>Assess</th>
<th>Transform</th>
<th>Sustain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security transformation</strong></td>
<td><strong>Cyber threat management</strong></td>
<td><strong>Identity and access management</strong></td>
</tr>
<tr>
<td>Security program assessment</td>
<td>Threat intelligence</td>
<td>Strategy and governance</td>
</tr>
<tr>
<td>Security strategy and roadmap</td>
<td>Security monitoring</td>
<td>Request and approval</td>
</tr>
<tr>
<td>Security risk assessment</td>
<td>Incident response</td>
<td>Provisioning and de-provisioning</td>
</tr>
<tr>
<td>Benchmarking</td>
<td></td>
<td>Enforcement</td>
</tr>
<tr>
<td></td>
<td>Vulnerability identification</td>
<td>Review and certification</td>
</tr>
<tr>
<td></td>
<td>Remediaion</td>
<td>Role and rules management</td>
</tr>
<tr>
<td></td>
<td>Countermeasure planning</td>
<td>Reconciliation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reporting and analytics</td>
</tr>
</tbody>
</table>

## Data protection

- Data protection strategy
- Host security
- Asset management
- Data loss prevention (DLP)

## Resilience

- Business continuity management strategy
- Emergency management
- Incident management

- Technical resilience
- Supply chain disruption response
- Sustainability
- Predicative risk modelling

---

**Cybersecurity – RCP: looking at the current situation | March 2015**
# EY Cyber Breach and Forensic Services

## Accelerators

- Business and industry sector focus
- Regulator and legal involvement in major breaches
- Technical research through industry specific forensic labs
- Diverse personnel who drive fact-based, investigations
- Proprietary frameworks, tools and thought leadership
- Global operations

## Cybercrime diagnostic

- Proactively detect cybercrime using forensically sound techniques which do not taint evidence or reveal the investigation to hacker
- Forensically detect attacks by:
  - Log forensics
  - Traffic forensics
  - Host forensics

## Cybercrime investigative services

- Computer forensics
- Compromise analysis
- Parallel proceedings planning and preparations
- Live interviewing & scope analysis
- Factual findings reporting
- Remediation planning
- Stakeholder communications

## Litigation services

- Global end-to-end eDiscovery capability
- Unstructured and structured data processing and hosting
- Technology Assisted Review
- Global managed document review
- Discovery advisory services
- PMO for multi-party and law firm management

## Insurance claims services

- Focusing on getting cash advances as quickly as possible
- Strategic claim recovery planning
- Quantum of claim analysis
- Insurance claim document coordination and management
- Carrier relationships

## Client outcomes

- Determine if organization is at risk, provide intelligence, trigger investigation
- Ensure evidence is not tainted in the event that investigation is required
- Legally defensible and forensically sound investigative approach
- Consistent coordination with corporate legal and risk functions with outside counsel
- Structured approach to litigation readiness for cyber breach
- Consolidated and streamlined function to respond to regulatory, civil and criminal complaints
- Structure approach to insurance claims for cyber breach
- Speed to recovery of funds from improved claims process
Our experience

► EY has supported many clients who have had massive breaches involving millions of account numbers stolen in the retail sector.

► EY has had a remarkable 10-year history helping to resolve these types of intrusions. We have worked on many similar and even more sophisticated matters.

► Our global presence in more than 45 locations worldwide with a staff of more than 700 in forensics (2,800 investigators) can provide broad support.

► We have extensive experience interacting with board of directors and audit committees on cyber breaches to explain the case updates in easy-to-understand terminology.
EY’s incident response services and global capabilities

► Dedicated industry teams to bring cybercrime incident response and investigative solutions that have industry-specific contents

► Experienced certified professionals who help our clients throughout the life of a security incident and cybercrime dispute or investigation

► Deep experience working with regulators and local law enforcement agencies in responding to a variety of cyber breach incidents

► Global operational capabilities:
  ► More than 3,000 professionals globally
  ► Worldwide forensic data preservation
  ► Global methodologies and standard computer forensic certification process
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2015 Ernst & Young LLP.
All Rights Reserved.

BSC no. 1503-1420799
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.