CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
SEPTEMBER 2015
“Even an unlimited budget for information security will not eliminate your cyber risk.”

— Tom Reagan
Marsh Cyber Practice Leader
CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES

STAKEHOLDERS

• **Risk Manager:**
  – Ensure connectivity between stakeholders.
  – Understand the evolving cyber insurance market and overall risk finance options.

• **CFO:**
  – Potential costs of a cyber event and what the impact could be on the bottom line.
  – Security of the sensitive information that the office controls.

• **CEO/Board:**
  – Accountable for overall business and company performance.
  – Fiduciary duty to assess and manage cyber risk. Regulators expect top leadership to be engaged.

• **Legal/Compliance:**
  – Keep stakeholders informed and compliant.
  – If a cyber incident occurs, lawsuits often follow within hours.
CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES

STAKEHOLDERS

• **CISO/CIO:**
  – The responsibility for executing the cyber security strategy usually rests largely with the CISO and the CIO working together and with the business units.

• **Operations:**
  – Maintaining daily operations, business processes, and workplace stability is critical during a cyber event.

• **HR/Employees:**
  – Simple errors — or deliberate actions — by employees can lead to costly cyber incidents.
  – Training on best practices is critical.

• **Customers/Suppliers:**
  – Interactions with customers and vendors can open a company to attack.
CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
FIN4: STEALING DATA FOR A TRADING EDGE

- **FIN4**: Financially motivated threat group that seeks access to market moving information before it is public.
  - Tools and techniques can be simple but insidiously effective.

Source: FireEye

FIN4 uses a hijacked e-mail account at Advisory Firm A to spearphish M&A specialists at Advisory Firm B. Both Advisory Firm A and Advisory Firm B are advising Public Company A on a large M&A opportunity.

FIN4 sends a second spear phishing email to the M&A team at Public Company A as well as to several of the M&A team’s advisors at outside firms.

Public Company A announces its plans regarding a possible M&A deal with Public Company B.

The market responds to the public announcement with wide fluctuations in the stock prices of both Public Company A and Public Company B.
FIN4 Targets

- 80+ public companies, mostly in health care sector.
- Law firms.
- Investment banks.
- Investor relations firms.

FIN4 Targeted Over 100 Publicly Traded Companies and Advisory Firms

- 68% Publicly Traded Health care and Pharmaceutical Companies
- 20% Firms Advising Public Companies on Securities and M&A Matters
- 12% Other Publicly Traded Companies

Source: FireEye
FIN4 Targeting Cycle
- Focused on monitoring e-mail.
- Stole legitimate attachments and weaponized stolen files for credential phishing.
- Replied-all with malicious attachment.

Frequent Phishing Targets:
- C-level executives and senior leadership.
- Legal counsel.
- Regulatory, risk, and compliance personnel.
- Researchers.
- Scientists.
- Other advisory roles.
CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES

FIN4: INITIAL ACCESS — PHISHING LURES

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT

Pursuant to Section 13 OR 15(d) of the
Securities Exchange Act of 1934

- SEC filings (some in draft form).
- Discussions of pending legal cases.
- Stock analyst reports.
- Promotional materials for investor conferences.
- Medical research/publications.
- Internal planning documents between boards of directors and their advisors.
- Letters of interest in pending M&A deals.
- Safety reports.
- Commercial supply agreements.
- Regulatory comments.
- Medicare and Medicaid themed documents.
- Code-named projects about media campaigns concerning public companies.
• Emails originate from **trusted senders.**
  – Links to fake Outlook Web Access portal.
  – Documents with embedded macros.
    • Weaponized stolen documents.

Source: FireEye
Several victims were repeatedly targeted.
Attempts to minimize chances of discovery made.

Source: FireEye
CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
COMBATTING SPEAR PHISHING

• Awareness:
  – Spear phishing exercises.
• Tightly manage controls over what people have access to.
• Technology:
  – Two-factor authentication.
  – Segmenting high-value information.
• Maintain the network.
THIRD-PARTY RISK
Threat actor motivations for targeting the firm’s clients, partners, and peers:

- **All threat actors:**
  - Exploitation of weakened authentication requirements.
  - Data theft of network topology and device configuration details.
  - Socially engineered exploitation of trust relationships.
  - Exploitation of shared or outsourced network.

- **Nation state actors:**
  - Maintain access to high priority targets in support of espionage operations.
  - Collect intelligence on targets from third parties.

- **Financially motivated actors:**
  - Facilitate fraud.
  - Obtain access to PII.

- **Hacktivist actors:**
  - Embarrassment.
  - Exposure of symbolic targets.

Source: FireEye
Specialized software firm with visibility into major asset transfers between firms and investors.

Targeted by APT12 in late 2012.
- China-based group.
- Capable of quickly evolving in response to exposure.

APT12 had access to the network for several months.
- Stole utilities and files for interacting with victim’s RSA soft token implementation.
- Possible that actors accessed data about organizations using the firm’s software to manage their assets.

Source: FireEye
CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
THIRD-PARTY EXPOSURE: CASE STUDIES

• **Reduced Authentication: Global Transportation Manufacturer**
  – Threat actors gained access by exploiting reduced authentication requirements on a VPN shared with vendor.
  – Stole data on victim’s SecurID implementation.

• **Subverting Trust: Engine and Component Repair Company**
  – Threat group accessed e-mail, replied to conversation in-thread.
  – Added malicious attachment, forwarded message to employees at partner company.

• **Network Reconnaissance: IT Service Provider**
  – Threat actors simultaneously compromised victim and business partners.
  – Data theft focused on network configurations and diagrams.
  – Likely an attempt to collect intelligence on network topology of future targets.

Source: FireEye
“These are threat actors who are determined and have ample tools and tactics at their disposal. When they hit a road block, they will adapt or switch up their tactics.”

— Kristen Dennesen
FireEye Senior Intelligence Threat Analyst
Example: HAMMERTOSS Backdoor Network Communications

- Twitter + GitHub + Cloud Drive
• APT17 configured BLACKCOFFEE malware to use Microsoft TechNet for C2 communications.
  – “Dead drop resolver”: Encoded IP address reached out to legitimate forum threads.
  – BLACKCOFFEE supports ~15 commands, including creating a reverse shell, uploading and downloading files, and enumerating files and processes.

Source: FireEye
Of all the compromised machines Mandiant identified in 2014, only ~50% had malware on them.

Source: FireEye
A thorough understanding of your risk profile is critical, and that means more than the typical compliance audit. You need to inventory cyber-vulnerable assets, identify new and emerging threats — internal and external — and model an event’s potential impact. The evolving nature of cyber risk requires you to continuously monitor changes in your organization’s risk profile — then adapt.

Cyber risk management typically requires a balance of:
- *Prevention* — to stop cyber-attacks from succeeding.
- *Preparation* — to make sure you are ready when an event happens.
- *Risk transfer* — to transfer the exposure off your balance sheet.

You likely cannot stop a cyber-attack from occurring, but you can control how you respond to them. A quick, effective reaction is essential, and the decisions you make after an event can have lasting implications.
Approaching Cyber Risk...

Quantifying the data breach epidemic.

Data breaches are an increasingly prominent and costly security challenge for a broad spectrum of U.S. companies, and they are growing in size and frequency. Companies incur millions of cyber attacks each week. A successful breach can yield millions of personal records that will be later sold on an illicit market.

With today’s data moving freely among organizations and consumers, through mobile devices, the cloud, and new points of vulnerability, data breaches may grow even more common.

Prudent risk management requires organizations to quantify the potential costs from this growing threat. However, determining accurate projections can be difficult. Many projections that are currently available include unassessable costs or are based on limited data.

Privacy IDEAL – Frequency

What is the probability that XX will have a data breach event over the next 12 months?

Privacy IDEAL – Range of Potential Outcomes

Privacy IDEAL – Cost Analysis

Note: Costs do not include business interruption due to the high degree of variability.

MARSH
High-profile losses having an impact on cyber insurance markets.
Insureds generally should anticipate increases in both retentions and premiums.
Average pricing, not including the retail and health care sectors, has increased 19.1%.
Average pricing for the retail sector has increased 32.1%.
Buyers entering the market at a more rapid pace.
Many existing insureds significantly increasing their limits.