THE NEW REALITY OF RISK

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES

SEPTEMBER 2015

MARSH

CYBER RISK IS HERE TO STAY

"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

MANAGING CYBER RISK ACROSS THE ENTERPRISE

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

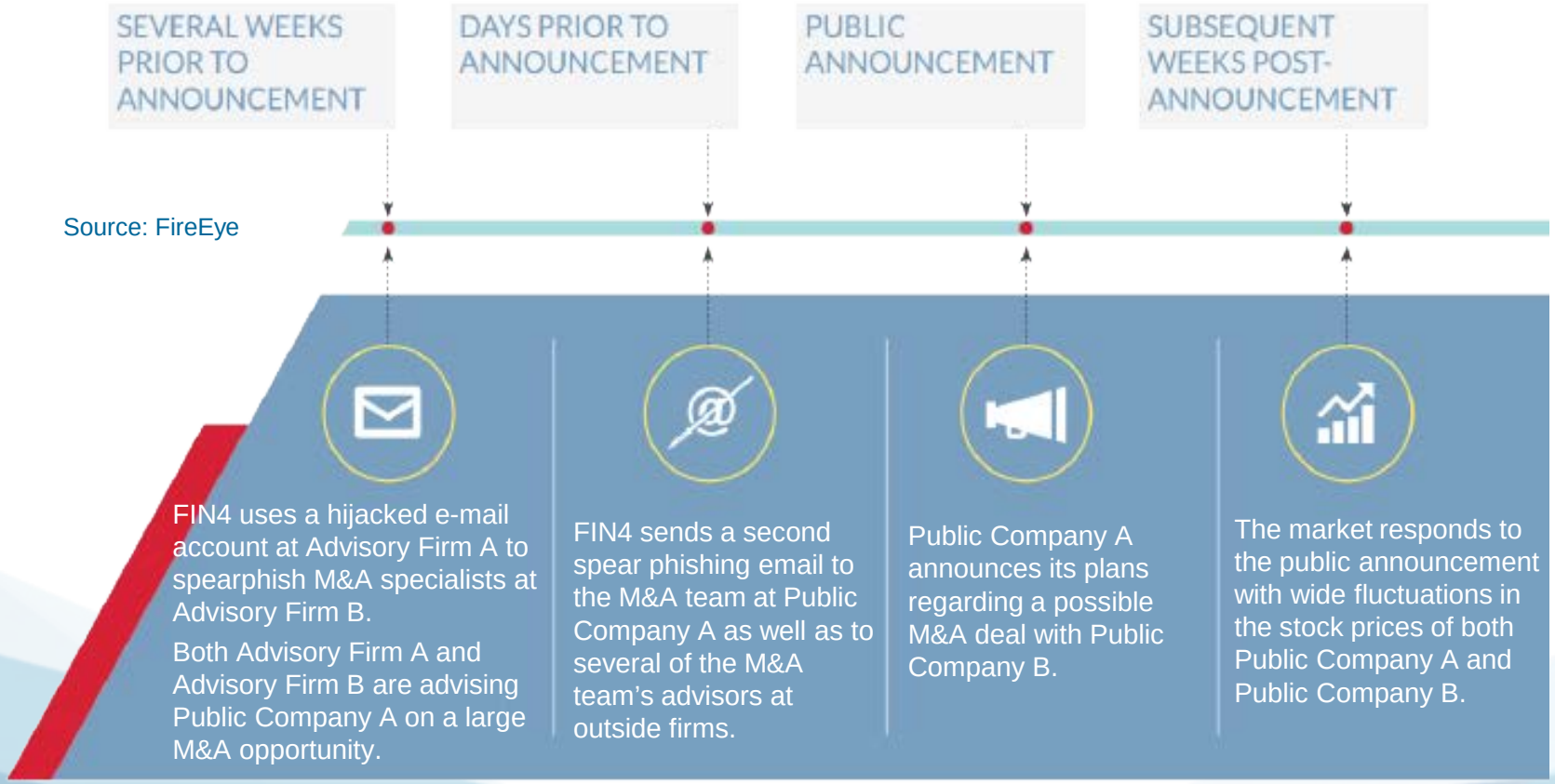
- **CISO/CIO:**
  - The responsibility for executing the cyber security strategy usually rests largely with the CISO and the CIO working together and with the business units.
- **Operations:**
  - Maintaining daily operations, business processes, and workplace stability is critical during a cyber event.
- **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: SPEAR PHISHING

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.

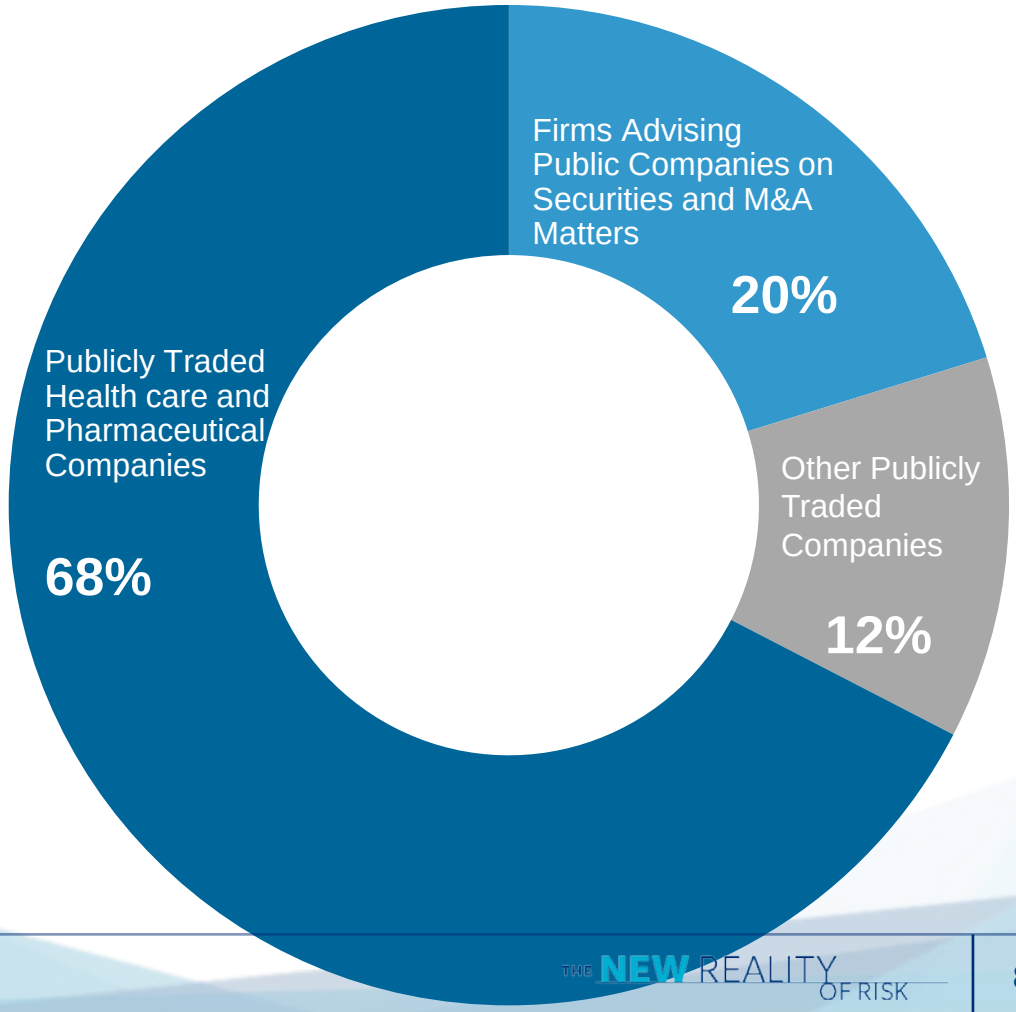


CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
FIN4: TARGETING INSIDER DATA FOR A MARKET ADVANTAGE

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



Source: FireEye

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
FIN4: A FLY ON MANY WALLS — LATERAL COMPROMISE

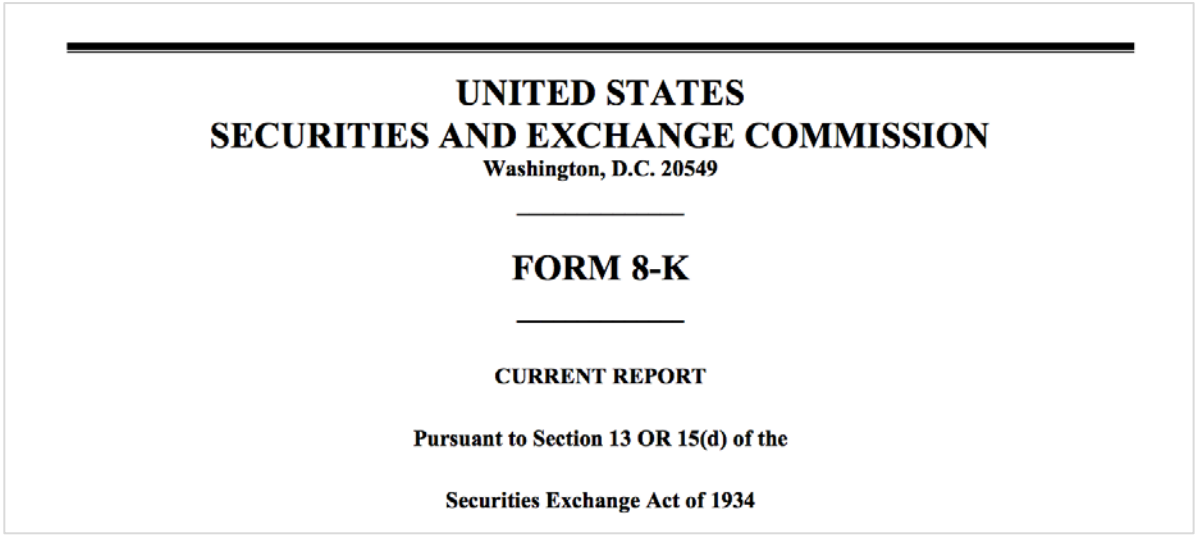
FIN4 Targeting Cycle

- 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

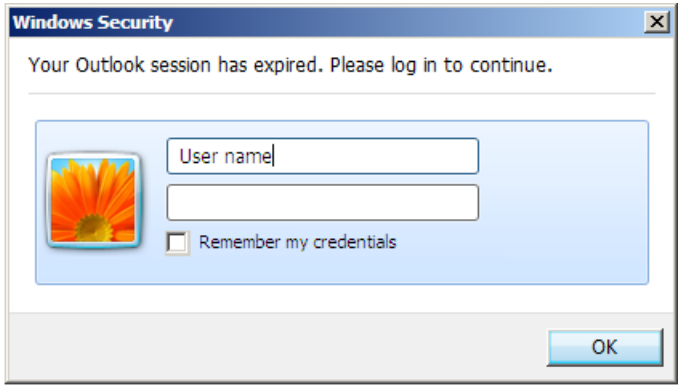
Pursuant to Section 13 OR 15(d) of the

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.

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
FIN4: INITIAL ACCESS — TRUSTED SENDERS

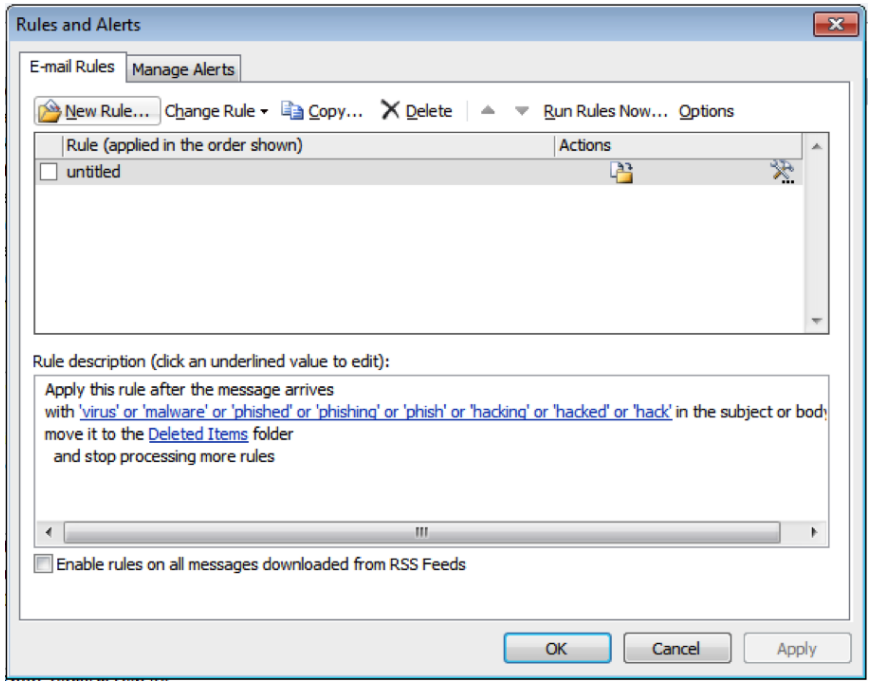
- Emails originate from **trusted senders.**
  - Links to fake Outlook Web Access portal.
  - **Documents with embedded macros.**
    - **Weaponized stolen documents.**

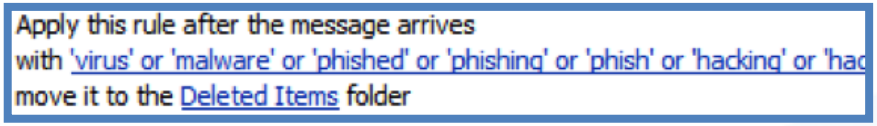


Source: FireEye

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
FIN4: MAINTAIN ACCESS

- 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

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
THREAT ACTOR MOTIVATIONS

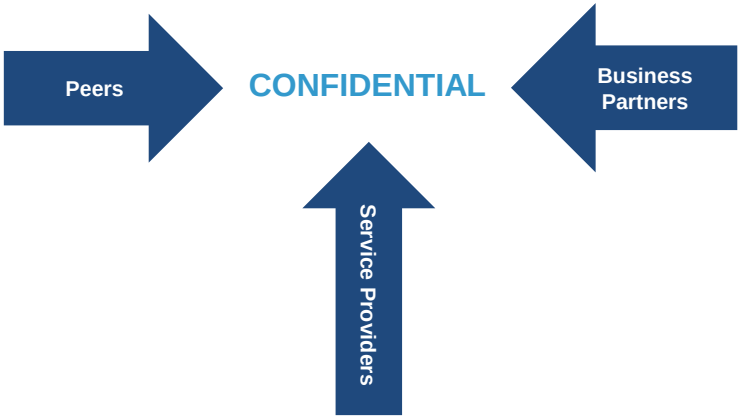
Threat actor motivations for targeting the firm's clients, partners, and peers:

- 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

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
EXPOSURES VIA TRUSTED THIRD PARTIES

Attackers use trusted third parties as vectors for access to high-value data and systems.



CASE STUDY:
FINANCIAL SERVICES SOFTWARE FIRM

- 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

ACTIVE ADVERSARIES

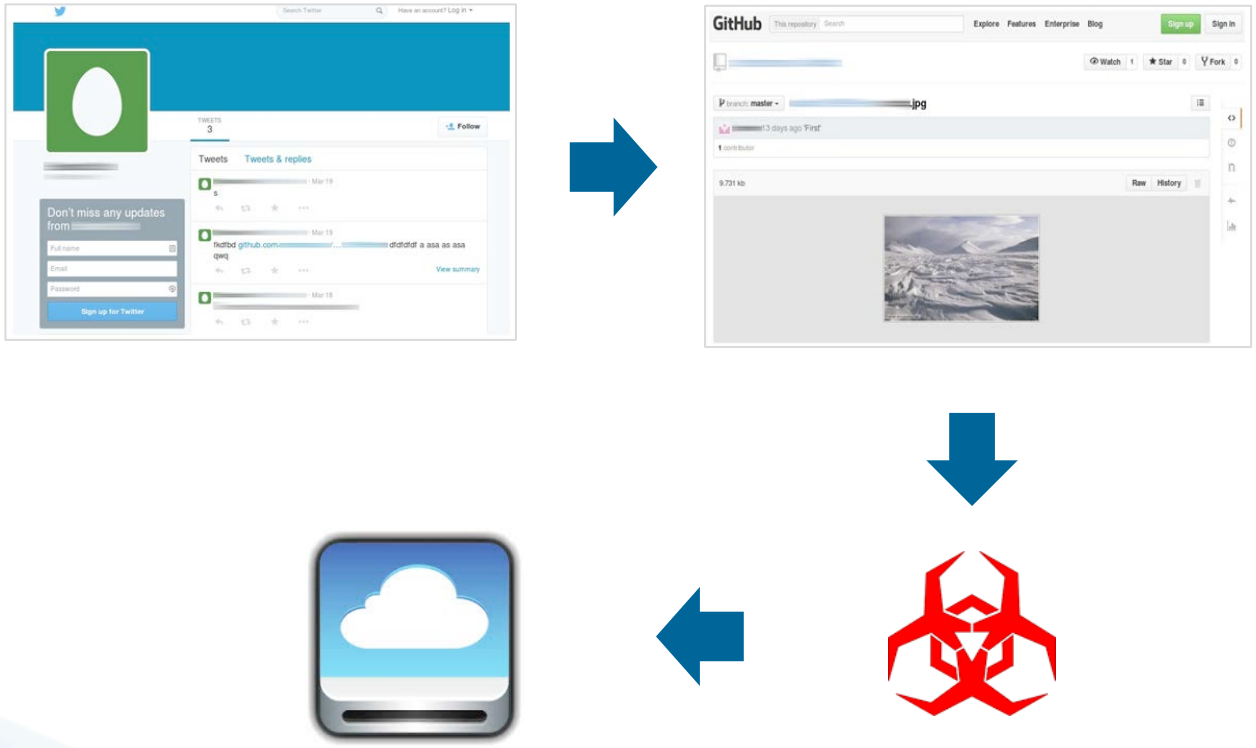
"These are threat actors who are determined and have ample tools and tactics at their disposal. When they hit a road block, they will adapt or switch up their tactics."

— Kristen Dennesen
FireEye Senior Intelligence Threat Analyst

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
LEVERAGING LEGITIMATE CLOUD SERVICES

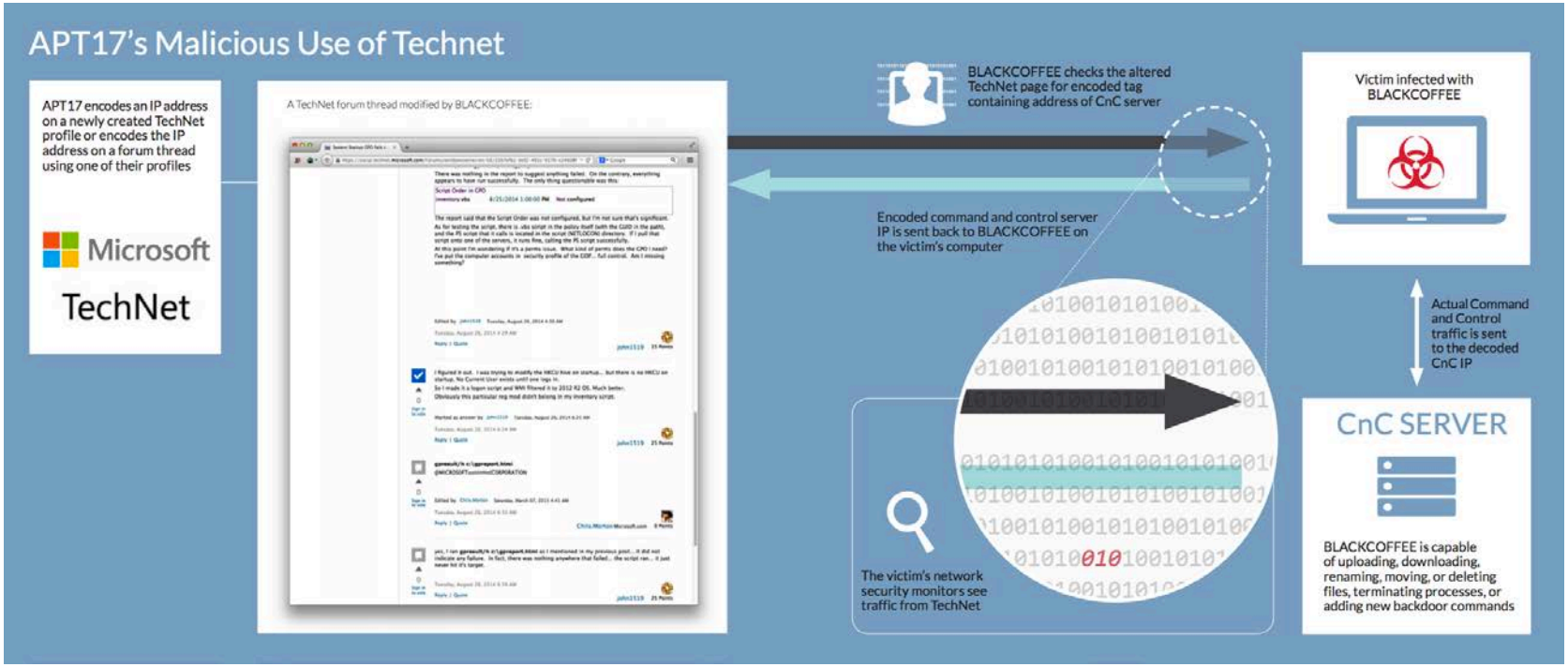
Example: HAMMERTOSS Backdoor Network Communications

- Twitter + GitHub + Cloud Drive



Source: FireEye

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
EXPLOITATION OF LEGITIMATE SERVICES

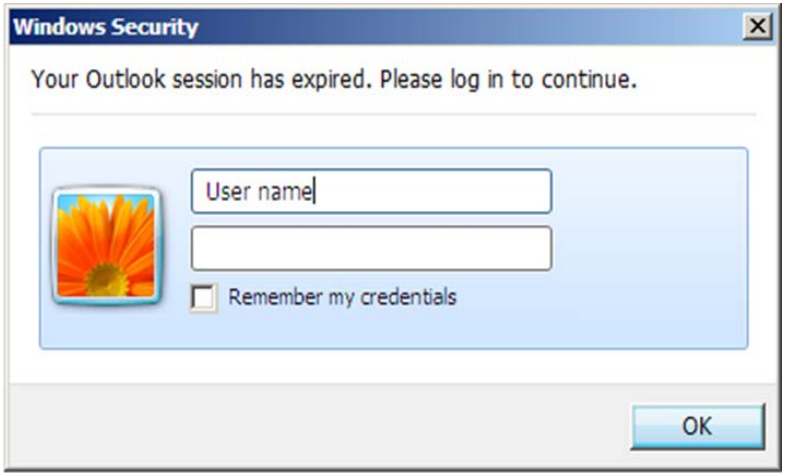


- APT17 configured BLACKCOFFEE malware to use Microsoft TechNet for C2 communications.
  - "Dead drop resolver": Encoded IP address reached out to legitimate forum threads.
  - BLACKCOFFEE supports ~15 commands, including creating a reverse shell, uploading and downloading files, and enumerating files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

Source: FireEye

AND ON AND ON…

- FIN4
- Facebook
- Twitter
- Dropbox/OneDrive



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

Source: FireEye

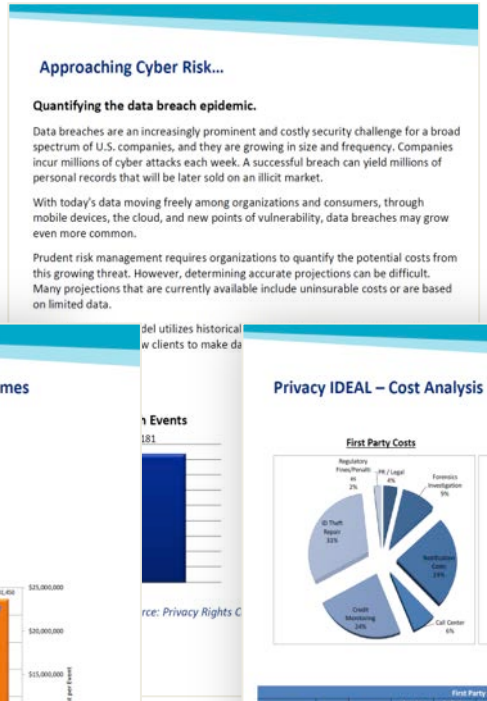
CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES

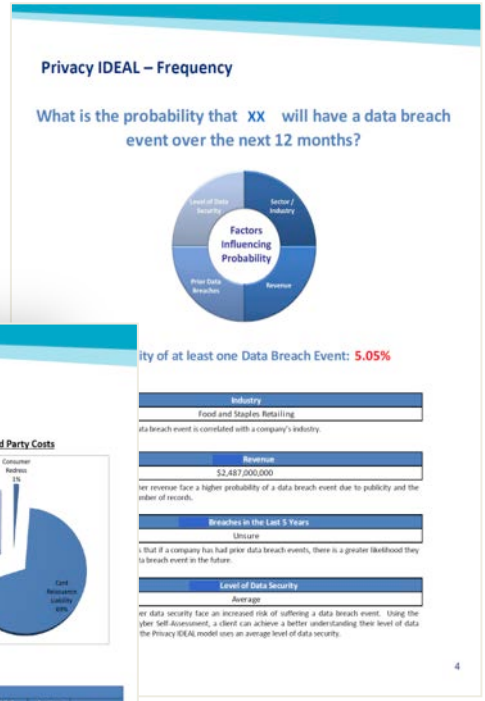
CYBER RISK FRAMEWORK

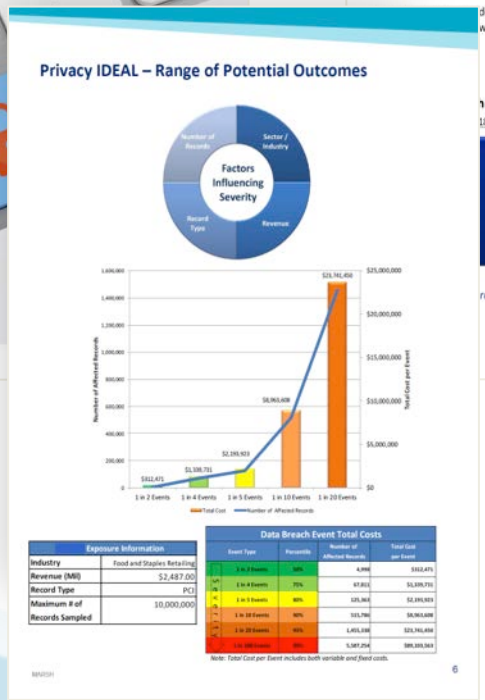
Marsh's Cyber Risk Management Framework		
Assess	**Manage**	**Respond**
Identify | Quantify | Analyze	**Prevent | Prepare | Transfer**	**React | Recover | Communicate**
A thorough understanding of your risk profile is critical, and that means more than the typical compliance audit. You need to inventory 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.

CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES

CYBER IDEAL: PRIVACY EVENT MODEL







CYBER RISK MANAGEMENT: NEW THREATS, NEW APPROACHES
CYBER INSURANCE MARKETS

- 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.