AGENDA – DATA COMPROMISE AND CYBER

What is the problem?
How does this happen?
What is your business impact and cost?
How do you protect yourself?
WHAT IS DATA COMPROMISE?

An incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.

searchsecurity.techtarget.com, 2010

DATA COMPROMISE – THINK IT CAN’T HAPPEN TO YOU?

System Hack
Burglary
Class-Action Lawsuit

Hackers installed card skimmers onto a business’s payment card system. Over the course of several weeks, they were able to collect hundreds of debit and credit card numbers. The business must investigate and notify all of the affected individuals.
DATA COMPROMISE – THINK IT CAN’T HAPPEN TO YOU?

System Hack
Burglary
Class-Action Lawsuit

A business owner arrived at work and discovered the office in disarray from a burglary. Several computers were stolen and file cabinets were broken into, which contained confidential customer and employee information, including social security numbers, addresses, and credit card information.

DATA COMPROMISE – THINK IT CAN’T HAPPEN TO YOU?

System Hack
Burglary
Class-Action Lawsuit

Following a serious data breach, a business promptly notified all of the affected individuals that had their personal identifying information compromised. Several months later, the business was served with a class-action lawsuit alleging they failed to properly safeguard the customers’ information.
DATA COMPROMISE—HOW CAN IT HAPPEN?

- Laptop computer theft
- Lost data
- Trash theft
- Hackers
- Employee
- Theft

DATA COMPROMISE – RESPONSE EXPENSE COVERAGE*

- Public Relations Services
- Services to Affected Individuals
- Forensic IT Review
- Legal Review
- Notification to Affected Individuals

*Subject to sub-limits
2015 DATA BREACH STATISTICS

• Can your business survive a data breach or privacy loss?

- 2015 Cost of Data Breach Study – United States; Ponemon Institute® LLC and IBM®

Average Cost of Compromised Record

$217 49%

- 2015 Cost of Data Breach Study – United States; Ponemon Institute® LLC and IBM®
2015 DATA BREACH STATISTICS

- Can your business survive a data breach or privacy loss?

$217 49%
Malicious or Criminal Attacks

-- 2015 Cost of Data Breach Study -- United States, Ponemon Institute LLC and IBM®

DATA COMPROMISE – DEFENSE AND LIABILITY COVERAGE

This protection helps cover the costs to defend against, and the legal obligations to pay or settle, third-party claims and suits brought by affected individuals as a result of the data breach.
WHAT is a CYBER-ATTACK?

An attempt to **damage, disrupt, or gain unauthorized access** to a computer, computer system, or electronic communications network.

CYBER-ATTACK—How it Happens

**Contribution to Denial of Service Attack**
- Breach of Third-Party Business Information

**Virus Infection**
- Denial of Service

**Former Employee**
- Transmitting Malware

CYBER THREATS—Fraudulent Tech Support
March 28, 2017

For Reference of NECA Now 2017 San Antonio
Attendees Only

CYBER THREATS–Wire Transfer E-mail Spoofing

Date: [date email received]
From: [spoofed executive's email address]
To: [each of the targeted recipients]
Subject: Company Acquisition [target's name].

Regarding a new Acquisition we are finalizing, Attorney Gary Cooper will be contacting you shortly. I need you to provide him with some of our accounting details so they can finish and file the financial forms required for the due process. We will also need to proceed with several payments, the first one to lock the Acquisition and the followings to finalize it. He will further explain to you how to execute the wire instructions following the regulations in place.

It is crucial for the company this operation is executed swiftly, efficiently and with extreme discretion. Again, you need to keep this matter very confidential to avoid any financial fines or worst, you understand. Any question you may have must be addressed directly to Gary.

Thank you for treating this with your utmost attention.
Best Regards.
[spoofed executive's name]

---

CYBER THREATS–Ransomware

---

FBI Public Services Announcement
CYBER THREATS–Ransomware

- 97% of malware is Ransomware!
  - Proofpoint 2016 Q3 Threat Summary Report
- 48% of companies infected by ransomware paid the ransom
  - Ponemon Institute Report

CYBER THREATS–Tactics

- Reconnaissance
- Create/modify malware
- Deliver malware
- Establish communication channel to command and control system
- Pivot Network
- Search for data of value
- Extract data of value
CYBER THREATS–Malware

CYBER THREATS–Malware Delivery
CYBER THREATS–Target Data

<table>
<thead>
<tr>
<th>Data Range</th>
<th>Percent of Incidents</th>
<th>Median</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>27%</td>
<td>50,000</td>
</tr>
<tr>
<td>PHI</td>
<td>11%</td>
<td>1,900</td>
</tr>
<tr>
<td>FI</td>
<td>10%</td>
<td>791</td>
</tr>
<tr>
<td>Non-card/Financial</td>
<td>0%</td>
<td>55</td>
</tr>
</tbody>
</table>

Note: Data sourced from [insert source here]

Table 1: Details on the Incidence of Cyber Threats

CYBER THREATS–Business Impact

- **Notifications**
  - Impacted individuals
  - Regulatory agencies
  - Major news media

- **Regulatory Fines**
  - Improvement plans
  - Audits
CYBER THREATS—Business Impact

- Operations
  - Productivity
  - Expenses

- Brand and Reputation
  - Public relations
  - New business closing ratios
  - Retention goals

Security Layers – Fraudulent Tech Support

- Technology
  - Internet browsing protection
- Process
  - Retainer with computer forensic firm needed?
- People
  - Training
Security Layers – Wire Transfer E-mail Spoofing

- Technology
  - E-mail filter protection
- Process
  - Second approver required for wire transfers?
- People
  - Training

Security Layers – Ransomware

- Technology
  - E-mail filter protection
  - Anti-malware on workstations/servers
- Process
  - Second approver required for wire transfers?
- People
  - Training
Security Layers – Encryption

- Full Disk Encryption for Laptops
- Mobile Device Protection
- Transferring Sensitive Data
  - Secure e-mail
  - Secure ftp

Security Layers – Basic Network Procedures

- Physical security
- Limit access to data
- Data backup and restore
- Patching systems
- NIST – Small Business Information Security:
  - The Fundamentals
2015 INTERNET SECURITY THREAT STATS

There were more than 317 million new pieces of malware created last year (2014), meaning nearly one million new threats were released each day.

– ISTR20 Internet Security Threat Report, Symantec®

2015 INTERNET SECURITY THREAT STATS

In 2014, Symantec® observed that 70% of social media scams were manually shared.

– ISTR20 Internet Security Threat Report, Symantec®
### 2015 Internet Security Threat Stats

Last year (2014), **60%** of all targeted attacks struck small- and medium-sized organizations.

- [IST020 Internet Security Threat Report; Symantec®](#)

### Cyber – Computer Attack Coverage*

<table>
<thead>
<tr>
<th>Coverage Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Restoration Costs</td>
</tr>
<tr>
<td>Public Relations Services</td>
</tr>
<tr>
<td>Data Recreation Costs</td>
</tr>
<tr>
<td>Business Income &amp; Extra Expense</td>
</tr>
<tr>
<td>System Restoration Costs</td>
</tr>
</tbody>
</table>

*Subject to sub-limits*
CYBER – NETWORK SECURITY LIABILITY COVERAGE

- Breach of Third-Party Business Information
- Malware Transmission
- Contribution to Denial of Service Attack

Two Coverage Options*:

- **Data Compromise**, $50K-$1M Limits
  - Response Expenses
  - Defense & Liability

- **Cyber**, $50K-$100K Limits
  - Computer Attack
  - Network Security Liability

*Subject to sub-limits
BUSINESS COMPUTER COVERAGE – OPTIONS INCLUDE

Electronic Data, Media, and Computer Software Programs

Extra Expense

Property in Transit or at Temporary Locations

Business Computer Equipment (Hardware)

COMPUTER AND FUNDS TRANSFER FRAUD

Funds Transfer Fraud

Computer Fraud
**Directors and Officers (D&O) Liability**

- Punitive or exemplary damages
- Bodily injury or property damage liability
- Cyber or data extortion, blackmail, or ransom
- Reputational harm or damage
- Business income and extra expense from dependent properties
- Fines or penalties

**Assessments, such as those by the Payment Card Industry (PCI)**

- Payment Network's Fraud Liability Shift (associated with EuroPay, MasterCard®, and Visa® (EMV))

- Software, system, or network upgrades

---

**RISK MANAGEMENT – eRISKHUB®**

- Learning Center
- Incident Roadmap
- Risk Manager Tools
- News Center
- eRisk Resources Directory
Complimentary Resources

SUMMARY

What is the problem?

How does this happen?

What is your business impact and cost?

How do you protect yourself?
Questions

Up Next: Lunch on Event Lawn 1

Breakouts resume at 1:30

Don’t forget to fill out the online evaluation at www.necanet.org/NNSurvey2017