National League of Cities

Risk Information Sharing Consortium

Libby Benet, JD, CIPP-US, CIPM
President, Cyber Secure Work, Inc.
October 16, 2019
“It’ll Never Happen to Me”: Avoiding and Managing Cyber Attacks On Municipalities

<table>
<thead>
<tr>
<th>Level Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Alarming Stats</td>
</tr>
<tr>
<td>What Are The Threats?</td>
</tr>
<tr>
<td>What Needs Protecting?</td>
</tr>
<tr>
<td>Common Types of Attacks</td>
</tr>
<tr>
<td>Frameworks/Standards/Compliance</td>
</tr>
<tr>
<td>Compliance v. Security</td>
</tr>
<tr>
<td>Systems Fail. Now What?</td>
</tr>
<tr>
<td>Typical Types of Coverages and Services</td>
</tr>
<tr>
<td>Issues to Growth</td>
</tr>
</tbody>
</table>
It’s Complicated…
What do Business Leaders Need To Know - Information Security

Objective of information security is to ensure information’s confidentiality, integrity, availability and accountability.

The focus of information security is to reduce the potential for damage to, loss of, modification of or unauthorized access to systems, facilities or data.

Information security includes the technical and physical controls of IT systems, building security, remote users, vendors, third parties and the creation and maintenance of business-continuity and disaster-recovery plans.
What do Business Leaders Need To Know - Privacy

The objective of privacy protections is to ensure that individuals receive the following considerations about their protected data:

Notice, choice and consent and the option to correct misinformation.

Privacy protections attach to the people who give a business their personal information.

These protections are concerned with the individual’s ability to control the use of that information.
One Is the “What” and the Other Is the “How”!
15 Alarming Cyber Security Facts and Stats According to Cybint Solutions:

• 95% of breached records came from only three industries in 2016
• There is a hacker attack every 39 seconds
• 43% of cyber attacks target small business
• The average cost of a data breach in 2020 will exceed $150 million
• In 2018 hackers stole half a billion personal records
• Over 75% of healthcare industry has been infected with malware over last year
• Large-scale DDoS attacks increase in size by 500%

https://www.cybintsolutions.com/cyber-security-facts-stats/
15 Alarming Cyber Security Facts and Stats According to Cybint Solutions:

- Approximately $6 \textbf{trillion} is expected \textbf{to be spent globally} on cybersecurity by 2021
- By 2020 there will be roughly 200 billion \textbf{connected devices}
- Unfilled cybersecurity jobs worldwide will reach \textbf{3.5 million} by 2021
- 95% of cybersecurity breaches are due to \textbf{human error}
- More than 77% of organizations do not have a Cyber Security Incident Response plan
- Most companies \textbf{take nearly 6 months to detect} a data breach, even major ones
- 46% of all Bitcoin transactions involve illegal online activity
- Total cost for cybercrime committed globally has added up to over $1 trillion dollars in 2018
Where Are the Insider Threats?

- Employee negligence
  - Security failures
  - Lost portable devices
  - Unintended disclosures by email, fax, phone or in person

- Failure to encrypt portable devices
  - Employee ignorance
    - Improper disposal of personal information (dumpsters)
    - Lack of education and awareness
  - Malicious and/or nosey employees
Where Are the Outside Threats?

- Hackers
  - Malware
  - Phishing and spear phishing
- Thieves/Organized Crime
  - Social engineering tools
  - Stolen portable devices
- Vendors/Business Associates
- Nation State Actors
## Where Is the Risk? Threat Actors and Their Attacks

<table>
<thead>
<tr>
<th>Actors</th>
<th>Attack Example</th>
<th>Motivation</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber criminals; organized crime</td>
<td>Bank, govt. or other sector account takeover via malware and/or impersonation</td>
<td>Financial gain</td>
<td>Financial loss for victim</td>
</tr>
<tr>
<td>Insiders</td>
<td>Financial, political, economic attack</td>
<td>Financial or political gain</td>
<td>Financial loss Disruption</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Anonymous attacks on payment processors in defense of WikiLeaks founder</td>
<td>Political or social statement</td>
<td>Service disruption</td>
</tr>
<tr>
<td>Cyber espionage actors</td>
<td>Theft of IP from chip manufacturer, planting and using back doors in firewalls</td>
<td>Information, economic, financial gain</td>
<td>IP loss Economic loss</td>
</tr>
<tr>
<td>Nation-states</td>
<td>U.S. attacks Iran with Stuxnet, Iran attacks U.S. bank websites Misinformation</td>
<td>Disable critical infrastructure Affect political outcomes</td>
<td>Temporary ? setbacks or outages</td>
</tr>
</tbody>
</table>
The Landscape To Secure

- Desktops
- Laptops
- Networks
- Mobile
- Websites
- Email
- Industrial Control Devices
- Cloud
- Internet of Things (IoT)
What Does It Mean To Protect?
Defense In Depth


© 2010, 2012 Northrop Grumman Corporation
What data is there to protect?

• Mortgage documents, deeds, births, deaths, ugly divorces, medical records, Social Security numbers and military discharge documents are among the many types of publicly accessible documents that may contain PII (personally identifiable information), PHI (personal health information) or other sensitive data.

What Is Happening? - City of Baltimore

https://www.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html
2019 Events....

According to CNN, “Just this year alone, **140 attacks** targeting public state and local governments and health care providers have been reported, according to a tally by the cybersecurity firm Recorded Future, which has tracked attacks on local governments since 2013 and the healthcare industry since 2016.”

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

https://www.cisecurity.org/ms-isac/
5 Top Security Concerns of the Center For Internet Security

- Lack of funding for cyber
- Inadequate cyber professionals
- Increasing sophistication of threats
- Lack of documented practices
- Emerging technologies
Issues for Municipalities

• Lack of skilled and trained personnel in cybersecurity.
• Lack of disaster recovery plans.
• Lack of third-party risk management in place for their supply chain.
• Complexity of state and federal regulations. (e.g. HIPPA, Mental Health Regulations, Criminal Justice Regs, Department of Health).
• Shared Infrastructure.
• Decentralized/Siloed management of IT/IS.
• Budget limitations.
• Lack of cybersecurity training for employees.

Common Types of Cyber Attacks

**Malware** is a term used to describe malicious software, including spyware, ransomware, viruses, and worms.

Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

Once inside the system, malware can do the following:

- Blocks access to key components of the network (ransomware)
- Installs malware or additional harmful software
- Covertly obtains information by transmitting data from the hard drive (spyware)
- Disrupts certain components and renders the system inoperable

Common Types of Cyber Attacks

**Phishing** is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email.

The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine.

Phishing is an increasingly common cyberthreat.

Common Types of Cyber Attacks

**Man-in-the-middle (MitM) attacks**, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor’s device and the network. Without knowing, the visitor passes all information through the attacker.

2. Once malware has breached a device, an attacker can install software to process all of the victim’s information.

Common Types of Cyber Attacks

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth.

As a result, the system is unable to fulfill legitimate requests.

Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

Common Types of Cyber Attacks

A **Structured Query Language (SQL)** injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not.

An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Common Types of Cyber Attacks

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

# Frameworks/Standards/Compliance

<table>
<thead>
<tr>
<th>Government</th>
<th>Industry</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIAP</td>
<td>PCI DSS</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>GDPR</td>
<td>HIPAA/HITEST</td>
<td>ISO 27002</td>
</tr>
<tr>
<td>US Swiss Privacy Shield</td>
<td>FFIEC</td>
<td>NIST CIC</td>
</tr>
<tr>
<td>OSFI</td>
<td>NCUA</td>
<td>NIST 171</td>
</tr>
<tr>
<td>FISCAM</td>
<td>NYDFS</td>
<td>FAIR</td>
</tr>
<tr>
<td>SOX</td>
<td>DFAR</td>
<td>ISF</td>
</tr>
<tr>
<td>PIA</td>
<td>NERC CIP</td>
<td>COBIT 5</td>
</tr>
<tr>
<td>GLBA</td>
<td></td>
<td>AICPA</td>
</tr>
<tr>
<td>CCPA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key Areas Covered in Assessments

- Acceptable Use/Employee Data Policy
- Identity and Access Policy
- Business-Continuity Planning/Disaster-Recovery Plan Execution
- Data Classification and Privacy
- Incident Management
- Vulnerability Scans/Penetration Testing
- Company Culture/Governance
- Actual Breach/Cyber Hazard Event
"Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it enables risk-based implementations that are customized to the organization's needs. "

National Institute of Science and Technology Cybersecurity Framework Core
# Deeper Dive

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Asset Management</td>
<td>ID.AM</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>ID.BE</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>ID.GV</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>ID.RA</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Risk Management</td>
<td>ID.SC</td>
</tr>
</tbody>
</table>

| Protect        | Identity Management and Access Control | PR.AC  |
|               | Awareness and Training                  | PR.AT  |
|               | Data Security                           | PR.DS  |
|               | Information Protection Processes & Procedures | PR.IP  |
|               | Maintenance                            | PR.MA  |

## Subcategory

<table>
<thead>
<tr>
<th>ID.BE-1: The organization's role in the supply chain is identified and communicated</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Informative References</strong></td>
</tr>
<tr>
<td>COBIT 5, APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05</td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2</td>
</tr>
<tr>
<td>NIST SP 800-53 Rev. 4 CP-2, SA-12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Informative References</strong></td>
</tr>
<tr>
<td>COBIT 5, APO02.06, APO03.01</td>
</tr>
<tr>
<td>ISO/IEC 27001:2013 Clause 4.1</td>
</tr>
<tr>
<td>NIST SP 800-53 Rev. 4 PM-8</td>
</tr>
</tbody>
</table>
Compliance v. Security - What's the difference?

https://phoenixnap.com/blog/security-vs-compliance
Let’s look at the cybersecurity requirements imposed by the New York State Department of Financial Services.

Financial institutions, banks, credit unions, insurance firms, financial advisors and more are covered by the law.

The law itself is good start at establishing minimal standards but does not prescribe how to secure.

For example, the regulation requires that a scan be performed twice a year, but the regulation provides no guidance as to what kind of scan ought to be done.

Instead the state has left it to the regulated entity to decide and self-certify a scan has been performed twice a year.

If you use a network scanner twice a year your organization may have met the regulatory requirement, but does that mean the system is secure? Not really.
You did all the right things, but the system failed anyway. Now what?

**Event or Incident**
- National Institute of Standards and Technology defines an event as “any observable occurrence in a system or network,” such as a server receiving a request for a web page, a user sending an e-mail message, or a firewall blocking an attempt to make a connection.

**Adverse Event**
- The guide also defines adverse events as those with a “negative consequence, such as ... unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.”

**Privacy Event**
- As defined by the U.S. Department of Homeland Security, a privacy incident is an adverse event that happened as a result of violating DHS’ privacy policies and procedures. The privacy incident must “pertain to the unauthorized use or disclosure” of regulated data, like personally identifiable information or protected health information.

**Data Breach**
- If a privacy incident meets specific legal definitions, per state and/or federal breach laws, then it is considered a data breach. Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies or the media. Additionally, contractual obligations require notice to business clients if the incident affected clients’ employees or customers.

Is it an incident or a breach? How to tell and why it matters. [https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/](https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/)
Where Can the Losses Come From?

<table>
<thead>
<tr>
<th>Loss Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data breaches—personal data, corporate intellectual property compromised</td>
</tr>
<tr>
<td>Malware/hostage for ransom</td>
</tr>
<tr>
<td>Systems development/network security of the enterprise</td>
</tr>
<tr>
<td>Digital supply chain</td>
</tr>
<tr>
<td>Phishing/email and mobile phone text scams</td>
</tr>
<tr>
<td>Regulatory fines—GDPR/California Consumer Data Privacy Act</td>
</tr>
<tr>
<td>Business interruption, data restoration and data protection</td>
</tr>
<tr>
<td>Liability for actual damages and punitive awards</td>
</tr>
<tr>
<td>Bank recovery of card fraud loss</td>
</tr>
<tr>
<td>Loss of funds/property through social engineering</td>
</tr>
</tbody>
</table>
US Insurance Industry – Stand Alone = $1B
Typical Types of Coverage and Services

<table>
<thead>
<tr>
<th>Breach Response Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Council</td>
</tr>
<tr>
<td>Forensics</td>
</tr>
<tr>
<td>Credit Monitoring</td>
</tr>
<tr>
<td>Public Relations &amp; Crisis Management</td>
</tr>
<tr>
<td>Required Notifications</td>
</tr>
<tr>
<td>Voluntary Notifications</td>
</tr>
<tr>
<td>Call Center</td>
</tr>
<tr>
<td>Law firm to determine indemnification under contract with indep contractor</td>
</tr>
<tr>
<td>Data Breach Coach</td>
</tr>
<tr>
<td>Fraud Consultation to customers</td>
</tr>
<tr>
<td>Restoration of Identity</td>
</tr>
</tbody>
</table>
Typical Types of Coverage and Services

- Business Interruption
- Systems Failure
- Consequential Reputational Income Loss
- Dependent Systems Failure
- Dependent Security Breach
- Cloud Computing
- Extortion
- Data Recovery
- Good Faith Advertising to regain customer loyalty

First Party
Typical Types of Coverage and Services

- Network Liability
- Privacy Liability
- Regulatory Defense and Penalty
- Consumer Redress Fund
- Credit Card Liabilities and Costs
- Media Liability
- Miscellaneous Professional
- Third Party
Typical Types of Coverage and Services

Crime Coverages

- Fraudulent Instruction
- Funds Transfer Fraud
- Telephone Fraud
- Criminal Reward
Typical Types of Coverage and Services

- Employee Training
- Sample Incident Response Plans
- Educational pieces, posters, webinars
- Ala carte Prevention Services
Key Exclusions

Liability

- Bodily Injury and Property Damage
- Intentional or Criminal Acts
- War – is there a terrorism or nation state carve back?
- Loss of Funds

First Party

- Hardware or software replacement
- Fire, Flood, Earthquake etc

Prior Notice and Prior or Pending Litigation
Other Considerations

- Trigger - Claims Made for Liability
- Trigger - Incident Discovered for First Party
- Are Expenses Inside or Outside the Limit?
- Review Definitions
- How much Limit is Needed?
- Underwriting Process
On the Horizon

NEW PRIVACY LAWS – STATE OR FEDERAL

UN CYBERSECURITY GOVERNANCE

NEW TECHNOLOGIES

CYBER CAT
### What are the biggest obstacles to writing cyber insurance policies? (select up to 3)

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not understanding exposures</td>
<td>75%</td>
</tr>
<tr>
<td>Not understanding coverage</td>
<td>56%</td>
</tr>
<tr>
<td>Cost</td>
<td>42%</td>
</tr>
<tr>
<td>Application process</td>
<td>35%</td>
</tr>
<tr>
<td>Different policy forms/coverages in market</td>
<td>26%</td>
</tr>
<tr>
<td>Scope of coverage</td>
<td>12%</td>
</tr>
<tr>
<td>Lack of value added products/services</td>
<td>7%</td>
</tr>
<tr>
<td>Capacity constraints in market</td>
<td>6%</td>
</tr>
</tbody>
</table>

Advisen and Partner Re 2018 Survey Of Cyber Insurance Market Trends
Thank you!

Any questions?