Cyber Risk for

Small and Medium-Sized Enterprises (SMEs)

Presenters: Jing Guo, Junyi Yang

09/09/2016
New York Times Headlines: “No business too small to be hacked”

- Rokenbok Education
- 7 employees
- Restructure Their Entire Business and IT System
Key Findings

Cyber Risk for SMEs

Perception V.S. Reality

Challengers for Insurance Carriers

Cyber Insurance for SMEs

Actions & Challenges for SMEs

Monitoring and Tracking Process

Conclusion
Key Findings

- Cyber risk - A Real and Growing Concern for SMEs
- SMEs: cyber risk management
- SMEs vary by business sector
What is Cyber Risk for SMEs?

❖ Operational Risk

❖ Four Categories:

➢ Attacks on Physical Systems
➢ Authentication & Privilege Attacks
➢ Denial of Service
➢ Malicious Internet Content
The Perception V.S. The Reality

**Perception**
- Too Insignificant
- Large Businesses are more Targeted

**Reality**
- **HALF** SMEs are Victims
The Perception V.S. The Reality

**Perception**
- Applied Appropriate Security Protocols

**Reality**
- Inadequate Resources
- Less Time & Money Devoted
- Have no data security policies
The Reality Continuous - Business Impact

- 93% of SMEs that suffered a cyber breach have had an impact on their business
- 60% of SMEs will be out of business within 6 months of a cyber attack
- In General, Cyber Impact Cost Increased 238% from $8,700 (2013) to $20,700 (2014)
The Reality Continuous - Business Impact

❖ Reputation Damage
❖ Loss of Clients
❖ Ability to Operate
❖ Loss of Money/Savings
The Reality Continuous - Business Impact

- **Time to Recover**

<table>
<thead>
<tr>
<th></th>
<th>AUG. 2013</th>
<th>DEC. 2014</th>
<th>DEC. 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 day</td>
<td>38%</td>
<td>30%</td>
<td>25%</td>
</tr>
<tr>
<td>Between 1 - 3 days</td>
<td>39%</td>
<td>34%</td>
<td>34%</td>
</tr>
<tr>
<td>Between 3 - 7 days</td>
<td>11%</td>
<td>14%</td>
<td>15%</td>
</tr>
<tr>
<td>More than a week</td>
<td>7%</td>
<td>9%</td>
<td>10%</td>
</tr>
<tr>
<td>More than two weeks</td>
<td>5%</td>
<td>13%</td>
<td>16%</td>
</tr>
</tbody>
</table>
Actions to Reduce Cyber Risk

❖ A Formal Password Policy

➢ Weak Password

➢ Writing Down Instead of Memorizing

➢ Frequently Changed
Actions to Reduce Cyber Risk

❖ Providing Proper Training to the Employees

➢ 75%: Social Media Usage

➢ Restriction on Internet Access

➢ Regulate usage of external equipments (e.g. USB)
Actions to Reduce Cyber Risk

❖ Monitoring their IT Network
  ➢ Store their data online
  ➢ Timely Actions
  ➢ Access
Actions to Reduce Cyber Risk

❖ Conduct IT system security test

➢ Operation security is up to date

❖ Establish a cyber incident response team/plan
Challenges for SMEs

❖ Complexity of Cyber Risk

➢ Difficult for SMEs to fully understand
Challenges for SMEs

❖ Operational Risk

❖ Four Categories:

➢ Attacks on Physical Systems
➢ Authentication and Privilege Attacks
➢ Denial of Service
➢ Malicious Internet Content
Challenges for SMEs

❖ SMEs Vary by Business Sector

[Chart showing market size and cyber breaches by sector]
Challenges for SMEs

❖ Countless Cybersecurity Options But No Guidance

➢ Antivirus Software

➢ Cybersecurity Consultants

➢ Cyber Insurance/ Broker
Cyber Insurance

SMEs
Less than 3% of SMEs Have Cyber Insurance

Large Businesses
40% of Large Businesses Have Cyber Insurance
Cyber Insurance (First-Party Coverage)

- Physical Asset Damage
- Business Interruption
- State-Sponsored & Terrorists Cyber Attacks
- Theft
- Business Loss & Client Loss
- Recovery of Data & System
- Forensic Cost
- Response Cost
Cyber Insurance (Third-Party Coverage)

- Bodily Injury
- Third-Party Asset Damage
- Privacy Liability
- Reputational Liability
- Third-Party Privacy Liability
- Regulatory Fines & Penalties
Challenges for Insurance Carriers

❖ Need to be customized by business sector
❖ Need to be easily accessible with clearly defined benefits and coverage levels
❖ The underwriting process needs to be streamlined
❖ Need to be affordable and comprehensive
Monitoring and Tracking Cyber Risk Costs

❖ Database

➢ Monitoring

➢ Update Frequently

➢ Predictive Model
Conclusion and Next Steps

- Cyber Risk is underestimated by SME owners.
- Actions can be taken initially but individual SME cannot manage all of their cyber risk.
Conclusion and Next Steps

❖ Cyber insurance for SMEs is not well-developed
❖ Cyber Insurance needs to be customized by needs
❖ Develop a monitoring and tracking process
❖ The Goldenson Center for Actuarial Research
Q & A

Team Members:
Jay Krutiak: jay.krutiak@uconn.edu
Jing Guo: jing.guo@uconn.edu
Junyi Yang: junyi.yang@uconn.edu

Project Manager:
Niu Gao: Niu.Gao@uconn.edu

Project Director:
Jeyaraj Vadiveloo:
Jeyaraj.Vadiveloo@uconn.edu
# Q & A

## First-Party Coverage

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Asset Damage</td>
<td>Damage on IT equipment, IT systems and technology.</td>
</tr>
<tr>
<td>Business Interruption</td>
<td>Result from denial of services, website offline and employee down time.</td>
</tr>
<tr>
<td>State-Sponsored and Terrorists Cyber Attacks</td>
<td>Cyber attacks result from cyber warfare or terrorists.</td>
</tr>
<tr>
<td>Theft</td>
<td>Theft of data, economic value of intellectual property, finished goods in</td>
</tr>
<tr>
<td></td>
<td>processes, extortion, computing resources and deceptive fund transfer.</td>
</tr>
<tr>
<td>Business Loss and Client Loss</td>
<td>Data disclosure of personal and business information that result in a</td>
</tr>
<tr>
<td></td>
<td>business losing its revenue during normal operation.</td>
</tr>
<tr>
<td>Recovery of Data and System</td>
<td>The cost to restore data or systems that has been damaged or destroyed.</td>
</tr>
<tr>
<td>Forensic Cost</td>
<td>The cost to investigate cyber incidents and notification expenses.</td>
</tr>
<tr>
<td>Response Cost</td>
<td>The cost to minimize post-incident losses.</td>
</tr>
</tbody>
</table>
## Q & A

### Third-Party Coverage

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bodily Injury</td>
<td>Mental suffering, mental injury, shock, fright or other similar terms.</td>
</tr>
<tr>
<td>Third-Party Asset Damage</td>
<td>Infringement of third-party intellectual property such as designs, symbols, images and new ideas.</td>
</tr>
<tr>
<td>Privacy Liability</td>
<td>Loss of clients' private information and employee personal data.</td>
</tr>
<tr>
<td>Reputational Liability</td>
<td>Infringement of third party company's brand through first-party's network.</td>
</tr>
<tr>
<td>Third-Party Privacy Liability</td>
<td>Liability relating to third-party company's information.</td>
</tr>
<tr>
<td>Regulatory Fines and Penalties</td>
<td>Government or state fines on inappropriate data leaking caused by cyber incidents.</td>
</tr>
</tbody>
</table>