ROKENBOK® EDUCATION

R

UCONN

UCONN

Janet and Mark L. Goldenson Center for Actuarial Research

Illuminating Industry Innovation

Cyber Risk for

Small and Medium-Sized Enterprises (SMEs)

Presenters: Jing Guo, Junyi Yang

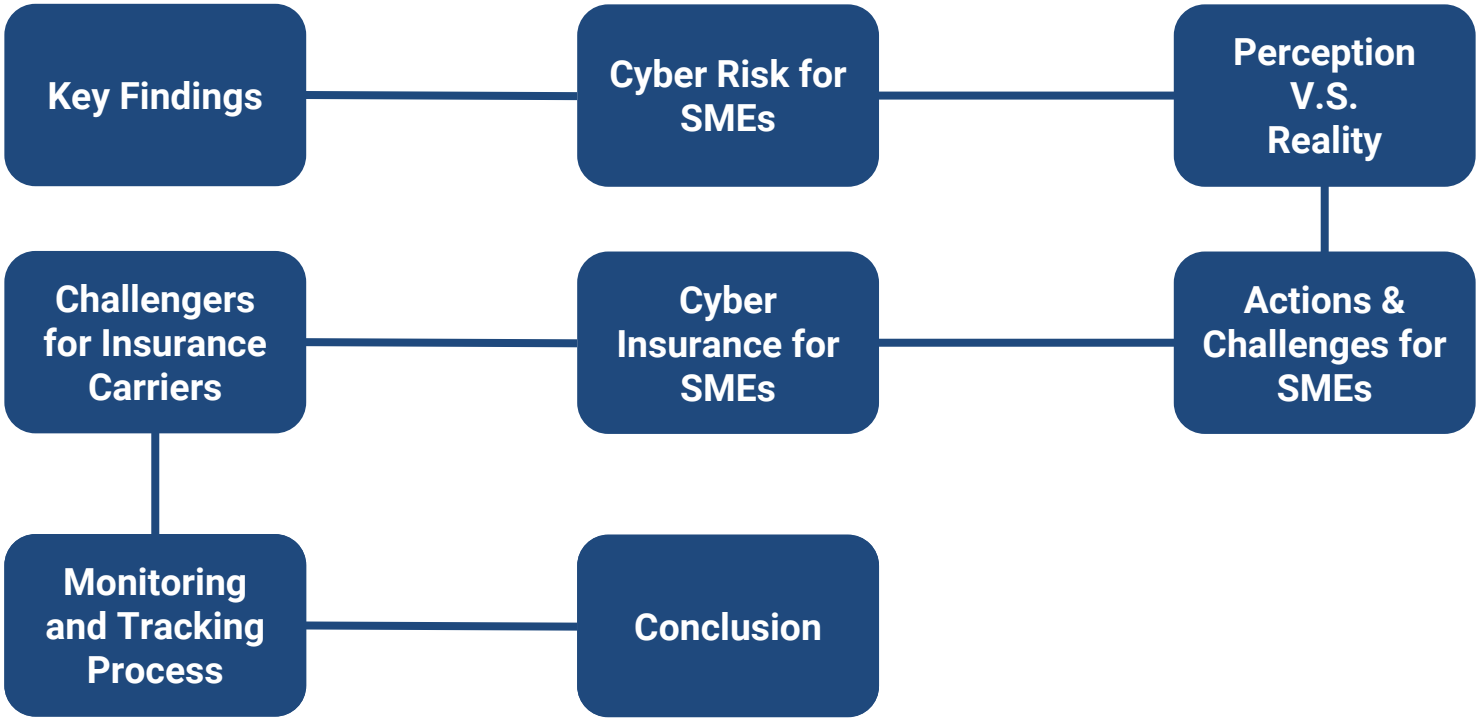
09/09/2016

UCONN

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

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

Presentation Flow Chart



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		Reality
Too Insignificant		**HALF** SMEs are Victims
Large Businesses are more Targeted		

The Perception V.S. The Reality

Perception

Reality

Applied Appropriate Security Protocols

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)

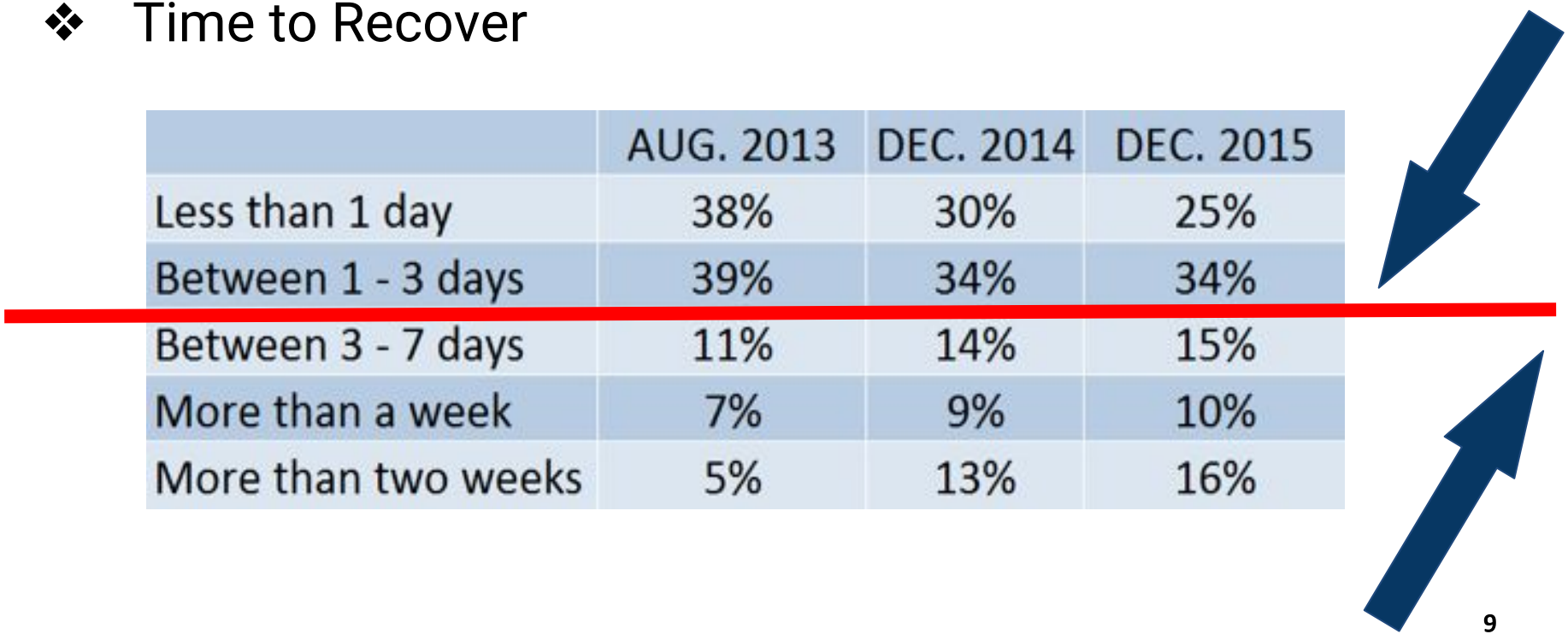
The Reality Continuous - Business Impact

- Reputation Damage
- Loss of Clients
- Ability to Operate
- Loss of Money/Savings

The Reality Continuous - Business Impact

- Time to Recover

	AUG. 2013	DEC. 2014	DEC. 2015
Less than 1 day	38%	30%	25%
Between 1 - 3 days	39%	34%	34%
Between 3 - 7 days	11%	14%	15%
More than a week	7%	9%	10%
More than two weeks	5%	13%	16%



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

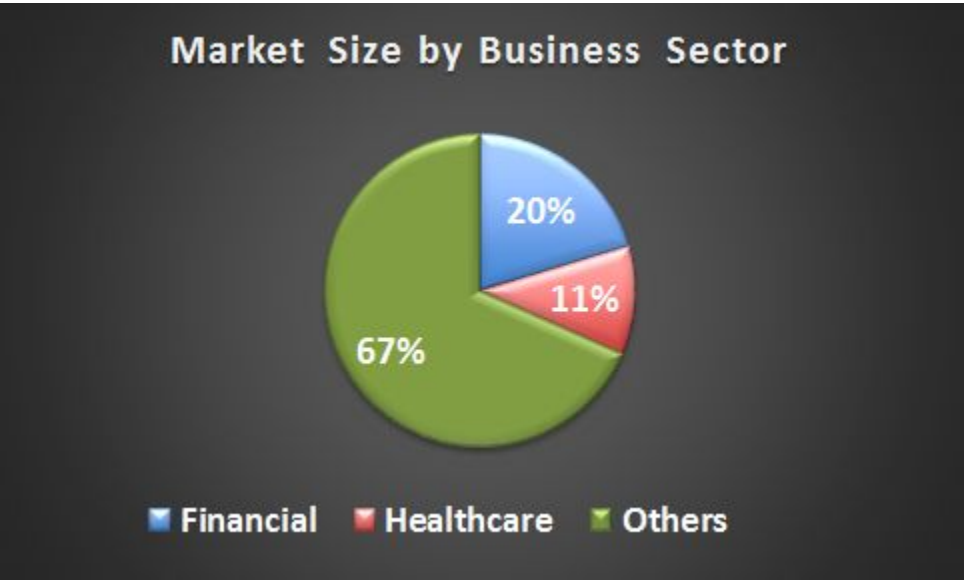
- Complexity of Cyber Risk
  - Difficult for SMEs to fully understand

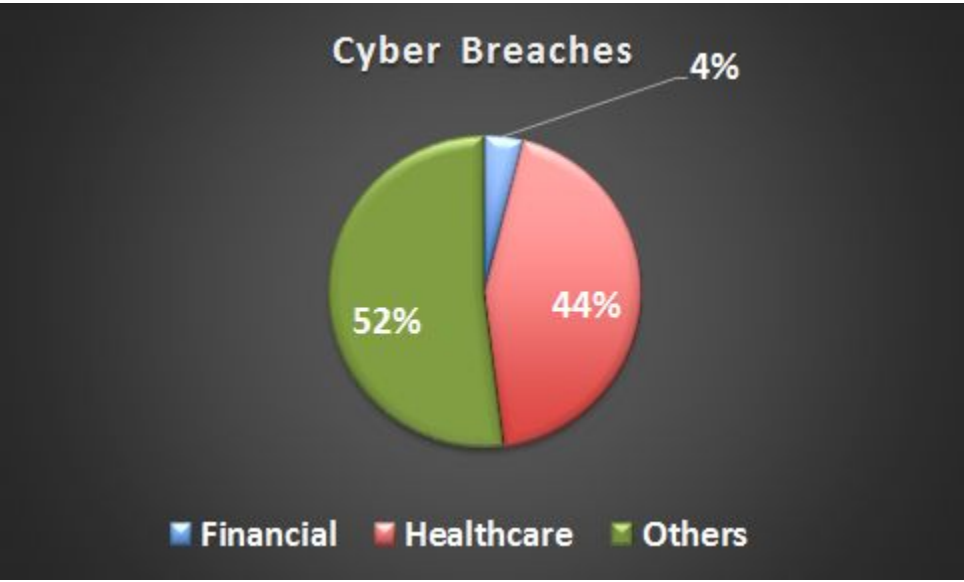
Challenges for SMEs

- 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





Challenges for SMEs

- Countless Cybersecurity Options But No Guidance
  - Antivirus Software
  - Cybersecurity Consultants
  - Cyber Insurance/ Broker

Cyber Insurance

SMEs

Large Businesses

Less than **3%** of SMEs Have Cyber Insurance

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

UCONN
Janet and Mark L. Goldenson Center for Actuarial Research
Illuminating Industry Innovation

Q & A

UCONN
Janet and Mark L. Goldenson Center for Actuarial Research
Illuminating Industry Innovation

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	
Category	Description
Physical Asset Damage	Damage on IT equipment, IT systems and technology.
Business Interruption	Result from denial of services, website offline and employee down time.
State-Sponsored and Terrorists Cyber Attacks	Cyber attacks result from cyber warfare or terrorists.
Theft	Theft of data, ecnomic value of intellectual property, finished goods in provess, extortion, computing recources and deceptive fund transfer.
Business Loss and Client Loss	Data disclosure of personal and business information that result in a business losing its revenue during normal operation.
Recovery of Data and System	The cost to restore data or systems that has been damaged or destoryed.
Forensic Cost	The cost to investigate cyber incidents and notifcation expenses.
Response Cost	The cost to minimize post-incident losses.

Q & A

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