Cyber Threats Faced by Public Entities

Mike Oworth
CPCU, ARM, ASLI
VP & Sr. Unit Manager

Ben Eggert, Esq.
Wiley Rein LLP

GENESIS
Start with Security

NATIONAL CYBER SECURITY AWARENESS MONTH
Local Gov’t Data Breaches

When are we going to be hacked?
Local Gov’t Data Breaches

Reports are EVERYWHERE

Aug 2016: Hackers stole password of local official in Gila County, AZ

Sept 2016: DHS warns Congress that Russian hackers are targeting local election systems
Local Gov’t Data Breaches

But asking “when” is the wrong question.

It already happened.
Local Gov’t Data Breaches

• Data breaches occur every 2-3 months

• On average, local government had 9.4 breaches in the last 2 years
Local Gov’t Data Breaches

How have we been hacked?
Local Gov’t Data Breaches

Top 5 Cybersecurity Vulnerabilities

1. Passwords
2. Access
3. System Locks
4. Data Backups
5. User restrictions/tracking
Policy Framework

- Security
- Privacy
- Data Management and Standardization
- Funding and Investment

NATIONAL CYBER SECURITY AWARENESS MONTH
Technologies - Traditional

- Laptops
- Desktops
- Mobile Devices
- Software
Technologies – Health Care

- Electronic visit verification (GPS)
- Home health monitoring
- Fitness trackers
Technologies - Transportation

• Ports/GPS – charge for miles driven vs. gas tax
• Closed-circuit television for traffic
Technologies – Public Safety

• Next Generation 911
• Dashboard cameras
• Body cameras
• Emergency management
Technologies – Other

- Tourism (bluetooth/wifi)
- Facilities management
- Agricultural management
- Emergency management
Federal vs. State/Local Gov’t

• Recovery
• Prevention
• Detection
• Containment
Federal vs. State/Local Gov’t

- Negligent Insider
- Zero-day attacks
- Third-party mistakes
- Failure to patch
Local Gov’t Challenges

• Personnel
• Politics
• Budget
• Technologies
• Lack of sharing
Local Government Risks

**High Risk**
- Applications
- Data bases
- Mobile devices

**Low(er) Risk**
- Storage devises
- Laptops/desktops
Planning – Cyber Risks

Cyber incident vs. Cyber Disruption
Planning – Cyber Risks

Cyber incident planning

- Impacts
- Targets
- Causes
Planning – Cyber Risks

Cyber disruption planning

Impacts
Targets
Causes
Planning – Threat Intelligence

What is it?
Planning – Threat Intelligence

Why not share?

• Slow & unwieldy
• Lack of resources
• Lack of trust
Planning – Threat Intelligence

- Collaboration
- Situational Awareness
- Improve Security Posture
- Timeliness
- Actionability
Planning – Cyber Analytics

“Cyber Analytics”

What is it?
Questions?
Proprietary Notice & Disclosure

Proprietary Notice
The material contained in this presentation has been prepared solely for informational purposes by Genesis Management and Insurance Services Corporation and Wiley Rein LLP. The material is based on sources believed to be reliable and/or from proprietary data developed by Genesis and Wiley Rein LLP, but neither Genesis nor Wiley Rein LLP represent as to its accuracy or its completeness. The content of this presentation is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Disclosure
Genesis Insurance Company is licensed in the District of Columbia, Puerto Rico and all states. Genesis Insurance Company has its principal place of business in Stamford, CT and operates under NAIC Number 0031-38962