EVERYTHING YOU WANTED TO KNOW ABOUT CYBER RISK
But were afraid to ask!

Rachel Burley, Lead Security Analyst, Diligent
Josh Fruecht, Governance Advisor and Former Clerk, Diligent

Tuesday, October 22
Agenda

• Recent research & common security misconceptions
• Local government examples
• Strategic actions you can implement now
• Asking the right questions
• Next steps
Introductions

Rachel Burley
Lead Security Analyst, Diligent

• Security and compliance professional whose career focus includes enhancing companies’ security posture through governance, risk, and compliance.

• Successfully implemented security-related frameworks for multiple SaaS companies. These frameworks include ISO 27001, NIST Cybersecurity Framework, Service Organization Controls (SOC) and NIST SP 800-53.

• She is a graduate of Wilmington University with a B.S Computer and Network Security and MS Homeland Security – Information Assurance.

• She has earned various security and audit certifications, the most recent being the BSI ISO/IEC 27001:2013 Internal Auditor certification.
Introductions

Josh Fruecht, MPA, CMC
Governance Advisor, Diligent

- Working with and for local governments for over 10 years
- Master of Public Administration from Florida State University
- IIMC Certified Municipal Clerk
- Experienced in guiding people through the ins and outs of making technology projects successful
RECENT RESEARCH & COMMON SECURITY MISCONCEPTIONS
50% of directors around the globe discuss sensitive material via personal channels.
71% of boards use unsecure private emails and pdfs to manage their documents
IT is responsible for risk management

Cybersecurity is something that can be fixed

Management, left to its own devices, will give cyber risks the attention they deserve

Public information, therefore, no need to protect
Early focus on large corporations with a shift towards smaller targets

Early focus
- Banks and large corporations

Shift towards
- Smaller targets are seeing an increase in attacks

Securities and Exchange Commissions issued strong suggestions for boards

Corporate directors are responsible for preventing cyberattacks
Data Breach Investigations Report

The Verizon Data Breach Investigations Report (DBIR) provides crucial perspectives on threats that organizations face.

The DBIR is built on real-world data from over 41,000 security incidents and over 2,000 data breaches provided by 73 data sources, both public and private entities, spanning across 86 countries worldwide.

https://enterprise.verizon.com/resources/reports/dbir2019/public-administration
Cyber Risk by the Numbers

- 2 million
  - Number of cyberattacks reported in 2018

- $45 billion
  - Total cost of losses from cyber incidents in 2018

- 12% rise
  - Business targeted ransomware

- $6 trillion
  - Annual cost of cyber crime damages by 2021

- 1 in every 131
  - Emails is malicious

- 95%
  - Cyber attacks could be prevented by updating software & training

Check out “Have I Been Pwned?”
haveibeenpwned.com

Online Trust Alliance Annual Cyber Security Report, 2018
How much is your personal data worth to hackers

The NY Post discloses how much your stolen information is worth

- **Email password details**: $2.29
- **Netflix password details**: $3.05
- **Drivers License details**: $20
- **Credit card details**: $22.39
- **Medical record**: $1,000
LOCAL GOVERNMENT EXAMPLES
Recent local government examples

**Atlanta, GA**
- Government data and systems
- $51,000 bitcoin
- $2.7M (June 2018)

**Baltimore, MD**
- 911 Dispatch hacked
- IT staff restored system

**Brookhaven, NY**
- 76 government sites
- Content changed to ISIS propaganda

**Colorado**
- SamSam ransomware infection
- 2,000+ systems offline
- $2M Cost
SamSam Ransom Payments

SamSam ransom Payments - Total: $5.9 Million USD
January 12th 2016 - July 21st 2018

Source: Sophos
STRATEGIC ACTIONS YOU CAN IMPLEMENT NOW
Building a Cyber Security Program

1. Identify
   1. Systems
   2. People
   3. Assets
   4. Data
   5. Capabilities

2. Protect
3. Detect
4. Respond
5. Recover

Security Breach Response Plan

The National Institute of Standards and Technology (NIST) developed five functions of the NIST cybersecurity network that serve as the pillars for a comprehensive and successful cybersecurity program. With these components in mind, local governments can follow these tips for building an effective security breach response plan.

1. IDENTIFY
   Nail down the varying ways in which your local government could be impacted if a group or individual successfully hacked into your systems. This allows you to prioritize your efforts while developing an identified risk management strategy.

2. PROTECT
   Align data security practices to your local government’s risk management strategy so that all local government staff are properly educated on their roles in cybersecurity. This ensures that access to information will be protected and kept confidential.

3. DETECT
   Implement systems that will identify anomalies and unusual events so that you can best determine the potential impact they could have. These systems will help your local government better identify the occurrence of a security breach at the earliest opportunity.

4. RESPOND
   Establish a plan to respond appropriately to a cybersecurity incident quickly and with tact. Preparing a response plan ahead of time minimizes damages and keeps employees and the community informed and up-to-date.

5. RECOVER
   Despite efforts to prevent any damages, local governments will inevitably face some negative aftermath following a security breach. Recovery activities should be aimed at the goal of restoring the government’s operations to normalcy as soon as possible to reduce the overall impact of the breach.

#ICMA2019
STEP #1: Identify

The first step in creating a cyber security response program is to identify the key areas that need to be protected. It’s important to look at the following areas:

• Systems
• People
• Assets
• Data
• Capabilities

The identification step allows local governments to prioritize their efforts while aligning them with their risk management strategies.
STEP #2: Protect

Ensure the local government will be able to defend critical infrastructure services by protecting physical and remote access to information that local governments retain.

Protecting information entails creating training and awareness of local government staff on their roles in cybersecurity.

Implement information protection processes and procedures to manage and maintain information systems and assets. Processes that are designed to protect the government’s information should include remote maintenance.

Local governments need to ensure that activities in the protection step are consistent with the government’s organizational policies, procedures and agreements.
STEP #3: Detect

Identify the occurrence of a security breach event at the earliest opportunity.

This step requires having systems in place to identify anomalies and unusual events and to understand their potential impact.

Local governments need to have a process in place to continuously monitor cybersecurity events and verify the effectiveness of their protective measures.
STEP #4: Respond

Establish a plan to respond appropriately to a cybersecurity incident in a timely manner.

Responding quickly and completely will minimizing damage and keeping employees and the community informed. One of the most important activities involved in this step is managing communications with law enforcement and the public, which requires a detailed plan.

Local governments can continually improve this step by staying current with emerging breaches that affect other governments and learning from any lessons gained from the detection step.
STEP #5: Recover

Identify and implement activities to restore damage or other issues caused by a security breach. Activities should be designed to restore the government’s operations to normalcy at the earliest opportunity, which will reduce the overall impact of the breach.

The recovery step is also the time to implement the communications plans that the government identified in Step #4, the Response step.

Once the security breach response plan has been formed, it’s important for local governments to remain current with new developments and to review their plans at least annually to ensure effectiveness.

The five-step plan is the most viable way to ensure that local governments are doing their due diligence in protecting their communities from a security breach.
Amazing City is a small city with a population of 200,000 people. The city has become victim to a ransomware attack. Reported issues resulting from the ransomware attack include: Corporate email is down, Traffic tickets cannot be paid, and real-estate transitions cannot be processed.

Group Action: In your group think of 3-5 steps that should be completed based on the cyber security response program step assigned to your group. (Steps 1 through 5)

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover
Practices You Can Implement Now

➤ Understanding the legal implications of data comprise
➤ Internal audit
➤ Investing in a highly secure transparency portal that support good governance principles
➤ Applying tools discussed today
➤ Getting cyber insurance
➤ Continuously training staff
ASKING THE RIGHT QUESTIONS
Asking the right questions

• How are we protecting citizen/operational data?
• What are the biggest vulnerabilities & how are we preparing (e.g., planning, training, cyber risk insurance, other)?
• Does your current insurance policy cover cyber incidents? What exclusions do you have?
• How are incidents handled? Cooperative vs. Hands off?
• How do we know our security/privacy program works?
• How is compliance applied – every three years, quarterly, other?
NEXT STEPS
Next steps

• Have a conversation at the board/council table

• Clear picture of what it would take to ensure security practices are followed in your organization

• Contact us to learn more about how our software can fit into your cyber risk program
THANK YOU

Questions?

Community
BY DILIGENT

ICMA | conference