NASC: Staying Secure When Transforming To A Digital Government
Branson (MO), March 2020
Speaker Introduction

Rajiv Das
Principal
Plante Moran Management Consulting
Cybersecurity Practice
Email: Rajiv.Das@plantemoran.com
Phone: 517-898-2033
Security in the Public Sector
What makes the public sector an attractive target?

- Security is not often a top (or well-funded) priority
- Governments maintain valuable and sensitive citizen information
- Attacks have been successful
Current Breach Events

- At least 87 million records breached
  - Date disclosed: March 17, 2018

- 37 million records breached
  - Date disclosed: April 2, 2018

- Date Disclosed: November 30, 2018
  - Massive data breach affecting up to 500 million guests

- Date disclosed: March 22, 2018
  - Emergency contracts worth $2.7 million to help restore the city’s computer network

List continues .......
Understanding the Why

• 76% of breaches were financially motivated
• Most cybercriminals are motivated by cold, hard cash. If there is a way they can make money from you, they will.
• Most attacks are opportunistic and do not target the wealthy or famous. They target the unprepared.
• Almost three-quarters (73%) of cyberattacks were perpetrated by outsiders. Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12%.
• Over a quarter (28%) of attacks involved insiders. The insider threat can be particularly difficult to guard against—it is difficult to spot the signs when someone is using their legitimate access to data for nefarious purposes.
Understanding of the Numbers

Causes of incidents, 2018

- Hack or malware: 47%
- Accidental disclosure: 20%
- Insider: 10%
- Social engineering: 8%
- Portable device: 6%
- Physical loss/non-electronic record: 5%
- Unknown/other: 3%
- Payment card fraud: 1%
IT Risks in the Public Sector

88% of IT operations teams are at least partially responsible for data breaches or security incidents in the Public Sector.

75% of organizations in the Public Sector do not have a separate information security function.

33% of organizations in the Public Sector had compliance issues in 2016.

As per Security Scorecard Research Report 2017: Public Sector received one of the lowest security scores, when compared to 17 other major industries.
Data Compromised in the Public Sector

- Personal Data, 41%
- Confidential Data, 41%
- Credentials, 14%
- Medical Data, 9%
A Few More Facts

• The odds of a data breach today are 1 in 4, with a 27 percent probability that an organization will experience a data breach over a two-year period.
• The average total cost of a data breach was $3.86 million, up 6.4 percent from last year, and the average total loss for a stolen record was $148, up 4.8 percent from last year.
• In the United States alone, the average total cost of a data breach was $7.9 million, up 7 percent from 2017, and the average cost of a stolen record was $233, up 3 percent.
• For public sector organizations, specifically, the total average cost of a data breach was $2.3 million, with an average cost of $75 per record.
• The risk factors increasing the chances of data breaches were third-party involvement, compliance failure and extensive cloud mitigation.
Early Detection Is A Must

**DETECTION AND INCIDENT RESPONSE**

- **77%**
  - Of 2,800 IT professionals in a survey said their organizations do not have a formal cybersecurity incident response plan.

- **66 DAYS**
  - The average time needed to fully contain a data breach in 2017.

- **191 DAYS**
  - The average length of time it takes for organizations to identify a data breach.
Public Sector Cyber Threats
Public Sector Cyber Threats

- Insider and Privilege Misuse
- Cyber Espionage
- Malware Attacks
- Malicious Insider
- Point of Sale Intrusion
- Social Error
- Trojan
- Ransomware
- Spyware
- Web Application Attacks
- Virus
- Denial of Service
- Human Error
- Lost and Stolen Asset
- Phishing
- Payment Card Skimmers
Top 5 Cyber Threats

- Misuse (52%)
- Phishing (49%)
- Malware (47%)
- Spam (42%)
- Data leakage (39%)
Phishing

Phishing is a process of contacting a person through an email message or a call where the receiver is tricked into leaking sensitive data such as personal identifiable information.

9.23% of people in Public Sector have clicked on phishing emails.

4% of people will click on any given phishing campaign.

Malicious payloads are commonly delivered via:

- 13% Drive-by-download
- 73% Email

As per the Verizon DBIR 2018

91% of cyber attacks start with a Phishing email.

You have 16 minutes until the first click on a phishing campaign. The first report from a savvy user will arrive after 28 minutes.
Phishing Attack Example

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/smartphone/network.

9. The hacker uses the backdoor to steal information.
Ransomware

- Ransomware is a malware that works by encrypting information and then demanding ransom to decrypt it.
- Public Sector is one major target of ransomware attacks because of the large volumes of citizen’s sensitive information.

5.9% of Public Sector entities were hit by ransomware attacks in 2016. Making the Public Sector the second highest hit rate of ransomware attacks after Education.

21,239 Total number of security incidents in Public Sector in 2016.

Source: Verizon DBIR 2017, Bitsight Insights
“Facebook scams (social engineering), Trojans, and iFrames remain popular tools for gaining initial access to users’ computers and organizational networks.”

Source: CISCO Mid Year Security Report
Information Security Foundation
Information Security Foundation

- IT Governance, Policy and Operational Monitoring
- Protecting Information
- Information Storage and Backup
- Information Retention and Destruction
Information Security Foundation

- Protecting limited disclosure and sensitive information
- Clear Desk / Clear Screen
- Locking / Logging off your workstation
Disaster Recovery Plan

• Structured and documented approach for responding to unplanned incidents
• Step-by-step plan that minimizes the effects of a disaster
• Typically, disaster recovery planning involves analysis of business processes and continuity needs
• Disaster Recovery Plan checklist
Password Policy

• Keep passwords confidential
• Use a pass phrase
• Remember to change your password
Email (and Internet) Usage Policy

• Internet access for business use
• Email awareness
To Sum it All Up

• Prepare. Take time to assess business risks, and know the locations of sensitive data.
• Pay attention to third parties. Understand how vendors use data and ensure they are being as careful as necessary.
• Practice good cyber hygiene. Upgrade and patch software when required.
To Sum it All Up

• Monitor logs. But also determine and select events that are “suspicious and actionable.”

• Encrypt data. Avoid data loss with encryption.

• Train users. Persuade users to do the right thing, and pay attention to insider threats.

• Share stories. Put cyber-risks in terms that shareholders understand.
To Sum it All Up

• Adequate rights. Limit access to the people who need it to do their jobs, and have processes in place to revoke it when they change roles.

• Encrypt sensitive data. By encrypting your data you can render it useless if it is stolen (e.g. Use two-factor authentication).
How can we help you?

**Cyber governance**
- NIST Cybersecurity Standards
- COSO/COBIT Standards
- SAS Top 20 Security Controls
- Security awareness
- Cyber incident response planning
- BCP/DRP
- 7-point cyber assessment

**IT audits**
- General controls review (access, physical, operational controls)
- Application controls assessment (SAP, Oracle, PeopleSoft, QAD, Plex, Epicor)
- User access reviews
- ERP security & controls
- Pre/Post-implementation controls review

**Security compliance**
- Sarbanes-Oxley
- PCI DSS
- HITRUST
- ISO27001 Security Standards
- Financial services regulations (FTIEC, BSA, NACHA, etc.)
- Privacy regulations (HIPAA/HITECH, GLBA, FERPA, GDPR, etc.)

**Cyber risk assessments**
- Data & application mapping
- Vendor management
- Threat analysis
- Controls mapping
- Maturity models
- Risk-based IT audit planning
- Cybersecurity program

**Attack & pen**
- External penetration testing
- Infrastructure security assessment
- Vulnerability assessment services
- Social engineering tests
- Web application security
- Database security
- Wireless security
- Virtualization security
- Cloud computing security
- Mobile device security

**SOC examinations**
- Readiness assessment
- SOC 1
- SOC 2
- SOC 3
- SOC for cybersecurity
- Privacy reviews
Thank you!

“Awareness is the greatest agent for change.”
— Eckhart Tolle

Rajiv Das
517-898-2033
Rajiv.Das@plantemoran.com