December 19, 2018

Staying Secure When Transforming To A Digital Government

Speaker Introduction

Alex Brown
Principal

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

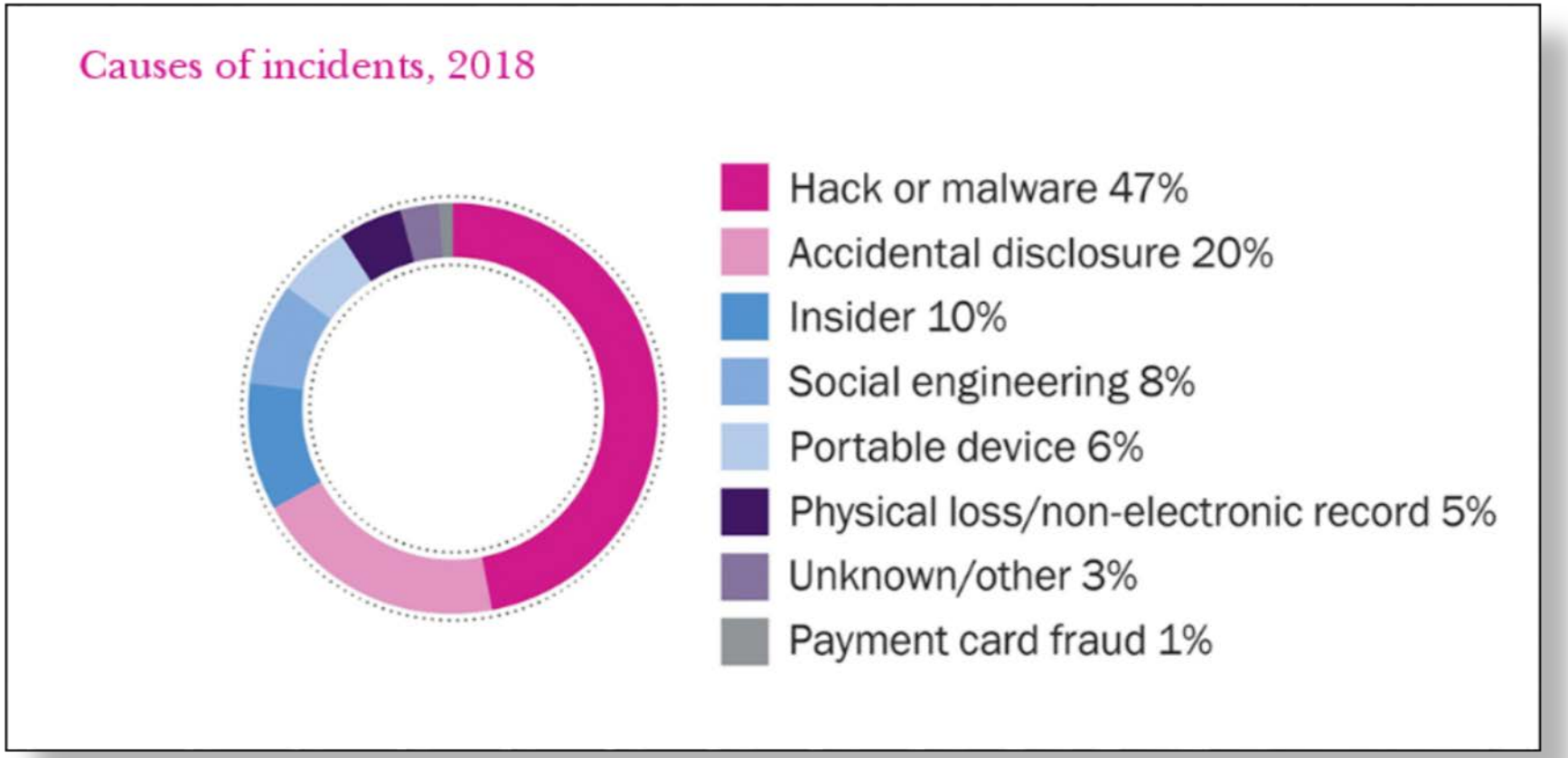
- Date Disclosed: November 30, 2018
- Massive data breach affecting up to 500 million guests

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

Understanding the Why

- 76% of breaches were financially motivated
- Most cybercriminals are motivated by cold, hard cash. If there's some way they can make money out of you, they will..
- Most attacks are opportunistic and target not the wealthy or famous, *but 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's hard to spot the signs if someone is using their legitimate access to data for nefarious purposes.

Understanding of the Numbers



IT Risks in the Public Sector

88%

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

75%

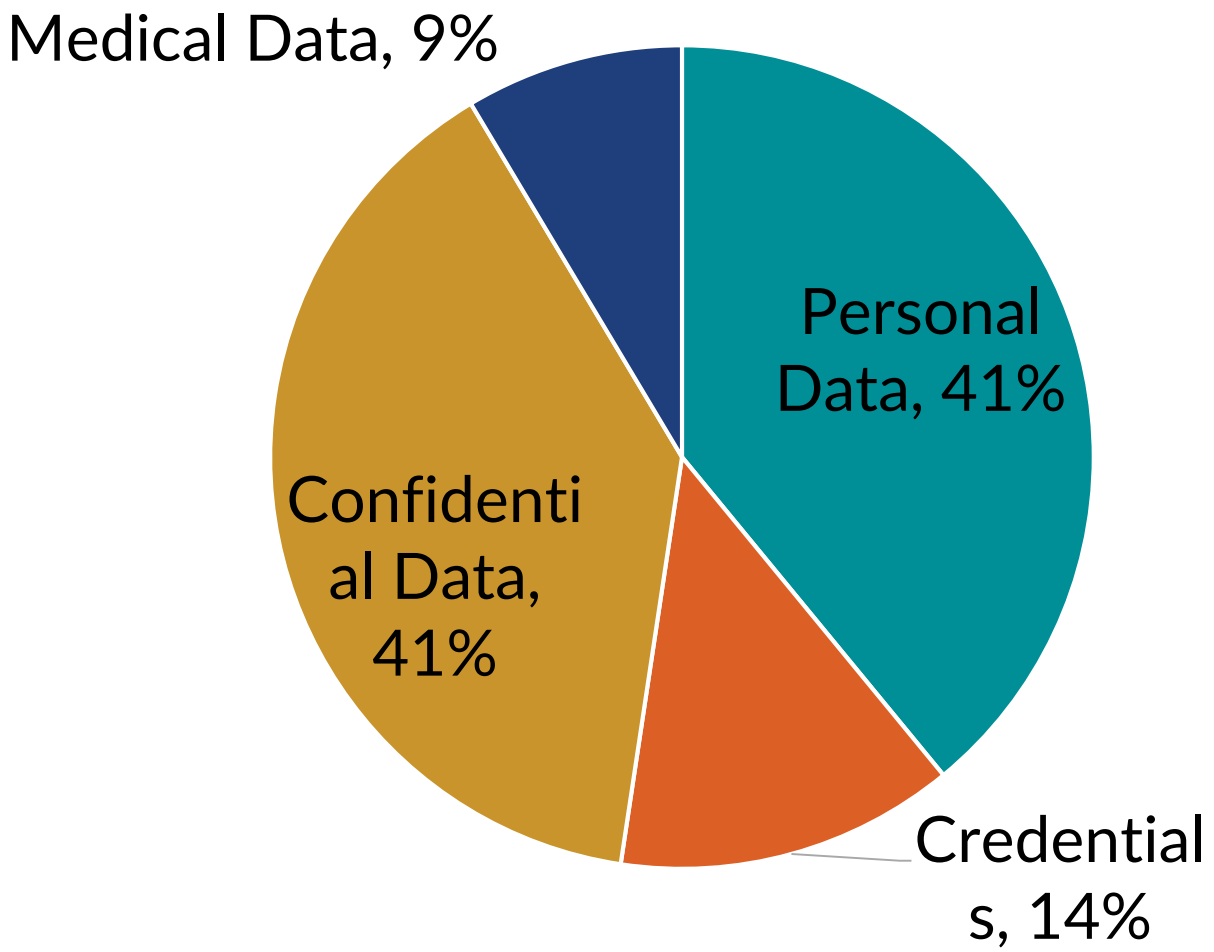
of organizations in Public Sector do not have any separate information security function.

33%

of organizations in 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.

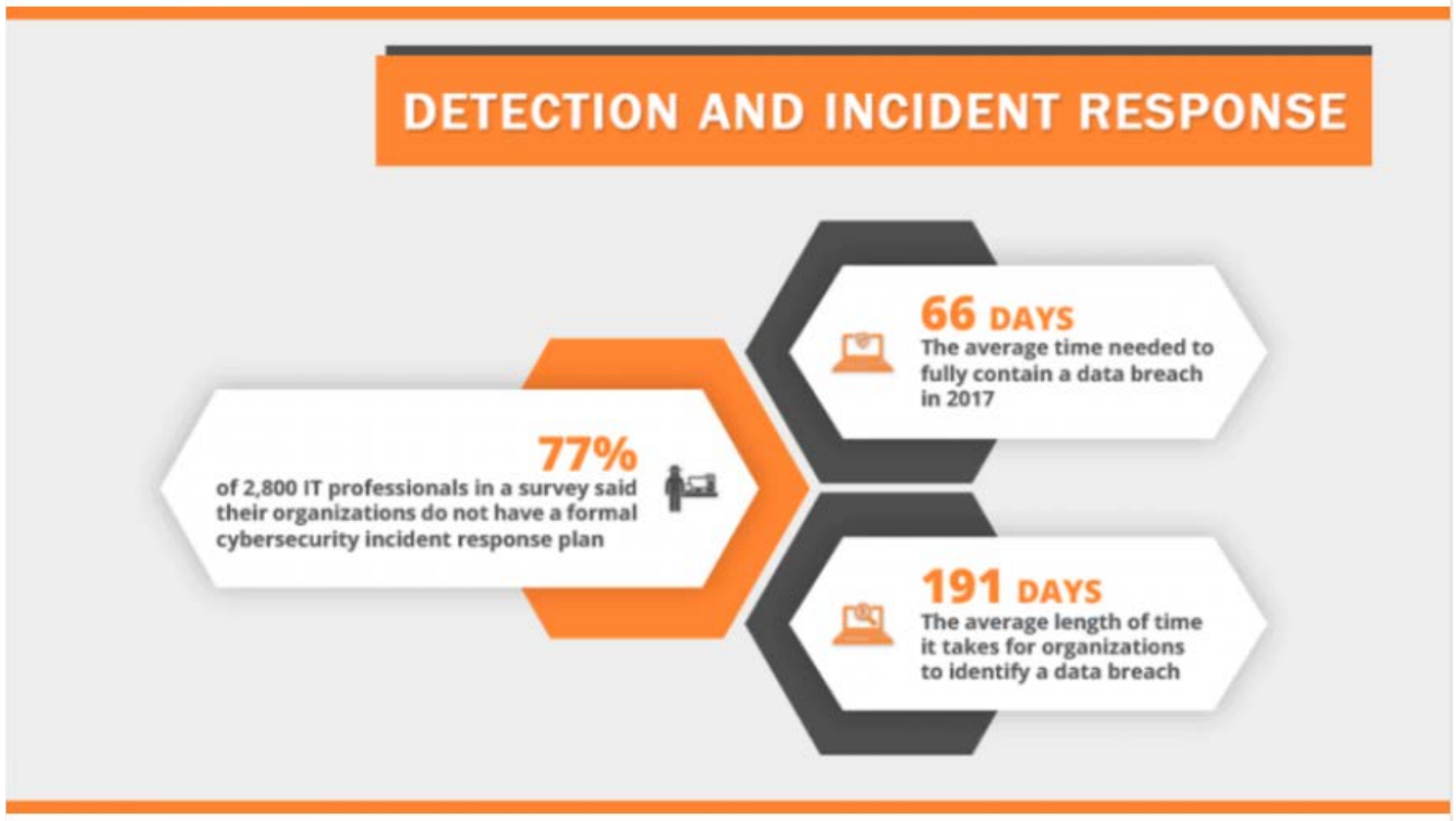
Data Compromised in the Public Sector



A Few More Facts

- The odds of a data breach today is **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



Public Sector Cyber Threats

Public Sector Cyber Threats

Cyber Espionage

Point of Sale Intrusion

Insider and Privilege Misuse

Malware Attacks

Virus

Lost and Stolen Asset

Social Error

Phishing

Trojan

Web Application Attacks

Ransomware

Payment Card Skimmers

Malicious Insider

Denial of Service

Human Error

Spyware

Top 5 Cyber Threats

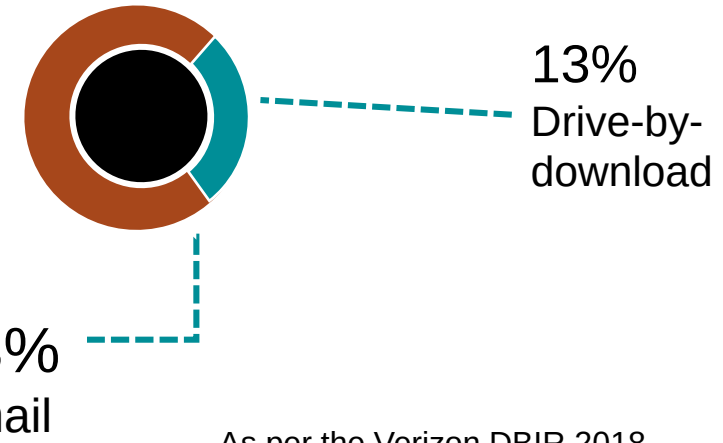
Phishing

Phishing is a process of contacting a person through email, message or call where the receiver is tricked to leak sensitive data such as personally 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:

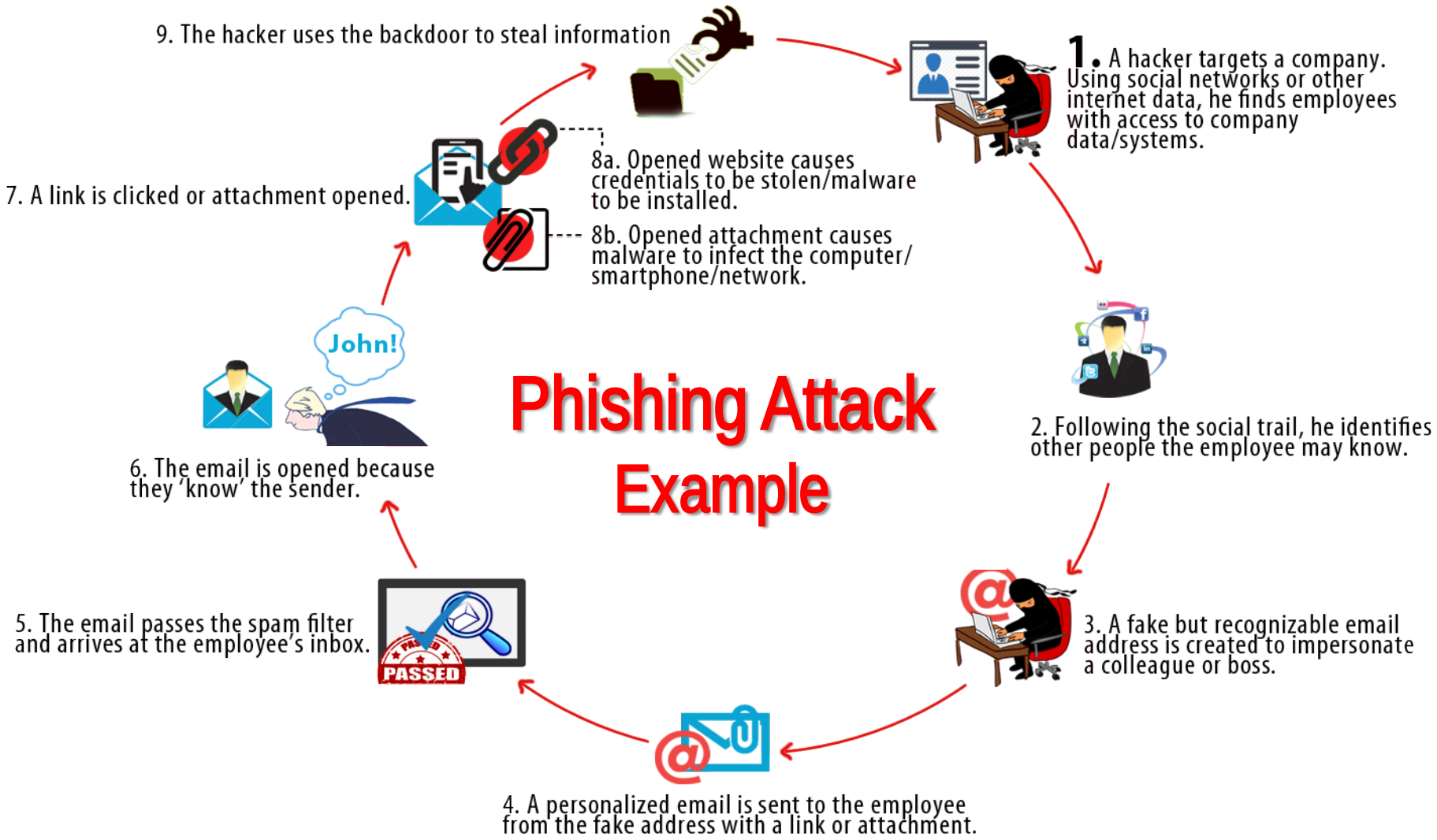


As per the Verizon DBIR 2018

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



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.

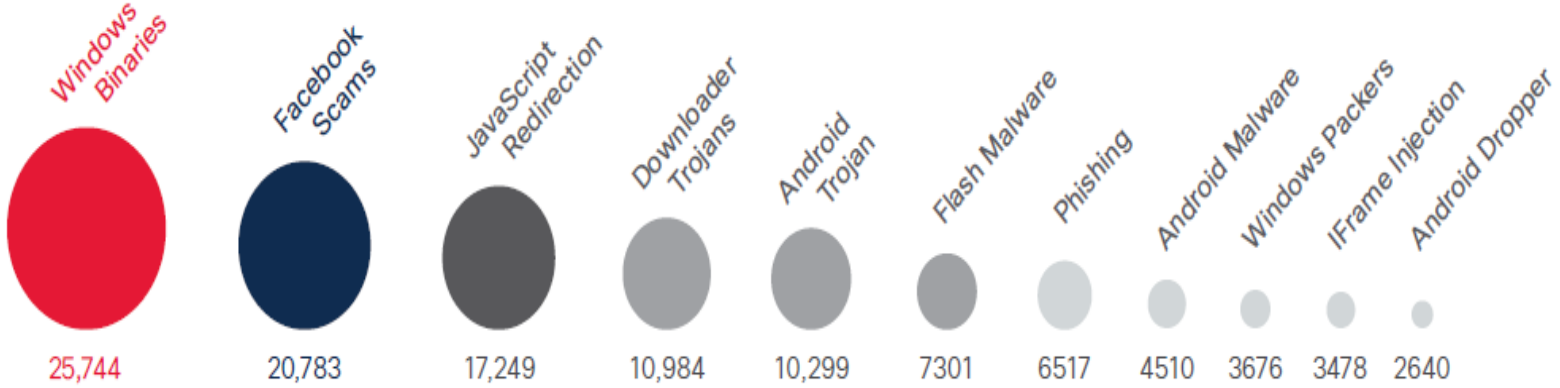
5.9% of Public Sector entities were hit by ransomware attacks in 2016. Making the Public Sector the second highest hit rate of ransomware attacks after Education.

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

Source: Verizon DBIR 2017, Bitsight Insights

Malware

“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 and Policy
- 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 cyberhygiene. 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
- SANs 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 (FFIEC, 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


Questions?

Thank you!

"Awareness is the greatest agent for change."
— Eckhart Tolle

F. Alex Brown
248-223-3396
furney.brown@plantemoran.com