Central Florida Chapter

Florida Government Finance Officers Association

Florida
Government
Finance
Officers
Association

Staying Secure when Transforming to a Digital Government

plante moran

audit • tax • consulting

Agenda

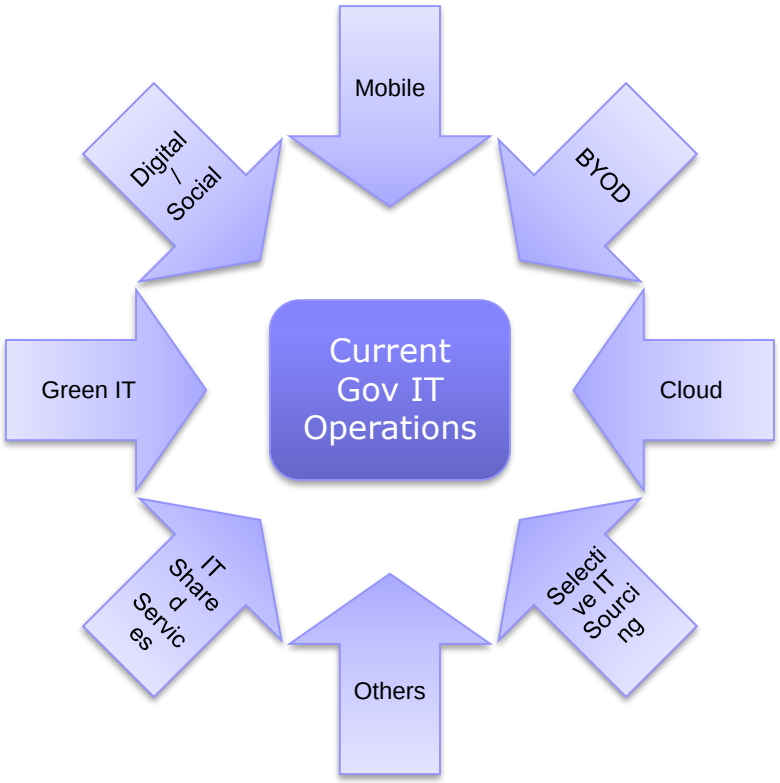
- Plante Moran Introductions
- Technology Pressures and Challenges Facing Government
- Technology Risks and Mitigation Strategies
- Technology Cost Considerations
- Technology Best Practices
- Questions

Alex Brown

- Over 20 years of experience in management and technology consulting
- In depth experience in the assessment of technology risk and evaluation of IT controls associated application security assessments and security within technology driven business processes
- Serviced a wide range of clients and industries including municipalities and special districts

Technology Pressures Facing Local Government

- External influences will impact your future direction as much as or more than maintaining the existing environment
- Will drive future technology policy, planning, investments and ***RISK***
- Not every IT "buzzword" should be immediately actionable

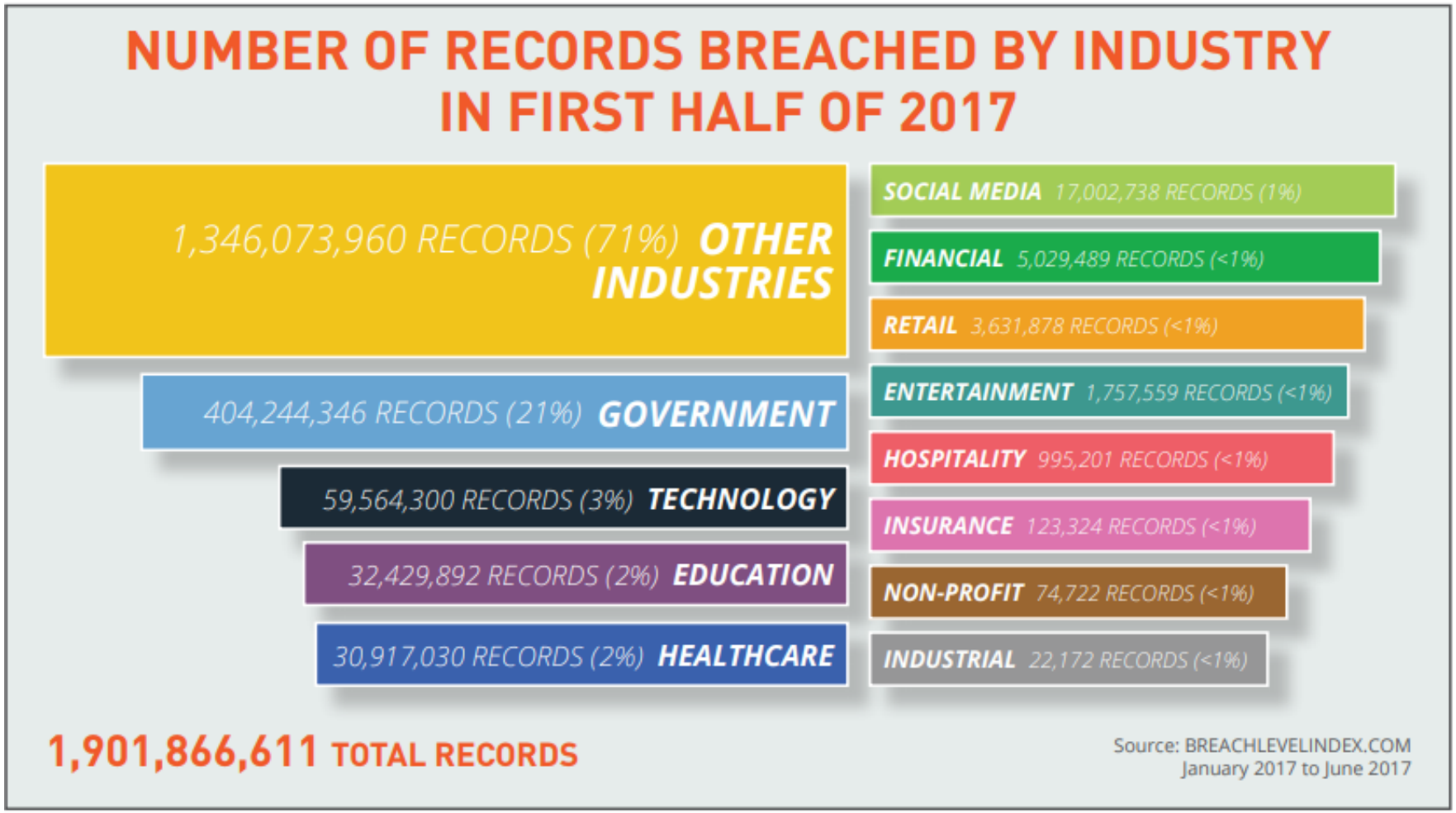


Technology Challenges Facing Government

- Security and Data Breaches
- Insufficient staffing / skill-gap
- Budget constraints
- Lack of IT governance
- Competing project priorities
- Outdated infrastructure
- Aging software systems
- Accountability to citizens
- Slow changes due to bureaucracy
- Lack of reporting and transparency capabilities

Security Breaches

Data Breaches by Industry



Cost of Data Breach

Data breach hits organizations squarely in the wallet. The average cost per record goes up depending on who or what caused the exposure.

Other 'Costs' of Data Breach

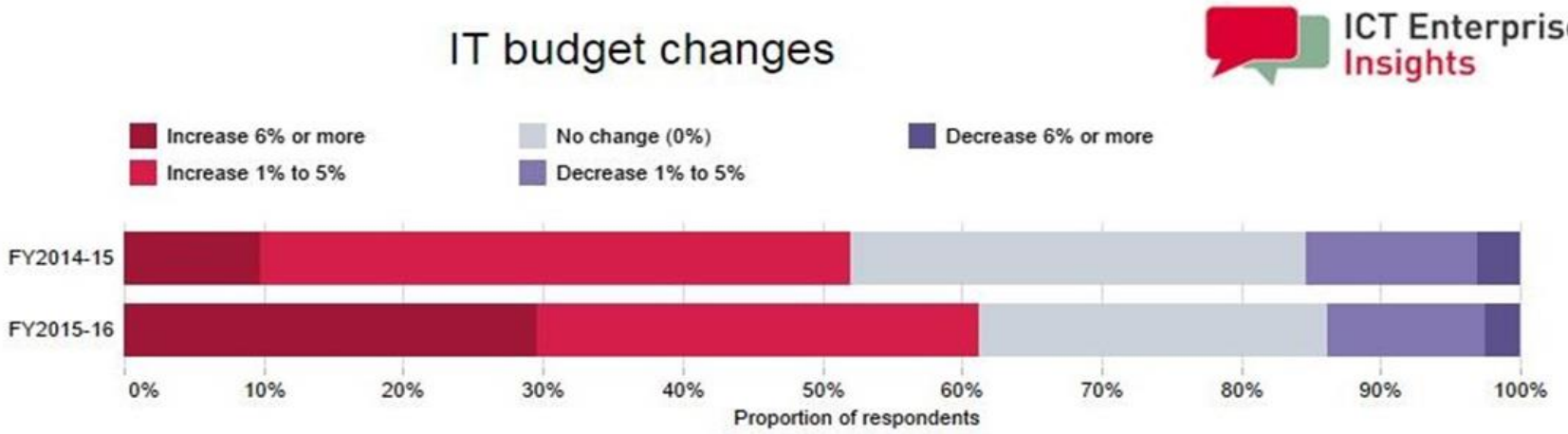
- Reputation damage / negative publicity
- Lost / compromised data
- Lost productivity
- Potential further affects on clients (e.g. identify theft)

Technical Staffing Challenge
Cybersecurity Skills Gap

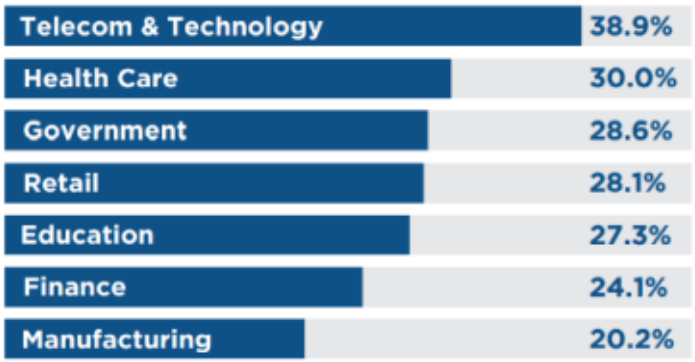
- **2 Million** – Global Shortage of Cybersecurity Professionals by 2019
- **84%** – Organizations believe half or fewer of Applicants for open security jobs are qualified
- **53%** – of organizations experience delays as long as 6 months to find qualified security candidates

Source: Seefit.com

IT Security Spending

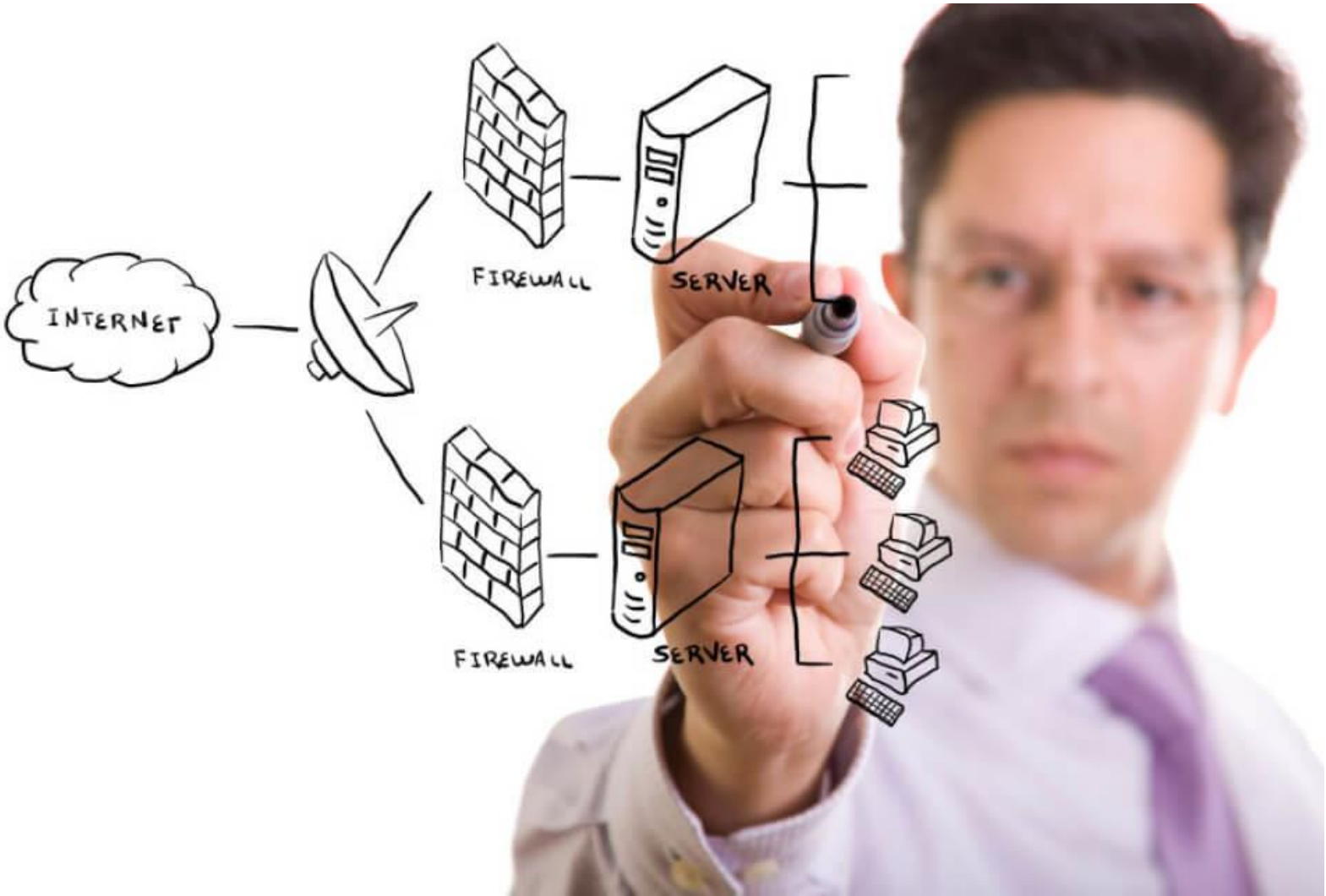


Source: Ovum



Percentage spending 16% or more on security

Planning for Security



IT Governance

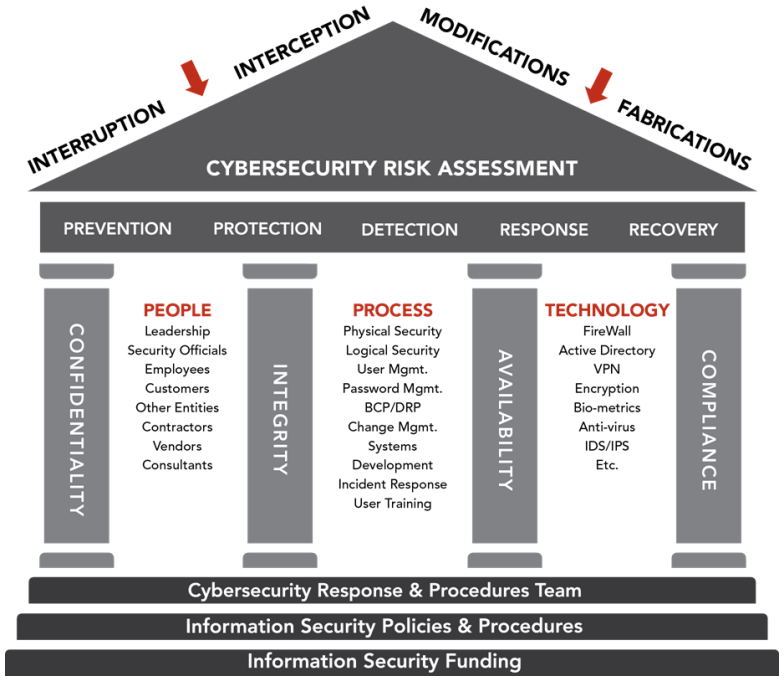
Identify Risk and Understand Risk

- Understanding risk helps to:
  - Identify areas of security weakness and gaps
  - Prioritize and coordinate IT security activities.
  - Budget for security services and IT hardware/devices
  - Determine technical skills required to support current and future operations
  - Comply with regulatory requirements
  - Identify resources commitments required security projects and engagements

Identify Risk and Understand Risk (Continued)

- Develop risk management procedure
  - Identify and prioritize risks
  - Perform periodic risk assessments
  - Develop risk mitigation / contingency plan
  - Implement risk mitigation plan
  - Monitor progress

IT Governance Structure



Establish a Strong IT Governance Structure

- Policy Administration
- Procedures and Guides
- Security Compliance
- Training
- Project Administration
- Change Administration
- Strategic Planning
- Annual technology budgeting
- Project portfolio management

Aligning IT Policy with Strategy

- **Keep policy current**
  - Who makes IT policy?
  - Who identifies policy requirements prior to a project?
- **IT policy building blocks**
  - Disaster Recovery Plan
  - Password Policy
  - Email Usage Policy
  - Change Management Policy
  - Infrastructure Refresh Policy
  - Patch Management Policy

Example IT Policies

IT Governance Area	IT Policy
Access Management	■ Password Policy
	■ Email Usage Policy
	■ Computer and Internet Usage Policy/Acceptable Use Policy
	■ Social Media Policy
	■ Acceptable Use Policy
	■ Remote Access Policy
	■ Mobile and Personal Device Policy
	■ User Access Policy

IT Governance Area	IT Policy
IT Operations	■ Portable Storage Policy
	■ Data Management and Retention Policy
	■ Data Back-up Policy
	■ Compliance Policy
	■ Performance Metrics
	■ IT Asset Management Policy
	■ Help Desk Policy
	■ Security Penetration Testing Policy
	■ Disaster Recovery Plan
	■ Infrastructure Refresh Policy
	■ Change Management Policy
	■ Patch Management Policy

Vendor Management

Third-party vendor relationships can create additional risks to your organization. Best practices to manage third-party vendors:

- Conduct third-party screening, onboarding, and due diligence during RFP process
- Establish a tone at the top with management-level oversight
- Ensure appropriate investment and staffing
- Align vendor IT security plan with organization

Data Protection

IT Security Planning

- **Protecting Information**
  - You are the first and best defense in protecting applications and data information
  - Be mindful of where information “lives” and how it can be protected
  - Don’t be tricked into divulging sensitive information (e.g. Passwords, financial data, future projects, vendor information)
- **Security Awareness and Training**
  - Important information should be stored on network drives (e.g. U, Y, etc.) which should be included in the back up of network data
- **Information Retention and Destruction**
  - Identify and define requirements for electronic data retention and disposal

IT Security Planning

- **Information Storage and Backup**
  - Establish data classification standards. (e.g. Public, Public restricted, Internal Use Only, Restricted Access)
  - Establish storage locations where critical or Important information should be stored. (e.g. on network drives
- **Information Retention and Destruction**
  - Establish requirements for data retention and disposal requirements.

IT Security Planning

- **Educate employees**
  - Conduct regular user security trainings to help employee aware of security threats and to avoid common malware pitfalls (e.g. malware infection through email attachments, downloads, and web browsing
- **Restrict administrative and system access**
  - Limit the number of user accounts to staff roles and responsibilities
  - Remove all default system administrator accounts

IT Security Planning

- **Conduct Regular Backups**
  - Conduct regular backups of your system and store the backups offline and preferably offsite so that they cannot be accessed through your network
- **Separate Backup System**
  - Backups should be stored on a separate system that cannot be accessed from a network and updated regularly to ensure that a system can be effectively restored after an attack.

IT Security Planning

- **Maintain and update software**
  - Maintain and update software to protect against and/or ensuring early detection of ransomware
- **Use Strong Passwords**
  - Do not use the same password for everything.
  - Do not use easy-to-guess passwords. Use strong passwords that are at least twelve characters in length and include capitals, numbers, and alternate characters.
  - Be paranoid and change your passwords often.

Password Policy

- **A good method for creating strong passwords is to use a pass phrase, and change certain characters. Examples (please don't use these):**
  - I8p@mFR! – I ate pizza at my favorite restaurant
  - Msi6&pP0 – My son is 6 and plays piano
- **Industry minimum password standard include:**
  - Password Change: Every 60 – 90 day
  - Password History: Last 12 Passwords Restricted
  - Password Length: 12 Characters
  - Password Complexity: Enables
  - Password Characteristics: Upper, Lower, Special Character required
- **It is best to have different user names and passwords for work and personal (home) use**

Information Security Basics

- **Protecting limited disclosure and sensitive information**
  - Do not release or provide access to limited disclosure or sensitive information unless security requirements are met
  - Be careful when using office systems including printing, faxing and mail
- **Clear Desk / Clear Screen**
  - Be sure information is properly secured during non-working hours or when you're away from your desk
- **Locking / logging off your workstation**
  - If you are going to be away from your desk or leaving for the day, you should either log off your workstation or "lock" the screen with a password protected screen saver

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 includes:**
  - Definition of what constitutes a ‘disaster’
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
  - Identify most serious threats and vulnerabilities
  - Disaster recovery strategies
  - Response team roles and responsibilities

Email (and Internet) Usage Policy

- **Internet access is intended for business use and is monitored**
- **Email should be treated as public communications**
  - Email is sent over the Internet in clear text (meaning messages can be read in transit if it is being monitored)
- **SPAM**
  - Establish an email location to forward unwanted messages to a define location SubmitSPAM@example.us
- **Email attachments**
  - You should be very cautious about opening any attachment
  - If you don't know the sender or were not expecting the attachment, do not open it as it may contain viruses, spyware or other malicious software

Security Incidents and Reporting

- **Security incidents can happen at any time – common examples include:**
  - Information is missing or damaged
  - Information is disclosed to an unauthorized individual
  - Equipment is stolen
  - Your computer is infected with a virus
- **When possible, write down what you are observing and report as soon as possible**
- **Important – do not try to investigate or resolve the incident yourself – contact your security liaison or IT department as soon as possible**


Q&A

Furney (Alex) Brown
248 223-3396
Furney.Brown@Plantemoran.com