Agenda

• Introduction and General Overview
• 2018 Cyber Trends
• Your Assets, Your Threats, Your Vulnerabilities
• Cybersecurity Risk Management
• Vendor Management
• Cyber Insurance
2018 Cyber Trends
Types of Cyber Attacks

Source: Ponemon Report - 2017
Data at Risk

Source: Ponemon Report - 2017
Root Cause of Cyber Attacks

Source: Ponemon Report - 2017
Small & Medium Business Cyber Security Attack Statistics

- 60% of SMBs go out of business within 6 months of a cyber attack.
- 61% of SMBs were victims of a cyber attack, with 48% of these a result of phishing or social engineering.
- 52% of SMBs experience a ransomware attack (up from 2% in 2016).
- 54% of respondents had data breaches involving customer and employee information in the past 12 months.
- SMBs are losing more records in a data breach (9,350 in 2017 vs. 5,079 in 2016).
- 68% of SMBs do not strictly enforce or are unsure if they enforce password policies.

Source: Ponemon Report - 2017
Cyber Stats

- Companies spent an average of $1,027,053 because of damage or theft of IT assets.
- Disruption to normal operations cost an average of $1,207,965.
- By 2019, the global cost of data breaches is projected to exceed $2 trillion annually.
How Can You Minimize Being a Statistic?

• What are your assets?
• What are your threats?
• What are your vulnerabilities?
Your Assets

• What are your “crown jewels”? 
• What are you trying to protect? 
• What differentiates your business / products / services from that of your competitors? 
• What do you have to protect by law?
Your Threats

• People
  – This is your single largest, most pervasive threat.

• Technology

• Environmental Factors
Your Vulnerabilities

- Ineffective access management
- Unsecured communications
- Poor coding and configuration practices
- Poor security training and awareness
The Compliance Roadmap

- What assets are you trying, or required, to protect?
- What processes do you, should you, or are you required to follow?
- Where are you doing business?
- Where is your data held, stored, transmitted or processed?
Mapping Your Course

• What federal, state, and international laws apply to your business?

• What risks do you face?

• What is your company’s risk tolerance?

• What is the value of mitigating your risks?
Why Should Your Not for Profit Organization be Concerned?

• “High value” donor, client, and employee data that hackers would love to intercept.
• Inadequate internal controls or securities in place.
• What game plan to employ?
  – Identify all systems and data used.
  – Apply multiple layers of defense (i.e. technical controls and user training).
User Education and Awareness

- Acceptable Use Policy / Agreement
- Security awareness and policy training
  - Secure Password Construction
  - Phishing
  - Whaling Attack
  - Social Engineering
  - Physical Access
  - Malware
  - Ransomware
  - Confidential Data Handling
- Compliance and Monitoring

Source: SANS Security Awareness
Home and Mobile Working

- How many organizations have a Virtual Office Policy / Mobile Working Policy, or Agreement?
- Threats: Network Attacks, Viruses, Data Loss, and other remote user hazards
- Protect Data in Transit and at Rest
- Secure Baseline Build for all Devices
  - i.e. Ensure devices have updated virus protection software and appropriate firewall status before allowing them on VPN
Secure Configuration

- Current System Inventory List
- Baseline Build for all Devices
- Patch Management Policy/Process

- Are you at risk? Practices to be avoided:
  - Use of default passwords for systems and devices
  - Lack of formal configuration management process
  - Lack of consistent software install process
  - Unnecessary software installed on networks/servers
  - Improper file and directory permissions
  - User accounts with unnecessary access privileges
Removable Media Controls

• What is the Risk?
  – Loss of sensitive information
  – Introduction of malware
  – Reputational damage

• Corporate Removable Media Policy

• Best Practices to Implement:
  – Limit use of removable media
  – Scan all media for malware
  – Formally issue media to users
  – Encrypt information held on media
  – Manage reuse/disposal of removable media
  – Educate users and maintain awareness
Managing User Privileges

• Access Control Policy
• User Provisioning
  – Formal request and approval
  – Principle of least privilege (network, app, and db)
  – Regulate the creation of new accounts, administration of rights, and the editing of account details
• User Deprovisioning
  – Access disabled/deleted within 1-3 business days
  – Admin password change when support leave
• User Access Reviews
• Restrict Administrative Access
Monitoring

• Monitoring Strategy & Supporting Policies
• Continuously Monitor all Systems & Networks
• Capture and Analyze Logs for Unusual Activity
• Real-Time Monitoring:
  – Monitor network performance / availability / traffic
  – Monitor user activity (i.e. Detect and stop malicious activity before security is compromised)
  – Monitor computer operations (key backups / batches)
Malware Protection

• Corporate Malware Policy

• Personal Vigilance
  – Be wary of emails with attachments, links, or requests to enter your User ID and password

• Protective Tools
  – Anti-virus security package
  – Scan for malware across the organization
  – Automatically filter out malicious attempts
  – Only compliant machines gain network access
Network Security

• Security Policy
• Apply the Principle of Least Privilege
• Dual Authentication
• Segmented Networks
  – Create clear separation of data within network based on security requirements (i.e. isolate cardholder data from the rest of network)

• Network Security Scanner
• Vulnerability Scanning
• Patch Management
Vendor Management

• By 2020, 75% of Fortune Global 500 companies will treat vendor risk management as a board-level initiative to mitigate brand and reputation risk.

• Vendor selection
  – Vendor risk management program
  – Basic security assessment on all vendors

• Increased Demand for Cyber Insurance
  – The continuous onslaught of cyber attacks have companies and vendors pointing the finger at each other regarding responsibility, and insurance carriers looking for ways to deny claims
Cyber Insurance

• As more and more claims are filed, insurance companies are looking for ways to avoid paying claims.
• If the organization has weak IT controls...claims could be denied or limited
  – Pay close attention to any sections on exclusions, exemptions, limitations and indemnity
Be Prepared

SECURITY STANDARDS
Cyber Risk Assessment

**Figure 2-2. Risk Management Framework**

**Process Overview**
- **Starting Point**
- **Organizational Inputs**
  - Laws, Directives, Policy Guidance
  - Strategic Goals and Objectives
  - Priorities and Resource Availability
  - Supply Chain Considerations

**Risk Management Framework**
- **Step 1**: Categorize Information System
- **Step 2**: Select Security Controls
- **Step 3**: Implement Security Controls
- **Step 4**: Assess Security Controls
- **Step 5**: Authorize Information System
- **Step 6**: Monitor Security Controls

**Architecture Description**
- Architecture Reference Models
- Segment and Solution Architectures
- Mission and Business Processes
- Information System Boundaries
Questions
Contact

Antonina McAvoy, CISA
Manager, Cyber & Control Risk Services

PBMares, LLP
150 Boush Street, Suite 400
Norfolk, VA 23510
Phone: (757) 355-6011
amcavoy@pbmares.com

Visit www.pbmares.com to read our blog and learn of upcoming events.
About the Speaker

Antonina K. McAvoy, CISA

- Manager, Cyber and Control Risk Services
- Education:
  - BS in Business Management & Accounting, Babson College
  - Pursuing MS in Cybersecurity, Utica College
- Experience:
  - 10 years in information technology (IT) auditing experience
  - Certified Information Systems Auditor (CISA)
  - Focus areas: Cybersecurity, IT General Controls (ITGC), Cyber Risk Assessments, HIPAA security reviews, SOC audits, and Internal Audit.
About PBMares
Cyber & Control Risk Services

- PBMares has been specializing in IT and Cyber Security auditing for more than 15 years. Service include:
  - Attestation
    - IT General Controls Audits (ITGC)
    - Service Organization Control (SOC) Audits
  - Consulting
    - Cyber Risk Assessments
    - Review of Cyber Insurance Coverage
    - Vulnerability Scans of Network (Internal and External)
    - Penetration Testing
    - Incident Response Consulting
    - Data Classification Process Design and Consulting
    - Review of Information Security Program Policies and Procedures
    - Information Security Awareness Training
    - User Life Cycle Management Consulting