Vital Protection Mechanisms

Critical polices, procedures and technical controls that should be implemented.

About the Presenter

James Taylor – Sr. IT Security Consultant

- Vantage Point Solutions
- Background:
  - B.S., Information Security
  - A.S., Criminal Justice
- Specialties:
  - Cyber Security Auditing
  - Staff and Employee Training
- James.Taylor@vantagepnt.com

Why is IT Security Important?

- Critical Infrastructure Control
- Protecting Customer Data
- Reputation

The Three Core Principles

- **Confidentiality** – Who can access what assets?
- **Integrity** – Who is authorized to modify?
- **Availability** – What assets are available and when?

What Can I do Today

- CIS top 20 - www.cisecurity.org/controls/cis-controls-list/
- NIST - https://www.nist.gov/cyberframework
- FFIEC - https://www.ffiec.gov/cybersecurity.htm

Endpoint Security

Antivirus software on all user devices

Shared drives scanning for malicious signatures

Scheduled company-wide patching process

Monitored Devices

FIREWALLS

INTRUSION DETECTION/PREVENTION SYSTEMS

Privilege Access Management

- User Accounts vs Admin Accounts
- Access Control Lists
- Disable Unused Network Ports

Patch Management

Make a regular schedule to apply updates

Ensure patches are applied in a test environment before update is pass globally

Utilize a WSUS Server to automate updates

Vulnerability Assessment

- Annual Assessments (minimum)
- Useful to help identify vulnerabilities and weakness you may have been unaware of.
- The reports can assist in minimizing threats and your network's attack surface.

User Training and Testing

- Train, train and train some more
- Test your employees

Logging Systems

- Security Information and Event Management (SIEM)
- Maintain a digital record on network resources
- Track what changes were made and who modified them
- Helpful to identify the source of a breach

Backups

- Foundation of good cybersecurity
- Key factor in protecting asset integrity and availability
- Can be a safety net from ransomware and phishing attacks
- Can save time and money in the event of a disaster

Asset Management

Incident Response

- Incident Response Plan and Team
- Regularly meet and revise as needed
- Practice Tabletop Exercises

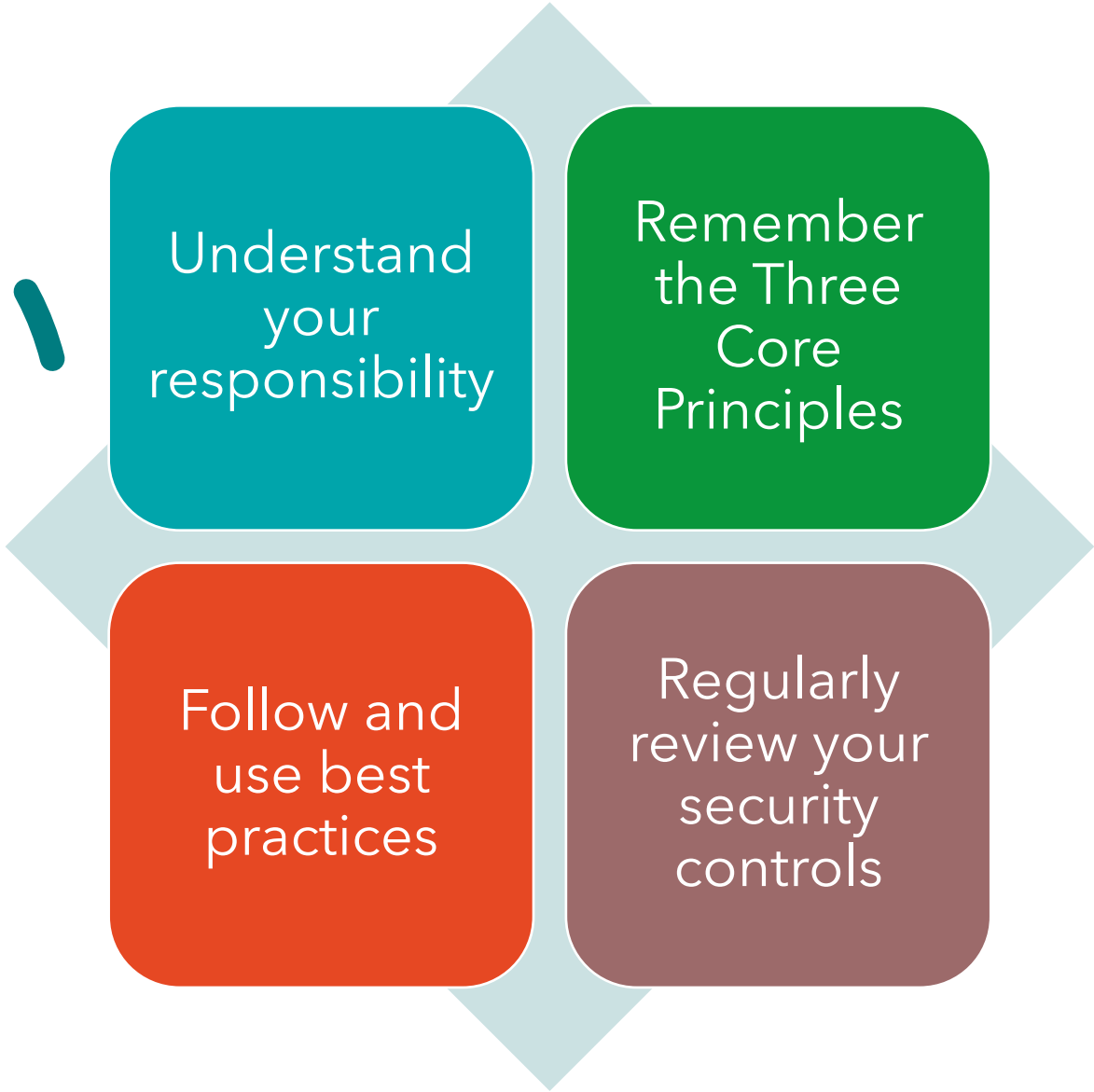
Physical Security

- Ensure all visitors or third-party vendors are accounted for.
- Surveillance systems & alarm systems
- Employee Training

Most Utilized Vulnerability - According to the U.S. Government for 2020

- Microsoft OLE – think sound, video clip integration for documents
  - How do you stop it – PATCHING, disallow certain file types
- Targeting VPN
  - How do you stop it – PATCHING, Hardening Guidelines and Security
- Cloud Service Attacks
  - How do you stop it – PATCHING, Hardening Guidelines and Security

In Conclusion



Thank you

James.Taylor@vantagepnt.com