Managing IT Risk and Assessing Vulnerability

2016 ACCS Conference, "Exploring the Possibilities"

Association of Collegiate Computing Services of Virginia

March 17, 2016
Portsmouth, VA

AIS Network

Presenter

AISN Site: www.aisn.net
Facebook: www.facebook.com/AISNetwork
Twitter: @AIS_Network
YouTube: www.youtube.com/user/AISNVideo

AIS Network

- Founded 1993
- Premier eGov Services Provider to the Commonwealth of Virginia

- **Contracts**

Contract VA-120416-AISN (Hosting Services)

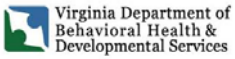
CAI Virginia IT Contingent Labor Contract Statement of Work (App Development)

Contract VA-120413-BPI (Web Apps Maintenance/ Operations)

Virginia SWaM Small Business #697064

Select Virginia eGov Clients

Agencies and Education



Outline

- Understanding the Landscape for Data Breach
- Steps Toward Managing IT Risk
  - Establishing a Risk Culture
  - IT Risk Assessment & Planning
- Mitigating Risk
  - Tools and Tactics for Assessing and Minimizing Vulnerability
- Remediation
  - Respond and Improve
- Q & A

Understanding the Landscape for Data Breach

Source: Privacy Rights Clearinghouse & online media reports

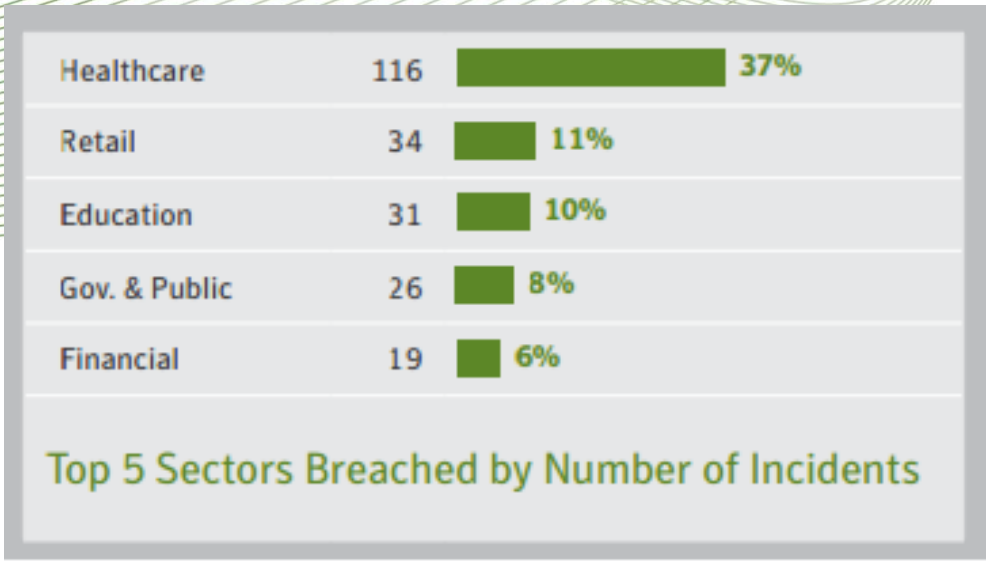
Schools Are Vastly Unprepared

Education Ranks #3 Among Top Sectors Breached

- Tinfoil Security tested 557 state universities with a cross-site scripting (XSS) attack.
- **One quarter of all networks were vulnerable.**

• Why Education?

- Protecting schools is more difficult than protecting corporations, because schools have a BYOD environment. Schools lack strict control over hardware/software used by faculty and students.



Symantec Internet Security Threat Report, 2015

Who Tries to Breach U.S. Campuses?

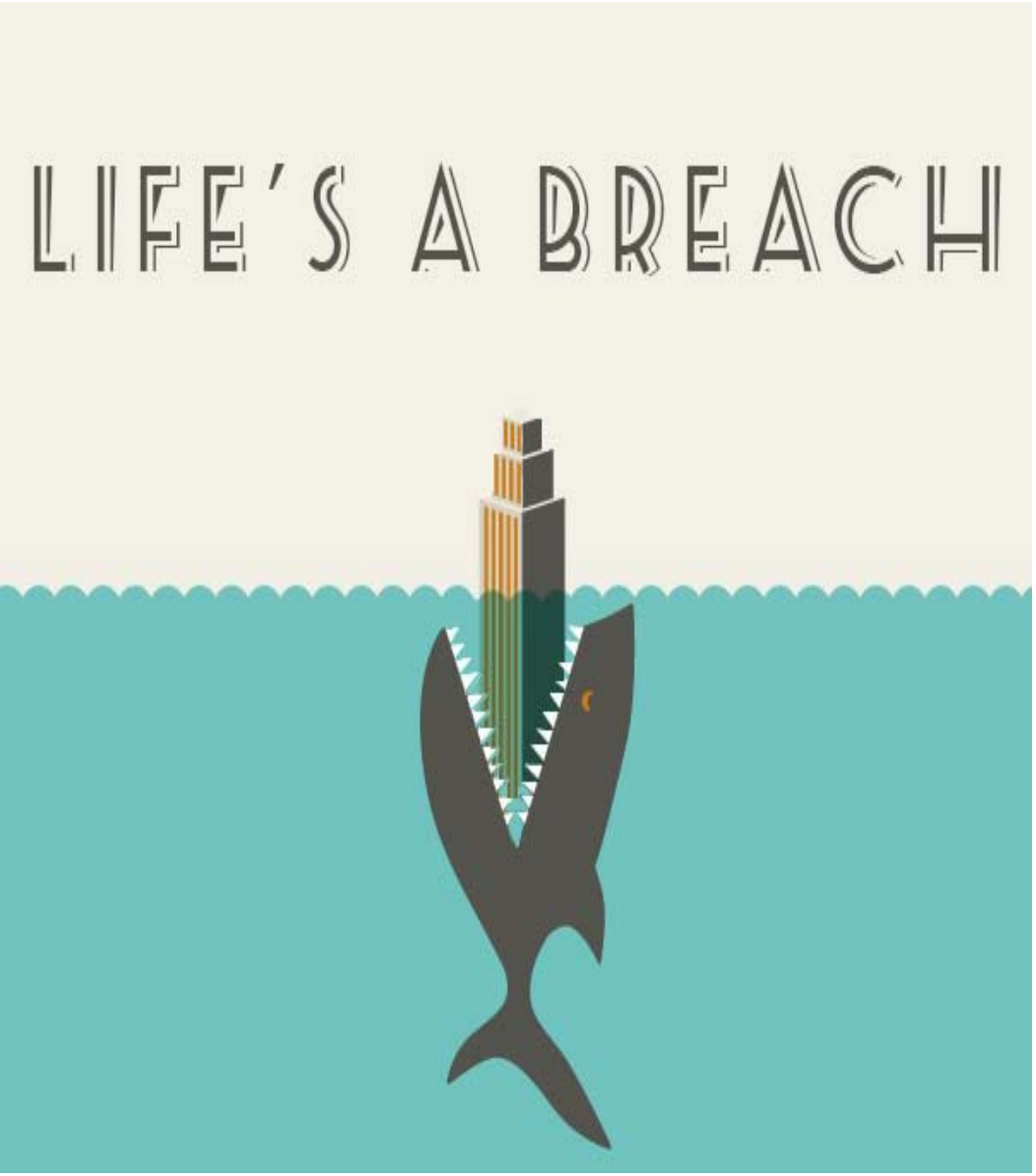
FBI Says….

- Hackers looking to make a profit
- Foreign and domestic businesses
- Individual entrepreneurs
- Competing academics
- Foreign intelligence services
- Terrorist organizations

Villain Ernst Stavro Blofeld, SPECTRE, *You Only Live Twice,* 1967

Why?
Universities are HUGE repositories of monetizable data.

- Steal technical information, compromising researchers' ability to get first-to-market with ideas
- Access intellectual property developed through university research (*e.g.,* technologies that serve to protect the U.S. militarily, economically or otherwise)
- Gather sensitive/classified research (*e.g.,* facilities that handle bio agents or radiation)
- Bypass expensive research and development
- Recruit individuals for espionage/ terror groups
- Spy for animal rights and eco rights terrorism
- Exploit the student visa program for improper purposes
- Conduct computer intrusions
- Collect sensitive personal/ financial information (identity theft, fraud, etc.)
- Compromise campus safety and safety of U.S. students studying abroad
- Spread false information for political/other reasons



Data Breach

Common Causes

- Malware
- Hacking
- Malicious insider/ outsider
- Unsolicited emails/phishing
- Unintended disclosure
- Payment card fraud
- Portable device
- Stationary device
- Physical loss
- Insider
- Schools don't have strict control over hardware/software used on campus

Graphic courtesy of KirkpatrickPrice

Steps Toward Managing IT Risk

Establishing a Risk Culture
IT Risk Assessment & Planning

Why Establish a Risk Culture?

Key Drivers

- Regulatory compliance with FERPA, HIPAA, PCI, etc.
- Institutional reputation
- Leadership/ executive tone
- Strategy/ decision making
- Risk governance structure
- Recruitment and competence
- Bottom line

Risk Culture Demonstrates

- You're not "driving like you can afford the accident"
- Consistent role modeling from senior leadership
- Clear/ well articulated risk strategy incorporates physical and behavioral characteristics
- Transparent/ unified decision making
- Rapid escalation of threats

Why a Risk Management Plan?

Regulatory Requirements

- FERPA. HIPAA, PCI and others require institutions to certify that their data is secure from malicious threats.
- Protect against fines/penalties, class action lawsuits, reputational damage and income loss

Campus Security

- The BYOD culture invites risk issues.
- Every time an institution adds new hardware, changes network configurations, installs new software or performs major upgrades, it risks exposing its network unknowingly.

Teamwork

- Information Technology
- Information Security
- Risk Management
- Legal
- Compliance
- Privacy
- Human Resources
- Physical Security/Campus Police
- Communications (Public/Gov't. Relations)
- Board of Directors


Conduct Risk Assessment Survey
Identify Risks
Assess Risk Importance & Risk Likelihood
Create Risk Management Action Plan
Implement Risk Management Plan
Risk Management Process

IT Risk Assessment & Planning

Addressing High-Risk Behaviors

- Weak passwords
- Sharing passwords
- Using identical passwords
- Using unsecure Internet connections
- Failure to purge old files
- Manual collection of PII by teachers/assistants
- Sloppy vendor practices
- Not reporting lost hardware
- Leaving computers unattended
- No privacy screen use
- Connecting unsecure devices to the work network
- Using unencrypted USB drives to store critical files
- Traveling with travel devices “fully loaded”

Planning

Considerations for Action Plan Development

- **Regulations.** The government is not waiting for a breach to inspect your compliance. Use a risk-based perspective when following compliance laws.
- **Cyber security.** Plan to invest in security to prepare to withstand a cyberattack. Also, do you have cyber coverage/ data breach insurance?
- **Vendors.** Vendor risk cannot be outsourced. It must be managed. Are your vendors compliant? If you maintain HIPAA compliance, are vendor BAAs in place?
- **Privacy/compliance counsel.** A privacy/ compliance attorney can guide you on how to work out steps with regard to discovery of an event, forensic investigation/ evaluation of the event, managing the short-term crisis and handling the long-term consequences (identify notification and credit monitoring vendors, call centers, etc.).
- **Wearable technology and portable devices.** Update and enforce your BYOD and secure wearables policies.
- **The "weakest link."** You're only as strong as your weakest link. Educate your people and promote healthy security awareness on campus.

IT Risk Management Action Plan

Based on Survey Results and Risk Ranking

Must-Haves

- Awareness training for students, researchers, faculty, admin
- Specific threat information if available
- Brochures or other literature about threats
- More robust security procedures if needed
- FBI consultation (be prepared to work with them on security concerns)

Implement the Plan

- Serve as a resource for questions/concerns (e.g., export control matters)
- Monitor suspicious incidents closely
- Be aware of regional counterintelligence meetings with academics, businesses and US intelligence community personnel
- Prepare for continual training/ review

Mitigating Risk

Tools and Tactics for Assessing and Minimizing Vulnerability

Anticipating Attacks: 10 Tips From the FTC

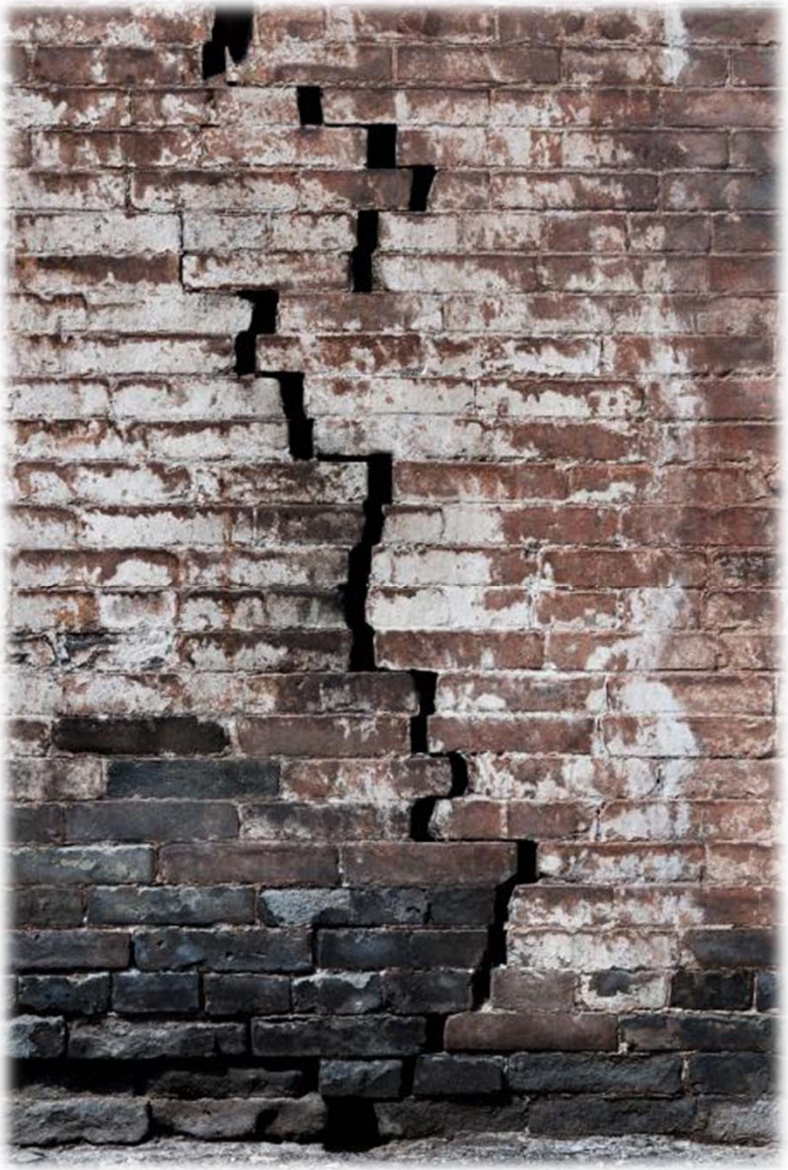
1) Start with security.
2) Control access to data sensibly.
3) Require secure passwords/ authentication.
4) Store sensitive personal info. Securely and protect it during transmission.
5) Segment your network; monitor who is trying to get in/out.
6) Secure remote access to your network.
7) Apply sound security practices when developing new products.
8) Ensure service providers implement reasonable security measures.
9) Put procedures in place to keep your security current and address vulnerabilities that may arise.
10) Secure paper, physical media and devices.

"Start With Security: A Guide for Business," FTC, June 2015.

Security Architecture Mindset

Policies Align With Tools

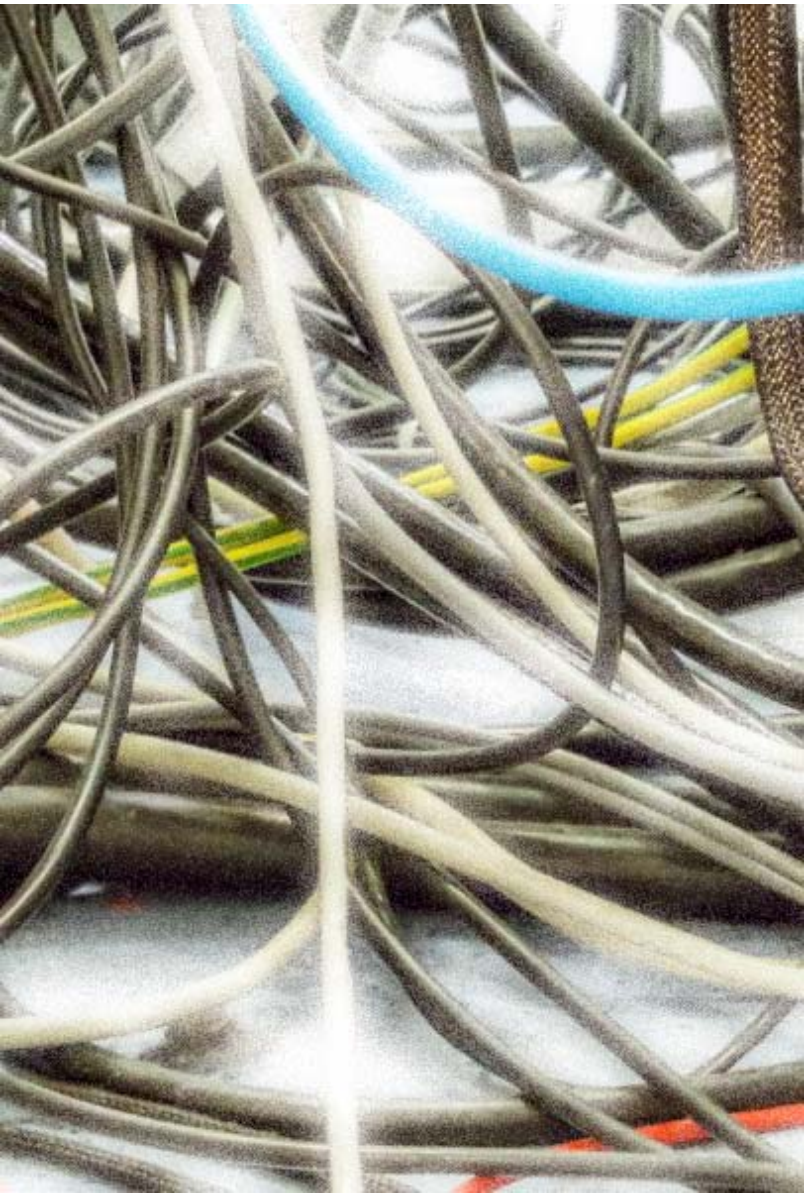
- Sloppy security days are gone.
- Security must be architected now.
- Align clear policies against the objectives of the tools that are available.
- There's an amazing array of security innovation today.
- Microsoft and VMware are changing the landscape of how applications are built and delivered securely.
- Invest and enable.



Assessing Vulnerability

Tools to Find, Classify, Verify & Remove Threats

- Vulnerability Scanning (External/ Internal)
- Penetration Testing
- Enterprise Threat Simulation
- Continuous Auditing
- Data Encryption
- DDoS Protection
- Event Management
- Firewall and VPN Services
- Intrusion Detection Services
- Malware Protection
- Change Management
- Two-Factor Authentication
- Web Application Firewall
- Compliance Management
- Log Management
- SSL Certificates



IT Checklist

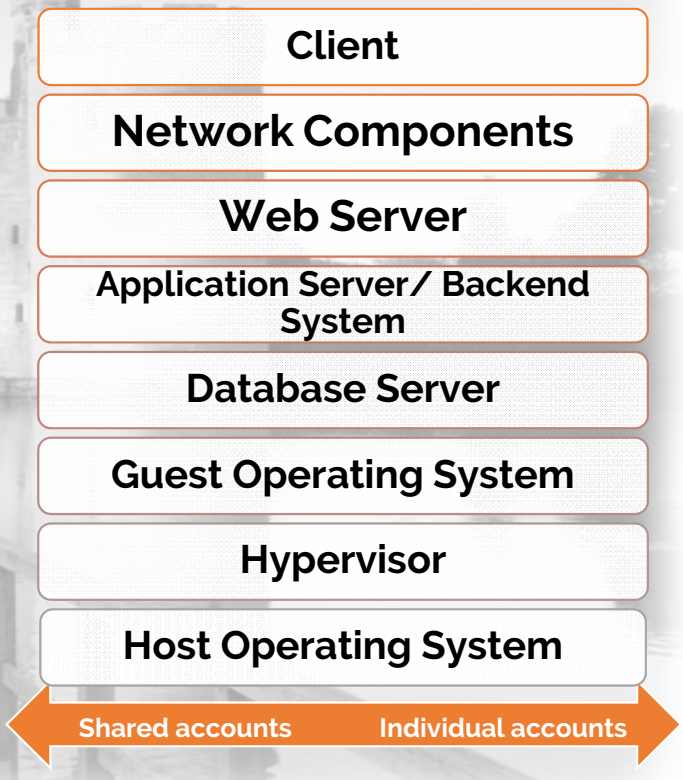
Tactics for Minimizing Vulnerability

- Keep operating systems up-to-date.
- Update a computer program or data regularly with patches.
- Patch Management/Maintenance Windows
- Standardize the application software.
- Block third-party cookies and pop-ups in web browsers.
- Delete caches more often.
- Use sophisticated passwords.
- Monitor sharing.
- Encrypt sensitive data.
- Manage alerts.
- Quantify risks and soft spots.

IT Checklist

Policies for People With Keys to the Kingdom

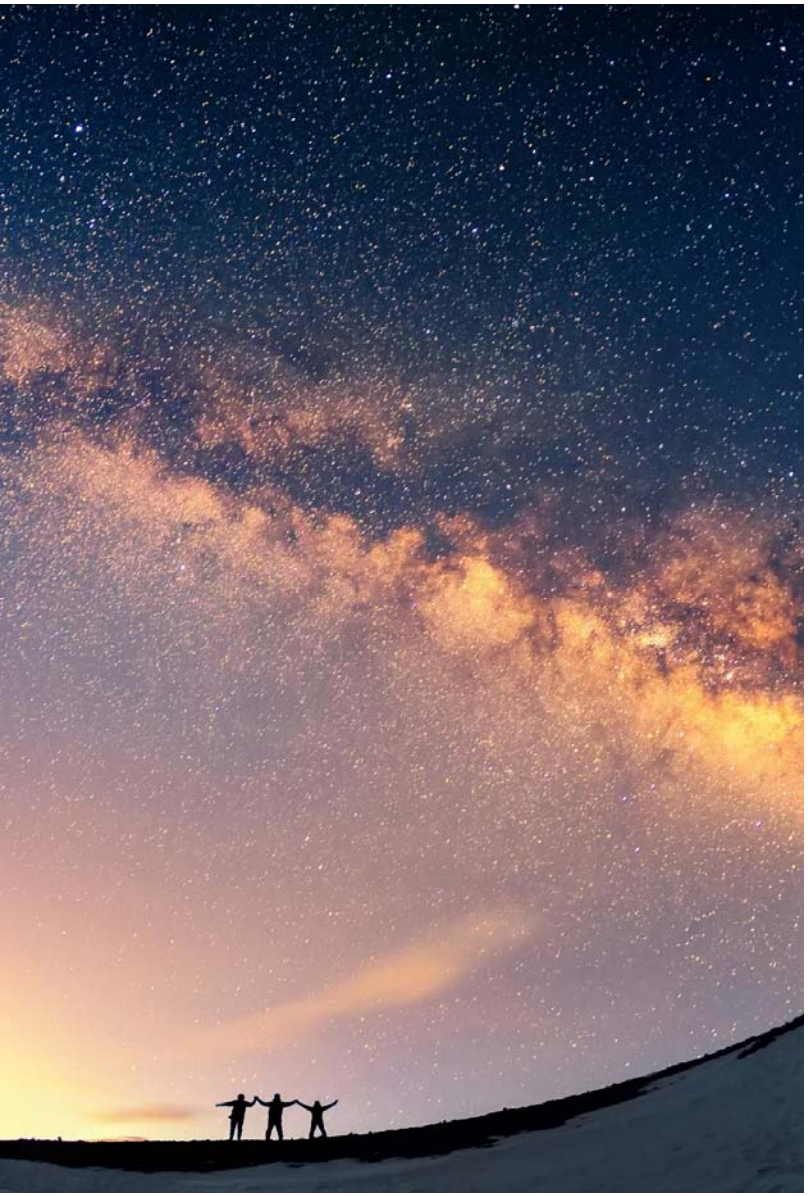
- Have an “exit policy” for employees/ students who leave the school
- Require complex passwords
- Maintain clear visibility into access privileges
- Manage all privileged accounts




Remediation
Respond and Improve

In Remediating Vulnerabilities, Prioritize….

- Not all vulnerabilities are equal.
- Not all assets are equal.
- Encryption is not a panacea.
- Remediation actions may be inconvenient to users/ normal operations.
- Government policy alone won't guide you.



Identify Gaps & Improve

Apply Your Knowledge to Predict & Prevent

- Test environments
- Simulations
- Tabletop exercises
- Threat modeling
- Pairing exercises (tester + responder)
- Security assessments
- Walk through common techniques/ protection mechanisms
- Test your communication channels


Q & A

Thank You

AISN Site: www.aisn.net
Facebook: www.facebook.com/AISNetwork
Twitter: @AIS_Network
YouTube: www.youtube.com/user/AISNVideo