CyberSecurity Solutions

projexIMC

Overview

- Cybersecurity threats
- Cybersecurity standards
- Multi-layer cybersecurity solution
- Next steps

projexIMC

Cybersecurity Threats

PROJEX IMC | January 2018

Definition

- **Cybersecurity**

  [noun]

  The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

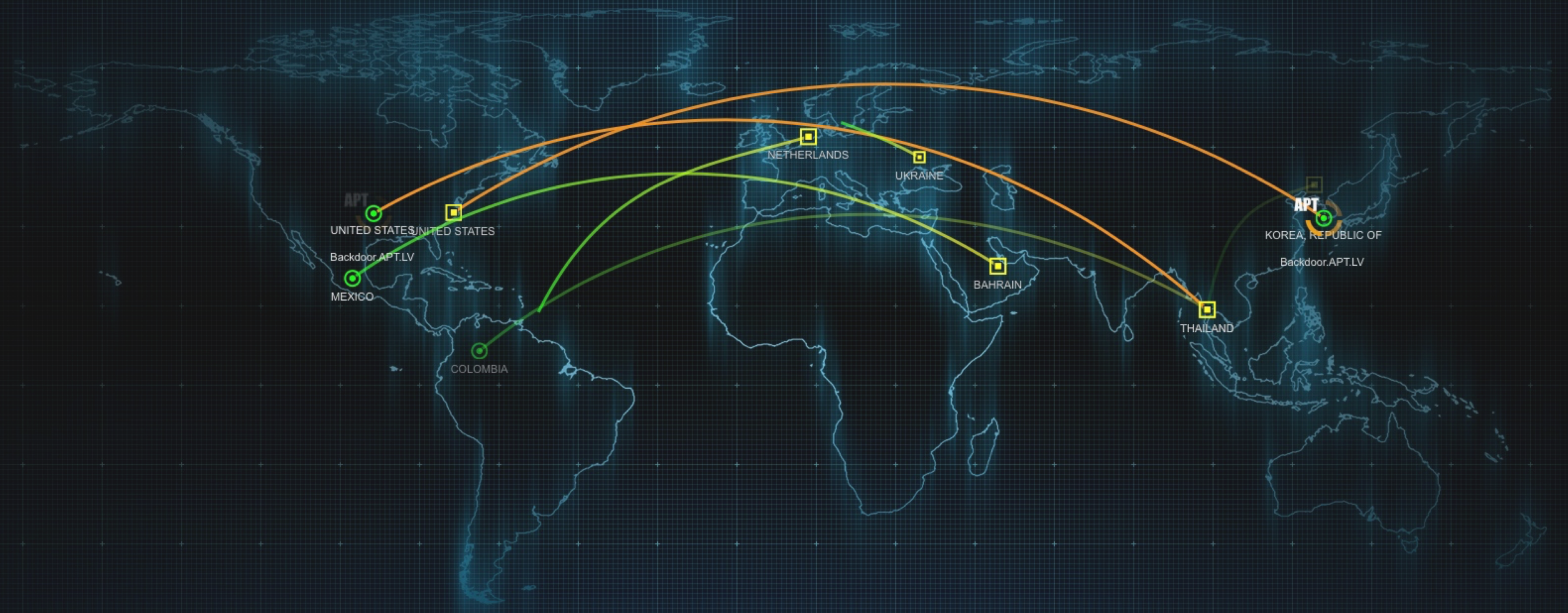
- **Cybersecurity**

  Refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access

- **Cyber security**

  The practice of defending computers and servers, mobile devices, electronic systems, networks and data from malicious attacks

Cybersecurity landscape



Source: FireEye® Cyber Threat Map (https://www.fireeye.com/cyber-map/threat-map.html)

Cybercriminal objectives

- Steal personal information
- Steal business information (financial/technical)
- Steal intellectual property (trade secrets/patents etc.)
- Request money (ransom)
- Harm IT infrastructure

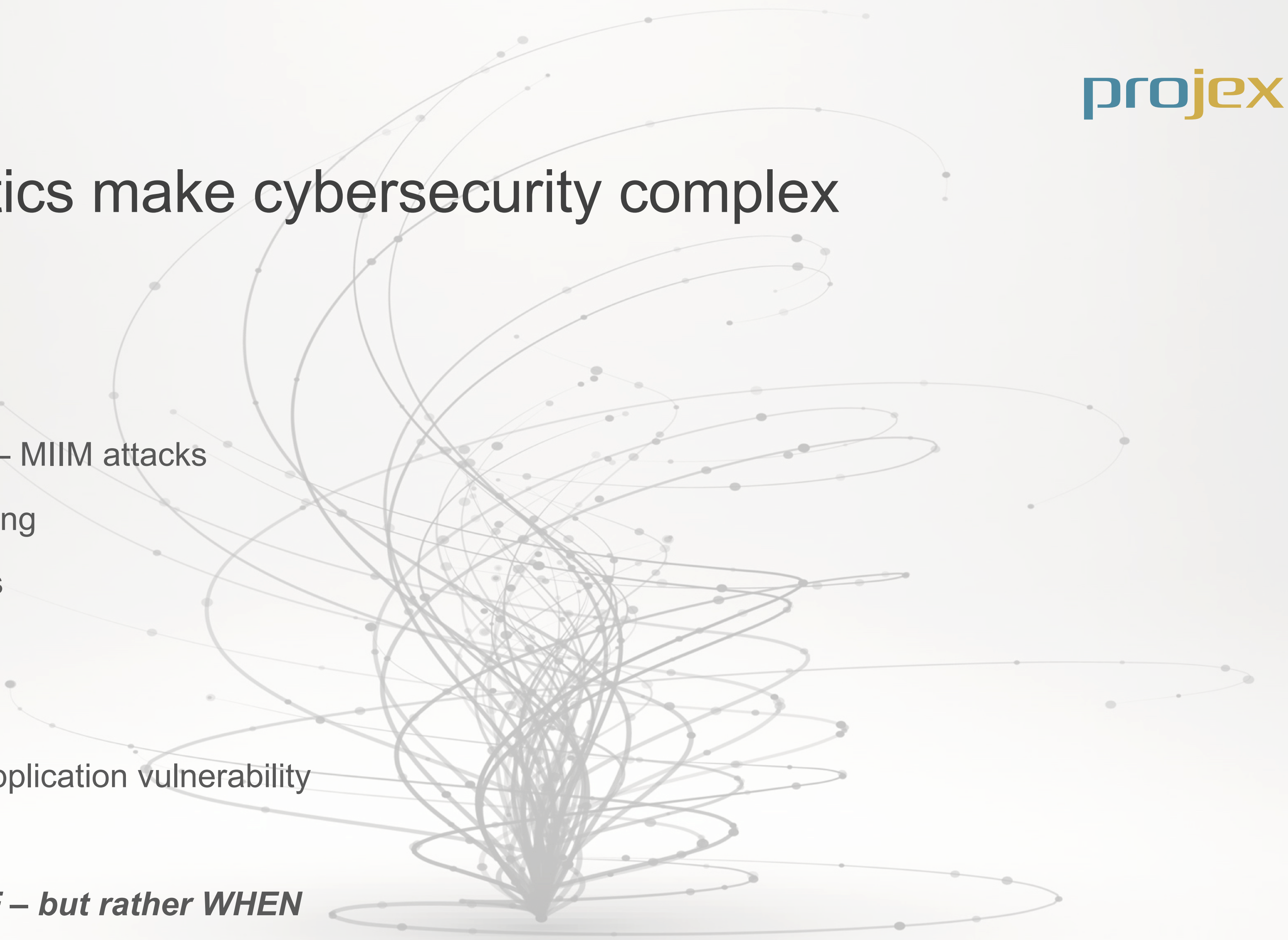
Common threats

- **Malware** – Refers to a variety of hostile, intrusive programs
- **Ransomware** – Programs intended to hijack computers/data and request money in exchange
- **Computer viruses** – Malicious programs typically intending to steal/delete data or computer control
- **Rogue security software** – Programs (usually popup offers) claiming to help “fix” security issues
- **Trojan horses** – Malicious programs disguised as legitimate software
- **Malicious spyware** – Malicious programs intended to steal passwords and other sensitive information
- **Computer worms** – Malicious programs designed to replicate rapidly (often used in DDOS attacks)
- **Botnets** – Groups of compromised computers connected to the Internet
- **Spam** – Unsolicited junk mail that often contains links to malicious websites or programs
- **Rootkit** – Collection of tools used to obtain administrative access to a PC

Evolving tactics make cybersecurity complex

- Fake tech support
- Phishing schemes
- Man In The Middle – MIIM attacks
- Fraudulent advertising
- Social media scams
- Bitcoin scams
- Social engineering
- OS (Windows) or application vulnerability

It is not a matter of IF – but rather WHEN



Ongoing OS and application SW vulnerabilities

SMBs face multiple challenges as they address cybersecurity issues …

- Cyber criminals constantly find new vulnerabilities in OS and apps
- New technology emerges at a very fast pace
- PC hardware and software is usually replaced every 5 years
- Cybersecurity hardware and software platforms keep changing just as fast
- The majority of cybersecurity solutions are aimed at large businesses
- This results in cybersecurity solutions that are overly complex and usually too expensive for SMBs and local governments

Cybersecurity Standards

PROJEX IMC | January 2018

NIST 800-171 cybersecurity standards

Only independent set of standards (UL for cybersecurity) …

- US Dept of Commerce – National Institute of Standards & Technology
- Required for DFARS contractors/suppliers (DOD, DHS, etc.)
- Recommended for commercial businesses and non-federal agencies
- Practical set of 14 cybersecurity processes and methods
- Minimum requirement for sustainable protection

Basic cybersecurity requirements – NIST 800-171

REQUIREMENT	PURPOSE
Access control	Limit/control system access
Awareness and training	Educated users and best practices
Audit and accountability	Identify and trace incidents
Configuration management	Control network hardware and software
Identification and authentication	Verify users and devices
Incident response	Detection and recovery process
Maintenance	Implement sustainable processes
Media protection	Physically control and secure
Personnel security	Pre-qualified users/access rights
Physical protection	Limit access to physical spaces
Risk assessment	Scan for vulnerabilities
Security assessment	Periodically assess “as is” situation
System and communications protection	Protect inbound / outbound
System and information integrity	Identify malicious code and users

projexIMC

Roadmap to achieving sustainable protection

NIST 800-171 standards …

- Network/Security Assessment = “AS IS” threats
- Review/remediate known threats = report and recommendations
- Review compliance to NIST cybersecurity standard
- Implement cybersecurity infrastructure, best practices and user training

projexIMC

projexguard

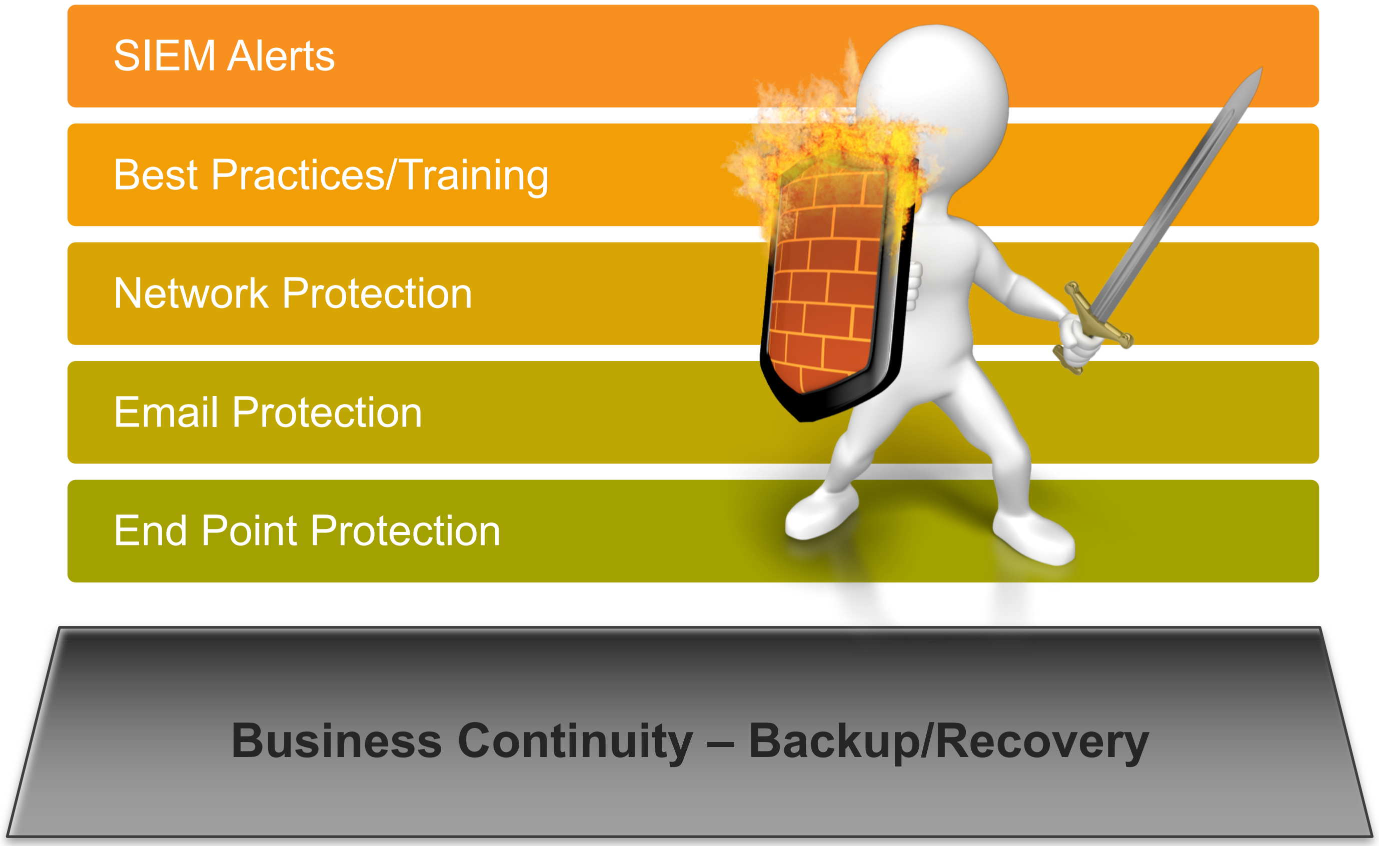
The Multi-Layer Cybersecurity Solution

PROJEX IMC | January 2018

projexIMC

Layered approach to cybersecurity

Cybersecurity Layered Solution



SIEM Alerts

Best Practices/Training

Network Protection

Email Protection

End Point Protection

Business Continuity – Backup/Recovery

Threats/Countermeasures – Dynamic situation

THREAT	END POINT	EMAIL	NETWORK	BEST PRACTICES/ USER TRAINING	SIEM ALERT
Malware	3			3	3
Ransomware	3		3	3	3
Computer Virus	3	3			3
Rogue Security Software		3		3	3
Trojan Horse	3	3		3	3
Malicious Spyware	3	3	3	3	3
Computer Worm	3		3	3	3
Botnet	3		3		3
Spam		3			3
Rootkit	3	3	3		3

projexIMC

Starting point: BDR

Business Continuity / Disaster Recovery …

- Local (on-site) backups
  - Windows backup to local or external disk
- Off-site backups
  - IBackup cloud backup service
- Disaster Recovery as a Service (DRaaS)
  - Infrascale DRaaS uses on-premise appliance for local backup
  - Cloud replication for off-site backup
  - Enables booting up protected system(s) in the local appliance or in the cloud

Endpoint protection

- **Webroot SecureAnywhere Business Endpoint Protection**
  - Protects against threats across email/browsers/files/URLs/ads/apps in real time
  - Uses advanced behavioral heuristics to identify and protect against never-before-seen threats
  - Backed by Webroot's Threat Intelligence Platform - using massive machine learning in the cloud, classifies 95% of the Internet three times a day
- **Security patching with help desk ticket support**
  - Remote Monitoring and Management (RMM) enables automatic support ticket creation in our help desk ticketing system
  - RMM 24 x 7 proactive patch management (Windows and third party security updates)
  - Includes Webroot SecureAnywhere® EndPoint Protection

Email protection

- **EveryCloud Anti Spam Filtering**
  - A powerful cloud-based spam filtering service blocks 99.99% of spam, viruses and even newsletters (optional) in the cloud before they reach your network.
  - The email filtering service provides complete protection against spam, viruses, malware, phishing, denial of service attacks and data loss for your organization, without the time or expense of managing hardware and software systems.
  - With optional EveryCloud Email Continuity, you can, in the event of any kind of email/server failure, restore up to 90 days worth of historical email to the powerful web mail interface.

Network protection – DNS Service

Internet policy enforcement …

- **Webroot SecureAnywhere DNS Protection**
  - DNS service – no appliance required. Simply redirect web browsing (DNS server) through the Webroot DNS cloud.
  - Gain immediate control of users' internet activity. The most dangerous websites are blocked automatically and all the other sites are under real-time URL category policy control.
  - Block websites according to 82 specific site categories (security, adult, productivity, etc.)
  - Allow/Block (whitelist/blacklist) support

Network protection – Security Appliance

Next Generation Firewall (NGFW) …

- **FortiNet NGFW**
  - FortiGate 30E, 50E, 60E, or 80E Security Appliance
  - Innovative security processor (SPU) technology for high performance application layer security services (NGFW, SSL inspection, and threat protection)
  - Protects against known exploits, malware and malicious websites using continuous threat intelligence provided by FortiGuard Labs security services
  - FortiGuard NGFW service delivers proven application control and intrusion prevention (IPS) technologies to improve overall security posture
  - Detects unknown attacks using dynamic analysis and provides automated mitigation to stop targeted attacks

Monitoring, detection and response

Security Information and Event Management (SIEM) …

- Collect information from all network devices: end-user devices, servers, routers, firewalls, switches, etc.
- Present information in a centralized dashboard for ease of access.
- Store information for future analysis and reporting.
- Aggregate and distill information and present actionable security events.
- Facility response in near real-time to Cybersecurity alerts

Monitoring, detection and response

Security Information and Event Management (SIEM) …

- **ProjexGuard™ SIEM**
  - CyberSecurity Internal Threat Detection and Alerting Virtual Appliance.
  - Daily Network and Security Scans looking for Anomalies, Changes, and Threats.
    - Users logging in at times outside their historical patterns, or a USB drive plugged into a computer that has been tagged as being "locked down.“
    - Changes to user security permissions, or new device added to the network that wasn't there before.
    - Critical security hole or a machine with missing security patching.
  - Enables response via daily email alerts or IT Ticket creation
  - Weekly notices summarizing ALL changes to network/compute environment.

Best practices

Develop IT policies that address …

- Internet and email use policy
- Physical security policy
- Logical security and password policy
- Removable device policy
- Bring Your own device policy
- Mobile device policy/management

> *“**Among 874 incidents**, as reported by companies to the Ponemon Institute for its recent 2016 Cost of Data Breach Study, **568 were caused by employee or contractor negligence**; 85 by outsiders using stolen credentials; and 191 by malicious employees and criminals.”*

User training — IT best practices

- Backup, business continuity and disaster recovery policy
- Physical security policy
- Bring Your Own Device (BYOD) policy
- Password policy
- Removable device (USB) policy / encryption
- Mobile Device Management (MDM) solution
- Cyber security awareness training

Cybersecurity awareness training

Periodic training to bring awareness to latest cybersecurity threats:

- Insider threats
- Malicious links
- Malware
- Password
- Physical security
- Ransomware
- Social engineering
- Social networking
- Spear phishing

Next Steps

Next steps – Known threats

- Complimentary Network and Security Assessment
  - Establish the baseline security level
- Develop Remediation Plan
  - In response to the Network and Security Assessment develop a plan to correct any security deficiencies found
- Analyze Overall Security Posture
  - Determine if security layers have all been addressed and take appropriate action

Network assessment

Identify critical network issues …

- Active/inactive user/login analysis
- Active/inactive computer/age inventory
- Major application installation inventory
- Password strength analysis (Microsoft Baseline Security Analyzer - MBSA)
- Missing security updates (Microsoft Baseline Security Analyzer - MBSA)
- Server/computer hard drive/storage analysis
- Anti-virus, anti-spyware software detection
- Remote listening ports

projexIMC

Security assessment

Identify critical security risks …

- Outbound security - system leakage
- Outbound security - web filtering
- Outbound security - wireless access
- External security vulnerability
- Password policy analysis
- Account lockout policy analysis
- Computer login analysis
- User login analysis

Thank You!

projexIMC