Security Risks, Things to Consider

Education PII Data has become very popular around the WORLD!!

It's been estimated that 60% of current malicious activity is focused on Education Data.

MS-ISAC
Center for Internet Security
(Multi State Information Sharing & Analysis Center)

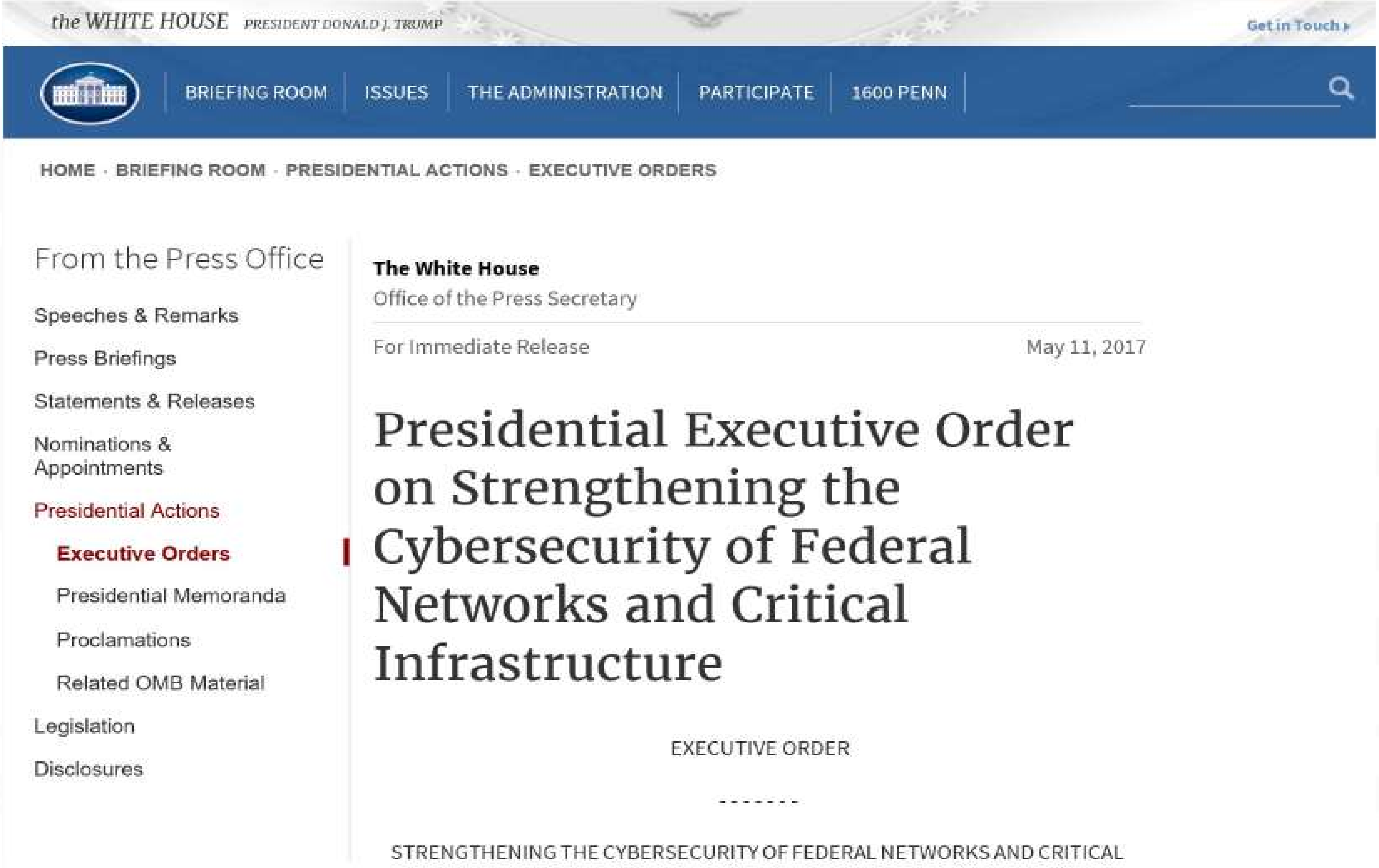
- On August 8, 2018 Issued an Alert
- FBI Private Industry Notification (PIN) - Connected Education Technology and Mass Data Collection on Students Necessitates Increased Cybersecurity
- Focus on Increased Activity of Criminals Targeting Education Data, EdTech Services and Resources

Targeted Data

- Personally Identifiable Information (PII)
- Academics
- Biometrics
- Behavioral
- Disciplinary
- Medical
- Web Browsing History
- Geolocation
- IP Addresses
- Classroom Activities
- Other Sensitive Indicators

Malicious Use

- Social Engineering
- Bullying
- Tracking Students
- Identity Theft
- Social and Other Threats to Parents
- Other Harmful Activities Targeting Children



The White House
Office of the Press Secretary

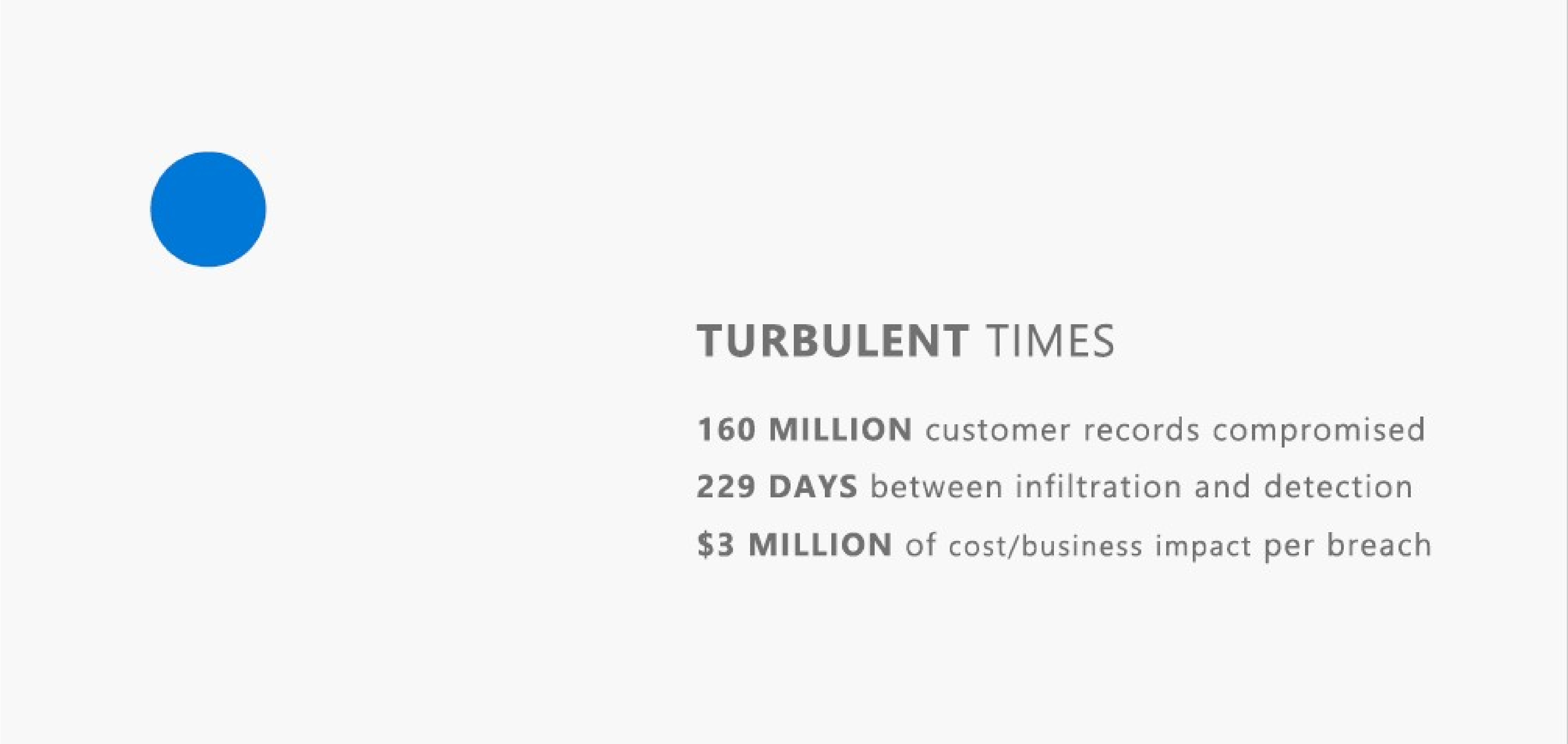
For Immediate Release May 11, 2017

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

EXECUTIVE ORDER

- - - - - - -

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL



TURBULENT TIMES

160 MILLION customer records compromised

229 DAYS between infiltration and detection

$3 MILLION of cost/business impact per breach

Phishing

"Email phishing shows no sign of stopping anytime soon and there is little defense to protect an endpoint where the user unknowingly cooperates with the attacker by clicking within the email."

"Phishing attacks will continue to work, and without major changes in cyber defense strategy, these attackers will continue to get in and steal your data."

Phishing Types

- **Deceptive Phishing**

Ex: You get an email from a bank claiming that your account has been frozen unless you click on the link provided and enter your account information.

- **Spear Phishing**

Ex: You get an email that's supposedly from your organization's HR department asking you to verify your benefits policy information.

Phishing Types

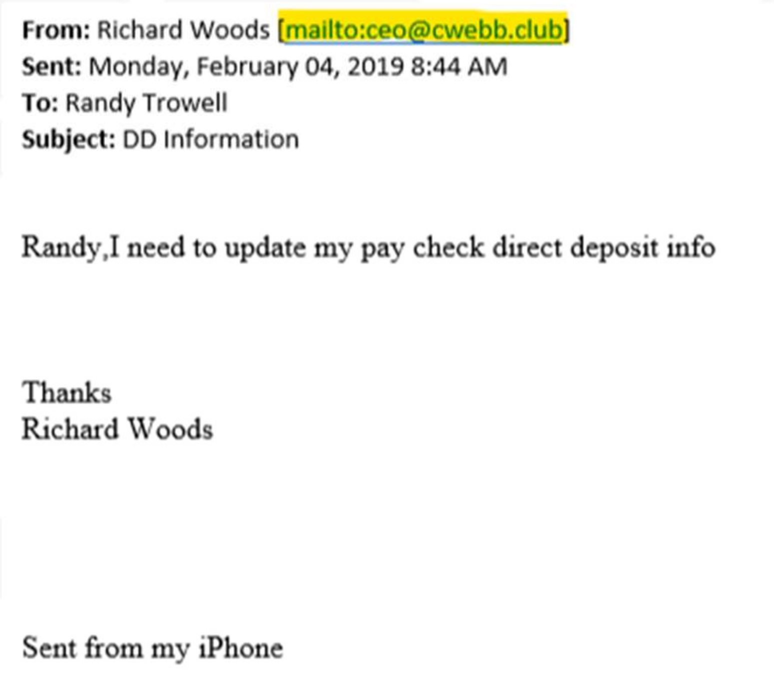
- **CEO\Executive Fraud Phishing**

Ex: You get an email that's supposedly from your CEO saying they need you to wire transfer the money, and to let you know when you're free so they can send you the information of where it needs to go. (W2's)

- **Malware-Based Phishing**

Ex: You get an email from someone you don't know asking you to download an invoice.

Used to deliver viruses, worms, Trojan horses, ransomware, or other malicious programs.

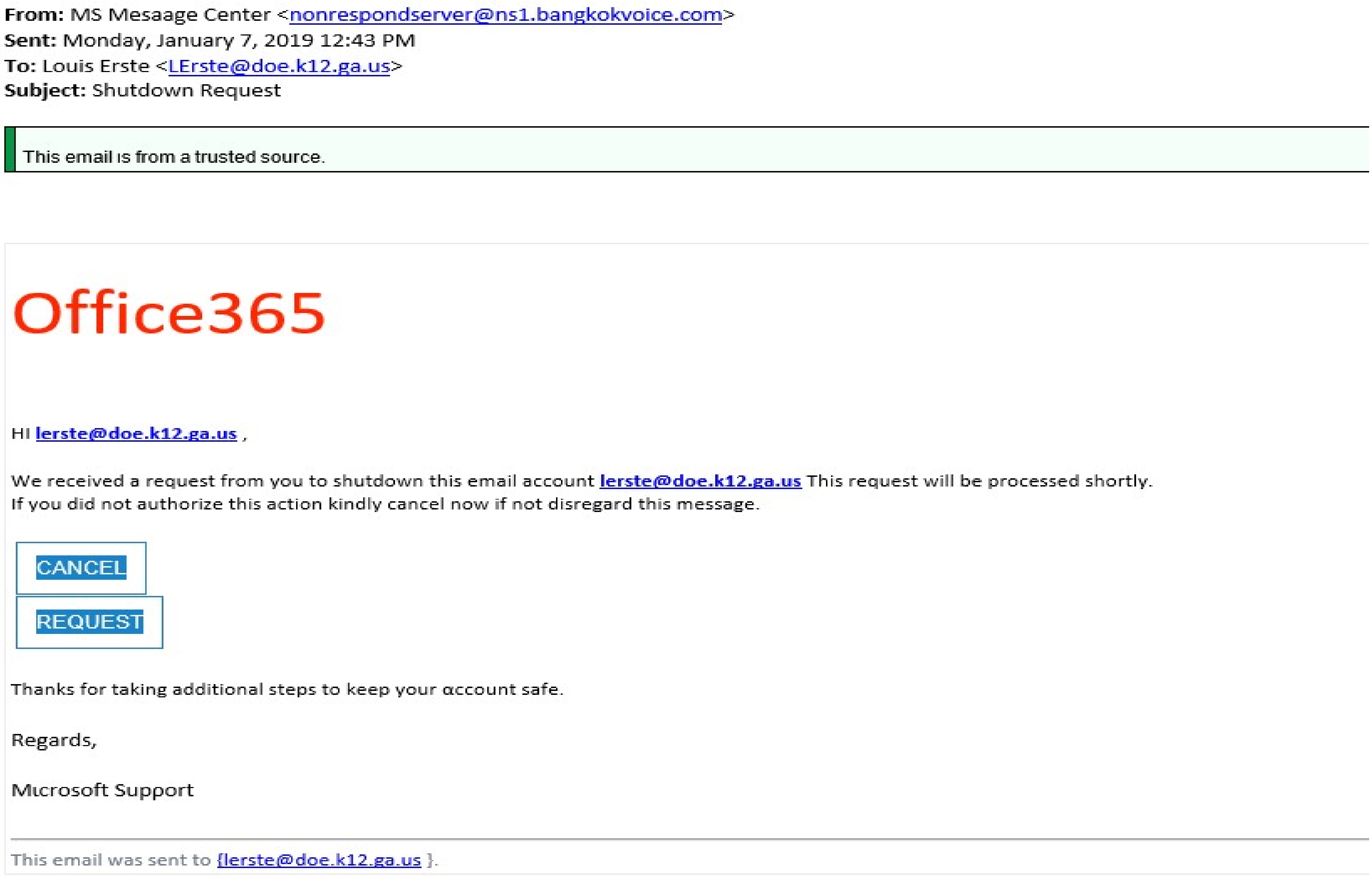


From: Richard Woods [mailto:ceo@cwebb.club]
Sent: Monday, February 04, 2019 8:44 AM
To: Randy Trowell
Subject: DD Information

Randy,I need to update my pay check direct deposit info

Thanks
Richard Woods

Sent from my iPhone



From: MS Mesaage Center <nonrespondserver@ns1.bangkokvoice.com>
Sent: Monday, January 7, 2019 12:43 PM
To: Louis Erste <LErste@doe.k12.ga.us>
Subject: Shutdown Request

This email is from a trusted source.

Office365

HI **lerste@doe.k12.ga.us** ,

We received a request from you to shutdown this email account **lerste@doe.k12.ga.us** This request will be processed shortly.
If you did not authorize this action kindly cancel now if not disregard this message.

Thanks for taking additional steps to keep your account safe.

Regards,

Microsoft Support

This email was sent to {lerste@doe.k12.ga.us }.

Recent Phishing

- Estimated 550 million email users in the Q1 2018
- Phishing emails have surged past malware 21:1 in Q1 from the previous year
- Appeared as popular brands, online services and telecom providers
- Augusta University Health – Exposure of medical and personal information on about 417,000 individuals
- Phishing targeted 24 university faculty and administrators
- Confirmed breach on July 31, 2018, Activity in September 2017

Who Remembers the ATL Ransomware?

ATL Experience

- March 22, 2018 - System shutting down
- Sam Sam Ransomware (Brute-Force Attack)
- Prior attacks were small government to a large state agency and a large medical center
- June 1/3 of their applications were still down impacting multiple systems across multiple offices
- $2.7 million original, later updated to $9.5 million
- Today systems are still impacted
- Audit in January 2018 found 1500 to 2000 vulnerabilities

Attackers go for the low-hanging fruit:

Humans

Most Attacks Rely on Social Engineering

Humans

Email

- Phishing
- Spear-Phishing
- Malware Attack

Social Media

- Reconnaissance
- Fake Friends
- Use of breached data

Trends

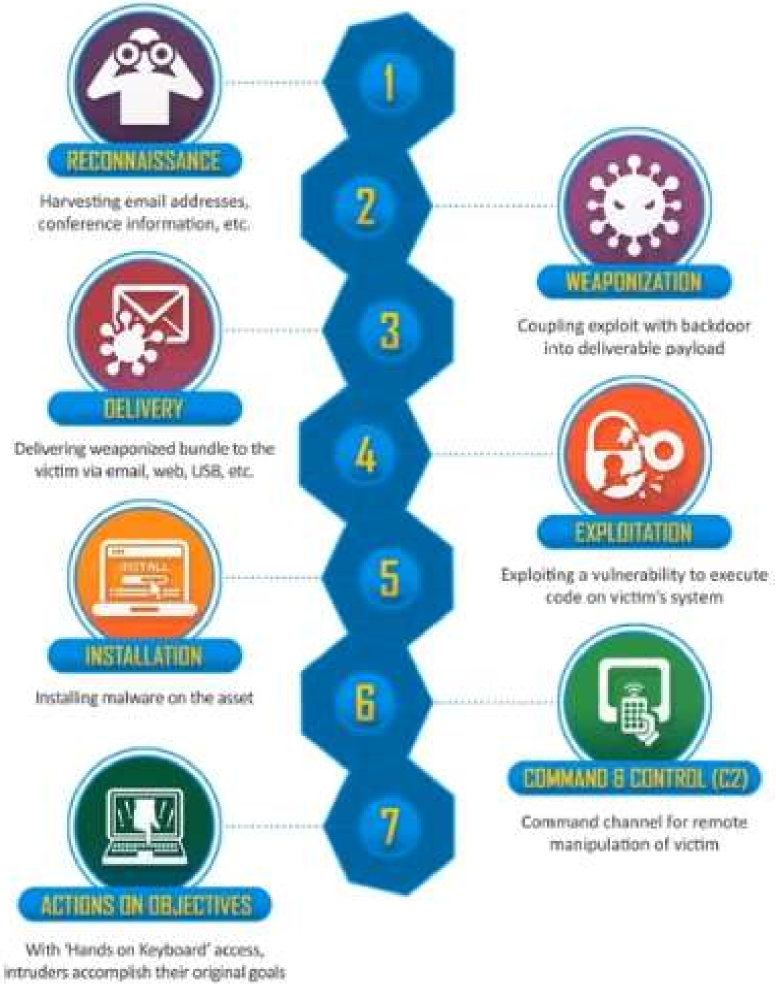
- Ransomware (Pseudo)
- Extortion
- Search result poisoning

Criminal Groups

- Malicious insiders
- Organized crime
- Hackers
- Terrorist

Attack Vectors

- Physical on-site attacks
- Endpoint
- Mobile
- Network
- Cloud (Internet)



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

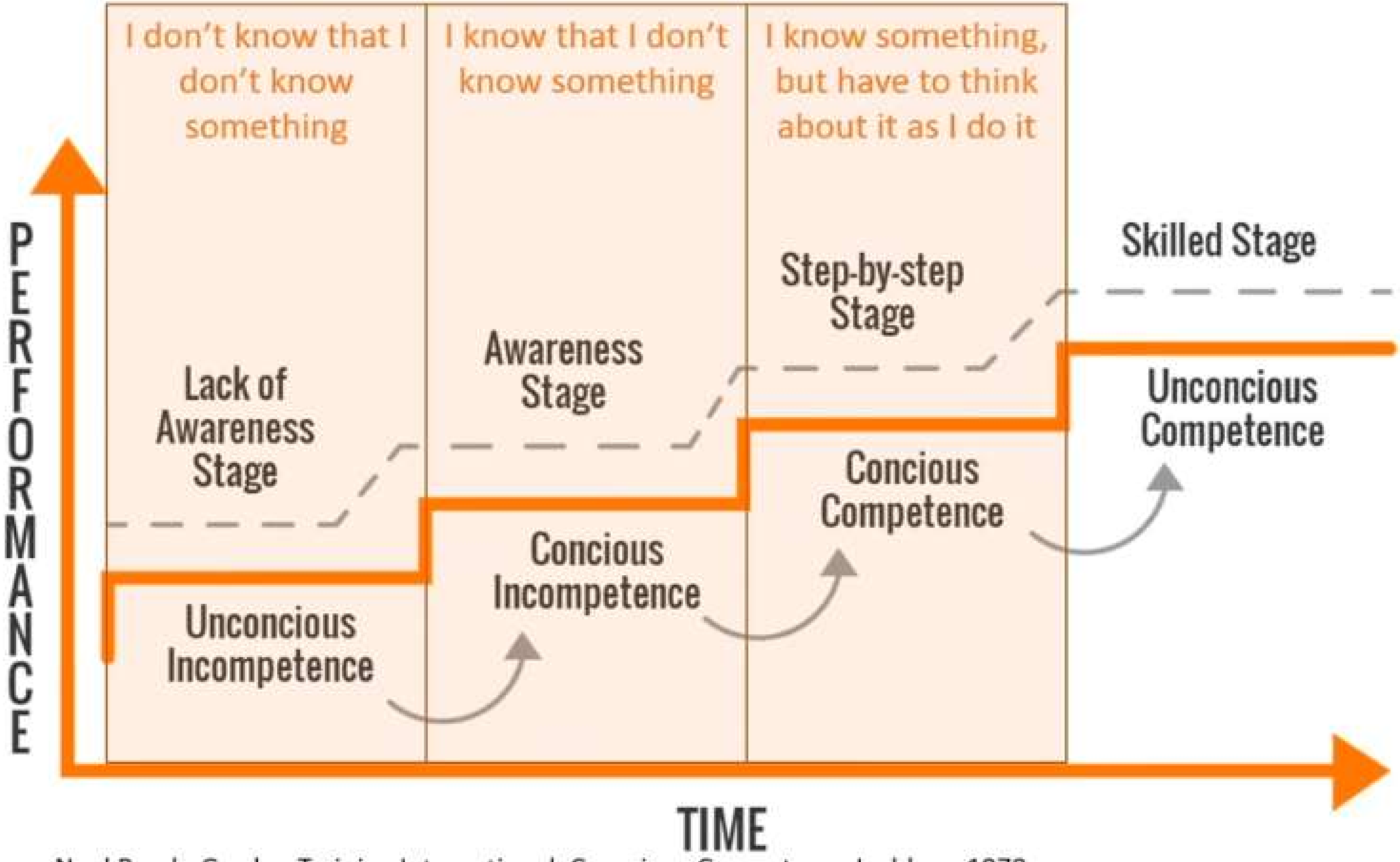
5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Employees are your last line of defense

The Four Stages of Competence

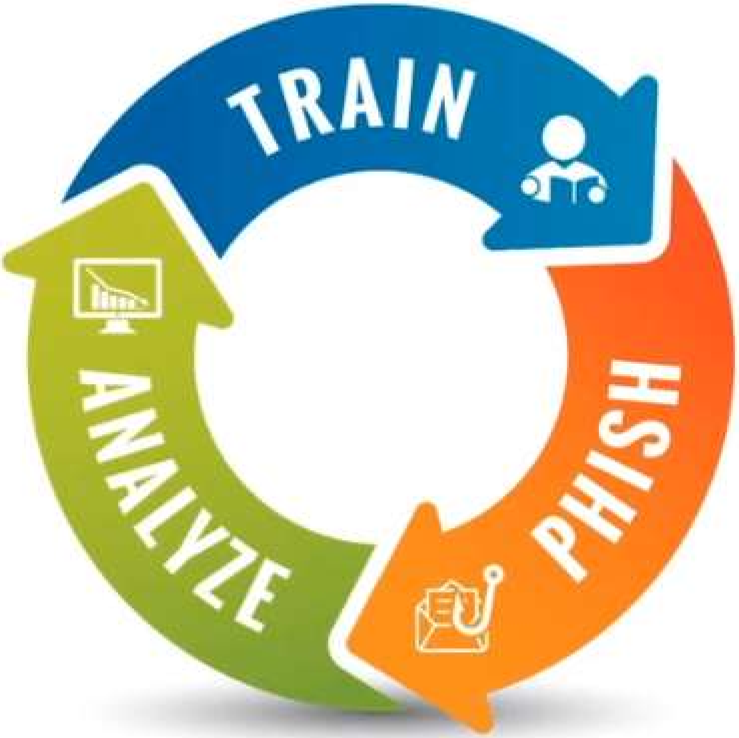


Noel Burch, Gordon Training International, Conscious Competence Ladder – 1970s

Train, Train, Train
Aware, Aware, Aware

This is the only way to attack the human factor and you can’t do this alone. This takes a team and typically an outside resource.

Phishing Awareness



Training and Awareness

- **Baseline Testing**

Test to assess your users in falling for simulated phishing attacks.

- **Train Your Users**

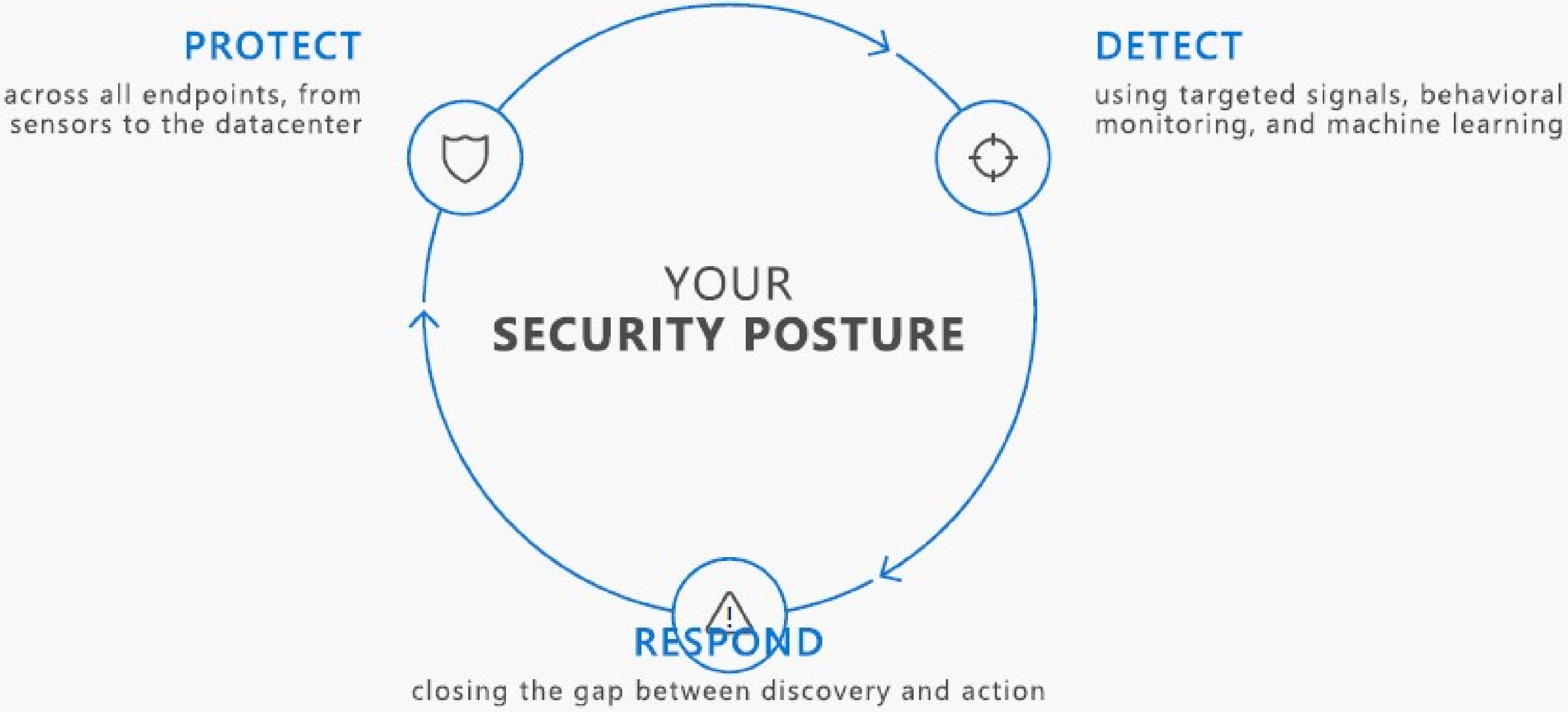
Provide real world examples and use 3rd party content providers when possible.

- **Phish Your Users**

Use tools that have templates that mimic actual companies and accounts they are familiar with.

- **See the Results and Share**

Analyze and share stats and graphs of trainings and phishing exercises with staff and leadership.



PROTECT

across all endpoints, from sensors to the datacenter

DETECT

using targeted signals, behavioral monitoring, and machine learning

YOUR **SECURITY POSTURE**

RESPOND

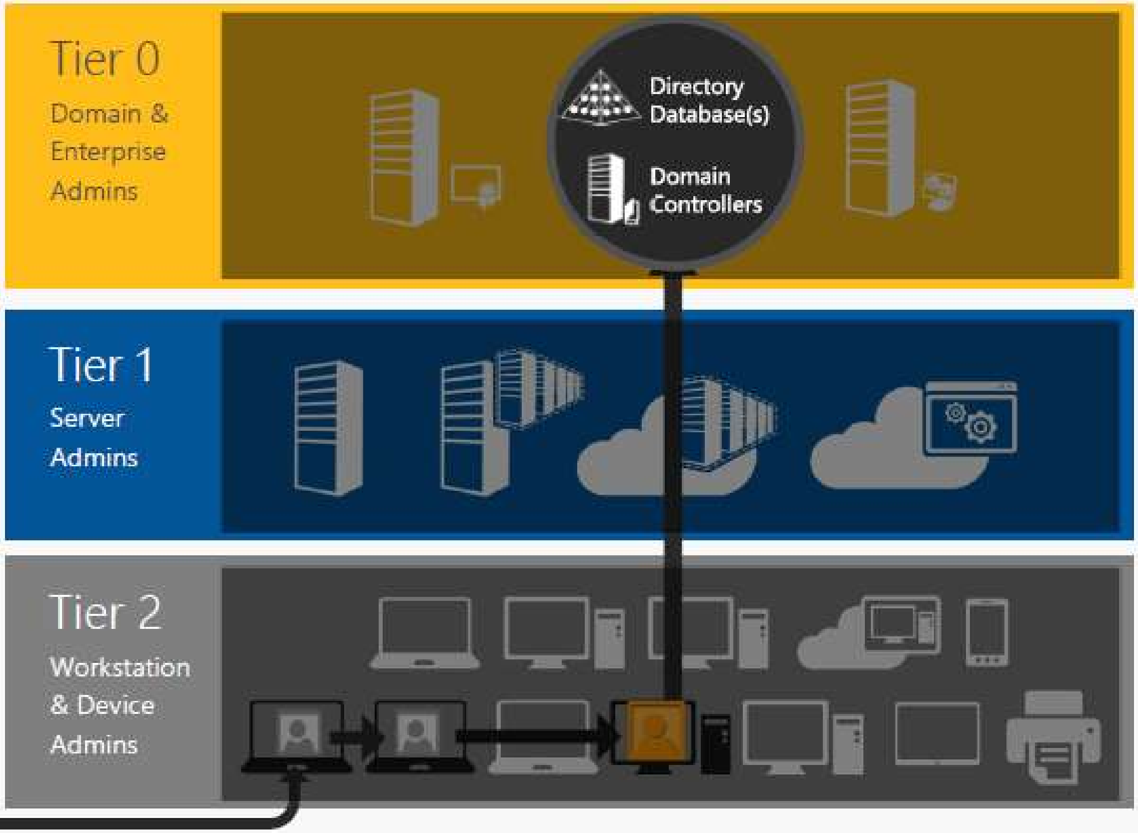
closing the gap between discovery and action

Phase 1 Critical Mitigations: Typical Attack Chain

Compromises privileged access

24-48 Hours

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Steal Credentials
   b. Compromise more hosts & credentials
3. Privilege Escalation
   a. Get Domain Admin credentials
4. Execute Attacker Mission
   a. Steal data, destroy systems, etc.
   b. Persist Presence



Tier 0
Domain & Enterprise Admins

Directory Database(s)

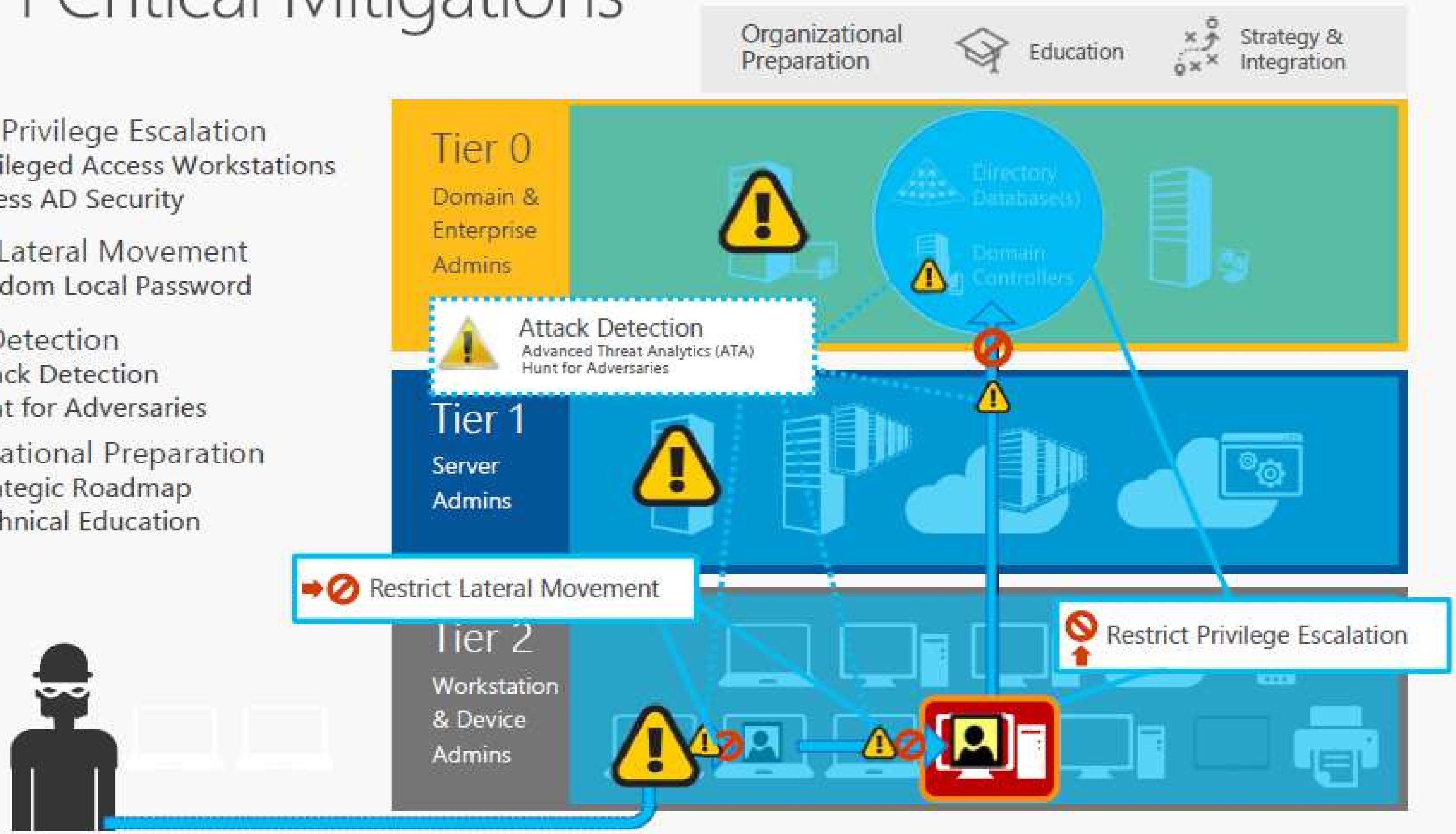
Domain Controllers

Tier 1
Server Admins

Tier 2
Workstation & Device Admins

Phase 1 Critical Mitigations

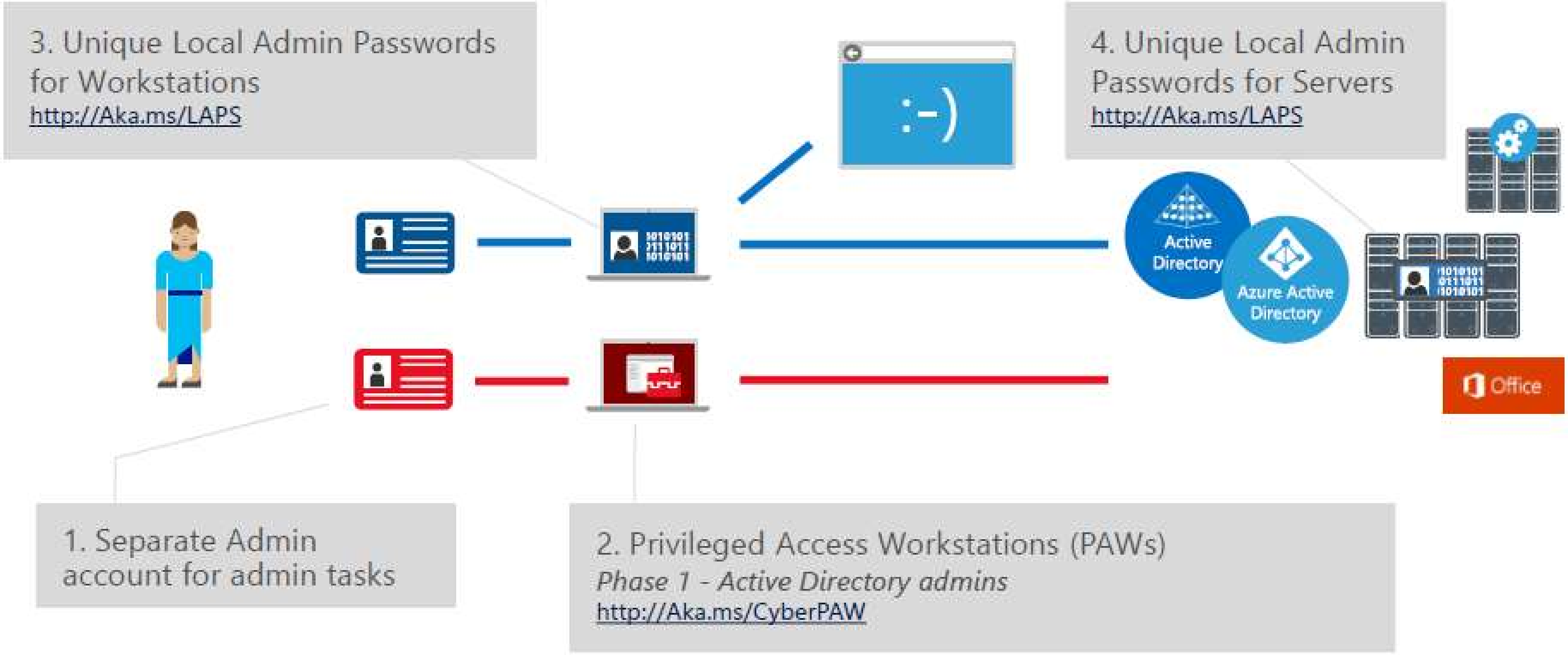
1. Restrict Privilege Escalation
   a. Privileged Access Workstations
   b. Assess AD Security
2. Restrict Lateral Movement
   a. Random Local Password
3. Attack Detection
   a. Attack Detection
   b. Hunt for Adversaries
4. Organizational Preparation
   a. Strategic Roadmap
   b. Technical Education


Organizational Preparation
Education
Strategy & Integration
Tier 0
Domain & Enterprise Admins
Directory Database(s)
Domain Controllers
Attack Detection
Advanced Threat Analytics (ATA)
Hunt for Adversaries
Tier 1
Server Admins
Restrict Lateral Movement
Tier 2
Workstation & Device Admins
Restrict Privilege Escalation

Protecting Active Directory and Admin privileges

2-4 weeks | 1-3 months | 6+ months

First response to the most frequently used attack techniques



3. Unique Local Admin Passwords for Workstations
http://Aka.ms/LAPS

4. Unique Local Admin Passwords for Servers
http://Aka.ms/LAPS

1. Separate Admin account for admin tasks

2. Privileged Access Workstations (PAWs)
Phase 1 - Active Directory admins
http://Aka.ms/CyberPAW

It takes a village to be successful in making a dent with securing our data and resources.

It can never be done alone.

Thank You!