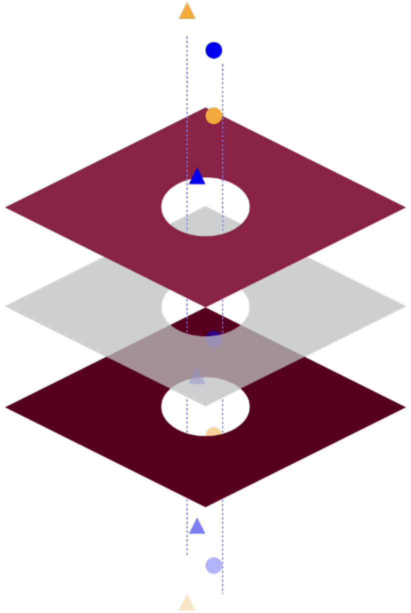
Stay Connected Security Workshop

{Month Day, Year}

Agenda

9:00 AM	WELCOME & INTRODUCTION
9:15 AM	SECURITY FUNDAMENTALS
10:15 AM	MORNING BREAK: 15-30 MINUTES
10:30 AM	MICROSOFT SECURITY REVIEW
12:30 PM	WORKSHOP WRAP-UP



Welcome & Introduction

Allen Jenkins, CISO & VP of Consulting

- 30+ years in IT / 20+ years at SyCom

- Multiple IT and Security Certifications including:
  - CISA – Certified Information System Auditor
  - GSLC – GIAC Security Leadership Certification
  - GSEC – GIAC Security Essentials Certification
  - CISSP – Certified Information Systems Security Professional

- Dual Role at SyCom as CISO & VP of Consulting
  - Make us more secure
  - Make our customers more secure

Rob Spitzer, Microsoft PAM

- 20+ years in IT / 15+ years at SyCom
- Multiple Microsoft Certifications including:
  - MCITP – Microsoft Certified IT Professional
  - MCSA – Microsoft Certified Solutions Associate
  - MCSE – Microsoft Certified Solutions Expert
  - MCTS – Microsoft Certified Technology Specialist
- Microsoft Practice Area Manager – oversees two Microsoft engineering teams and Microsoft dedicated staff

Microsoft® CERTIFIED
IT Professional

Microsoft CERTIFIED
Solutions Associate

Microsoft CERTIFIED
Solutions Expert

Microsoft® CERTIFIED
Technology Specialist

Bill Blank, Systems Engineer

- 20+ years in IT / 3+ years at SyCom

- Multiple Microsoft Certifications including:
  - MCSE – Microsoft Certified Systems Engineer
  - MCP – Microsoft Certified Professional
  - MCTS – Microsoft Certified Technology Specialist

- Systems Engineer – Microsoft Cloud and Infrastructure Team

Microsoft
MCSE

Microsoft
CERTIFIED
Professional

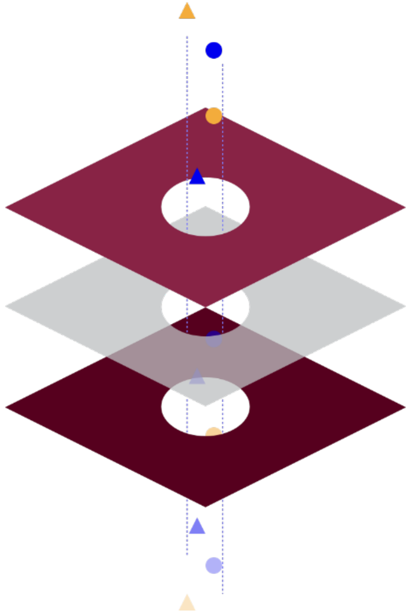
Microsoft®
CERTIFIED
Technology
Specialist

Jonathan Fox, Microsoft Adoption Specialist

Customer Immersion Experience

- 10+ years in IT / 2+ years at SyCom
- Multiple Microsoft Certifications including:
  - Microsoft Certified Service Adoption Specialist
  - Microsoft Certified Productivity Customer Immersion Experience
  - Microsoft Certified Security Customer Immersion Experience
- Microsoft Cloud and Infrastructure Team Member – specializes in Microsoft solutions, adapting them to enable achieve customer goals

Customer Introductions / Business Impact Analysis

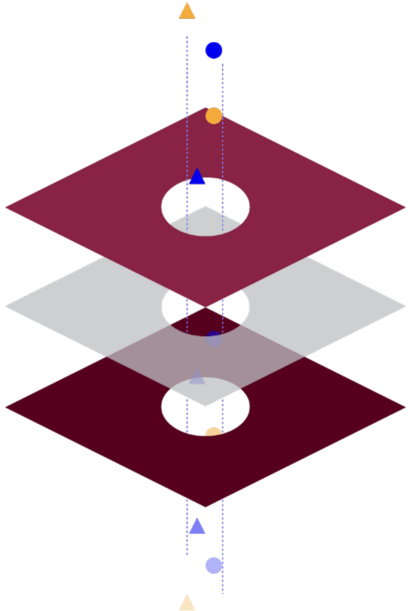


1. Name?

2. Role at organization?

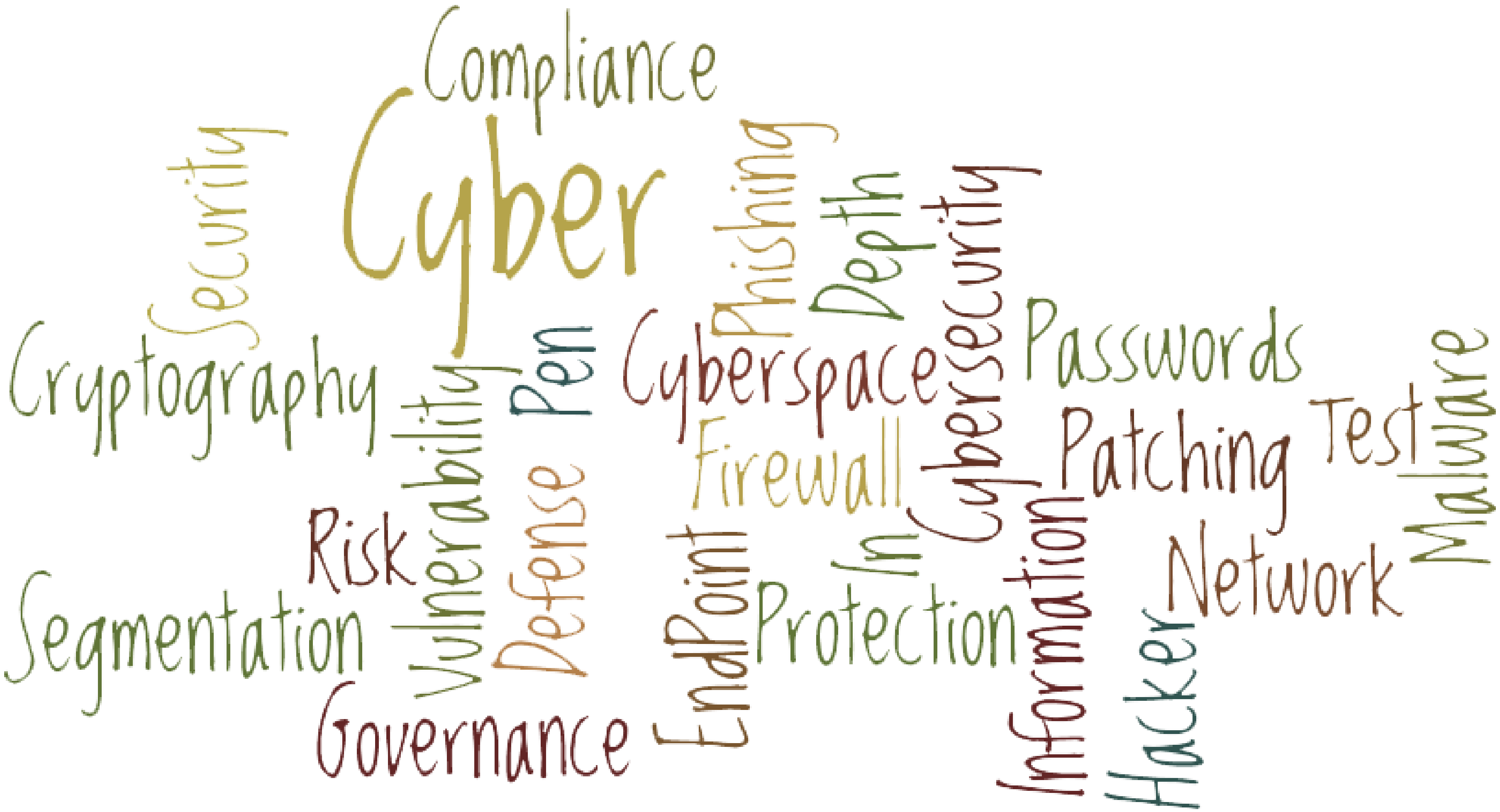
3. How long at organization?

4. What are the 2-3 most important technology tools in place?
   a) Example 1 – Accounting System
   b) Example 2 – Email
   c) Example 3 – CRM
   d) HINTS
      i. Would hurt most if unavailable or compromised
      ii. Would affect the most users



Security Fundamentals

Cybersecurity – What is it?

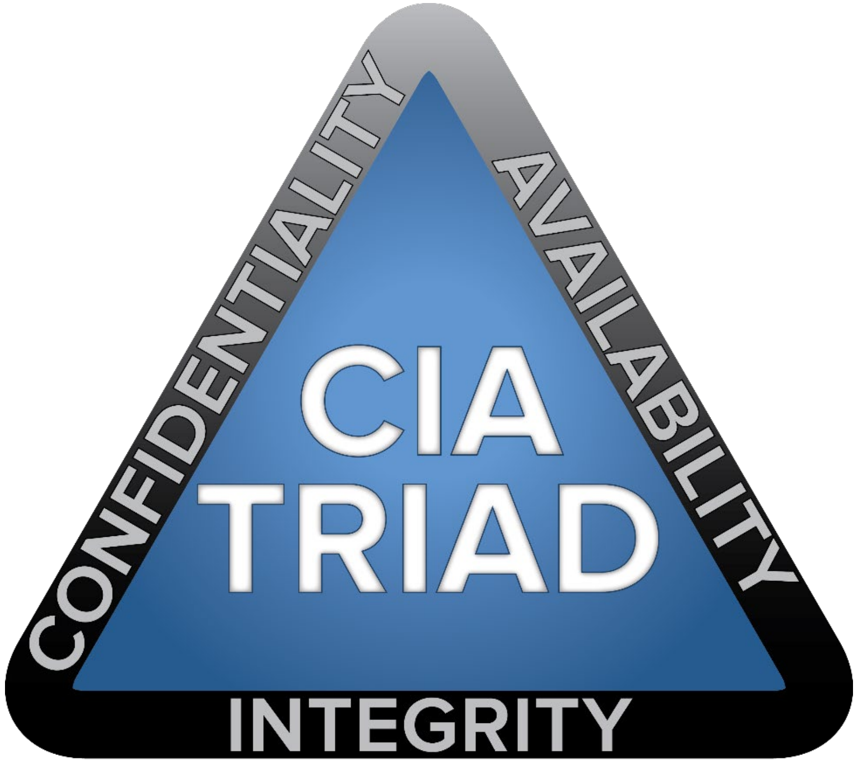


All organizations must deal with Cybersecurity.

How they deal with Cybersecurity is really what matters.

CIA

Concerns over Confidentiality, Integrity and Availability of Critical Information Technology Assets



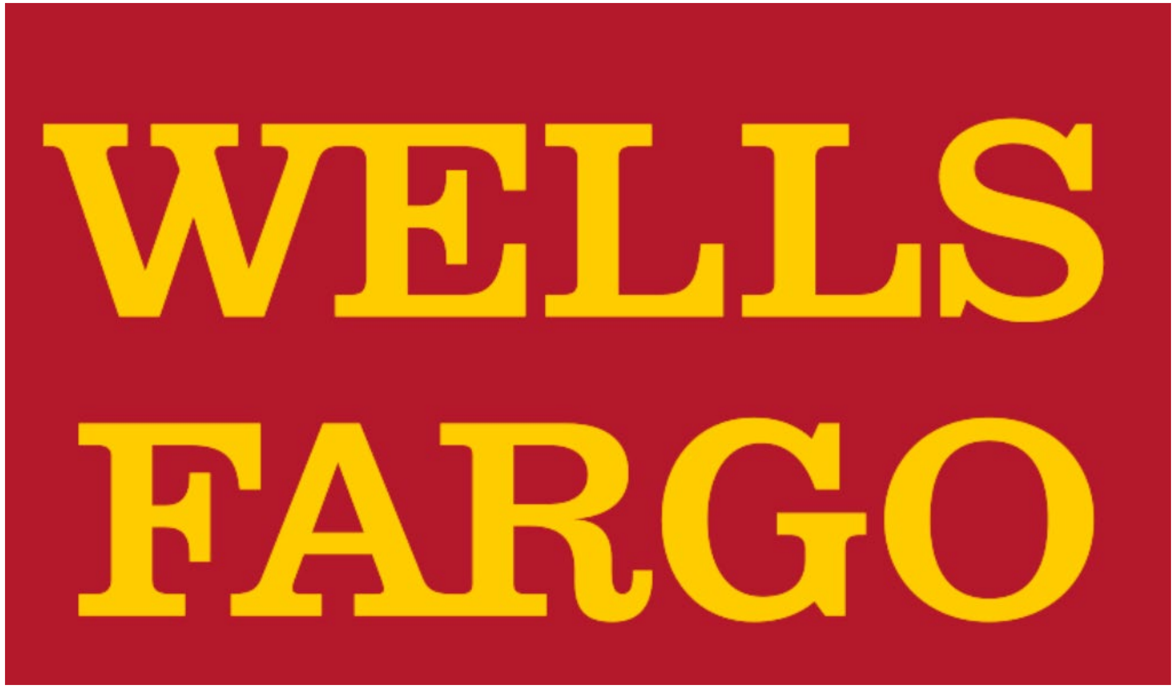
CIA Discussion - Flashcards

C, I, or A = most important?

WELLS
FARGO

CIA Discussion - Flashcards

C, I, or A = most important?

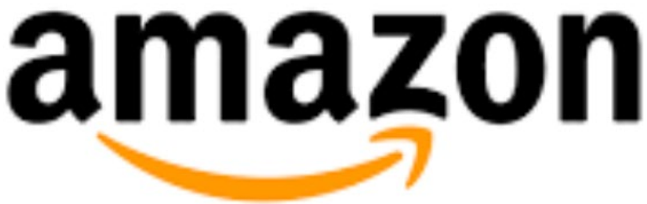


CIA Discussion - Flashcards

C, I, or A = most important?

CIA Discussion - Flashcards

C, I, or A = most important?



CIA Discussion - Flashcards

C, I, or A = most important?

CIA Discussion - Flashcards

C, I, or A = most important?

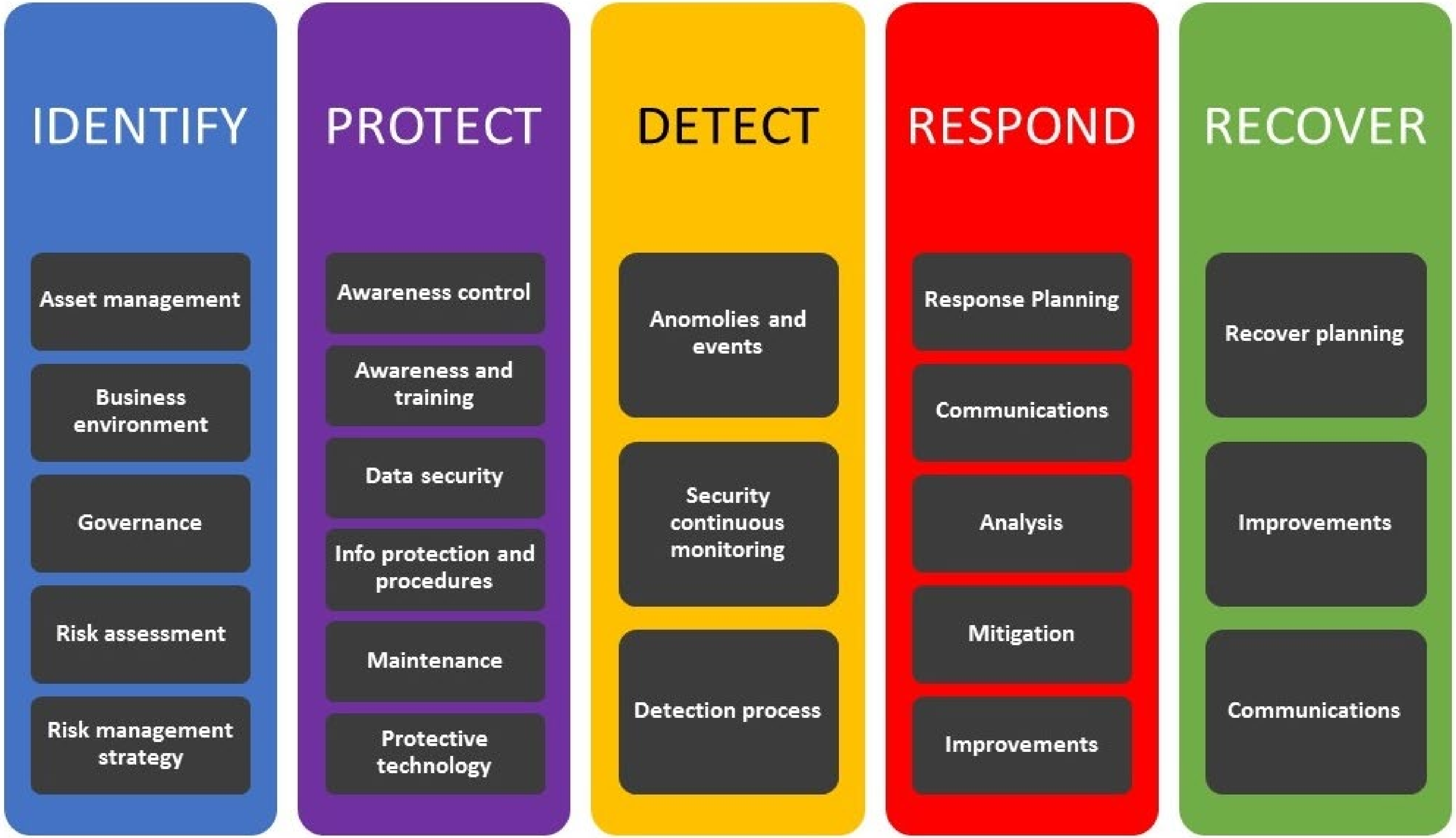
CIA Discussion - Prioritization

- ALL Important, but…which is most high priority???
- Prioritization of Approach based on what is important to organization – generally speaking…
- Confidentiality = Health Care, Government
- Integrity = Finance
- Availability = E-commerce

BIA and CIA Re-cap

1. BIA and CIA explanation re-cap
2. Review of findings and exercises
3. Discuss most important systems

NIST Cybersecurity Framework



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Awareness control
- Awareness and training
- Data security
- Info protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomolies and events
- Security continuous monitoring
- Detection process

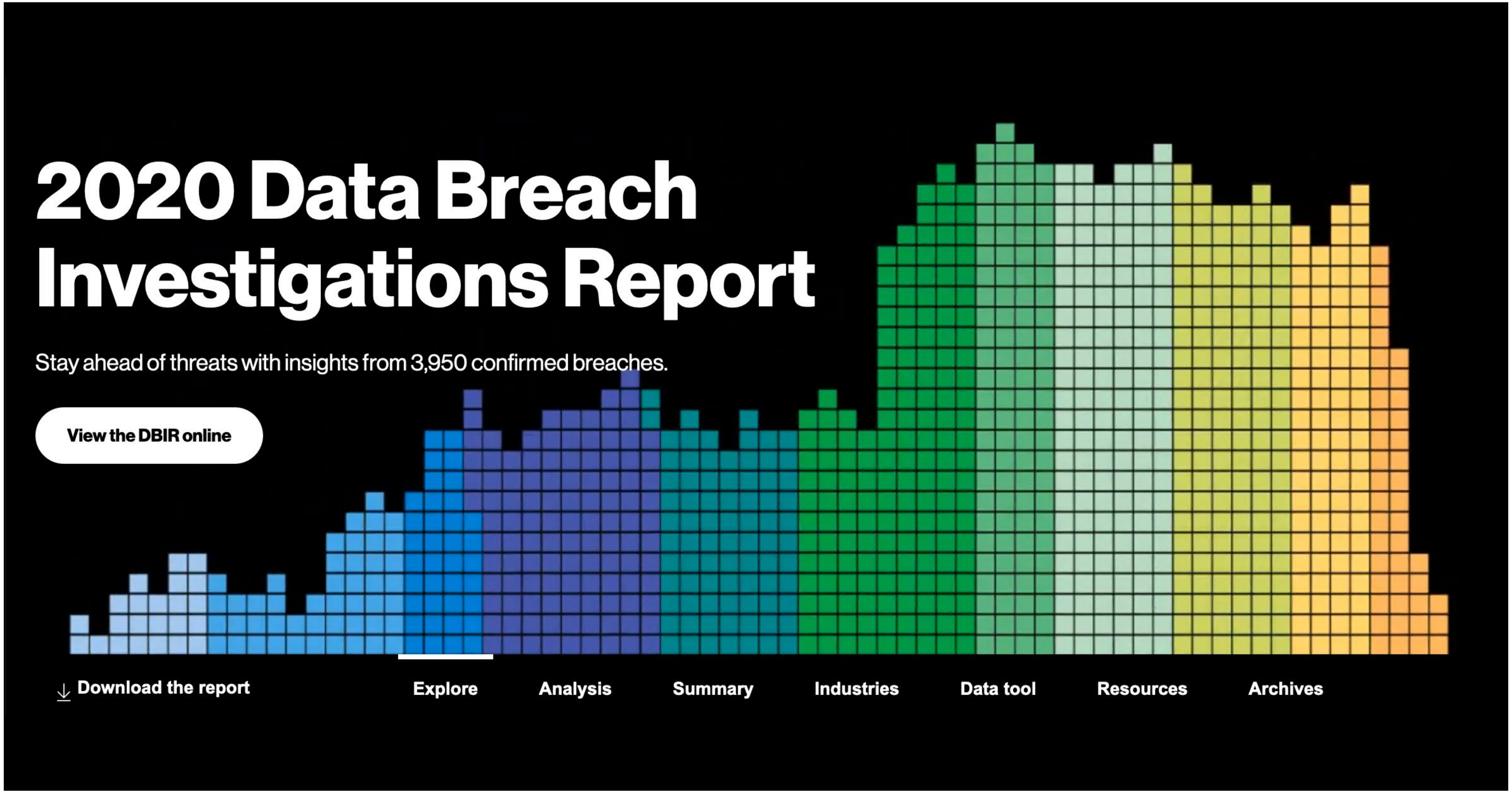
RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications

Verizon Data Breach Investigation Report



2020 Data Breach Investigations Report

Stay ahead of threats with insights from 3,950 confirmed breaches.

Verizon Data Breach Report - Top Threats

Figure 12. Top threat Action varieties in incidents (n = 23,619)

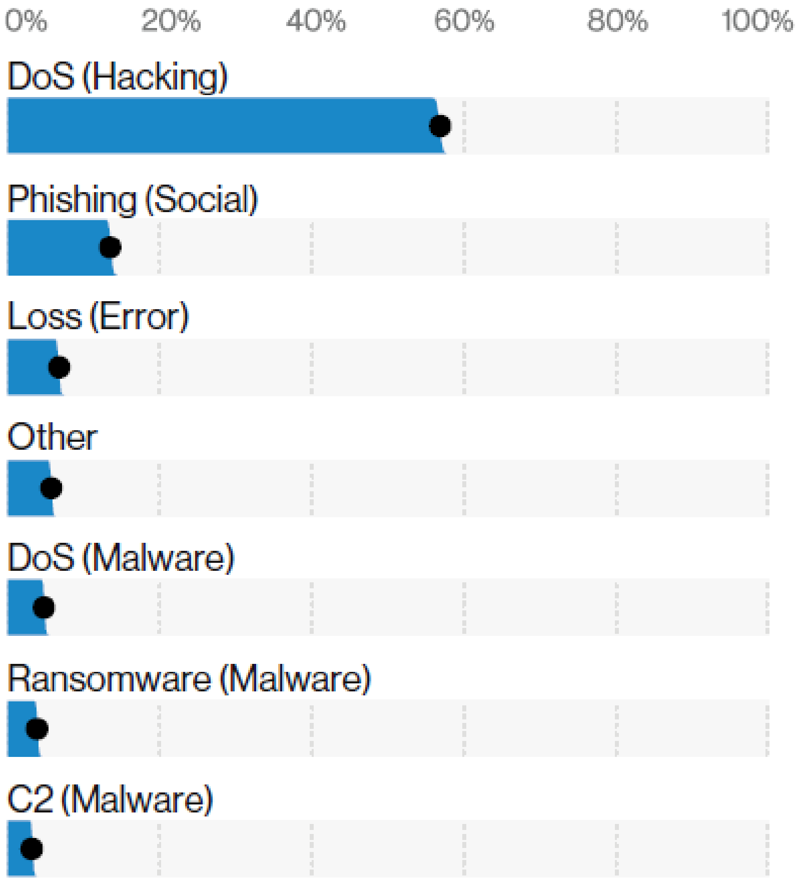
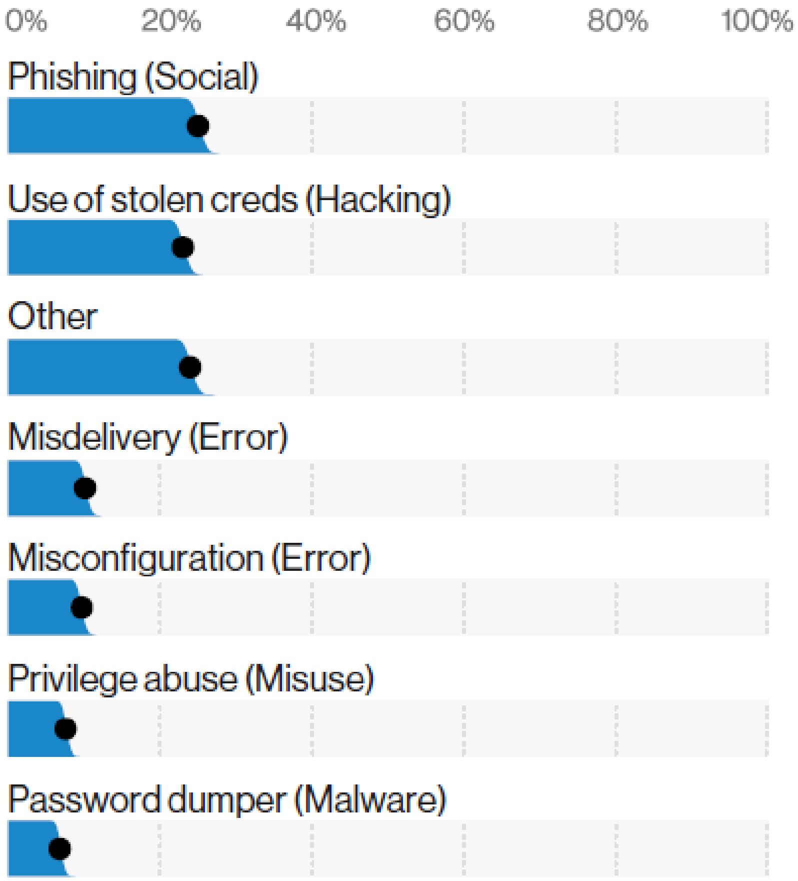
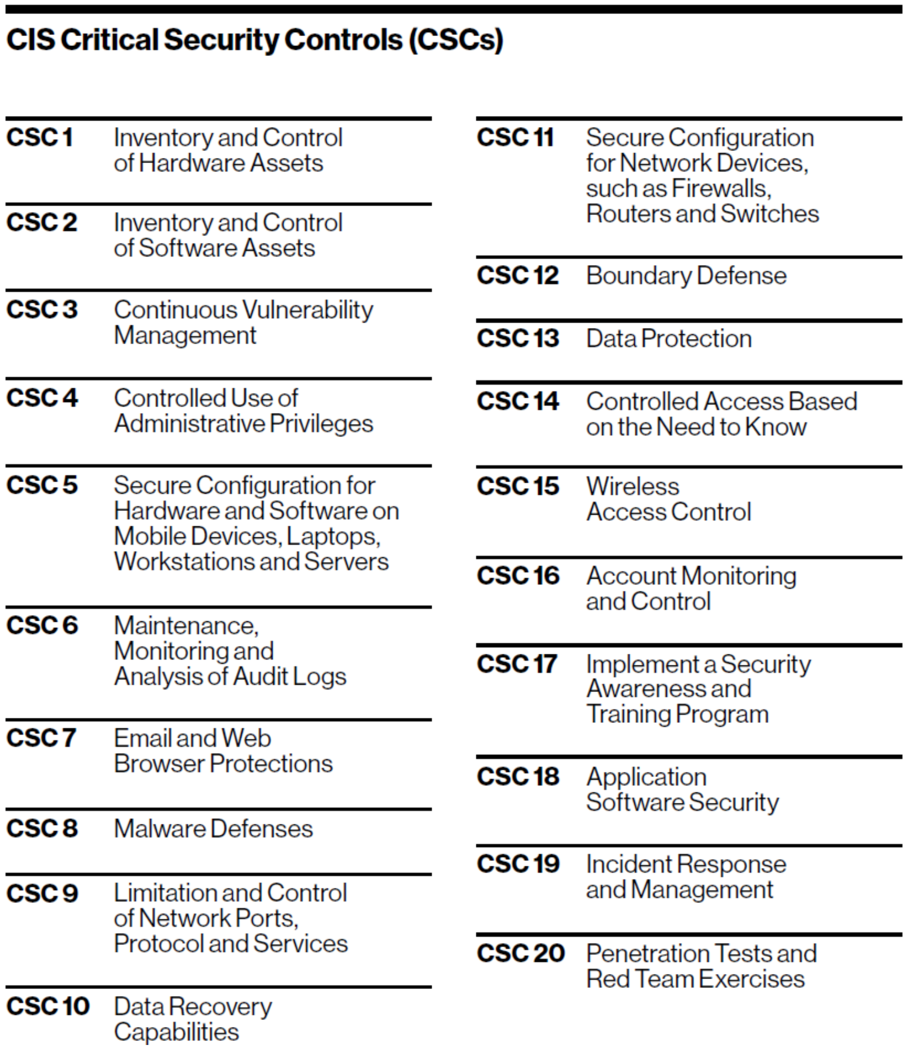


Figure 13. Top threat Action varieties in breaches (n = 2,907)



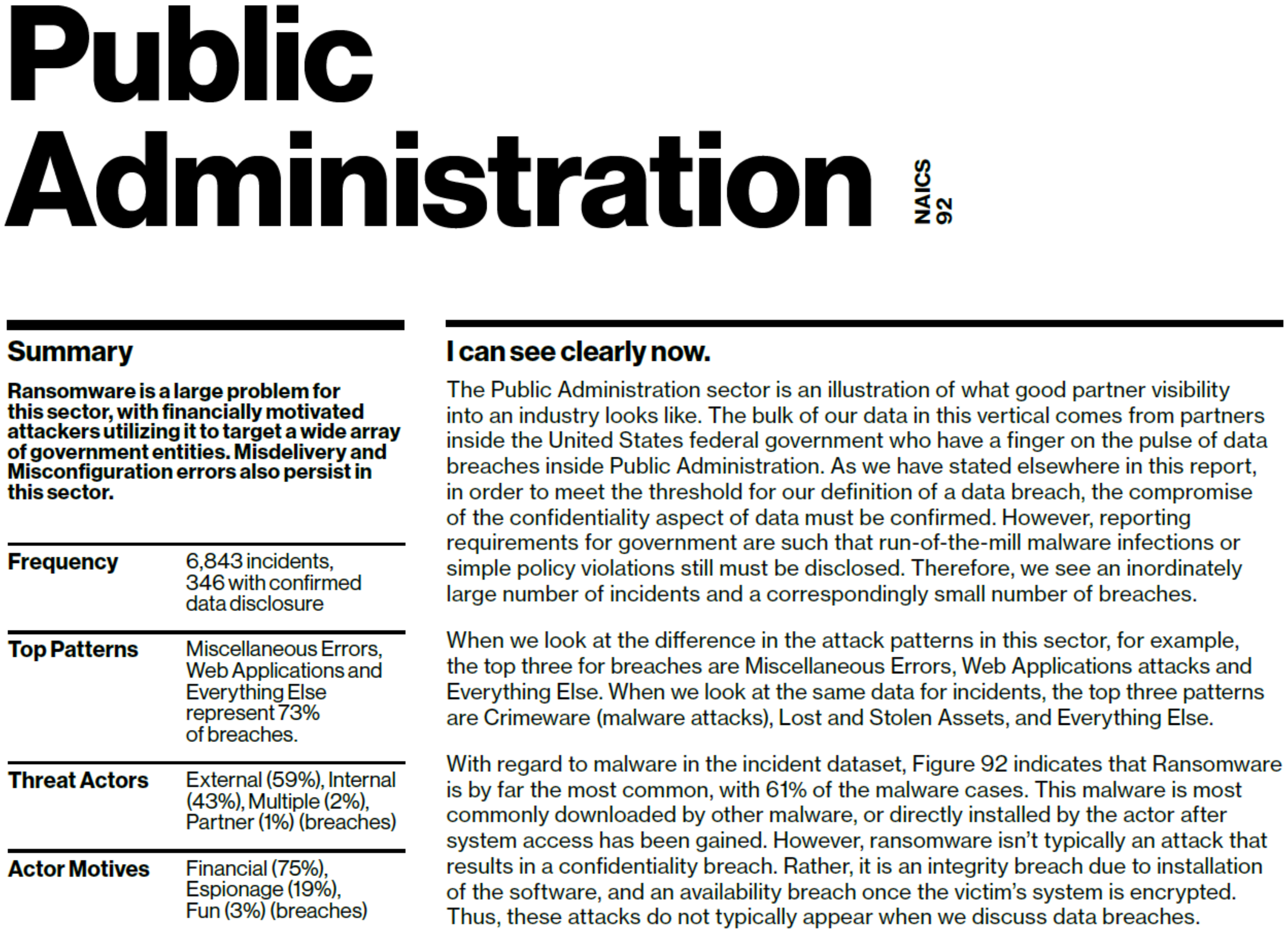
Verizon Data Breach Report – Center for Internet Security 20 CSCs



CIS Critical Security Controls (CSCs)

CSC 1	Inventory and Control of Hardware Assets
CSC 2	Inventory and Control of Software Assets
CSC 3	Continuous Vulnerability Management
CSC 4	Controlled Use of Administrative Privileges
CSC 5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 6	Maintenance, Monitoring and Analysis of Audit Logs
CSC 7	Email and Web Browser Protections
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocol and Services
CSC 10	Data Recovery Capabilities
CSC 11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account Monitoring and Control
CSC 17	Implement a Security Awareness and Training Program
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

CIS 20 and YOU (sample public sector)



Public Administration

NAICS 92

Summary

Ransomware is a large problem for this sector, with financially motivated attackers utilizing it to target a wide array of government entities. Misdelivery and Misconfiguration errors also persist in this sector.

Frequency	6,843 incidents, 346 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 73% of breaches.
Threat Actors	External (59%), Internal (43%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (75%), Espionage (19%), Fun (3%) (breaches)

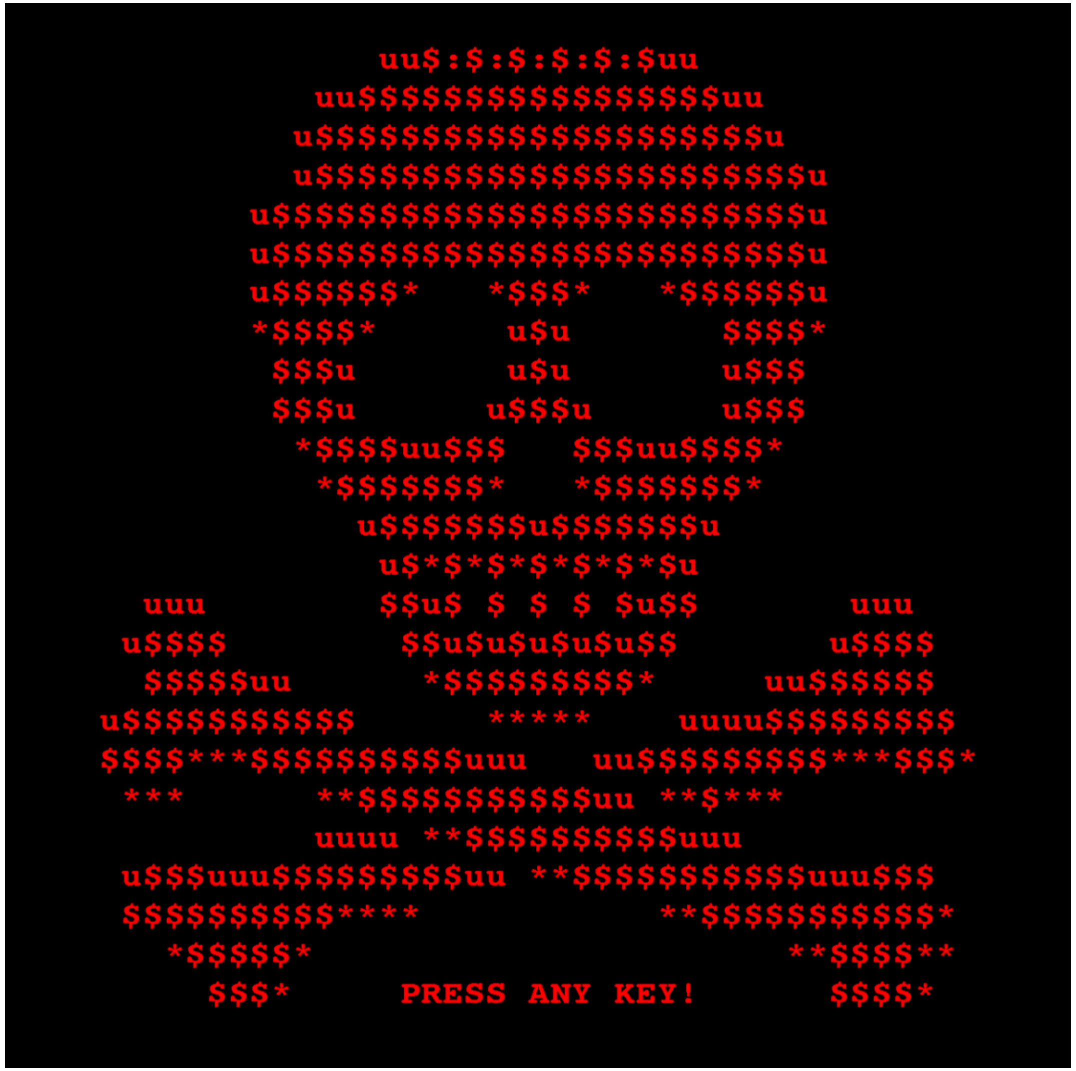
I can see clearly now.

The Public Administration sector is an illustration of what good partner visibility into an industry looks like. The bulk of our data in this vertical comes from partners inside the United States federal government who have a finger on the pulse of data breaches inside Public Administration. As we have stated elsewhere in this report, in order to meet the threshold for our definition of a data breach, the compromise of the confidentiality aspect of data must be confirmed. However, reporting requirements for government are such that run-of-the-mill malware infections or simple policy violations still must be disclosed. Therefore, we see an inordinately large number of incidents and a correspondingly small number of breaches.

When we look at the difference in the attack patterns in this sector, for example, the top three for breaches are Miscellaneous Errors, Web Applications attacks and Everything Else. When we look at the same data for incidents, the top three patterns are Crimeware (malware attacks), Lost and Stolen Assets, and Everything Else.

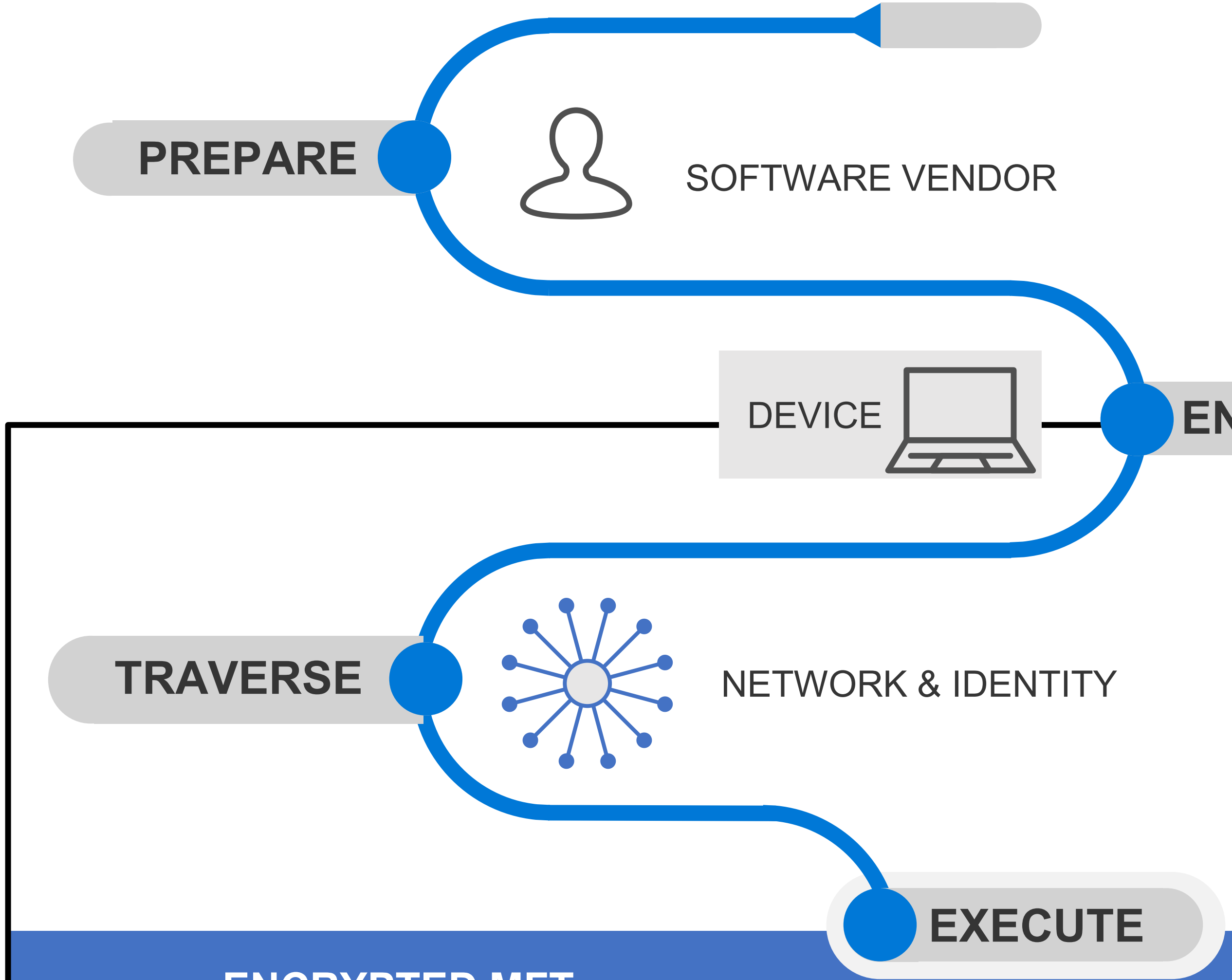
With regard to malware in the incident dataset, Figure 92 indicates that Ransomware is by far the most common, with 61% of the malware cases. This malware is most commonly downloaded by other malware, or directly installed by the actor after system access has been gained. However, ransomware isn't typically an attack that results in a confidentiality breach. Rather, it is an integrity breach due to installation of the software, and an availability breach once the victim's system is encrypted. Thus, these attacks do not typically appear when we discuss data breaches.

NotPetya



```
             uu$:$:$:$:$:$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$u$u$u$u$u$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$      *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

Anatomy of a NotPetya Attack



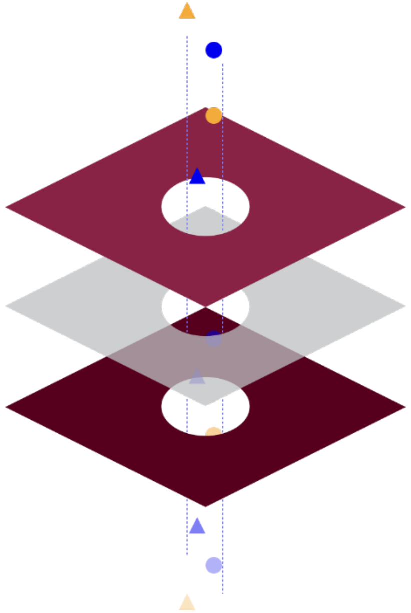
1. Attackers compromised software update infrastructure for MEDoc financial application

2. Trojan MEDoc update installed launching malicious code

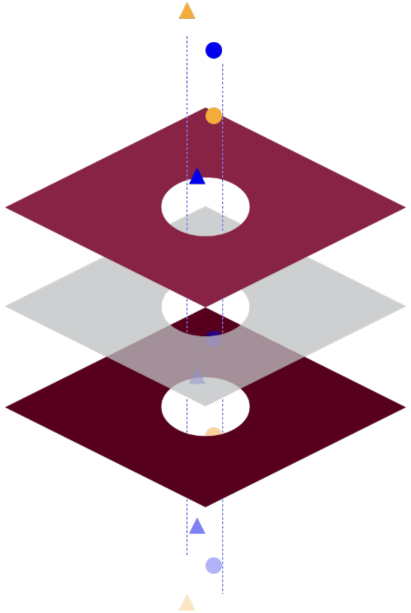
3. Multiple techniques used to spread rapidly:
   - MS17-010 Vulnerability (released March 2017) (EternalBlue/NSA)
   - Credential theft and impersonation (MimiKatz)

- **ENCRYPTED MFT**
- **MADE SYSTEMS UNBOOTABLE**

- **CLEARED WINDOWS EVENT LOGS**
  - ***JUST STANDARD PRACTICE?***
  - ***HIDING OTHER ACTIONS?***

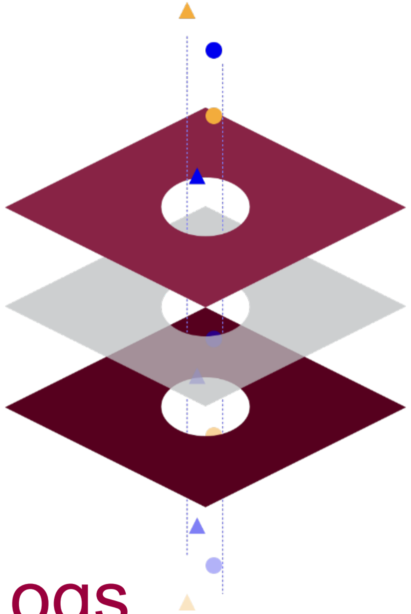


10 Minute Break



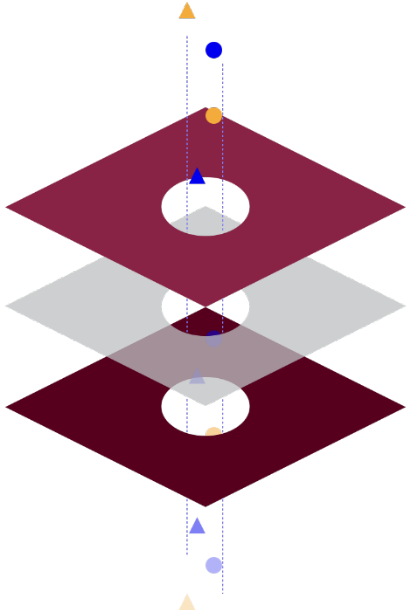
Microsoft Security Review

CIS to MS Mappings



- **CIS 3** – Continuous Vulnerability Management
- **CIS 4** – Controlled Use of Administrative Privileges
- **CIS 5** – Secure Configuration of Hardware and Software
- **CIS 6** – Maintenance, Monitoring, and Analysis of Audit Logs
- **CIS 12** – Boundary Defense
- **CIS 13** – Data Protection
- **CIS 17** – Implement a Security Awareness and Training Program

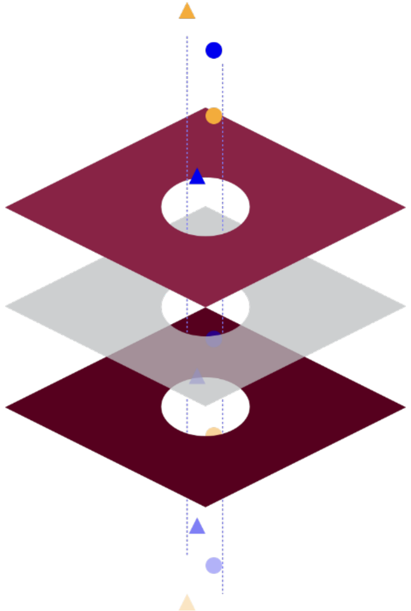
Microsoft Tools - CIS3



- Windows Update
- Secure Score
- Baseline Security Templates
- Azure Security Center

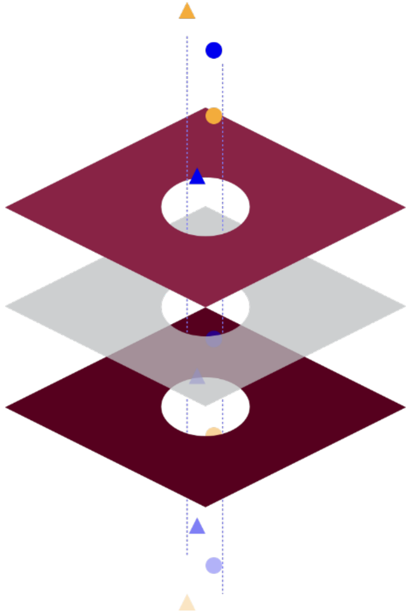
Microsoft Tools – CIS4

- Azure Multi-Factor Authentication (MFA)
- Separate Admin Accounts
- Privileged Identity Management
- Just-in-Time Access

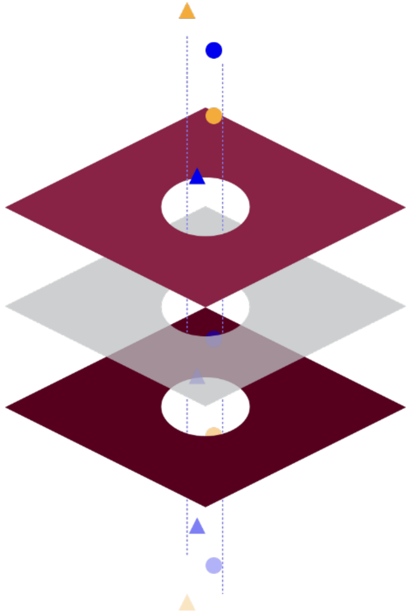


Microsoft Tools – CIS5

- Microsoft Intune
- Windows Defender ATP
- Baseline Security Templates
- Azure Security Center
- Azure Update Manager

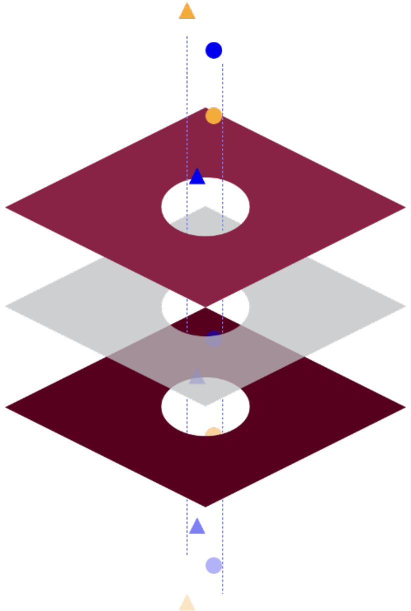


Microsoft Tools – CIS6



- Azure Advanced Threat Protection (ATP)
- Azure Sentinel

Microsoft Tools – CIS12

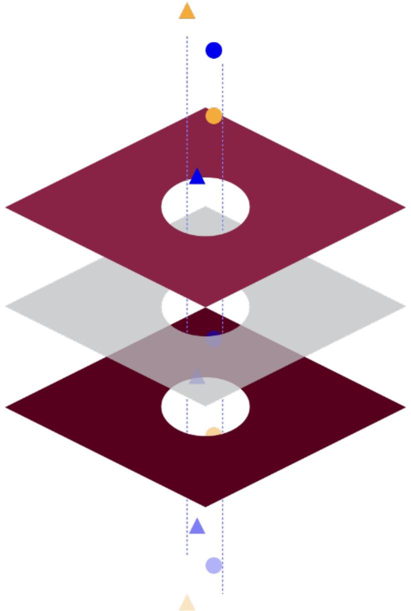


- Exchange Online Protection
- SPF and DKIM
- Office 365 Advanced Threat Protection (ATP)
- Azure Single Sign On (SSO)
- Conditional Access
- Cloud App Security

Microsoft Tools – CIS13

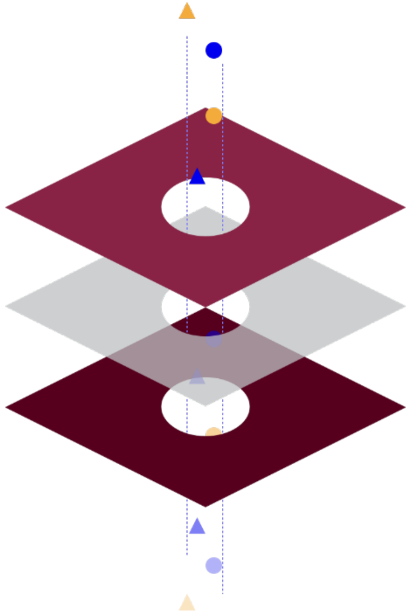
- SharePoint Online / OneDrive for Business
- Data Loss Prevention (DLP)
- Windows Virtual Desktops (WVD)
- Azure Information Protection
- Customer Lockbox
- Cloud App Security
- Azure Backup
- Azure Site Recovery

Microsoft Tools – CIS17



- Office 365 Advanced Threat Protection (ATP)
- Compliance Manager

Assessment Wrap-Up / Q&A



- What Questions does customer have?
- What gaps in Controls exist?
- What are logical next steps?

Connecting More Than Technology

SyCom