Cybersecurity Essentials for Public Health Leadership – A Jargon-free Discussion of Cybersecurity Concepts

Jared Warner, MEM, REHS
Highland County Health Commissioner
AOHC Conference, September 2024

Rural Health Commissioner Job Duties

November 2024 will mark 10 years as Health Commissioner in Highland County

- Job duties could also include:
  - Toilet valve repair
  - Tail light replacement
  - Traffic control
  - Escaped bat catcher
  - Raccoon head remover

IT Support and Cybersecurity Specialist

Workforce Development Grant

- Problem: I needed to make cybersecurity decisions, without having the necessary background and framework to make those decisions.
- Workforce Development Funds became available in 2023
- Solution: 6-month Cybersecurity Bootcamp at The Ohio State University, College of Engineering
  - 3 days a week, 6PM to 9PM each day
- CompTIA Security+ Certification: Industry standard entry level certification

Alternative Presentation Title: What I Learned at Computer Camp

- AI generated image of adult going to computer camp.

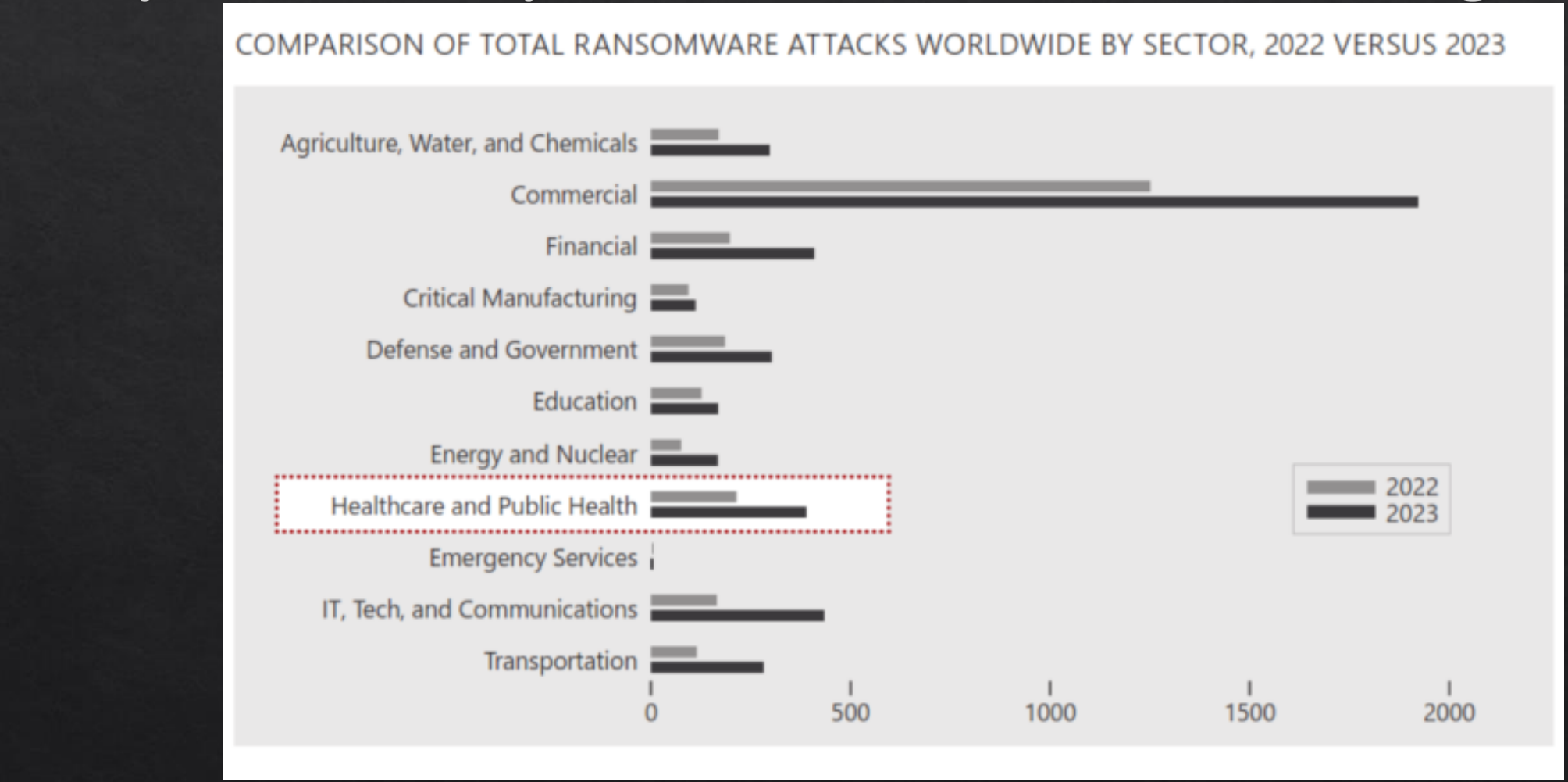
Cybersecurity no longer just secures computers, it secures society – Mikko Hyppönen

Recent Cybersecurity Headlines

Why should Public Health leaders be paying attention to cybersecurity?

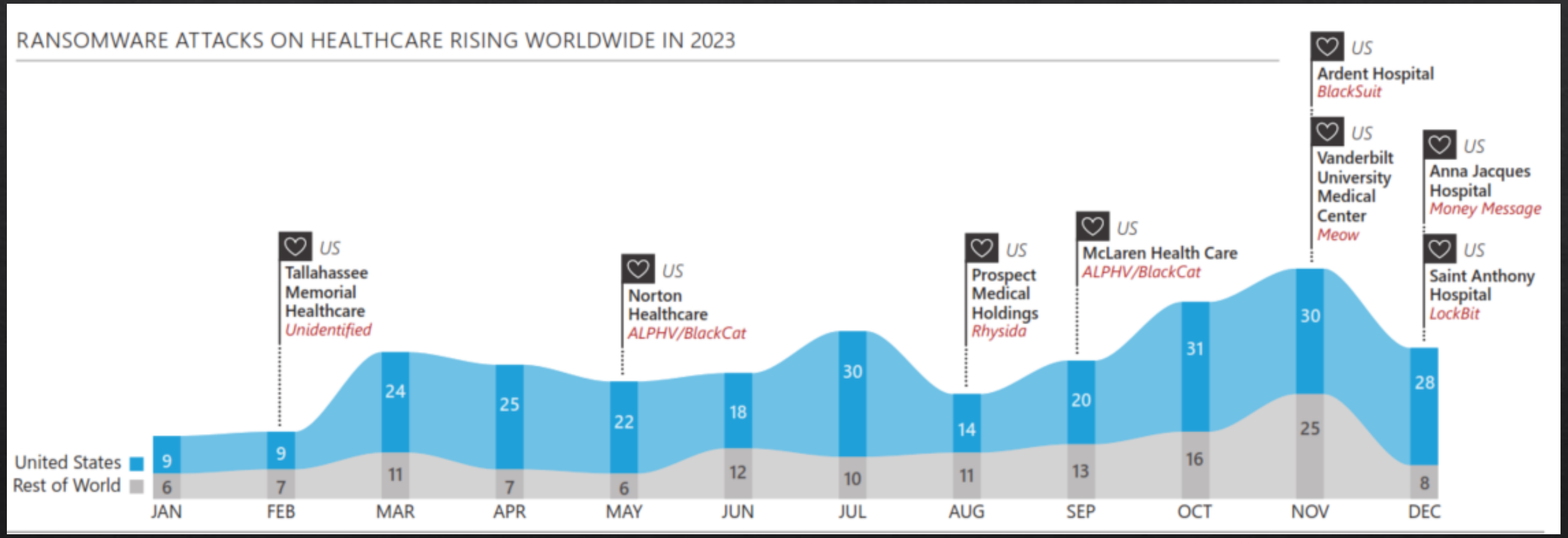
- 2024 – Change Healthcare – Ransomware and Data Breach
- 2024 – County of Los Angeles Public Health – Phishing Attack and Data Breach
- 2024 – City of Cleveland and City of Columbus – Ransomware
- 2024 – Florida Department of Health – Ransomware and Data Breach

Cybersecurity Attacks on Healthcare Agencies

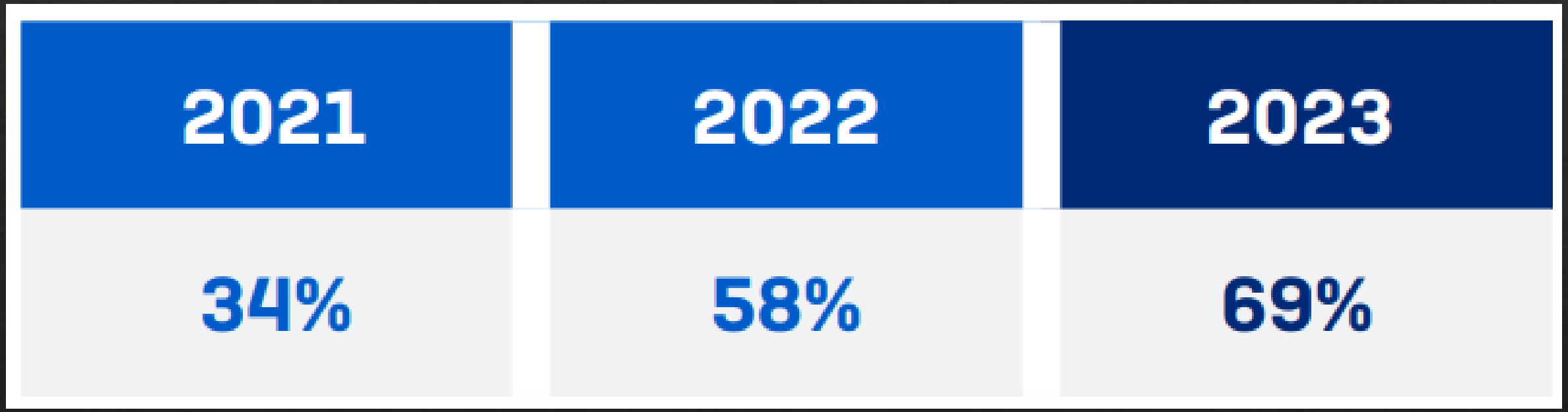


https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf

Cybersecurity Attacks on Healthcare Agencies



2023 Ransomware Attacks on State and Local Government



- Sophos 2023 Government Ransomware Report
- https://assets.sophos.com/X24WTUEQ/at/tjrvgbkkv8vppwgsskqqpg/sophos-state-of-government-2023-wp.pdf

Learning Objectives

- **Identifying Threats and Vulnerabilities:** Identify common cybersecurity threats, such as malware, phishing, and ransomware, and potential vulnerabilities within public health systems.
- **Identifying Cybersecurity Frameworks and Core Concepts:** Identify core concepts and frameworks for cybersecurity risk management, preparedness, and response that each public health leader should understand.
- **Promote a Culture of Cybersecurity:** Encourage public health leaders to foster a culture of cybersecurity within their organizations, and identifying some key concepts and takeaways that every public health agency should be implementing in their organization.

Contents

- Identifying Threats and Vulnerabilities
- Identifying Cybersecurity Frameworks and Core Concepts
- Promoting a Culture of Cybersecurity
- What Next?
- Questions and Answers

Identifying Threats and Vulnerabilities

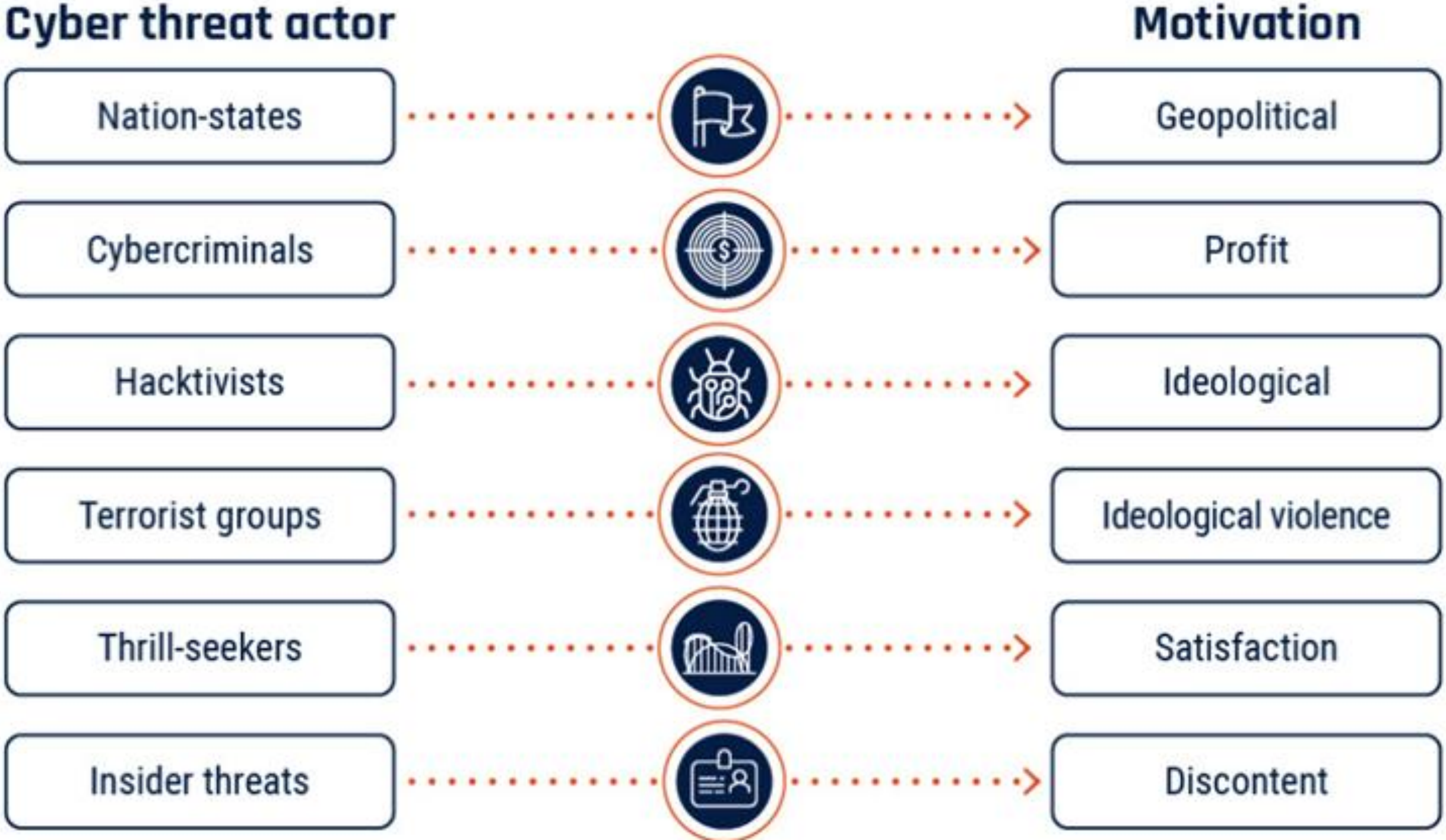
Who Attacks and How Attacks Happen

- Who are the people and organizations that commit cyber crimes
- What are their motivations?
- What are the most common attack methods for healthcare and government organizations?

- We need to understand these concepts in order to built strong information systems.

Where do cybersecurity threats originate?

- State Actors – hostile nations who disrupt infrastructure, steal data, or gain strategic advantages
- Criminal Organizations – cyber attacks for financial gain.
- Hacktivists – cyber attacks to promote causes, draw attention to their organizations, or express dissent.
- Terrorist Groups – Sometimes identified as a separate group from hacktivists, but with similar political or cultural objectives.
- Insider Threats – Trusted individuals who abuse their access to sell data, or otherwise damage company systems (sometimes accidentally!).
- Thrill Seekers – Hackers of various skill who are most interested in seeing if they can access vulnerable systems.


Cyber threat actor
Motivation
Nation-states
Geopolitical
Cybercriminals
Profit
Hacktivists
Ideological
Terrorist groups
Ideological violence
Thrill-seekers
Satisfaction
Insider threats
Discontent

WANTED BY THE FBI

CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE

Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud

Wang Qian

Xu Ke

Liu Lei

Wu Zhiyong

CAUTION

WANTED BY THE FBI

SERGEY ALEKSANDROVICH MORGACHEV

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Aggravated Identity Theft; Conspiracy to Commit Money Laundering

Siemens Contractor Pleads Guilty to Planting 'Logic Bomb' in Spreadsheets

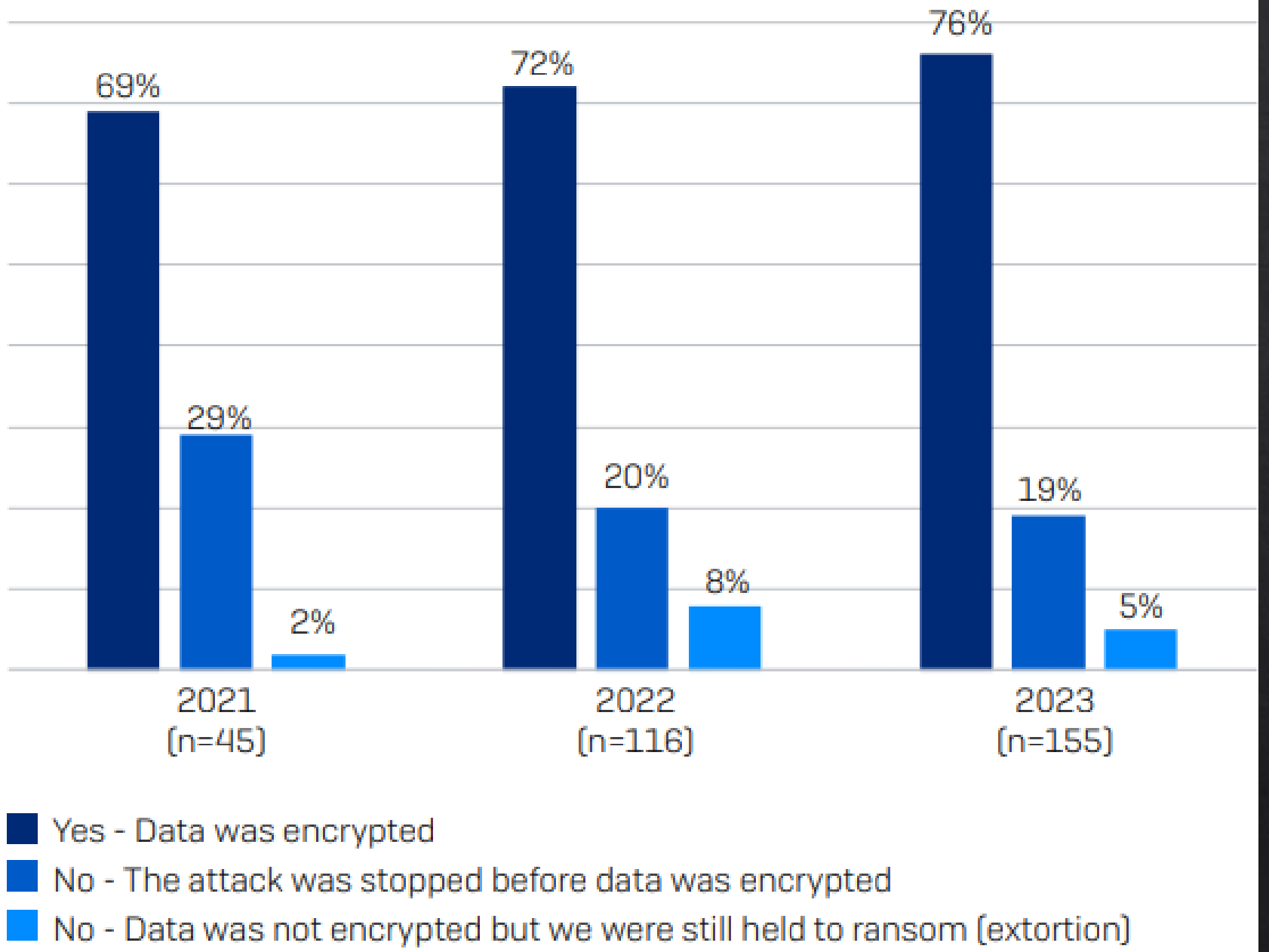
Jul 24, 2019 Wang Wei

An 11-year-old changed election results on a replica Florida state website in under 10 minutes

Nation Aug 12, 2018 5:00 PM EDT

Most Common Attack Methods for Healthcare and Government

- Phishing
  - Whaling
  - Smishing
  - Vishing
  - Spear Phishing
- Ransomware – Encryption of computer data to lock out legitimate users. Decryption key is then offered to the system owner, for a price.



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack?
Selection of answer options. Base numbers in chart

	STATE AND LOCAL GOVERNMENT	CROSS-SECTOR AVERAGE
Got data back	99%	97%
Used backups to restore data	75%	70%
Paid the ransom to get data back	34%	46%
Used other means to get data back	2%	2%

Did your organization get any data back? Yes, we used backups to restore the data; Yes, we paid the ransom and got data back; Yes, we used other means to get our data back. n=1,497 (cross-sector); n=118 (state and local government).

Most Common Attack Methods for Healthcare and Government

- Credential Stuffing and Password Spraying – Once attackers have a list of company emails, they can try to log into systems with emails and commonly used passwords or known stolen passwords to see if any fit. This is automated.
- DDoS – Distributed Denial of Service Attacks – Overwhelming a system by flooding it with requests for resources.
- Exploiting Known Vulnerabilities – Systems with known vulnerabilities can be targeted, often with automated processes, allowing system access. These could be older systems, or newly discovered vulnerabilities in new systems.

Hacking-as-a-service

- Significant rise of HaaS and Ransomware-as-a-service recently, which lowers the technical threshold needed to carry out cyber attacks.
- HaaS vendors work as consultants and software engineers, and usually require a percentage of any ransomware payment in exchange for their services and use of their platforms.
- Some HaaS offer subscription plans in exchange for access to online DDoS, phishing, and ransomware platforms.

Other Attack Types

- There are many other attack methods that could impact an agency
  - Rubber Ducky
  - Typo Squatting
  - QR Phishing
  - SQL Injection
  - Water Hole Attacks
  - And More!

QR Phishing

City official parking sticker should have parksmarter.com

○ City Official Parking Sticker

Fraudulent sticker can be identified here with parksmarter.app

X Fraudulent Parking Sticker


://PAYFORYOURPARKING.CO
MBER 2004
VAILABLE
PARKING
OF CON

Social Engineering

- Social engineering: “Any act that influences a person to take an action that may or may not be in their best interest.”
- Used to obtain sensitive information, gain unauthorized access, disrupt operations, or commit fraud
- Most breaches involve a human element – 68% of all successful attacks involved human interaction at some level (Verizon DBIR)


- Defense in Depth
- Patched systems
- 24/7 monitoring/ alerting
- Annual compliance auditing
- Experienced IT/ Security team
User clicks on an email

Other Vulnerabilities in Healthcare and Government

- Legacy Systems
- Limited Access to IT Services and Expertise
- Limited Budgets for Cybersecurity Initiatives

AOHC

Association of Ohio Health Commissioners, Inc.

Wireless Internet Access

Scan this QR code to connect to free high-speed internet for the conference!

Highland County Health Department

Home / Contact / Administration / Public Health Nursing / Environmental Health / Vital Statistics & Birth And Death Records / Emergency Planning / Health Education / News And Updates / Calendar / Search Website

AOHC

CONNECT TO AOHC CONFERENCE WIFI

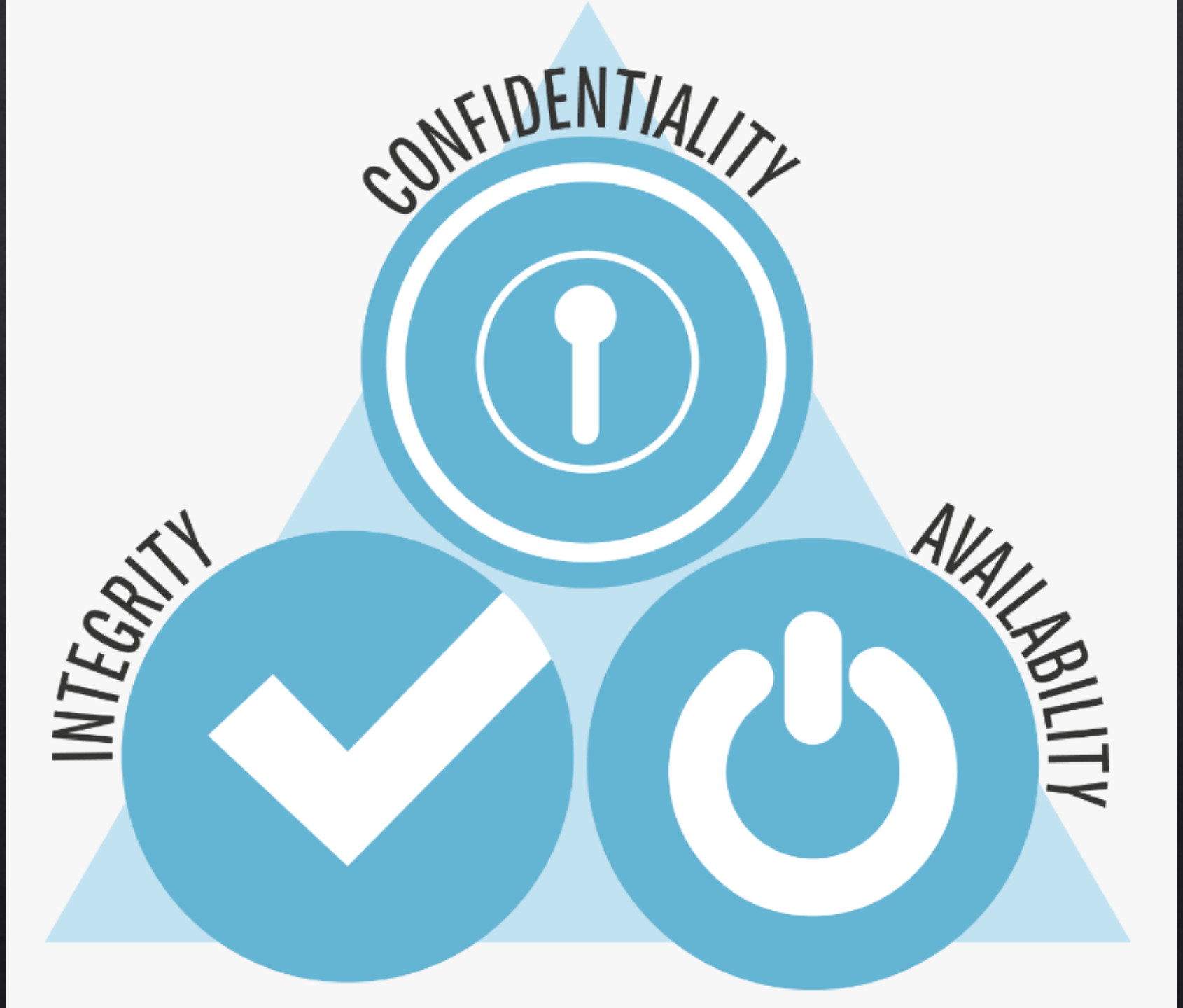
Identifying Cybersecurity Frameworks and Core Concepts

CIA Triad

A simple risk management framework for cybersecurity

- **Confidentiality** – Can I protect my information and make sure it is only accessible to authorized people?
- **Integrity** – Can I trust information to be true, accurate, and trustworthy?
- **Availability** – Can I get to my information when I need it?

- Essentially all cybersecurity risk management tools will address one or more of these areas


CONFIDENTIALITY
INTEGRITY
AVAILABILITY

Multifactor ID Concepts

- Allowing a log in using only a user name and password is risky.
- MFA Could be a combination of several things:
  - Something you know – Password, Passphrase, PIN
  - Something you are – Retinal Scan, Fingerprint Scan, Facial Recognition, Gait Analysis
  - Something you have – One-Time Password, Smart Card, Physical Key, USB Key
- MFA Bombing / MFA Fatigue – Social engineering attack where a user is constantly bombarded with authentication requests until they access the log in.

AAA

- Authentication – Who are you?
- Authorization – What are you allowed to do?
- Auditing – What are you doing?

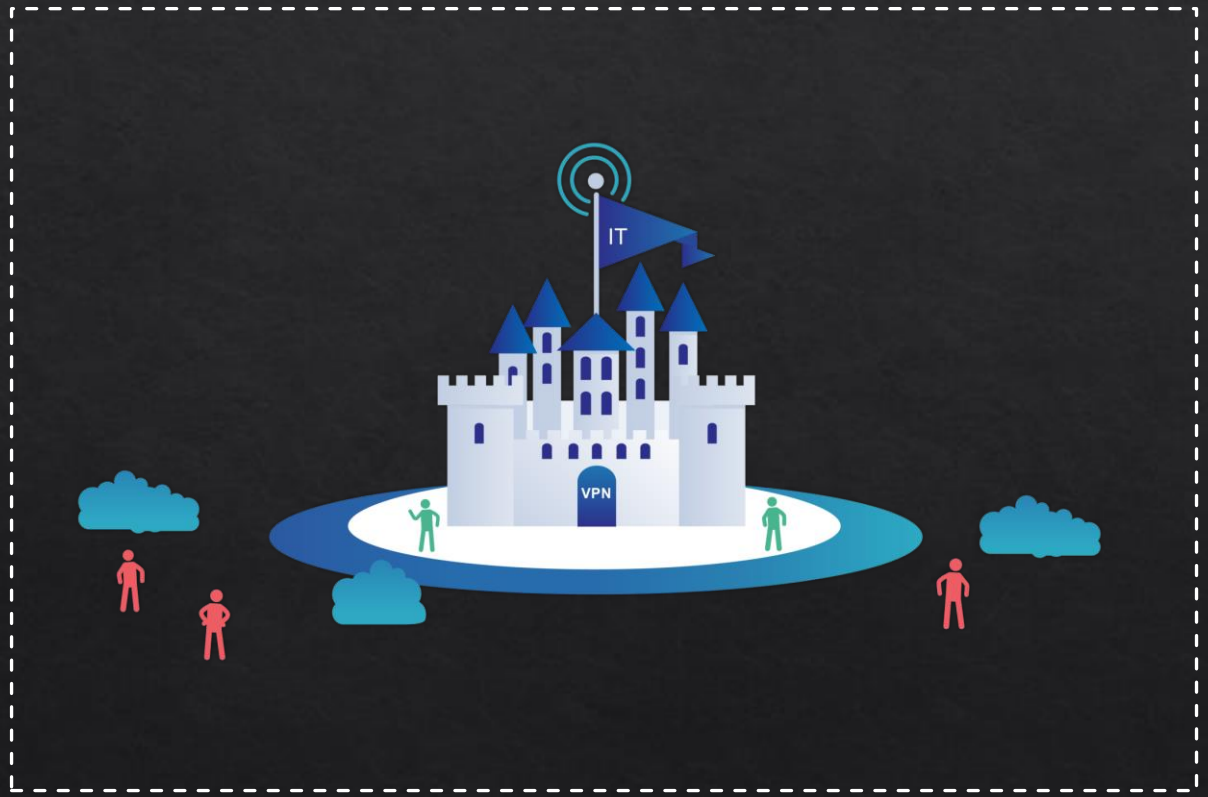
- IAM – Identity and Access Management

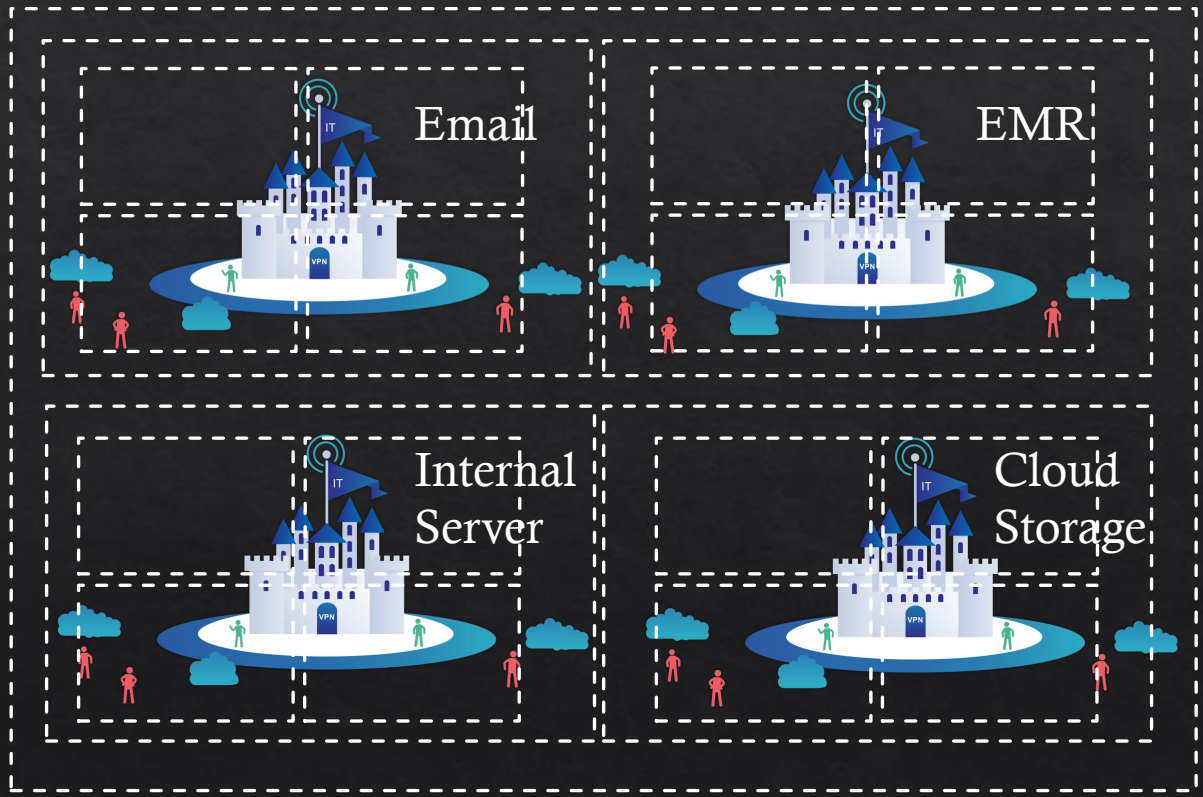
Principle of Least Privilege

- Only provide authorization for specific tasks for a set time in a limited area
- Organize users based on roles, authorization levels, or specific job needs

- The gardener can work in the lawn, but can’t remodel the kitchen

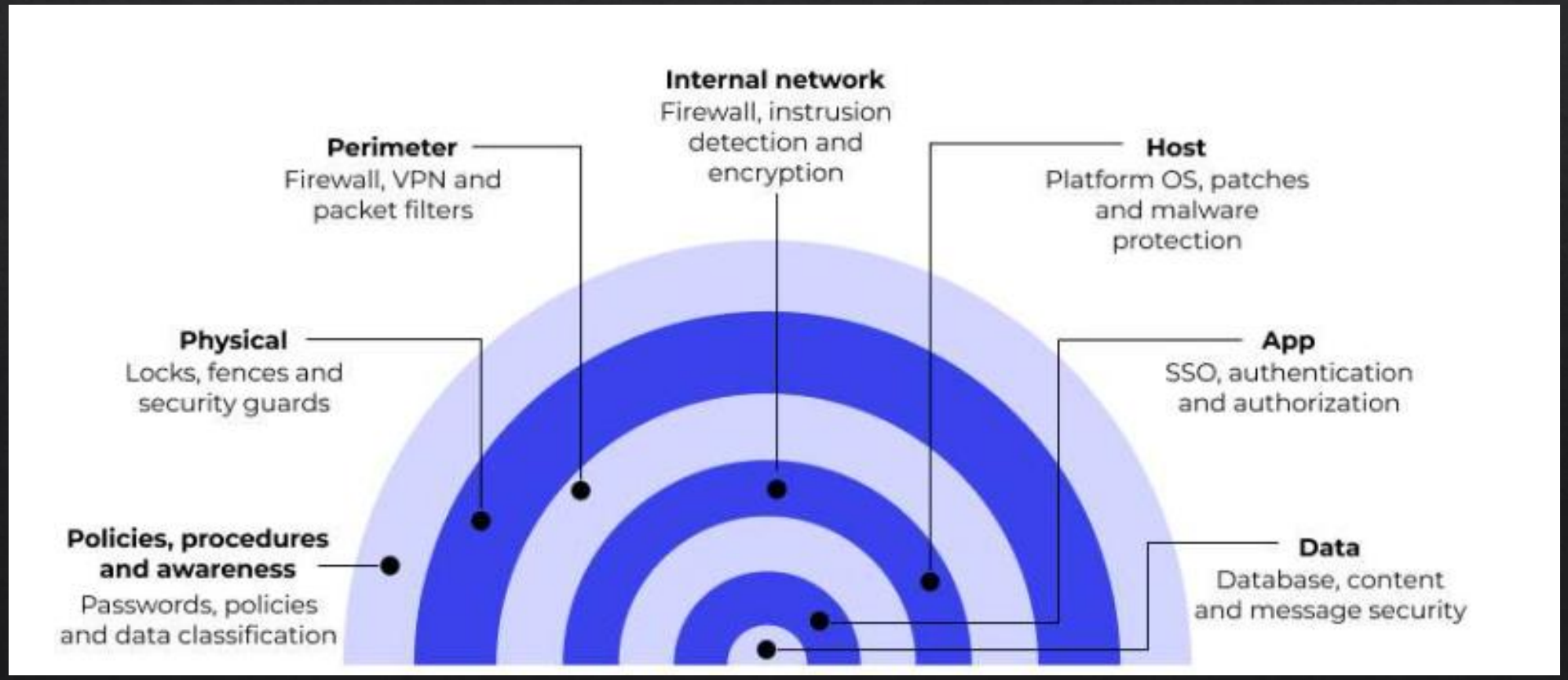
Implicit Trust vs. Zero Trust Security Models

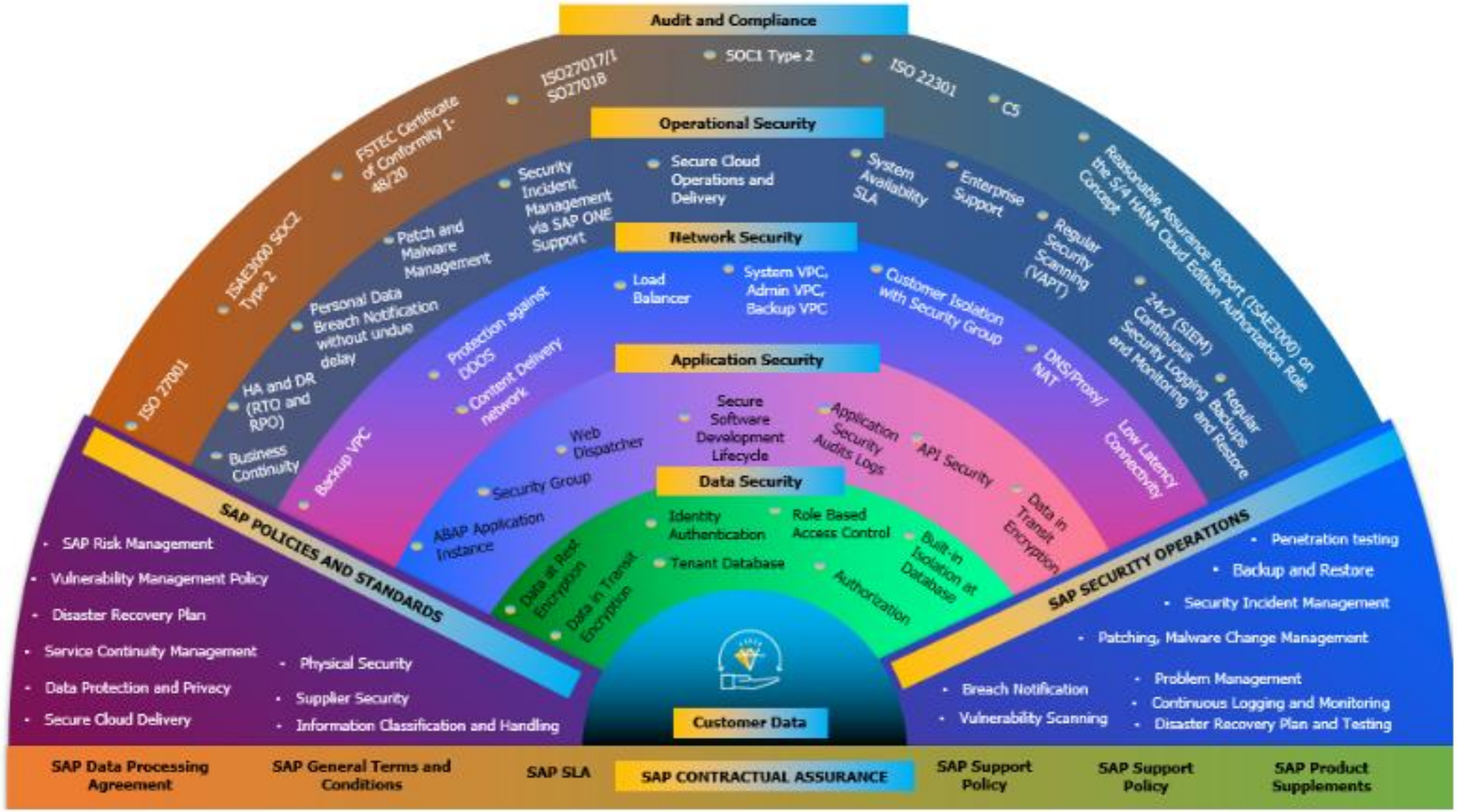




Layered Security – Defense in Depth Model

- Multiple layers of prevention, detection, and protection at various depths within a system



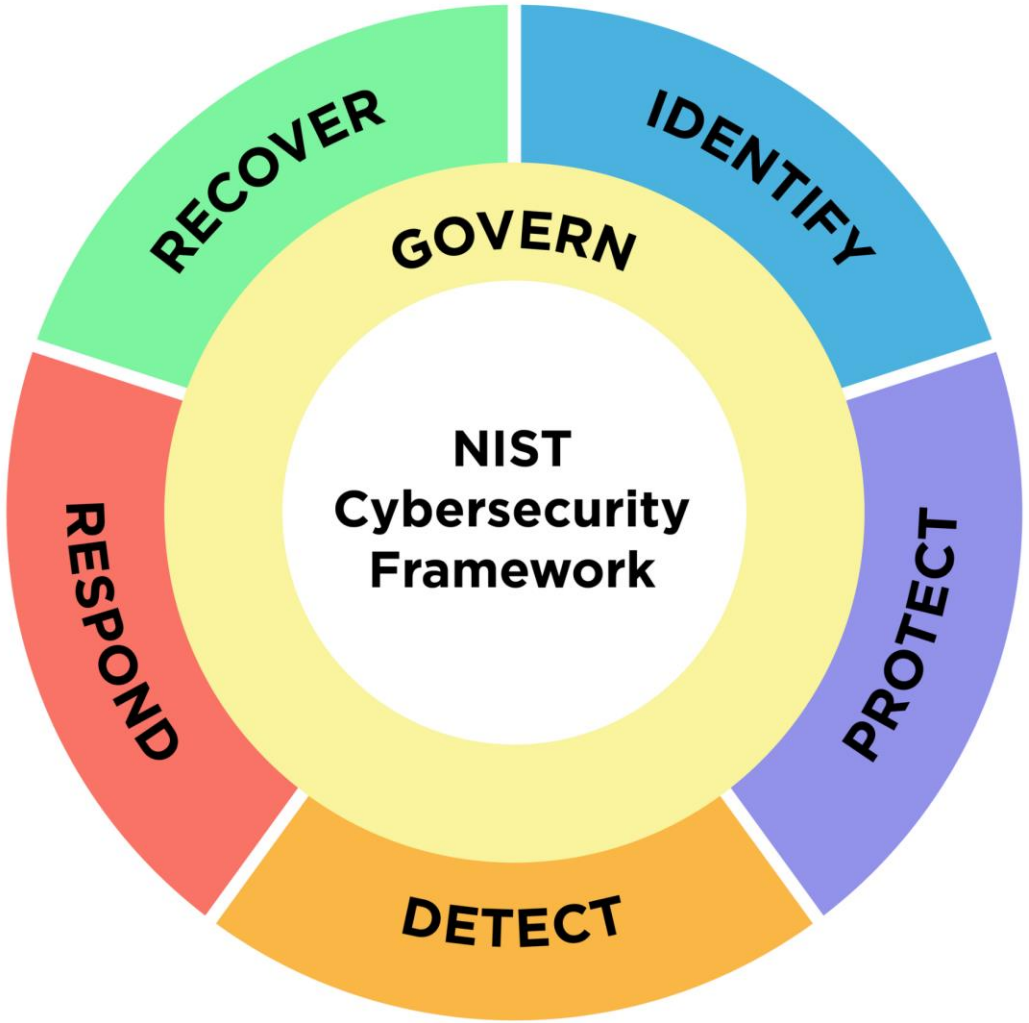

Audit and Compliance
ISO 27001
ISAE3000 SOC2 Type 2
FSTEC Certificate of Conformity 1-48/20
ISO27017/1 SO27018
SOC1 Type 2
ISO 22301
C5
Reasonable Assurance Report (ISAE3000) on the S/4 HANA Cloud Edition Authorization Role Concept
Operational Security
Business Continuity
HA and DR (RTO and RPO)
Personal Data Breach Notification without undue delay
Patch and Malware Management
Security Incident Management via SAP ONE Support
Secure Cloud Operations and Delivery
System Availability SLA
Enterprise Support
Regular Security Scanning (VAPT)
Network Security
Backup VPC
Protection against DDOS
Content Delivery network
Load Balancer
System VPC, Admin VPC, Backup VPC
Customer Isolation with Security Group
DNS/Proxy/ NAT
24x7 (SIEM) Continuous Security Logging and Monitoring
Regular Backups and Restore
Application Security
Security Group
ABAP Application Instance
Web Dispatcher
Secure Software Development Lifecycle
Application Security Audits Logs
API Security
Low Latency Connectivity
Data Security
Data at Rest Encryption
Data in Transit Encryption
Tenant Database
Identity Authentication
Role Based Access Control
Authorization
Built-in Isolation at Database
Data in Transit Encryption
SAP POLICIES AND STANDARDS
SAP Risk Management
Vulnerability Management Policy
Disaster Recovery Plan
Service Continuity Management
Data Protection and Privacy
Secure Cloud Delivery
Physical Security
Supplier Security
Information Classification and Handling
Customer Data
SAP SECURITY OPERATIONS
Penetration testing
Backup and Restore
Security Incident Management
Patching, Malware Change Management
Breach Notification
Vulnerability Scanning
Problem Management
Continuous Logging and Monitoring
Disaster Recovery Plan and Testing
SAP Data Processing Agreement
SAP General Terms and Conditions
SAP SLA
SAP CONTRACTUAL ASSURANCE
SAP Support Policy
SAP Support Policy
SAP Product Supplements

Cybersecurity Frameworks

- Several cybersecurity frameworks exist to guide organizations through creating secure information systems:
  - NIST Cybersecurity Framework
    - NIST Cybersecurity Framework (CSF)– voluntary, high level framework for all org types and sizes
    - NIST 800-171 – Unclassified information, non-federal organizations that work with federal organizations
  - CISA Cross-Sector Cybersecurity Performance Goals
  - HHS 405(d) – Specific measures for healthcare and public health sectors
  - ISO/IEC 27000 Series

NIST Cybersecurity Framework

- Primary framework components:
  1. Govern: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
  2. Identify: The organization's current cybersecurity risks are understood.
  3. Protect: Safeguards to manage the organization's cybersecurity risks are used.
  4. Detect: Possible cybersecurity attacks and compromises are found and analyzed.
  5. Respond: Actions regarding a detected cybersecurity incident are taken.
  6. Recover: Assets and operations affected by a cybersecurity incident are restored.

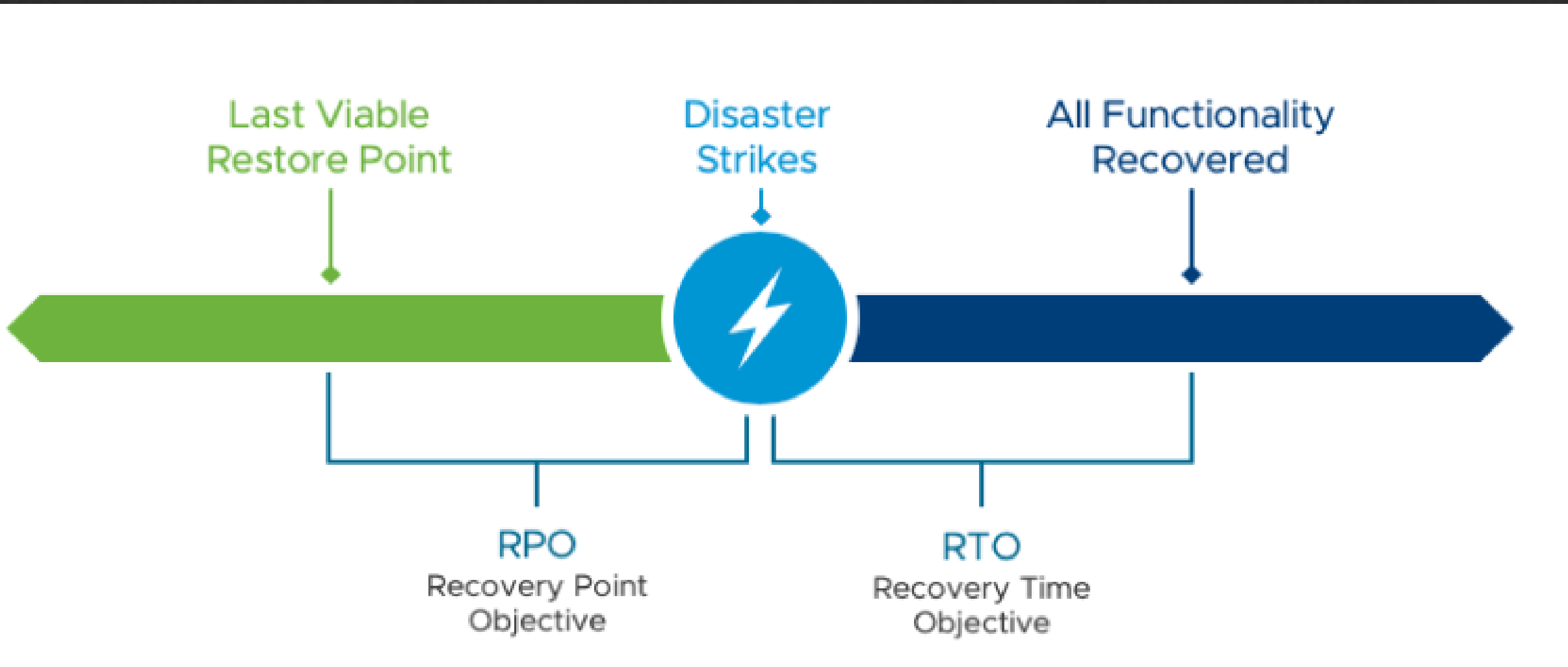

RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT

Risk Assessment Terminology

- RTO – Recovery Time Objective – How soon do my information systems need to be available again after something goes wrong? How long will recovery take?

- RPO – Recovery Point Objective – How much data can my organization afford to lose after an outage? What is your risk tolerance?

- RTA – Recovery Time Actual – How long does it actually take to recover your systems.


Last Viable
Restore Point
Disaster
Strikes
All Functionality
Recovered
RPO
Recovery Point
Objective
RTO
Recovery Time
Objective

Hashing and Checksums

- Hashing is a mathematical function that transforms data into a fixed length string of text. Using modern hashing methods, this string can be very difficult to decrypt.
- Hashing is often applied to data in order to create a checksum, which is used to ensure that data remains unchanged and reliable during transit and while in storage.
- Hashing is also an essential part of the private and public key infrastructure that is used to secure digital communications.
- Modern hashing algorithms will never produce identical strings from different inputs. (Hash Collision)

Hashing Example

- SHA256 Hash Protocol
  - Jared=eb338a96b0e78f261140ff6863f5d1f700f438f5e50c21a33809883f68b89ad3
  - jared=27d300fe53b3b94f115cfd63be02d868bcb8f755e5689370941808 4c1bfab1cd

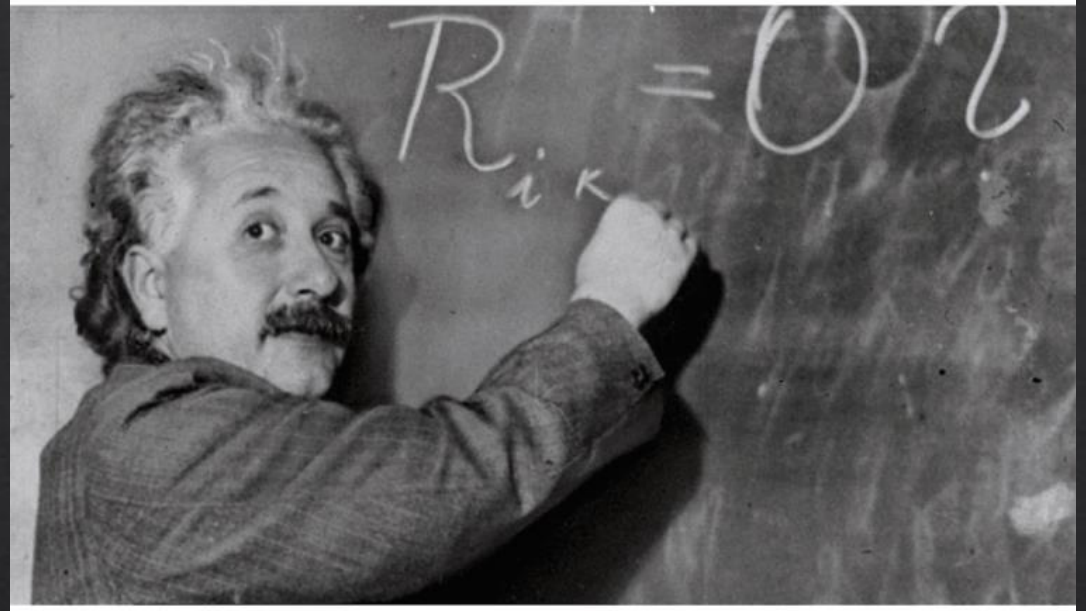
- Checksums allow us to verify data integrity.

Promoting a Culture of Cybersecurity

Built In – Not Bolt On

- Cybersecurity must be an integral part of information systems management in your organization
- Cybersecurity needs to be an assigned role for someone in your organization
- Cybersecurity needs dedicated, consistent funding as part of an agency's IT budget.

How I think I look explaining cyber risk to the board



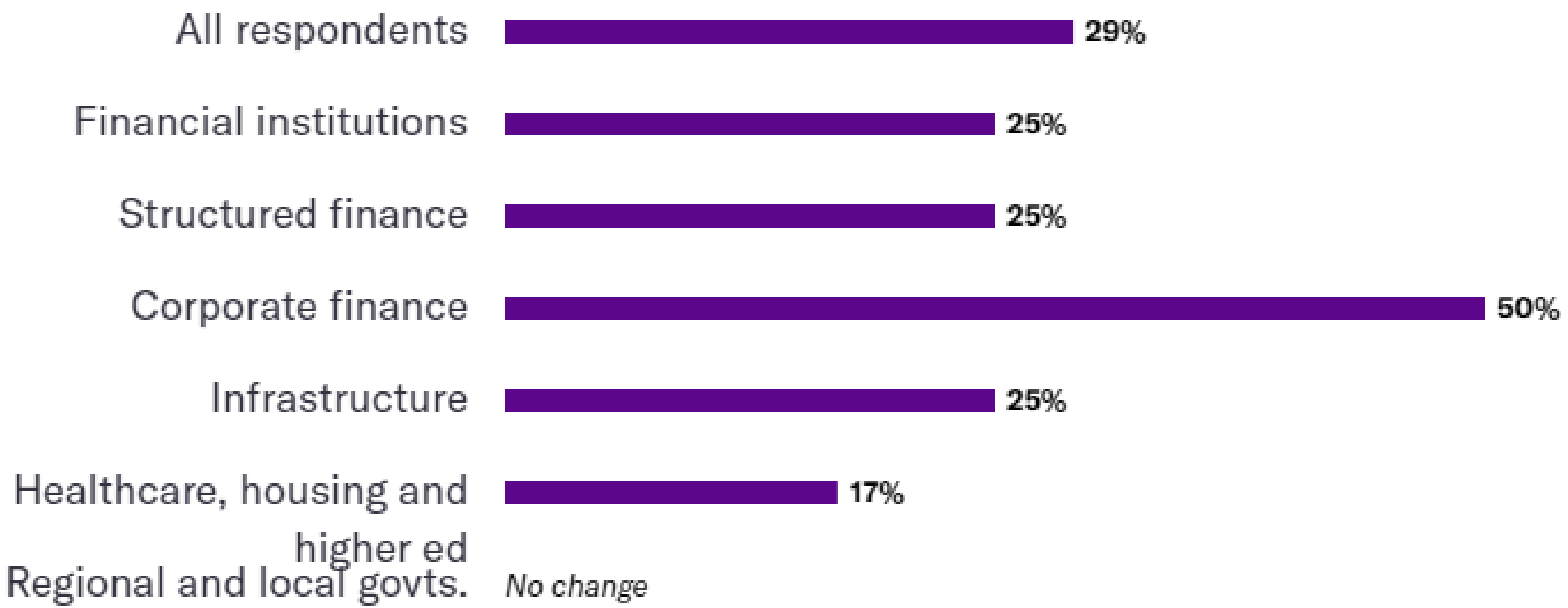
How I actually look

Cybersecurity Investment

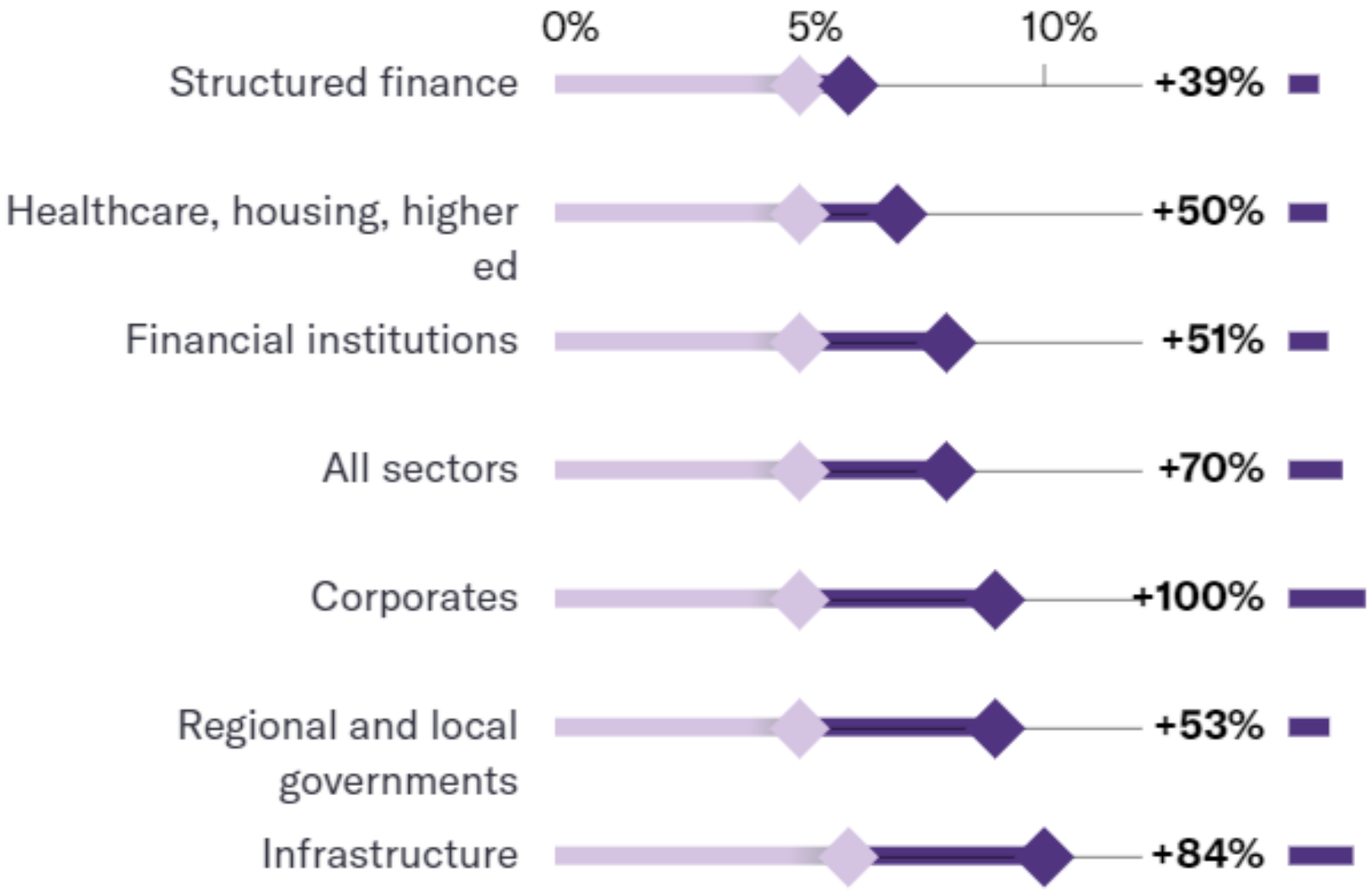
- Cybersecurity investments worldwide increased 70% between 2019 and 2023.
- Cyber insurance costs rose 50% between 2020 and 2022.
- Healthcare and Education saw premiums increase by 300% in this same timeframe.

- Results from Moody's 2023 Cyber Survey Highlights Report
- https://www.moodys.com/web/en/us/about/insights/data-stories/2023-cyber-survey-highlights.html

Change in full time cybersecurity employees from 2019 to 2022



Cybersecurity spending as a share of technology budget, ◆ 2019 and ◆ 2023



Develop Policies

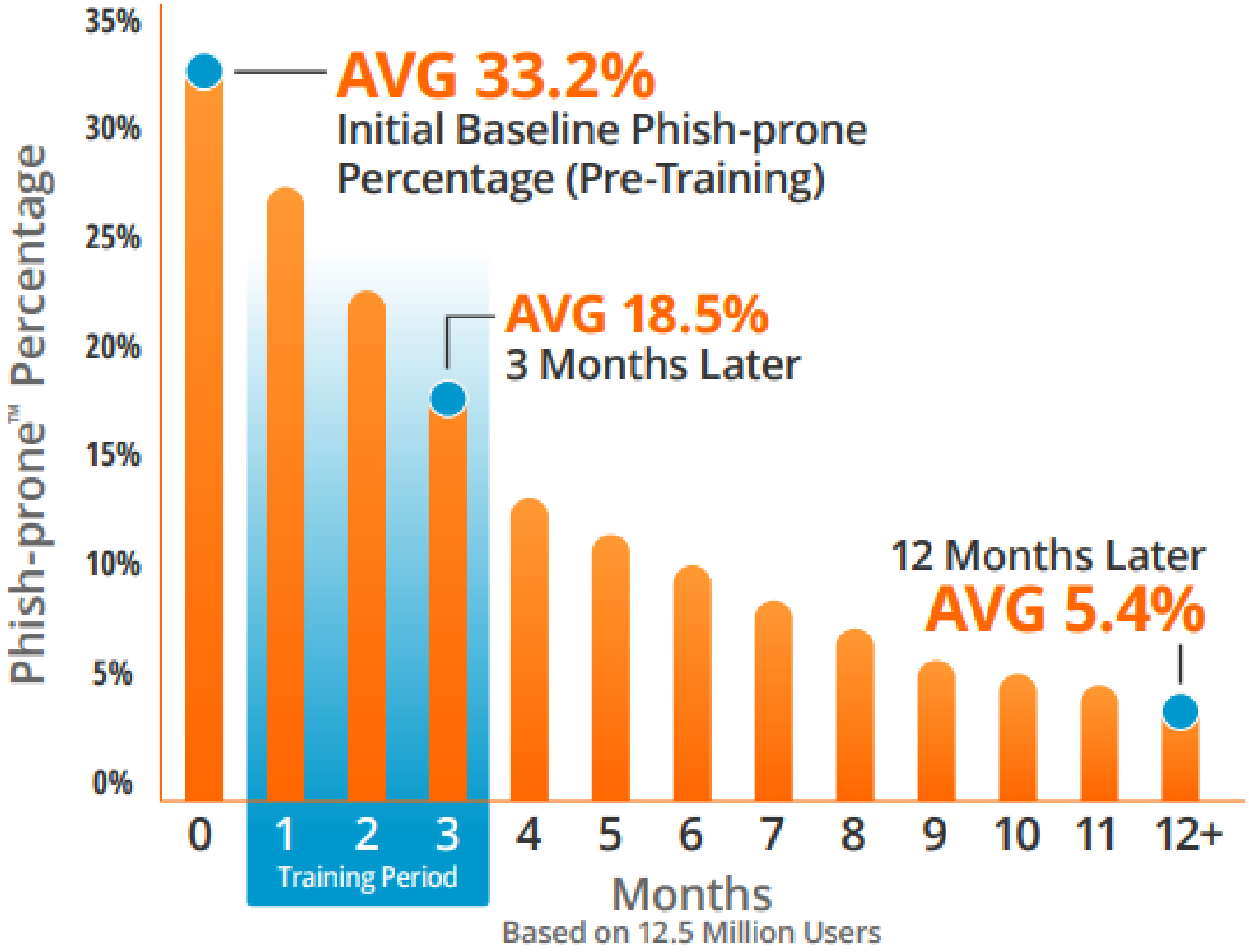
- Develop written policies to guide cybersecurity efforts.
- Written policies also provide clear expectations and performance standards to measure yourself against.

Train People

- Empower your staff as active participants in cybersecurity (not inherent weaknesses in the system).
- 94% of organizations in 2023 had email security incidents.
- 68% of data breaches included a human factor (Verizon DBIR)

- Egress Email Security Report 2024
- https://www.egress.com/media/o1sbpq5t/egress_email_security_risk_report_2024.pdf

- KnowBe4 Industry Benchmark White Paper
- https://www.knowbe4.com/hubfs/Data-Confirms-Value-of-SAT-WP_EN-us.pdf?hsLang=en-us
- https://www.knowbe4.com/hubfs/2024-Phishing-by-Industry-Benchmarking-Report-EN_US.pdf?hsLang=en



Source: 2023 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Phishing Prevention Training

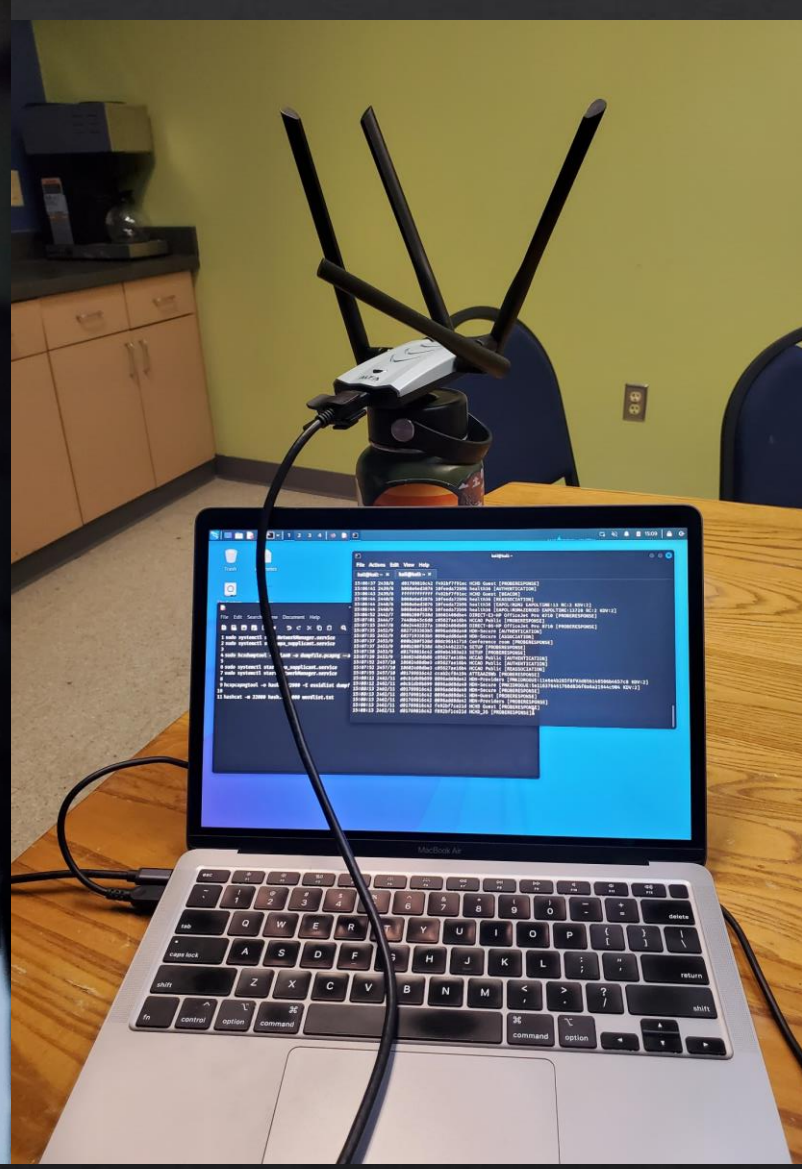
- Phish-prone Percentage (PPP) – Likelihood that a user will click a simulated phishing test.
- Based on KnowBe4 2024 Benchmark data

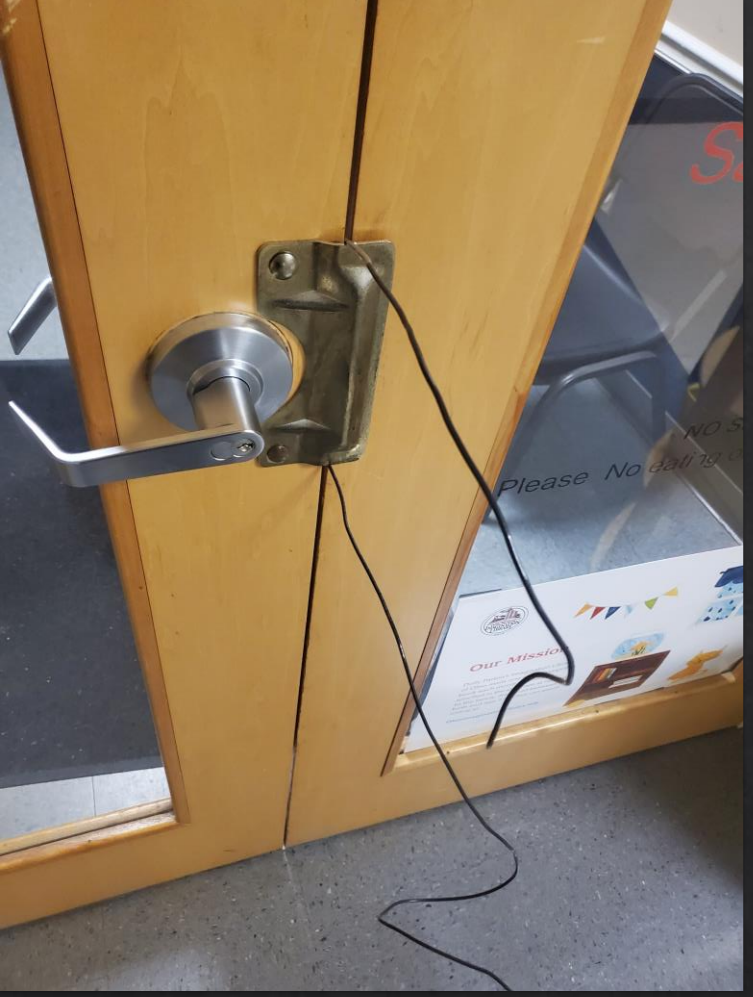
N. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	29%	19.8%	4.3%
250-999	32.6%	19.9%	4.6%
1000+	39.1%	17.9%	4.6%
Average PPP Across All Organization Sizes	35.1%	18.9%	4.5%

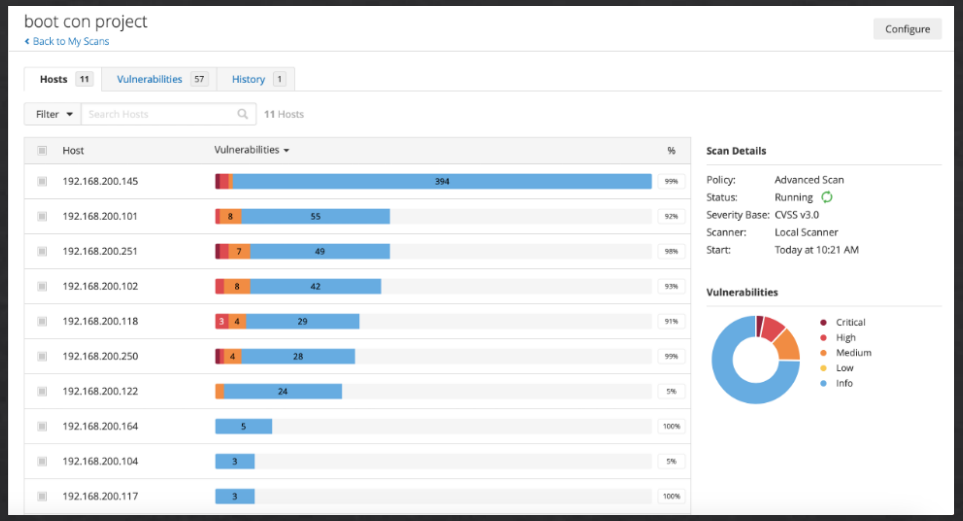
Test Your Organization

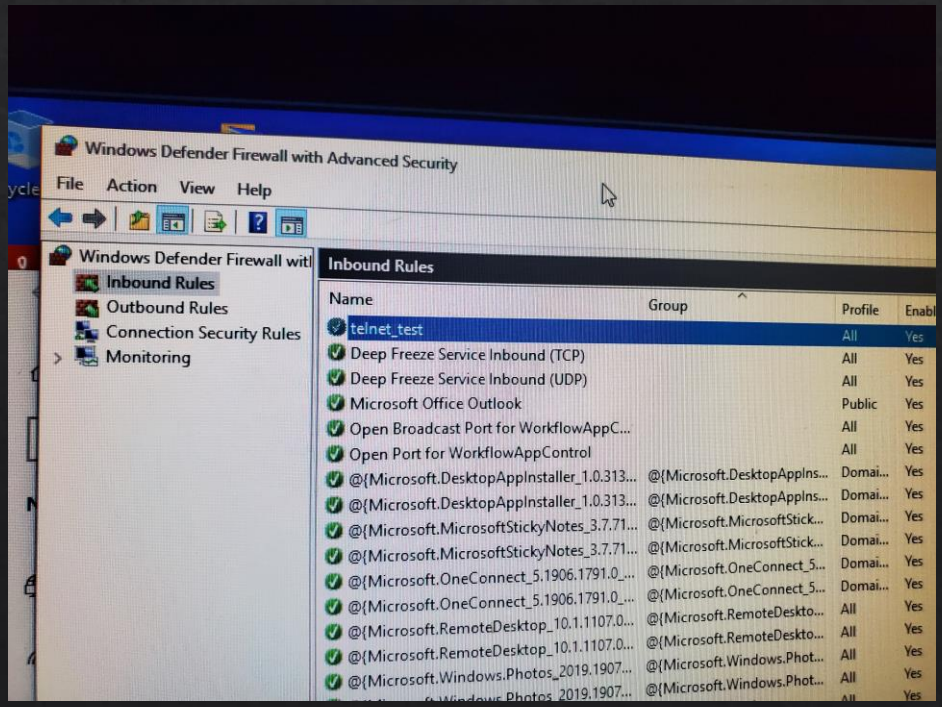
- Have you exercised your response to a potential ransomware, breach, or other incident?
- For agencies farther down the cybersecurity path, have you conducted red team / penetration testing?


EXIT
Little Giant LEVERAGE




Please No


boot con project
Back to My Scans
Configure
Hosts 11
Vulnerabilities 57
History 1
Filter
Search Hosts
11 Hosts
Host
Vulnerabilities
%
192.168.200.145
192.168.200.101
192.168.200.251
192.168.200.102
192.168.200.118
192.168.200.250
192.168.200.122
192.168.200.164
192.168.200.104
192.168.200.117
Scan Details
Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:21 AM
Vulnerabilities
Critical
High
Medium
Low
Info


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
telnet_test
Deep Freeze Service Inbound (TCP)
Deep Freeze Service Inbound (UDP)
Microsoft Office Outlook
Open Broadcast Port for WorkflowAppC...
Open Port for WorkflowAppControl

Cybersecurity Checklist

- At a minimum, your agency should be:
  - Developing and maintaining policies for cybersecurity, such as an Access Control Plans, Network Security Policy, Backup Policy, Third-Party Risk Management Policy, and others.
  - Implementing MFA / 2FA **wherever possible**. Microsoft reports a 99.2% risk reduction when this is enabled.
  - Using a patch management program. This will help protect systems from new vulnerabilities, and will help to identify legacy services that need to be removed from use.
  - Implementing Zero Trust principles. Use least privilege access control, segment systems, and assume breach.
  - Training your team. Implement phishing training programs and other cybersecurity training programs to educate and empower staff.
  - Controlling access to physical equipment and technical assets.


Counties
Counties using now
Counties plan to use
Zero-trust model
Security Orchestration Automation and Respon...
Micro-segmentation
Enterprise security operation centers
Governance risk and compliance
Pen/red team testing
Security as a Service
Security information and event management (SIEM)
0
10%
20%
30%
40%
50%
60%
70%
80%


Cities
Cities using now
Cities plan to use
Zero-trust model
Security Orchestration Automation and Respon...
Micro-segmentation
Enterprise security operation centers
Governance risk and compliance
Pen/red team testing
Security as a Service
Security information and event management (SIEM)
0
10%
20%
30%
40%
50%
60%
70%
80%

What Comes Next?

- Increase in both mandated cybersecurity risk management AND funding to address cybersecurity threats – both the carrot and the stick
- Increased opportunities for collaboration to share resources, tools, and staff
- More attacks and more breaches as HaaS expands, and as AI becomes more involved in attacks

Improved Visibility

- Better visibility of cybersecurity incidents is coming – Cyber Incident Reporting for Critical Infrastructure Act of 2022.
- Will require reporting of cybersecurity incidents from covered entities, including local government agencies of 50,000 population and higher. Rules under review currently.

Thank You!

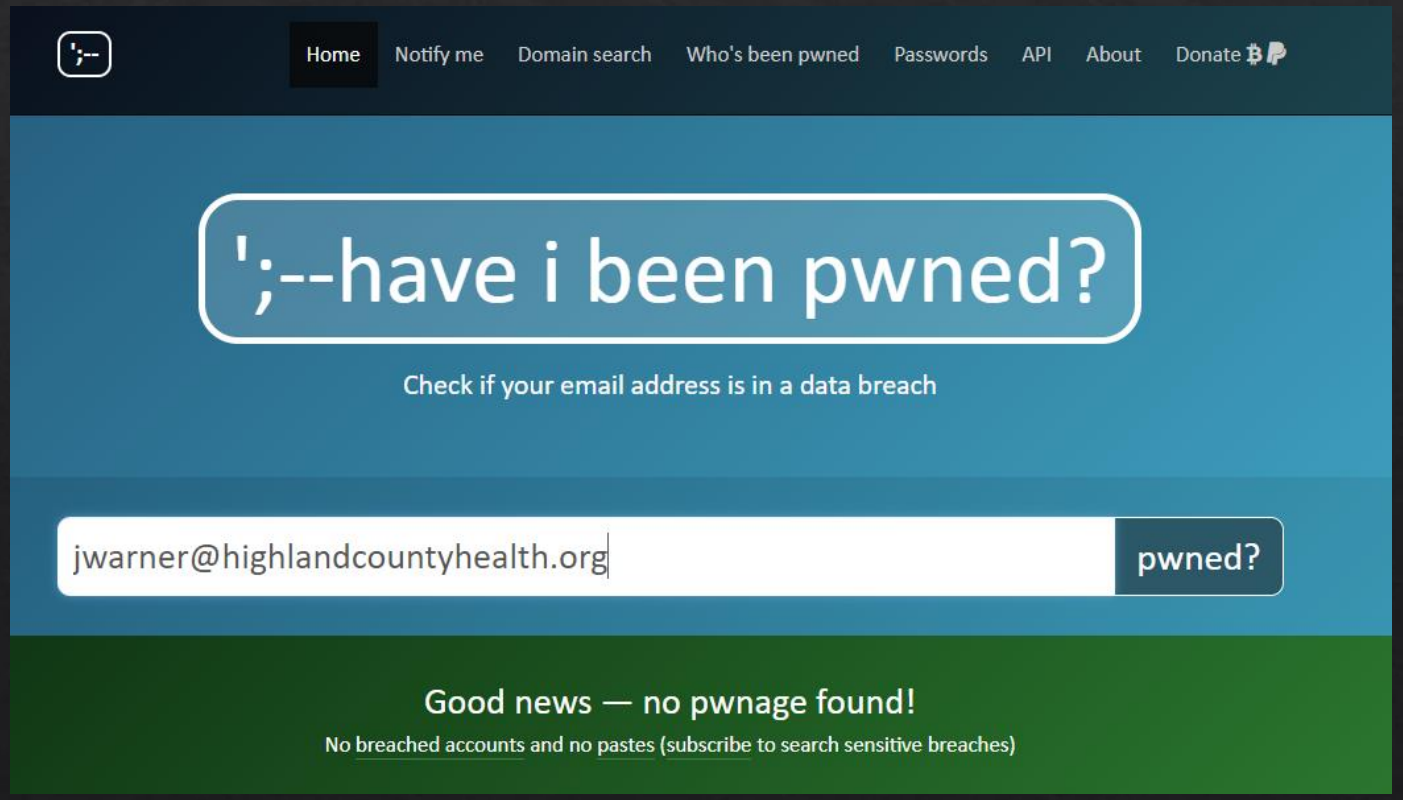
- Questions?
- For a list of my presentation sources and reading material, send me an email: jwarner@highlandcountyhealth.org

Extra Slides

- Extra slides in case I talk too fast

haveibeenpwned.com

- Website ran by Microsoft Regional Director Troy Hunt.
- Allows users to compare emails and passwords to a list of over 13 BILLION accounts and 228 MILLION passwords that have been leaked online after data breaches.



Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

••••••••••

pwned?

Oh no — pwned!

This password has been seen 78 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

Building a Cybersecurity Culture

- **Govern**: Set policies and determine your levels of acceptable risk.
  - Use NIST, HHS Cybersecurity Performance Goals, or other frameworks to guide what policies are needed
  - Examples:
    - Can personal devices log into your systems?
    - Can international IP addresses log into your email?
    - What cybersecurity standards do you require outside vendors to follow?
    - Are shared accounts allowed to be used?
    - Have you removed default device passwords?
    - How often will your users be required to receive cybersecurity training?

Building a Cybersecurity Culture

- **Identify:** Assess your risks. What is working well, what isn't, what resources are available, what legacy systems are vulnerable?
- NIST SP 800-171A Rev. 3 – Comprehensive assessment framework
- Public Entity Pool Cybersecurity Assessment – Free, high level review of cybersecurity risk and controls

Building a Cybersecurity Culture

- Protect: Implement or improve protection efforts
- Could include Technical Controls:
  - Firewalls, Unified Threat Management, Next Gen Firewalls, Cloud Access Security Brokers, etc.
  - Load Balancing
  - Network Segmentation
  - Patch Management
- Could include Physical Controls:
  - Physical Access Control
  - USB Port Disabling
  - Cable Locks for Devices

Building a Cybersecurity Culture

- Detect: Possible cybersecurity attacks and compromises are found and analyzed.
- Could include things like:
  - Intrusion Detection Systems, Intrusion Prevention Systems
  - Security Information and Event Management (SIEM) systems
  - Vulnerability Scanning

Building a Cybersecurity Culture

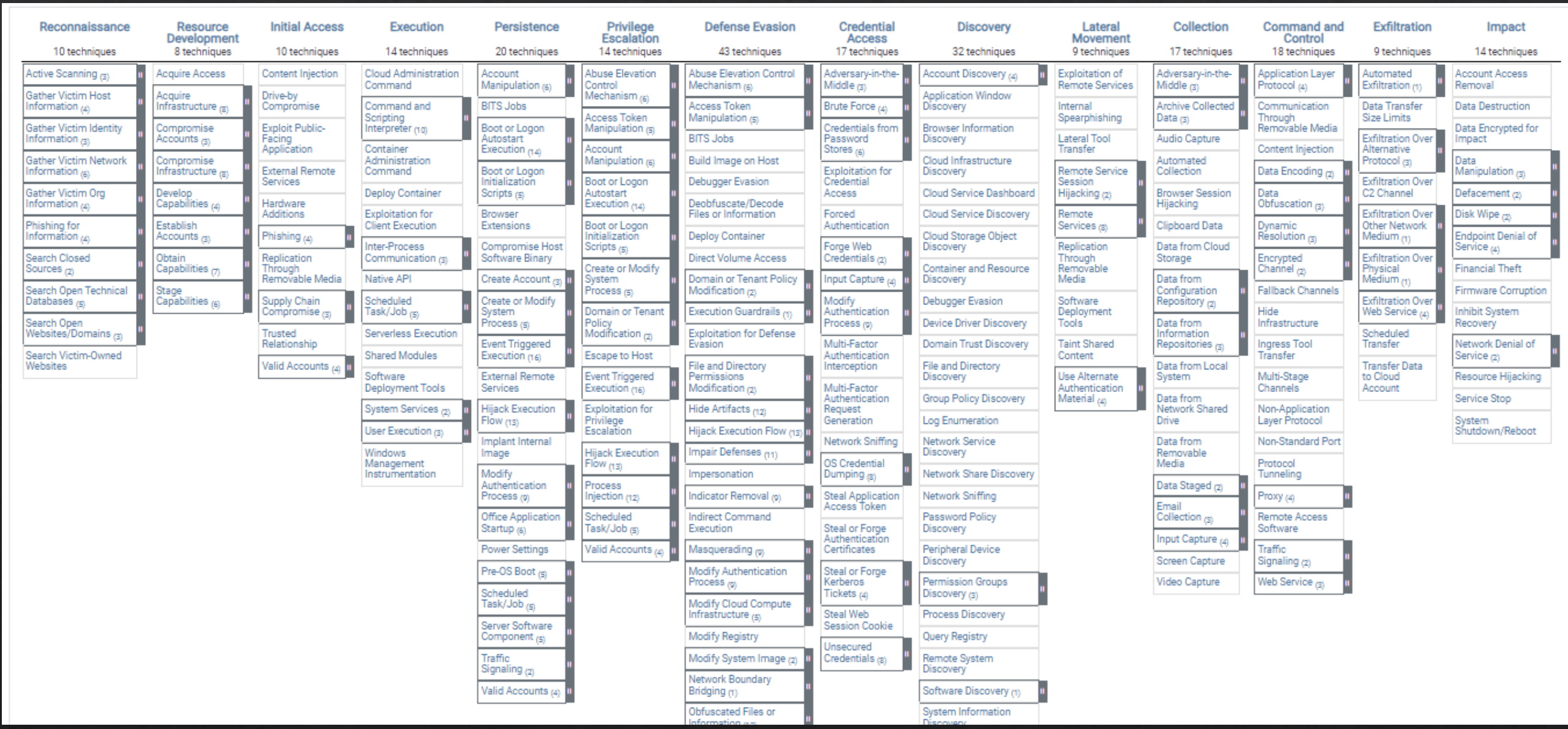
- **Respond:** Actions regarding a detected cybersecurity incident are taken.
- Could include things like:
  - Isolation and Quarantine of Impacted Assets
  - Forensic Tools
  - Incident Response Playbooks
  - Stakeholder Notification
  - Mandatory Reporting Requirements

Building a Cybersecurity Culture

- Recover: Assets and operations affected by a cybersecurity incident are restored.
- Could Include:
  - Automated Data Backups
  - System Image Backups
  - Disaster Recovery Plans
  - Data Recovery Tools
  - Hot, warm, and cold site recovery options

MITRE ATT&CK Matrix

- Recon
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact


Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (4)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (3)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (8)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (7)
Stage Capabilities (6)
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (10)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation
Persistence
20 techniques
Account Manipulation (5)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Host Software Binary
Create Account (3)
Create or Modify System Process (5)
Event Triggered Execution (16)
External Remote Services
Hijack Execution Flow (13)
Implant Internal Image
Modify Authentication Process (9)
Office Application Startup (6)
Power Settings
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (5)
Traffic Signaling (2)
Valid Accounts (4)
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
Account Manipulation (6)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (5)
Domain or Tenant Policy Modification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Hijack Execution Flow (13)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (12)
Hijack Execution Flow (13)
Impair Defenses (11)
Impersonation
Indicator Removal (9)
Indirect Command Execution
Masquerading (9)
Modify Authentication Process (9)
Modify Cloud Compute Infrastructure (5)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or
Credential Access
17 techniques
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (9)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Unsecured Credentials (8)
Discovery
32 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Adversary-in-the-Middle (3)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (2)
Data from Information Repositories (3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Screen Capture
Video Capture
Command and Control
18 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Content Injection
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (2)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (4)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
14 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot