NFES Cybersecurity Update

Steven Hernandez
Chief Information Security Officer
United States Department of Education

Office of the Chief Information Officer
U.S. Department of Education

Agenda

- Introduction
- Overview of the present threatscape
- Best practices
- Federal resources that can help
- Questions

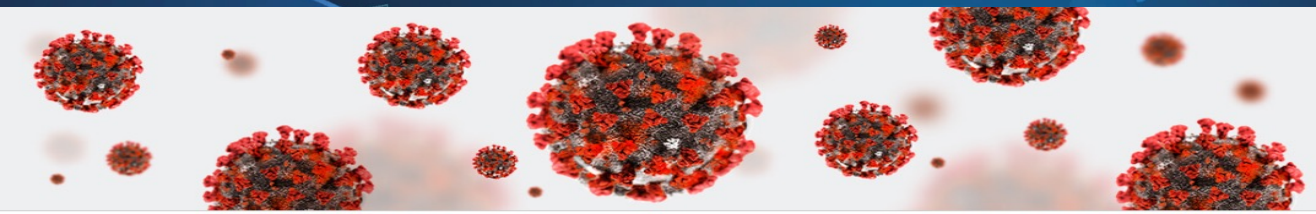
Introduction

- Steven Hernandez
- MBA, CISSP, CISA, CNSS, CSSLP, CDPSE, SSCP, CAP, ITIL
- Chief Information Security Officer (CISO)
- US Department of Education
- Co-Chair US Federal CISO Council

- Prior Roles:
- Vice Chairman Board of Directors $(ISC)^2$
- CISO HHS OIG
- Senior Official for Privacy, HHS OIG

3

Current Threatscape



- Telework and Hybrid
- Ransomware
- Supply Chain and Vendor Security

Teleconferencing Vulnerabilities

1. CISA teleconferencing toolkit
2. https://www.cisa.gov/publication/telework-essentials-toolkit

Ransomware

- Only increasing in volume of attacks
- Increasingly persistent and sophisticated
- Payouts are increasing, driving new entrants

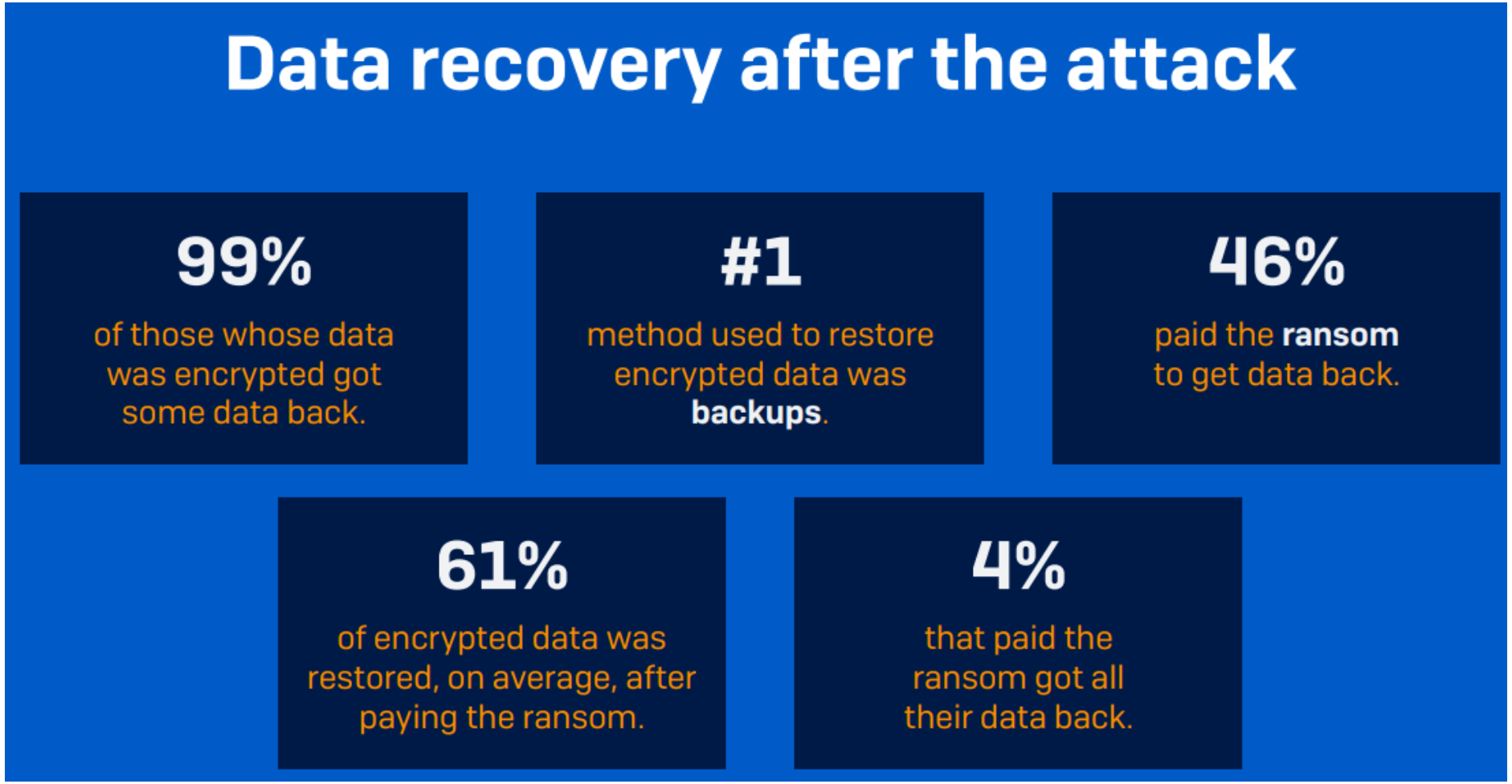
Ransomware

- Sophos (anti-virus and cybersecurity company)
- Vanson Bourne Conducted Global Survey

https://www.sophos.com/en-us/content/state-of-ransomware

Ransomware

- Sophos (anti-virus and cybersecurity company)



https://www.sophos.com/en-us/content/state-of-ransomware

Ransomware

- Verizon DBIR 2022

Summary

Educational Services follows an eerily similar trend to the majority of the other industries; it is experiencing a dramatic increase in Ransomware attacks (over 30% of breaches). In addition, this industry needs to protect itself against stolen credentials and phishing attacks potentially exposing the personal information of its employees and students.

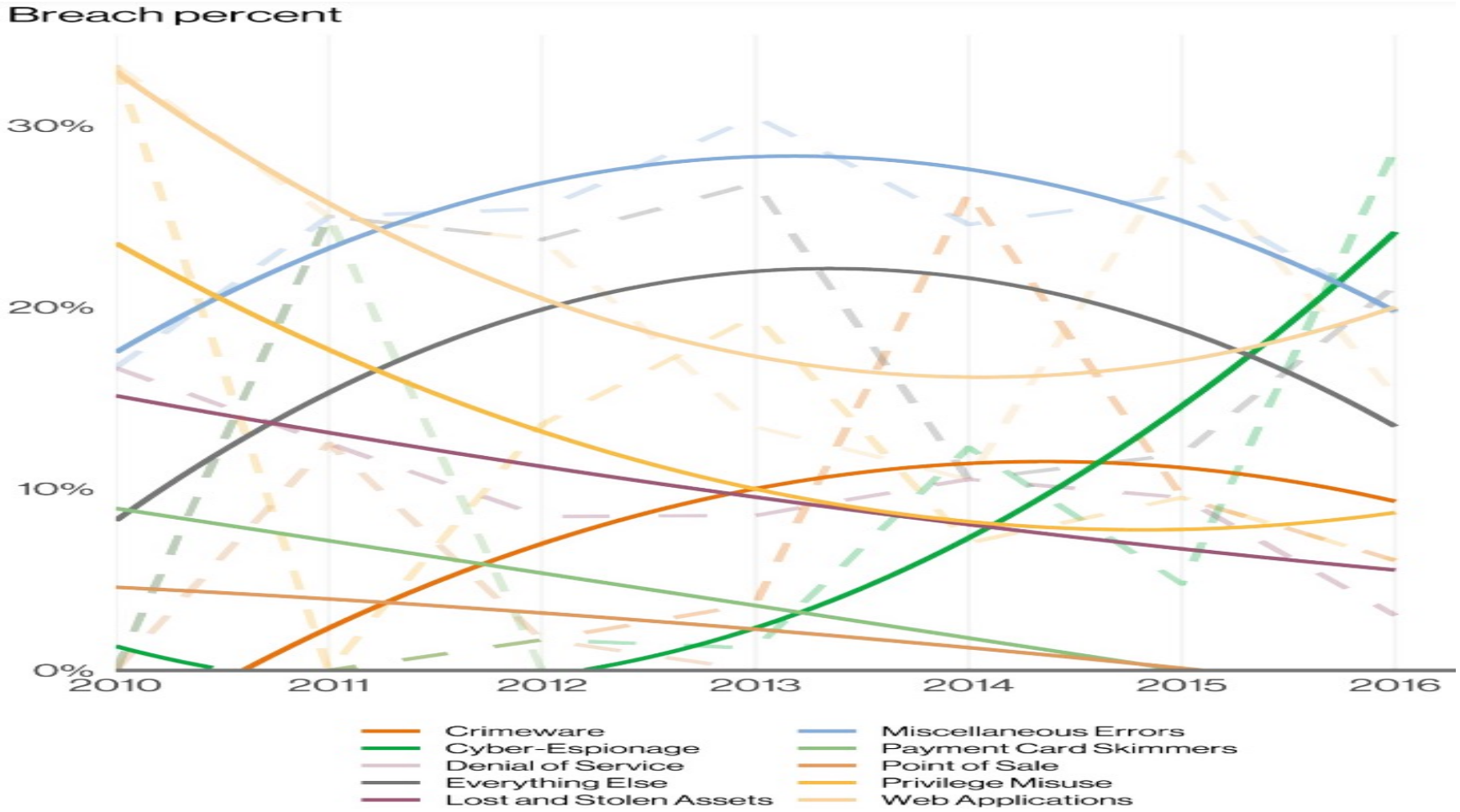
Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Greater	Less
System Intrusion	Greater	Greater	Greater
Miscellaneous Errors	No change	Less	Greater

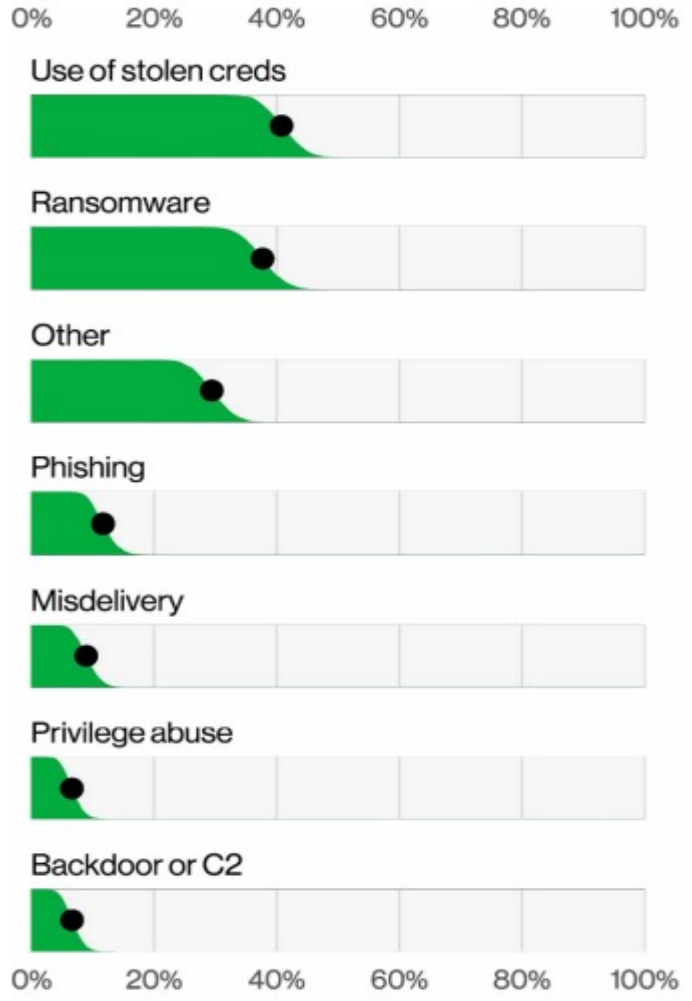
Frequency	1,241 incidents, 282 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 80% of breaches
Threat actors	External (75%), Internal (25%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (63%), Credentials (41%), Other (23%), Internal (10%) (breaches)

https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Ransomware

- Verizon DBIR 2022





https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

Ransomware

- Triple extortion
  - Exfiltrate data
  - Encrypt systems
  - Engage additional stakeholders to force negotiations

"I suspect what's happening is some of these hackers are saying 'I know how to put pressure on the school district to pay the ransom, I will start embarrassing them by communicating directly with parents,' then parents say 'Oh my gosh! You've got to do something about this,'" said Jose Lineros, a cybersecurity expert and professor at University of North Texas.

And it worked. Allen ISD began getting questions from parents about the emails.

Allen ISD Parents Concerned About Receiving Cybersecurity Breach Emails - CBS DFW (cbsnews.com)
https://www.rhisac.org/special-interest-resilience/ransomware-double-and-triple-extortion/

Mitigation Strategies

- Cyber Hygiene
  - Vulnerable internet facing systems
    - Patching is critical!
    - Only exposing necessary ports and services
    - Remote Desktop Protocols and similar without multifactor
  - Phishing
    - Vulnerable users
    - Not reporting quickly

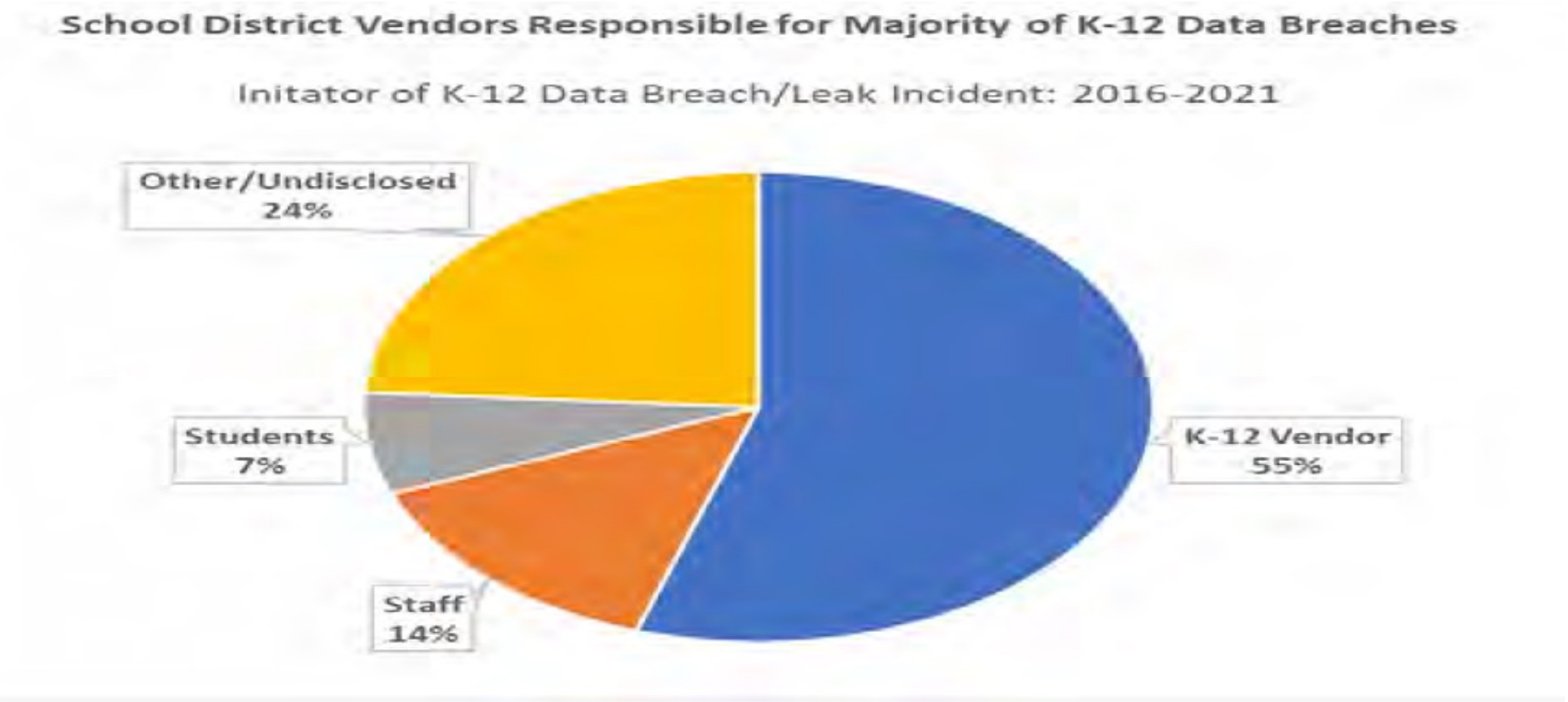
Mitigation Strategies

- Backups
  - Keep them encrypted and on separate services
  - TEST TEST TEST!
  - Only partially as good now due to data exfiltration.
- Phishing-Resistant Authenticators!!
  - Hard Tokens for admins like Yubi keys or Titan keys
  - Webauthn for websites (certificate-based authentication)
  - More information here: https://blog.hypr.com/what-is-phishing-resistant-mfa

Mitigation Strategies

- Resources:
  - On September 30, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center released a joint Ransomware Guide, which is a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware attack. CISA and MS-ISAC are distributing this guide to inform and enhance network defense and reduce exposure to a ransomware attack:
  - **Ransomware Guide (Sept. 2020)**

Vendor Cybersecurity



https://www.k12six.org/

Vendor Cybersecurity

illuminate education

CONTACT SUPPORT LOG IN GET A DEMO

WHY ILLUMINATE SOLUTIONS PRODUCTS RESOURCES RESEARCH ABOUT

MTSS Management | Comprehensive Assessment | Social Emotional Behavior (SEB) | Universal Screening

Progress Monitoring | Dyslexia Screening | Data Visualization | Equity & Disproportionality

MTSS Management

Screening and progress monitoring assessments for academics and SEB, combined with whole child data visualizations and built-in tools for key MTSS practices

https://www.legalscoops.com/illuminate-education-data-breach-class-action-investigation/

Best Practices for Data Focused Missions

- Identify Your “Crown Jewels”
  - Least Function
  - Least Privilege
  - De-Identification
  - Retention
- Have an Actionable Plan in Place Before an Intrusion Occurs
- Have Appropriate Technology and Services in Place Before An Intrusion Occurs
- Have Appropriate Authorization in Place to Permit Network Monitoring
- Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management to Reduce Response Time During an Incident
- Ensure Organization Policies Align with Your Cyber Incident Response Plan
- Engage with Law Enforcement Before an Incident
- Establish Relationships with Cyber Information Sharing Organizations

17

Best Practices for Data Focused Missions

- Building the Security in from the start
  - Consider leveraging cloud SaaS as much as possible
    - Review terms and SLAs, especially security!
    - Data Portability
  - Leverage FedRAMP systems
    - May not always be able to use GSA contracts
    - Federal Government Level of Security
    - You are still accountable for control configuration
    - State and local government representatives are encouraged to contact any FedRAMP Authorized CSP directly to determine their security package specifications.
  - StateRAMP
  - EDUCAUSE Higher Education Cloud Assessment Tool
    - Higher Education Community Vendor Assessment Toolkit | EDUCAUSE

Best Practices for Data Focused Missions

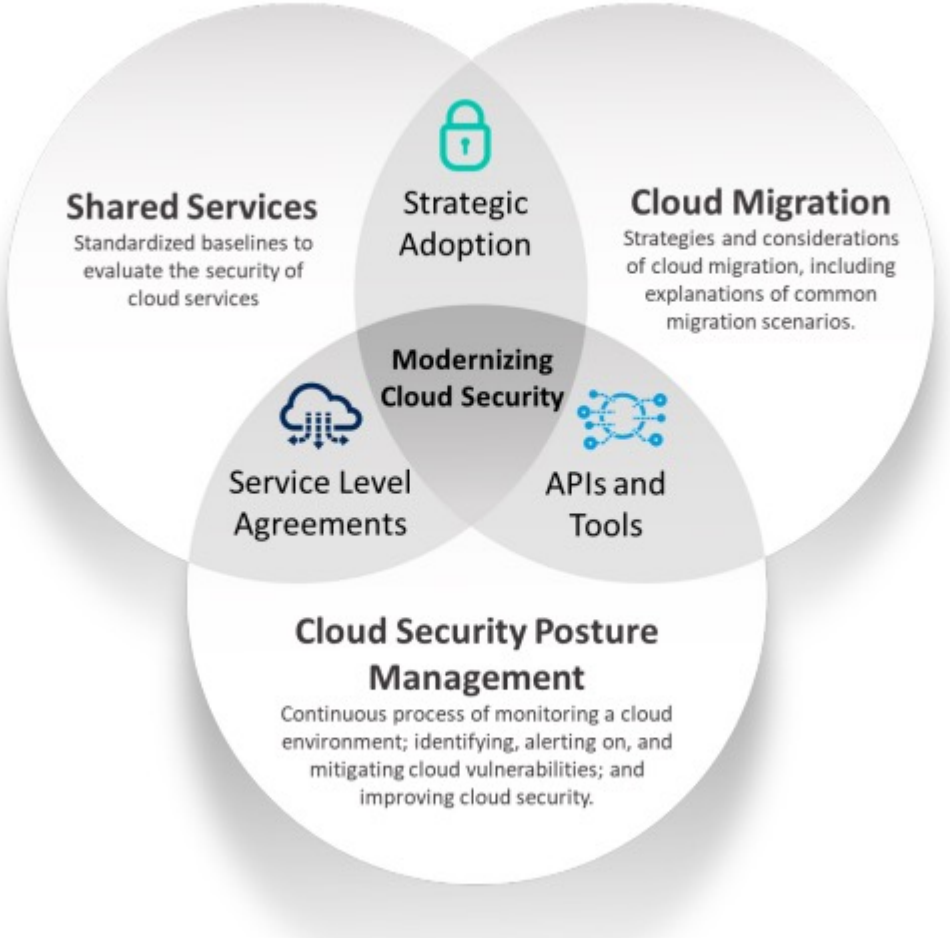
Cloud Security Technical Reference Architecture

Coauthored by:

Cybersecurity and Infrastructure Security Agency,

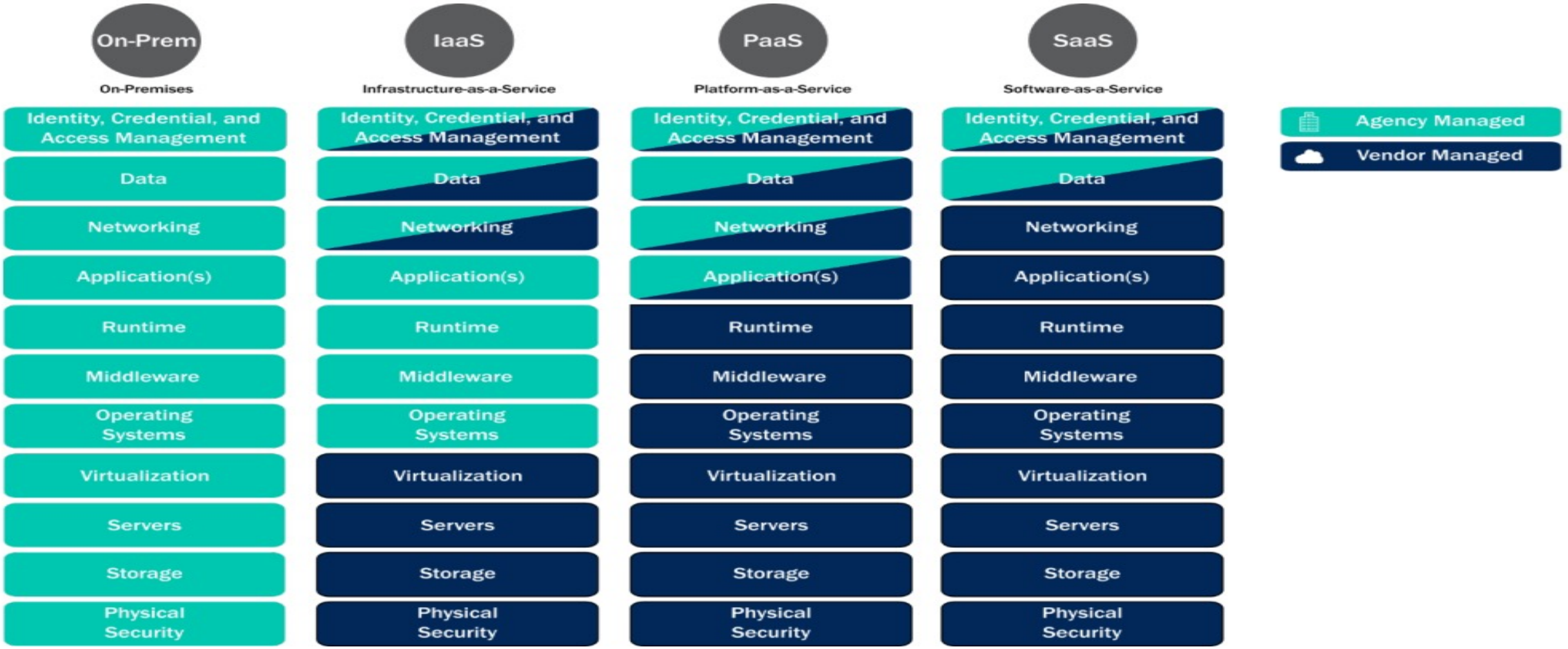
United States Digital Service, and

Federal Risk and Authorization Management Program

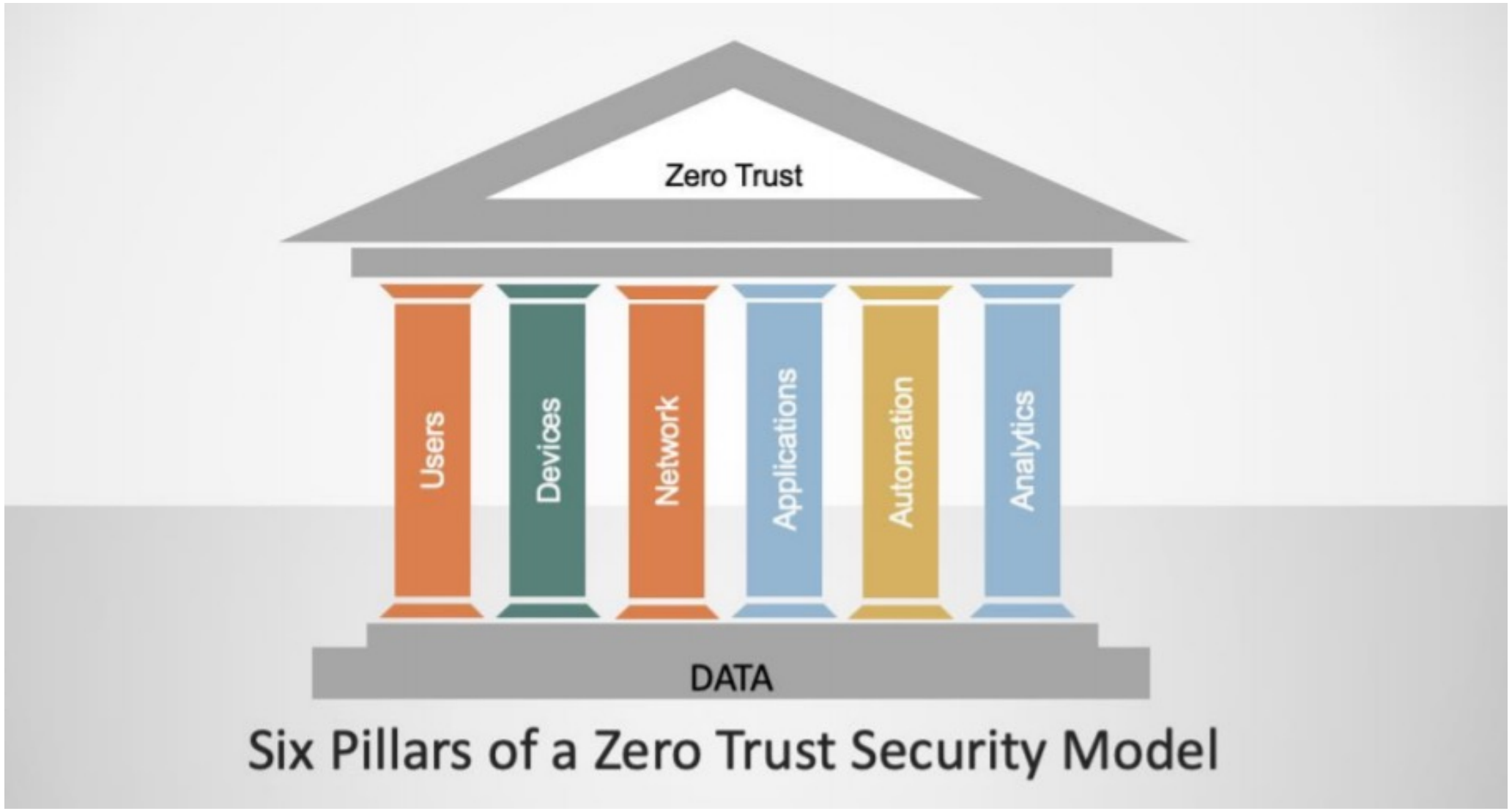


https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf

Best Practices for Data Focused Missions



Best Practices for Data Focused Missions



https://zerotrust.cyber.gov/

Best Practices for Data Focused Missions

- Zero Trust depends on five fundamental assertions:
  - the network is always assumed to be hostile;
  - external and internal threats always exist on the network;
  - network locality is not sufficient for deciding trust in a network;
  - every device, user, and network flow is authenticated and authorized; and
  - policies must be dynamic and calculated from as many sources of data as possible.

- https://www.actiac.org/zero-trust-cybersecurity-current-trends

Best Practices for Data Focused Missions

- Consider building towards a Zero Trust Architecture

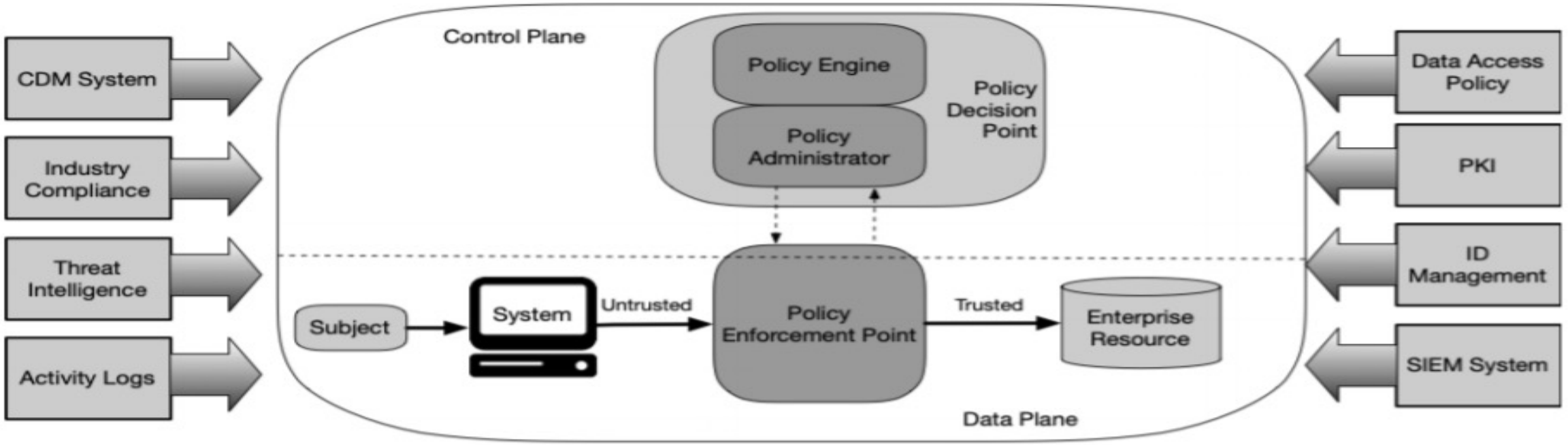


Figure 2: Core Zero Trust Logical Components

23

Best Practices for Data Focused Missions

Zero Trust Maturity Model

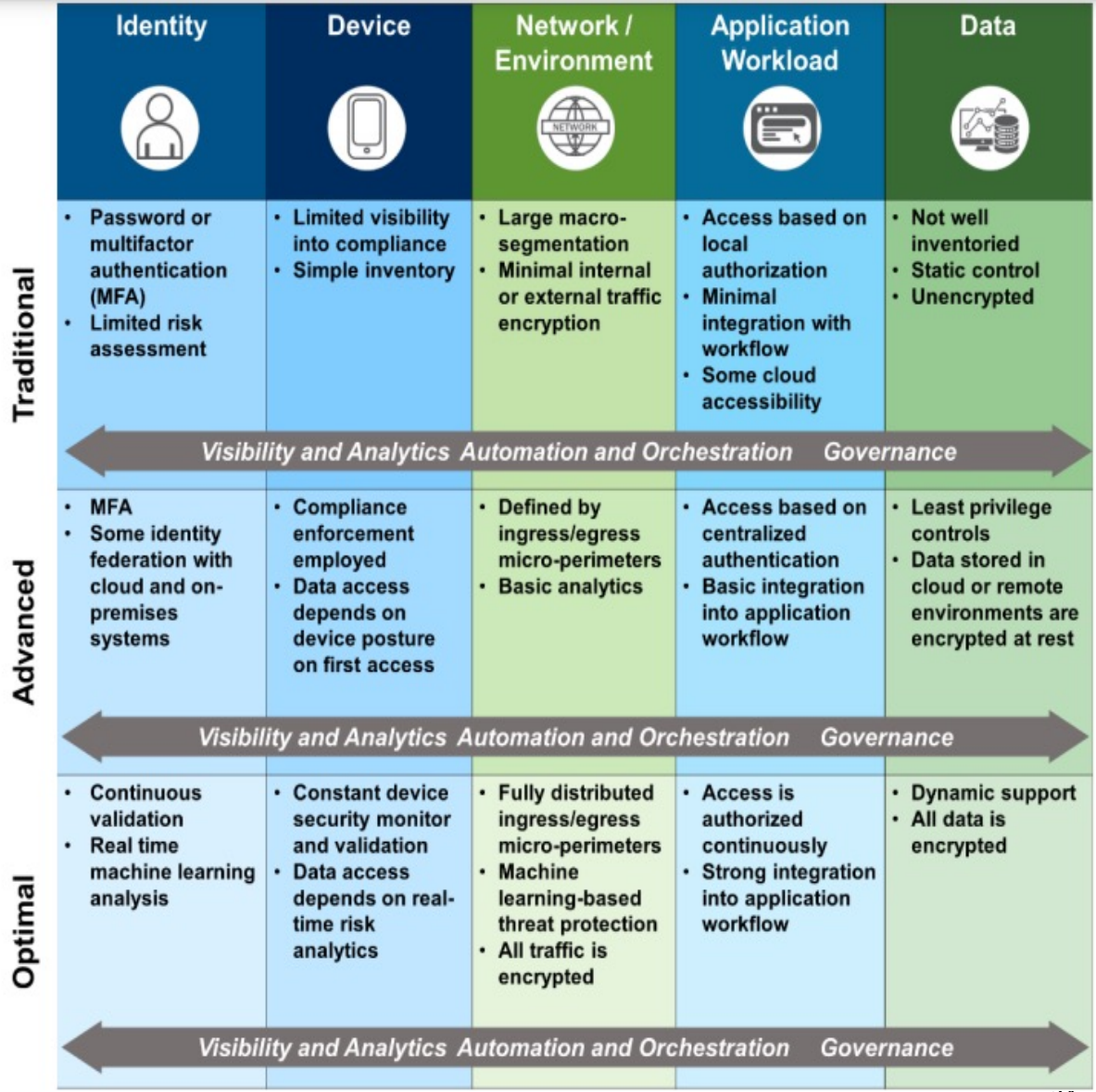
Pre-decisional Draft

June 2021

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf



Best Practices for Data Focused Missions

Zero Trust Architecture Resources:

1. https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture
2. https://media.defense.gov/2022/May/11/2002994383/-1/-1/0/CSA_Protecting_Against_Cyber_Threats_to_MSPs_and_their_Customers_05112022.PDF
3. https://csrc.nist.gov/publications/detail/sp/800-207/final
4. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf
5. https://www.actiac.org/zero-trust-cybersecurity-current-trends
6. https://www.mitre.org/publications/technical-papers/achieving-mission-assurance-for-enterprises-today-and-tomorrow-zero-trust-the-cloud-and-other-tools

Helpful Federal Resources

- US Department of Education
  - https://studentprivacy.ed.gov/
  - https://rems.ed.gov

- FBI
  - Internet Crime Compliant Center (https://www.ic3.gov/default.aspx)
  - Local Field Offices (Establish a relationship sooner than later!)
    - https://www.fbi.gov/contact-us/field-offices
  - Infragard (https://www.infragard.org/)

- Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml)
  - Electronic Crimes Task Forces (ECTFs) (United States Secret Service)

  - https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20An%20Introductory%20Guide%20v%201.1.pdf

Helpful Federal Resources

- DOJ Best Practices for Victim Response and Reporting of Cyber Incidents -
  - https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

- NSA's Top Ten Cybersecurity Mitigation Strategies
  - https://www.iad.gov/iad/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm

- United States General Services Administration FedRAMP Program
  - https://www.fedramp.gov/training/

- Not Federal ☺ StateRAMP
    - https://stateramp.org/faqs/

27

Helpful Federal Resources

Cyber Infrastructure and Security Agency

Request information about the service(s) you are interested in by emailing ncats_info@hq.dhs.gov.

All services are available at no cost to federal agencies, state and local governments, critical infrastructure, and private organizations generally.

Cyber Hygiene: Vulnerability Scanning helps secure your internet-facing systems from weak configuration and known vulnerabilities, and encourages the adoption of modern security best practices. DHS performs regular network and vulnerability scans and delivers a weekly report for your action. Once initiated, this service is mostly automated and requires little direct interaction. After we receive the required paperwork for Cyber Hygiene, our scans will start within 72 hours and you'll begin receiving reports within two weeks.
Cyber Hygiene Sample Report

A **Phishing Campaign Assessment** (PCA) measures your team's propensity to click on email phishing lures. Phishing is commonly used as a means to breach an organization's network. The assessment occurs over a 6 week period, and the results can be used to provide guidance for anti-phishing training and awareness.
Phishing Campaign Assessment (PCA) Sample Report

28

Helpful Federal Resources

Cyber Infrastructure and Security Agency

Request information about the service(s) you are interested in by emailing ncats_info@hq.dhs.gov.

All services are available at no cost to federal agencies, state and local governments, critical infrastructure, and private organizations generally.

Known Exploited Vulnerabilities:

https://www.cisa.gov/known-exploited-vulnerabilities

The KEV catalog sends a clear message to all organizations to prioritize remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework. Vulnerability management frameworks—such as the Stakeholder-Specific Vulnerability Categorization (SSVC) model—consider a vulnerability's exploitation status and the KEV catalog serves as the authoritative repository of that information. Organizations should also consider using automated vulnerability and patch management tools that automatically incorporate and flag or prioritize KEV vulnerabilities. Examples of such tools include CISA's cyber hygiene services, Palo Alto Networks Cortex, Tenable Nessus, Runecast, Qualys VMDR, Wiz, Rapid7 InsightVM, and Rapid7 Nexpose. Organizations with additional tools that are incorporating the KEV vulnerabilities can be added to this list by emailing CISA.JCDC@CISA.DHS.GOV.

29

Helpful Federal Resources

Helpful Federal Resources

Foundational Measures

All organizations should take certain foundational measures to implement a strong cybersecurity program:

- **Fix the known security flaws in software.** Check the CISA Known Exploited Vulnerabilities (KEV) Catalog for software used by your organization and, if listed, update the software to the latest version according to the vendor's instructions. **Note:** CISA continually updates the KEV catalog with known exploited vulnerabilities.
- **Implement multifactor authentication (MFA).** Use multifactor authentication where possible. MFA is a layered approach to securing your online accounts and the data they contain. When you enable MFA in your online services (like email), you must provide a combination of two or more authenticators to verify your identity before the service grants you access. Using MFA protects your account more than just using a username and password. Why? Because even if one factor (like your password) becomes compromised, unauthorized users will be unable to meet the second authentication requirement, ultimately stopping them from gaining access to your accounts.
- **Halt bad practices.** Take immediate steps to: (1) replace end-of-life software products that no longer receive software updates; (2) replace any system or products that rely on known/default/unchangeable passwords; and (3) adopt MFA (see above) for remote or administrative access to important systems, resources, or databases.
- **Sign up for CISA's Cyber Hygiene Vulnerability Scanning.** Register for this service by emailing vulnerability@cisa.dhs.gov. Once initiated, this service is mostly automated and requires little direct interaction. CISA performs the vulnerability scans and delivers a weekly report. After CISA receives the required paperwork, scanning will start within 72 hours and organizations will begin receiving reports within two weeks. **Note:** vulnerability scanning helps secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices.
- **Get your Stuff Off Search (S.O.S.).** While zero-day attacks draw the most attention, frequently, less complex exposures to both cyber and physical security are missed. Get your Stuff Off Search–S.O.S.–and reduce internet attack surfaces that are visible to anyone on web-based search platforms.

31

Helpful Federal Resources

Free Services and Tools

After making progress on the measures above, organizations can use the free services and tools listed below to mature their cybersecurity risk management. These resources are categorized according to the four goals outlined in CISA Insights: Implement Cybersecurity Measures Now to Protect Against Critical Threats:

1.Reducing the likelihood of a damaging cyber incident;
2.Detecting malicious activity quickly;
3.Responding effectively to confirmed incidents; and
4.Maximizing resilience.

Expand All Sections

Reducing the Likelihood of a Damaging Cyber Incident

Take Steps to Quickly Detect a Potential Intrusion

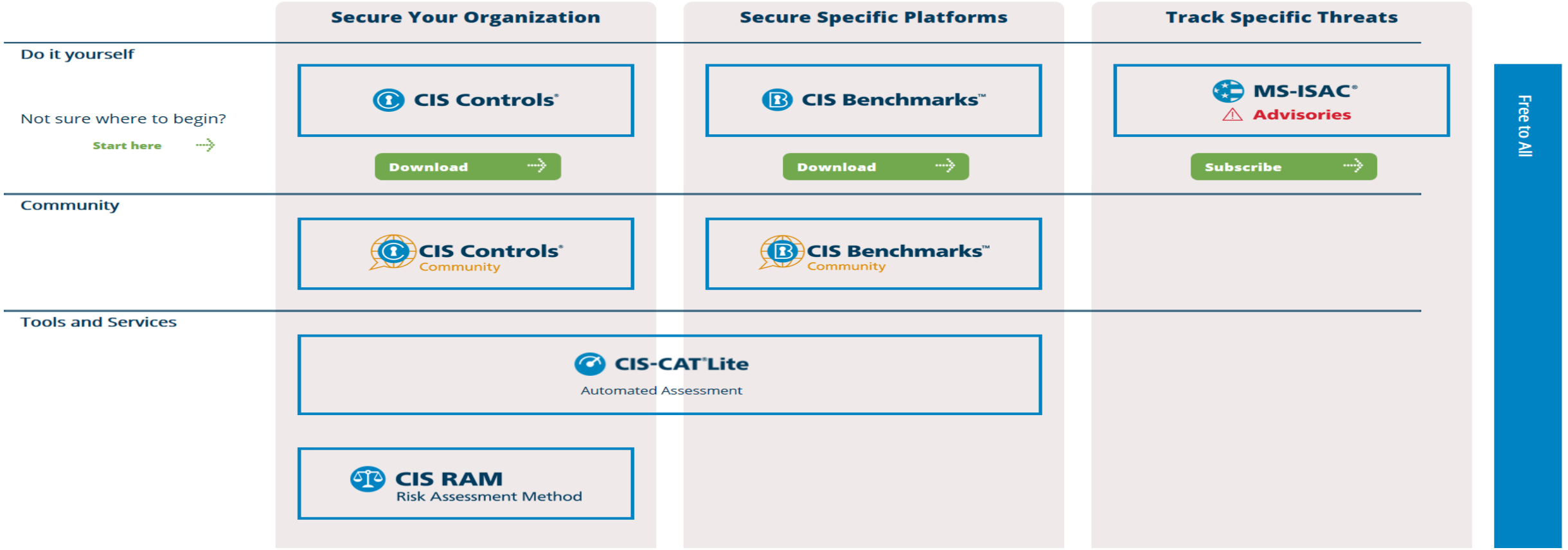
Ensure That The Organization is Prepared to Respond if an Intrusion Occurs

Maximize the Organization's Resilience to a Destructive Cyber Incident

32

MS-ISAC

- MS-ISAC (https://www.cisecurity.org/ms-isac/)
  - Connects back to the US Department of Homeland Security



MS-ISAC

CIS CSAT

CIS Hardened Images®

CIS Services®

CIS CyberMarket®

Albert
Network Monitoring

CIS SecureSuite®
Membership

Includes Build Kits and Automatic Remediation Content

CIS-CAT® Pro

MS-ISAC®
Membership

24/7 Security Operations Center
Incident Response Services

See All Benefits

Pay Per Use

Only for U.S. SLTT*

THANKS!!!!

Questions??

Contact me:

Steven G Hernandez

Steven.Hernandez@ed.gov

35