Cybersecurity Best Practices for Minnesota Housing Authorities

HI, I'M NATE SCHMITT

- Lead CIT's Cybersecurity team/vCISO
- Instructor
- 30+ ransomware engagements
- 250+ business email compromises
- Own two classic cars

linkedin.com/in/nateschmitt

Cybersecurity Best Practices for Minnesota Housing Authorities

Takeaways:

1. Understanding Cybersecurity Challenges
2. Core Cybersecurity Best Practices
3. Cybersecurity Beyond the Workplace

The Basics

Understanding Adversaries

Type of Threat Actor	Motives
State Sponsored	Espionage, theft, or furthers other national interests
Organized Crime	Financial gain
Hacktivists	Exposing secrets, disrupting service to those with differing morals
Insiders	Bypassing controls, further self-interests
Script Kiddies	Vandalism, Curiosity

Key Terminology

Security Incident

A security event that compromises an asset's integrity, confidentiality, or availability

Security Breach

*An incident that results in the **confirmed disclosure of data** to an **unauthorized party***

The Trends

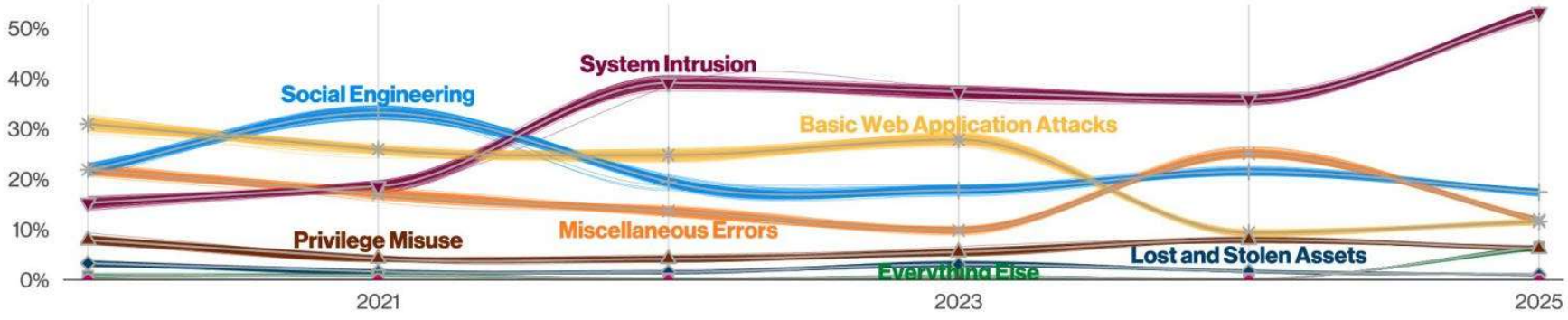


Figure 44. Patterns over time in breaches (n for 2025 dataset=12,195)

Credit: 2025 Verizon DBIR

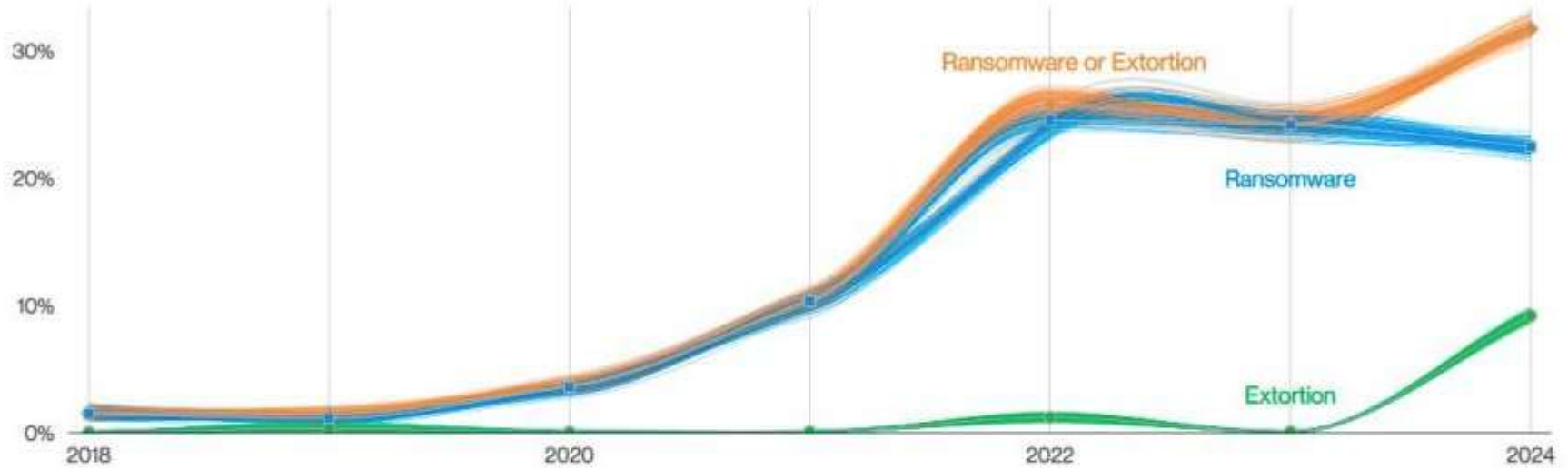
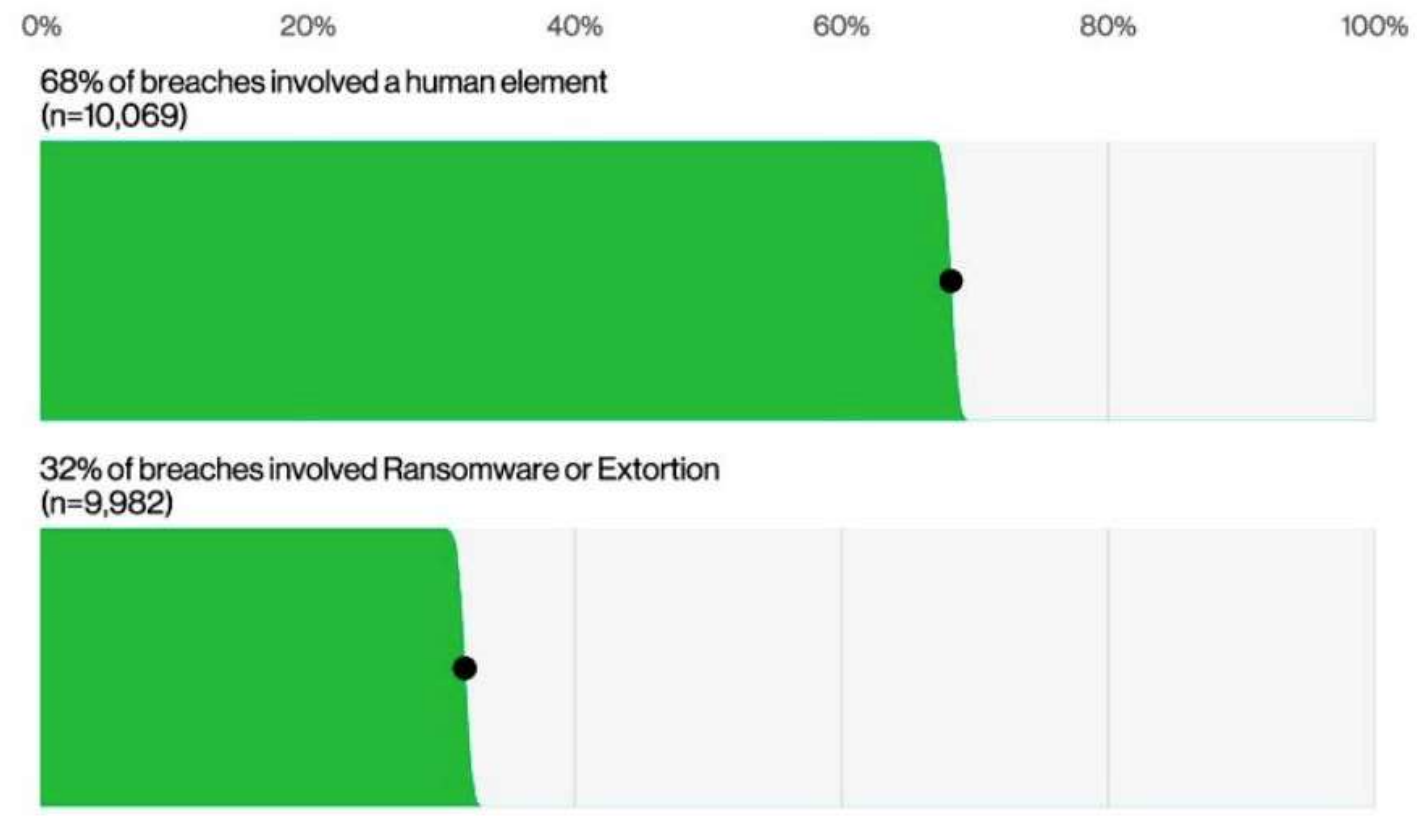


Figure 2. Ransomware and Extortion breaches over time

Credit: 2024 Verizon DBIR



Credit: 2024 Verizon DBIR

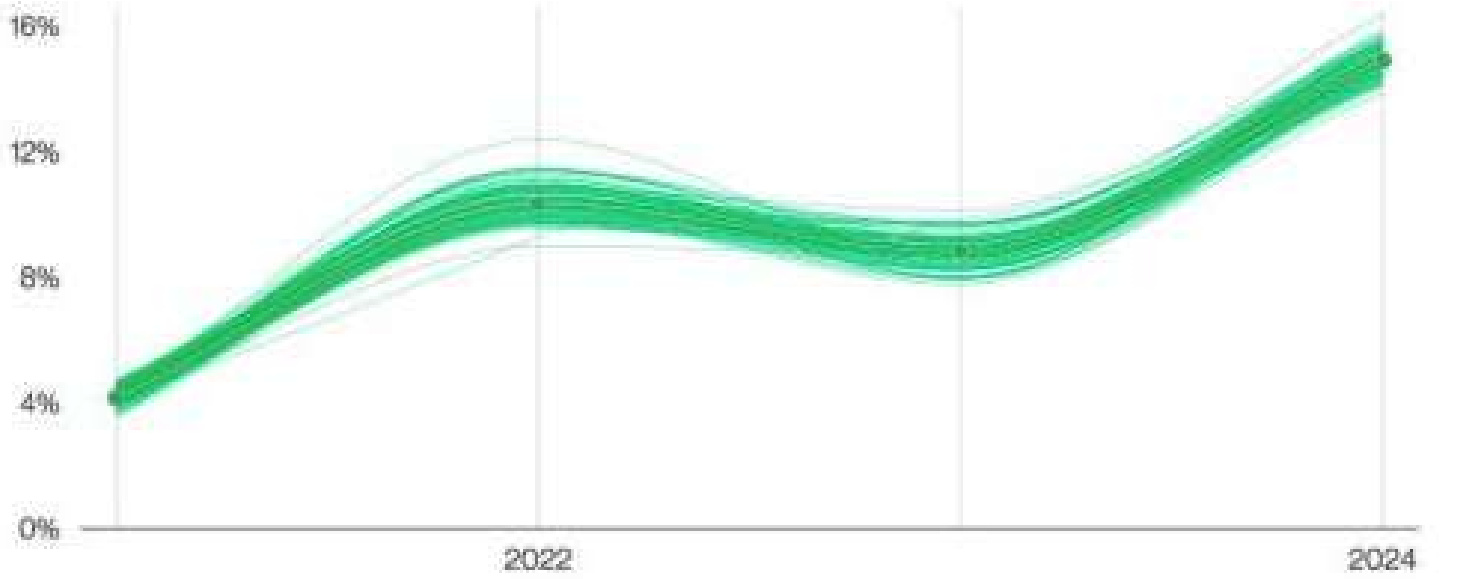
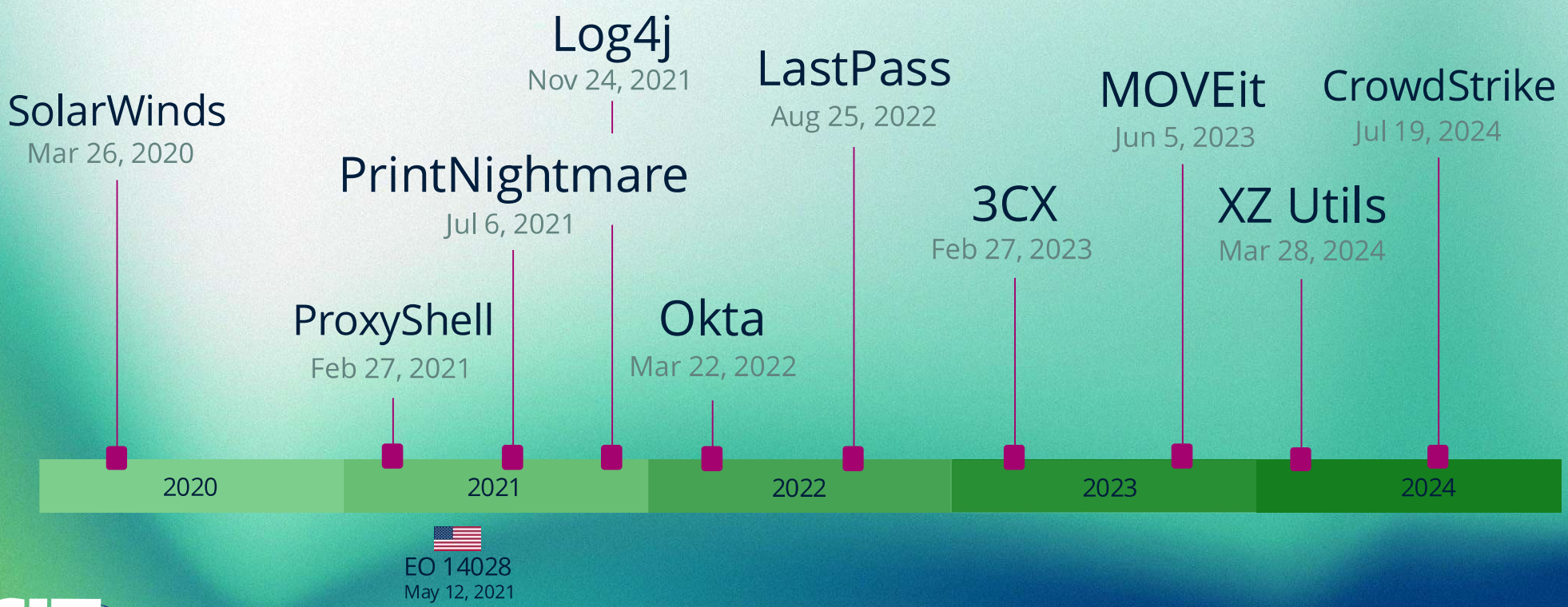


Figure 9. Supply chain interconnection in breaches over time

Credit: 2024 Verizon DBIR

Notable Supply Chain Events



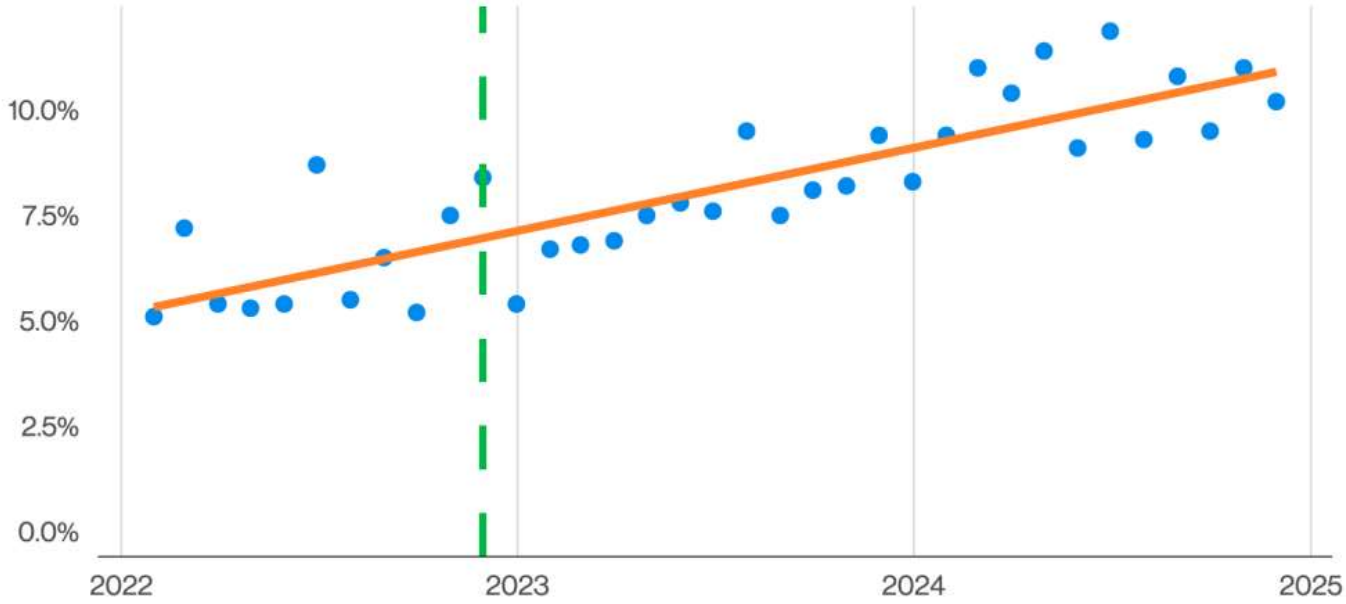


Figure 23. Percentage of AI-assisted malicious emails over time

Credit: 2025 Verizon DBIR

Housing Authority Challenges

1. Managing sensitive resident data
2. Communicating with partners/vendors securely
3. Limited on-staff IT personnel
4. High volume of new email contacts

Phishing Examples

CHANGE OF BANK INFORMATION -Jason Quigley

JQ

Jason Quigley <smtp@tpa-im.com>

To: Ali Berndt

This message is high importance.

Hi Ali,

I hope today is going well for you! Due to some issues with my previous bank, I had to switch, thus I need to update my bank information for my paycheck. Could you kindly assist me ?

Regards

Jason Quigley
Customer Relationship Manager
CIT

From: Zhuohui Wu <zhuohui.wu@email-bakermckenzie.com>
Sent: Saturday, February 22, 2025 08:03 AM
To: Kyle Etter <kyle.etter@cit-net.com>
Subject: Fw: Payment Due

Hello Kyle Etter,

We would like to kindly remind you that the payment for your invoice is related to the following services:

Market Entry Strategy and Compliance Advisory
Cross-Border Business Expansion and Global Mobility Solutions
Succession Planning and Value Optimization for Long-Term Growth
It is now overdue. As of today, the balance has remained unpaid for over 30 days. We highly value your partnership and are eager to resolve this matter immediately.
We kindly request that this issue be addressed promptly to avoid any further delays or potential disruptions. Please note that late fees have been accruing on the outstanding balance since December 5th.
We understand that unforeseen circumstances can sometimes arise, and we are more than willing to assist you in any way necessary to facilitate the payment process.

Thank you for your immediate attention to this matter. We look forward to your swift resolution.

Warm Regards,
Zhuohui Wu
Partner
2501 N. Harwood Street, Suite 1850, Dallas, TX 75201

Hello AP,

I am attaching the outstanding invoice, which Kyle Etter has asked me to forward to you. For your reference, the conversation below provides additional context regarding the matter.
We request payment be made as soon as possible, as the invoice is now significantly overdue.

Thank you.
Zhuohui Wu
Partner
2501 N. Harwood Street, Suite 1850, Dallas, TX 75201

Begin forwarded message:

From: Kyle Etter <kyle.etter@cit-net.com>
Sent: Saturday, Feb 22, 2025 10:46 AM
To: Zhuohui Wu <zhuohui.wu@email-bakermckenzie.com>
Subject: Payment Due

Hi Zhuohui,

I've received the attached invoice and reviewed it. I understand that the payment is overdue. Just a quick note—I provided nancy.plung@cit-net.com as the contact for all invoice-related matters during my onboarding with your firm.
Could you please make sure to send the invoice to that address? We will take care of it by tomorrow at the latest. Thanks for your attention to this.

Thank you,
Kyle Etter

COMPUTER INTEGRATION TECHNOLOGIES, INC. #013055296 Invoice

C

customersvc@leaseadmincenter.com <customersvc@leaseadmincenter.com>

To: Sarah Burns

013055296 COMPU...
621.8 KB

Download All • Preview All

Lease Administration Center

Attached is the current invoice for the above customer. To expedite and ensure accurate posting, please include a copy of the invoice coupon with your payment.

If you have any questions, please call Customer Service at 800.959.5936 or email Customersvc@leaseadmincenter.com for assistance.

Thank You,

Customer Service Department
Lease Administration Center

Email: Customersvc@leaseadmincenter.com
Phone: **800.959.5936**

Fax: **866.939.4705**

INV16898

1600-01-00-0100488-0001-0000497

ORACLE
FINANCING

ORIGINAL INVOICE
ISSUED 05/17/25

INVOICED IN
US DOLLARS

Date Due:	07/01/25
Invoice No.	013055296
Previous Amt Due:	$0.00 USD
Current Amt Due:	$20,479.56 USD
Total Amt Due:	$20,479.56 USD
AMT ENCLOSED	

BANC OF AMERICA LEASING
LEASE ADMINISTRATION CENTER
PO BOX 405874
ATLANTA, GA 30384-5874

For change of address,
please e-mail/fax Customer Service.

0100488 01 MB 0.62 **AUTO T3 1 1600 55125-440675 -C01-P00000-I 2

COMPUTER INTEGRATION TECHNOLOGIES, INC.
SARAH BURNS
2375 Ventura Dr
Woodbury, MN 55125-4406
UNITED STATES

REMIT TO:

BANC OF AMERICA LEASING
LEASE ADMINISTRATION CENTER
PO BOX 405874
ATLANTA, GA 30384-5874

0000006501305529650032411140000010000207867500002047956000020479560006085734 5

PLEASE RETURN TOP PORTION WITH YOUR PAYMENT TO ENSURE PROPER CREDIT

For assistance with your invoice:	PHONE	FAX	TIME	E-MAIL
CUSTOMER SERVICE INQUIRIES	800-959-5936	866-939-4705	8:30AM - 5:00PM EASTERN	customersvc@leaseadmincenter.com

ORACLE IS A REGISTERED TRADEMARK OF ORACLE AND/OR ITS AFFILIATES. USED UNDER LICENSE.
CONTACT US TO HAVE THIS INVOICE EMAILED

Federal Tax ID: 0
Invoice Number 013055296-75

Contract Number (Please see below) Customer Reference Number Description Model Number Serial Number	Location	Detailed Charge Description	Payment Due Date	Payment Amount	Tax	Total Due
PS232070 DTD2/18/25 PPA35160 EST1572102 SEE WIRE INSTRUCTIONS BELOW						
500-3241114-000 Your Ref: CLOUD	2375 VENTURA DR WOODBURY, MN 55125	PAYMENT	07/01/25	20,479.56		20,479.56
ASSIGNEE: BANK OF AMERICA N.A. 232070 WIRE INSTRUCTIONS: Bank Name:Bank of America N.A. Account Name: Banc of AmericaLeasing & Capital, LLC ABA: 026009593 / Account #:1257354255						
				CONTRACT SUBTOTAL		**$20,479.56**

TOTAL CURRENT CHARGES	$20,479.56 USD

BANC OF AMERICA LEASING **INVOICE NUMBER: 013055296**

Create a few educational phishing emails related to section 8 hosting.

Workflow

Certainly! Below are a few examples of educational phishing emails related to Section 8 housing. These examples are intended for training purposes only, to help individuals recognize and avoid phishing attempts.

Example 1: Fake Verification Request

Subject: Urgent: Section 8 Housing Verification Required

Dear [Recipient Name],

We hope this message finds you well. As part of our commitment to maintaining accurate records, we are conducting a routine verification of Section 8 housing assistance recipients.

To ensure that your benefits continue uninterrupted, please click the link below to verify your information:

Verify Your Account Here

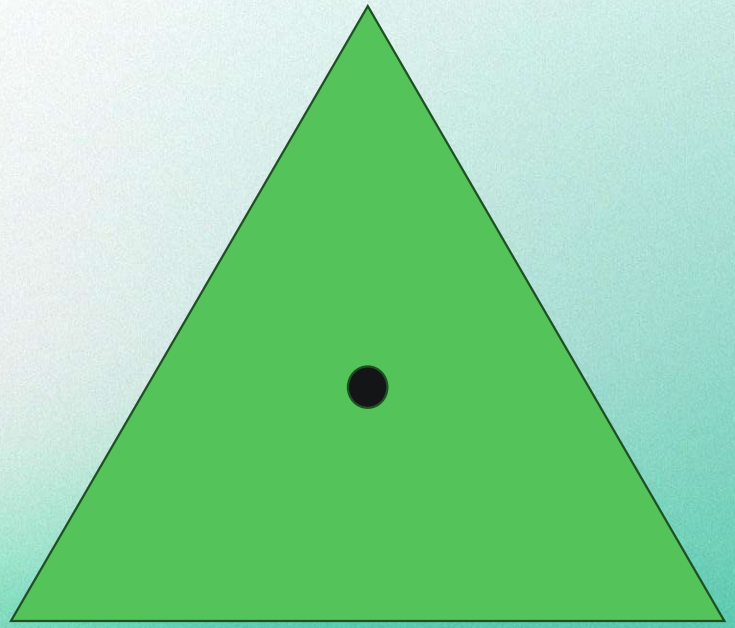
Failure to complete this verification by **June 5, 2025** will result in suspension of your benefits.

Thank you for your prompt attention to this matter.

Dark Web Tour

Corporate Protections

Security

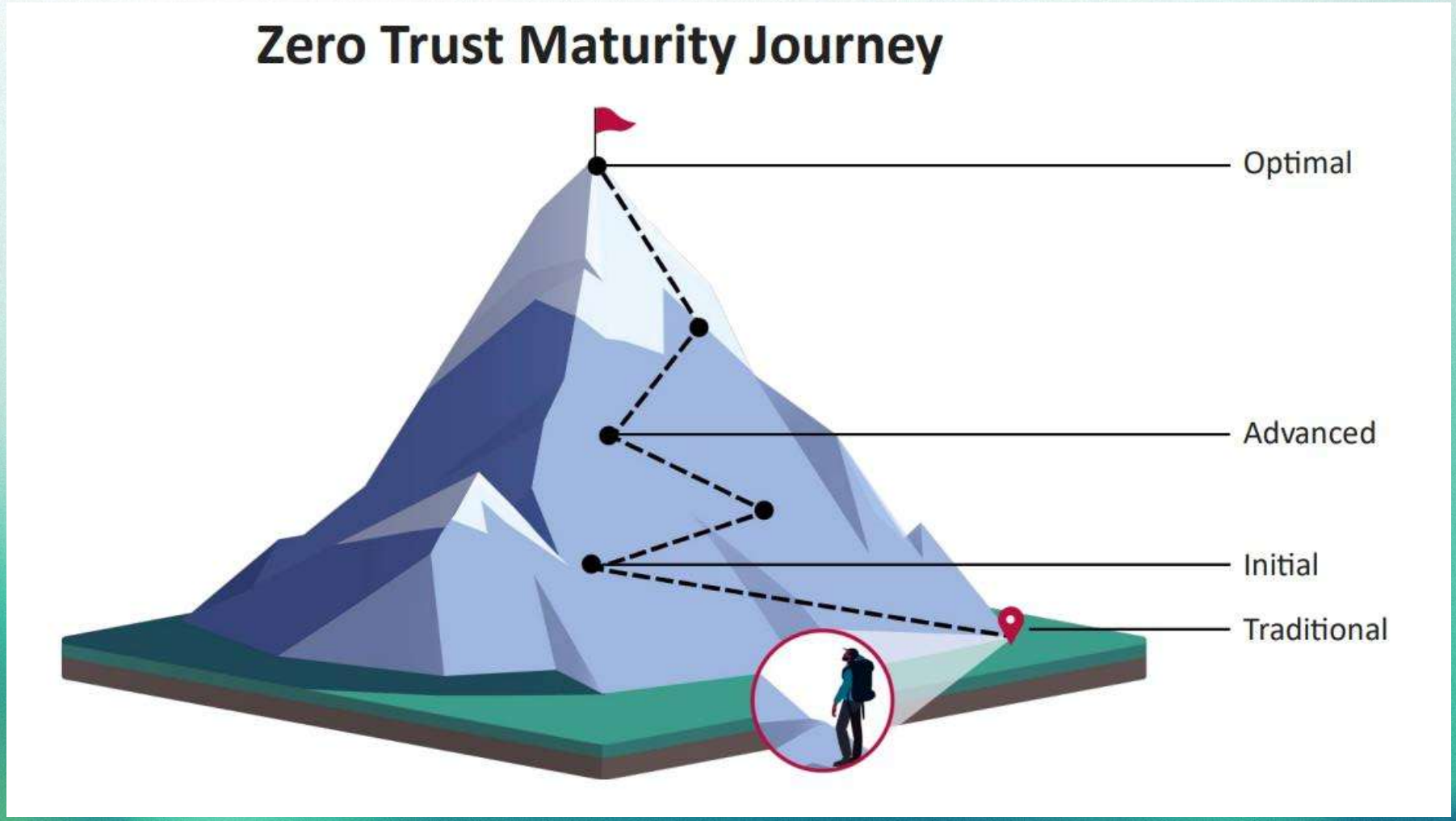


Functionality

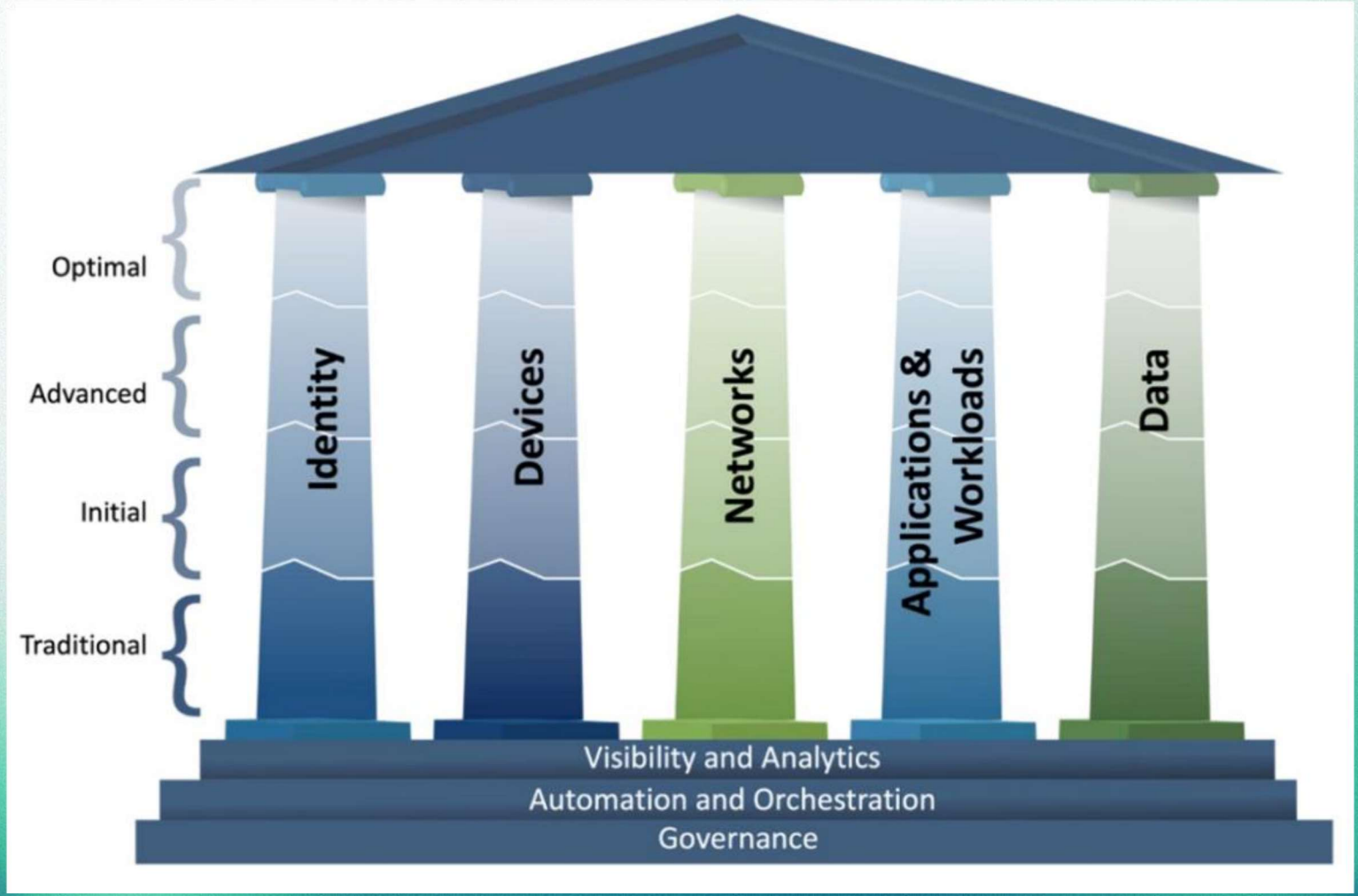
Usability

Introduction to Zero Trust

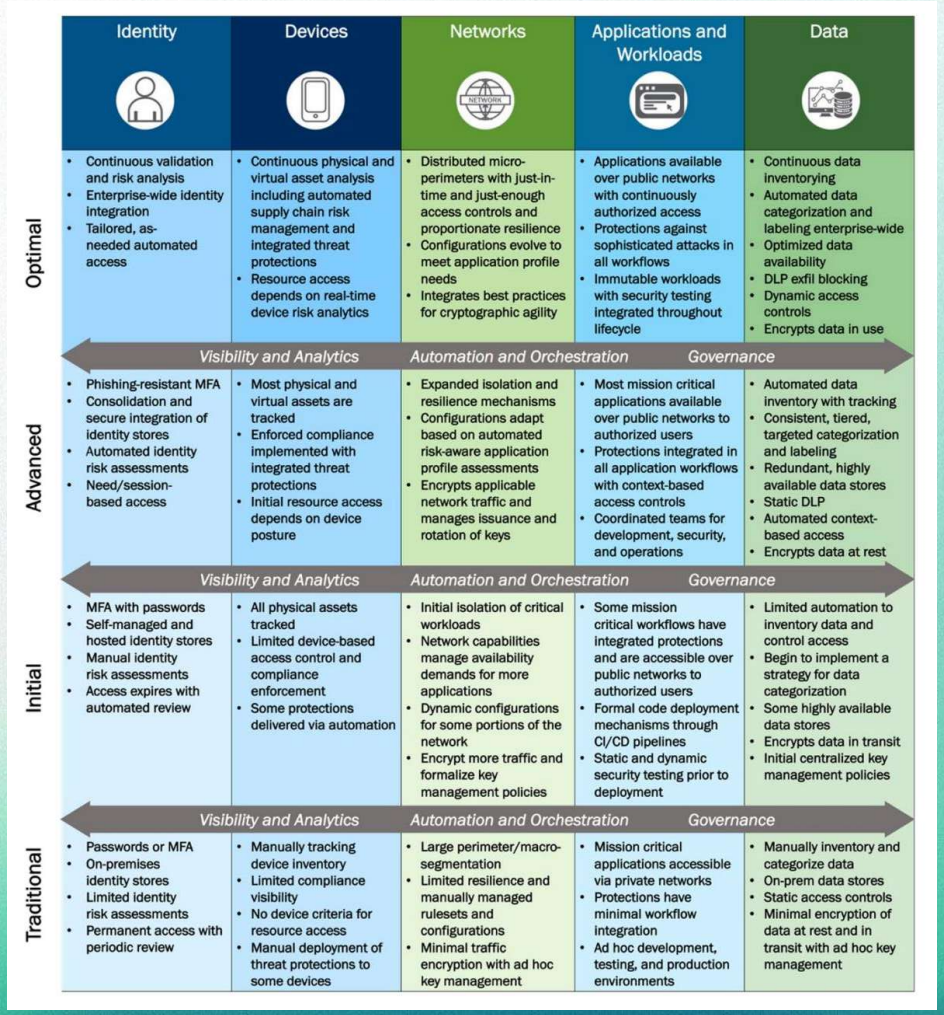
IS	IS NOT
A mentality/framework	A single product or technology
Data-focused	Perimeter-based security
Proactive	One-size-fits-all
Identity-centric	Easy to implement
Dynamic	A silver bullet to eliminate risk



Cybersecurity and Infrastructure Security Agency, 2023)



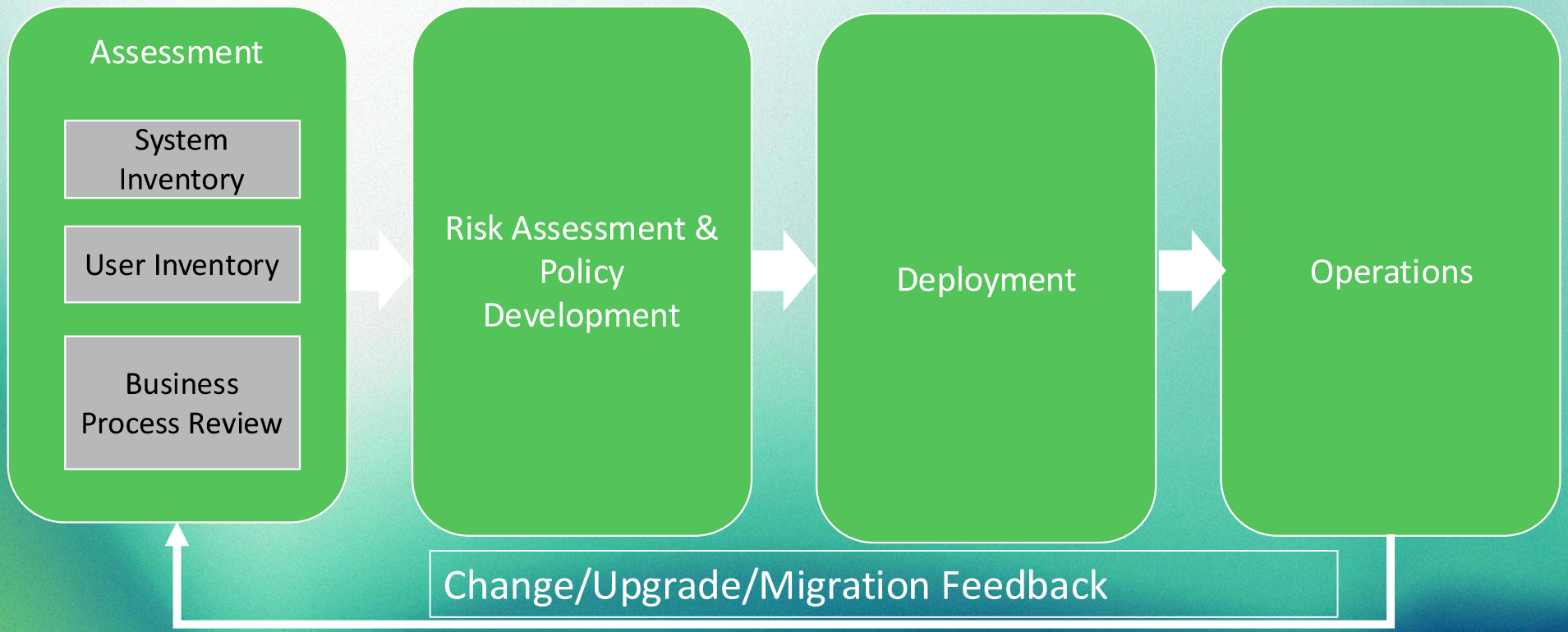
(Cybersecurity and Infrastructure Security Agency, 2023)



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

(Cybersecurity and Infrastructure Security Agency, 2023)

NIST SP 800-207 Deployment Cycle



Implementation Plan

1. Define Strategy
2. Inventory Resources
3. Define Scope

4. Enhance Device Security
5. Network Segmentation
6. Implement IAM

7. Implement SIEM
8. Deploy DLP
9. Automate Processes

10. Monitor & Adapt

Foundation & Strategy

Core Security Infrastructure

Advanced Capabilities

Continuous Improvement

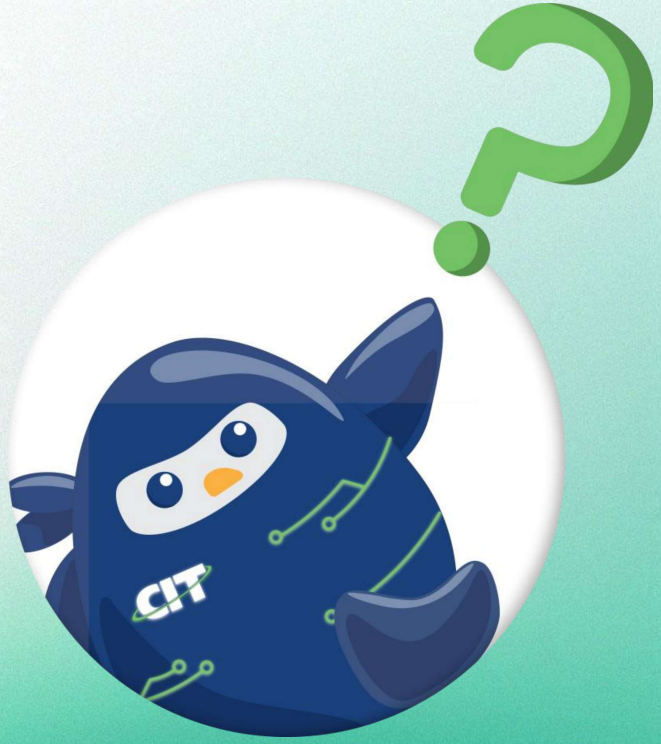
Core Recommendations

- Phishing Resistant MFA
- Endpoint Detection & Response (EDR)
- Application Allowlisting
- Privileged Access Management
- Zero Trust Network Access (ZTNA)
- Network Access Control (NAC)
- Security Awareness Training
- BCDR Review

Beyond the Workplace

Personal Recommendations

1. Freeze your credit
2. Do not reuse passwords (especially email/banking)
3. Enable multi-factor authentication
4. Assess current emotions while online
5. Educate family/friends


CIT

LET’S CONNECT

Nate Schmitt

www.cit-net.com

nate.schmitt@cit-net.com

651.255.5773

linkedin.com/in/nateschmitt

MAKING TECHNOLOGY WORK FOR BUSINESS