Information Security Compliance and Threat Trends at MIT

IT Partners June 14, 2022

Jessica Murray

Information Security Officer

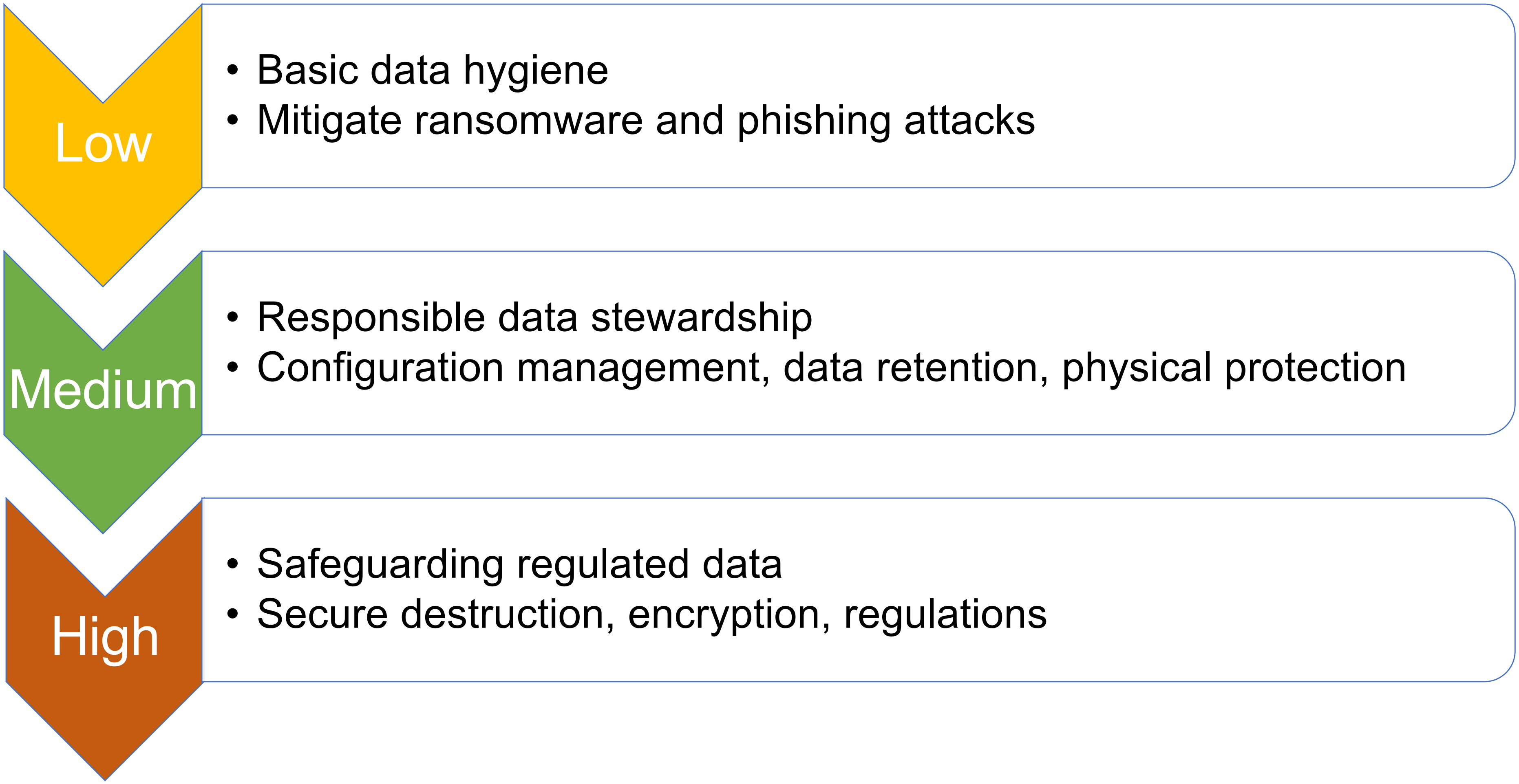
Information Systems & Technology

Outline

- Information Security Compliance Trends
- IS&T Security Phishing response workflows
- Phishing Feud

InfoProtect.mit.edu: Data Classification

A flexible framework that enables DLCs to appropriately secure MIT information according to level of risk posed by loss of confidentiality, integrity or availability



Low

- Basic data hygiene
- Mitigate ransomware and phishing attacks

Medium

- Responsible data stewardship
- Configuration management, data retention, physical protection

High

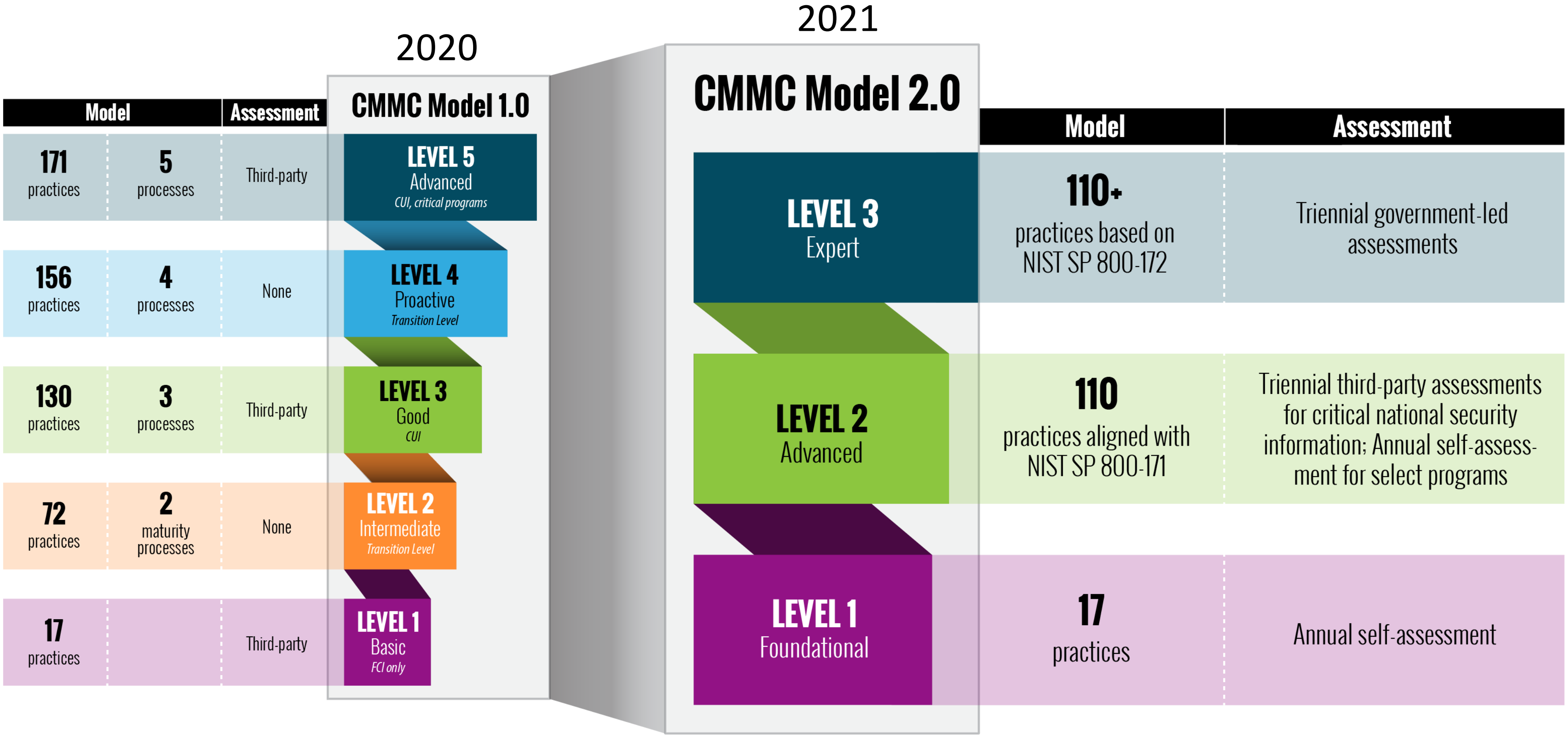
- Safeguarding regulated data
- Secure destruction, encryption, regulations

Data Security Compliance

Impact on MIT data

Framework	Applies to
CMMC	Federal Government and DoD funded research
NIST SP 800-171	Government contractors handling Controlled Unclassified Information (CUI - CMMC Level 3) Federal Student Aid
NASA	NASA sponsored research
NIH	NIH sponsored research
DOE	DOE sponsored research
HIPAA	Covered entities and Protected Health Information (PHI)
DUAs	Various state/local agency requirements, industry contracts

CMMC
Cybersecurity Maturity Model Certification



2020

CMMC Model 1.0

Model		Assessment	
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

2021

CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

SPRS – Supplier Performance Risk System

What is NIST SP 800-171?

110 Controls in 14 Categories

Access control

- limits system access to authorized users

Awareness and training

- alerts employees to information security risks

Audit and accountability

- creation, protection, retention, and review of system logs

Configuration management

- creation of baseline configurations and use of robust change management processes

Identification and authentication

- central authentication and multi-factor for local and network access to resources

Incident response

- developing operations to prepare for, detect, analyze, contain, recover from, and respond to incidents affecting

Maintenance

- maintenance of systems

Media protection

- sanitization and destruction of media containing CUI

Personnel security

- screening individuals before granting them access to information systems with CUI

Physical protection

- limiting physical access to systems to only authorized individuals

Risk assessment

- assessing the operational risk associated with processing, storage, and transmission of CUI

Security assessment

- assessing effectiveness of security controls and addressing deficiencies to limit vulnerabilities

System and communications protection

- use of secure design principles in system architecture and software development life cycle

System and information security

- monitoring for an alerting on system flaws and vulnerabilities

Implementing NIST 800-171

The following breakdown of impact is based on Virginia Tech's analysis

26 Controls have a potential **High Impact** to the Institute.

- Controls are difficult, if not impossible to accomplish in a higher education environment.

67 Controls have a potential **Medium Impact** to the Institute

- Can be accomplished, but will require changes to policy, operational procedure, or other methods.

16 Controls have a potential **Low Impact** to the Institute

- Either already being accomplished, or very little needs to be changed in order for the control to be met.

Sample High Impact controls:

- Monitor and control remote access sessions.
- Route remote access via managed access control points.
- Authorize wireless access prior to allowing such connections.
- Control connection of mobile devices.
- Provide audit reduction and report generation to support on-demand analysis and reporting.
- Limit management of audit functionality to a subset of privileged users. Track, review, approve/disapprove, and audit changes to information systems.
- Analyze the security impact of changes prior to implementation.
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
- Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
- Control the use of removable media on information system components.
- Prohibit the use of portable storage devices when such devices have no identifiable owner.
- Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).
- Control information posted or processed on publicly accessible information systems.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

NSPM-33

National Security Presidential Memorandum 33
On National Security Strategy for US Government-Supported Research and Development
Implementation Guidance January 2022

- All research institutions with research volumes >$50M need to establish research security program
  - Cybersecurity
  - Foreign travel security
  - Insider threat awareness and identification
  - Export control training
- Requirement to certify compliance
- Maintain description of security program and provide documentation to sponsoring agency upon request
- Establish a research security program ASAP

NSPM-33 Implementation Guidance Cybersecurity requirements

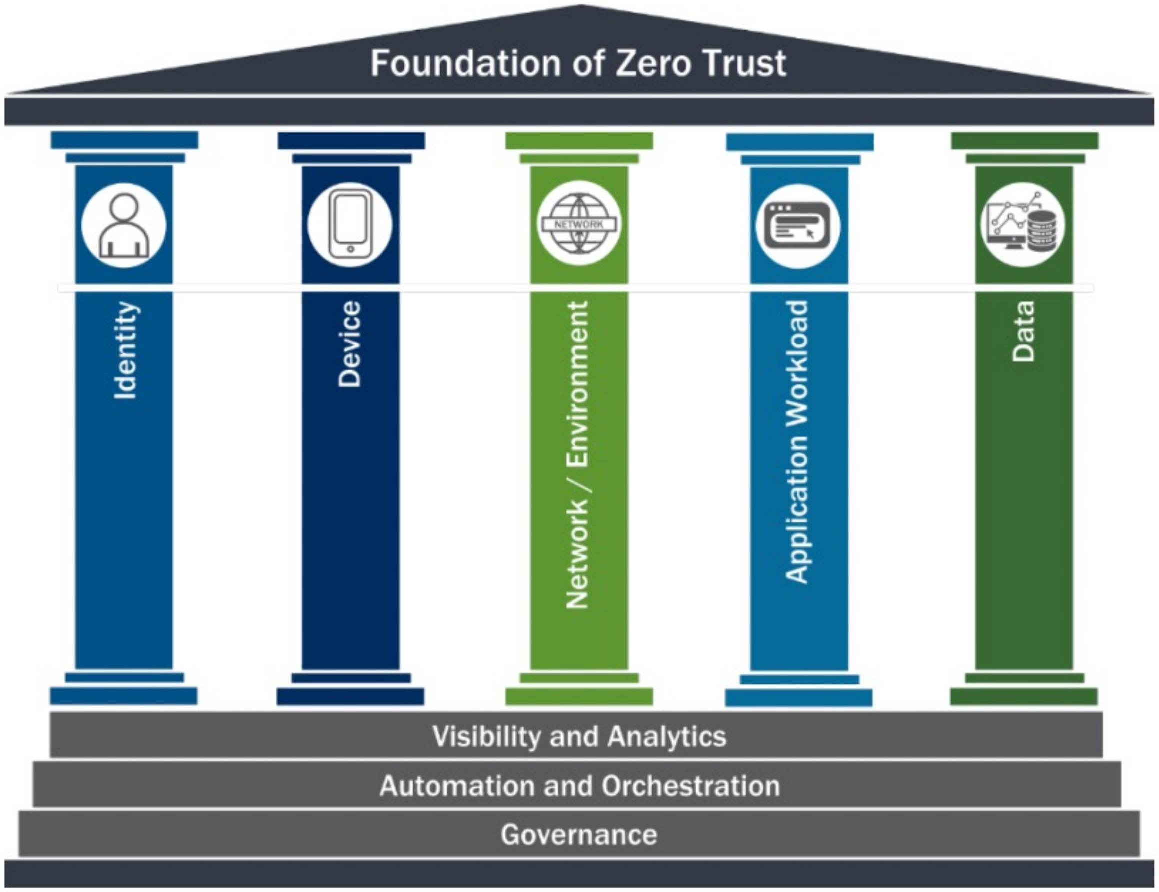
- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- Verify and control/limit connections to and use of external information systems.
- Control any non-public information posted or processed on publicly accessible information systems.
- Identify information system users, processes acting on behalf of users, or devices.
- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- Provide protection of scientific data from ransomware and other data integrity attack mechanisms.
- Identify, report, and correct information and information system flaws in a timely manner.
- Provide protection from malicious code at appropriate locations within organizational information systems.
- Update malicious code protection mechanisms when new releases are available.
- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

OMB M-22-09

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 2022

- May 17 MIT News article on LL efforts
- NIST SP 800-207 Zero Trust Architecture

- Identity: Enterprise managed identities and MFA
- Devices: A complete inventory of every device, and can prevent, detect, and respond to incidents on those devices
- Networks: Agencies encrypt all DNS and HTTP and break down their perimeters into isolated environments
- Applications and Workloads: Treat all applications as internet-connected, routinely scan and test
- Data: Deploy protections that make use of thorough data categorization.

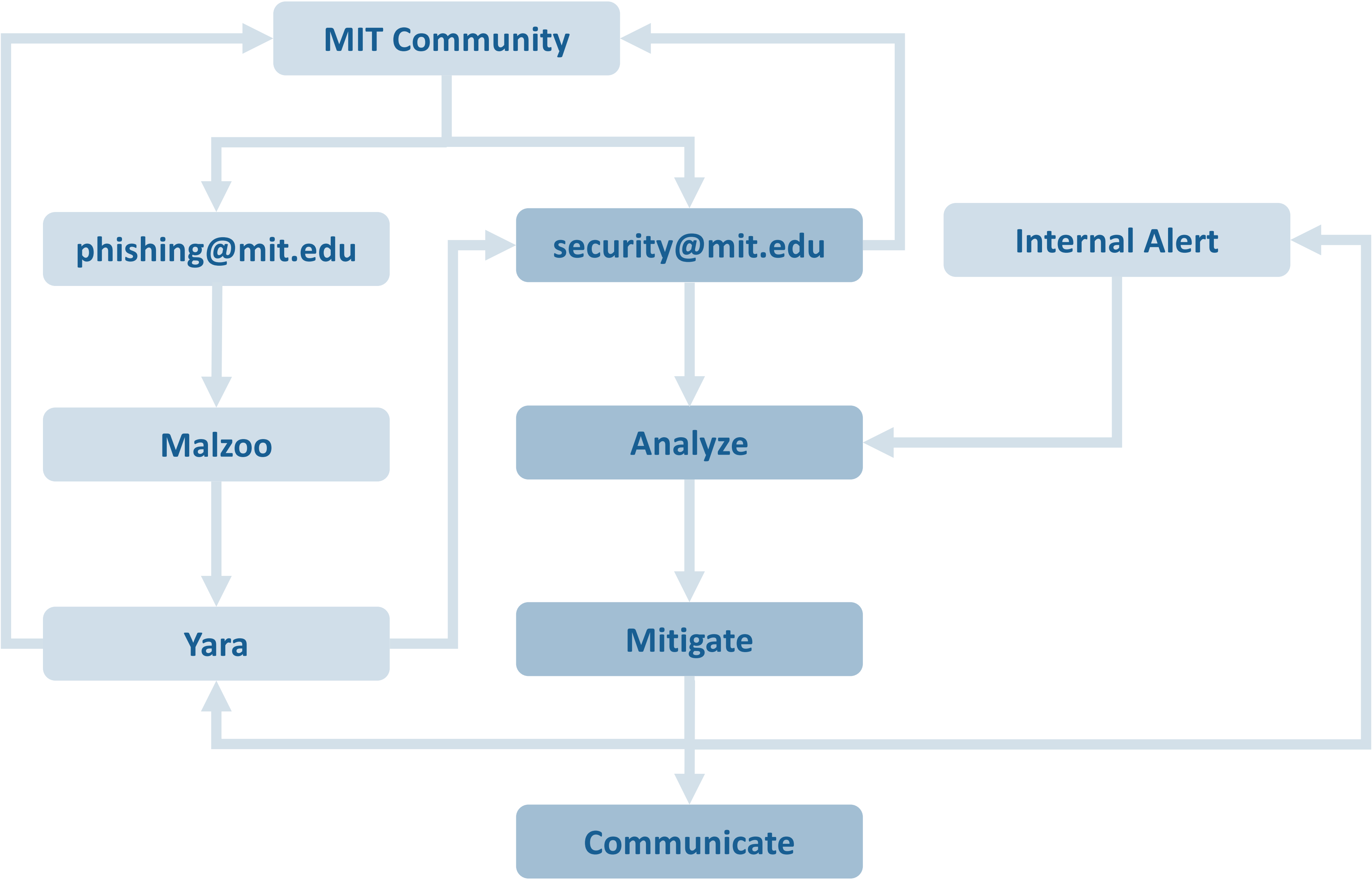


CISA’s Zero Trust Maturity Model

What does this mean for MIT?

Protecting our community	• Improved Cybersecurity Training – KnowBe4 • Centrally managed endpoint devices
Strengthening email security	• Accelerated O365 migration • Offer centrally provided Gmail • Retire personal email forwarding and transition local email systems
Modernize infrastructure	• Zero Password and Zero Trust authentication • Server backup infrastructure
Tightening up MIT network	• Retire open MIT wireless network • Migrate remaining public IP addresses behind firewalls

Phishing Response



MIT Community

phishing@mit.edu

security@mit.edu

Internal Alert

Malzoo

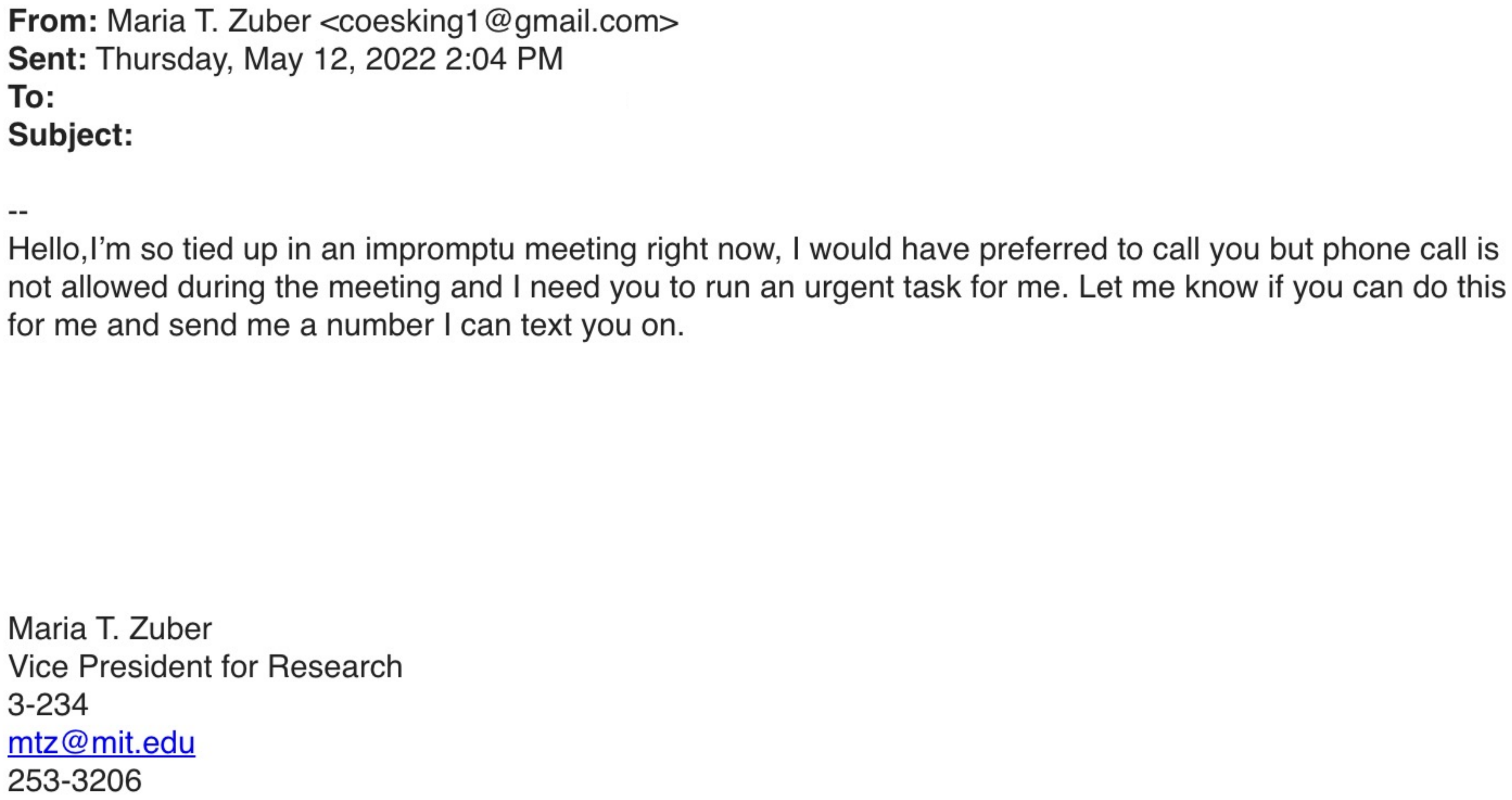
Analyze

Yara

Mitigate

Communicate

Impersonation email response



From: Maria T. Zuber <coesking1@gmail.com>
Sent: Thursday, May 12, 2022 2:04 PM
To:
Subject:

--
Hello,I'm so tied up in an impromptu meeting right now, I would have preferred to call you but phone call is not allowed during the meeting and I need you to run an urgent task for me. Let me know if you can do this for me and send me a number I can text you on.

Maria T. Zuber
Vice President for Research
3-234
mtz@mit.edu
253-3206

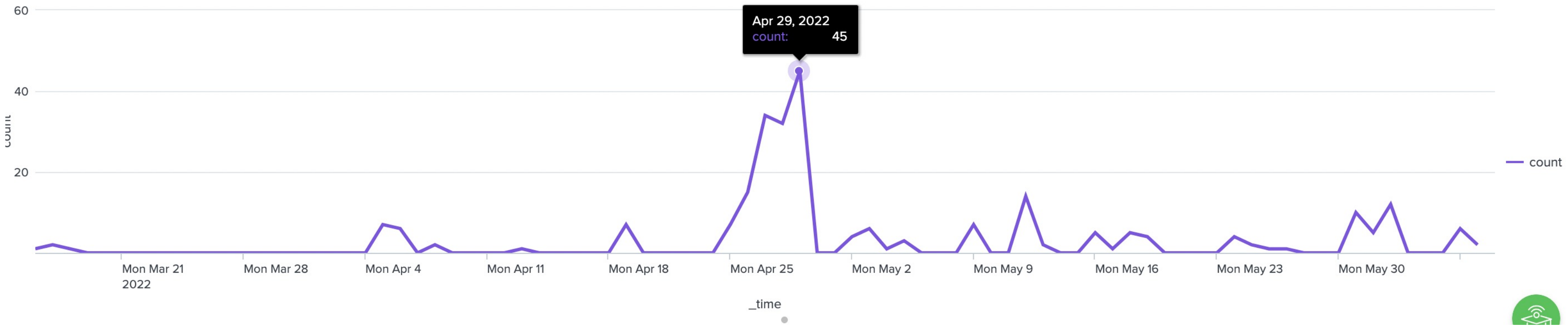
Impersonation email response

- When impersonation emails are reported to us, we have scripts that allow us to:
    - Send a notification email to everyone who received the impersonation to let them know it was fake
        - Sometimes they use the same email address to impersonate multiple people (changing the display name)
    - Request that the email being used to impersonate is blocked

Compromised Credential Dump response

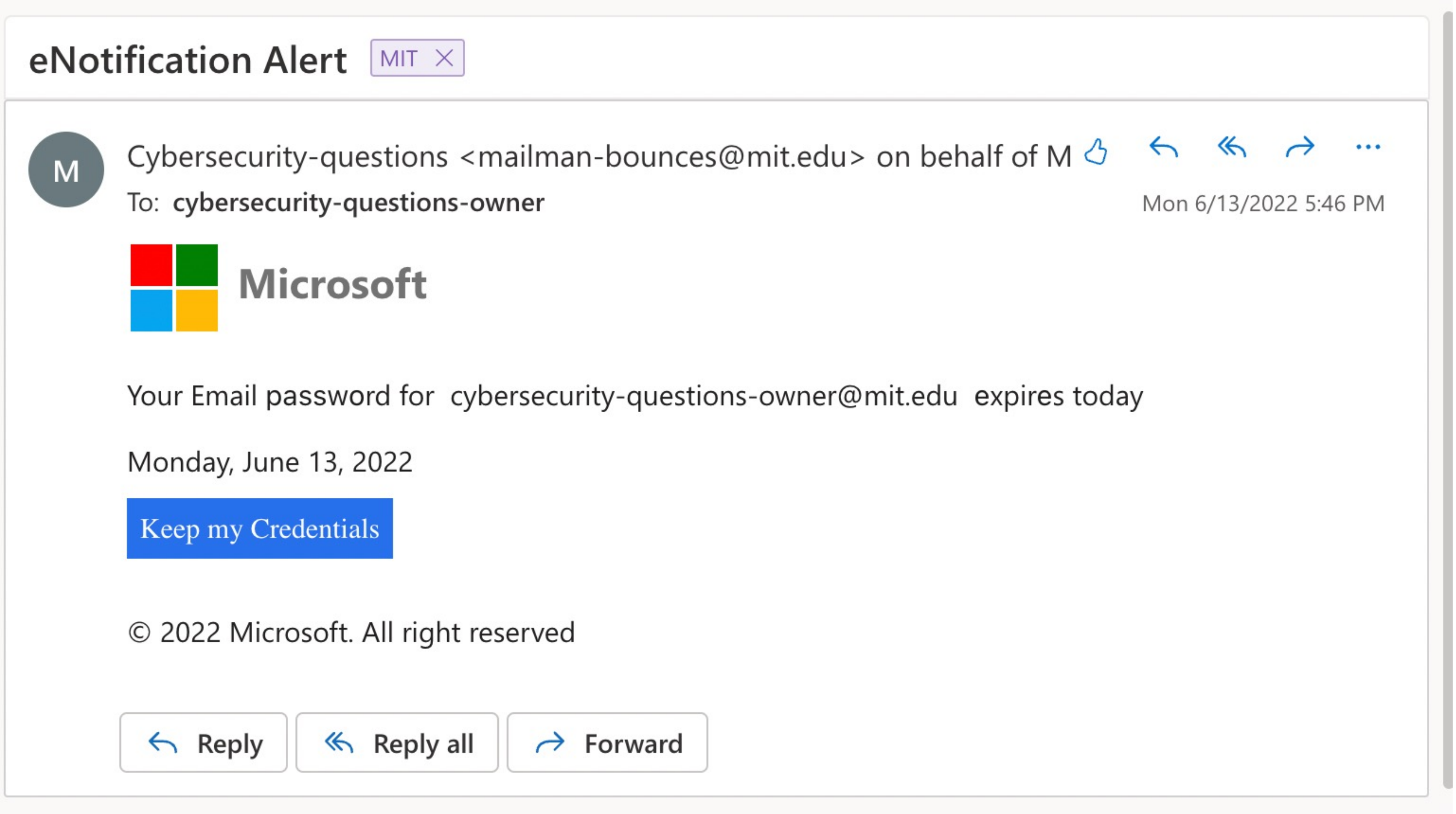
- Usernames and passwords from breaches are often consolidated into large lists
- They can be used in credential stuffing attacks, social engineering, etc.
- These are **NOT** from a breach of MIT systems, but accounts on third party websites where an MIT email address was used as the username
- When IS&T Security gets a copy of these lists, we
  - Check programmatically for password reuse against Kerberos account
  - Notify the owner of the account
  - If the compromised password was included, share that via LastPass by request
  - For other mail domains, media.mit.edu, csail.mit.edu etc, send the list of accounts to that DLC

2022 Phish-o-rama



- Past few years have seen an increase in the sophistication of phishing attacks
- Corresponding increase in the number of compromised MIT accounts

Yesterday’s phishing



eNotification Alert

M Cybersecurity-questions <mailman-bounces@mit.edu> on behalf of M

To: cybersecurity-questions-owner

Mon 6/13/2022 5:46 PM

Microsoft

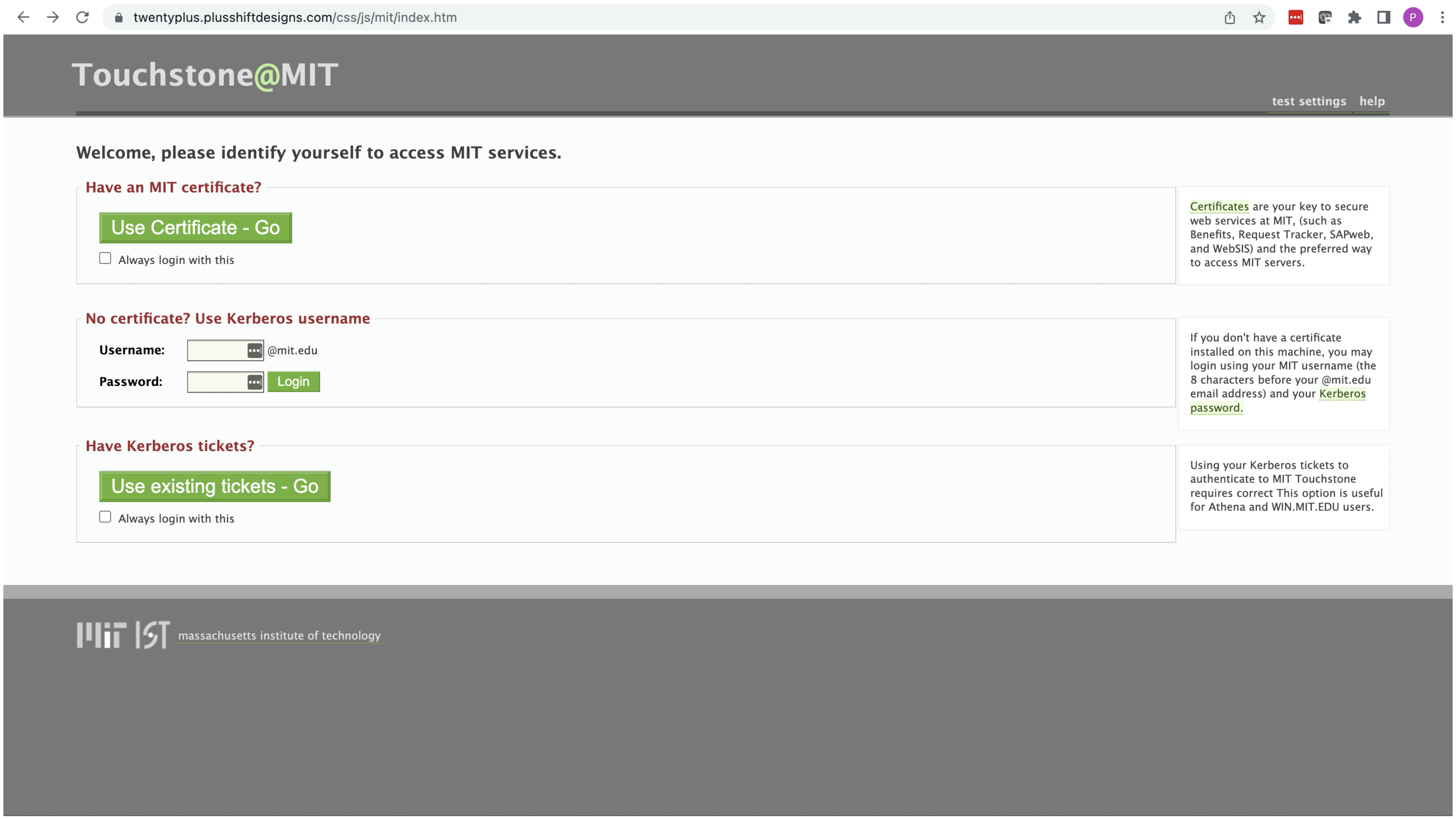
Your Email password for cybersecurity-questions-owner@mit.edu expires today

Monday, June 13, 2022

Keep my Credentials

© 2022 Microsoft. All right reserved

Yesterday’s phishing



twentyplus.plusshiftdesigns.com/css/js/mit/index.htm

Touchstone@MIT

Welcome, please identify yourself to access MIT services.

Have an MIT certificate?

□ Always login with this

Certificates are your key to secure web services at MIT, (such as Benefits, Request Tracker, SAPweb, and WebSIS) and the preferred way to access MIT servers.

No certificate? Use Kerberos username

Username: @mit.edu

Password:

If you don't have a certificate installed on this machine, you may login using your MIT username (the 8 characters before your @mit.edu email address) and your Kerberos password.

Have Kerberos tickets?

□ Always login with this

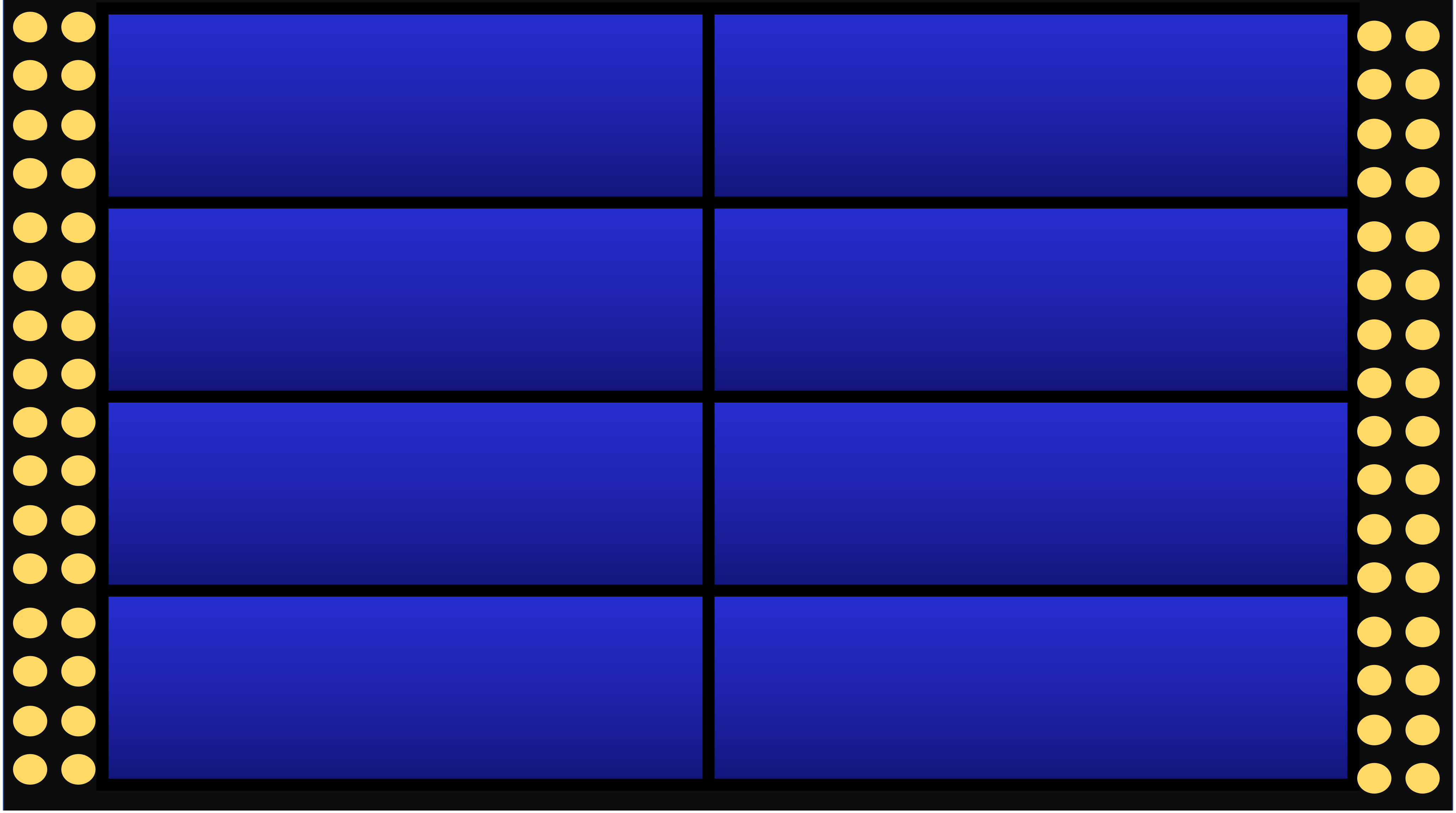
Using your Kerberos tickets to authenticate to MIT Touchstone requires correct This option is useful for Athena and WIN.MIT.EDU users.

Networks commonly used by attackers

Networks commonly used by attackers

- Another university
- Local ISP
- Microsoft
- AWS
- GCP
- VPN
- Other cloud vendor

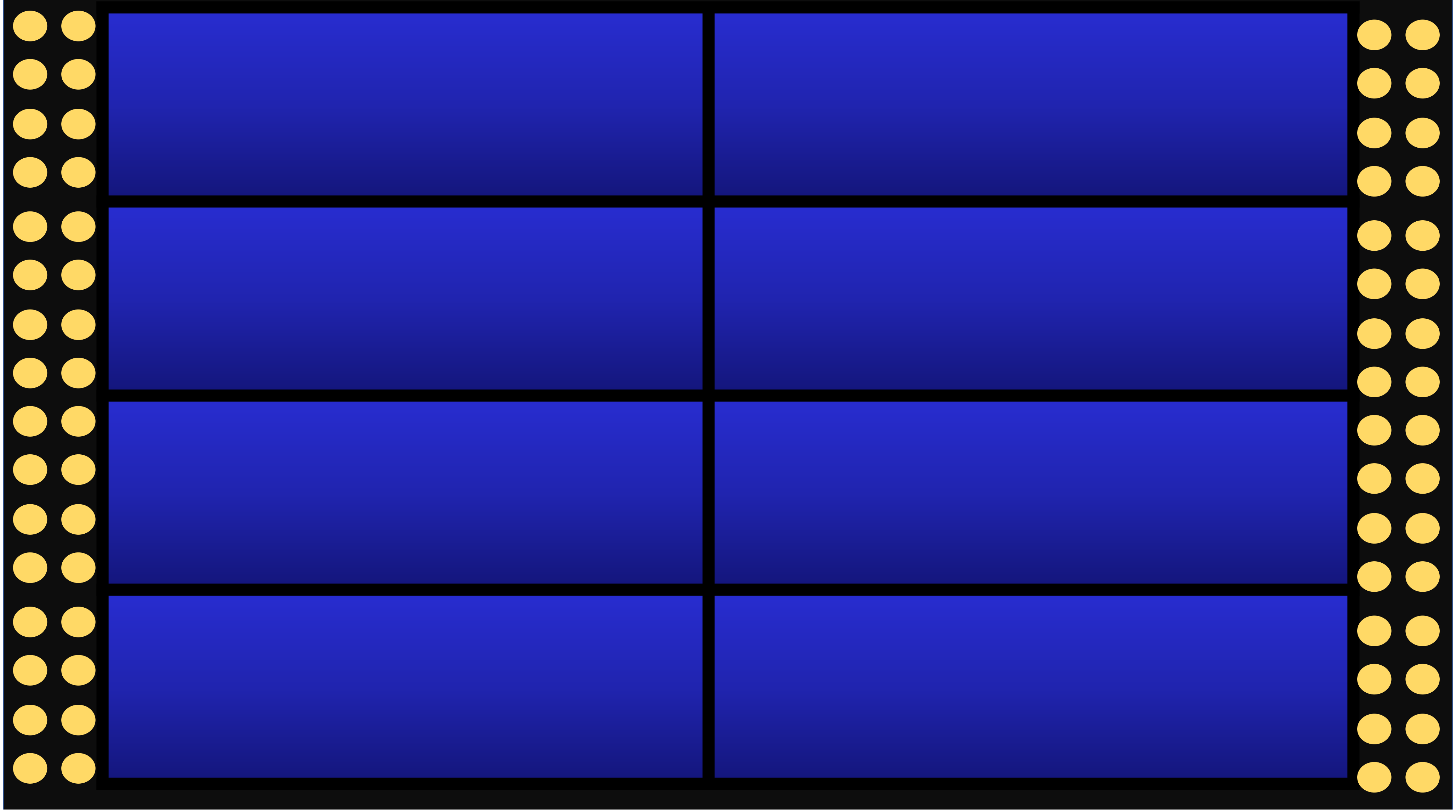
How attackers use compromised MIT accounts



How attackers use compromised MIT accounts

Send phishing	Add scripts to athena locker
Add Duo factors	Create mailing lists
Add inbox rules	Request a Drupal Cloud site
Conversation hijacking	Authorize apps in O365

Signs your MIT account may be compromised



Signs your MIT account may be compromised

Mail bounces	Resetting a compromised password to password1
Bobo with the canned meat	
Unexpected Duo prompts	
Call or text from someone asking for Duo passcode	

What should I do if my MIT Kerberos account is compromised?

- email security@mit.edu
- KB http://kb.mit.edu/confluence/x/MZIBCQ
- Change your password
- Check your Duo factors
- Check your mail forwarding settings
- Check for any new lists that may have been created
- Check mail forwarding settings and inbox rules
- Try to recover deleted items
- Check for applications using Microsoft 365 credentials