NATIONAL ASSOCIATION OF
Community Health Centers®

Considerations for Sustaining A Culture of Cybersecurity

Part 2

THE NACHC MISSION

America’s Voice for Community Health Care

The National Association of Community Health Centers (NACHC) was founded in 1971 to promote efficient, high quality, comprehensive health care that is accessible, culturally and linguistically competent, community directed, and patient centered for all.

Supported Vendors:

athenaOne

athenaFlow/athenaPractice (formerly Centricity)

eClinicalWorks

Greenway Intergy

NextGen Healthcare

(Coming Soon) EPIC

NACHC supports several user groups for Health Centers that utilize various Electronic Health Record (EHR) platforms. These user groups provide a vehicle for health centers to meet and discuss common issues, share experiences and gain valuable insight on accomplishments and best practices.

NACHCs EHR User Groups

Benefits of joining an EHR User Group:

- Connect with other Health Centers who use the same EHR platform as you do.
- Discuss issues and enhancements that are most important to Health Centers.
- Groups are led by Health Centers, HCCN's and PCA staff on a voluntary basis.
- Online forums to exchange ideas, lessons learned and best practices.
- Groups meet both virtually and in-person.
- NACHC provides support via WebEx, conference calls and meeting space at our major conferences.

Questions? E-mail: PStringfield@nachc.org

Today’s Session: Cybersecurity Risk & Preparation

Participants will:

- Learn how to quantify IT security risks in their organization
- Learn practical exercises to know what to do WHEN not IF a data breach happens to them
- Learn how to cultivate a culture of Security Awareness in their organization

Presenters:

- • **Arnel Mendoza,** Director of Information Systems, QueensCare Health Centers
- • **Michael Sanguily,** Director of CISO Services, Health Choice Network

Meet Your Speakers

Arnel Mendoza
Director of Information Systems
QueensCare Health Centers

Michael Sanguily
Director of CISO Services
Health Choice Network

Health Choice Network
a Family of Health Centers
25+ Years of Service

Understanding the Essentials

1 Learn How to Quantify Risks In Their Organization

2 Learn Practical Exercises to know what to do WHEN not IF a Data Breach Happens

3 Learn How To Cultivate A Culture of Security Awareness in their organization

Part 1 Recap

A Basic Infrastructure protects.

A Good Infrastructure enables.

A Great Infrastructure innovates.

Cybersecurity Best Practices

PEOPLE

- Password/User M
- Security Awarene
- Organizational Cu
- Compliance
- Security Awarene
- HIPAA & Cyber Ed staff
- Security Officer/L
- Role-Based Acces

PROCESS

ngoing Risk Management
ata Backup
yber-insurance in place
ompliance
ncident Response
usiness Continuity Processes
etwork Pen Testing
ngoing Audits

- Intrusion Protection Systems
- Device Encrypsion
- Segmented Networks
- MFA (Multi-Factor Auth

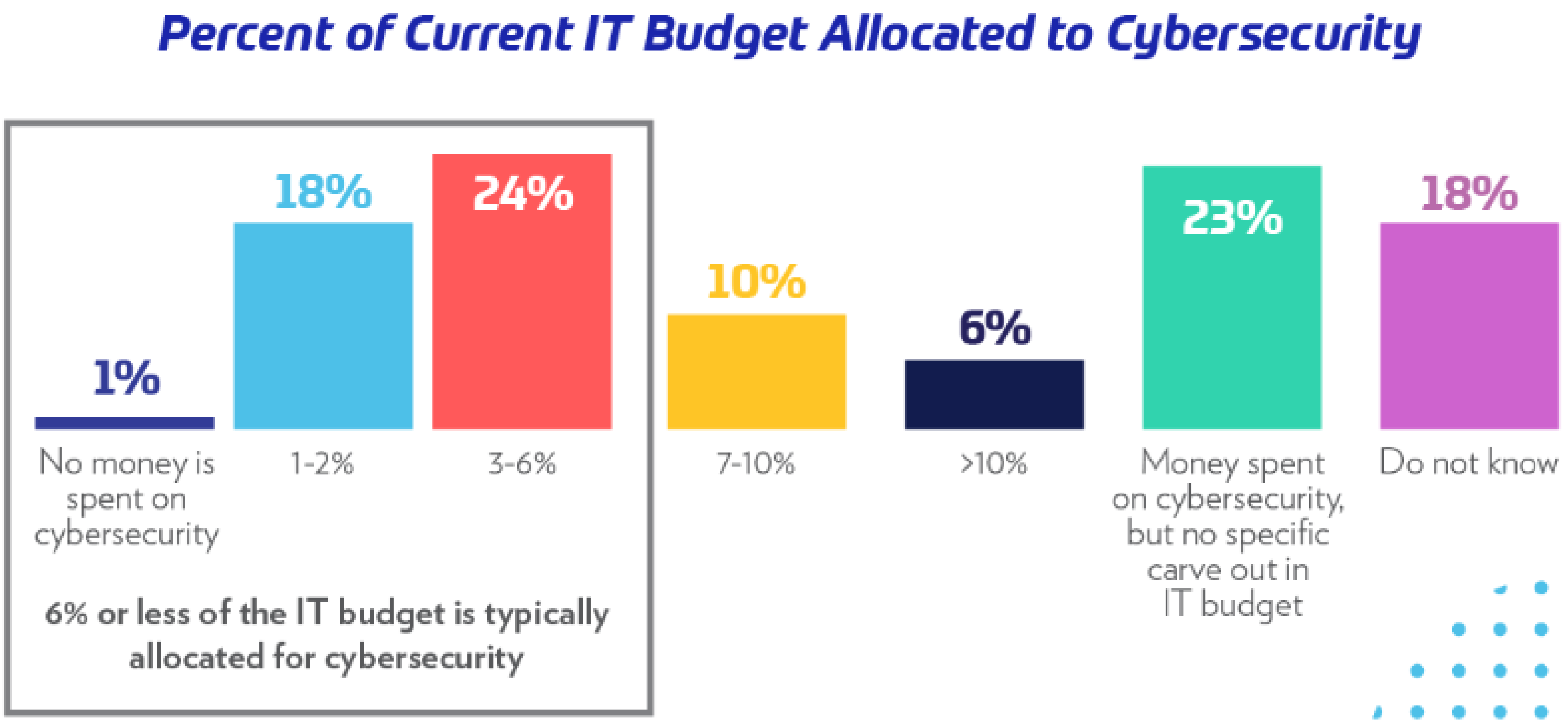
Cybersecurity Basics: GCA Cybersecurity Toolkit

GLOBAL CYBER ALLIANCE™

1. Know What You Have
2. Update Your Defenses
3. Beyond Simple Passwords
4. Prevent Phishing and Malware
5. Backup and Recover
6. Protect Your Email and Reputation

Adapted from https://gcatoolkit.org/

How Much Are You Spending For Cybersecurity?



Source: HIMMS Cybersecurity Survey 2021

A Word About Budgeting

When talking to vendors, always use the magic words: **NON-PROFIT PRICING**
Always look for **FREE** or **SIGNIFICANTLY DISCOUNTED** resources

monday.com for nonprofits

SALESFORCE FOR NONPROFIT

Microsoft 365 resources for nonprofits

Google for Nonprofits.

Mobile Beacon for Nonprofits

Nessus Essentials free vulnerability assessment solution

CISA's Cyber Hygiene Vulnerability Scanning email vulnerability@cisa.dhs.gov

prey **DEVICE TRACKING & PROTECTION**

Cloudflare Universal SSL certificate FREE

GRR RAPID RESPONSE Incident Response Framework

More Free from CISA

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

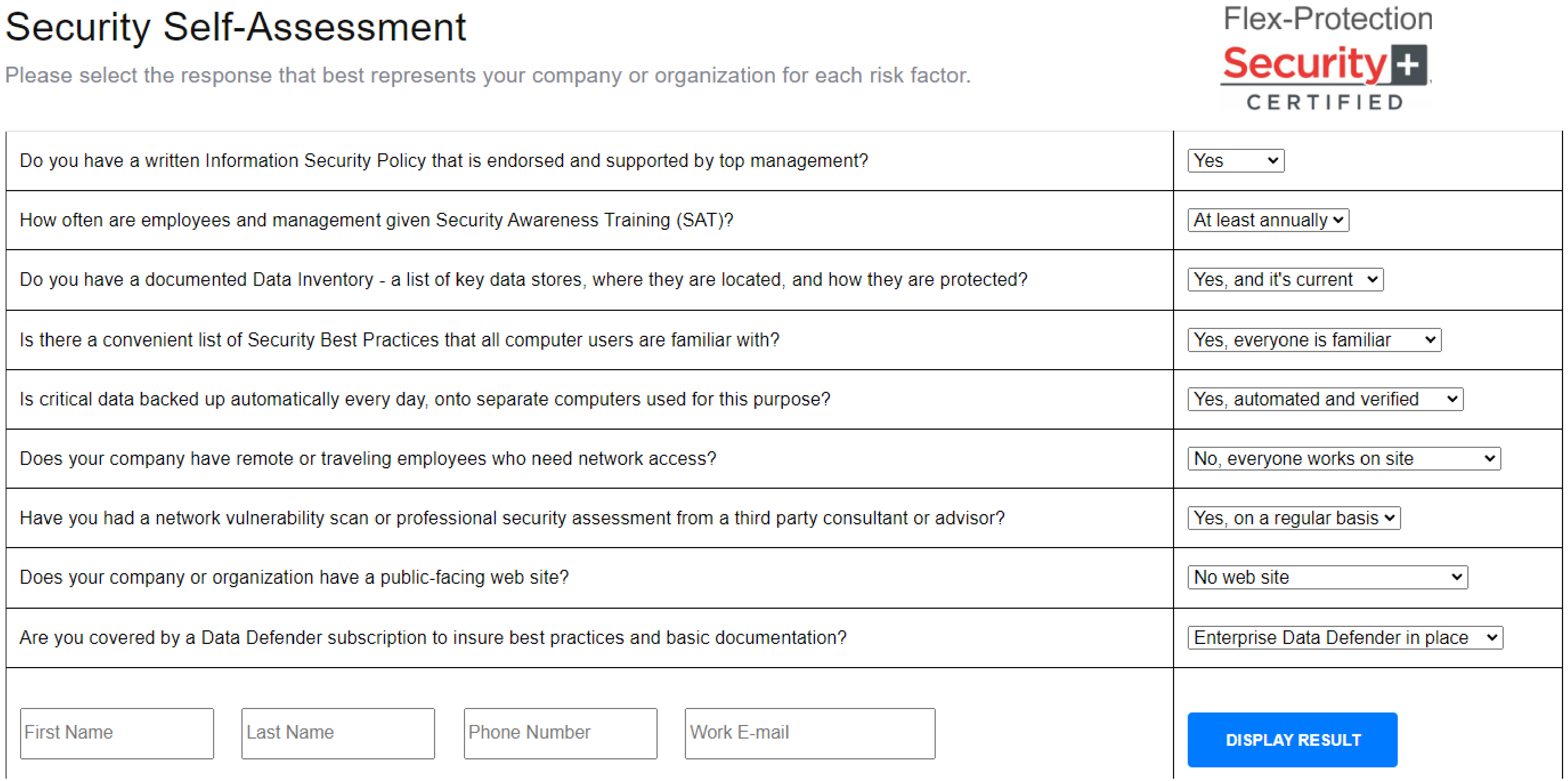
Free Cybersecurity Services and Tools | CISA
https://www.cisa.gov/free-cybersecurity-servies-and-tools

What To Do First: Quantify Your Risk

If you want to know what to spend on for cybersecurity, you must first determine where you are most vulnerable.

Basic Assessment

https://www.flex-protection.com/#self

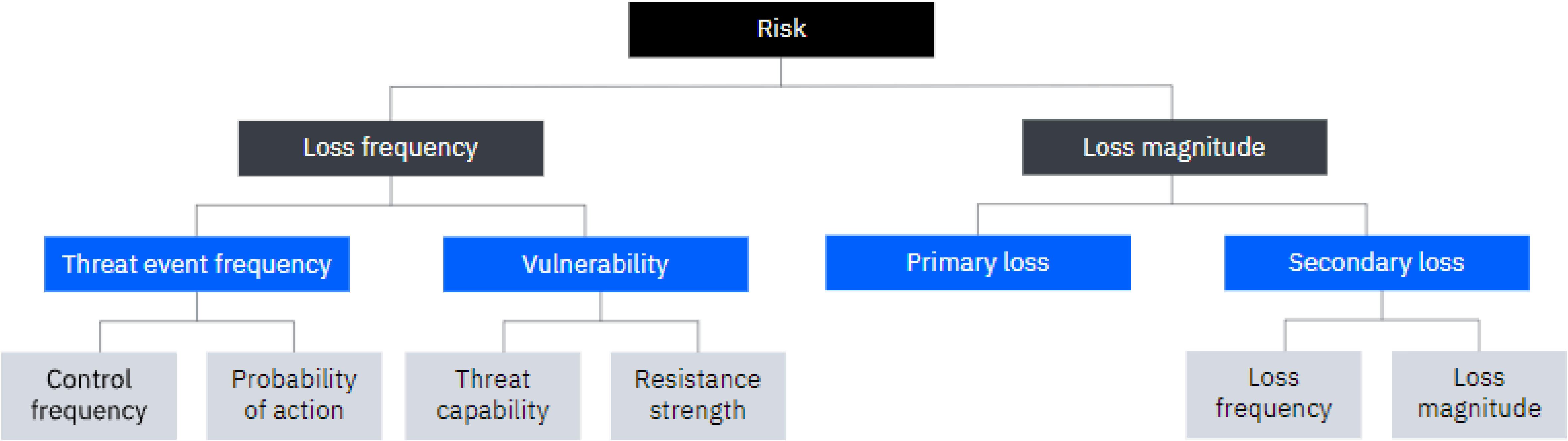


Security Self-Assessment

Please select the response that best represents your company or organization for each risk factor.

Do you have a written Information Security Policy that is endorsed and supported by top management?	Yes
How often are employees and management given Security Awareness Training (SAT)?	At least annually
Do you have a documented Data Inventory - a list of key data stores, where they are located, and how they are protected?	Yes, and it's current
Is there a convenient list of Security Best Practices that all computer users are familiar with?	Yes, everyone is familiar
Is critical data backed up automatically every day, onto separate computers used for this purpose?	Yes, automated and verified
Does your company have remote or traveling employees who need network access?	No, everyone works on site
Have you had a network vulnerability scan or professional security assessment from a third party consultant or advisor?	Yes, on a regular basis
Does your company or organization have a public-facing web site?	No web site
Are you covered by a Data Defender subscription to insure best practices and basic documentation?	Enterprise Data Defender in place

The Science of Risk Management for PROs



Risk

Loss frequency

Loss magnitude

Threat event frequency

Vulnerability

Primary loss

Secondary loss

Control frequency

Probability of action

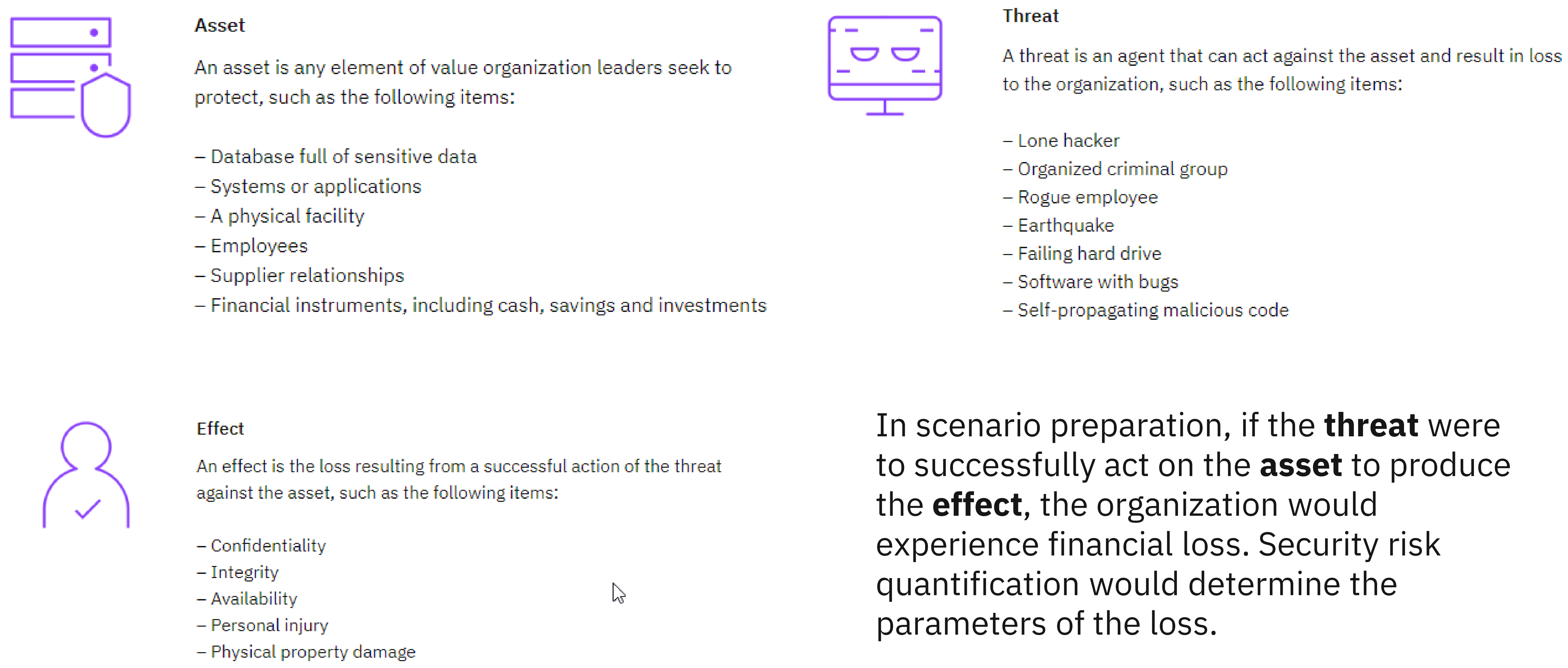
Threat capability

Resistance strength

Loss frequency

Loss magnitude

The Parameters



Asset

An asset is any element of value organization leaders seek to protect, such as the following items:

– Database full of sensitive data
– Systems or applications
– A physical facility
– Employees
– Supplier relationships
– Financial instruments, including cash, savings and investments

Threat

A threat is an agent that can act against the asset and result in loss to the organization, such as the following items:

– Lone hacker
– Organized criminal group
– Rogue employee
– Earthquake
– Failing hard drive
– Software with bugs
– Self-propagating malicious code

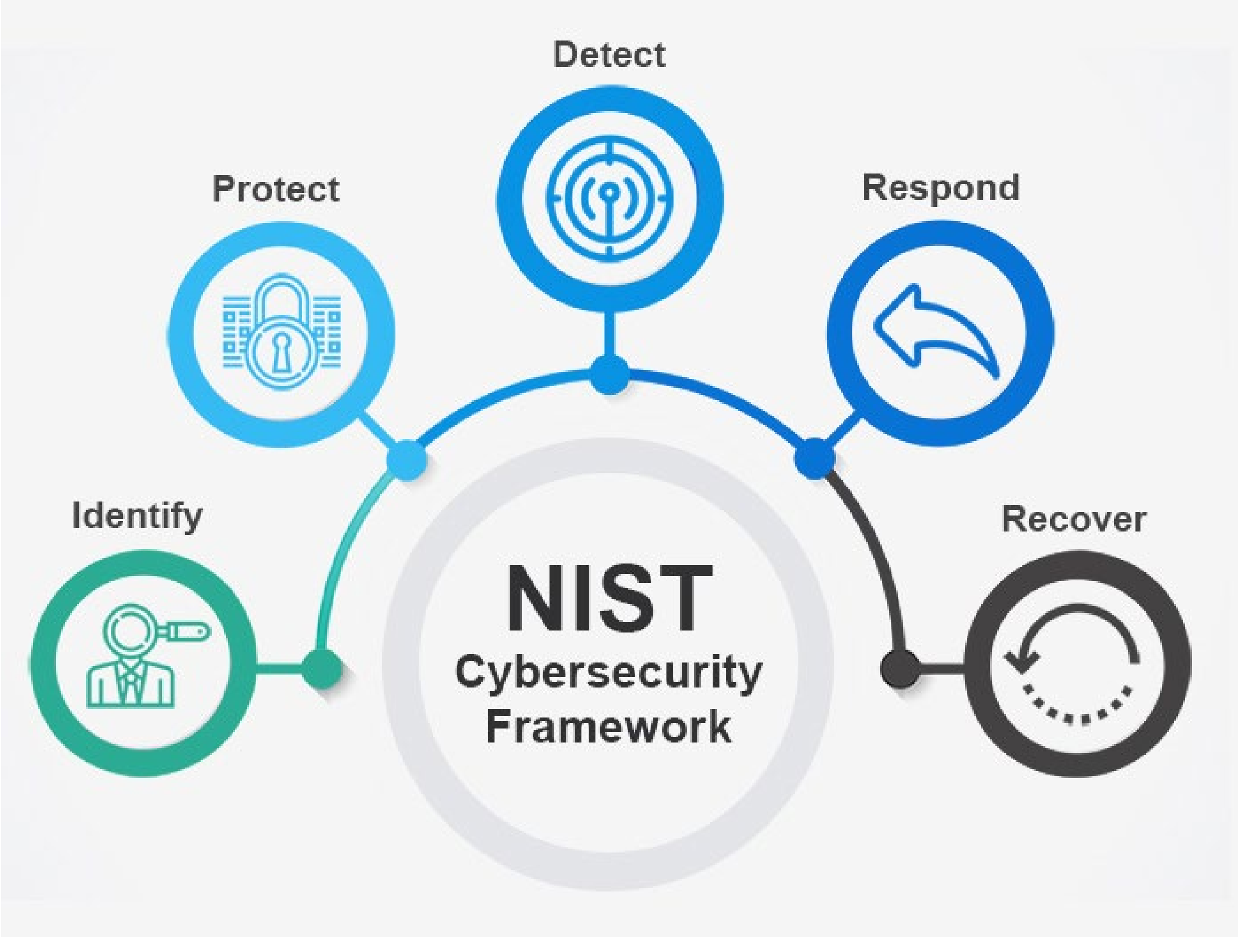
Effect

An effect is the loss resulting from a successful action of the threat against the asset, such as the following items:

– Confidentiality
– Integrity
– Availability
– Personal injury
– Physical property damage

In scenario preparation, if the **threat** were to successfully act on the **asset** to produce the **effect**, the organization would experience financial loss. Security risk quantification would determine the parameters of the loss.

NIST Cybersecurity Framework



Identify This function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

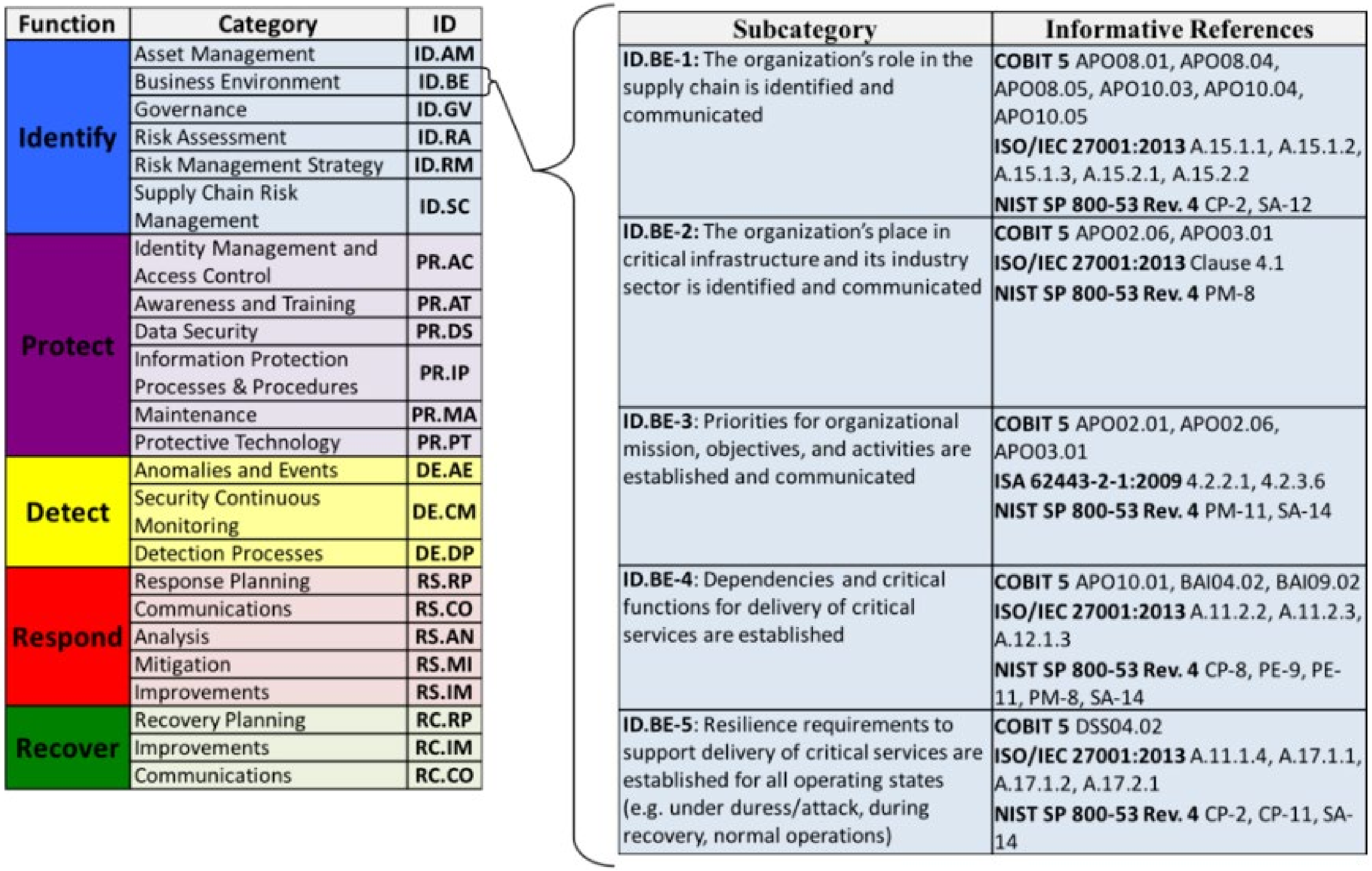
Protect This function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect This function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Respond This function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

Recover This function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

NIST Cybersecurity Framework



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Funtion	Category	Sub Category
Identify	6	29
Protect	6	39
Detect	3	18
Respond	5	16
Recover	3	6

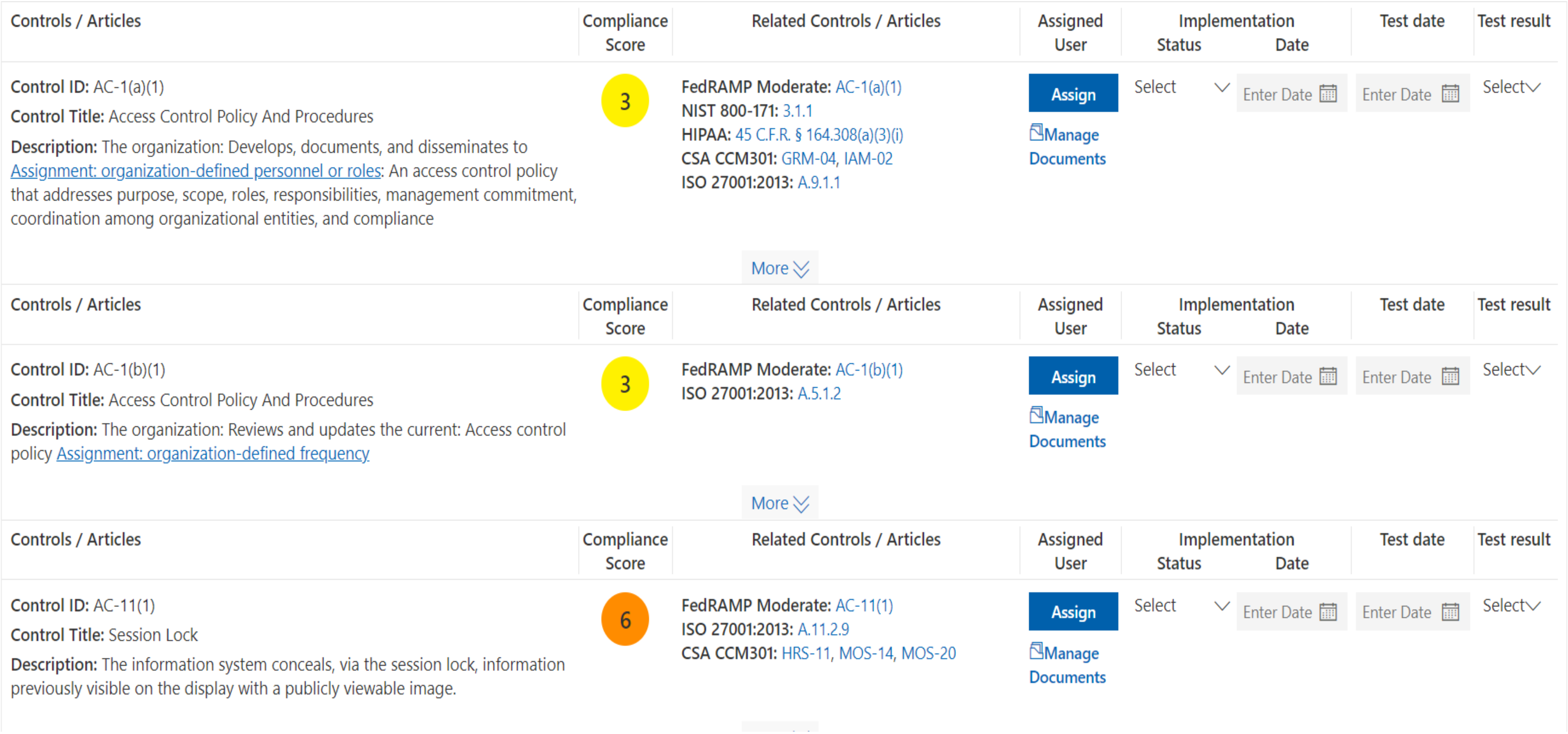
108 Total Questions

NIST Assessment Tools Are Available Online For Free

cipher
a PROSEGUR company

expel

Office 365 Has an NIST Governance Tool



Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Date	Test date	Test result
Control ID: AC-1(a)(1) **Control Title:** Access Control Policy And Procedures **Description:** The organization: Develops, documents, and disseminates to Assignment: organization-defined personnel or roles: An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	3	**FedRAMP Moderate:** AC-1(a)(1) **NIST 800-171:** 3.1.1 **HIPAA:** 45 C.F.R. § 164.308(a)(3)(i) **CSA CCM301:** GRM-04, IAM-02 **ISO 27001:2013:** A.9.1.1	Assign Manage Documents	Select	Enter Date	Enter Date	Select

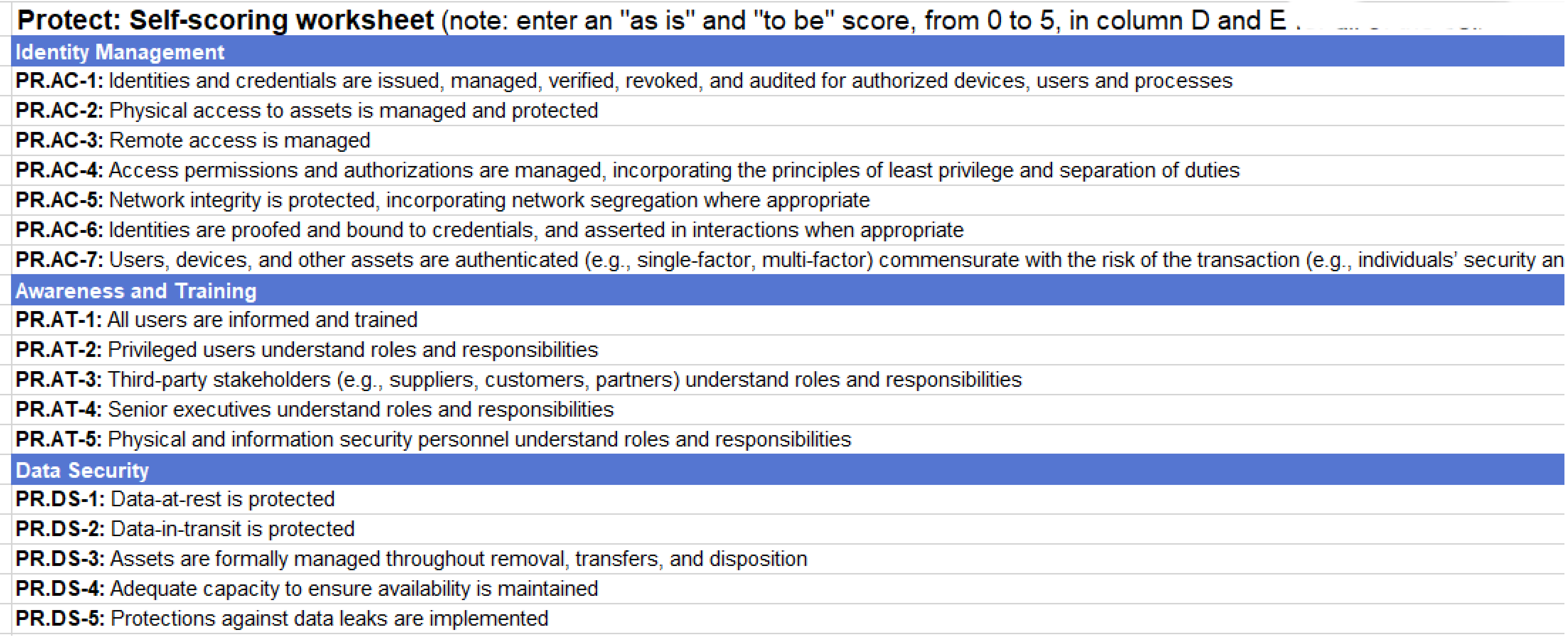
More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Date	Test date	Test result
Control ID: AC-1(b)(1) **Control Title:** Access Control Policy And Procedures **Description:** The organization: Reviews and updates the current: Access control policy Assignment: organization-defined frequency	3	**FedRAMP Moderate:** AC-1(b)(1) **ISO 27001:2013:** A.5.1.2	Assign Manage Documents	Select	Enter Date	Enter Date	Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Date	Test date	Test result
Control ID: AC-11(1) **Control Title:** Session Lock **Description:** The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	6	**FedRAMP Moderate:** AC-11(1) **ISO 27001:2013:** A.11.2.9 **CSA CCM301:** HRS-11, MOS-14, MOS-20	Assign Manage Documents	Select	Enter Date	Enter Date	Select

Fill Out The Spreadsheet Assessment



Protect: Self-scoring worksheet (note: enter an "as is" and "to be" score, from 0 to 5, in column D and E

Identity Management

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.AC-2: Physical access to assets is managed and protected

PR.AC-3: Remote access is managed

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate

PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security an

Awareness and Training

PR.AT-1: All users are informed and trained

PR.AT-2: Privileged users understand roles and responsibilities

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities

PR.AT-4: Senior executives understand roles and responsibilities

PR.AT-5: Physical and information security personnel understand roles and responsibilities

Data Security

PR.DS-1: Data-at-rest is protected

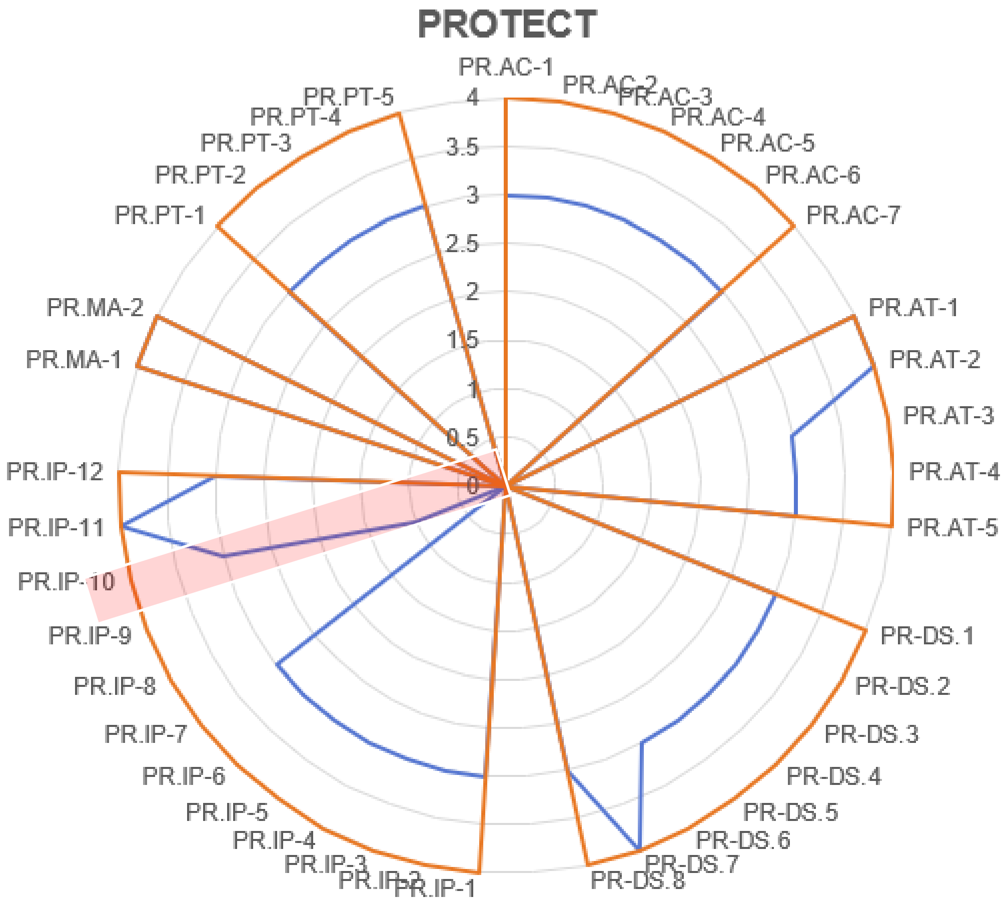
PR.DS-2: Data-in-transit is protected

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

PR.DS-4: Adequate capacity to ensure availability is maintained

PR.DS-5: Protections against data leaks are implemented

A Heatmap of Your Biggest Vulnerabilities



Example Weakness:
PR.IP-10: Response and recovery plans are tested

What the Pros Use: FAIR

One globally recognized security risk quantification methodology is the **Factor Analysis of Information Risk (FAIR™)**. It is a model that codifies and monetizes risk.

In other words, it breaks down risk by identifying and defining the building blocks that make up risk and their relationship to one another. The relationships between each building block or element of risk can be measured mathematically and assigned dollar values, so that ultimately risk can be calculated as financial loss exposure.

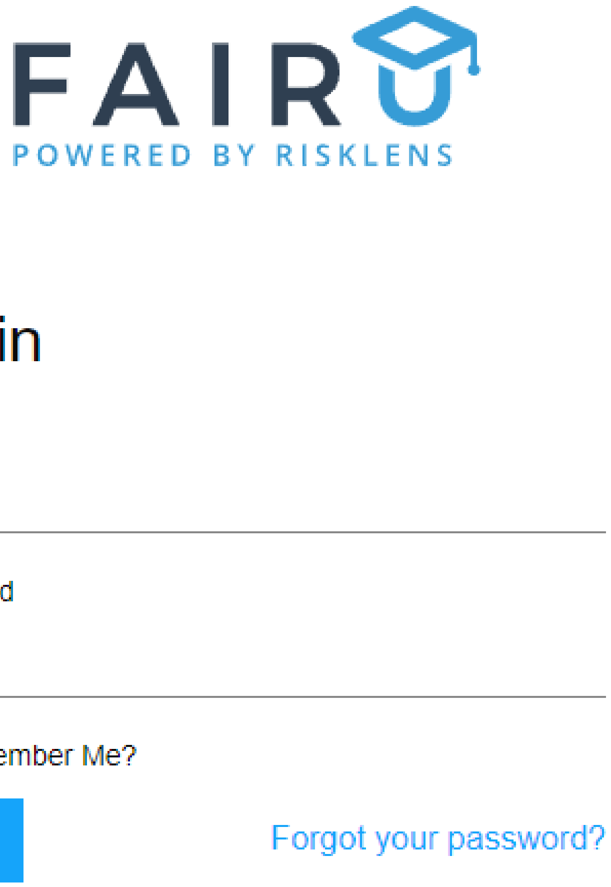
Why Is This That Important?

Technology Leaders Must Learn to Speak the Language of the C-Suites.

$$ $$

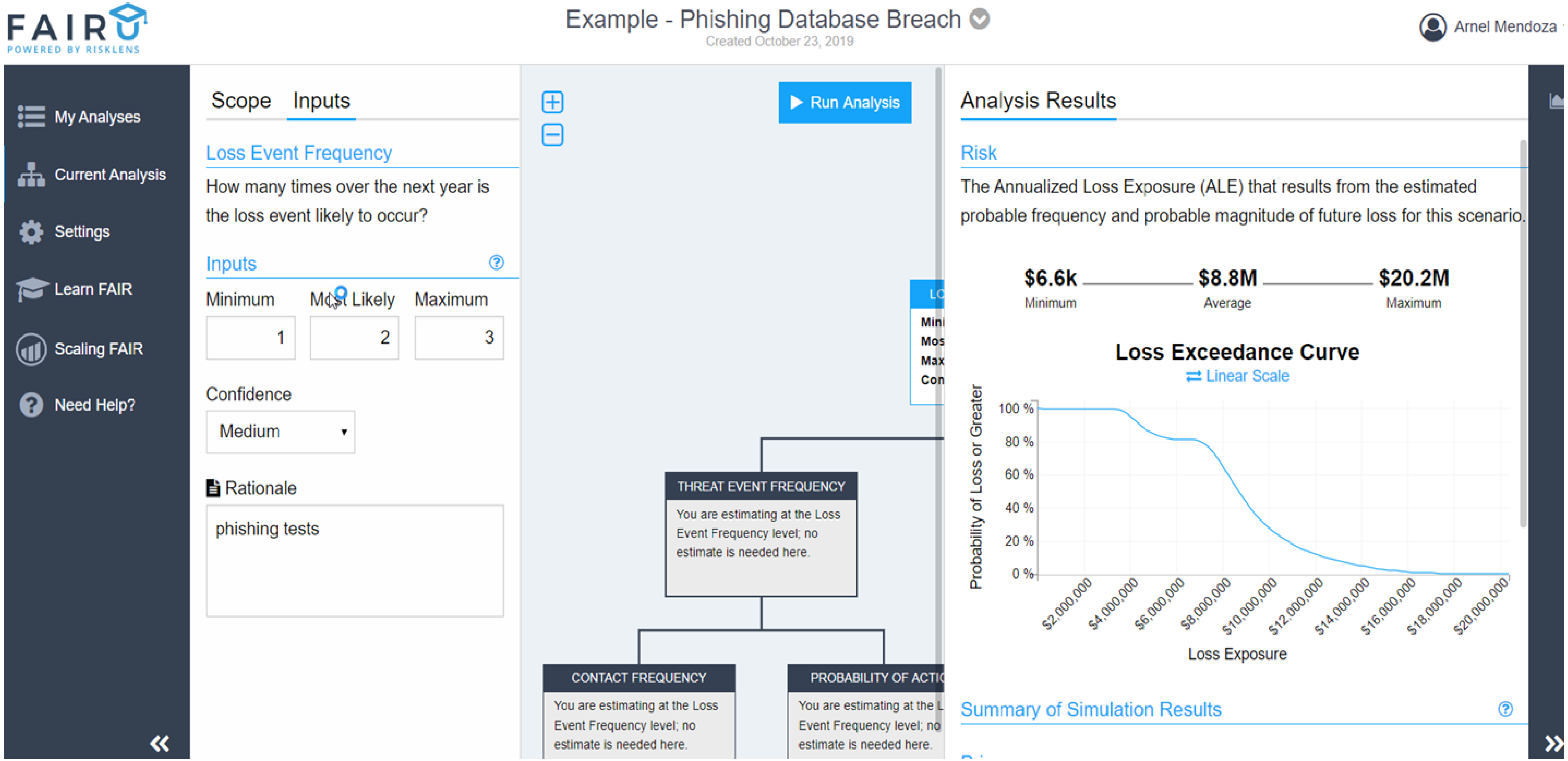
$$ $$

The Tool <FREE!>



https://app.fairu.net/

FairU Example



Example - Phishing Database Breach

Created October 23, 2019

Loss Event Frequency

How many times over the next year is the loss event likely to occur?

Inputs

Minimum	Most Likely	Maximum
1	2	3

Confidence

Medium ▾

Rationale

phishing tests

THREAT EVENT FREQUENCY

You are estimating at the Loss Event Frequency level; no estimate is needed here.

CONTACT FREQUENCY

You are estimating at the Loss Event Frequency level; no estimate is needed here.

PROBABILITY OF ACTI

You are estimating at the L Event Frequency level; no estimate is needed here.

Analysis Results

Risk

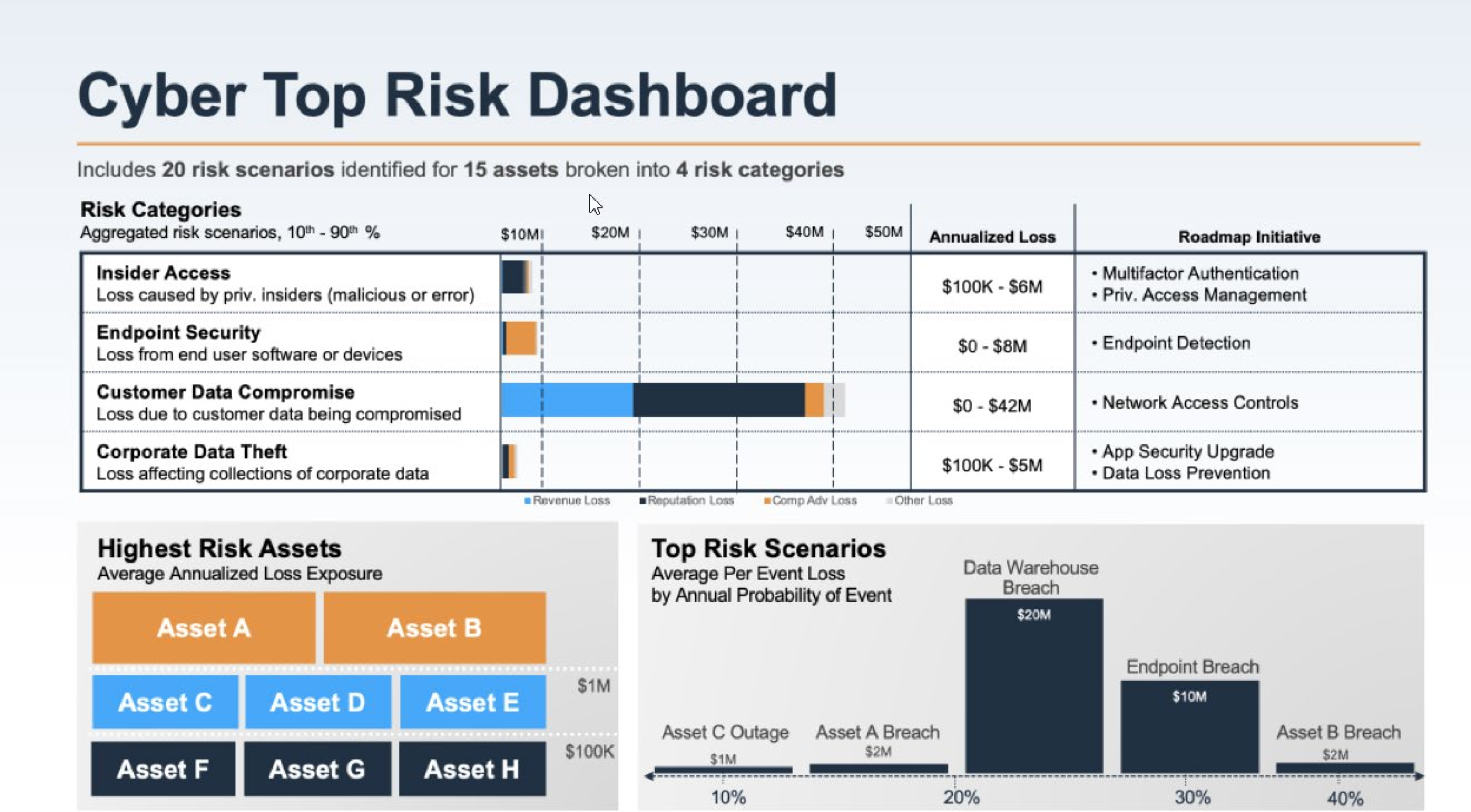
The Annualized Loss Exposure (ALE) that results from the estimated probable frequency and probable magnitude of future loss for this scenario.

$6.6k	$8.8M	$20.2M
Minimum	Average	Maximum

Summary of Simulation Results

The Gold Standard

Source: RiskLens



Cyber Top Risk Dashboard

Includes **20 risk scenarios** identified for **15 assets** broken into **4 risk categories**

Risk Categories Aggregated risk scenarios, 10th - 90th %	Annualized Loss	Roadmap Initiative
Insider Access Loss caused by priv. insiders (malicious or error)	$100K - $6M	• Multifactor Authentication • Priv. Access Management
Endpoint Security Loss from end user software or devices	$0 - $8M	• Endpoint Detection
Customer Data Compromise Loss due to customer data being compromised	$0 - $42M	• Network Access Controls
Corporate Data Theft Loss affecting collections of corporate data	$100K - $5M	• App Security Upgrade • Data Loss Prevention

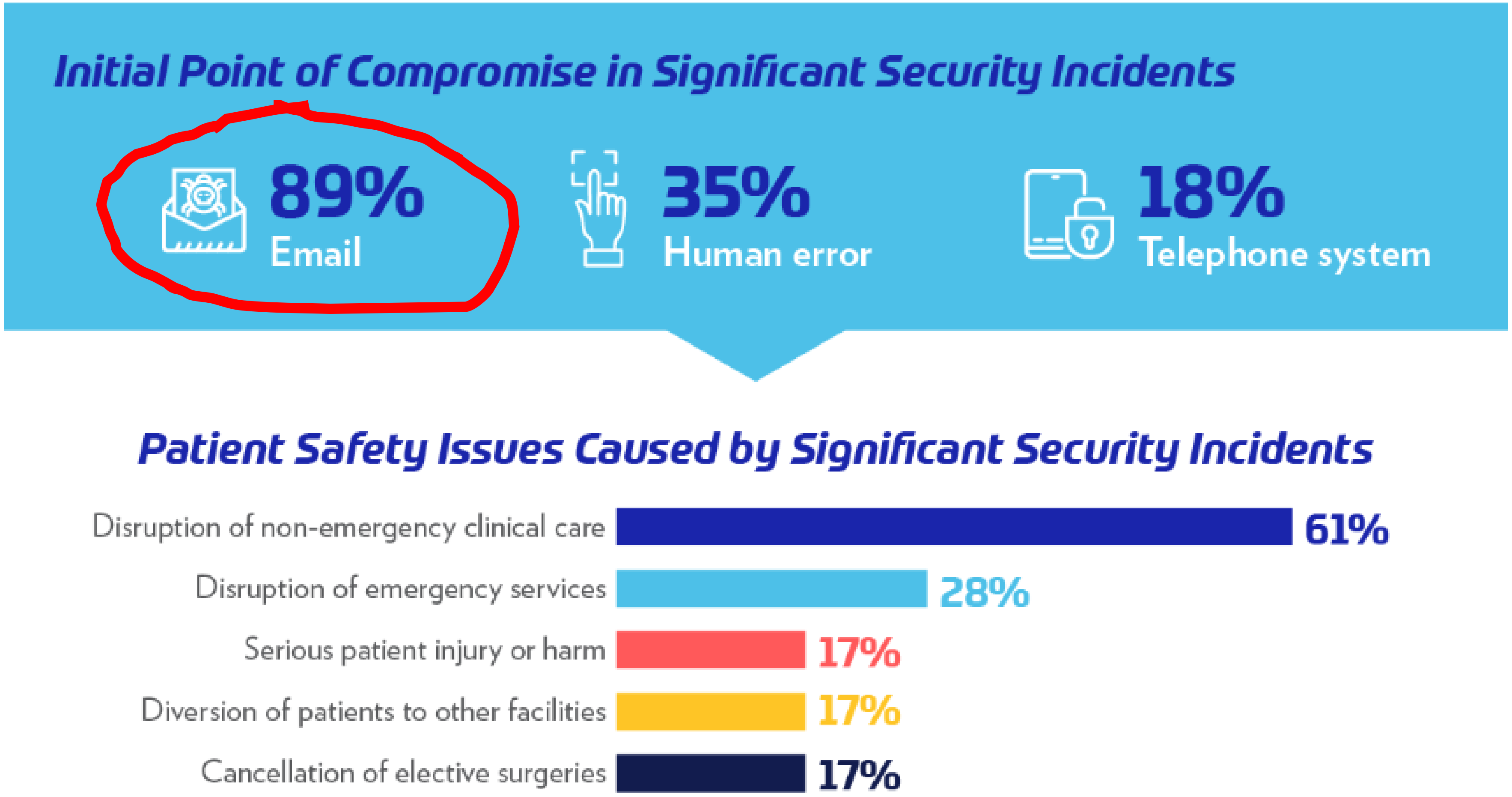
Highest Risk Assets

Average Annualized Loss Exposure

Top Risk Scenarios

Average Per Event Loss
by Annual Probability of Event

Where Does A Data Breach Start?



Initial Point of Compromise in Significant Security Incidents

89% Email

35% Human error

18% Telephone system

Patient Safety Issues Caused by Significant Security Incidents

Disruption of non-emergency clinical care	61%
Disruption of emergency services	28%
Serious patient injury or harm	17%
Diversion of patients to other facilities	17%
Cancellation of elective surgeries	17%

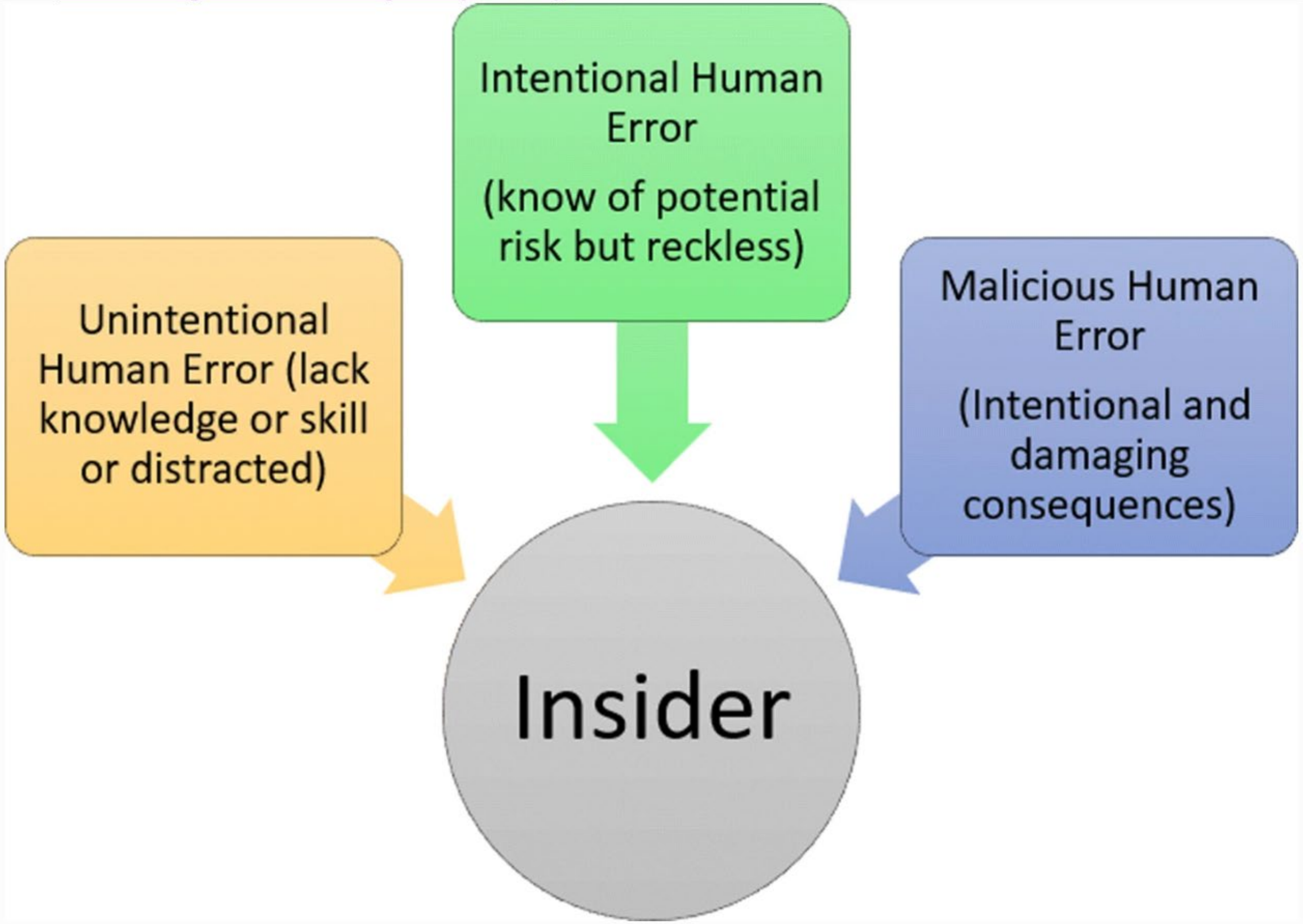
Source: HIMMS Cybersecurity Survey 2021

Phishing Statistics

- According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing.

- According to Verizon's 2021 Data Breach Investigations Report, 85% of breaches involved the human element.

The Human Error Factor


Intentional Human Error
(know of potential risk but reckless)
Unintentional Human Error (lack knowledge or skill or distracted)
Malicious Human Error
(Intentional and damaging consequences)
Insider

Proposed UIM human error as insider-anomaly concept

The Human Error Factor

- Unintentional human error can be due to lack of organized knowledge or operating skills. This error may remain unintentional or transforms to another type (intentional or malicious).

- Intentional human error is caused by a user who knows of risky behavior but acts on it, or misuses assets. The wrong action may not necessarily bring a sudden harm to the organization, but it may still breach of existing laws or privacy.

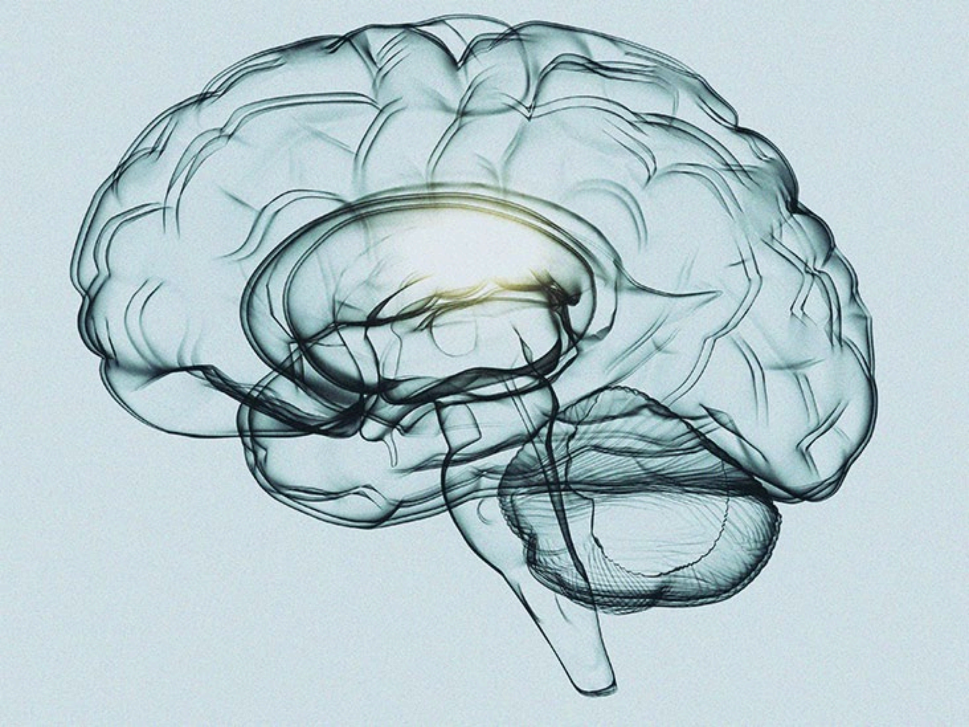
- Malicious human error is the worst error as it is intentional with specific and damaging consequences in mind.

What Did That Click Cost?

From the report Sophos State of Ransomware 2021, the average ransom paid by mid-sized organizations was **$170,404** while the average cost of resolving a ransomware attack was **$1.85 million**. This cost includes downtime, people time, device cost, network cost, lost opportunity, ransom paid, higher cybersecurity insurance premiums.

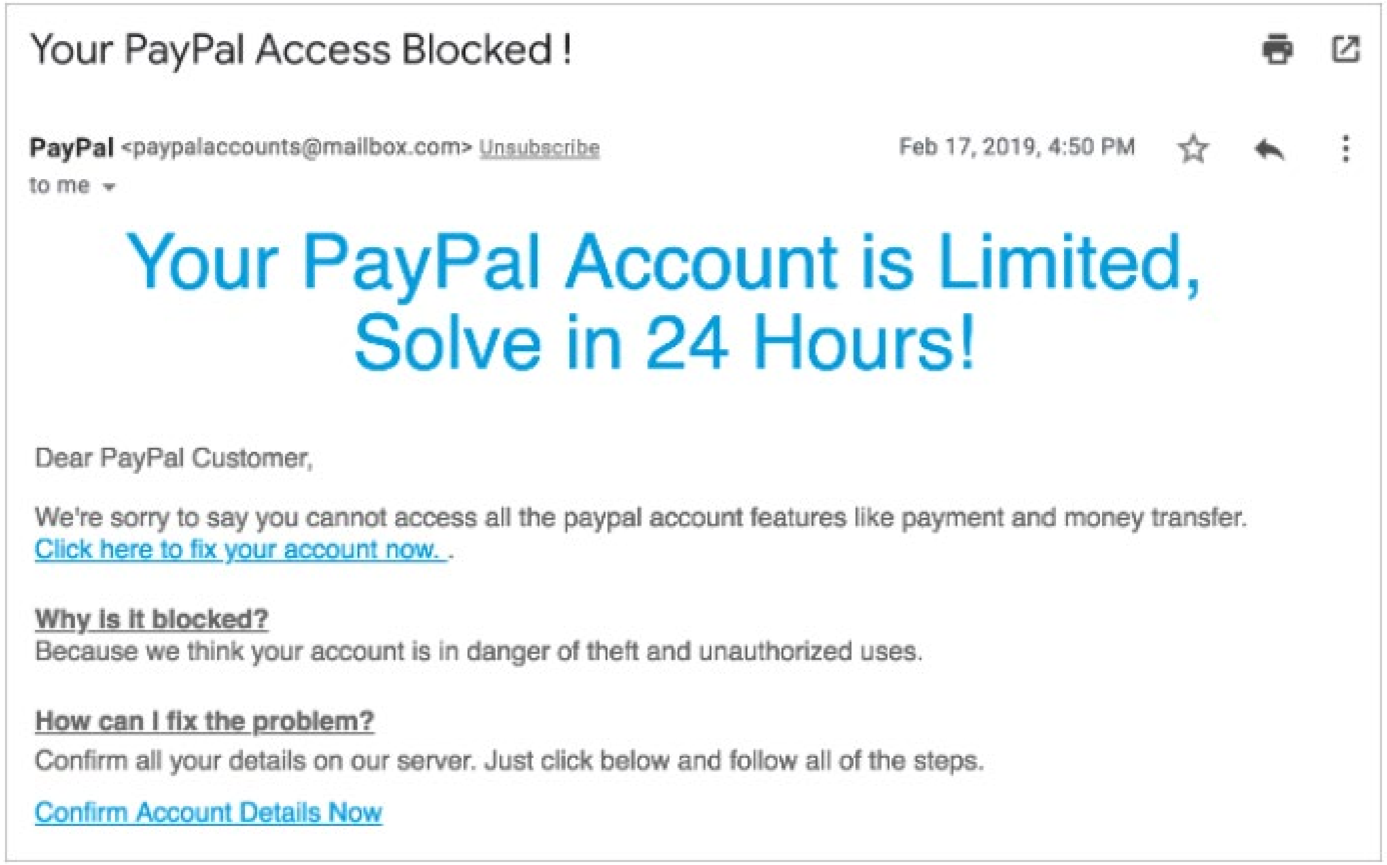
Why Do People Click? A Little Brain Science

Fact: The emotional brain is both quicker and stronger than the logical brain. Emotions, like fear and urgency, sidestep the frontal lobe and smack us right square in the amygdala, triggering a Fight or Flight Response



Continued:

Hackers trying to get access to your information, will introduce a psychological stressor, say in the form of a threatening email…



Your PayPal Access Blocked !

PayPal <paypalaccounts@mailbox.com> Unsubscribe   Feb 17, 2019, 4:50 PM

to me

Your PayPal Account is Limited,
Solve in 24 Hours!

Dear PayPal Customer,

We're sorry to say you cannot access all the paypal account features like payment and money transfer.
Click here to fix your account now. .

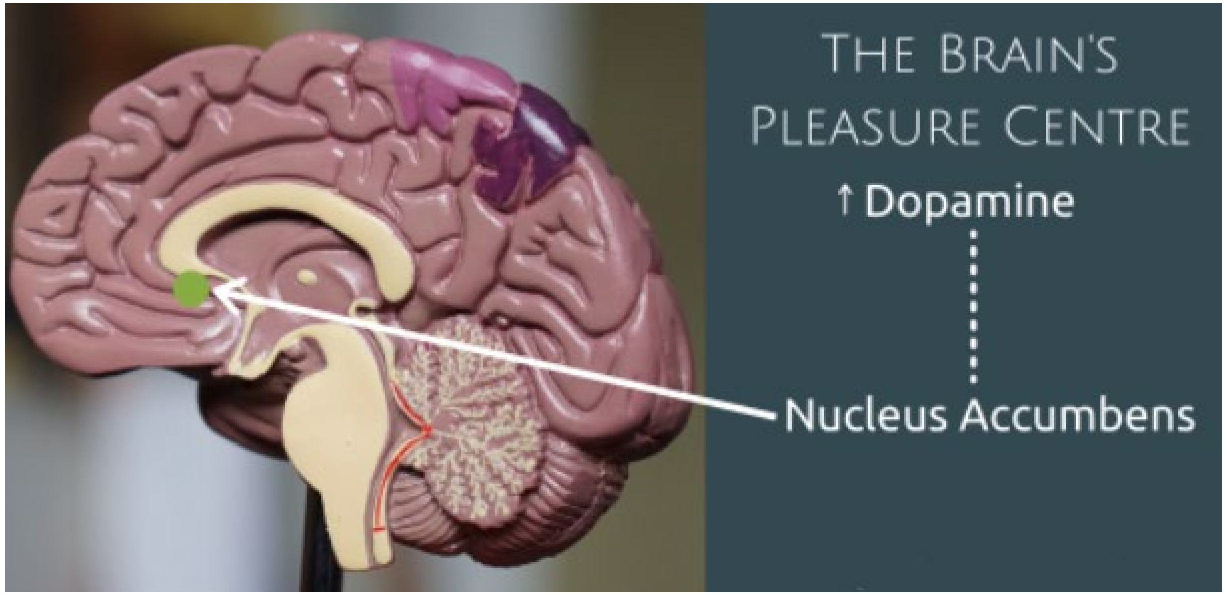
Why Is it blocked?
Because we think your account is in danger of theft and unauthorized uses.

How can I fix the problem?
Confirm all your details on our server. Just click below and follow all of the steps.

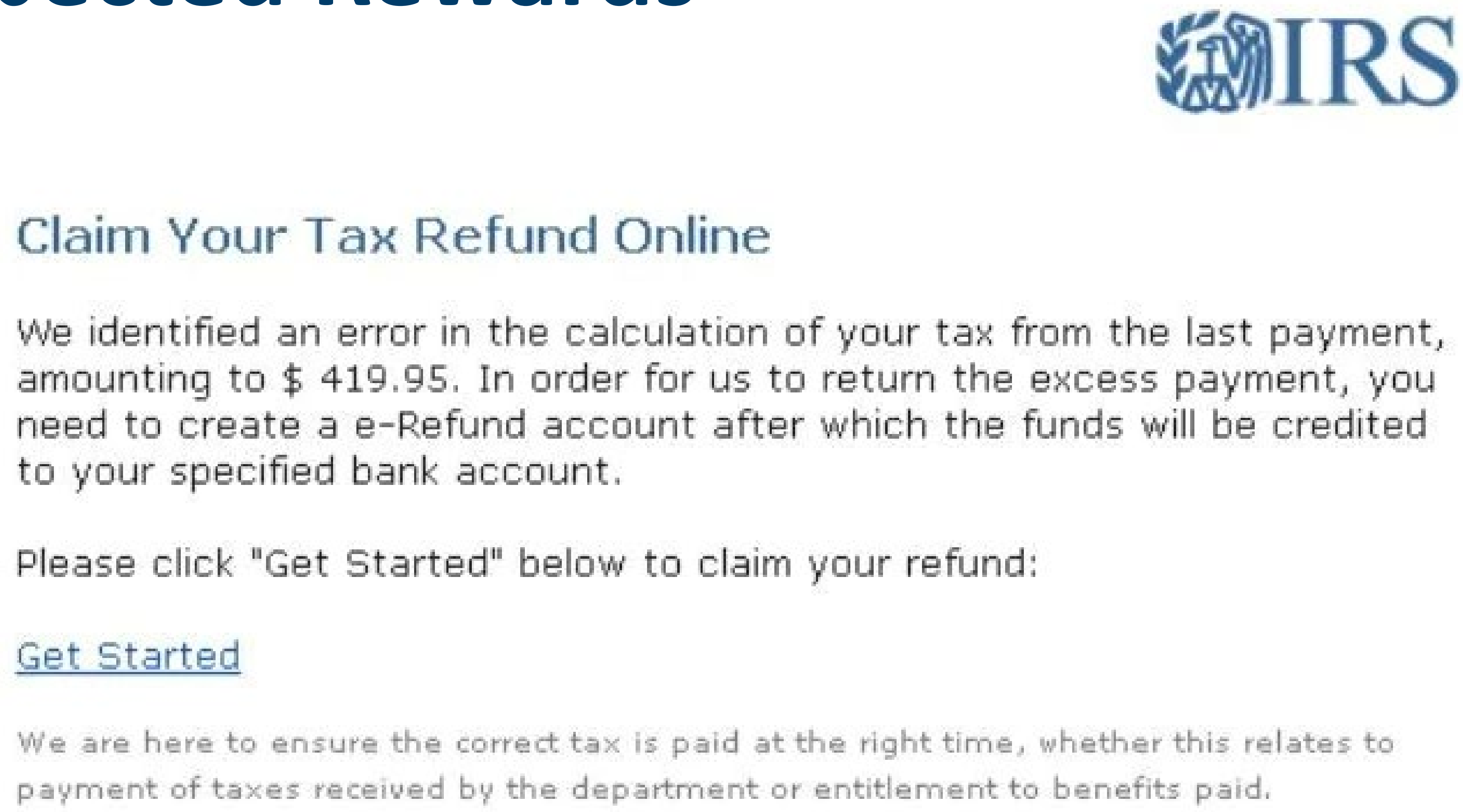
Confirm Account Details Now

Other Brain Hijacks

Humans have been found to have similar reactions to surprise rewards – specifically the anticipation of the reward. A pleasure center of the brain called the nucleus accumbens is highly activated by the possibility of receiving a reward.



Unexpected Rewards



Claim Your Tax Refund Online

We identified an error in the calculation of your tax from the last payment, amounting to $ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

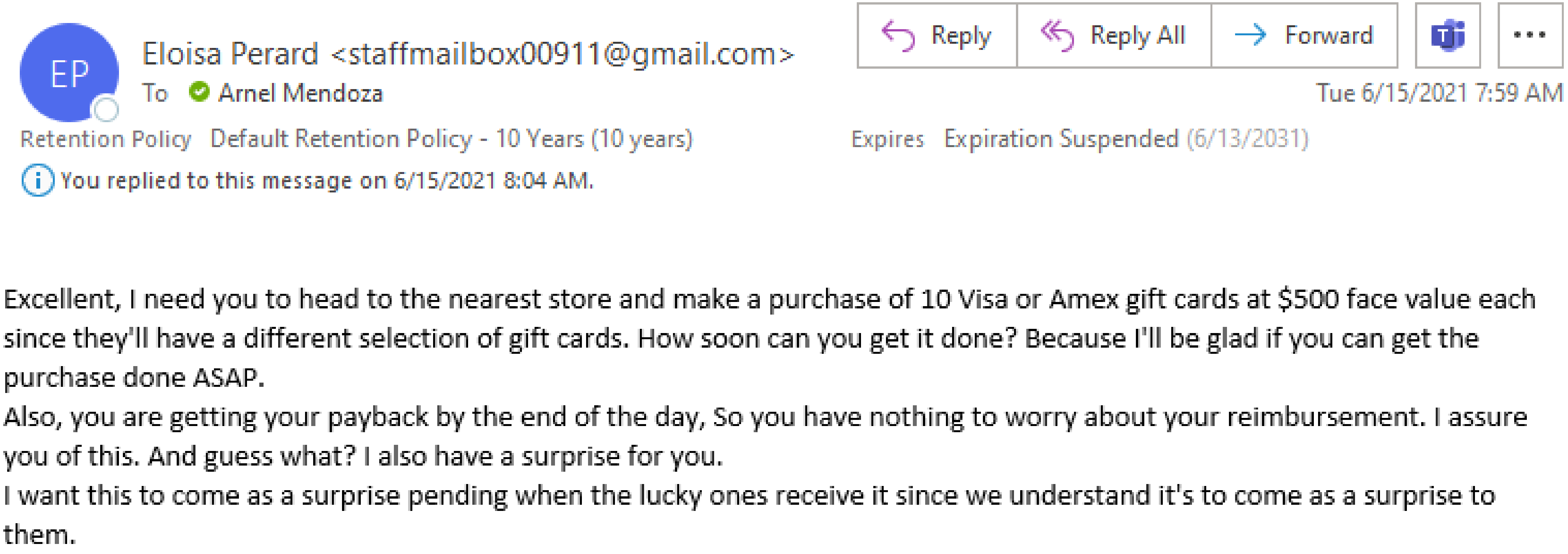
Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

When Emotions Take Over People Click

- **STRESS** Too busy/pre-occupied to pay close attention
- **FEAR** “Do this now, or else…”
- **OVERCONFIDENCE** Overly optimistic at our ability to recognize a phishing email
- **GREED** The unexpected reward
- **HIERARCHY AND AUTHORITY** People tend to comply with requests from authority figures, particularly in the organization

The Power of Authority



Eloisa Perard <staffmailbox00911@gmail.com>

To Arnel Mendoza

Tue 6/15/2021 7:59 AM

Retention Policy Default Retention Policy - 10 Years (10 years)

Expires Expiration Suspended (6/13/2031)

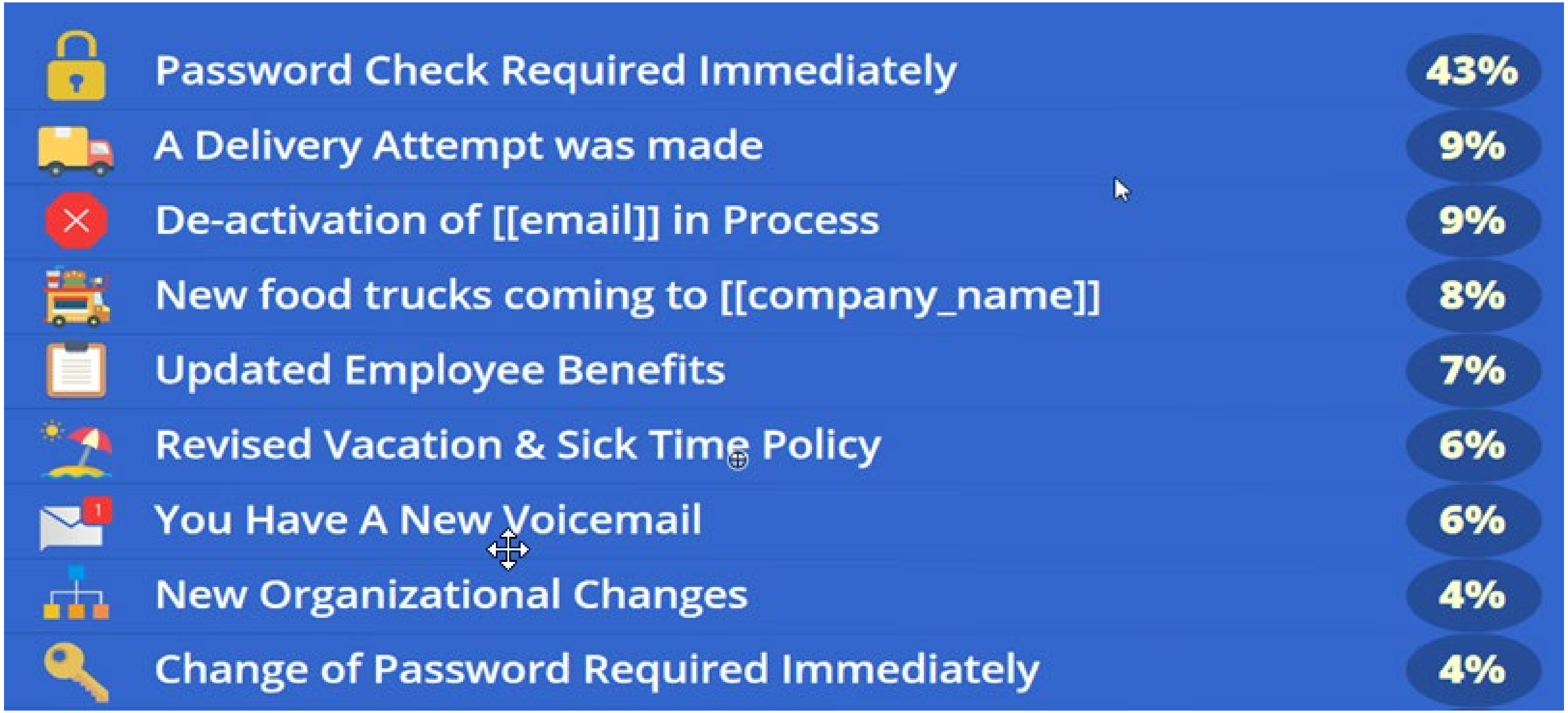
You replied to this message on 6/15/2021 8:04 AM.

Excellent, I need you to head to the nearest store and make a purchase of 10 Visa or Amex gift cards at $500 face value each since they'll have a different selection of gift cards. How soon can you get it done? Because I'll be glad if you can get the purchase done ASAP.

Also, you are getting your payback by the end of the day, So you have nothing to worry about your reimbursement. I assure you of this. And guess what? I also have a surprise for you.

I want this to come as a surprise pending when the lucky ones receive it since we understand it's to come as a surprise to them.

Top Phishing Email Subjects



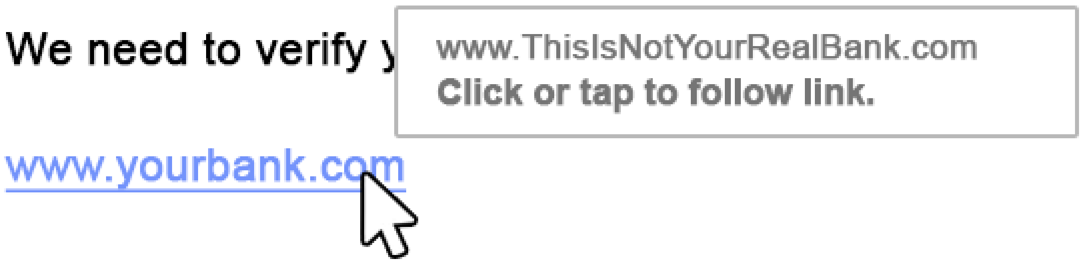
Password Check Required Immediately	43%
A Delivery Attempt was made	9%
De-activation of [[email]] in Process	9%
New food trucks coming to [[company_name]]	8%
Updated Employee Benefits	7%
Revised Vacation & Sick Time Policy	6%
You Have A New Voicemail	6%
New Organizational Changes	4%
Change of Password Required Immediately	4%

How Do You Cultivate A Culture of Cybersecurity Awareness?

- A one-hour training given annually is not enough.
- A culture of cybersecurity awareness is something that is cultivated.
- You MUST train like a NINJA!

THE SINGLE MOST IMPORTANT SKILL

HOVER over a link



We need to verify y

www.ThisIsNotYourRealBank.com
Click or tap to follow link.

www.yourbank.com

- If the email appears to be coming from a company, **does the hover link match** the website of the sender?
- Does link have a **misspelling** of a well-known website (Such as Micorsoft.com)?
- Does the link **redirect to a suspicious external domain** appearing to look like the sender's domain (i.e. micorsoft-support.com rather than microsoft.com)?
- Does the hover link show a URL that **does not match where the context** of the email claims it will take you?
- Do you **recognize** the link's address or did you even **expect to receive** the link?
- Did you receive a **blank email** with **long hyperlinks** and no further information or context?

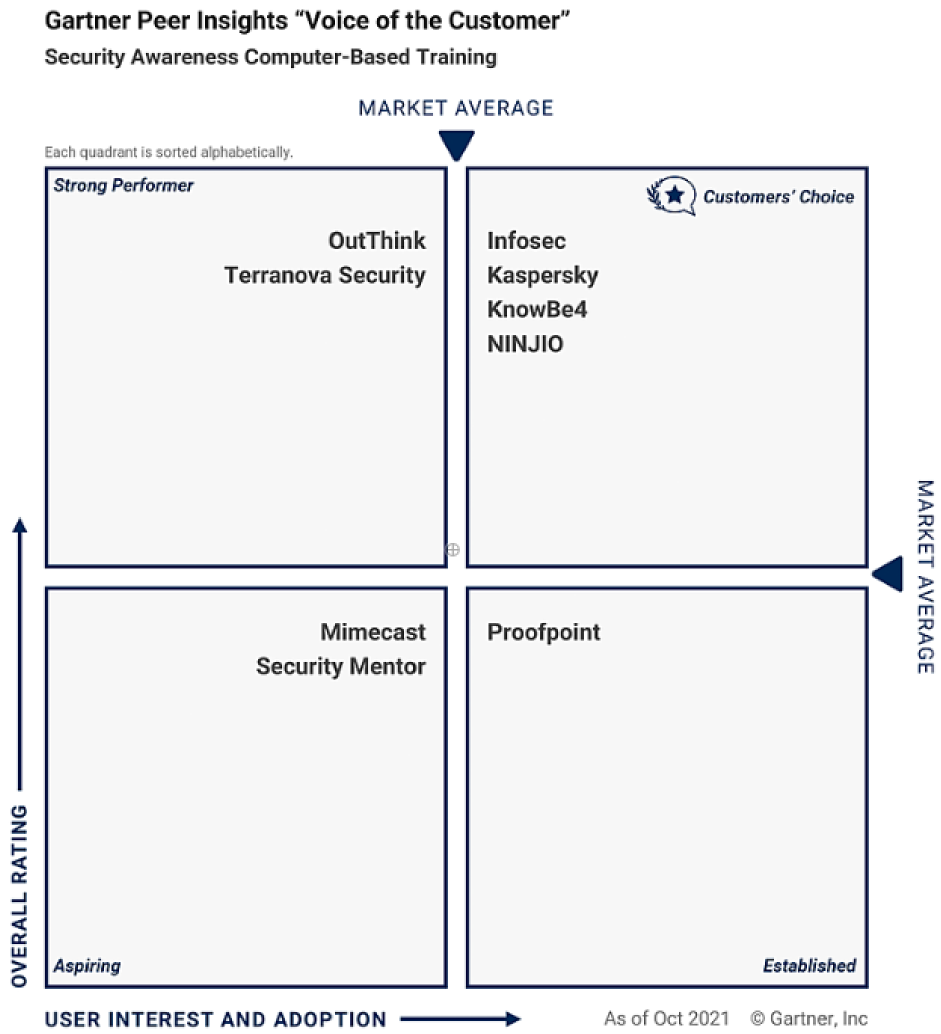
The OTHER Single Most Important Skill

Research shows that it takes 6 seconds for the brain chemicals that caused the brain hijack to diffuse.

Good Email Anti-Phishing Hygiene

- Assume that there’s something phishy about every link in every email
- Pay attention
- What is the email trying to get you to do?
- How is it trying to get you to do it?
- Remember the 6-second rule.

Security Awareness Platforms



Gartner Peer Insights "Voice of the Customer"

Security Awareness Computer-Based Training

Each quadrant is sorted alphabetically.

Strong Performer	Customers' Choice
OutThink Terranova Security	Infosec Kaspersky KnowBe4 NINJIO
Mimecast Security Mentor	Proofpoint
Aspiring	Established

As of Oct 2021 © Gartner, Inc

KnowBe4

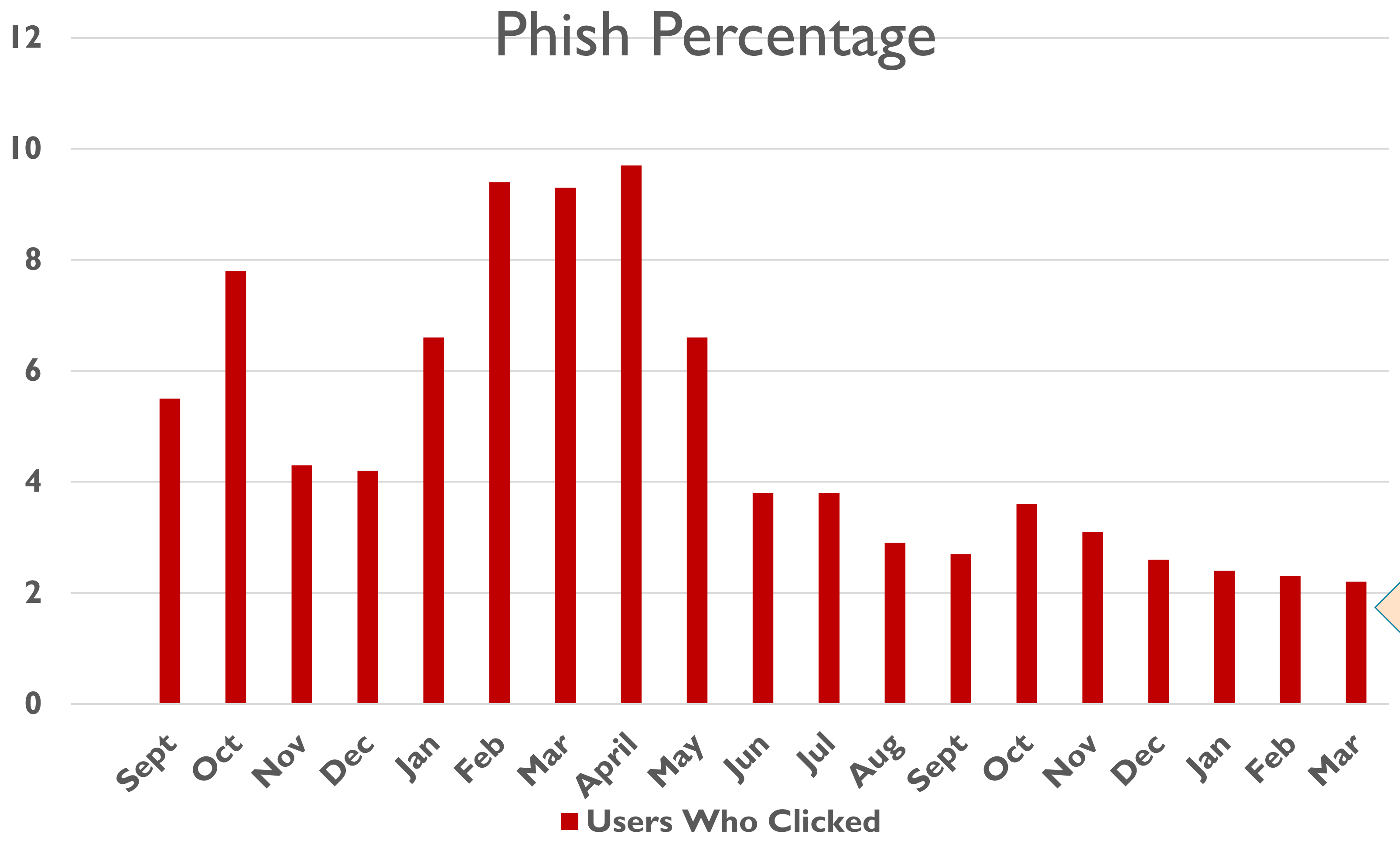
NINJIO

INFOSEC™

Cultivating a Cybersecurity Awareness Culture

- Phishing Tests done monthly
- “Clickers” automatically have to take online training class.
- Supervisors are notified and will get reminders if their staff do not complete training.
- Targeted mini-trainings implemented for groups identified as high-risk (e.g. MAs that have been with the company less than 6 mos., or users that have clicked 3x in the past year)

Testing Is Essential



2.2%
368 emails sent
8 links clicked

Source: QueensCare Health Centers

Identify Patterns

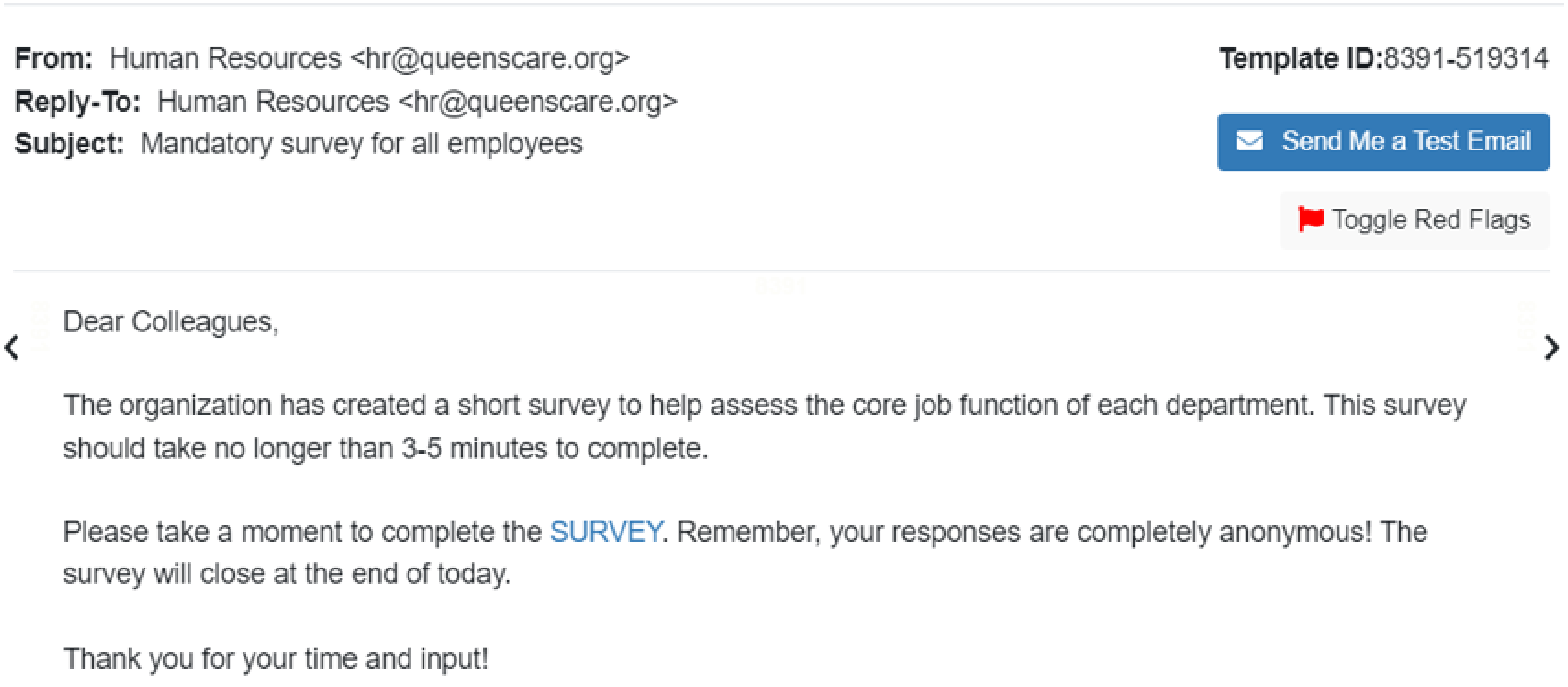
By Job Group

Community Health	1
MA/DA	4
Provider MD/NP/DDS/MH	0
HA/PSR/PAC/CTS	1
Admin/Finance/HR/ Business Services/Fac/ Executive Mgmt	2

By Location

Location 1	4
Location 2	0
Location 3	0
Location 4	1
Location 5	1
Corporate Office	2

Let Them Know What They Clicked On



From: Human Resources <hr@queenscare.org>
Reply-To: Human Resources <hr@queenscare.org>
Subject: Mandatory survey for all employees

Template ID:8391-519314

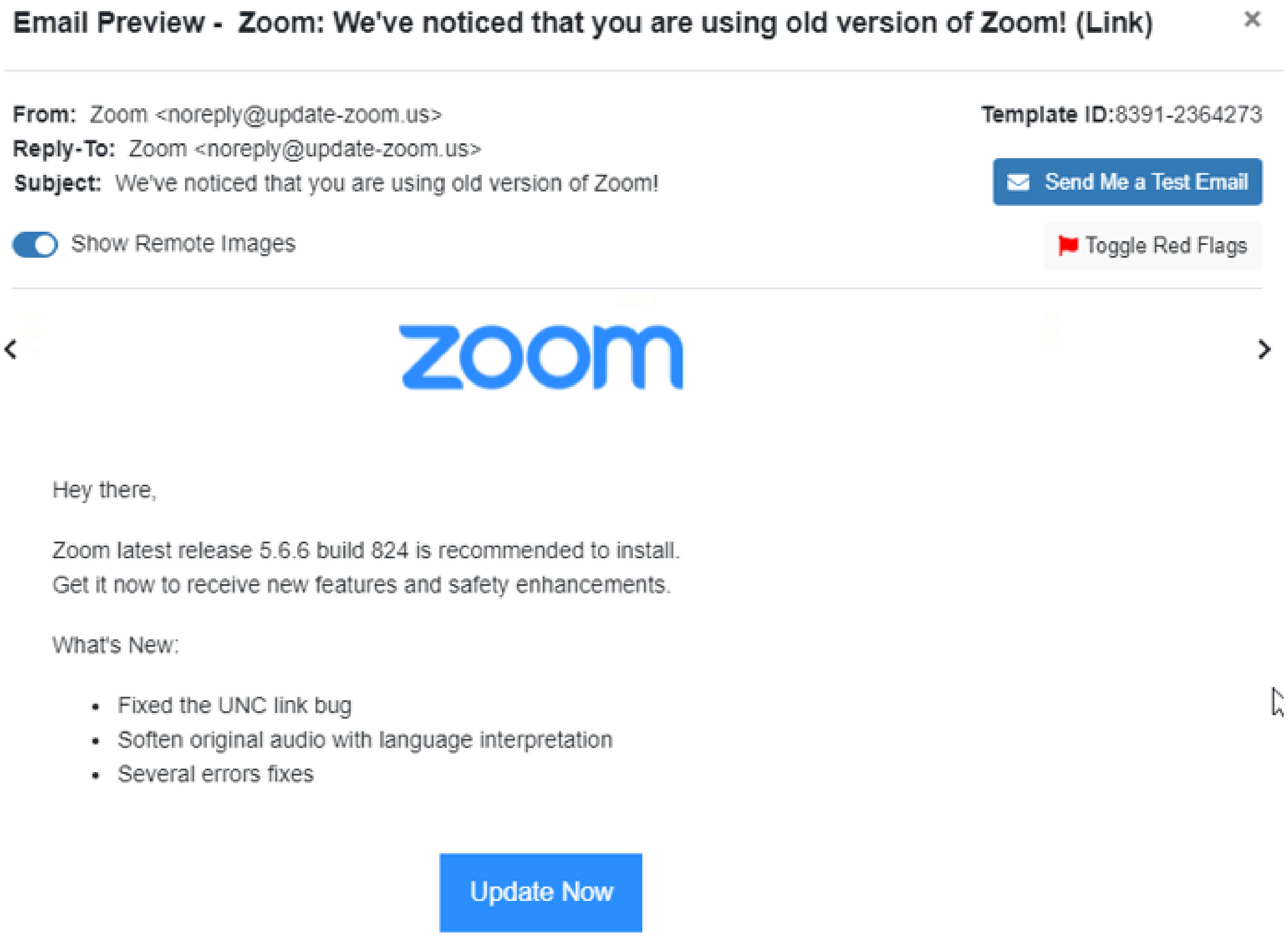
Dear Colleagues,

The organization has created a short survey to help assess the core job function of each department. This survey should take no longer than 3-5 minutes to complete.

Please take a moment to complete the SURVEY. Remember, your responses are completely anonymous! The survey will close at the end of today.

Thank you for your time and input!

Examples - Continued



Email Preview - Zoom: We've noticed that you are using old version of Zoom! (Link)

From: Zoom <noreply@update-zoom.us>

Reply-To: Zoom <noreply@update-zoom.us>

Subject: We've noticed that you are using old version of Zoom!

Template ID:8391-2364273

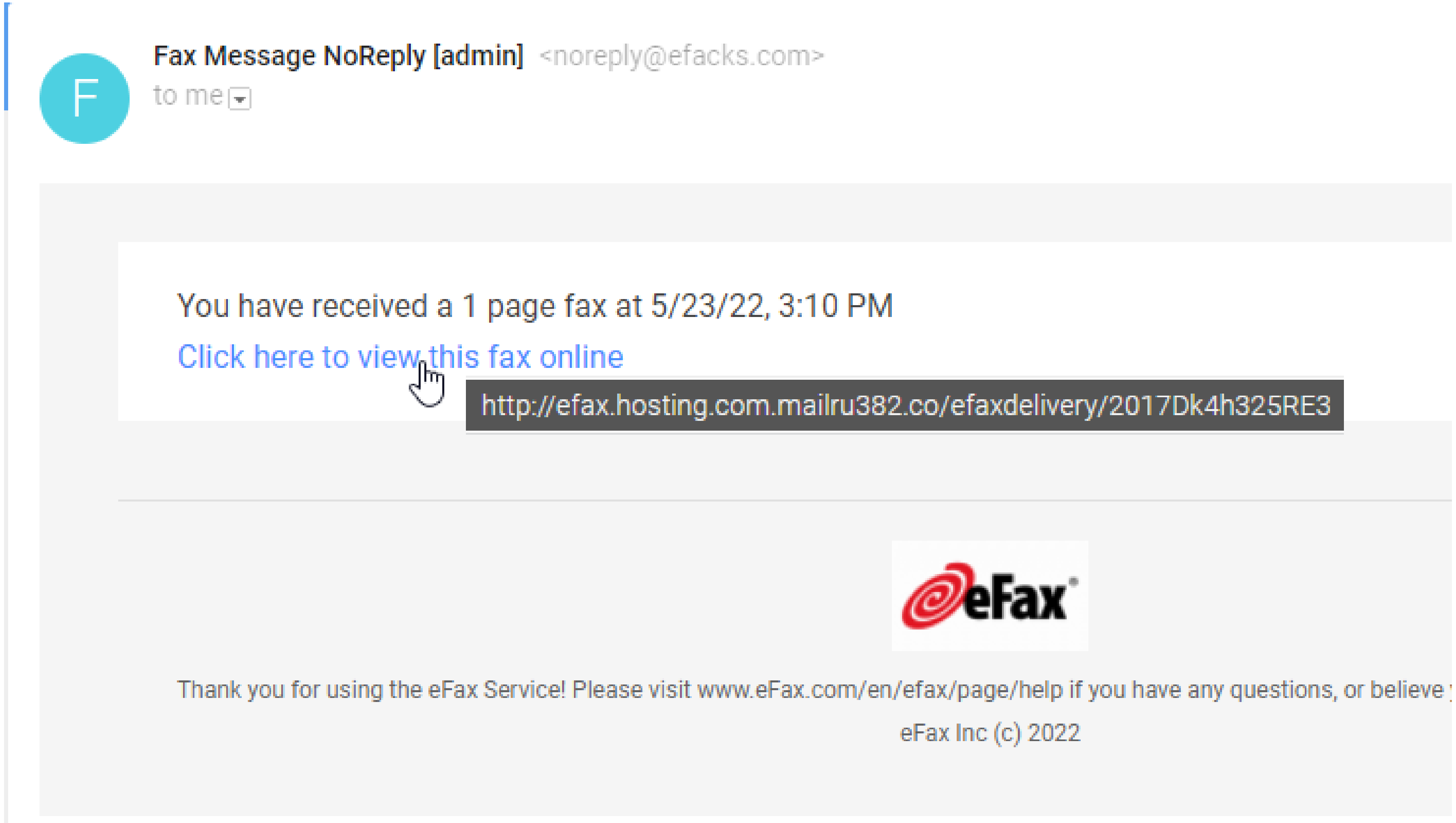
Hey there,

Zoom latest release 5.6.6 build 824 is recommended to install.
Get it now to receive new features and safety enhancements.

What's New:

- Fixed the UNC link bug
- Soften original audio with language interpretation
- Several errors fixes

TABLETOP EXERCISE



Fax Message NoReply [admin] <noreply@efacks.com>
to me

You have received a 1 page fax at 5/23/22, 3:10 PM

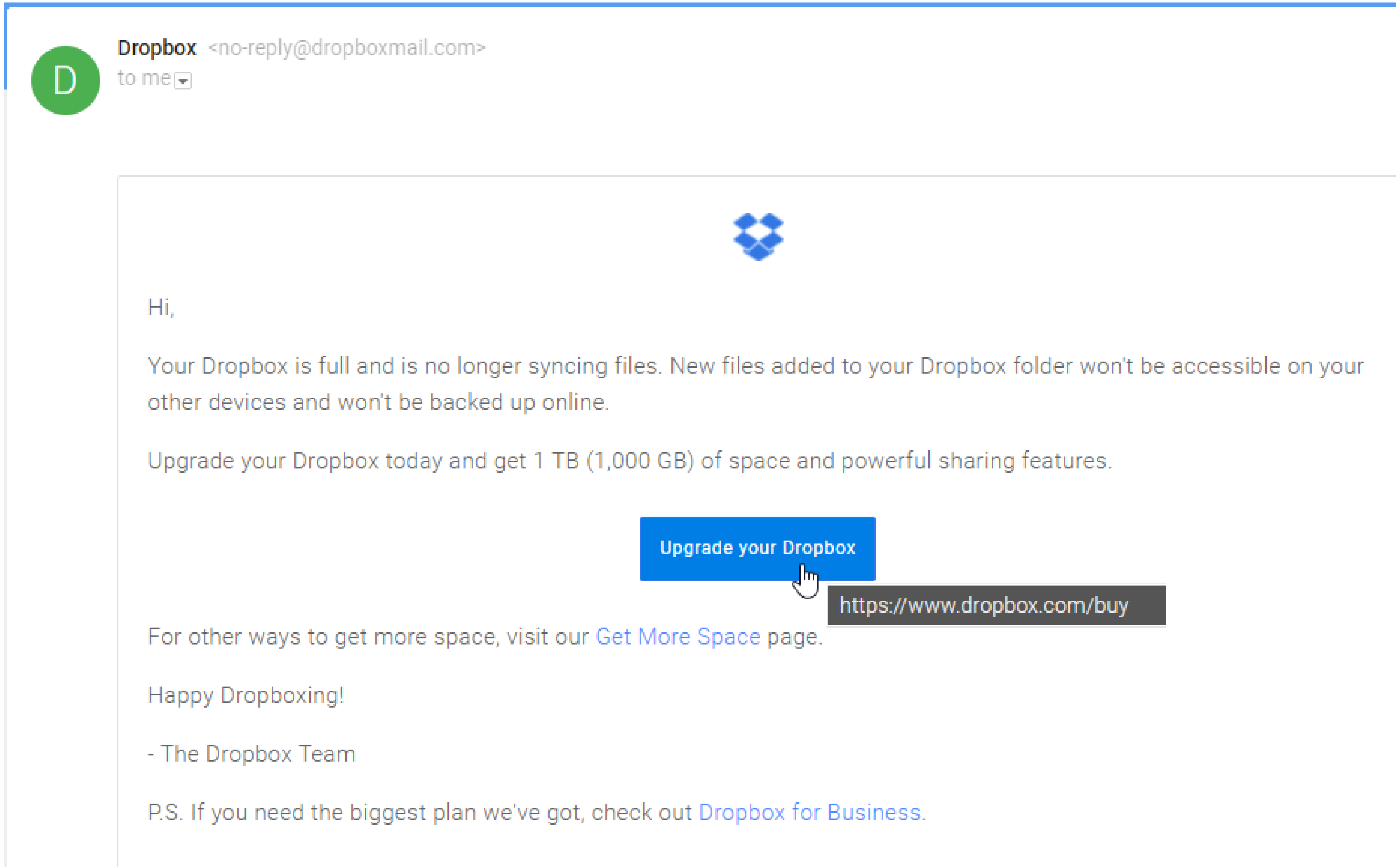
Click here to view this fax online

http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3

Thank you for using the eFax Service! Please visit www.eFax.com/en/efax/page/help if you have any questions, or believe

eFax Inc (c) 2022

TABLETOP EXERCISE



Dropbox <no-reply@dropboxmail.com>
to me

Hi,

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

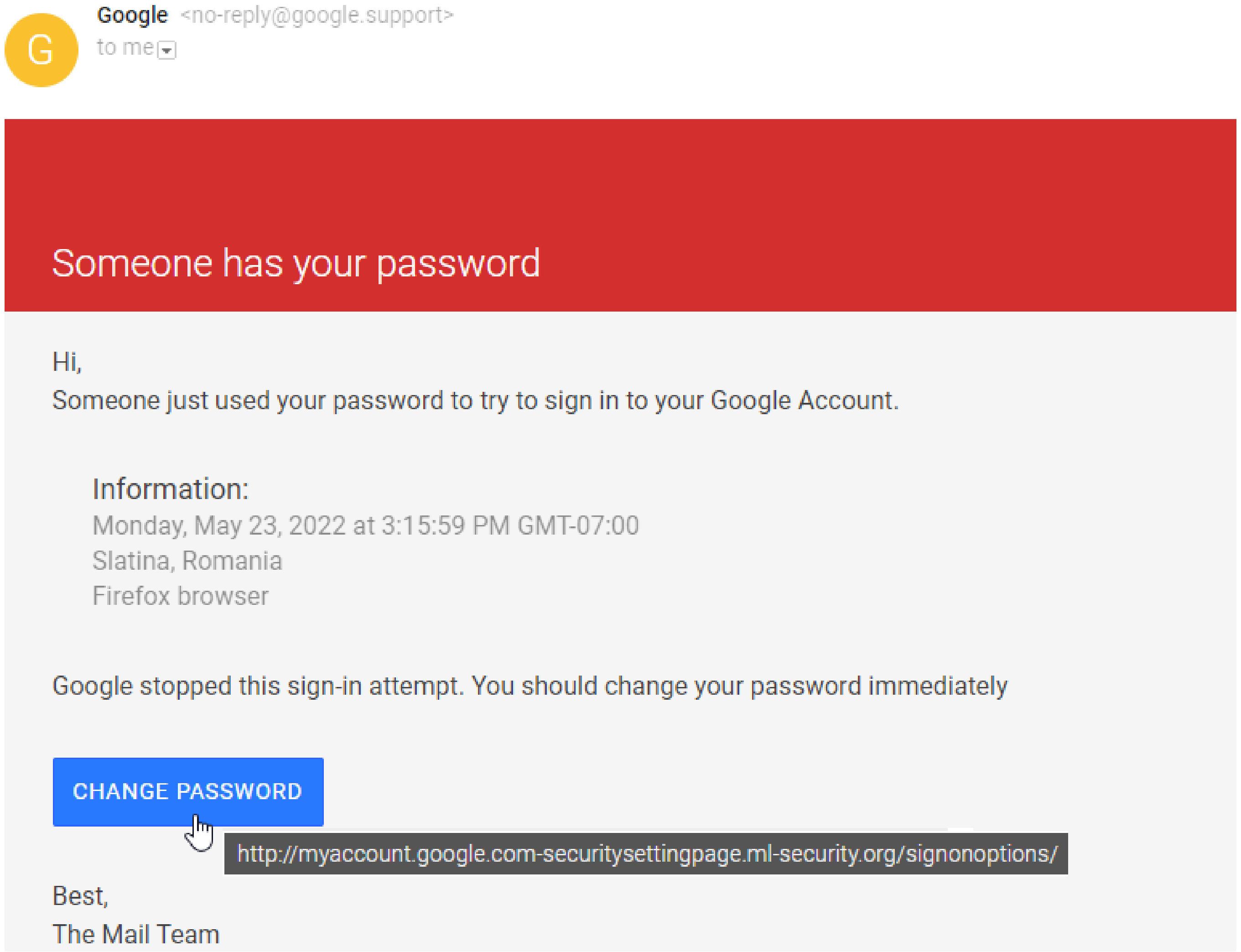
For other ways to get more space, visit our Get More Space page.

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, check out Dropbox for Business.

TABLETOP EXERCISE



Google <no-reply@google.support>
to me

Someone has your password

Hi,
Someone just used your password to try to sign in to your Google Account.

Information:
Monday, May 23, 2022 at 3:15:59 PM GMT-07:00
Slatina, Romania
Firefox browser

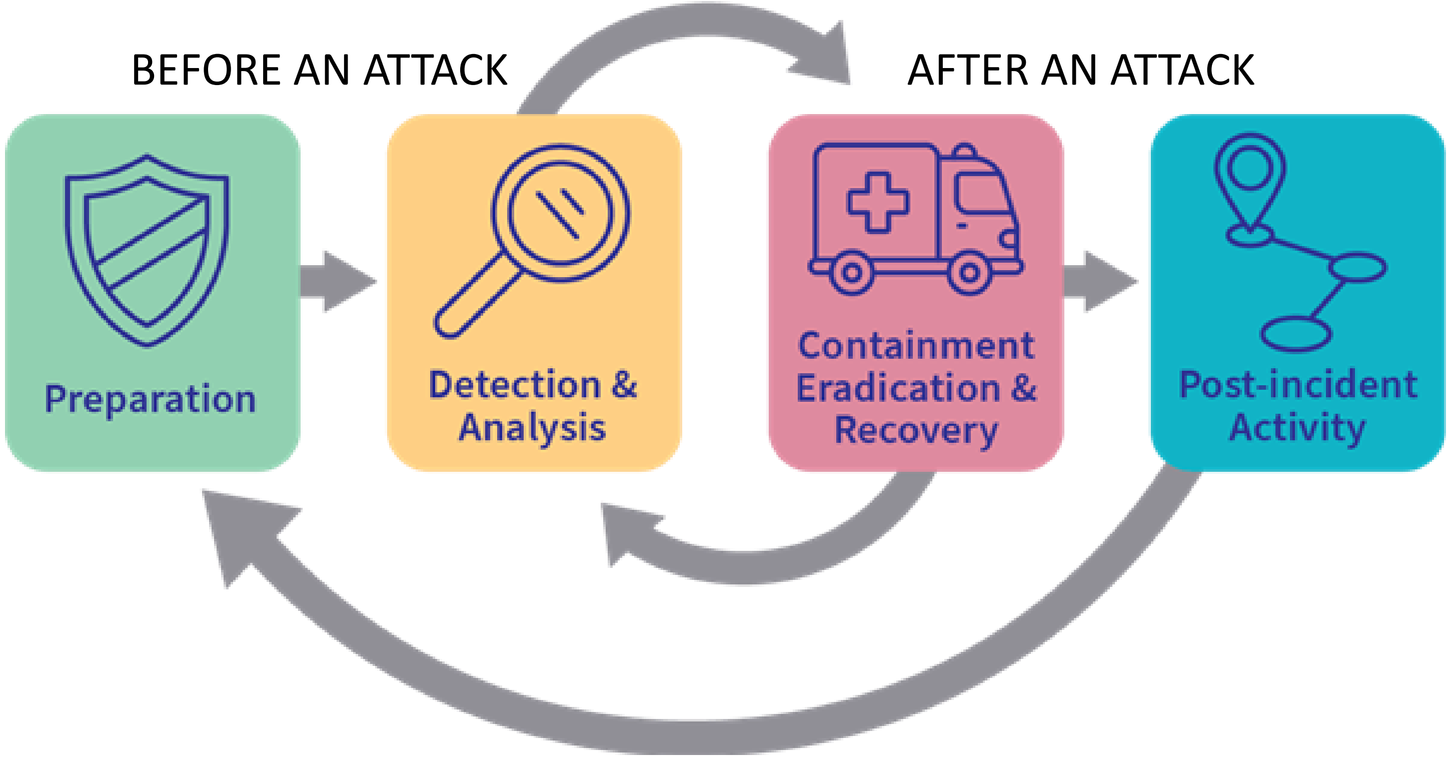
Google stopped this sign-in attempt. You should change your password immediately

http://myaccount.google.com-securitysettingpage.ml-security.org/signonoptions/

Best,
The Mail Team

WHAT HAPPENS WHEN SOMEONE CLICKS

NIST Incident Response Plan



BE Prepared

- Compile a list of IT assets such as networks, servers and endpoints.
- Identify their importance and which ones are critical or hold sensitive data.
- Set up monitoring so you have a baseline of normal activity. Determine which types of security events should be investigated.
- Create detailed response steps and communication guidelines for common types of incidents.

Detection and Analysis

- Implement monitoring systems for networks, systems, and logs in order to detect, alert, and report on potential security incidents.

- Identifying a baseline or normal activity for these systems. You must be able to correlate related events and see if and how they deviate from normal behavior.

Containment, Eradication, Recovery

- The goal of **containment** is to stop the attack before it overwhelms resources or causes damage. Your containment strategy will depend on the level of damage the incident can cause, the need to keep critical services available to employees and customers, and the duration of the solution—a temporary solution for a few hours, days or weeks, or a permanent solution.
- Containment methods include a **co-ordinated shutdown** and **blocking communication channels** and **network routes** once compromised systems are identified.
- **Eradication** step removes all elements of the incident from the environment, including malware from all compromised hardware.
- Login credentials must be changed on all compromised accounts.
- Once the threat is eradicated, the goal is a **recovery** to normal operations as quickly as possible.

Post Incident Activity

Questions to ask

- What happened, and at what times?
- How well did the incident response team deal with the incident? Were processes followed, and were they sufficient?
- What information was needed sooner?
- Were any wrong actions taken that caused damage or inhibited recovery?
- What could staff do differently next time if the same incident occurred?
- Could staff have shared information better with other organizations or other departments?
- Have we learned ways to prevent similar incidents in the future?
- Have we discovered new precursors or indicators of similar incidents to watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?

Sample Incident Response Plan Template

California Government Department of Technology Incident Response Plan – includes 17-step incident response procedure, with more detailed plans for specific incident types. Download .DOC file

https://cdt.ca.gov/wp-content/uploads/2017/03/templates_incident_response_plan.doc

Tabletop Exercise

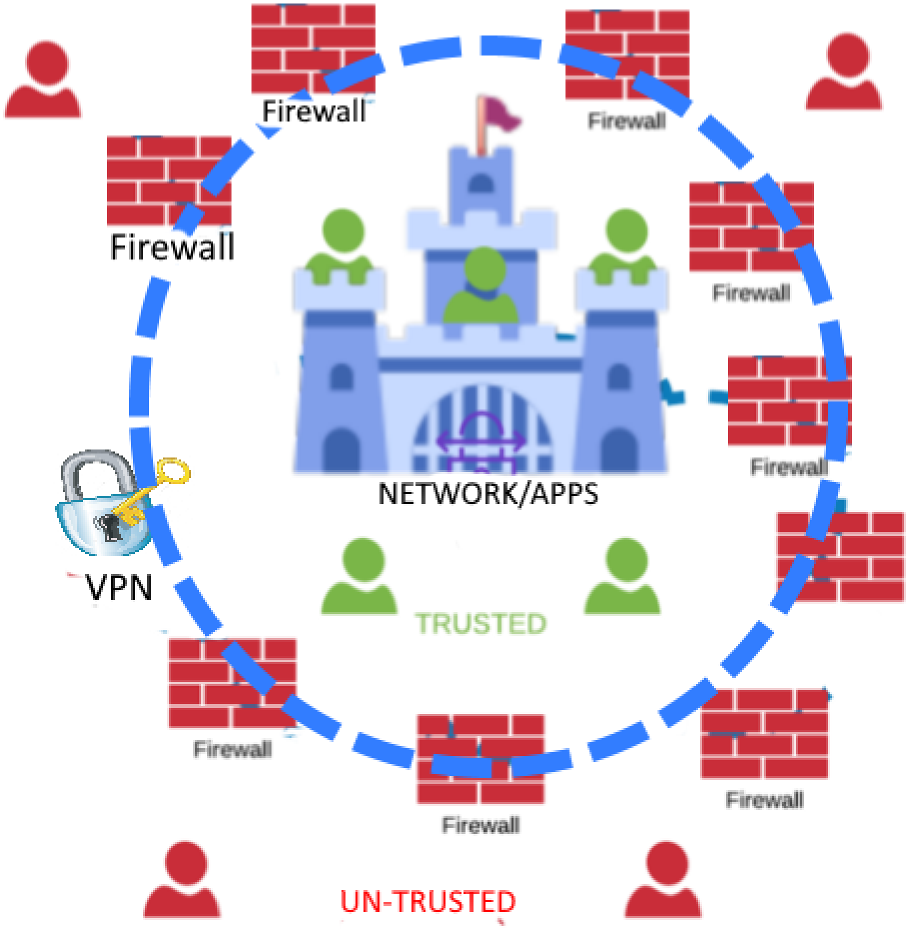
You (IT) get a call from one of your providers. Their company provided laptop got stolen from Starbucks.
You're not worried because:

A: Oh You're definitely worried
B: The laptop was encrypted
C: You have tools installed to track it and brick it
D: He said it was turned off
E: B and C

Future Proofing Cybersecurity: Zero Trust

The core concept of zero trust is simple: assume everything is hostile by default.

Traditional Network Security



The Castle and Moat Approach: Everyone inside the Moat is trusted, Everyone outside is untrusted

You get access to the inside by being already inside OR by connecting via the VPN.

Weaknesses

This approach does not accommodate for non-traditional workmodes (e.g. BYOD, remote work) well.

VPN bandwidth can be a limitation.

Single point of failure: An attacker can compromise a single endpoint within the trusted boundary and create/expand a foothold inside.

Note: Single largest reason for a data breach (9 out of 10 times) is a phishing email on one single user.

Zero Trust Model – What It Isn’t

It is not a piece of technology or any one Software implementation.

It is rather a framework that can be implemented by incorporating several security technologies that already exist and are already being used standalone or in some combinations.

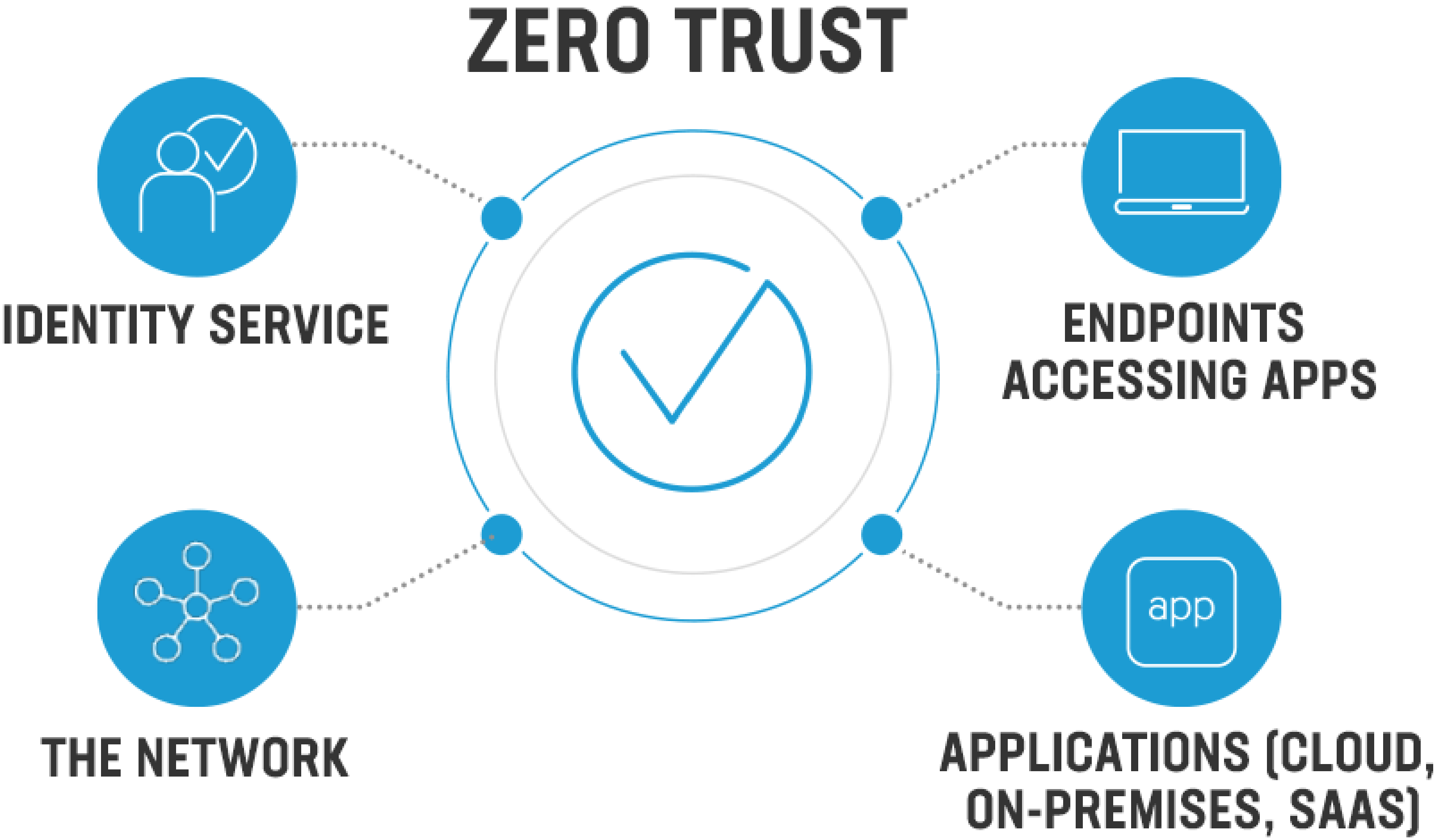
Zero Trust Model Principles

Trust No One. Always Verify.

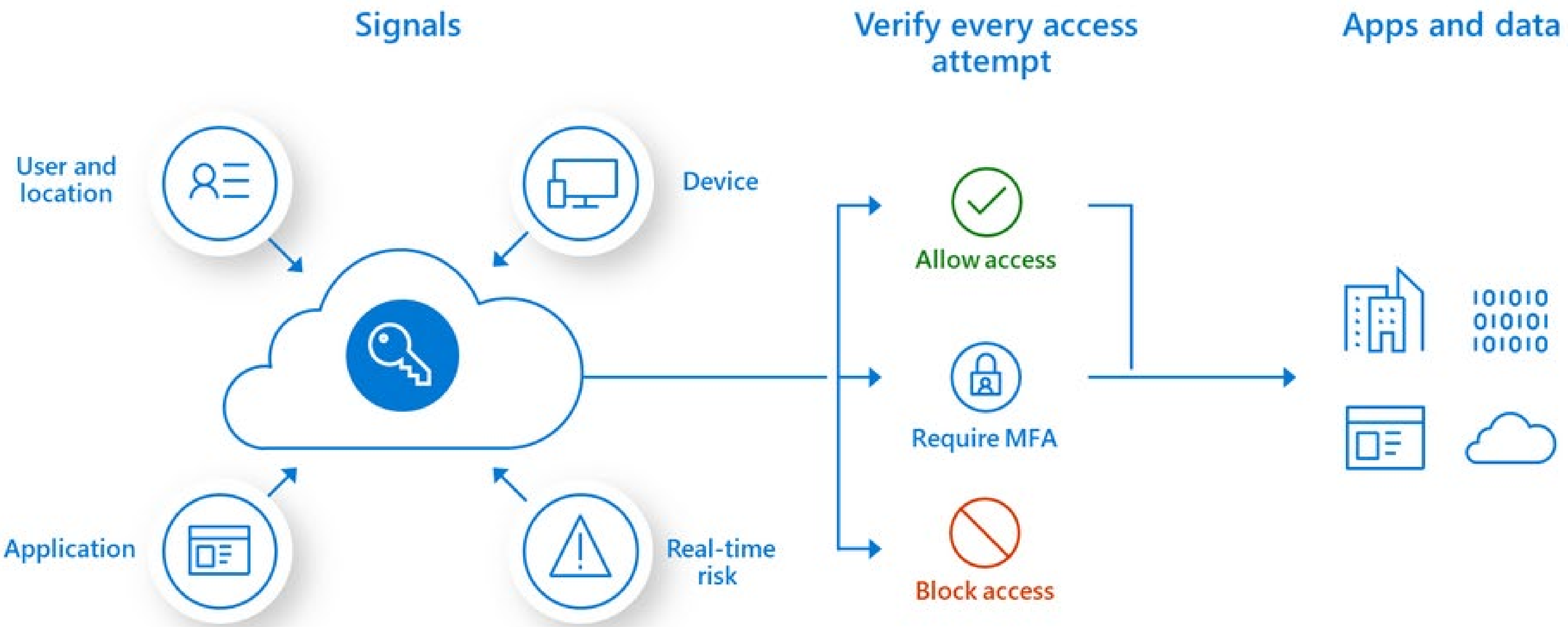
Use Least Privilege Access. Restrict User/Device to the MINIMUM permission required.

Assume breach. Every access attempt is considered hostile until verified otherwise.

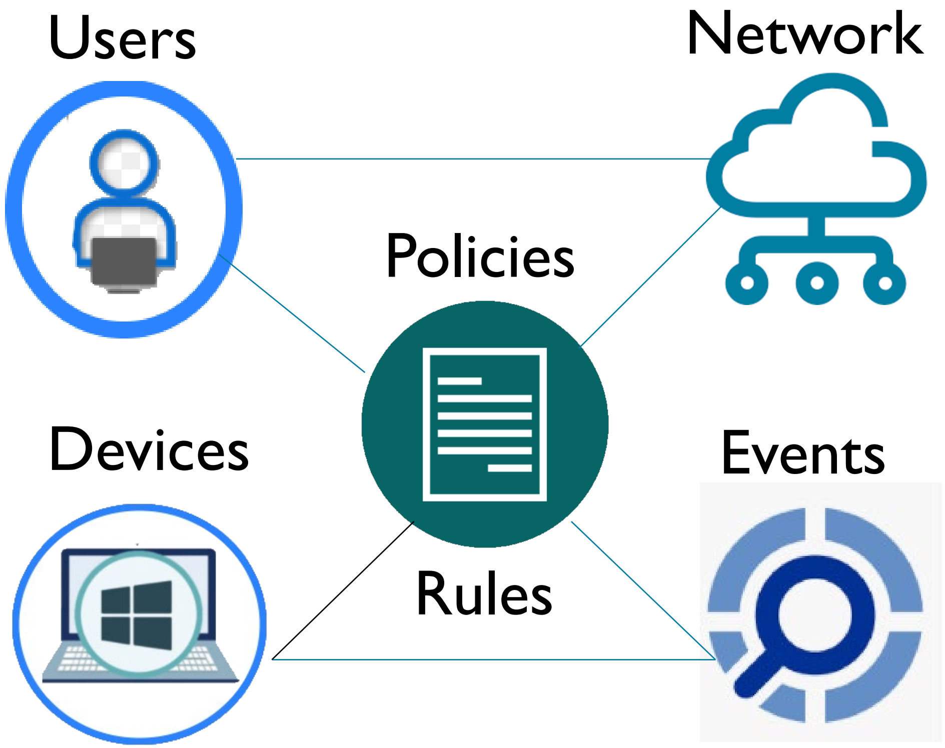
Zero Trust Components



Zero Trust – Practical Application Workflow

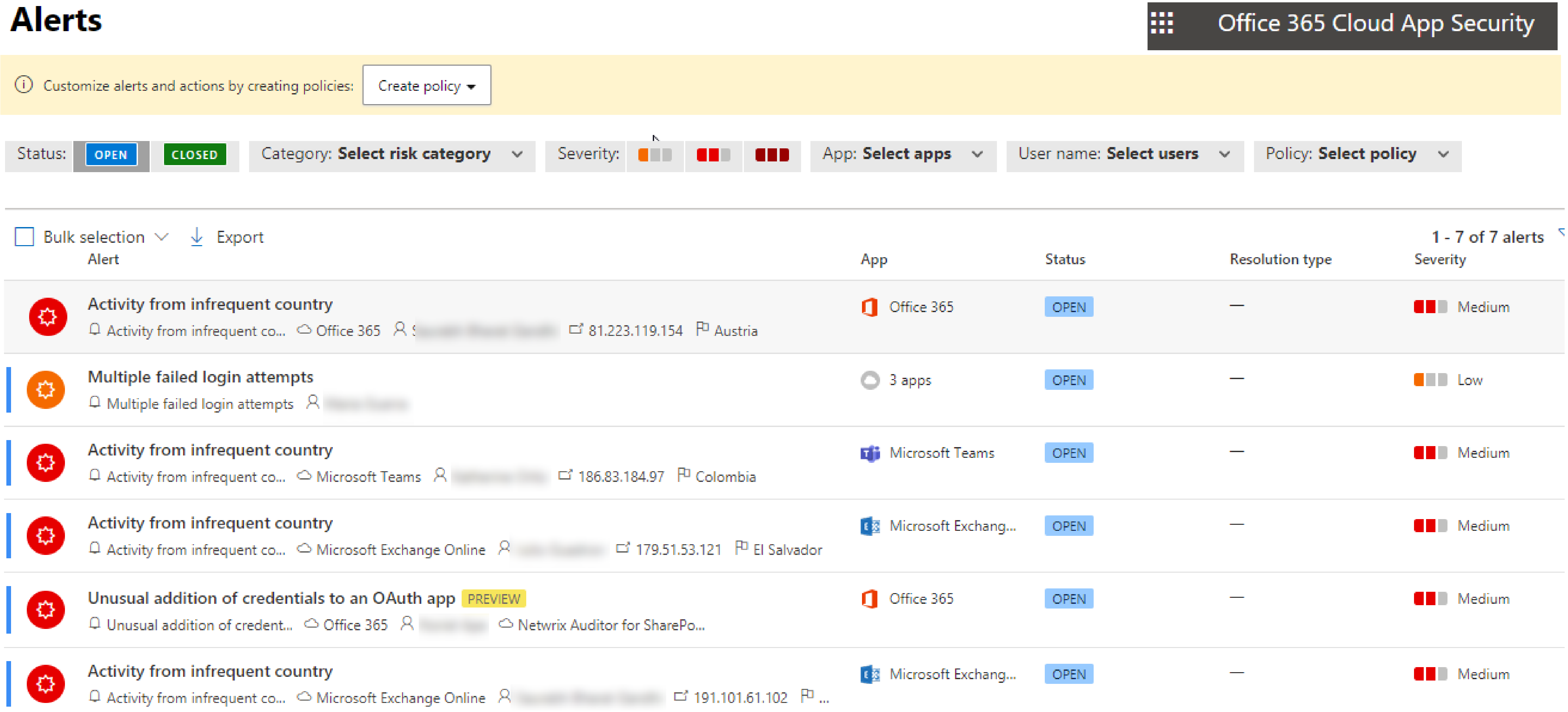


Zero Trust Framework – Interactive Parts



Rules:
Let in only specific users, IP Addresses, MAC addresses, geographic locations to specific networks, apps, and systems.

What Does It Look Like In the Real World



Office 365 Cloud App Security

Alerts

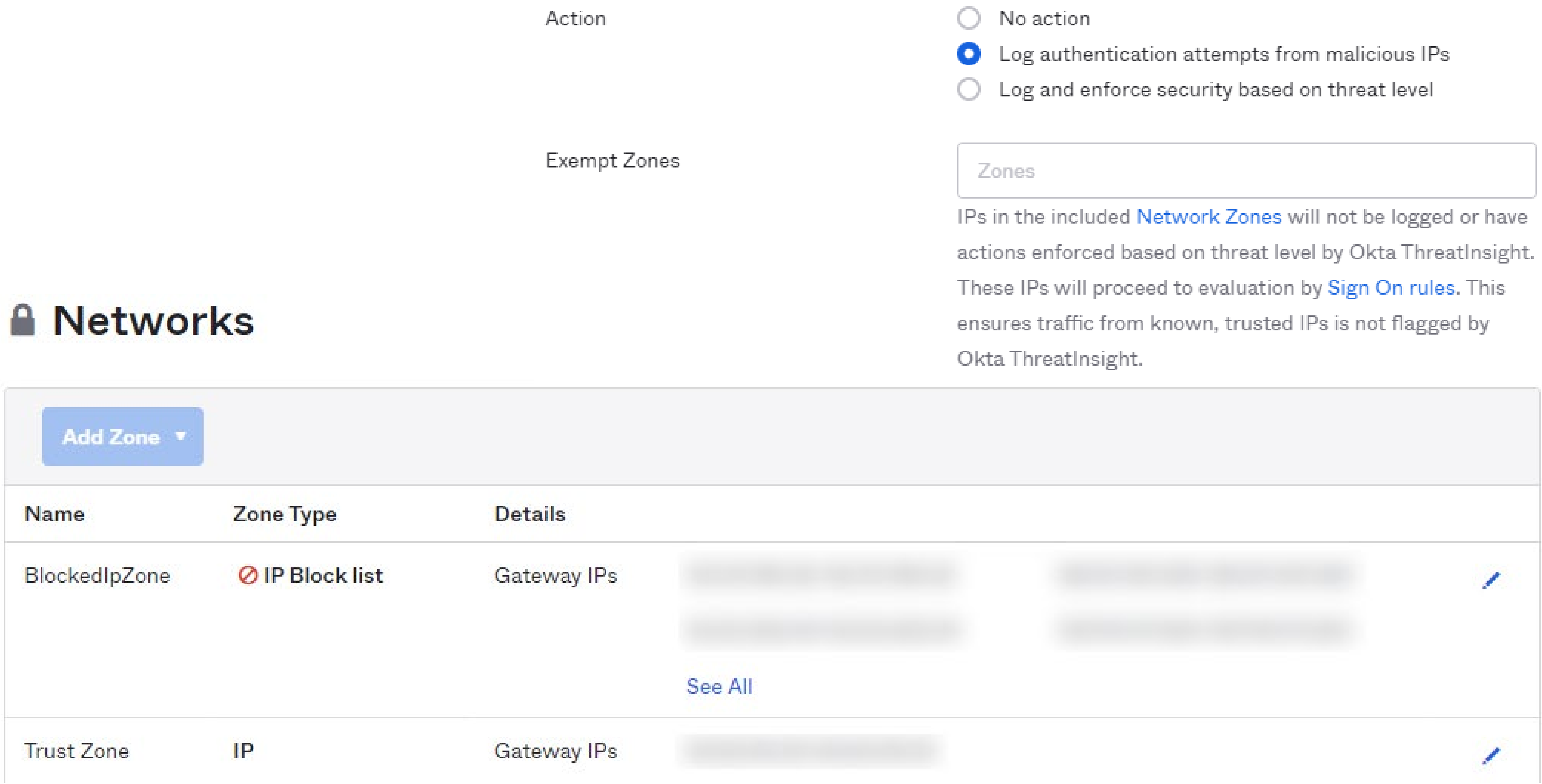
ⓘ Customize alerts and actions by creating policies: Create policy ▾

Status: OPEN CLOSED | Category: **Select risk category** | Severity: 🟧⬜⬜ 🟥🟥⬜ 🟥🟥🟥 | App: **Select apps** | User name: **Select users** | Policy: **Select policy**

□ Bulk selection ⌄ ↓ Export — 1 - 7 of 7 alerts

Alert	App	Status	Resolution type	Severity
Activity from infrequent country Activity from infrequent co... · Office 365 · [redacted] · 81.223.119.154 · Austria	Office 365	OPEN	—	Medium
Multiple failed login attempts Multiple failed login attempts · [redacted]	3 apps	OPEN	—	Low
Activity from infrequent country Activity from infrequent co... · Microsoft Teams · [redacted] · 186.83.184.97 · Colombia	Microsoft Teams	OPEN	—	Medium
Activity from infrequent country Activity from infrequent co... · Microsoft Exchange Online · [redacted] · 179.51.53.121 · El Salvador	Microsoft Exchang...	OPEN	—	Medium
Unusual addition of credentials to an OAuth app PREVIEW Unusual addition of credent... · Office 365 · [redacted] · Netwrix Auditor for SharePo...	Office 365	OPEN	—	Medium
Activity from infrequent country Activity from infrequent co... · Microsoft Exchange Online · [redacted] · 191.101.61.102 · ...	Microsoft Exchang...	OPEN	—	Medium

Example: Okta



Action

○ No action
● Log authentication attempts from malicious IPs
○ Log and enforce security based on threat level

Exempt Zones

Zones

IPs in the included Network Zones will not be logged or have actions enforced based on threat level by Okta ThreatInsight. These IPs will proceed to evaluation by Sign On rules. This ensures traffic from known, trusted IPs is not flagged by Okta ThreatInsight.

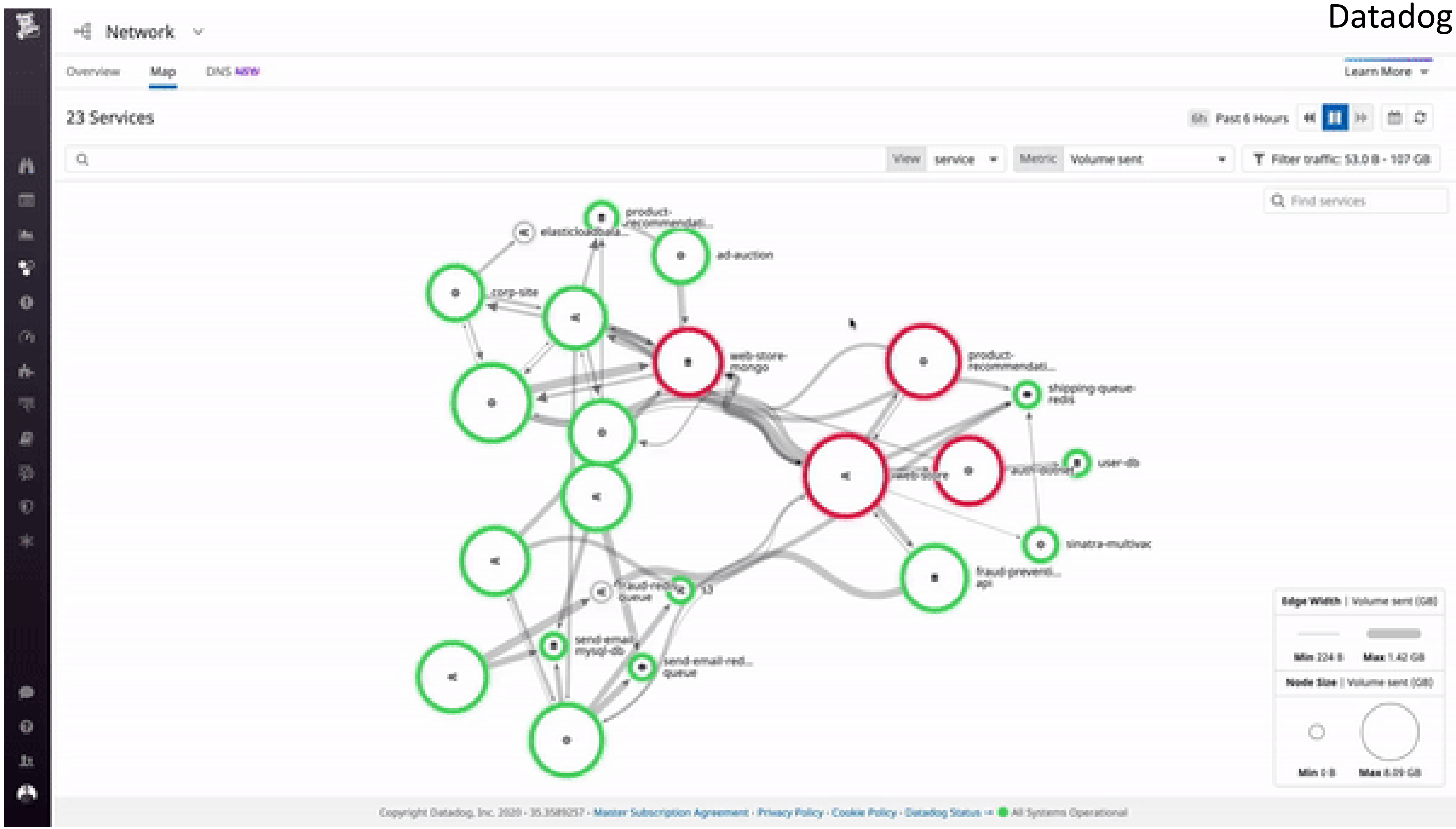
Networks

Add Zone ▾

Name	Zone Type	Details	
BlockedIpZone	⊘ IP Block list	Gateway IPs	[redacted] See All
Trust Zone	IP	Gateway IPs	[redacted]

Network Bandwidth Analyzer

Datadog



Network

23 Services

Past 6 Hours

View: service

Metric: Volume sent

Filter traffic: 53.0 B - 107 GB

Edge Width | Volume sent (GB)

Min 224 B Max 1.42 GB

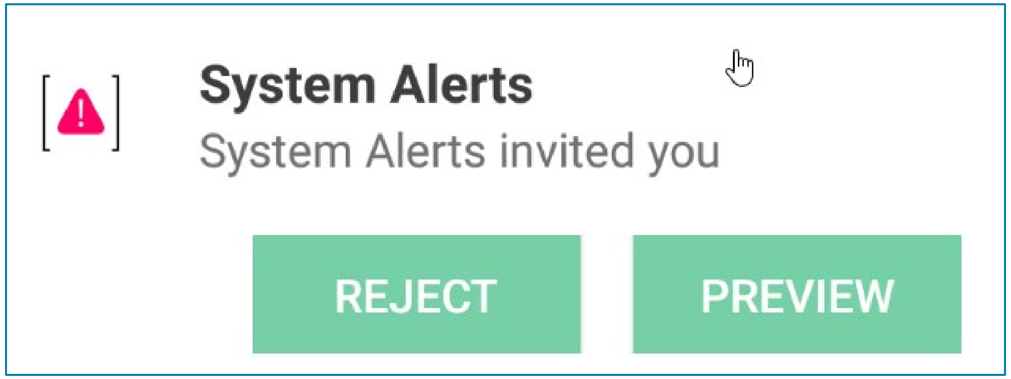
Node Size | Volume sent (GB)

Min 0 B Max 8.09 GB

Copyright Datadog, Inc. 2020 - 35.3589257 - Master Subscription Agreement - Privacy Policy - Cookie Policy - Datadog Status → All Systems Operational

New World of IT Maintenance

You will get LOTS more warnings and alerts.



System Alerts

System Alerts invited you

You will sleep better at night.

Thank You!

Questions and Answers?

How Can You Contact Us?

Michael Sanguily
MSanguily@hcnetwork.org

Arnell Mendoza
Amendoza@queenscare.org

ARE YOU LOOKING FOR RESOURCES?

Please visit our website **www.healthcenterinfo.org**

HEALTH CENTER
RESOURCE
CLEARINGHOUSE

Twitter.com/NACHC

Facebook.com/nachc

Instagram.com/nachc

Linkedin.com/company/nachc

YouTube.com/user/nachcmedia