

Cybersecurity Trends

2022 State of Cybersecurity



Presenter



Michael Nougquier, CISSP

Chief Information Security Officer

&

Director of Cybersecurity Services



Agenda



What is Cybersecurity



2022 Trends in Cybersecurity



Anatomy of a Cyberattack



Impacts of a Breach



Training



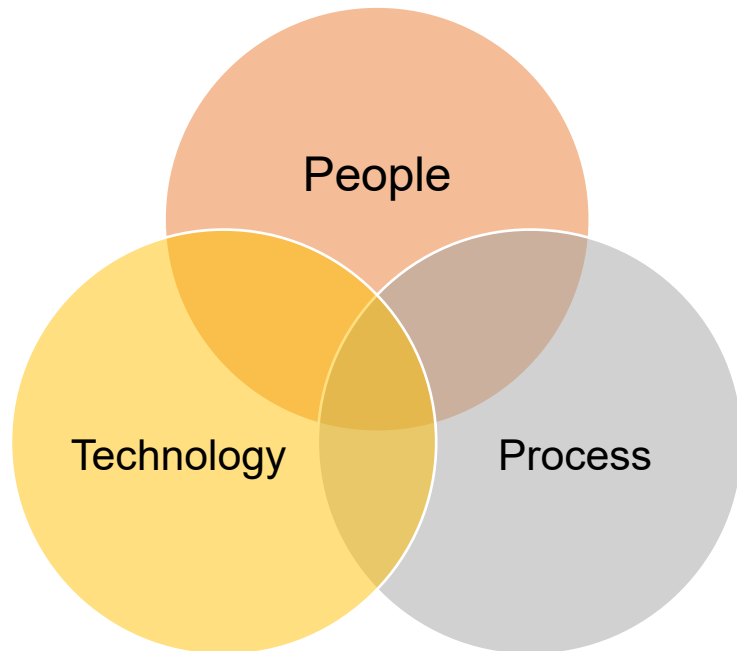
Best Practices



Q&A

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks by using a combination of People, Process and Technology together in an effort to ensure the Confidentiality, Integrity and Availability of information assets that allow your business to function.



Cybersecurity Trends

2022 Cybersecurity Trends

Ransomware



Popular because its effective

BEC



Business. Email.
Compromise.

Cyber Insurance



The new Life
Insurance

Ransomware



- Ransomware is a form of malicious software designed to block access to a computer system until a sum of money, often in cryptocurrency, is paid
- Often deployed via social engineering
- Double extortion tactics are commonly used
- A new ransomware attack occurs every 14 seconds
- 75% of small- and midsize businesses would be forced to close if a bad actor demanded a ransom
- \$20 MBillion is the estimated cost of Ransomware in 2022

RANSOMWARE | NEWS

College closes down after ransomware attack

Posted: May 12, 2022 by Jovi Umawing

16 AUG 2021 NEWS

Half of US Hospitals Shut Down Networks Due to Ransomware



Business Email Compromise (BEC)

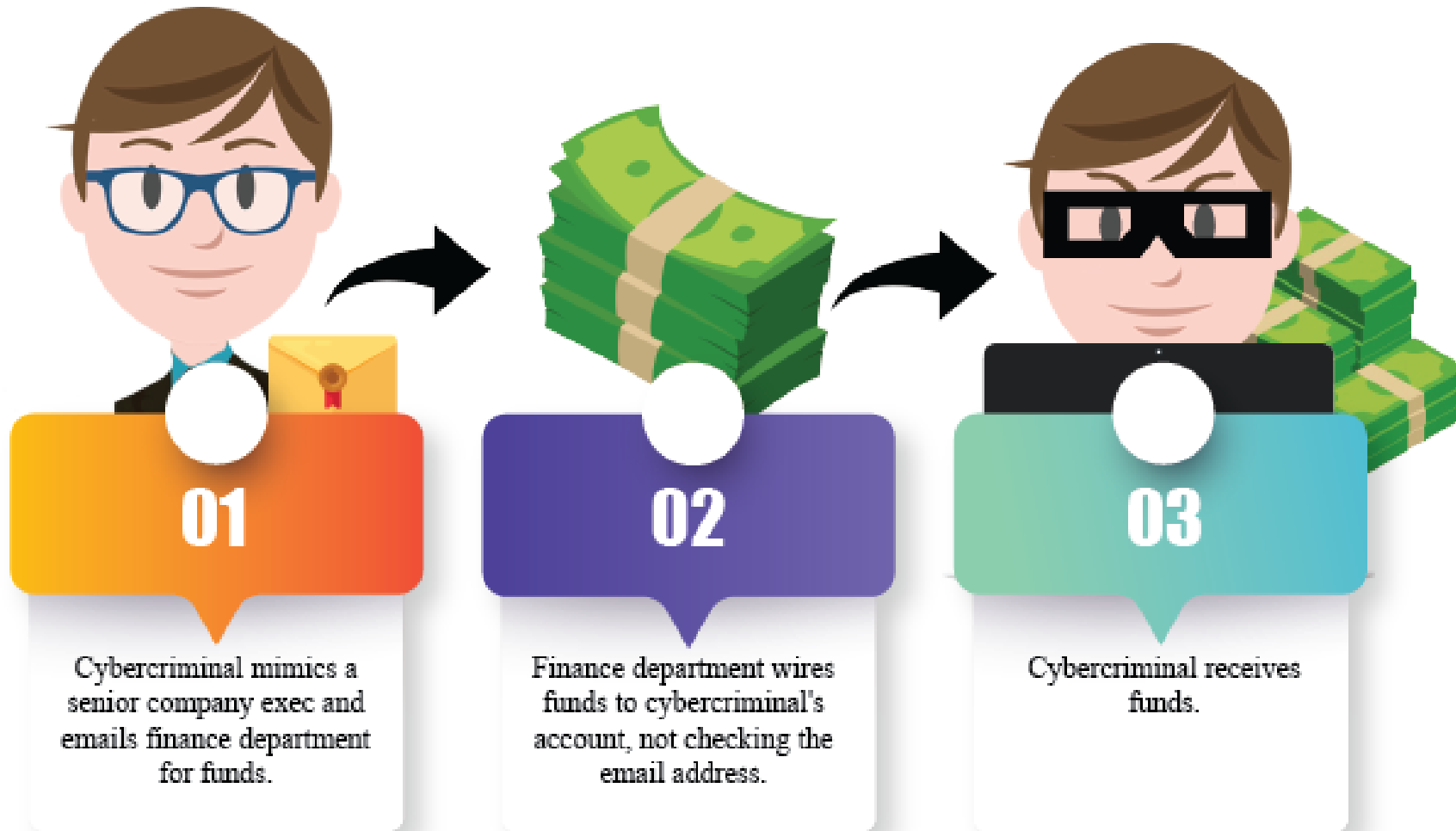
What is it?

- Business email compromise is a type of email cyber crime scam in which an attacker targets a business to defraud the company
- Typically, through the use of fake invoicing
- Social Engineering (phishing) is the common attack vector

Protections

- Security Awareness Training
- Consistent Phishing Tests
- Thoughtful Policies and Procedures
- Email/Identity Technologies
- Constant Vigilance

BEC Explained



Cyber Insurance



01 Increased Rates

Rates increased 110% in Q1
2022 – Marsh
Deductibles are on the
rise



02 Denial

Cyber Insurance can be
denied for lack of security
maturity.
Insurance Underwriters
are requiring Risk Self
Assessments



03 Restrictive Coverage

Detail Review Policy,
Exclusions, and Amendments
carefully. Ransomware is
often an extra rider.

Anatomy of a Cyberattack

Anatomy of a Cyberattack

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (5)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (5)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (5)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (5)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Remote Services (6)	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (5)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (2)	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)	Software Deployment Tools		Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Taint Shared Content	Data from Information Repositories (3)	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites	System Services (2)		System Services (2)	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
	User Execution (3)		User Execution (3)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Execution Guardrails (1)	Network Sniffing	File and Directory Permissions Modification (2)		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
	Windows Management Instrumentation		Windows Management Instrumentation	Implant Internal Image	Process Injection (12)	Exploitation for Defense Evasion	Network Share Discovery	Hide Artifacts (10)		Data from Removable Media	Protocol Tunneling		System Shutdown/Reboot
				Modify Authentication Process (5)	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	Network Service Discovery	Hijack Execution Flow (12)		Data from Staged (2)	Proxy (4)		
				Office Application Startup (5)	Valid Accounts (4)	Impair Defenses (3)	OS Credential Dumping (5)	Impair Defenses (3)		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (5)	Steal Application Access Token	OS Credential Dumping (5)		Input Capture (4)	Traffic Signaling (1)		
				Scheduled Task/Job (5)		Indirect Command Execution	Steal or Forge Kerberos Tickets (4)	Steal Application Access Token		Screen Capture	Web Service (3)		
				Server Software Component (5)		Masquerading (7)	Steal Web Session Cookie	Steal or Forge Kerberos Tickets (4)		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (5)	Unsecured Credentials (7)	Steal Web Session Cookie					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Unsecured Credentials (7)					
						Modify Registry							
						Modify System Image (2)							
						Network Boundary Bridging (1)							
						Obfuscated Files or Information (5)							
						Plist File Modification							
						Pre-OS Boot (5)							
						Process Injection (12)							
						Reflective Code Loading							
						Rogue Domain Controller							
						Rootkit							
						Subvert Trust Controls (5)							
						System Binary Proxy Execution (13)							
						System Script Proxy Execution (1)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

Anatomy of a Cyberattack (Simplified)



Impacts of a Breach



Impacts of a Cyberattack

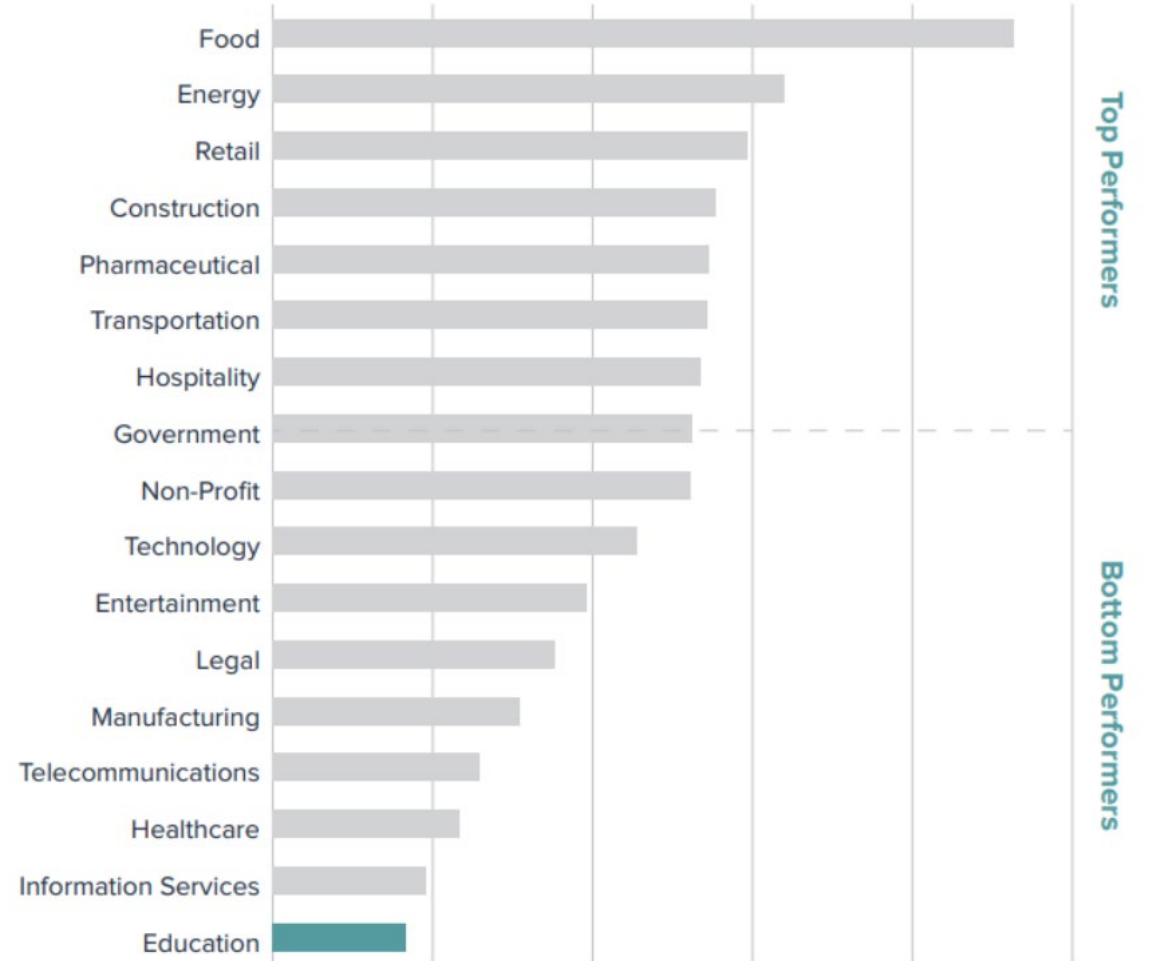
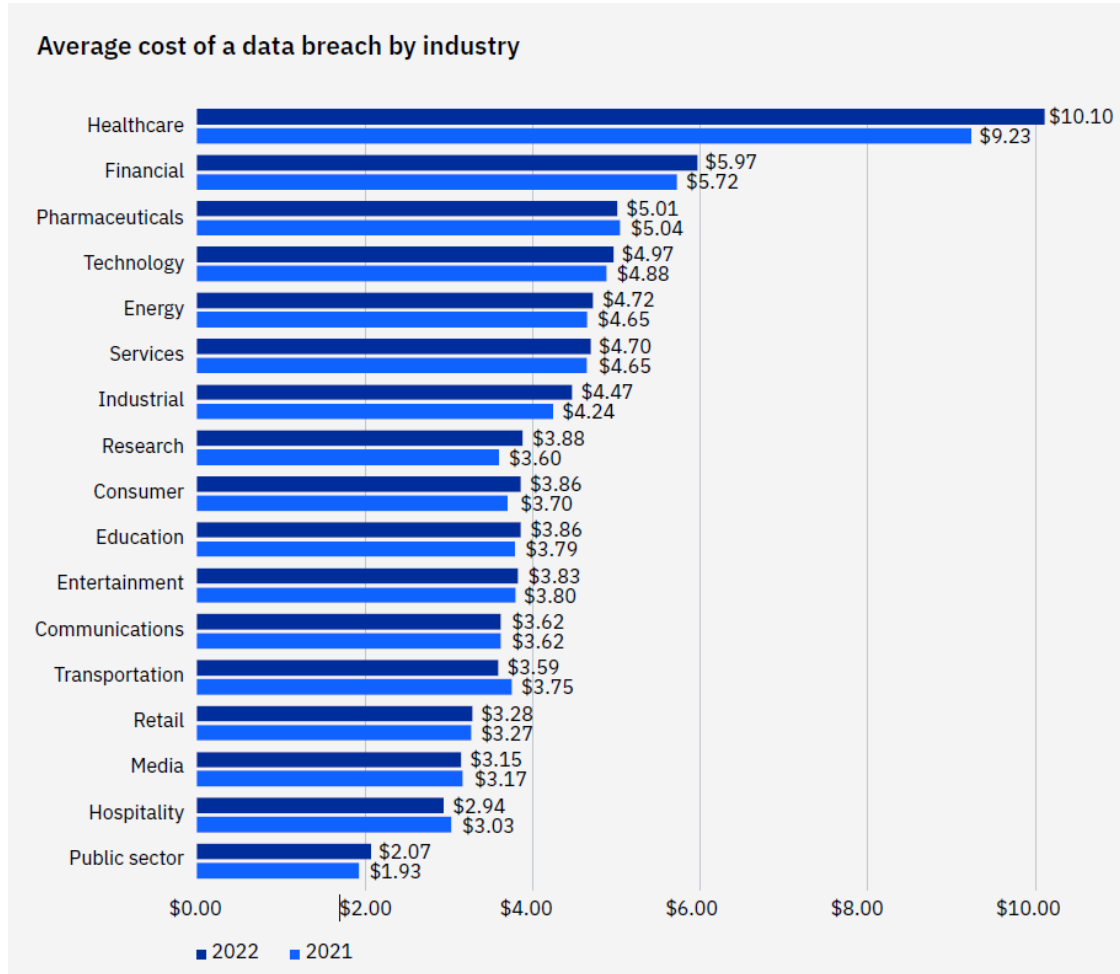
Reputational Damage

Business Interruption

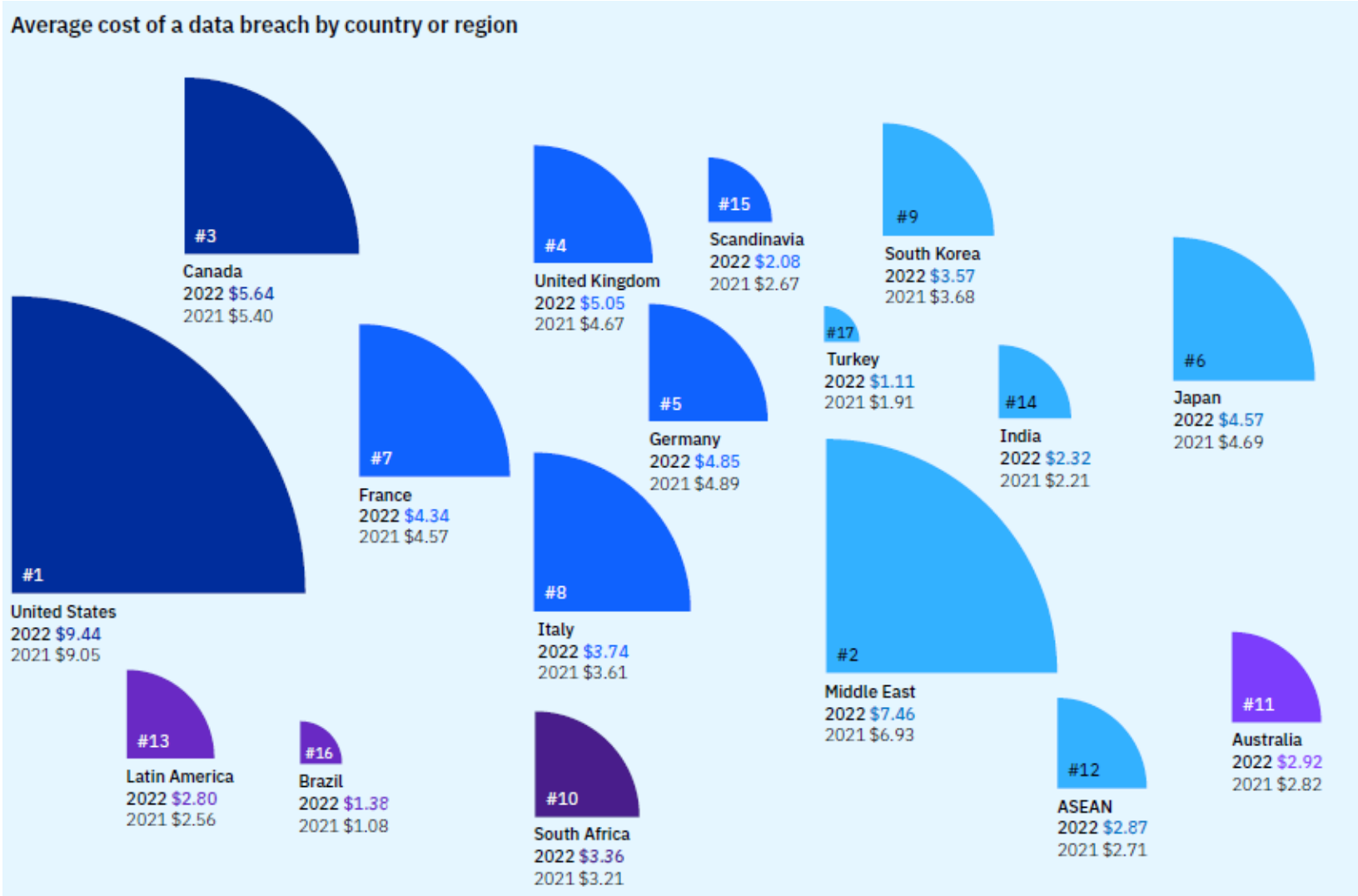
Legal and Regulatory Costs

Technical Recovery Costs

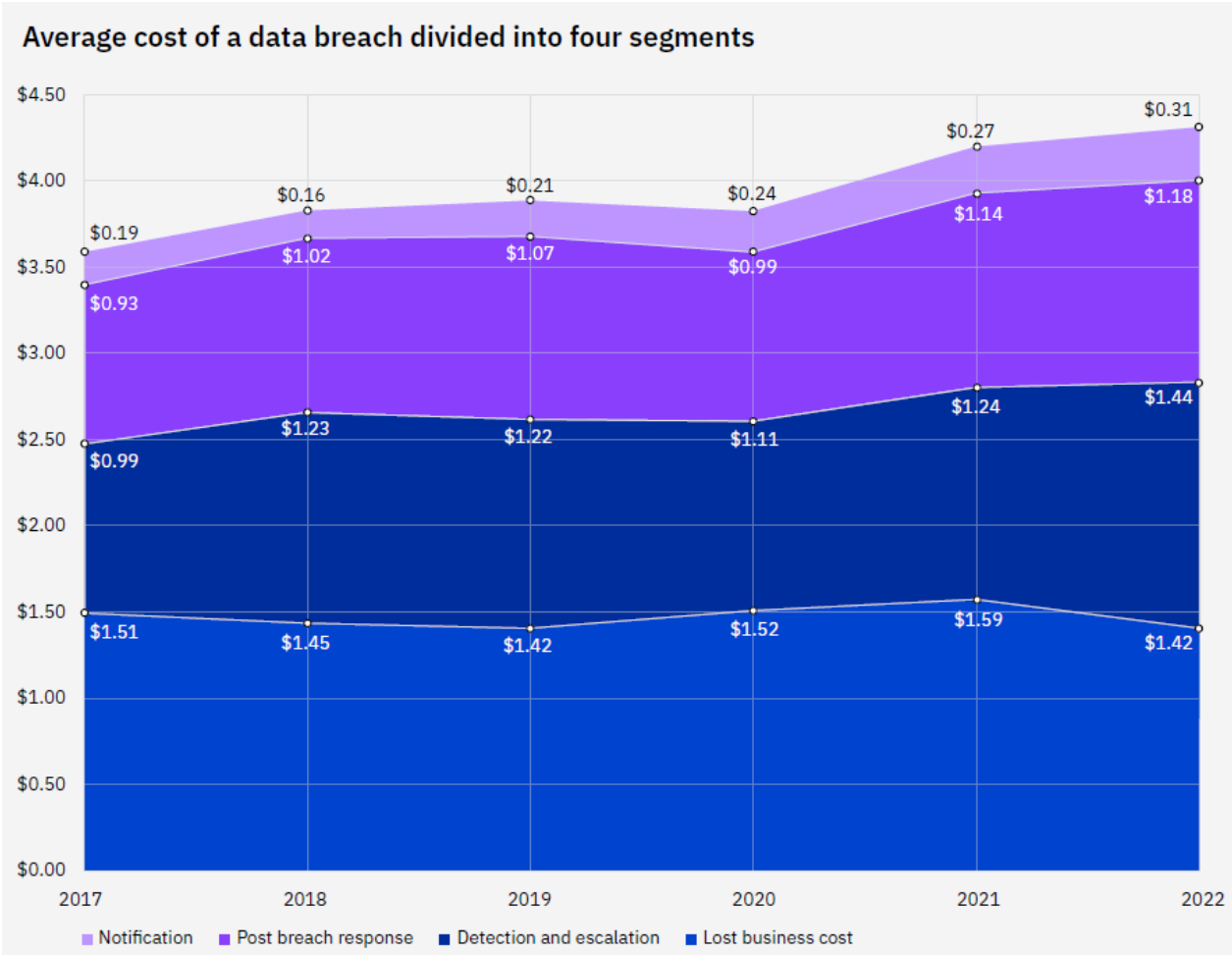
Breach by Industry



Cost of a breach



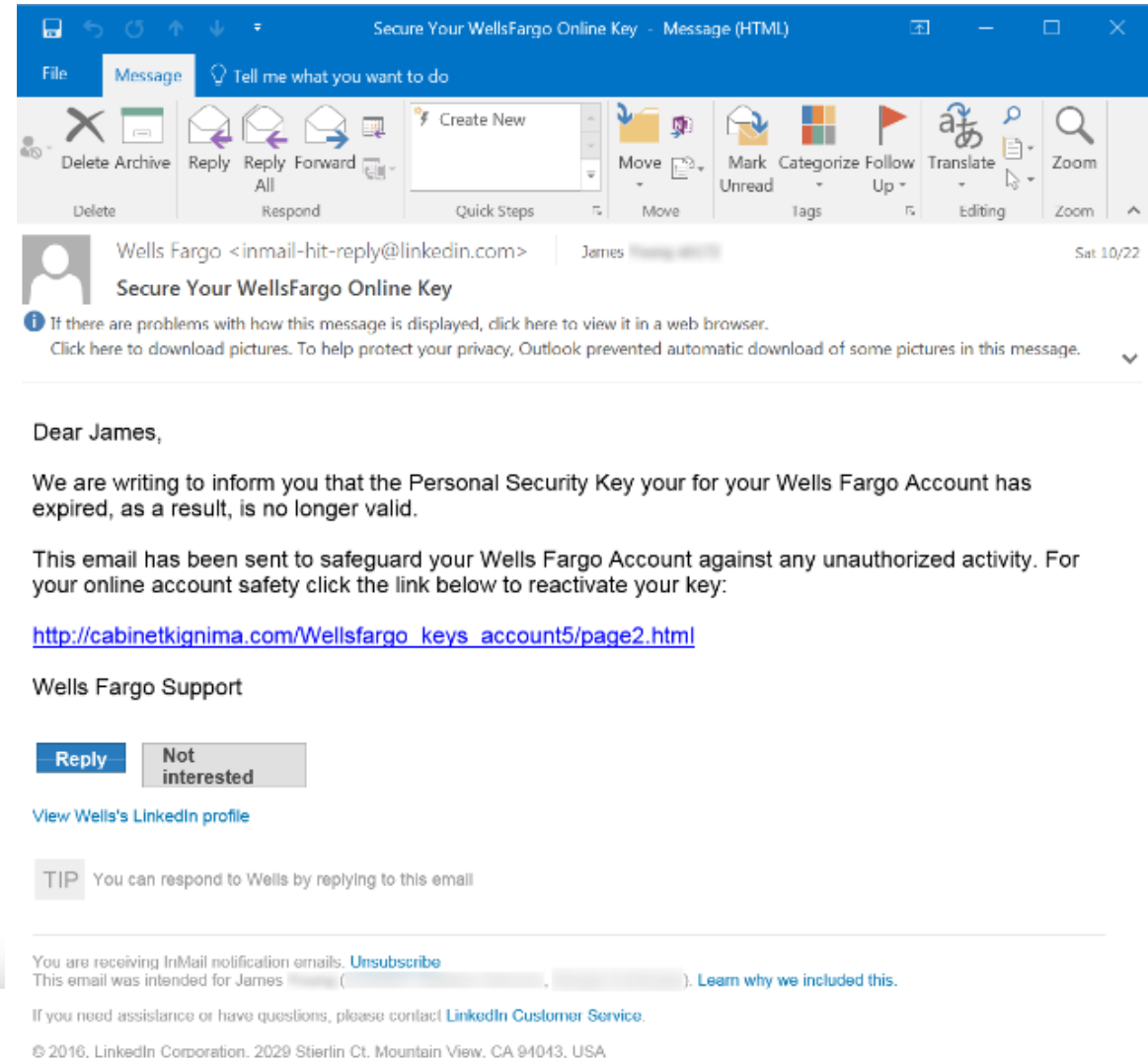
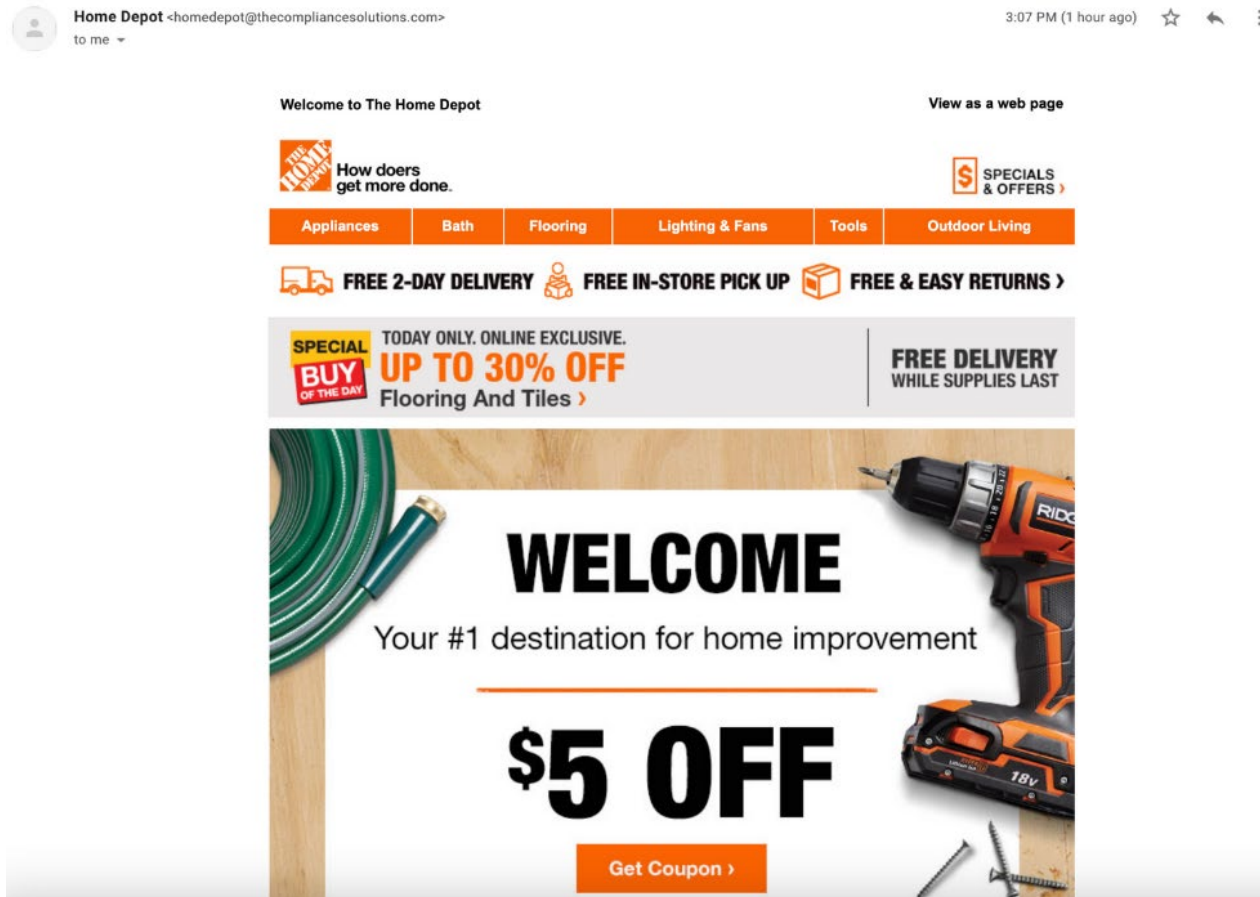
Cost per task



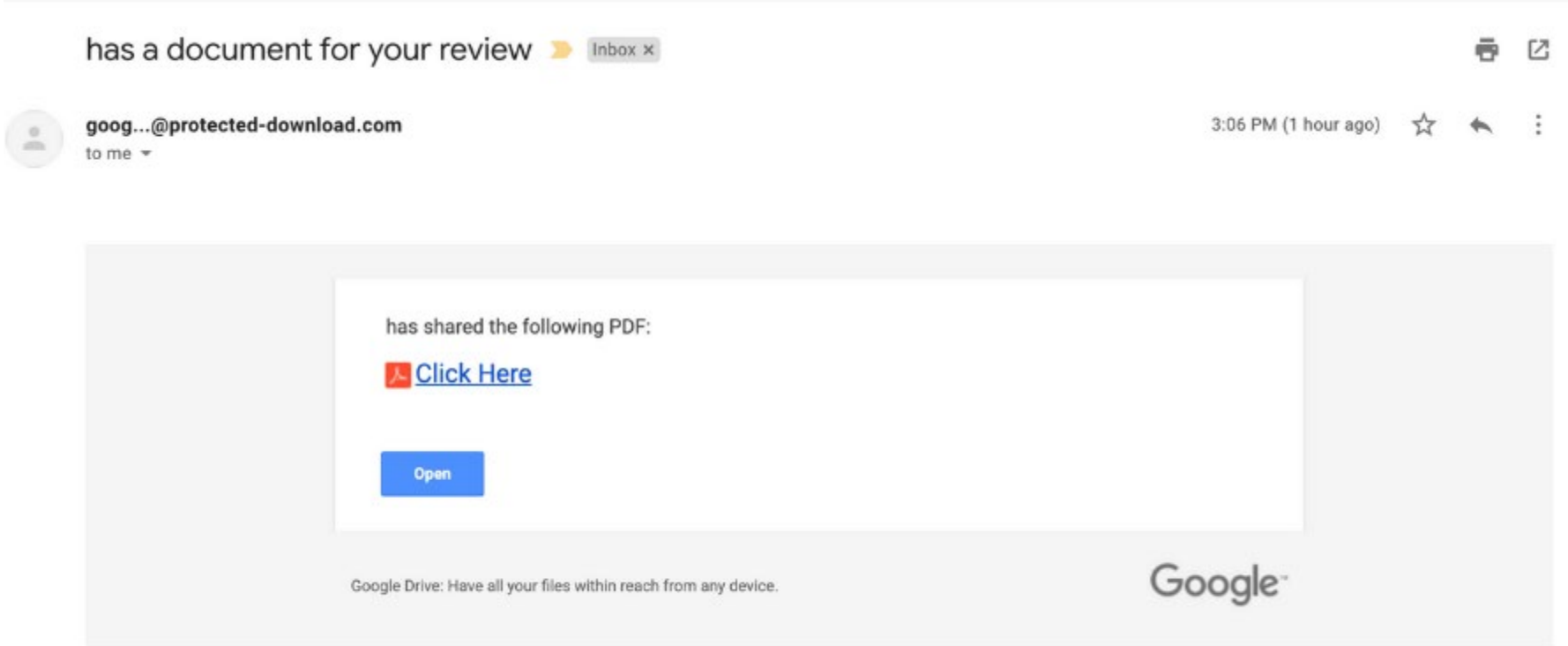
Phishing Examples



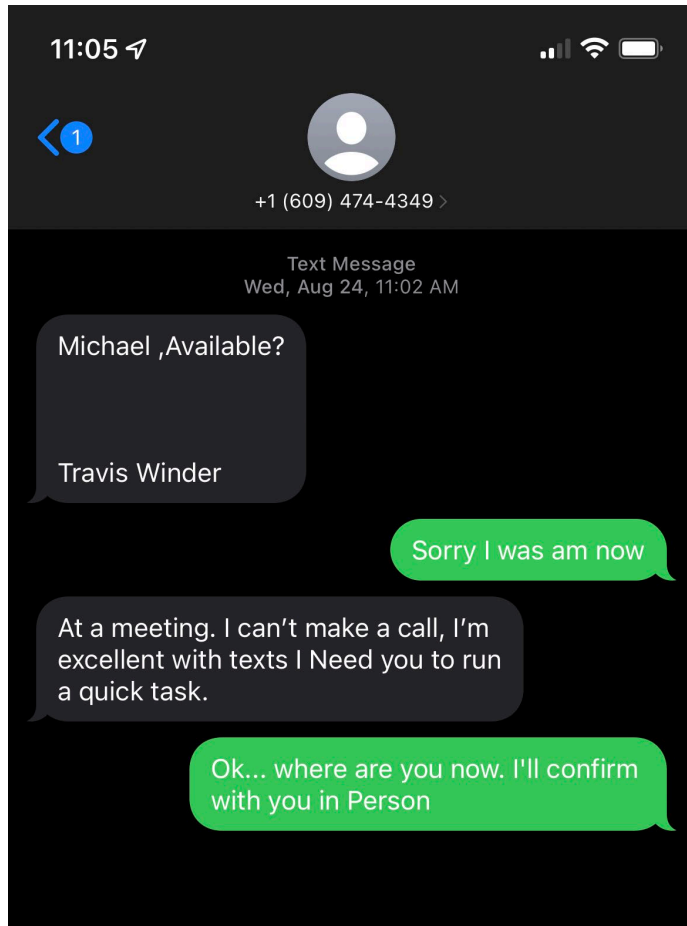
Phishing Email Example



Phishing Email Example



Phishing Example



NETFLIX

Reset your password

Hi {fname},

Let's reset your password so you can get back to watching.

RESET PASSWORD

If you did not ask to reset your password, [click here](#) to login and reset your password **immediately** to avoid unauthorized activity on your account.

Best Practices

Define the Program

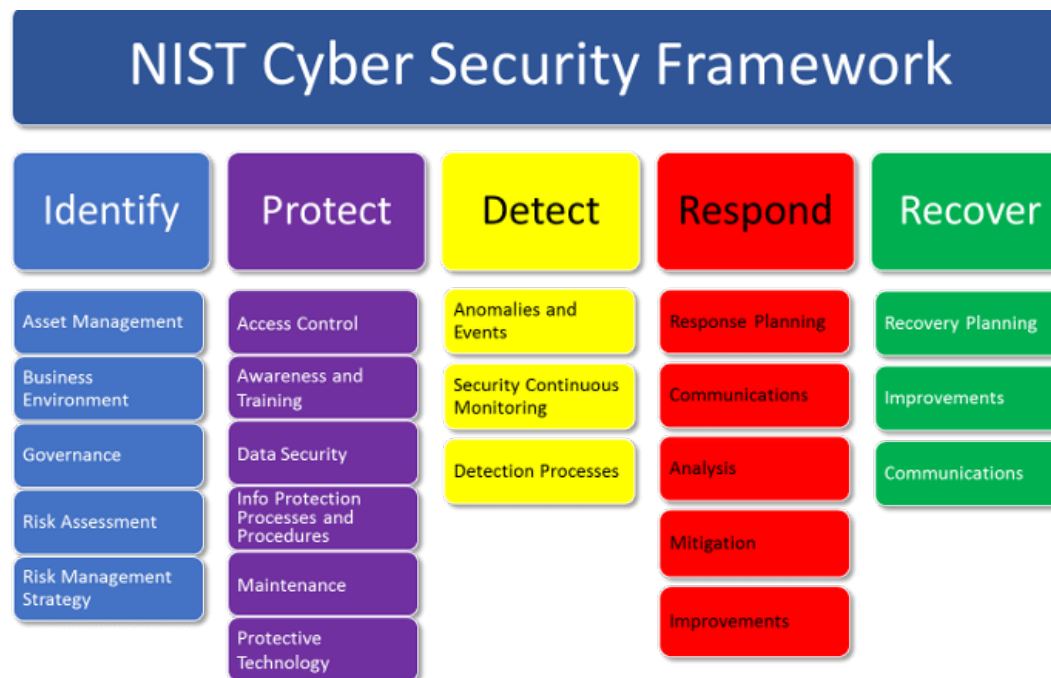
- Formalize and Document Cybersecurity Program
- Policies and Procedures
 - Acceptable Use Policy
 - Security Policy and Plan
 - Risk Management Policies and Procedures
- Leadership Buy In
- Security Steering Committee made up of Business Leaders
- Define Security Roles and Responsibilities

Get Visibility

- You need to know what you have in order to protect it
- Document Hardware and Software
 - CMDB
 - Spiceworks & ManageEngine
- Scan and Document Vulnerabilities
- Remediate and Patch Consistently

Assess

- Conduct a Maturity and Risk Self Assessment periodically
 - <https://github.com/brianwifaney/NIST-CSF>
- Utilize a 3rd Party to assess your Risk and Maturity Annually

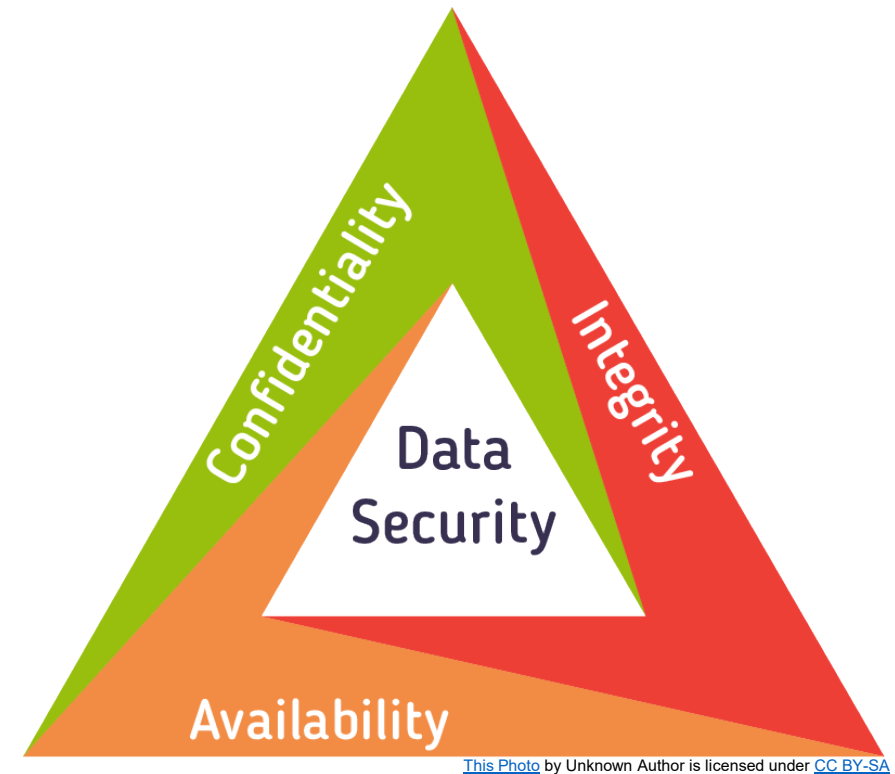


Focus on Resiliency

- Disaster Recover
- Business Continuity
- Incident Response
- “Failing to Plan is Planning to Fail”
- Perform Table Top exercises

Data Security

- Data in Transit
- Data at Rest
- Data in Use
- Data Destruction
- CIA Triad



Choose the Right Technology

- Endpoint Security/Anti-Virus
- Endpoint Detection and Response (EDR)
- Firewalls
- Logging/SIEM
- Identity and Access Management Solutions
- Vulnerability Management
- Asset Management

Access Control & Identity Management

- Principal of Least Privilege
 - Internal Users
 - Contractors
 - 3rd Parties
- Onboarding and Offboarding Policies and Procedures
- Multifactor Authentication is a Requirement
- Password management tools
 - LastPass
 - 1Password
 - Dashlane
- <https://www.security.org/how-secure-is-my-password/>
- <https://haveibeenpwned.com/>
- <https://haveibeenpwned.com/Passwords>

Password Complexity Requirements

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Educate | Train | Learn

- Utilize Automated Security Awareness Training
- Educate and Market Security within the organization
 - Dialogue with organization to answer questions
- Validate the effectiveness of your training through phishing simulations
- Tools:
 - KnowBe4 -
 - <https://www.knowbe4.com/free-it-security-tools>
 - <https://www.phishing.org/>
 - Microsoft (Included in some licensing)

Cheat Sheet Links

- Utilize the resources available to you below
- <https://staysafeonline.org/>
 - October is Cybersecurity Awareness Month - <https://staysafeonline.org/programs/cybersecurity-awareness-month/>
- <https://www.ic3.gov/>
- <https://www.cisa.gov/uscert>
- <https://www.nist.gov/cyberframework>
- <https://www.cisecurity.org/controls/v8>
- <https://www.sans.org/information-security-policy/>

Key Take Aways

- Cyberattacks are on the rise and the risk of a data breach is ever increasing
- Focus on Maturing your Cybersecurity Program through strategic planning and implementation of the right security controls
- Stay vigilant for social engineering attacks
- Cybersecurity is a Journey, Not a destination

Michael Nougquier

Chief Information Security Officer & Director of Cybersecurity Services

D 720.673.9338 | **T** 303.721.6131 | **C** 303.641.7295

E mnougquier@richeymay.com | www.richeymay.com

[9780 S. Meridian Blvd., Suite 500 | Englewood, CO 80112](#)

<https://richeymay.com/technology/>