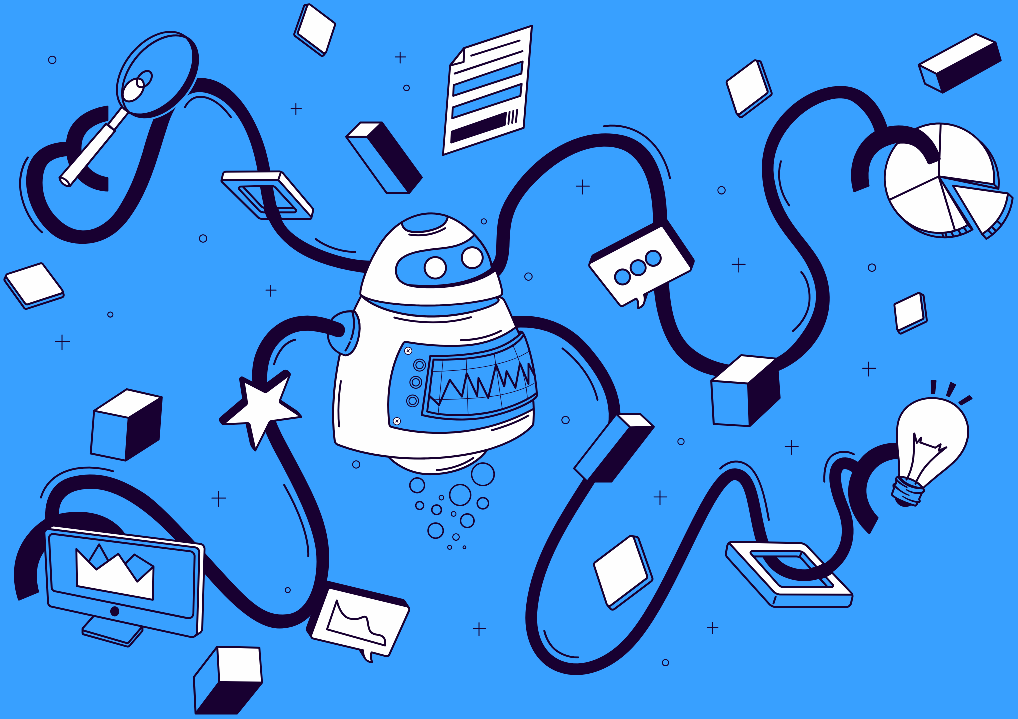
To the Right of Boom: What happens after a Cyber-Security Incident Occurs

Marissa Maldonado
CEO of Proda Technology

UC 2023

PCC
Pediatric EHR Solutions

Session Goals



01
What is NIST Cybersecurity Framework and Cybersecurity Defense Matrix?

02
4 Major Actions BEFORE & AFTER a security incident

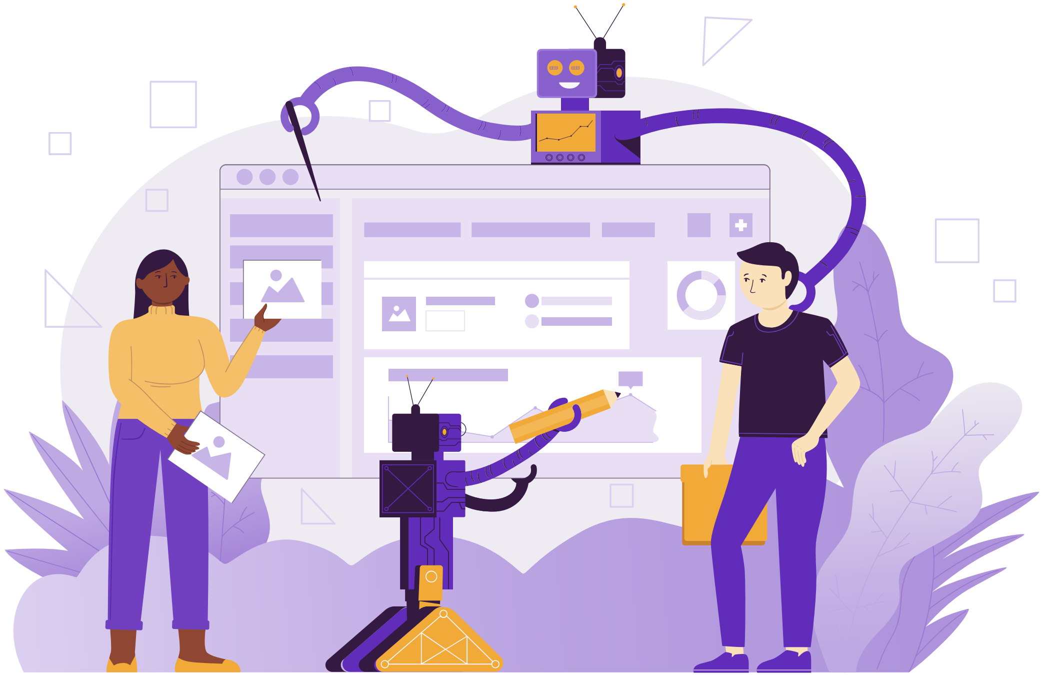
03
Deeper understanding of Cyber Security Insurance and why it matters

Humanizing IT

UC 2023

PCC
Pediatric EHR Solutions

The NIST Cybersecurity Framework



The US National Institute of Standards and Technology (NIST) was created in 1901! Mission is to promote American innovation and industrial competitiveness.

Executive order 13636 in 2013 was signed, titled Improving Critical Infrastructure Cybersecurity. One year later the NIST Cybersecurity Framework was released as a result.

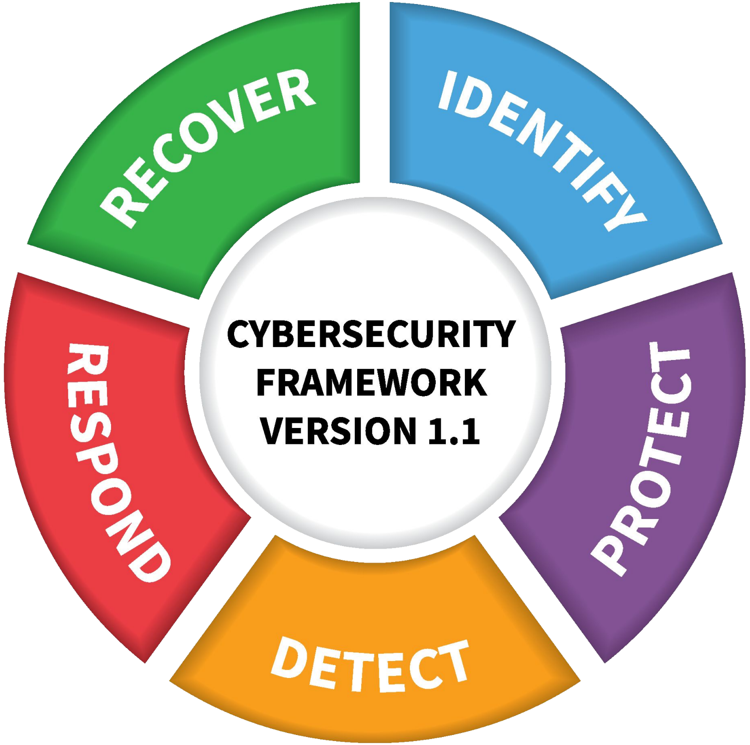
Today the NIST Cybersecurity Framework is the most popular cybersecurity framework across multiple industries. (HIPAA, HHS)

NIST Framework

- A common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders

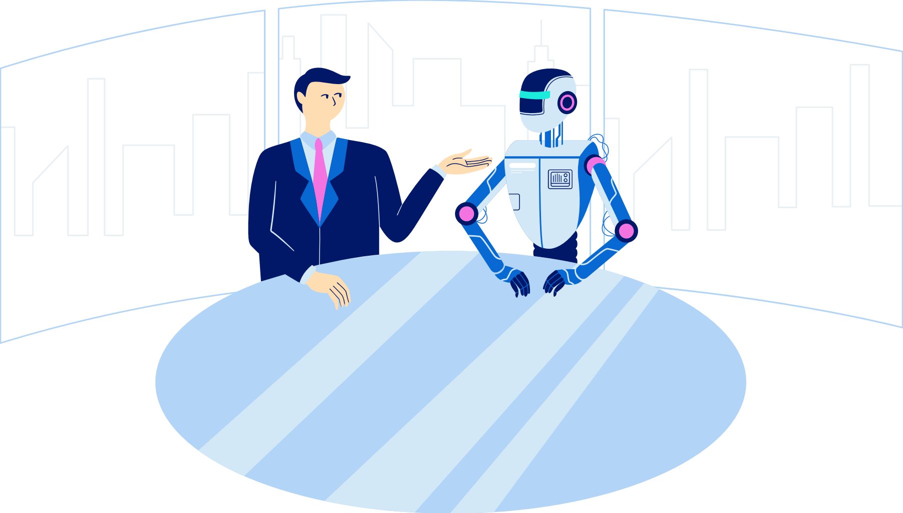
- Helps identify and prioritize actions for reducing cybersecurity risk

- A took for aligning policy, business, and technological approaches to managing risk



IDENTIFY (IT Assets and Network Activity)

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities



A

Foundation

Clear understanding the business context, the resources that support critical

B

Asset Management

A clear and precise understanding on where and what your assets are

C

Governance & Risk Assessments

Formal Committee with guidelines for how to make decisions

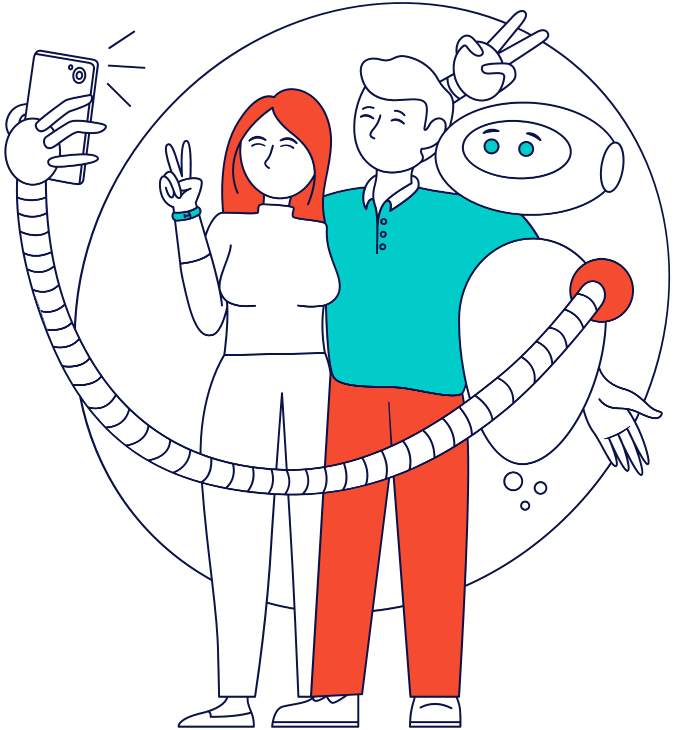
PROTECT (Defense Against Threats)

Develop and implement appropriate safeguards to ensure delivery of critical services

Limit or contain the impact of a potential cybersecurity event

Identity Management and Access Control, Awareness and Training, Data Security

Information Protection Processes and Procedures, Maintenance and Protective Technology



We are to the Left of Boom!

What are four key action items you need to take for your practice in order to IDENTIFY & PROTECT your data?

Identify Ideas:

- Vulnerability Scanning
- Annual Risk Review
- Improve (or automate) Asset Discovery
- Improve Documentation
- Darkweb Scanning

Protect Ideas:

- Computer patching
- Asset Lifecycle Management
- Security tools: AV, Endpoint DNS Filtering
- Spam Filtering & Email Security
- Single Sign On and/or a Password Management Tool
- SIEM with a 7x24 SOC (Security Operation Center)
- Phishing Simulation
- Security Awareness Training

Now we move to the Right of Boom!

Assume
Breach

Identify → Protect → Detect → Respond → Recover

To Right of Black Line, A Security Incident Has Occured

What is an Incident?!

EVENT

Any observable occurrence in a system or network

Security Incident (privacy incident)

An event that violates an organization’s security or privacy policies involving sensitive information

(Assume) Breach

Security or privacy incident that meets specific legal definitions as per state and federal breach laws. Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies and the media. Only a small percentage of privacy or security incidents escalate into data breaches but to identify them there’s a regulatory obligation to conduct an incident risk assessment.

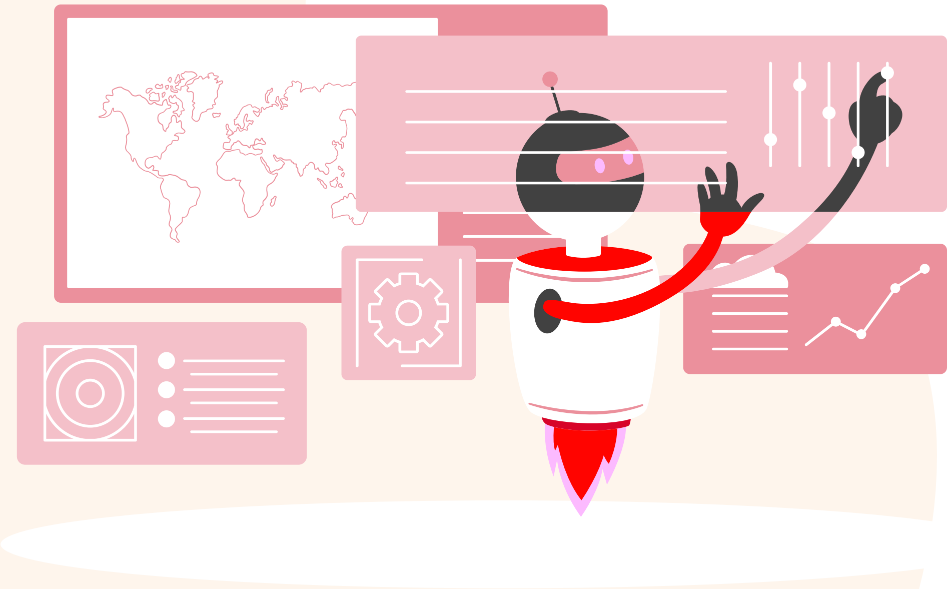
DETECT (Security Incident)

Develop and Implement appropriate activities to identify the occurrence of a cybersecurity event

- Enabling timely discovery of cybersecurity events
- Being able to detect anomalies and events
- Security Continuous Monitoring and Detection Processes

RESPOND (Security Incident Response)

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.



Supports ability to contain the impact of a potential cybersecurity incident.

PCC
Pediatric EHR Solutions

RECOVER (Restore after Incident)

Develop and implement activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident

Timely Recovery to Normalcy

Reduce Impact from a Cybersecurity Incident

Recovery Planning and Improvements

PR & Communications

Right of Boom

What are four key action items you need to take for your practice in order to DETECT, RESPOND & RECOVER your data?

DETECT Ideas

- Ransomware Protection
- 24x7 Security Operations Center
- Domain DNS Protection
- Network Management
- The items you have for PROTECT should also

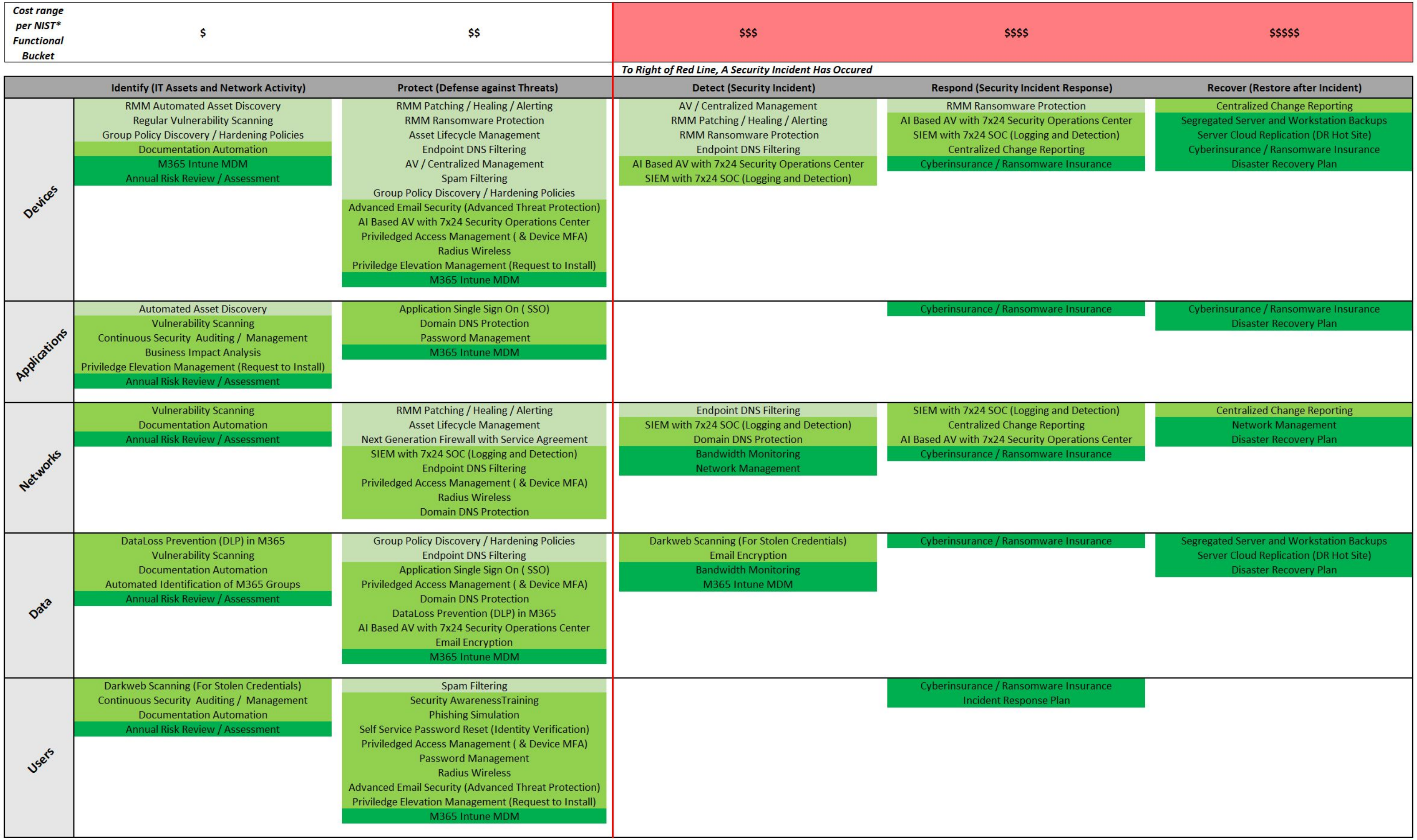
RESPOND Ideas

- Cybersecurity Insurance and Ransomware Insurance
- Clear and rehearsed Incident Response Plan

RECOVER Ideas

- Segregated Server and Workstation Backups
- Clear and rehearsed Disaster Recovery Plan

Cybersecurity Defense Matrix



Cost range per NIST Functional Bucket*	$	$$	$$$	$$$$	$$$$$
			To Right of Red Line, A Security Incident Has Occured		
	Identify (IT Assets and Network Activity)	**Protect (Defense against Threats)**	**Detect (Security Incident)**	**Respond (Security Incident Response)**	**Recover (Restore after Incident)**
Devices	RMM Automated Asset Discovery Regular Vulnerability Scanning Group Policy Discovery / Hardening Policies Documentation Automation M365 Intune MDM Annual Risk Review / Assessment	RMM Patching / Healing / Alerting RMM Ransomware Protection Asset Lifecycle Management Endpoint DNS Filtering AV / Centralized Management Spam Filtering Group Policy Discovery / Hardening Policies Advanced Email Security (Advanced Threat Protection) AI Based AV with 7x24 Security Operations Center Priviledged Access Management (& Device MFA) Radius Wireless Priviledge Elevation Management (Request to Install) M365 Intune MDM	AV / Centralized Management RMM Patching / Healing / Alerting RMM Ransomware Protection Endpoint DNS Filtering AI Based AV with 7x24 Security Operations Center SIEM with 7x24 SOC (Logging and Detection)	RMM Ransomware Protection AI Based AV with 7x24 Security Operations Center SIEM with 7x24 SOC (Logging and Detection) Centralized Change Reporting Cyberinsurance / Ransomware Insurance	Centralized Change Reporting Segregated Server and Workstation Backups Server Cloud Replication (DR Hot Site) Cyberinsurance / Ransomware Insurance Disaster Recovery Plan
Applications	Automated Asset Discovery Vulnerability Scanning Continuous Security Auditing / Management Business Impact Analysis Priviledge Elevation Management (Request to Install) Annual Risk Review / Assessment	Application Single Sign On (SSO) Domain DNS Protection Password Management M365 Intune MDM		Cyberinsurance / Ransomware Insurance	Cyberinsurance / Ransomware Insurance Disaster Recovery Plan
Networks	Vulnerability Scanning Documentation Automation Annual Risk Review / Assessment	RMM Patching / Healing / Alerting Asset Lifecycle Management Next Generation Firewall with Service Agreement SIEM with 7x24 SOC (Logging and Detection) Endpoint DNS Filtering Priviledged Access Management (& Device MFA) Radius Wireless Domain DNS Protection	Endpoint DNS Filtering SIEM with 7x24 SOC (Logging and Detection) Domain DNS Protection Bandwidth Monitoring Network Management	SIEM with 7x24 SOC (Logging and Detection) Centralized Change Reporting AI Based AV with 7x24 Security Operations Center Cyberinsurance / Ransomware Insurance	Centralized Change Reporting Network Management Disaster Recovery Plan
Data	DataLoss Prevention (DLP) in M365 Vulnerability Scanning Documentation Automation Automated Identification of M365 Groups Annual Risk Review / Assessment	Group Policy Discovery / Hardening Policies Endpoint DNS Filtering Application Single Sign On (SSO) Priviledged Access Management (& Device MFA) Domain DNS Protection DataLoss Prevention (DLP) in M365 AI Based AV with 7x24 Security Operations Center Email Encryption M365 Intune MDM	Darkweb Scanning (For Stolen Credentials) Email Encryption Bandwidth Monitoring M365 Intune MDM	Cyberinsurance / Ransomware Insurance	Segregated Server and Workstation Backups Server Cloud Replication (DR Hot Site) Disaster Recovery Plan
Users	Darkweb Scanning (For Stolen Credentials) Continuous Security Auditing / Management Documentation Automation Annual Risk Review / Assessment	Spam Filtering Security AwarenessTraining Phishing Simulation Self Service Password Reset (Identity Verification) Priviledged Access Management (& Device MFA) Password Management Radius Wireless Advanced Email Security (Advanced Threat Protection) Priviledge Elevation Management (Request to Install) M365 Intune MDM		Cyberinsurance / Ransomware Insurance Incident Response Plan	

CYBERSECURITY INSURANCE

What is it?

- It's Comprehensive
- It includes coverage for IR
- It includes critical crime coverages. (e.g. Ransomware)
- It's NOT compliance focused
- It's not attached to other lines of coverage (endorsements)

What's Included

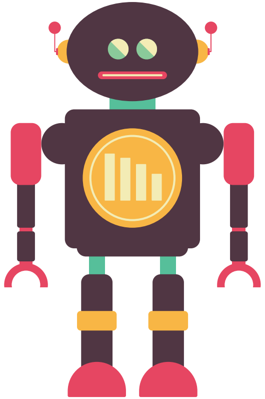
- Foresnsics
- Data Restoration
- Credit Monitoring
- Fraud Response
- Legal
- Privacy Regulations
- PR Expenses

Complicated?

A

2015 - 2018

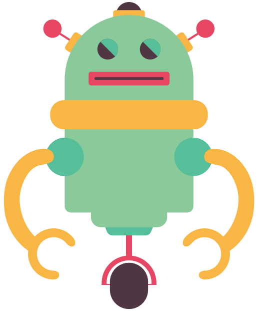
- Cyber insurance was low cost with very little underwriting.
- Adoption was low (around 10%) but the process was very simple and easy



B

2019

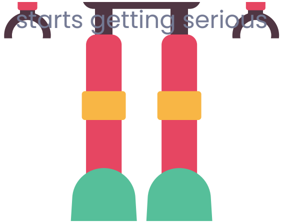
- Claims started rising significantly!
- Awareness and defenses are still low.
- Ransomware was hot on the scene - carriers were NOT prepared



C

2020

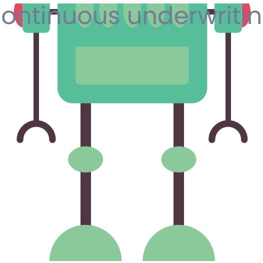
- Incidents still rising, and the pandemic forced work from home shift.
- Demand for cyber insurance skyrocketed and carriers are losing money rapidly.
- Underwriting actually starts getting serious



D

2023

- Incident volume is slowing down (partially due to conflict in Ukraine)
- More minimum standards required for cybersecurity controls
- New focus on continuous underwriting



How do I make sure I can

A) Get Cybersecurity Insurance and

B) Not have a claim denied?

NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Continuous Security Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Info Protection/ Processes/Procedures		Mitigation	**Cyber Insurance**
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology		**Cyber Insurance**	

Do you see a theme here? It all points back to the NIST Cybersecurity Framework. It just gets dressed differently….

Your Cybersecurity Framework Roadmap!

Immediate (0-6 Months)

Start an internal Governance Committee

Create an Incident Response Plan

Discuss with your IT on if you have proper controls for monitoring (and logging)

Short Term (3 – 12 Months)

Test Incident Response Plan

Run Tabletops

Audit It Monitoring Tools

Plan IT Budget

Long Term (12 Months +)

Risk Assessments and Management

Upgrades for IT Controls (based on IT Budget)

Run Security Assessment

Excellent FREE Resource for Health Industry Cybersecurity Practices

Knowledge on Demand

Cybersecurity Education Platform that includes multiple delivery methodologies to reach varied size health care facilities across the country!

https://405d.hhs.gov/knowledgeondemand

Health Industry Cybersecurity Practices (HICP) 2023 Edition

A foundational publication that aims to raise awareness of cybersecurity risks, provide best practices, and help the HPH Sector set standards in mitigating the most pertinent cybersecurity threats to the sector.

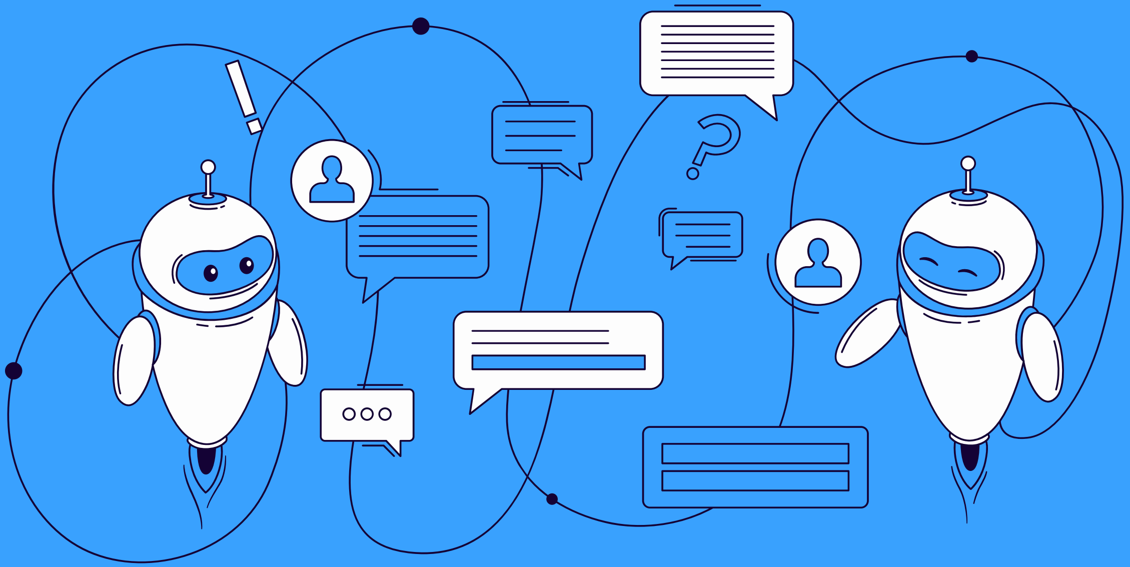
https://405d.hhs.gov/information

Session Takeaways

The NIST Framework is at the center of most all Cybersecurity concepts

“Assume Breach” and develop a Cybersecurity Roadmap from this philosophy

Take advantage of the free resources HHS has published: https://405d.hhs.gov



References

NIST Framework: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)

Health Industry Cybersecurity Practices: 405(d) :: Cornerstone Publications (hhs.gov)

What Questions Do You Have?

Later Viewing

This and all other UC2023 course recordings will be available for later viewing through the app.