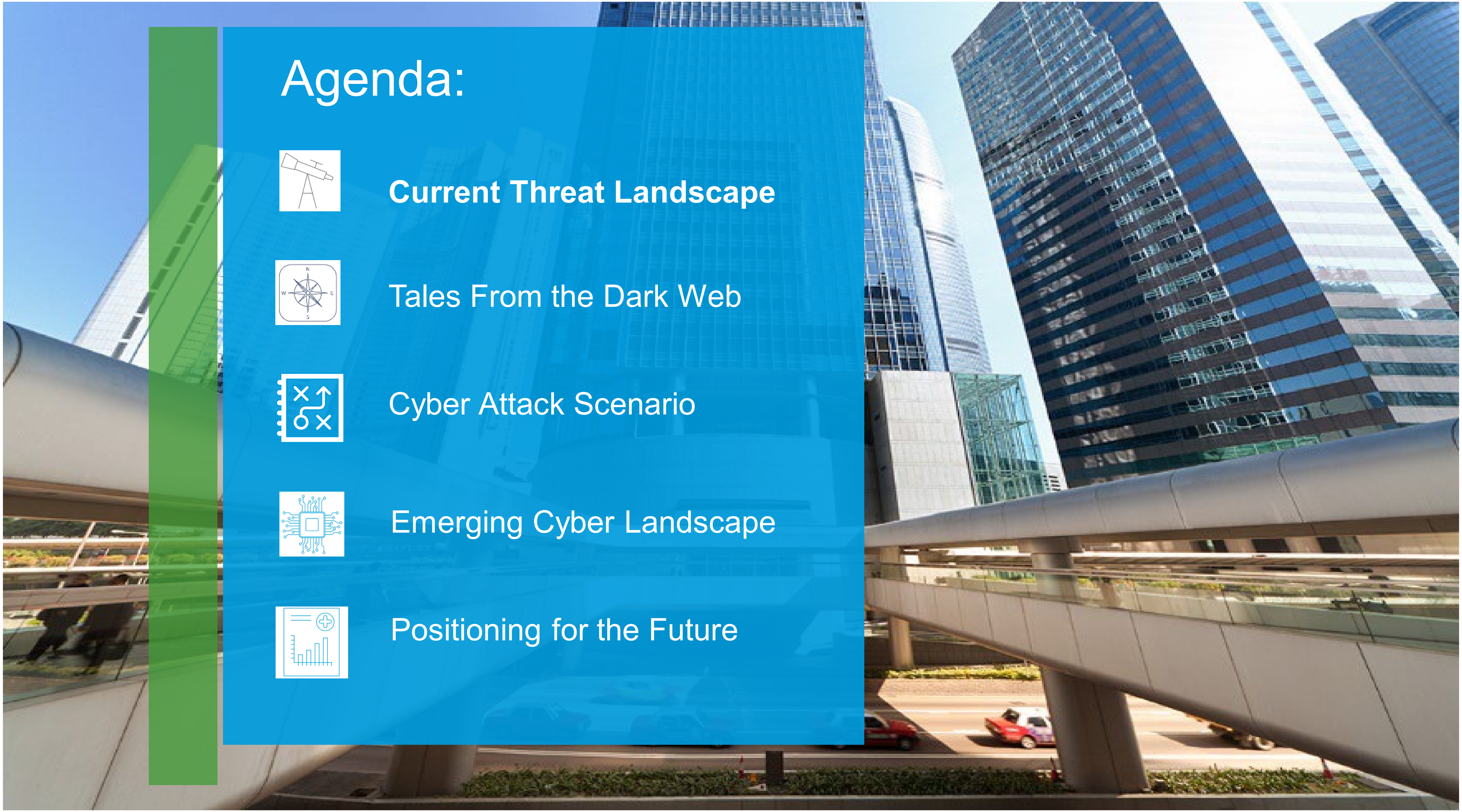
INTO THE DARK

Exploring Vulnerabilities, the Dark Web and Data Breaches in Healthcare

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING



Agenda:

- **Current Threat Landscape**
- Tales From the Dark Web
- Cyber Attack Scenario
- Emerging Cyber Landscape
- Positioning for the Future

Learning objectives

1. By the end of this course, you will be able to:
2. Identify current trends and themes in data breaches and dark web activity within the healthcare industry.
3. Learn how to effectively mitigate the risks associated with the dark web and data breaches Understand how to ensure your organization meets all necessary requirements to maintain compliance with health care data requirements

Current Threat Landscape

Cyber Trends

Top Five Threats for 2022 - 2023 :

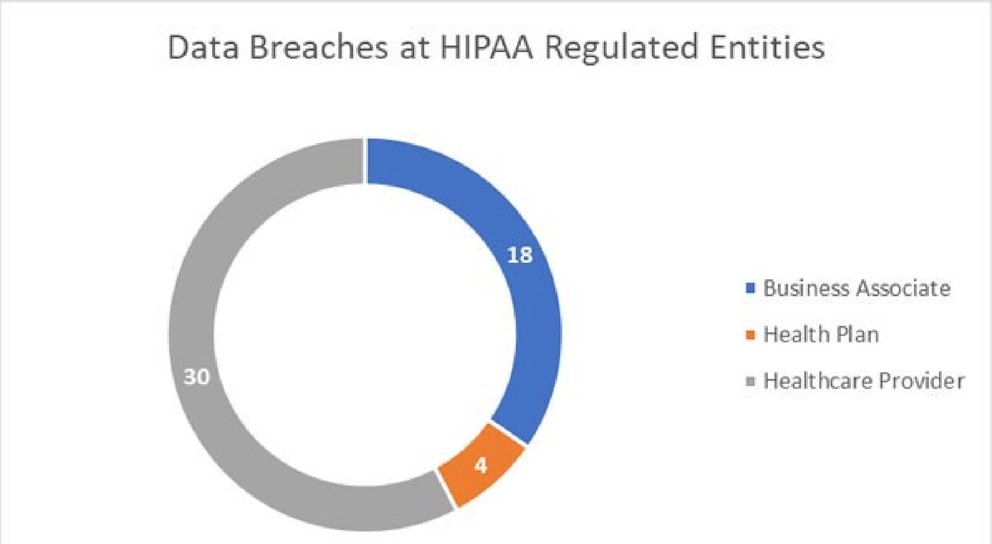
- 1. Ransomware Deployment
- 2. Phishing/Spear-Phishing Attacks
- 3. Third-Party/Partner Breach
- 4. Data Breach
- 5. Social Engineering

- 98% of attacks can be prevented with basic Security Hygiene

Attack Timeline - 102 min is the median time for an attacker to start lateral movement.
At 72 min they have access to your private data.

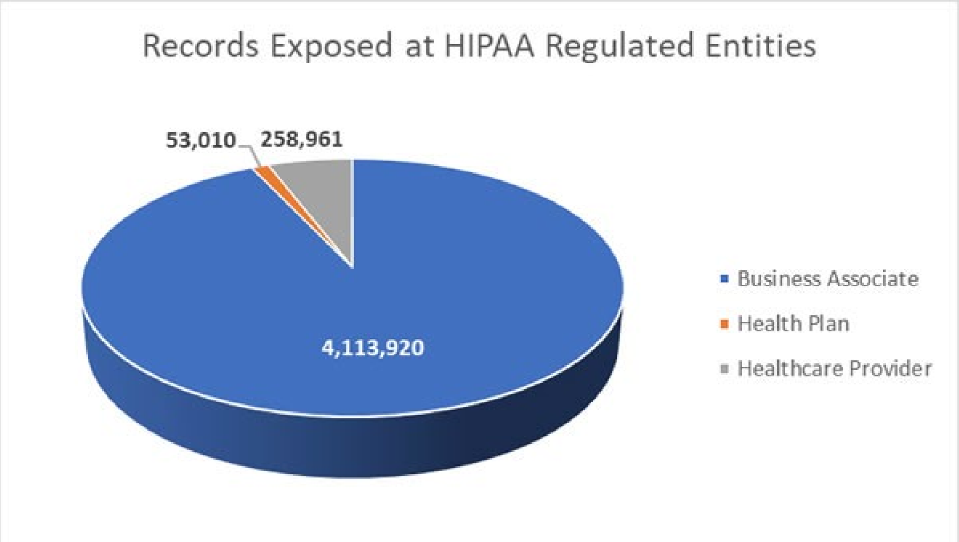
* Phishing shows exponential growth with Vishing and other forms increasing rapidly.
* Issues with privileged access control deficiencies resulted in Password attack increases from 74-93% YoY
* Unmanaged devices are 71% more likely to have malware.
* 84% of organizations who suffered from ransomware had no integrated security approach with on-prem solutions.

Healthcare Cyber Defense Trends of 2023

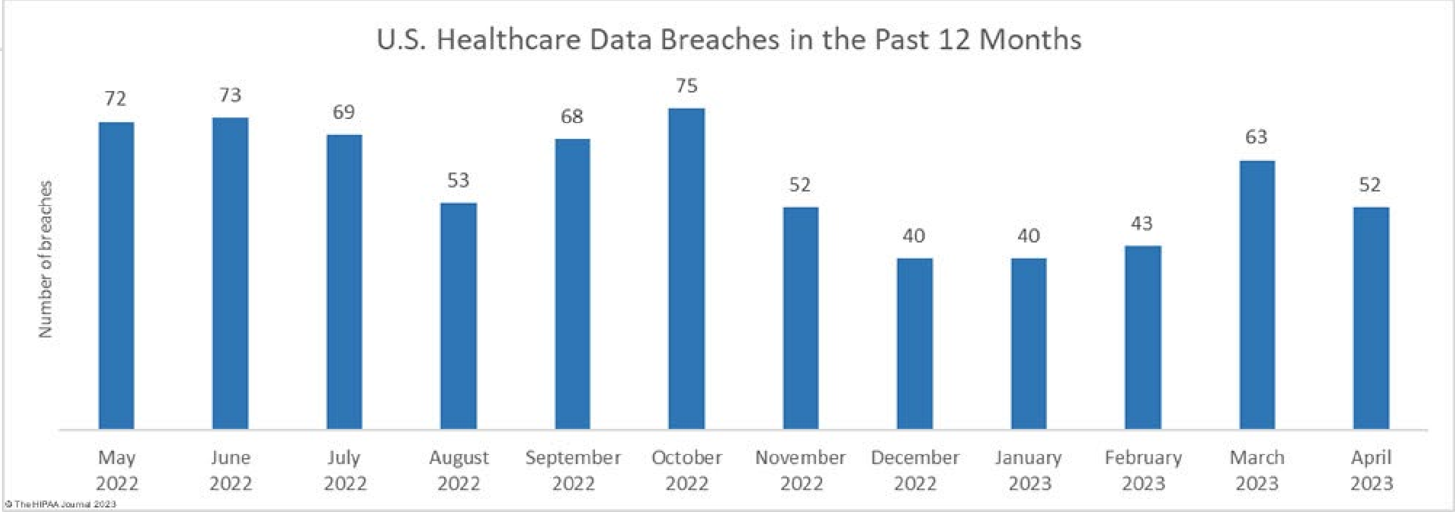


Data Breaches at HIPAA Regulated Entities

© The HIPAA Journal 2023



Records Exposed at HIPAA Regulated Entities

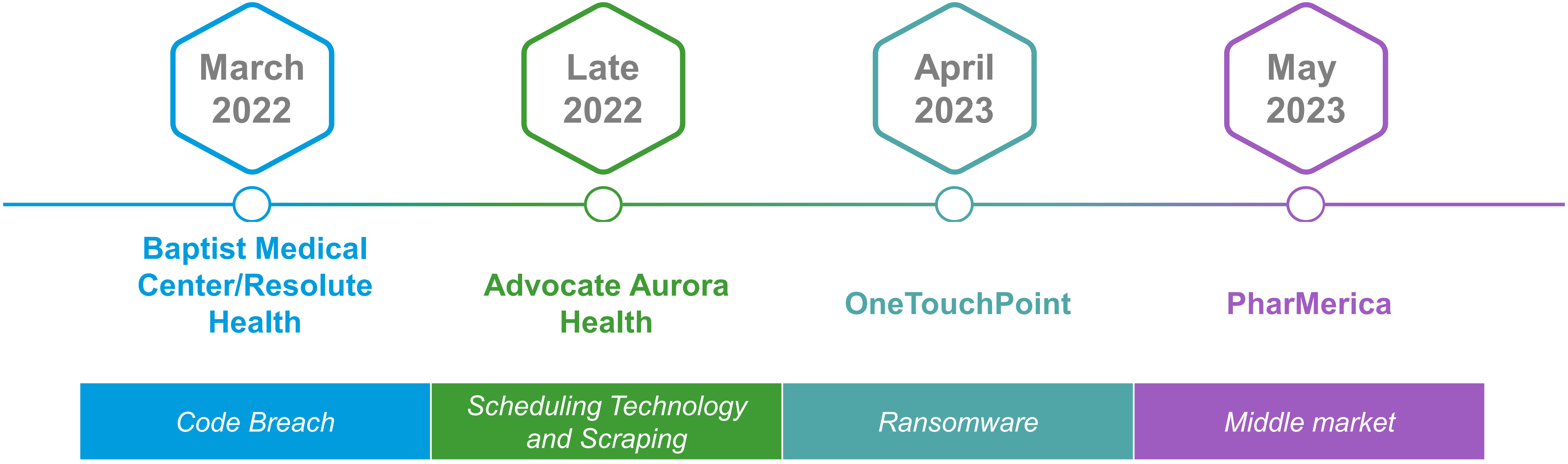


U.S. Healthcare Data Breaches in the Past 12 Months

© The HIPAA Journal 2023

Recent cyber attacks from the headlines

*According to a recent Reuters report, medical information is worth about 10 times more than credit card numbers on the black market.



March 2022	Late 2022	April 2023	May 2023
Baptist Medical Center/Resolute Health	**Advocate Aurora Health**	**OneTouchPoint**	**PharMerica**
Code Breach	*Scheduling Technology and Scraping*	*Ransomware*	*Middle market*
Theft of demographic details, SSNs, insurance data, diagnoses, treatments, reason for visit, claims data	Patient health information shared with Google and Facebook as a result of its use of Pixel	Printing and Mailing vendor disclosed patient names, member IDs, and information gathered from health assessments.	Data breach exposed personal data pertaining to 5.8 million individuals

2022 cyber attacks by the numbers

Frequency of malware

More than [1]

450,000

new malware programs are detected daily

Est. cost of cyber crime (globally)

$8 Trillion

up from $6 trillion in 2021 [2]

- 24 T by 2027
- 20 Year War on Terror was ~8T
- A trillion dollar bills, laid end to end, would stretch 96,906,656 miles

Open-source code vulnerability

84%

Of open-source code contained at least one vulnerability [3]

Avg. cost of data breaches in the US

Data breaches in the US

Cost Twice

the amount for global breaches $9.45M vs $4.35M [4]

Supply chain attacks in 2022 surpassed malware attacks by 40% impacting more than 10M individuals and leading to over 1,700 data breaches in the US

Key trends in the cybersecurity landscape

According to RSM’s 2023 Middle Market Business Index (MMBI) cybersecurity report:

- **Breaches are slightly down, but significant cybersecurity concerns persist**: 20% of middle market executives claimed their company experienced a data breach last year.
- **However, executives are still worried:** 68% anticipate that unauthorized users will attempt to access data or systems this year.
- **Technology is changing**: 50% of organizations have moved to the cloud in the past year due to security concerns, up from 36% last year.
- **So is cyber liability coverage:** 68% of companies carry a cyber insurance policy, and 70% say premium costs have increased.

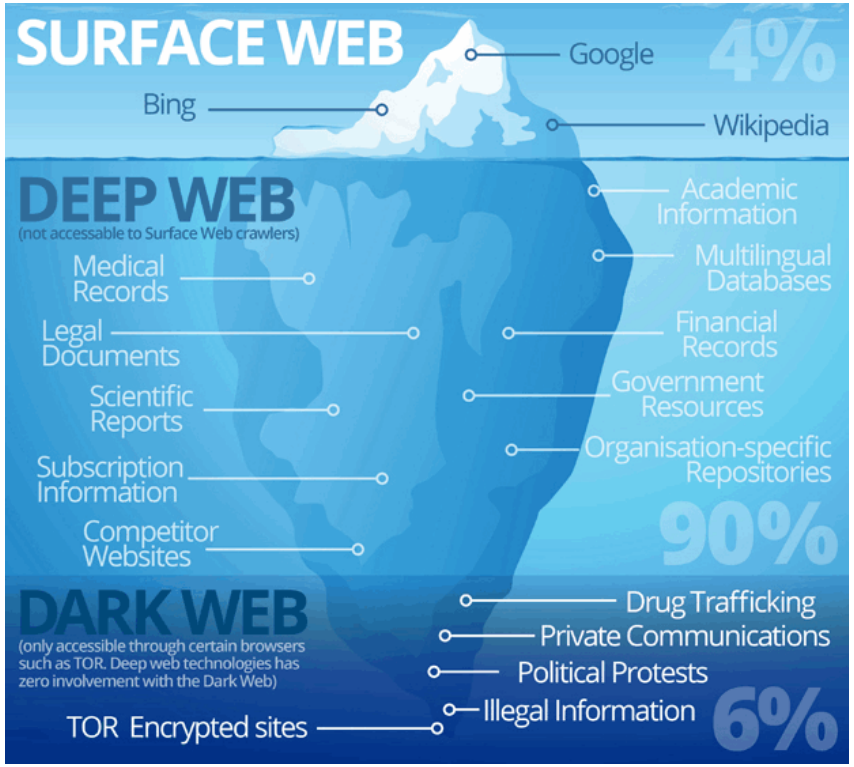
63%

of executives feel they are at risk for a ransomware attack in 2023.

Tales from the Dark Web

What is the *dark* and *deep* web?

- **Surface web (1% to 4%)** – able to be indexed by search engines
- **Deep web (96% to 99%)** – cannot be indexed by search engines
  - Sources behind login pages and paywalls
  - Intentionally non-indexed sources (https://www.grants.gov/)
- **Dark web** – subjective grouping of small subsection of deep web utilized for nefarious/unregulated purposes
  - Commonly associated with Tor browser



(*Image source:* What is the Dark Web? | The SSL Store)

The importance of Cyber Threat Intelligence (CTI)

CTI's objective is to generate timely and actionable intelligence about existing or emerging threats through collection and analysis of open and closed sources. Closed sources include the dark web and underground forums.

How does CTI provide value to a threat actor?

- Identify targets of interest (ToIs)
- Craft unique social engineering attacks
- Discover unintentional leakage of sensitive data to leverage for exploitation
- Identify and exploit vulnerabilities related to misconfigured protocols and enumerated software
- Map out network devices and architecture
- Purchase exposed credentials or previously exfiltrated data

How does CTI provide value to internal security?

- Identify instances of potential liability for an entity:
  - **Organizations**: misconfigured protocols, deprecated software, vulnerable ports, technical information leakages, etc.
  - **People**: exposed sensitive data, unnecessary information leakage, reputational liabilities, etc.
- Understand the visible attack surface of an entity
- Receive proactive intelligence regarding threat actors, attack vectors, vulnerabilities, etc.
- Identify data breaches as part of the incident response process

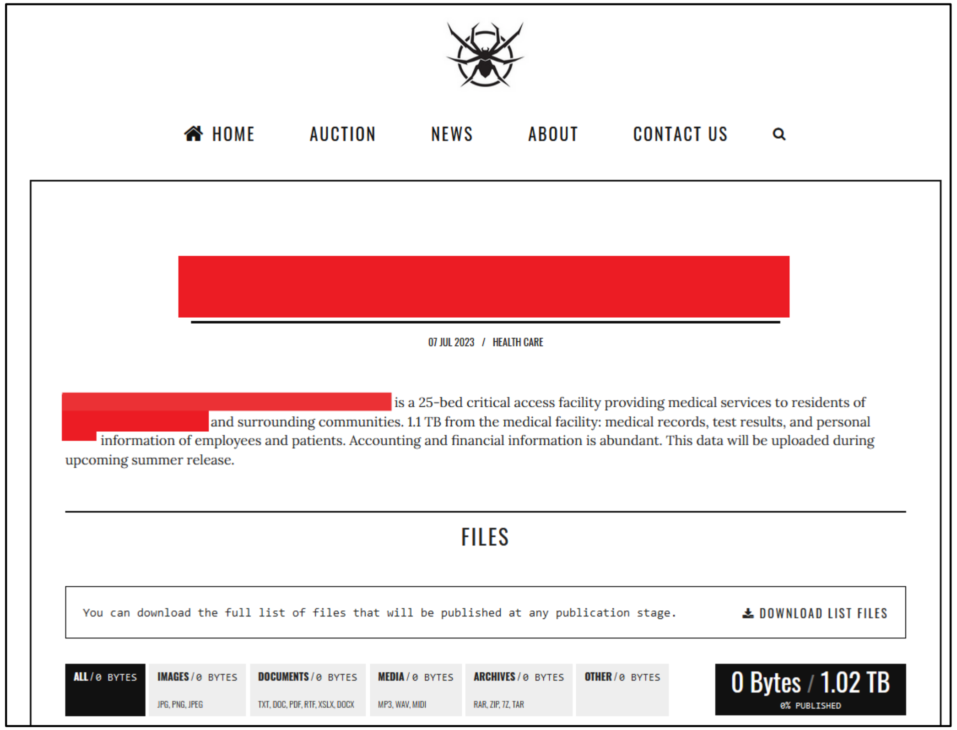
Cyber threat intelligence is valuable to organizations in any industry and of any size.

Sample of what we have found when performing CTI investigations

Finding	Recommendations
Cloud storage misconfigurations, resulting in exposure of customers' personally identifiable information (PII)	*Immediate notification is issued to the client* Alter configurations in accordance to provided cloud storage documentation and contact impacted individuals regarding their information being exposed.
Employees' personal credentials exposed in third-party breaches, potentially granting threat actors with access to employee accounts via password reuse attacks	Educate employees about the risk of using corporate email accounts on third-party platforms. As password reuse across platforms is common, ensure employees are not using similar passwords to those exposed by enforcing a strong password policy.
Publicly reported web application vulnerabilities which remained unpatched, resulting in threat actors being able to redirect users to malicious webpages via cross-site scripting (XSS) attacks	Patch the web application by leveraging internal standard operating procedures, along with the provided documentation regarding the specific vulnerability.
Employee's credentials exposed on a publicly-available website (a code repository). As this page is publicly-available, a threat actor could easily identify these credentials and utilize them to access portals associated with the user's account or attempt to perform password re-use attacks.	*Immediate notification is issued to the client* Reset the account credentials associated with the employee and remove the code snippet from the website. Consider making future code uploads private by default unless otherwise necessary.

Continued threats to healthcare: Ransomware and Extortionware

*The healthcare industry continues to be hampered by ransomware; however, more instances of data being stolen **as well as** encrypted are being reported*



[redacted]

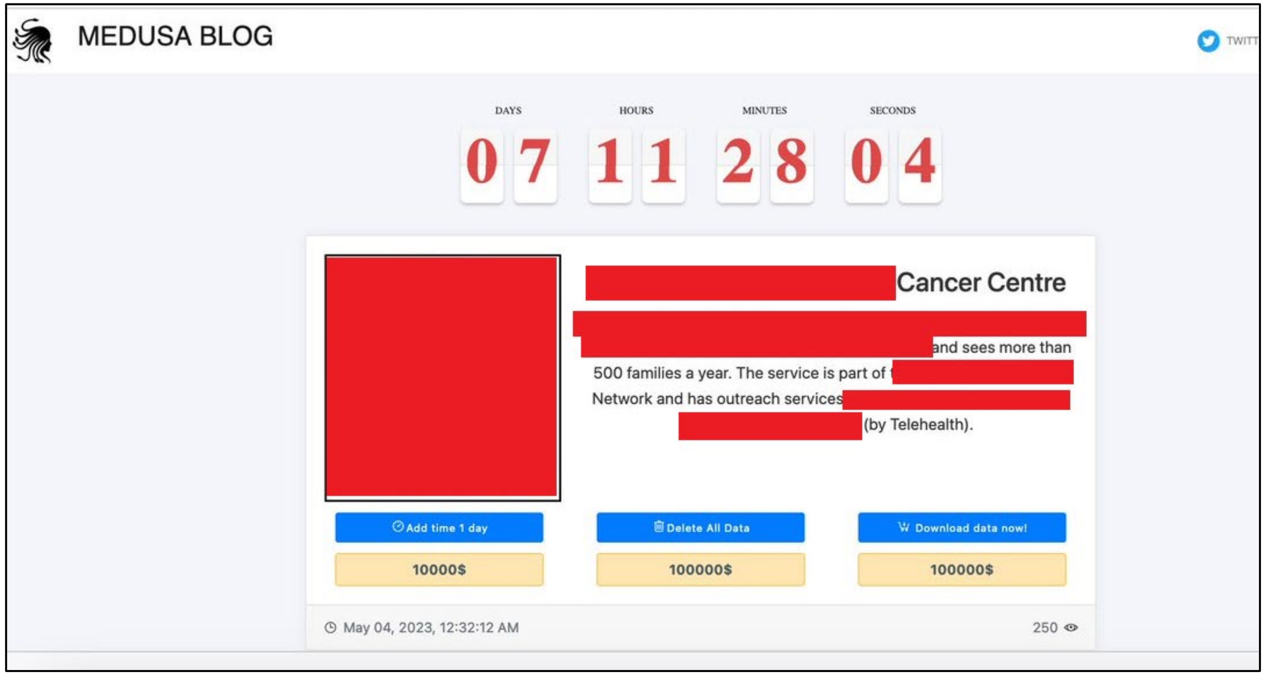
07 JUL 2023 / HEALTH CARE

[redacted] is a 25-bed critical access facility providing medical services to residents of [redacted] and surrounding communities. 1.1 TB from the medical facility: medical records, test results, and personal information of employees and patients. Accounting and financial information is abundant. This data will be uploaded during upcoming summer release.

FILES

You can download the full list of files that will be published at any publication stage.

July 2023 advertisement for ransomed data on data extortion group Karakurt's website



[redacted] Cancer Centre

[redacted] and sees more than 500 families a year. The service is part of [redacted] Network and has outreach services [redacted] (by Telehealth).

May 04, 2023, 12:32:12 AM

250

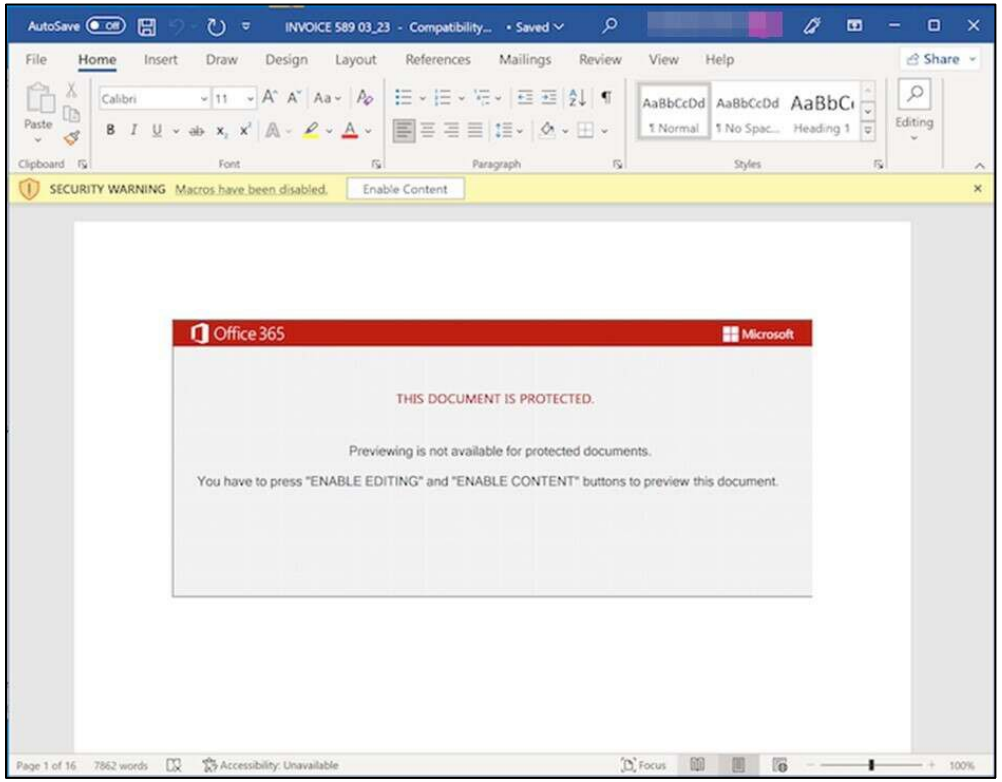
May 2023 advertisement for ransomed data on ransomware group Medusa's website

(*Sources:*
2023 Data Breach Investigations Report | Verizon
Various Materials | Recorded Future)

Intelligence news flash: Emotet returns…

Emotet, an advanced phishing Trojan, returned in March of 2023 after being offline for three months.

- Delivery of malicious documents embedded in ZIP archives through phishing emails ***resumed in March of 2023***
  - A new technique, binary padding, has been observed, which assists Emotet in ***avoiding detection***
- The malware will load several modules, such as ***spam*** and ***information stealer*** modules
- **Impact**: Emotet's various methods of entry, along with its ***persistence*** and ***evasion*** techniques, make it a difficult malware to guard against for organizations in all industries.
  - Infection could lead to ***breached account credentials*** and further malware infections, including ***ransomware***.



SECURITY WARNING Macros have been disabled. Enable Content

THIS DOCUMENT IS PROTECTED.

Previewing is not available for protected documents.

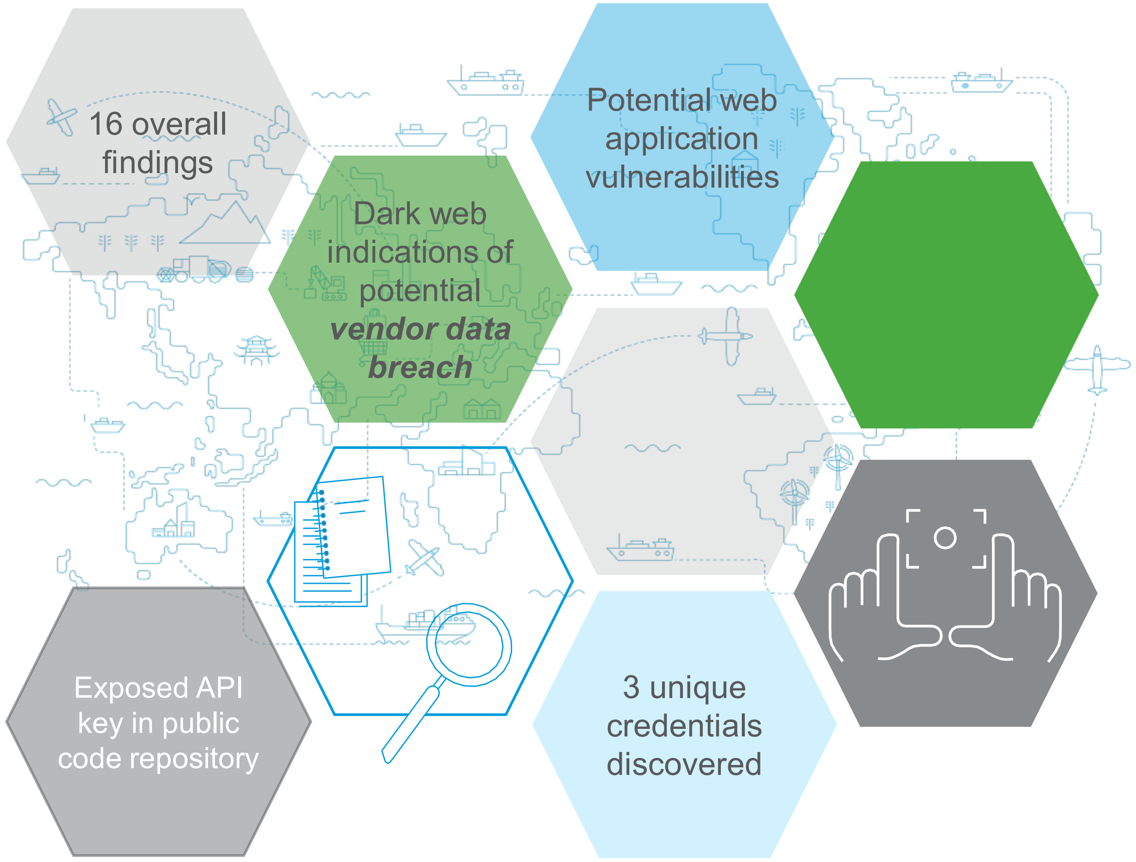
You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.

Prompt to enable macros on malicious document

(*Sources:*
[Emotet Returns, Now Adopts Binary Padding for Evasion](#) | Micro Trend
Various Materials | Recorded Future)

Case study – Medical Technology

Cyber threat intelligence (CTI) investigation



16 overall findings

Dark web indications of potential ***vendor data breach***

Potential web application vulnerabilities

Exposed API key in public code repository

3 unique credentials discovered

The Challenge

A **midsize medical technology organization** wanted to understand what intelligence threat actors may be able to gather about their organization from open and closed sources. With the ever-changing cyber landscape, it is essential for organizations to routinely perform these investigations.

The Solution

The CTI team was brought in to perform a rapid **cyber threat intelligence review**. During the investigation, the team identified indications of a ransomware attack against one of the organization's vendors, which may have exposed organizational data. Additionally, the team identified other findings that needed to be brought to the attention of the organization as soon as possible, such as an exposed API key in a public code repository.

Why RSM

- Ability to provide actionable intelligence to proactively strengthen an organization's defenses
- Ability to access millions of open and closed sources, including dark web communities
- Subject matter expertise regarding threat actors and attack vectors

Potential Cyber Attack Scenarios

Scenario 1

- Ransomware attack on a healthcare organization in 2023:

In the year 2023, a small clinic in a rural area of the United States is hit by a ransomware attack. The clinic is running on outdated software, and the attackers exploit a vulnerability to gain access to the system. Once inside, they deploy the ransomware and encrypt all patient data. The attackers demand a hefty ransom in exchange for the decryption key.

As a result of the ransomware attack, the clinic is unable to access any patient records, hospital systems, or electronic medical devices. Patient care is significantly impacted, with treatments being delayed or cancelled. The clinic is forced to revert to paper-based records, causing a delay in patient care and impacting their confidentiality. It takes a few days for the IT staff to restore the systems from a backup, but some data is still lost, requiring the staff to create new files manually.

Furthermore, the attackers threaten to sell the data on the dark web. It is not often organizations successfully prevent their data from being auctioned or leaked on extortionware websites, so it may be incredibly difficult to actually prevent this. Additionally, there is a high likelihood of an OCR investigation along with the cost of a settlement agreement and potential State and Personal lawsuits. To prevent this, the clinic must work with law enforcement to identify and catch the attackers. Ultimately, the clinic is able to restore its systems and recover from the attack, but the impact on patient care and the organization's reputation is significant.

Scenario 2

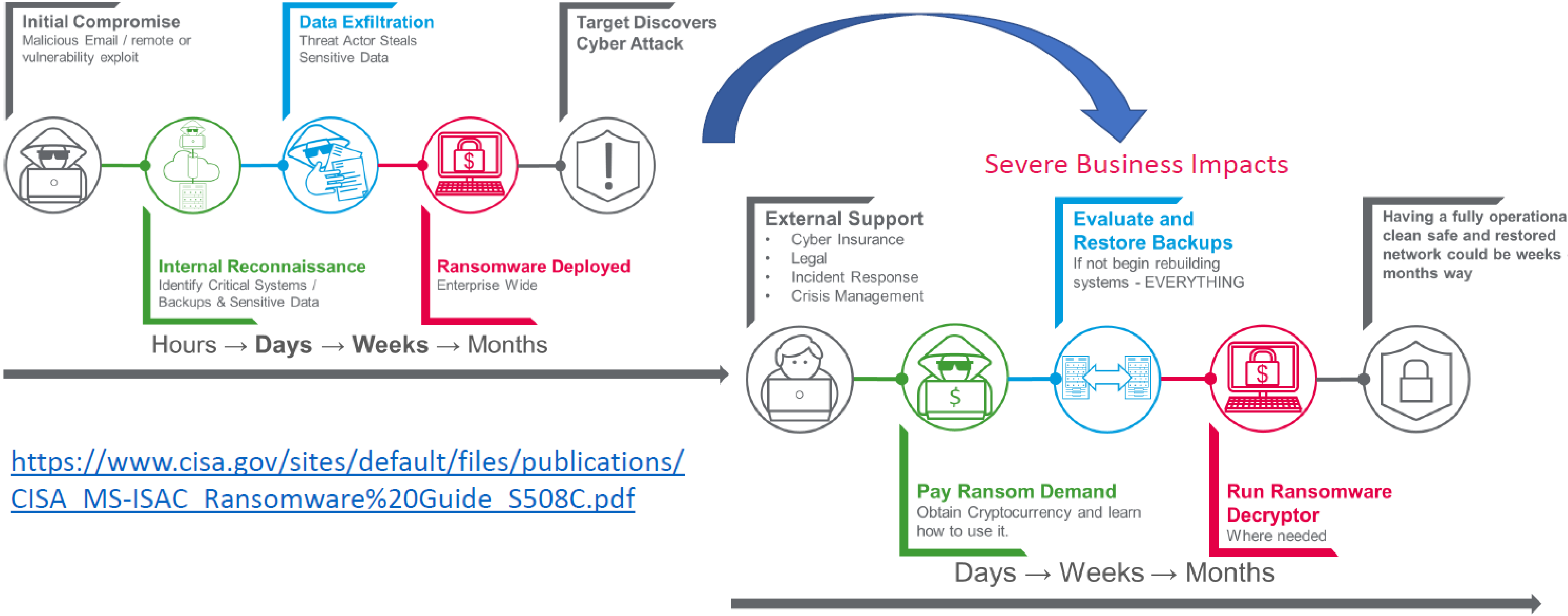
- Vishing (Voice Phishing) scenario on a healthcare organization in 2023:

An external attacker calls ABC Healthcare from a phone number spoofed to be related to a typical medical device service provider that ABC currently utilizes.

After reporting they are one of the technical support staff in charge of device maintenance, they explain that they are currently having difficulty accessing one of their devices and need the assistance of the employee. After leading the employee to a designated spoofed website purporting to be the vendors, they request the employee to click on a designated link to allow remote access. This link actually installs a local payload which gives system remote admin access and allows the nefarious actor control over the device and subsequent linked systems. At this time the caller thanks them for their assistance and hangs up. The actor is now free to work behind the scenes in gathering intel on the systems and network and being internal now, more opportunity to other systems not directly attached to the internet.

After determining the systems of highest value and installing additional command and control, the actor can begin exfiltrating data back to the original system or through another system with remote access . Additionally, this scenario could lead to the scenario one experience through Ransomware to gain both the data and possible financial gain.

Summary - Ransomware timeline



Initial Compromise
Malicious Email / remote or vulnerability exploit

Internal Reconnaissance
Identify Critical Systems / Backups & Sensitive Data

Data Exfiltration
Threat Actor Steals Sensitive Data

Ransomware Deployed
Enterprise Wide

Target Discovers Cyber Attack

Hours → **Days** → **Weeks** → Months

Severe Business Impacts

External Support
- Cyber Insurance
- Legal
- Incident Response
- Crisis Management

Pay Ransom Demand
Obtain Cryptocurrency and learn how to use it.

Evaluate and Restore Backups
If not begin rebuilding systems - EVERYTHING

Run Ransomware Decryptor
Where needed

Having a fully operational clean safe and restored network could be weeks or months way

Days → Weeks → Months

https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Emerging Cyber Landscape

Navigating the shifting cyber risk landscape

01

Impact of global economic headwinds

With high levels of uncertainty around inflation, challenges in the supply chain, and shrinking profit margins, cyber leaders are being asked to do more with less

02

Growing complexity of cyber solution landscape

Cybersecurity software industry is experiencing exponential growth resulting in an explosion of tools in the market however there are limited ways to assess solution value, overlap with existing solutions, and validating each is fully configured

03

Lack of board-level understanding of cyber risk

While cyber more often has a seat at the table, Boards are challenged to put cyber risk in context with business operations and its enterprise risks

04

Increasing gap in the cyber workforce market

The cyber workforce shortfall continues to grow leaving millions of positions unfilled and an increasing fight for talent

05

Minding the gap of shared responsibility

Vendors play an increasingly important role in cybersecurity (e.g., outsourcing, and cloud) but there is a lack of understanding regarding the division of responsibilities

Preparing for the evolving trends of cybersecurity

Identity is the New Perimeter

Changing borders of the workplace and IT landscape have forced a shift from network boundaries to focus defenses on digital identity

Tomorrow’s Cyber Workforce is Being Built Today

The war for talent is driving investments into internal staff development through both retooling and upskilling your workforce

Responsibility Must Align With “As a Service”

Complex vendor ecosystem requires constant alignment & communications while also adapting to evolving technologies and regulatory needs

Automation Will Drive Action Over Alerting

Automation will need to extend beyond detection and orchestration in order to drive decisioning in near real-time

Data Will Fuel Risk & Opportunity in Cyber

Data will serve as an increasingly valuable business and cyber asset but with tightening regulation and growing risk to organizations

Cyber Service & Platform Markets Will Consolidate

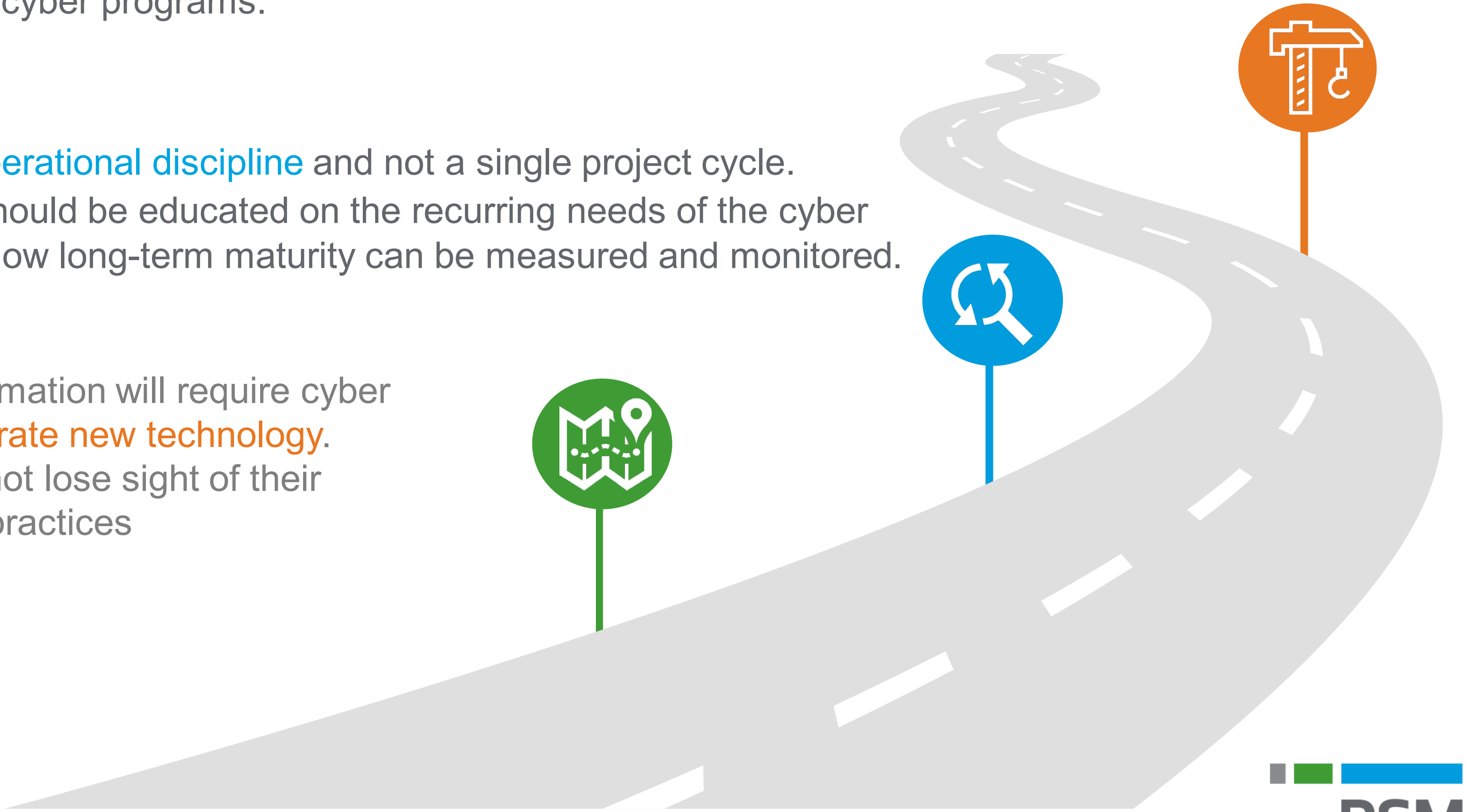
Anticipate vendor convergence to expand core capabilities, drive margin, enhance interoperationality, and unify disparate solutions

The road ahead

Organization should follow a Discover, Design, Deploy, Optimize approach to evaluating and maturing their cyber programs.

Cyber security is on-going operational discipline and not a single project cycle. **Organization** leadership should be educated on the recurring needs of the cyber security program as well as how long-term maturity can be measured and monitored.

Investment in digital transformation will require cyber programs to adapt and integrate new technology. However, programs should not lose sight of their foundational cyber hygiene practices



The role of transformative and emerging technology

Cyber leaders must balance securing their current IT landscape against economic headwinds while also enabling the organization to evaluate the new ‘IT buzzwords’ that have the potential to revolutionize how and where companies deliver on their mission

Cloud

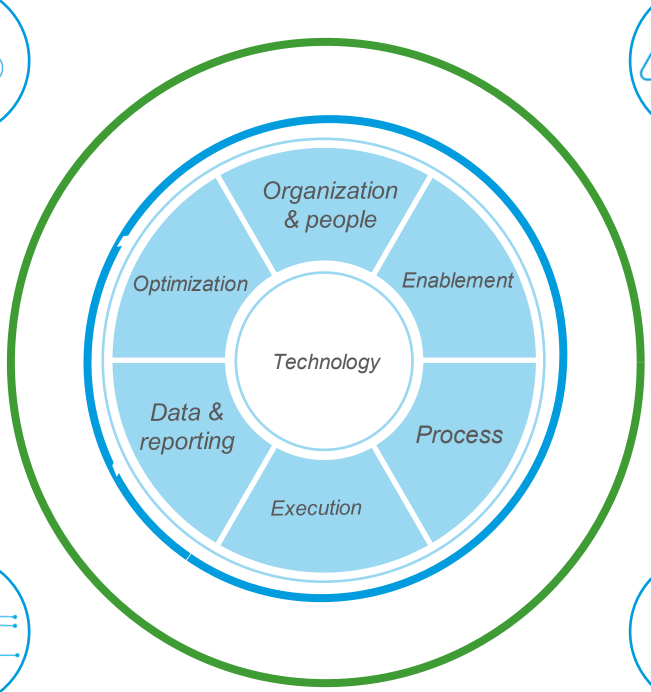
- No longer the “new kid on the block”, the use of Cloud-first has become business-as-usual
- Cyber teams are still struggling to keep up; 2023 will be the year to buckle down or source support to maintain a secure cloud environment

Blockchain

- Expanding use cases as digital contracts and differing formats of token-based financial products arrive in the market
- Cyber organizations are being asked to participate and embed security from asset verification pre-release to monitoring and response

Generative AI / Machine Learning

- Vendors will further embed AI into products
- Users expect that AI will be a daily part of their productivity
- Cyber criminals have adopted Large Language Models (LLMs) as a means to advanced attacks



Metaverse / Augmented Reality

- Metaverse adoption has been slow, but augmented reality devices and use cases continue to grow
- Implications from an identity and engineering protection perspective will be one that will require cyber’s attention to maintain an appropriate secure posture

Big Data

- Continued focus on gaining additional value from the data
- Expect expanded efforts towards improved usage of data (e.g., chatbot like features) and data correlation use cases
- This must be balanced with the expected growth of privacy and other regulatory requirements

Quantum

- Once thought of as only “over the horizon”, quantum computing is now becoming a reality.
- An immediate consideration for companies will be the “countdown” to when previously-considered encryption becomes obsolete and what that means for services providers who house their data. Plan ahead.

Converging with the increasingly complex compliance landscape

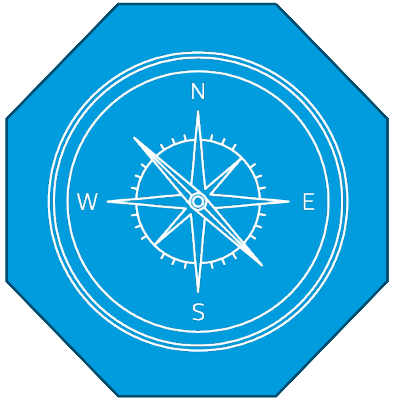
10 States Now With Data Privacy Laws. 10 More States in the Pipeline*

** As of June 2023*

Release of Whitehouse National Cybersecurity Strategy

EU Data Protection Board Continues to Issue Major Fines Against US Companies

Proposed SEC Rule for Reporting of Material Cybersecurity Incidents



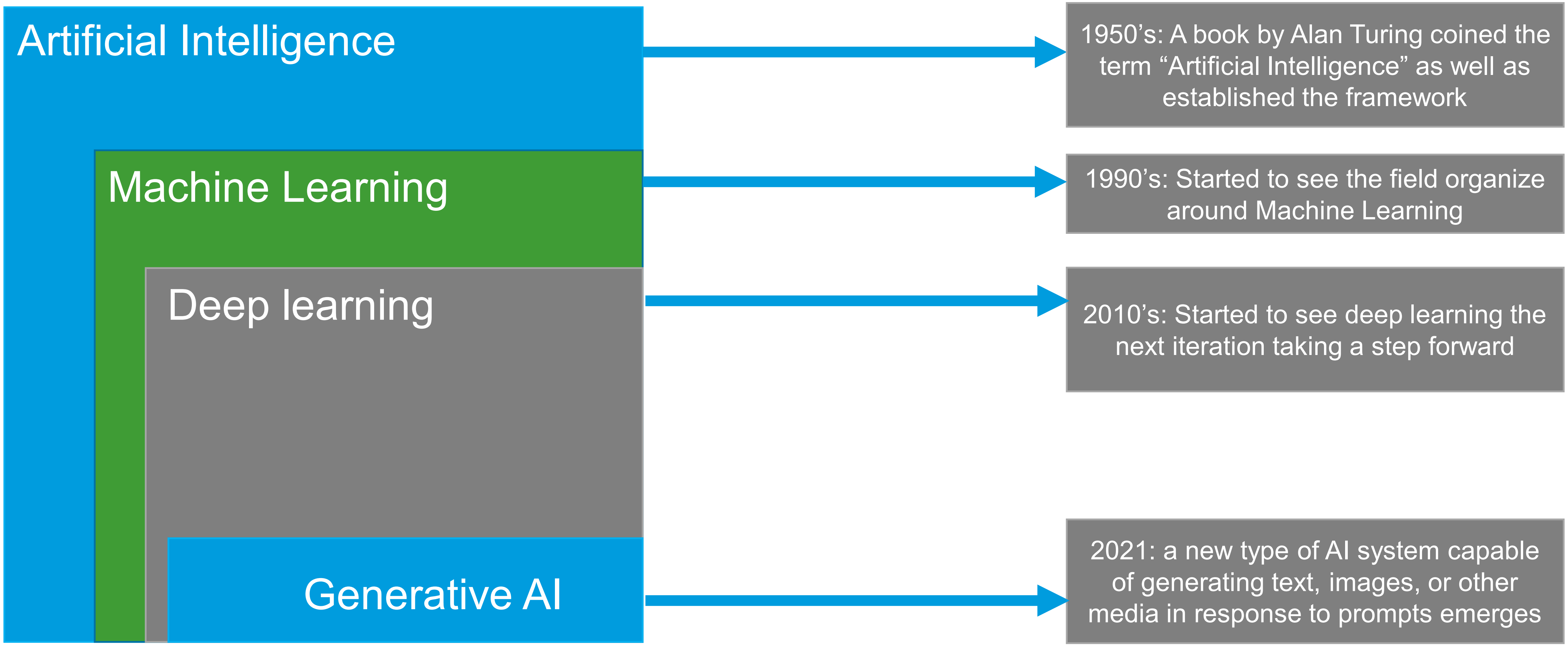
Major Version Change to NIST CSF Controls Framework

Federal Government Agency Mandate for Aligning to Zero Trust Standards

Expanded Scope of Organizations Impacted by FTC Safeguards Rule

State of NY Proposes Significant Expansions to Existing Cyber Regulations

Where did Chat GPT Come From?



Artificial Intelligence

Machine Learning

Deep learning

Generative AI

1950’s: A book by Alan Turing coined the term “Artificial Intelligence” as well as established the framework

1990’s: Started to see the field organize around Machine Learning

2010’s: Started to see deep learning the next iteration taking a step forward

2021: a new type of AI system capable of generating text, images, or other media in response to prompts emerges

Use Cases of Chat GPT in Health Care

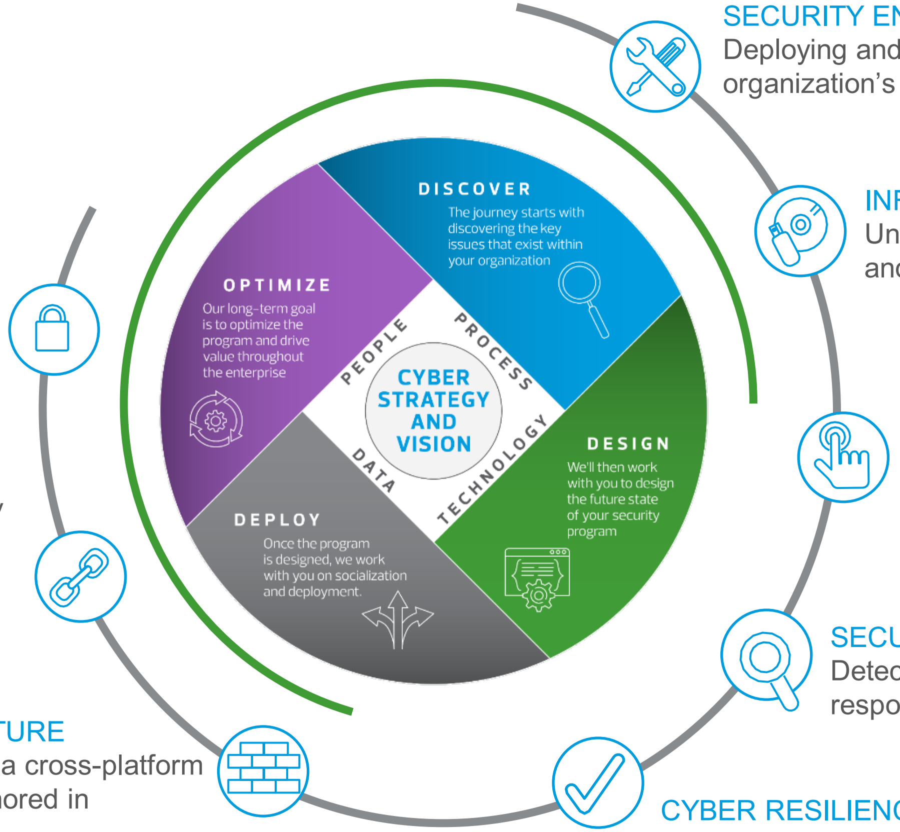
1. **Service Ticket Automation**
2. **Voicemail & Patient Messaging Automation**
3. **Patient Chart Summarization**
4. **Automated Service/Procedure Order Generation** with ChatGPT model for patient admission.
5. **Classify Payers' responses to Revenue Cycle**
   - Prior Authorization
   - Claim Status
   - Denial Follow-up
6. **Call Center**
   - Quality Assurance Monitoring
   - Knowledge Management,
   - Best Practice Sharing
   - Performance Analytics
   - Role-Playing and Simulation
7. **Supply Chain Documents and Contract Summarization**
8. **Telemedicine**
9. **Remote patient monitoring**

Positioning for the Future

How do we Deal with all of this?

Applying phased approach to cyber maturity

Developing your cyber program requires an iterative approach in which the organization proceeds starting with Discover through a Design and Deploy stage before progressing into an ongoing Optimize phase where long-term maintenance and enhancement occurs.



CYBER STRATEGY AND VISION

DISCOVER

The journey starts with discovering the key issues that exist within your organization

DESIGN

We'll then work with you to design the future state of your security program

DEPLOY

Once the program is designed, we work with you on socialization and deployment.

OPTIMIZE

Our long-term goal is to optimize the program and drive value throughout the enterprise

SECURITY PROGRAM MANAGEMENT

Enabling CISOs to further mature and enhance the capabilities within an organization's cybersecurity program, moving toward operating as a business enabler

RISK AND COMPLIANCE

Guiding alignment of cybersecurity efforts with broader enterprise risk management and compliance obligations

SECURITY ARCHITECTURE

Designing and maturing a cross-platform secure architecture anchored in standards and principles

SECURITY ENGINEERING AND OPERATIONS

Deploying and operating tools and technologies in alignment with the organization's secure architecture design

INFORMATION PROTECTION

Understanding the organization's most valuable assets and focusing protection efforts accordingly

IDENTITY AND ACCESS

Managing secure access to the organization's resources for individuals, systems and devices

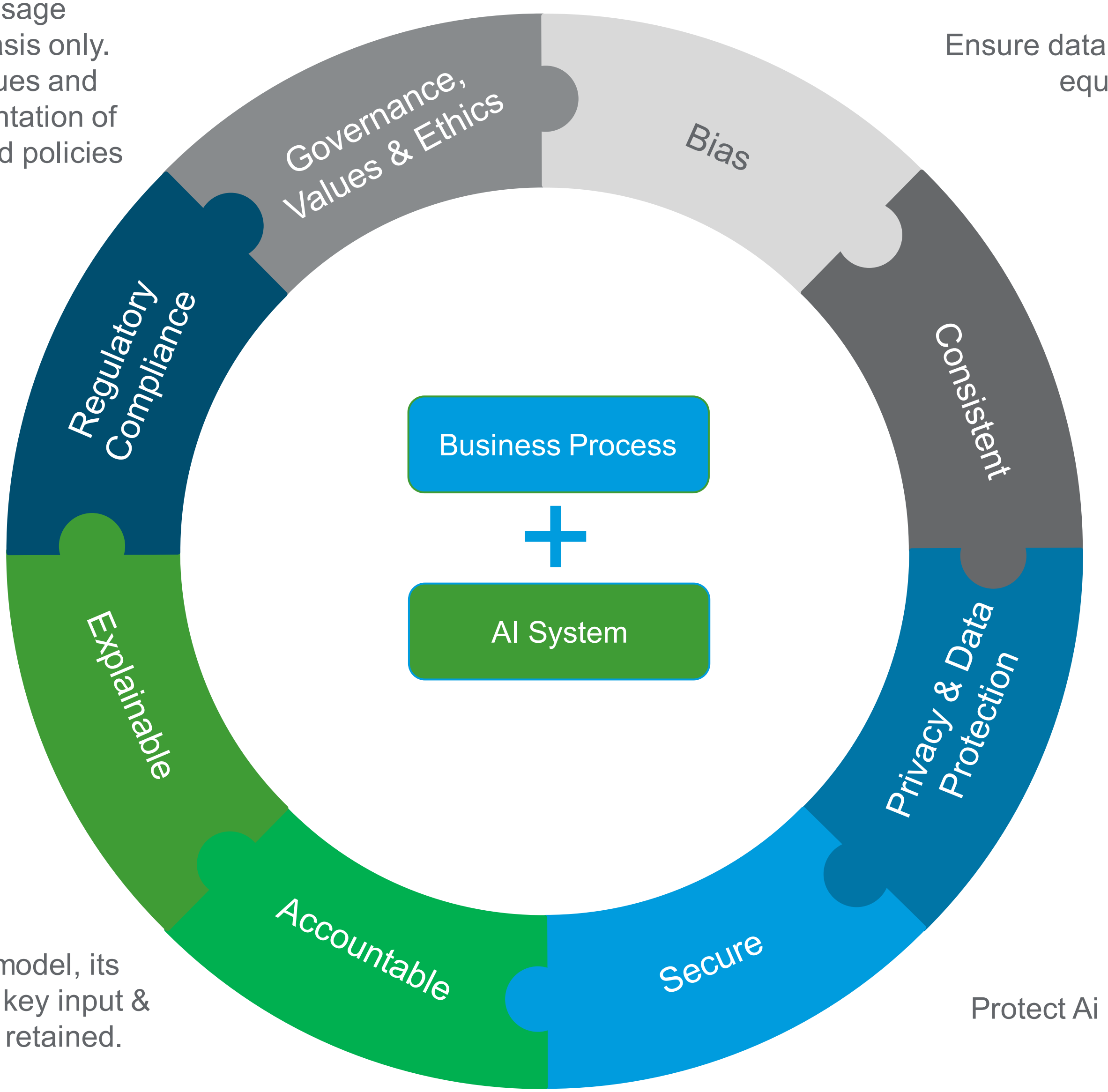
SECURITY MONITORING AND RESPONSE

Detecting anomalous behavior timely driving an informed response and resolution

CYBER RESILIENCY

Maintaining and recovering to normal operations in the wake of a destabilizing event

RSM AI Governance Framework



Require human oversight and usage authorization on a “need to use” basis only. Incorporate the organization’s values and ethics into the design and implementation of the system. Develop procedures and policies to govern Ai.

Ensure data leveraged for Ai systems are equitable and unbiased.

Factor applicable regulations into the design and implementation of the Ai system.

Train Ai systems to produce consistent results.

Incorporate data privacy rules and regulations into the design and implementation of the Ai system.

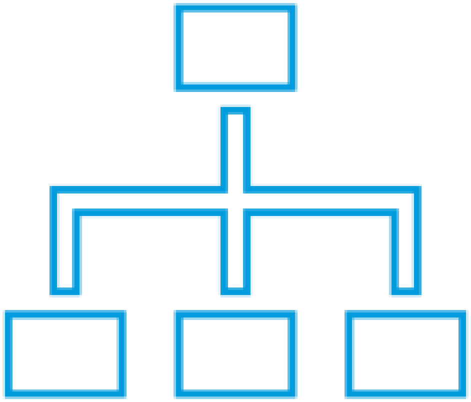
The stakeholders should be able to understand the input and explain the model’s output.

Clearly define ownership of the model, its input, and outputs. An audit trail of key input & updates should be captured and retained.

Protect Ai systems from cyber and physical attacks.

Integrating security risk management with enterprise risk management

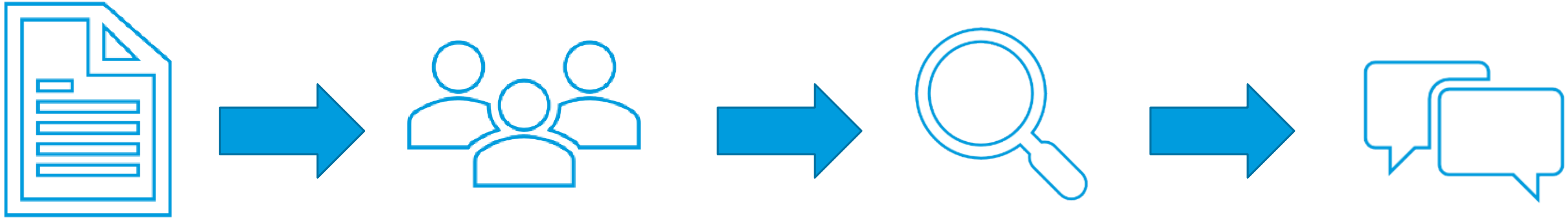
- Aligning risk acceptance processes
  - Integrated with security governance processes
  - Policies and procedures
  - Risk acceptance forms
  - Risk acceptance process (set acceptance frequencies)
  - Risk acceptance review process (periodically)
- Reduce shadow IT risks
  - Reduce opportunities to circumvent polices and procedures
  - ARBs don’t see everything
  - Leverage deployed security technology



Effective Governance Committee

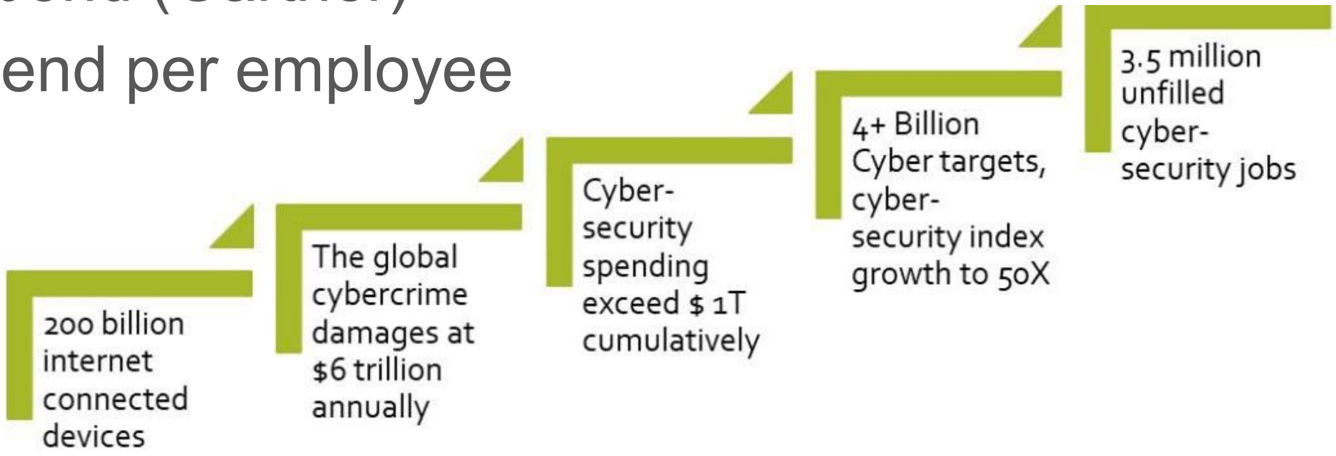
Implementing effective governance:

- Establish an effective committee charter
- Ensure affective committee composition
- Governance of policy oversight
- Mid-management risk review
- Document accountability
- Act on roles and responsibilities



Evaluating adequacy of IT spend

- Evaluating IT spend
  - Industry average 5% security team size against IT employee group (Gartner)
  - Industry Average IT spend 3.49% of revenue (Deloitte/WSJ)
  - Security spend 4.9% of IT Spend (Gartner)
  - Industry average security spend per employee spend $388 (Gartner)



200 billion internet connected devices

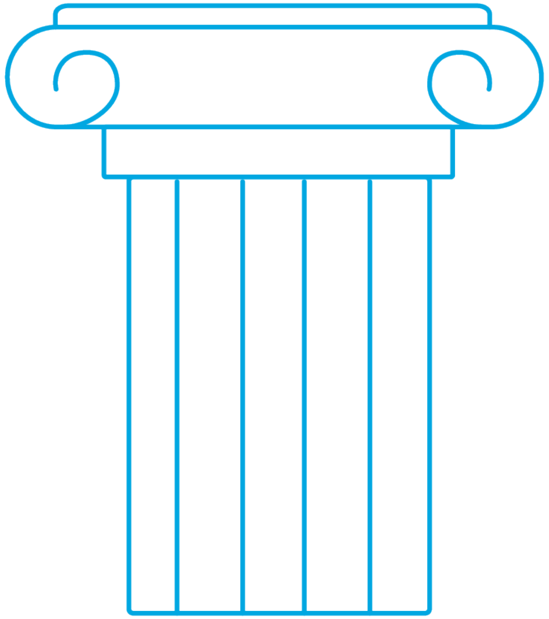
The global cybercrime damages at $6 trillion annually

Cyber-security spending exceed $ 1T cumulatively

4+ Billion Cyber targets, cyber-security index growth to 50X

3.5 million unfilled cyber-security jobs

HITRUST CSF purpose



What is it?

A *Common* Security and Privacy Risk Management Framework built from other standards and authoritative sources

Why is it used?

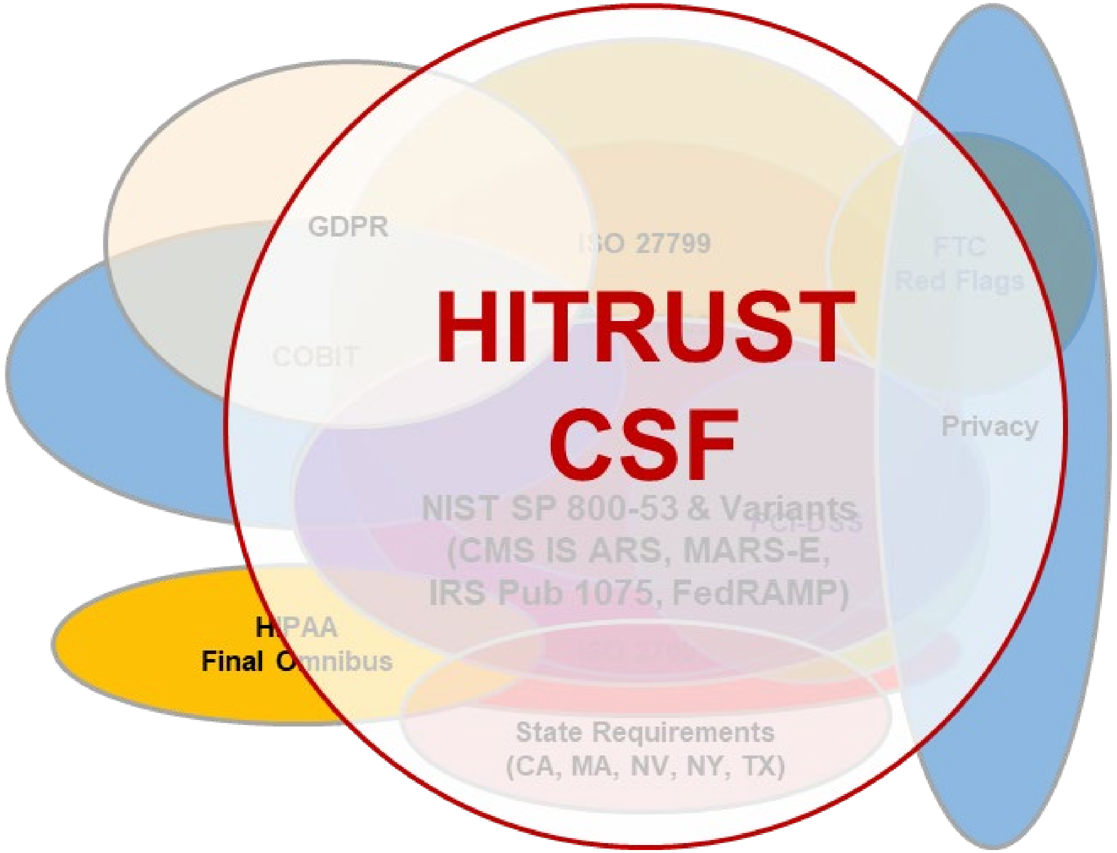
To provide coverage across *multiple* health care specific standards

Who uses it?

Any organization that creates, accesses, stores or exchanges Protected Health Information (PHI)

HITRUST CSF approach

- A comprehensive, industry-level overlay of the NIST RMF
    - Structured on ISO/27001
    - Built on NIST SP 800-53
    - Integrates many other relevant sources
- Designed by data protection professionals to address:
    - Risk Management Requirements
    - Security Requirements
    - Compliance Needs
- Provides the requirements and practices necessary to help ensure information and cybersecurity-related risks are managed smartly and consistent with business, risk and compliance objectives



Expanded HITRUST CSF Assessment Portfolio | Maturity Levels

The table below outlines the difference in testing requirements for the each of the assessment types in relation to the HITRUST CSF Maturity Levels:

Assessment Type	Number Requirement Statements	HITRUST CSF Maturity Levels				
		Policy	Procedure	Implemented	Measured	Managed
Cyber Essentials (e1) Assessment	44			✓		
Implemented (i1) Assessment	182			✓		
Risk Based (r2) Assessment	450+	✓	✓	✓	✓*	✓*

*The HITRUST CSF requires testing of the Policy, Procedure, and Implemented, the Measured and Managed maturity levels are optional and not required to be tested.

Applying More Focus on Privacy and Security for Healthcare Organizations

WHY IT MATTERS Each day security vulnerabilities are being identified and exploited by hackers which creates additional threats to healthcare organizations. The OCR remains committed with their oversight to protect individuals' health information privacy and security through enforcement and the pursuit of civil money penalties for violations that are not addressed.

The OCR's website for cases currently under investigation (*https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf*) reveal that within the past 24 months, 851 companies reported data breaches affecting nearly 91.3 million individuals. In 2023, 316 companies have reported data breaches affecting nearly 41.5 million individuals, where hacking or IT related incidents of network servers and email applications were listed among the highest areas affected. Nearly half of the reported data breaches were from business associates.

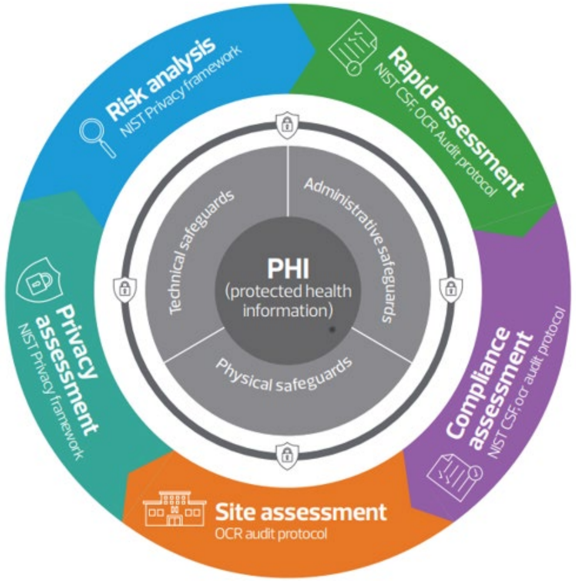
Entity breach reporting's within the past 7 months:

Type of Breach	
Hacking Incident	90%
Unauthorized Access	10%

Location of Breach	
Network Servers	97%
Email Application	2%

RSM HIPAA Privacy and Security for Healthcare

Comprehensive Privacy and Security Approach



- Risk modeling to identify threats and vulnerabilities
- Data boundary identification from on-premise to Cloud
- Defense-in-depth security mindset
- Aligned to Office for Civil Rights guidance
- Aligned to frameworks such as NIST CSF and Privacy

Security & Privacy Risk Analysis

- Assess organization-wide privacy and security programs
- Determine business unit data, system dependencies and process integration points
- Evaluate IT configurations and deployed security technology

Security & Privacy Compliance Assessments

- Assess compliance to the HIPAA regulations
- Evaluate alignment with OCR guidance
- Evaluate alignment to industry standards
- Develop recommendations and a strategic roadmap to strengthen compliance with industry and regulatory standards

Cybersecurity Services

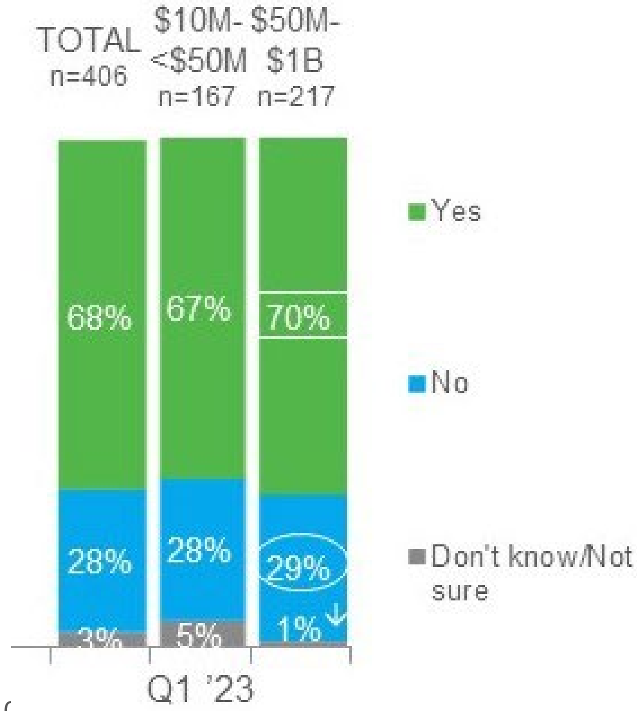
- Integrating cyber and enterprise risk
- NIST security engineering architecture assessments for system trustworthiness and resiliency
- Cloud architecture and configuration review
- Medical device security assessments
- Vulnerability and penetration security testing

Cyber insurance

68% of respondents currently utilize a cyber insurance policy to protect against internet-based risks, increasing from 61% in last year's report. The number of smaller middle market companies with cyber insurance increased to 67% this year from 65% in 2022, while larger companies that reported carrying a policy jumped significantly to 70% this year from 57% in 2022.

ORGANIZATION CARRIES A CYBER-INSURANCE POLICY

(BASE = total sample)



68%

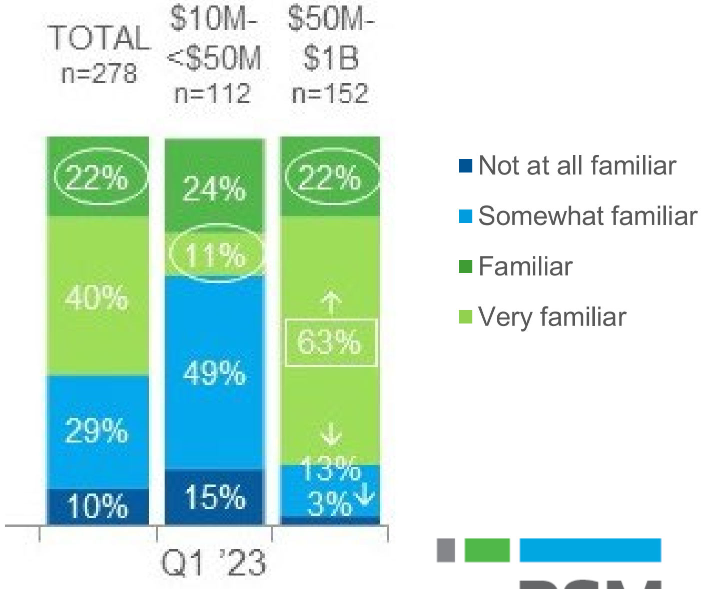
of middle market companies carry a cyber insurance policy, up from 61% last year.

70%

saw an increase in cyber insurance policy premiums. Only 2% saw a decrease.

FAMILIARITY WITH WHAT ORGANIZATION'S CYBER-INSURANCE POLICY COVERS

(BASE: carries cyber insurance)



Cyber Insurance: State of the Market Q1 ‘23

> *“Increased **competition** and **carriers’ focus on growth** has resulted in present conditions in the cyber insurance market that are far more favorable than just a quarter ago…”*

KEY FACTORS IMPACTING INSURANCE MARKETS

Pricing

- Many buyers may achieve increases of 25% or less at renewal. Select buyers with very strong programs may be able obtain preferrable pricing at lower than market rates
- Exceptional insureds may achieve flat renewals or slight rate decreases depending on their risk profile and whether they experienced substantial rate increases in 2021
- Majority of pricing flexibility is occurring in the excess layer of cyber insurance vs. the primary

Rebounding capacity

- Capacity returning to the market after seeing significant reductions in coverage in 2021 & 2022 as insurers look for additional sources of revenue and the population of insurable companies become more desirable for insurers

Bringing compliance into focus

- Emerging privacy laws and reporting requirements may contribute to increase in claims

Restrictive terms and conditions *(representative examples)*

- Focus on war exclusions in response to Russia-Ukraine war and past events (e.g., NotPetya)
- Ransomware/cyber extortion coverage continues to be limited without basic cybersecurity controls
- Widespread event exclusions and sub-limits (e.g., SolarWinds)

Cyber security controls continue to be scrutinized

- Robust controls remain a pre-requisite for insurance coverage for the foreseeable future
- Reviewing for accurate representation of controls; inaccuracies may complicate claims payouts

(Source: Lockton Companies) – For further information please contact Ashley Jones (abjones@lockton.com) at Lockton

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM