CYBERNOMICS: CURRENT STATE AND OUTLOOK OF HEALTHCARE CYBERSECURITY

SINADNITY
REQUEST
SECURITY
FUNDING
REQUEST
SUNDING
REQUEST
$

KEY TRENDS

RANSOMWARE & DOUBLE, TRIPLE EXTORSION

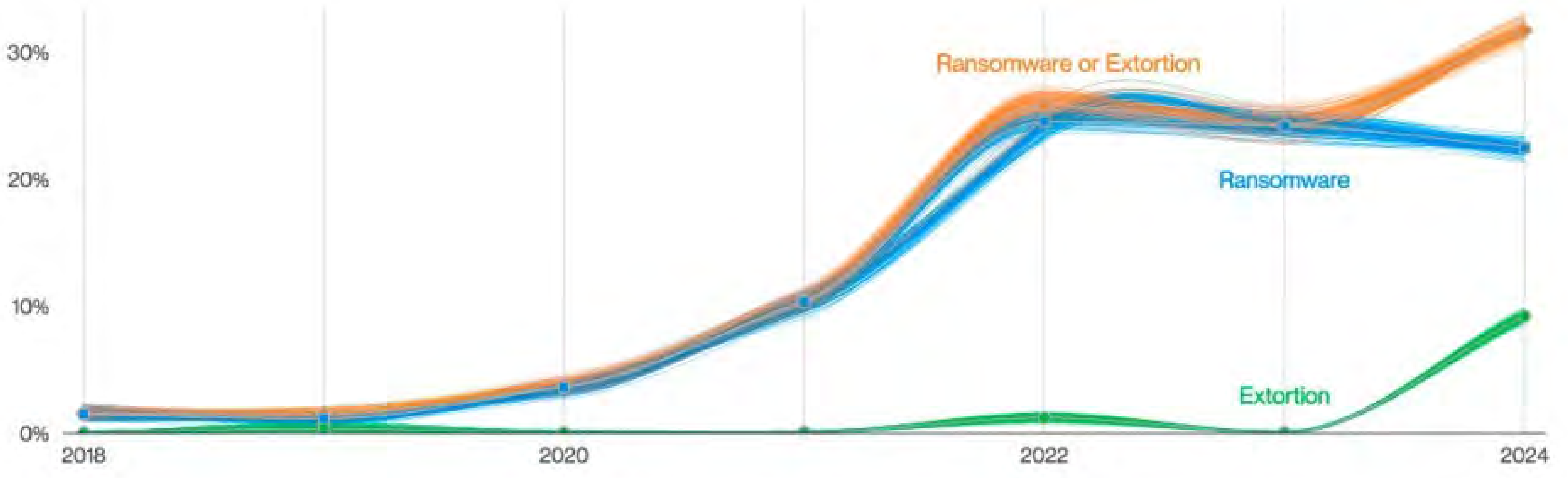
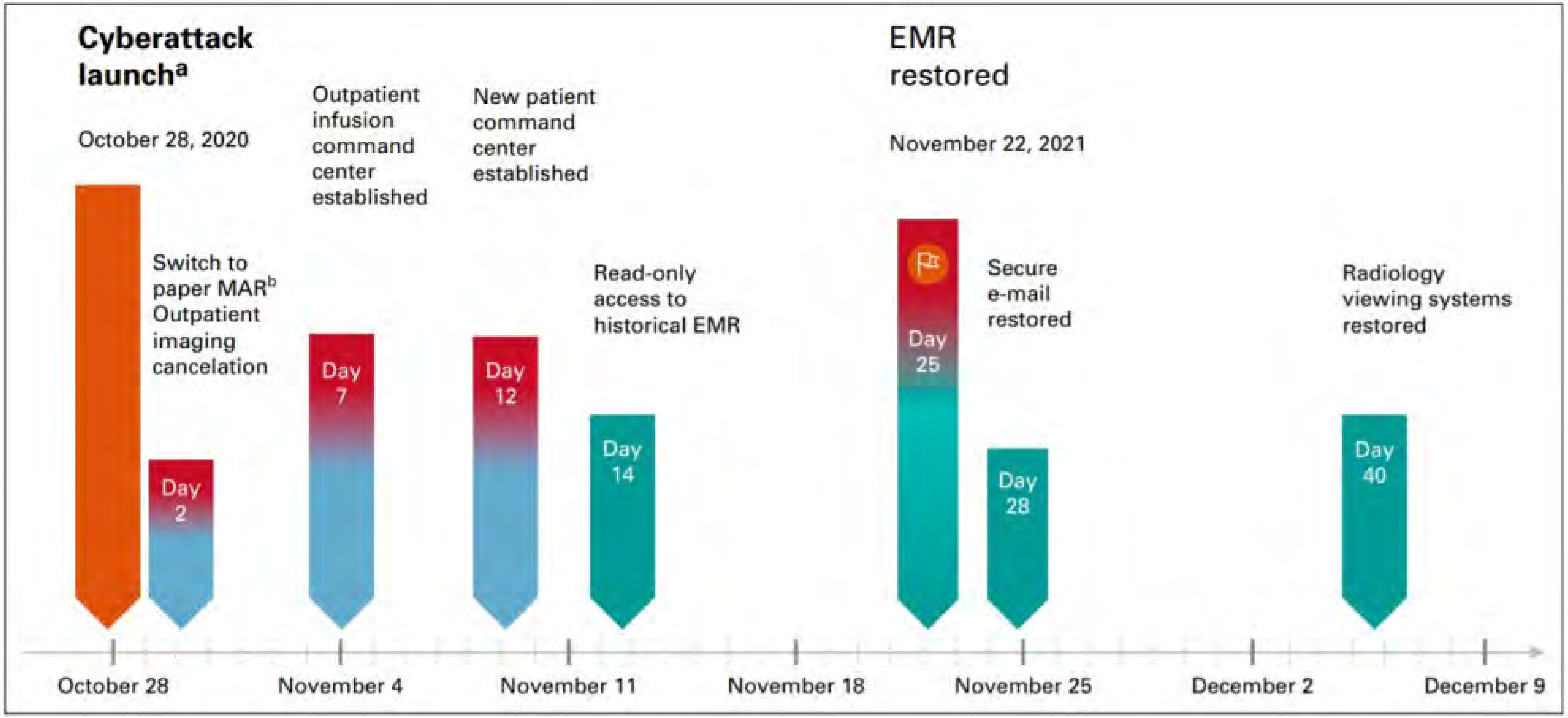


Figure 2. Ransomware and Extortion breaches over time

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

COMMON RANSOMWARE RECOVERY TIMELINE



https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

INTERNAL THREATS ON THE RISE

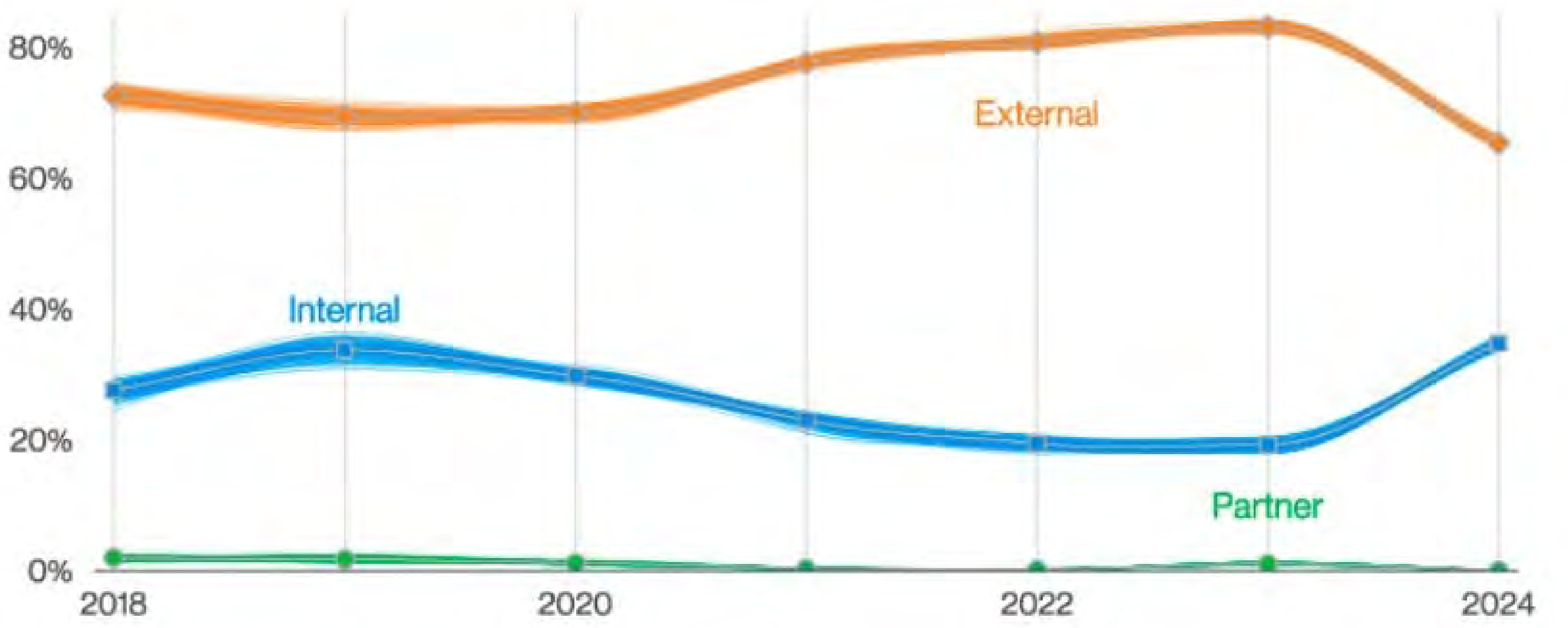


Figure 11. Threat actors in breaches over time

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

SUPPLY CHAIN RISK

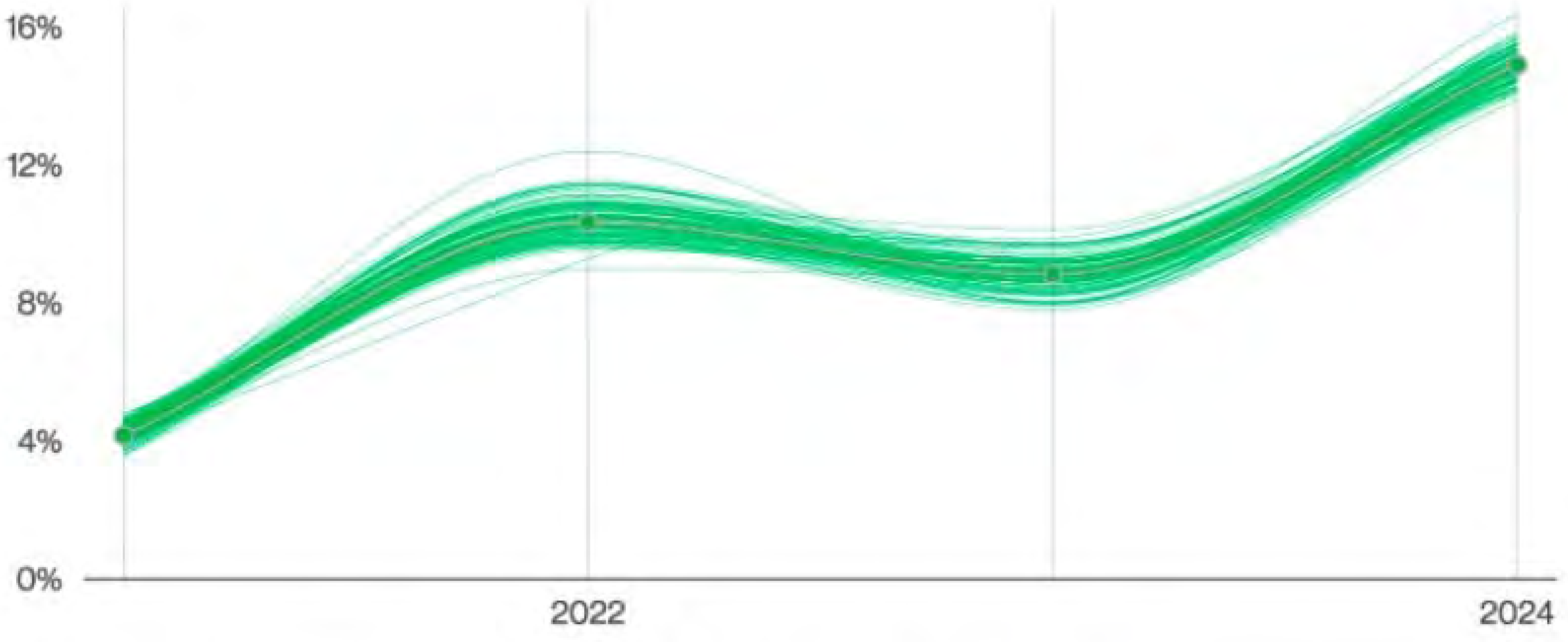


Figure 9. Supply chain interconnection in breaches over time

Solarwinds

Not Petya

Third Party Incidents (Change Healthcare)

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

:(
Your PC ran into a problem and needs to restart. We're
CROWDSTRIKE
complete
For more information about this issue and possible fixes, visit our website.

HEALTHCARE BREACH CAUSE DISTRIBUTION

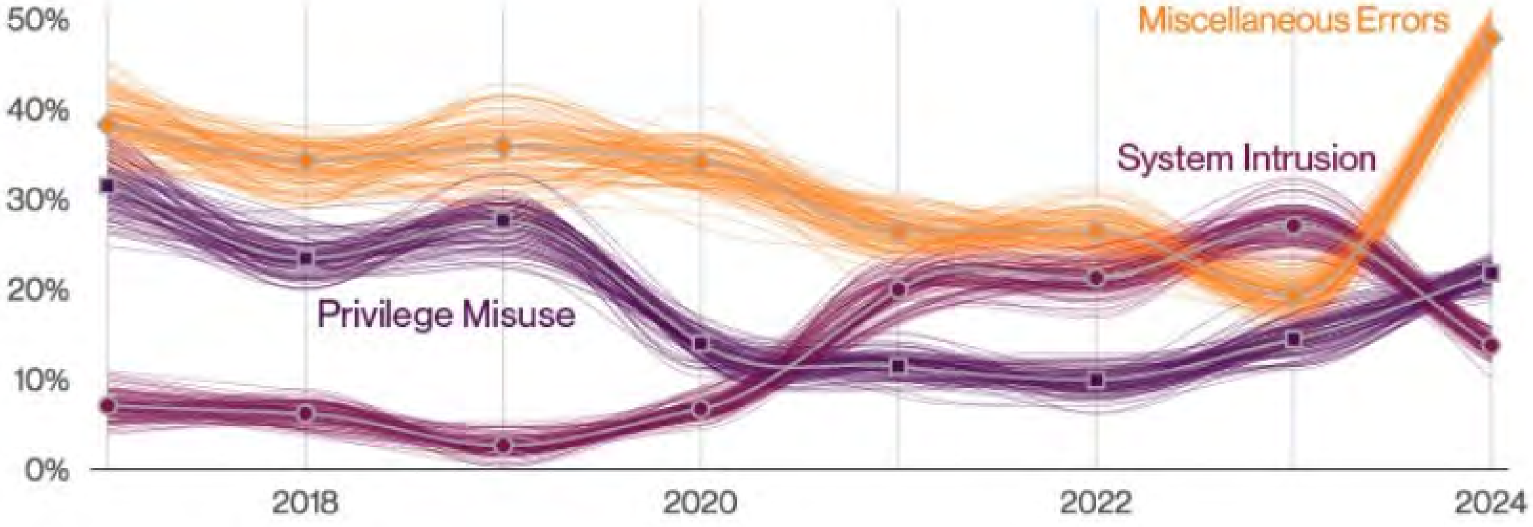


Figure 62. Top patterns in Healthcare industry breaches

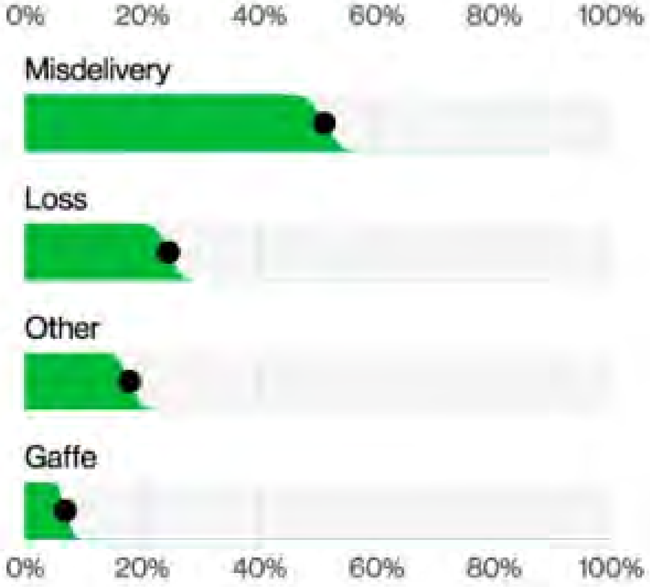


Figure 63. Top Error varieties in Healthcare industry breaches (n=568)

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

NON-ERROR TECHNIQUES

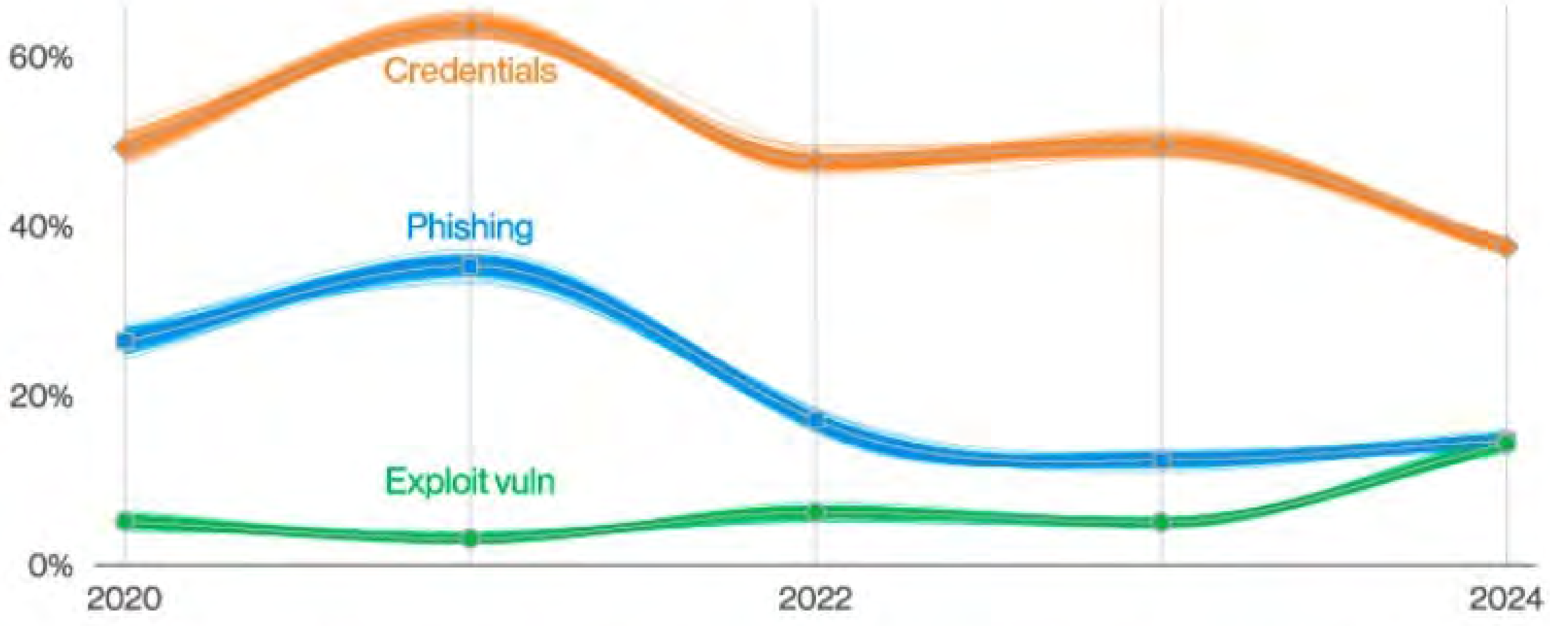


Figure 6. Select ways-in enumerations in non-Error, non-Misuse breaches over time

Ivanti

Pulse Secure

Citrix

MoveIT

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

VULNERABILITY DWELL TIME & EXPLOITATION

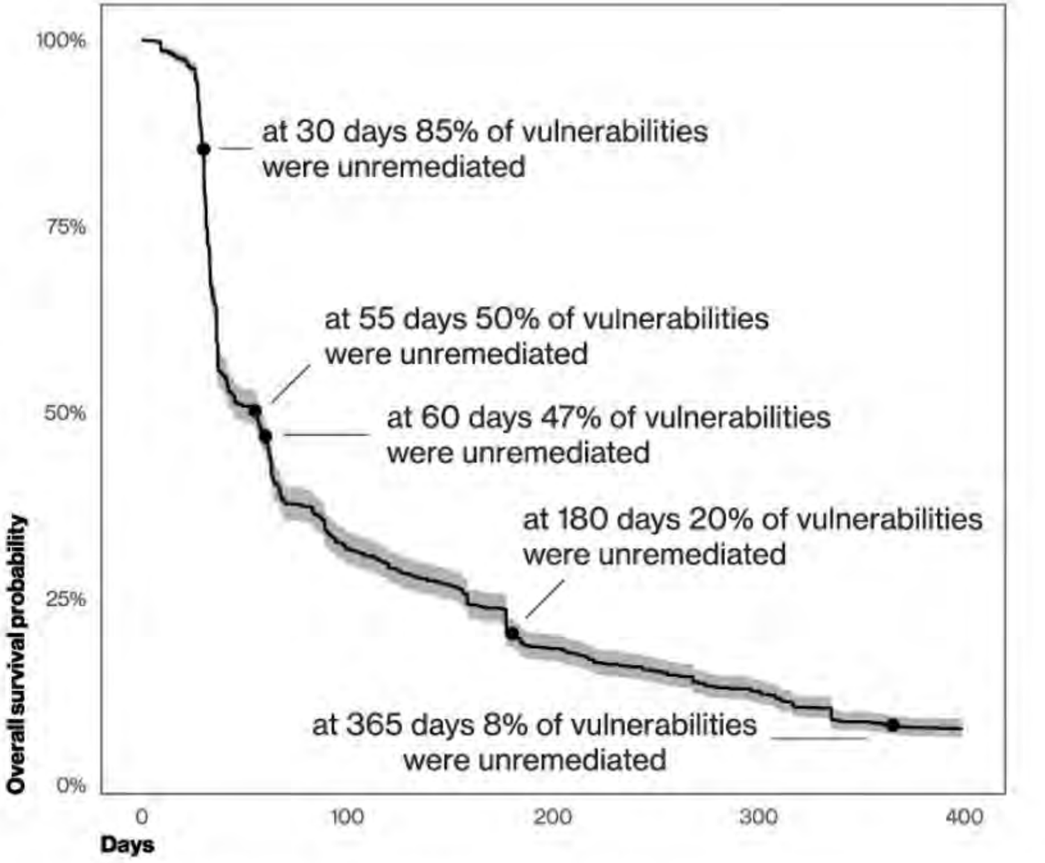


Figure 19. Survival analysis of CISA KEV vulnerabilities

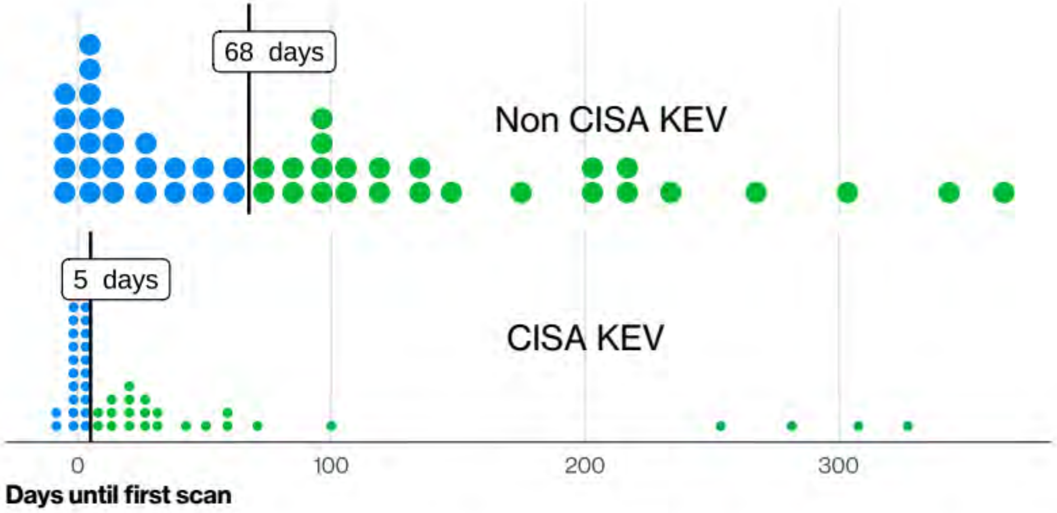


Figure 20. Time from publication of vulnerability to first scan seen (from 2020 onward)

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

BUSINESS EMAIL COMPROMISE

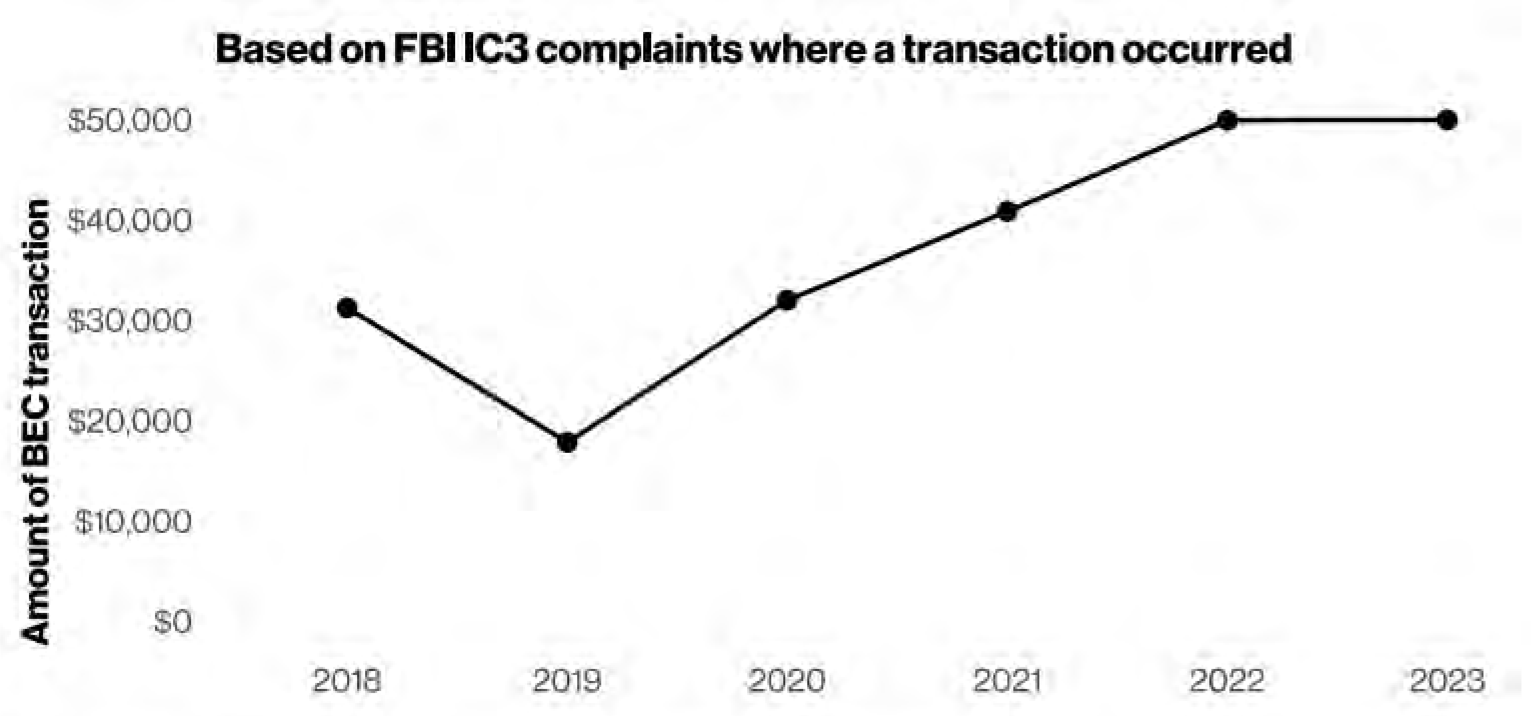


Figure 36. Median transaction size for BECs

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

PHISH CLICK & DATA ENTRY

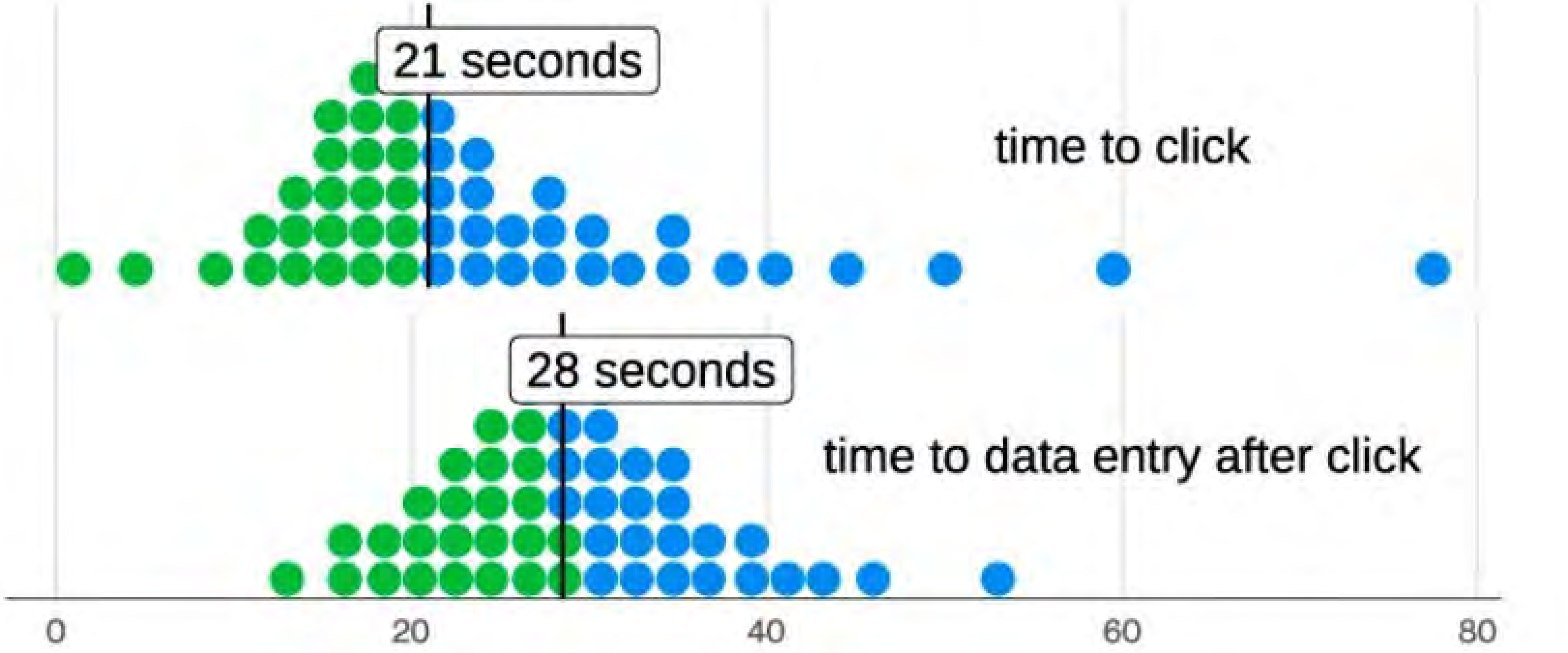
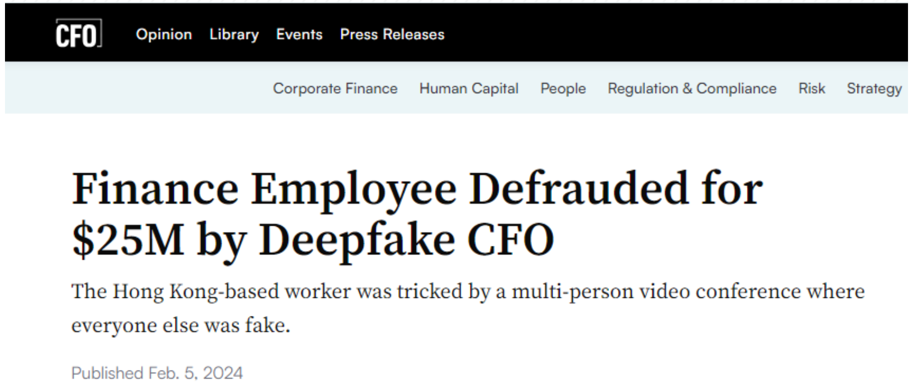


Figure 39. Time between email clicked and data entered

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

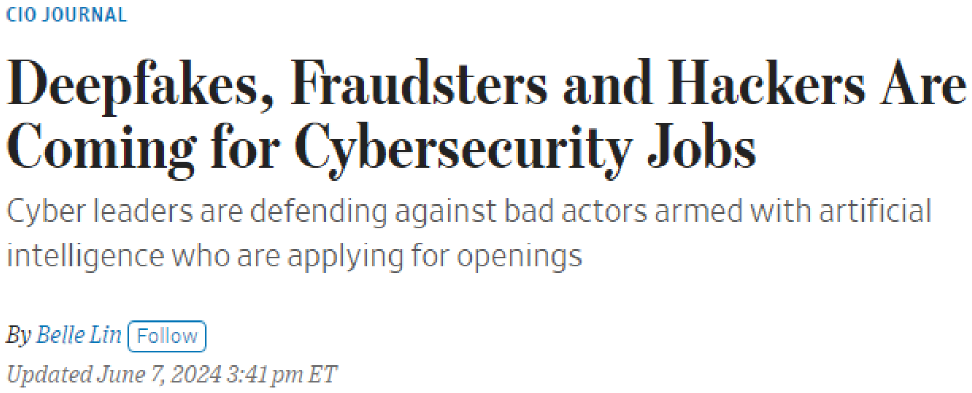
WHAT TO MAKE OF AI



Finance Employee Defrauded for $25M by Deepfake CFO

The Hong Kong-based worker was tricked by a multi-person video conference where everyone else was fake.

Published Feb. 5, 2024



Deepfakes, Fraudsters and Hackers Are Coming for Cybersecurity Jobs

Cyber leaders are defending against bad actors armed with artificial intelligence who are applying for openings

By Belle Lin

Updated June 7, 2024 3:41 pm ET

- Cross functional governance
- Cloud maturity is critical to AI development
- Understanding of AI models and data lifecycle
- Start small with business use cases
- Existing third-party AI adoption

https://youtu.be/wfAYBdaGVxs

REFRESHED BEST PRACTICES AND POTENTIAL REGULATORY CHANGES

DECEMBER 2023 HHS PRESS RELEASE HIGHLIGHTING ONGOING AND PLANNED STEPS TO IMPROVE CYBER RESILIENCY AND PROTECT PATIENT SAFETY

The HHS concept paper outlines the following actions:

- **Publish voluntary Health care and Public Health sector Cybersecurity Performance Goals (HPH CPGs).** HHS will release HPH CPGs to help health care institutions plan and prioritize implementation of high-impact cybersecurity practices.
- **Provide resources to incentivize and implement cybersecurity practices.** HHS will work with Congress to obtain new authority and funding to administer financial support and incentives for domestic hospitals to implement high-impact cybersecurity practices.
- **Implement an HHS-wide strategy to support greater enforcement and accountability.** HHS will propose new enforceable cybersecurity standards, informed by the HPH CPGs, that would be incorporated into existing programs, including Medicare and Medicaid and the HIPAA Security Rule.
- **Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity.** HHS will mature the Administration for Strategic Preparedness and Response's (ASPR) coordination role as a "one-stop shop" for health care cybersecurity which will improve coordination within HHS and the Federal Government, deepen HHS and the Federal government's partnership with industry, improve access and uptake of government support and services, and increase HHS's incident response capabilities.

https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html

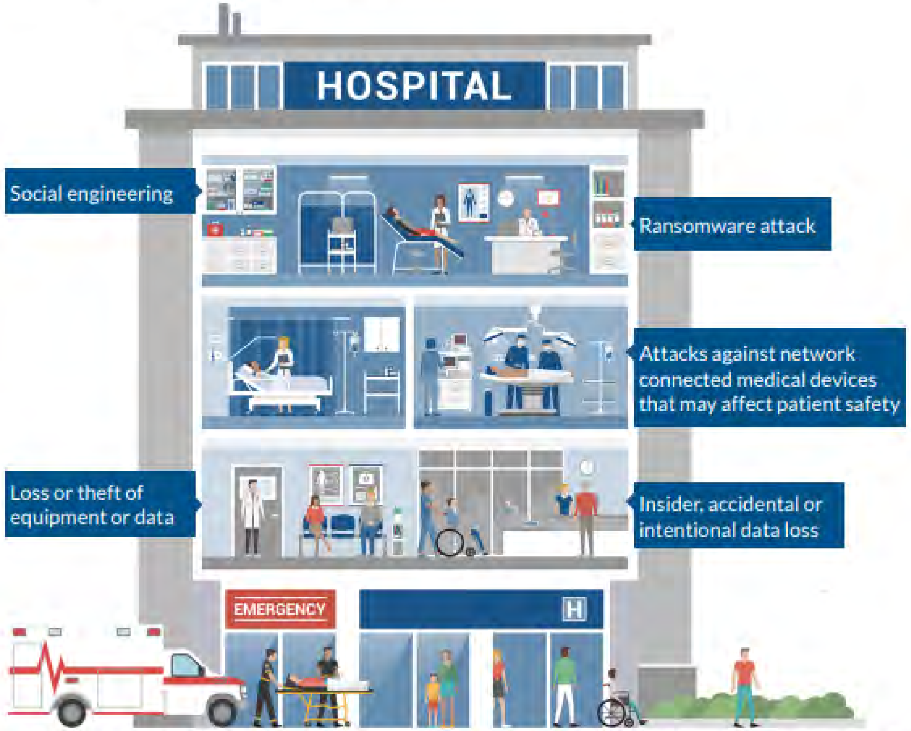
HHS HEALTHCARE & PUBLIC HEALTH CYBERSECURITY PERFORMANCE GOALS (CPGs)

Essential Goals	Enhanced Goals
Mitigate Known Vulnerabilities	Asset Inventory
Email Security	Third Party Vulnerability Disclosure
Multifactor Authentication	Cybersecurity Testing
Basic Cybersecurity Training	Cybersecurity Mitigation
Strong Encryption	How to Respond to Relevant Threats
Revoke Credentials	Network Segmentation
Basic Incident Planning and Preparedness	Centralized Log Collection
Unique Credentials	Centralized Incident Planning and Preparedness
Separating User and Privileged Accounts	Configuration Management
Vendor/Supplier Cybersecurity Requirements	

https://hhscyber.hhs.gov/performance-goals.html

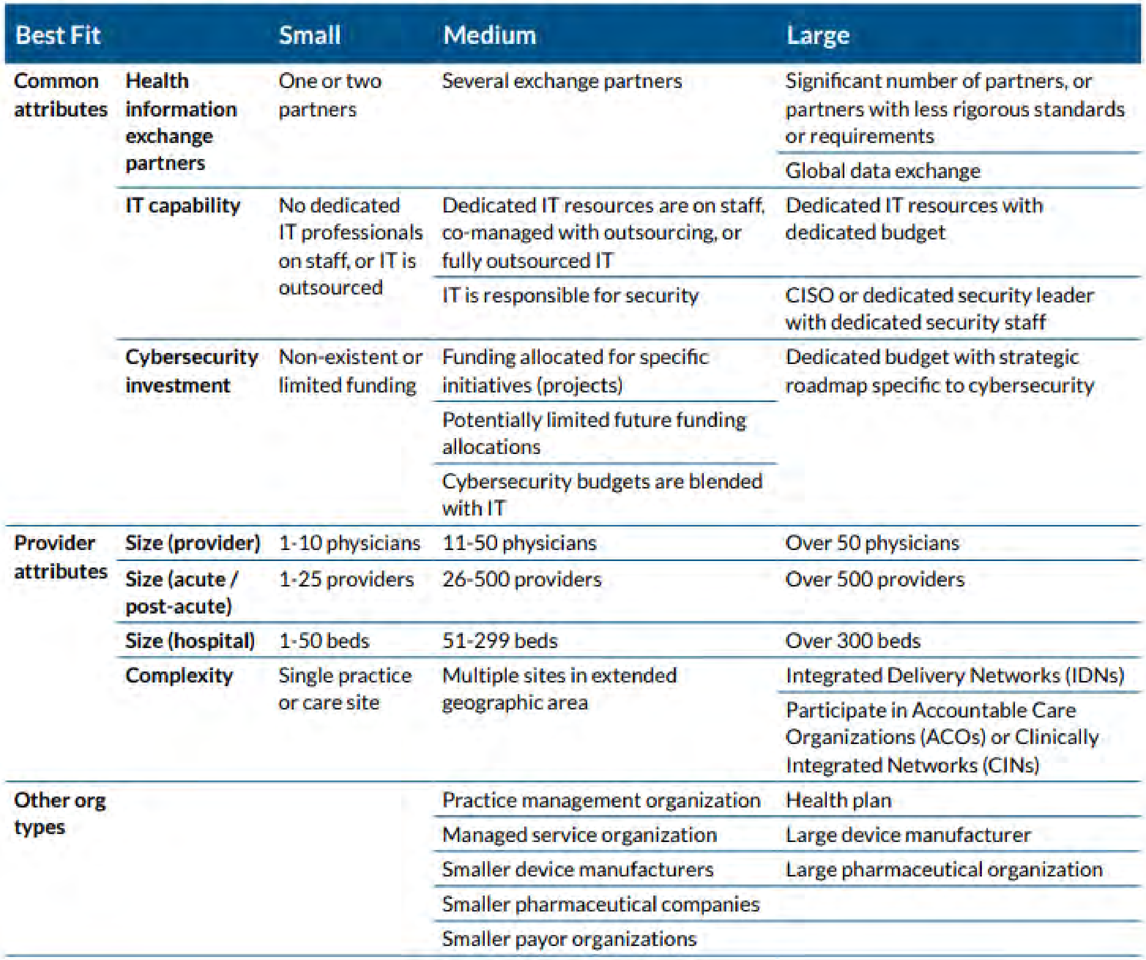
HHS 405(D) HEALTH INDUSTRY CYBERSECURITY PRACTICES (HICP)

Figure 6. Top 5 threats facing the HPH sector


HOSPITAL
Social engineering
Ransomware attack
Attacks against network connected medical devices that may affect patient safety
Loss or theft of equipment or data
Insider, accidental or intentional data loss
EMERGENCY
H

The threats portrayed in this graphic are meant to show that these threats can affect organizations in various parts of a hospital and in different healthcare settings. Cyber-attacks can happen anywhere, any time.

Table 1. Selecting the "Best Fit" For Your Organization

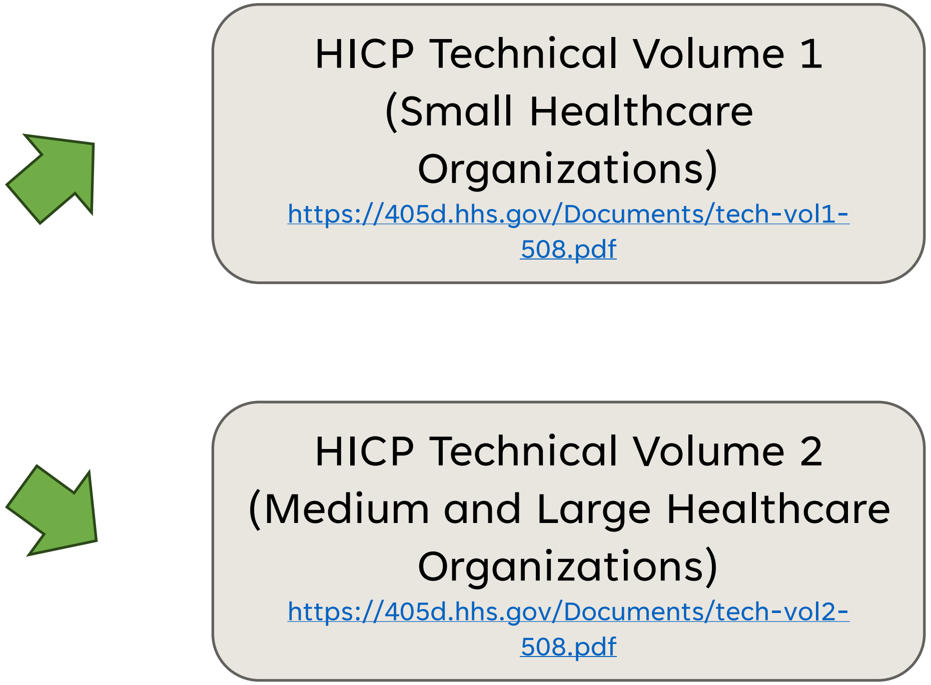


Best Fit		Small	Medium	Large
Common attributes	Health information exchange partners	One or two partners	Several exchange partners	Significant number of partners, or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, or IT is outsourced	Dedicated IT resources are on staff, co-managed with outsourcing, or fully outsourced IT IT is responsible for security	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Non-existent or limited funding	Funding allocated for specific initiatives (projects) Potentially limited future funding allocations Cybersecurity budgets are blended with IT	Dedicated budget with strategic roadmap specific to cybersecurity
Provider attributes	Size (provider)	1-10 physicians	11-50 physicians	Over 50 physicians
	Size (acute / post-acute)	1-25 providers	26-500 providers	Over 500 providers
	Size (hospital)	1-50 beds	51-299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated Delivery Networks (IDNs) Participate in Accountable Care Organizations (ACOs) or Clinically Integrated Networks (CINs)
Other org types			Practice management organization Managed service organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health plan Large device manufacturer Large pharmaceutical organization

https://405d.hhs.gov/
https://405d.hhs.gov/Documents/HICP-Main-508.pdf

HHS 405(D) HEALTH INDUSTRY CYBERSECURITY PRACTICES (HICP)

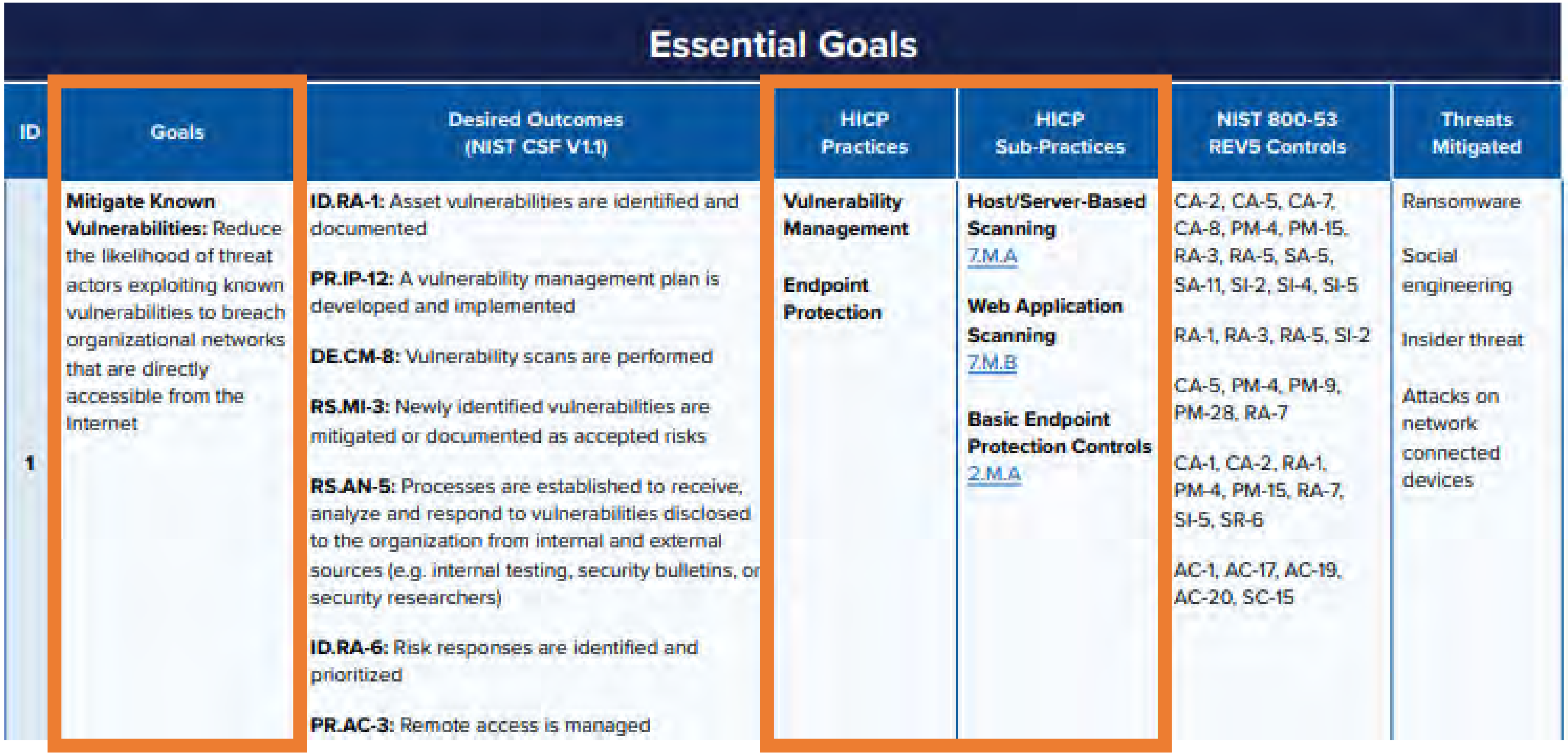
HICP Cybersecurity Practices	
CSP 1	Email Protection Systems
CSP 2	Endpoint Protection Systems
CSP 3	Access Management
CSP 4	Data Protection and Loss Prevention
CSP 5	Asset Management
CSP 6	Network Management
CSP 7	Vulnerability Management
CSP 8	Security Operations Center & Incident Response
CSP 9	Network Connected Medical Devices
CSP 10	Cybersecurity Oversight and Governance



HICP Technical Volume 1 (Small Healthcare Organizations)
https://405d.hhs.gov/Documents/tech-vol1-508.pdf

HICP Technical Volume 2 (Medium and Large Healthcare Organizations)
https://405d.hhs.gov/Documents/tech-vol2-508.pdf

HHS CPG & HICP CROSSWALK



Essential Goals						
ID	Goals	Desired Outcomes (NIST CSF V1.1)	HICP Practices	HICP Sub-Practices	NIST 800-53 REV5 Controls	Threats Mitigated
1	**Mitigate Known Vulnerabilities:** Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented **DE.CM-8:** Vulnerability scans are performed **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks **RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) **ID.RA-6:** Risk responses are identified and prioritized **PR.AC-3:** Remote access is managed	**Vulnerability Management** **Endpoint Protection**	**Host/Server-Based Scanning** 7.M.A **Web Application Scanning** 7.M.B **Basic Endpoint Protection Controls** 2.M.A	CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 RA-1, RA-3, RA-5, SI-2 CA-5, PM-4, PM-9, PM-28, RA-7 CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6 AC-1, AC-17, AC-19, AC-20, SC-15	Ransomware Social engineering Insider threat Attacks on network connected devices

https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf

PROPOSED LEGISLATION: HEALTHCARE CYBERSECURITY ACT OF 2024

- Sponsored by Sens. Jacky Rosen (D-Nev.), Todd Young (R-Ind.) and Angus King (I-Maine)
- Direct the Cybersecurity and Infrastructure Security Agency and the HHS to collaborate on improving cybersecurity in the sector and disseminate resources about cyber threat indicators and defense measures.
- Create special liaison to HHS within CISA that could help coordinate responses during cyberattacks.

https://www.congress.gov/bill/118th-congress/senate-bill/4697/text

WHAT DOES THIS MEAN FOR THE FUTURE OF CYBERSECURITY IN HEALTHCARE?

CYBERSECURITY SUCCESS IS A TEAM SPORT

- Create a culture of collaboration and shared ownership around cybersecurity
- Cybersecurity risk is another variation of patient safety risk and enterprise risk
- Regularly assess and calibrate cybersecurity roadmap and measure progress to a framework
- Processes should be stress tested to measure resilience
- Organizations must be flexible in responding to emerging threats and potential regulatory changes

THE NAME OF THE GAME IS CYBER RESILIENCE

Before Incident

During Incident

After Incident

Vulnerability Management

Identity and Access Management

Initial Detection Analysis

Forensics

Regulatory & Stakeholder Reporting

Incident Response Plan

Security Architecture

Impact Assessment

Threat Eradication

Attribution

Risk Analysis and Management

Security Program Governance

Crisis Management

System Restoration

Business Continuity Planning

Data Protection

Cyber Command

Regular Crisis Communication Updates

Industry Information Sharing

Threat Management

Asset Management

Containment

After Action Review

AREAS FOR COLLABORATION WITH SECURITY LEADERS

- Migrate away from/safeguard risky email workflows (e.g. AP, ERP approval)
- Initiate department and organizational business continuity discussions, tabletops and simulations
- Help establish disaster recovery and backup priorities
- Build a long-term strategy to fund technical debt remediation
- Regularly review finance team's system access and sensitive information storage
- Bring security into new initiative exploration early
- Integrate security into procurement processes
- Along with legal/regulatory leaders, keep a pulse on pending changes in regulatory environment and establish mechanism to fund potential new mandates

THANK YOU

Todd Hill

502-693-4253

todd.hill@bhsi.com