FORVIS™

Cyber Attacks on the Rise: Effects of Ransomware in Healthcare

January 25, 2024

IT Risk and Compliance - Healthcare

Ransomware in the *NEWS*

HEALTH TECH

Idaho hospital diverts ambulances, turns to paper charting following cyberattack

By Annie Burky • Jun 1, 2023 04:00pm

Cybersecurity | Emergency Care | Privacy and Security | cyberattack

After ransomware attack, state's second-largest health insurer says patient data stolen

Point32Health says current and former members of Harvard Pilgrim Health Care may have been affected

By Jessica Bartlett Globe Staff, Updated May 23, 2023, 7:38 p.m.

An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.

Hacking healthcare: With 385M patient records exposed, cybersecurity experts sound alarm on breach surge

Cybersecurity experts say healthcare companies must harden their defenses, but it may require regulators and lawmakers to raise the bar on security standards.

Cyberattack disrupts health-care system's services in several states

California-based Prospect Medical Holdings had some services shut down down at affiliated locations, and others were forced to rely on paper records

FORVIS

What is Ransomware?

FORVIS

Ransomware

Ransomware is a type of malware that encrypts victims' computer systems and data, rendering the systems unusable and the data unreadable. Ransomware restricts access to the data on infected machines until the ransom is paid.

The threat landscape has changed dramatically, with increased

velocity

volume

and

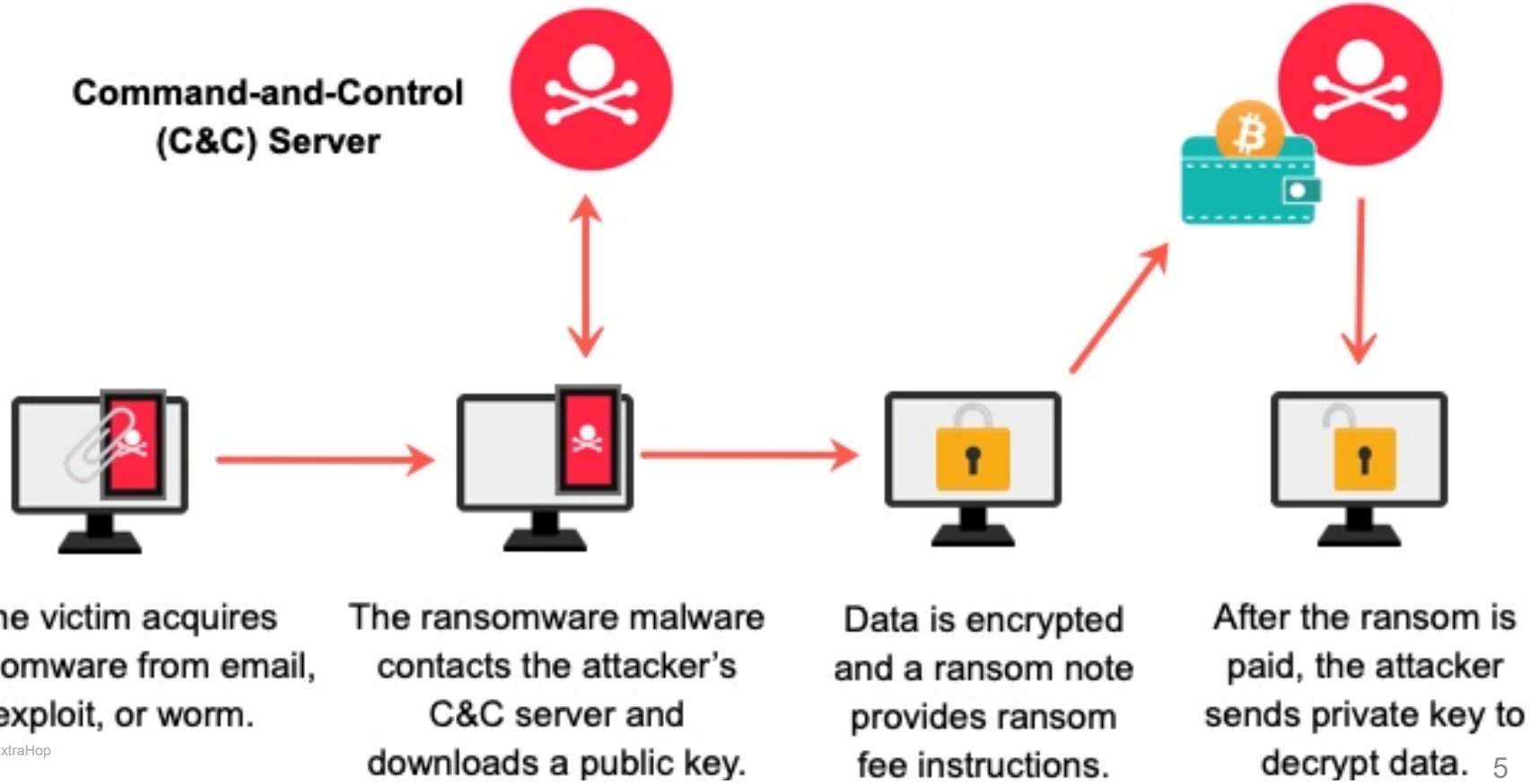
impact

of **criminal, hacktivist, and opportunistic attacks.** Ransomware defense and response have become the number one priority of most organizations.

FORVIS

How does Ransomware work

Ransomware is a type of malware that locks files on a victim machine, making data inaccessible. A ransom note appears on the victim's computer with instructions for paying the attacker (usually in a cryptocurrency such as Bitcoin) to unlock the files. Typical attacks are originated from email attachments, malicious links or malware.



Source: ExtraHop

FORVIS

The Change to the Cyber Crime Landscape – Top Variants

Ransomware Gangs

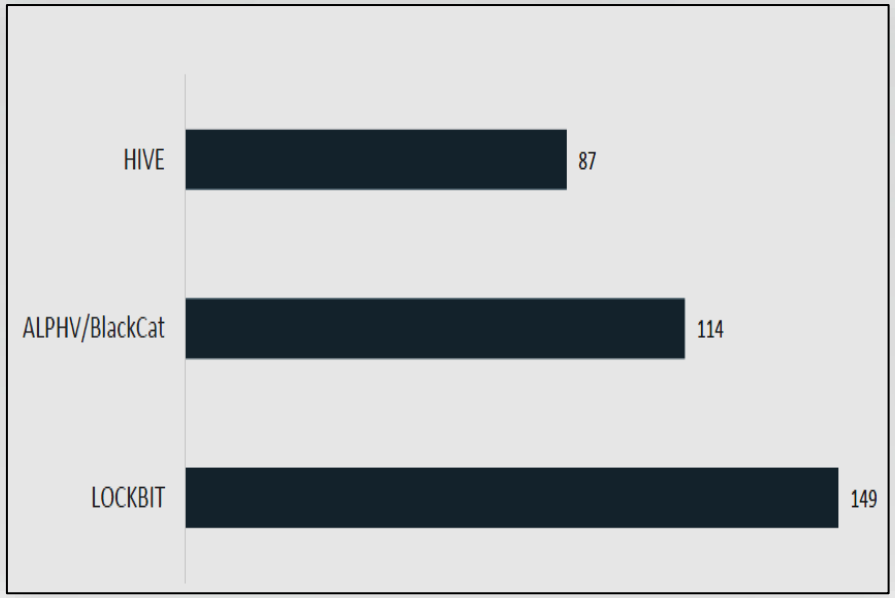
$456 million Ransom payments collected in 2022

The **United States** is the most targeted country targeted by **LOCKBIT3.0**.

Conti **expressed support for the Russian government** and threatened to target "enemies".

ALPHV/BlackCat is a veteran group that was responsible for the **Colonial Pipeline.**

Top Ransomware Variants Victimizing Critical Infrastructure – 2022 Incidents [1]



Ransomware Innovation

Internal files showed ransomware groups are exploring advanced new techniques. [2]

- Buying the same EDR tools we use to test their weaknesses
- Using blockchain smart contracts to expedite ransom payment
- Creating their own decentralized finance platforms

> Big companies have too many secrets that they hold on to, thinking that this is their main value, these patents and data.
>
> - Ransomware Leader

Threat actors are using AI to develop phishing emails, automate attacks, spread ransomware, rapidly exploit vulnerabilities, and develop complex malware code.

[1] 2022 FBI Internet Crime Report
[2] Conti Ransomware Group Diaries, Part IV: Cryptocrime – Krebs on Security. Krebsonsecurity.com.
[3] Political fallout in cybercrime circles upping the threat to Western targets – Cyber Scoop. cyberscoop.com.

FORVIS

Evolution of Ransomware

FORVIS

The Evolution of Ransomware - Timeline

1989

First Instance of Ransomware:

The AIDS Trojan (aka PC Cyborg)

- Created by Dr. Joseph Popp and Distributed to 20,000 attendees at the World Health Organization (WHO) AIDS conference.
- Released on **5 ¼ floppies**
- Demanded $189

2004/ 2005

Gpcoder

- Message displayed on a **user's home screen**, directing them to a .txt file posted on their desktop. The file contained details of how to pay the ransom and unlock the affected files.
- Demanded $200 ransom

2006

Archiveus Trojan

- Primarily a Windows-based attack
- Encrypted the MyDocuments Directory
- First ransomware to use **RSA encryption**

2009

Locker Ransomware (FBI MoneyPak)

- A category of ransomware that hit **mobile devices**
- Prominent examples: Winlock, Reventon

2013

Cryptolocker

- First ransomware to demand payment in **Bitcoin**

2014

CryptoWall

- Leveraged a **Java Vulnerability**
- Nearly 1,000 victims; estimated losses of at least $18 million

2016

Often called '"The Year of Ransomware"

Locky

- First widespread ransomware
- As many as 500,000 **Phishing** emails per day were sent out
- Other Ransomware made its debut in 2016 as well, including:

Cerber	Petya	SamSam
TeslaCrypt	Jigsaw	

WannaCry

- Attached an estimated 200,000 computers in 15 countries
- U.S. and U.K. officials claimed **North Korea** behind the attach

2017

NotPetya

- Variant of Petya that targeted victims in Ukraine, including the **National Bank of Ukraine**
- U.S. officials estimated damages from the ransomware at more than $**10 Billion**

2021

DarkSide

- **Colonial Pipeline** attack
- Pipeline was shut down for six days, Colonial paid $4.4 million bitcoin ransom

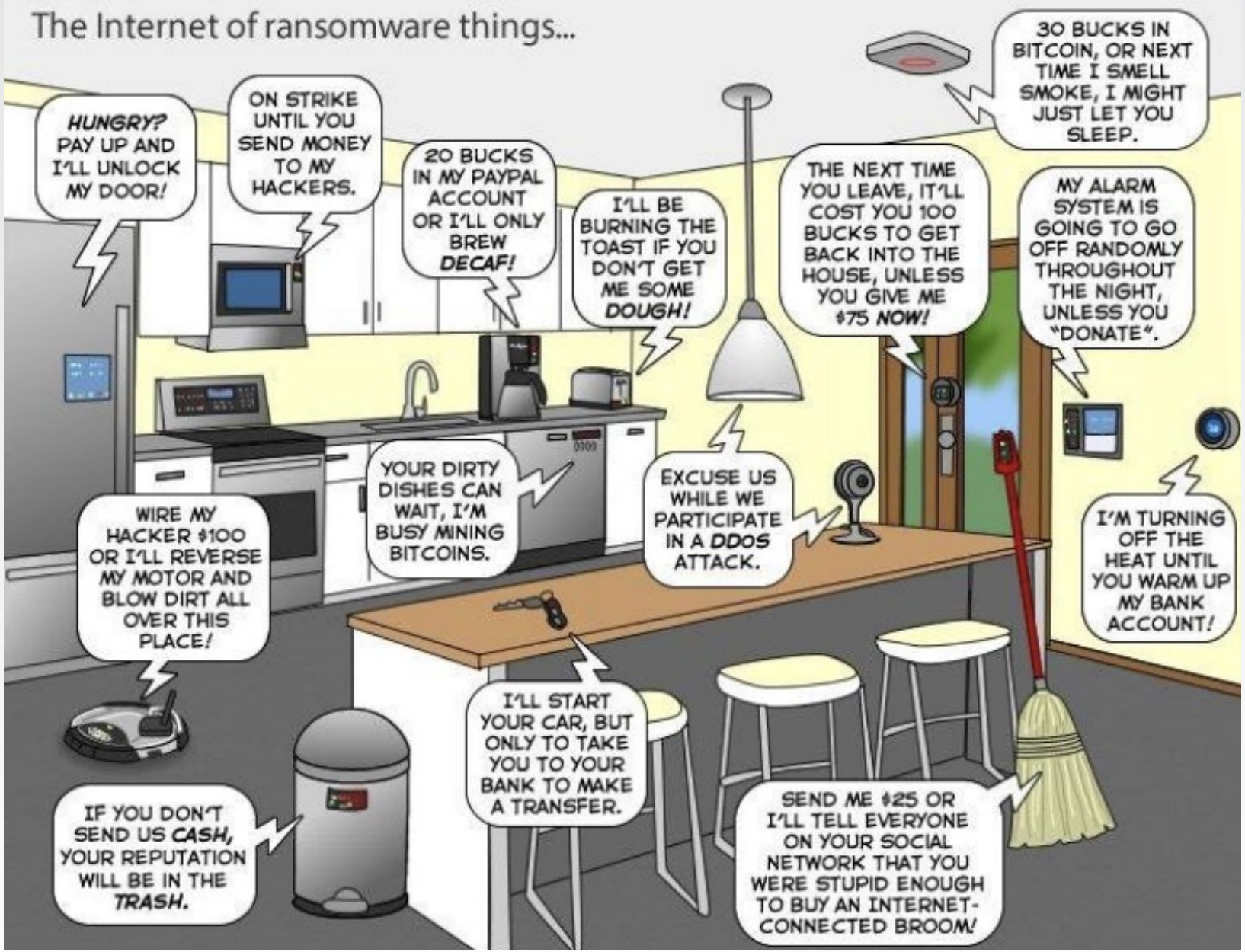
Source: Ransomeware.org

Note: This is not meant to be a comprehensive list of ransomware but rather an overview of major highlights in its history

FORVIS

What the Next Five Years May Hold!!!

Smart devices and internet connectivity offer new ways for businesses to create value for their customers; however, constant connectivity and data sharing also create new opportunities for data and personal information to be compromised.



Source: https://iotnewsletter.org/fintech-internet-of-things-the-internet-of-ransomware-things-iot

FORVIS

Artificial Intelligence Positives and Negatives

The effect of extensive security AI and automation on the financial impact of a breach

Security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches.

- Organizations that used these capabilities extensively within their approach experienced, on average, a **108-day shorter time** to identify and contain the breach.
- They also reported **USD $1.76 million lower data breach costs** compared to organizations that didn't use security AI and automation capabilities

---

Phishing / Deep Fakes

- AI can be used to automate and enrich phishing emails

Data Privacy / Breaches

- AI can be used to access and exploit personal data without permission or authorization

AI-assisted Fraud

- AI-assisted fraud can be used to bypass security measures and steal data.

Other Security Risks

- AI can be used to create security vulnerabilities or exploit weaknesses quickly

FORVIS

Cybersecurity Statistics & $$$ Impacts

FORVIS

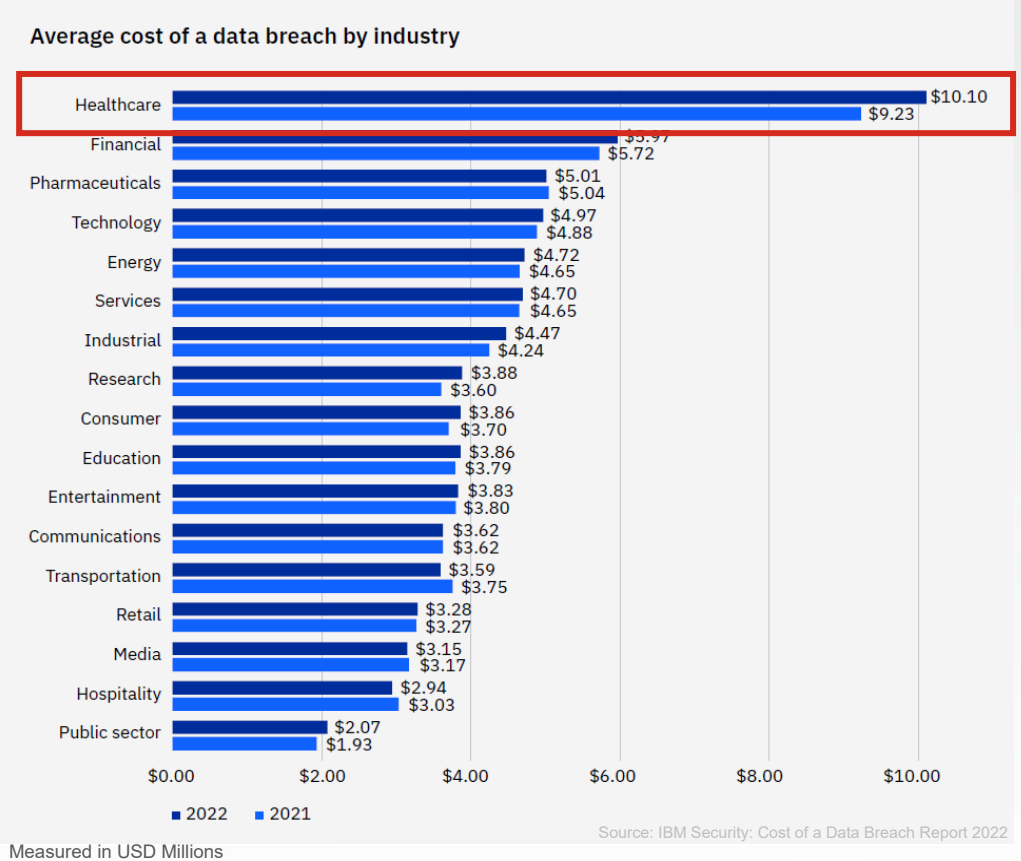
Data Breach Impacts

You can't afford to ignore Cybersecurity – Especially now!

FORVIS

Cost of a Data Breach including Ransomware

Healthcare was the highest-cost industry for the 13th year in a row.
The average total cost of a breach in healthcare increased from USD $9.23 million in the 2021 report to USD $10.10 million in 2022, an increase of USD $0.87 million or 9.4%. *Healthcare is one of the more highly regulated industries and is considered a critical infrastructure by the US government.*



Measured in USD Millions

USD $10.1 million
Average cost of a breach in the United States, the highest of any country

277 days
Average time to identify and contain a data breach

83%
Percentage of organizations that have had more than one breach

Data breaches in high data protection regulatory environments and **critical infrastructure** tended to see costs accrue in later years following the breach. In ***highly regulated industries***, an average of **24% of data breach costs were accrued more than two years** after the breach occurred. Regulatory and legal costs may have contributed to higher costs in the years following a breach.

FORVIS

Ransomware and Business Email Compromise Fast Facts

For 2022, the **FBI's Internet Crime Complaint Center (IC3)** received 2,385 complaints identified as **ransomware** with adjusted losses of more than **$35.4 million**.

In 2022, the IC3 received **21,832 complaints** of Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses at nearly **$2.7 billion.**

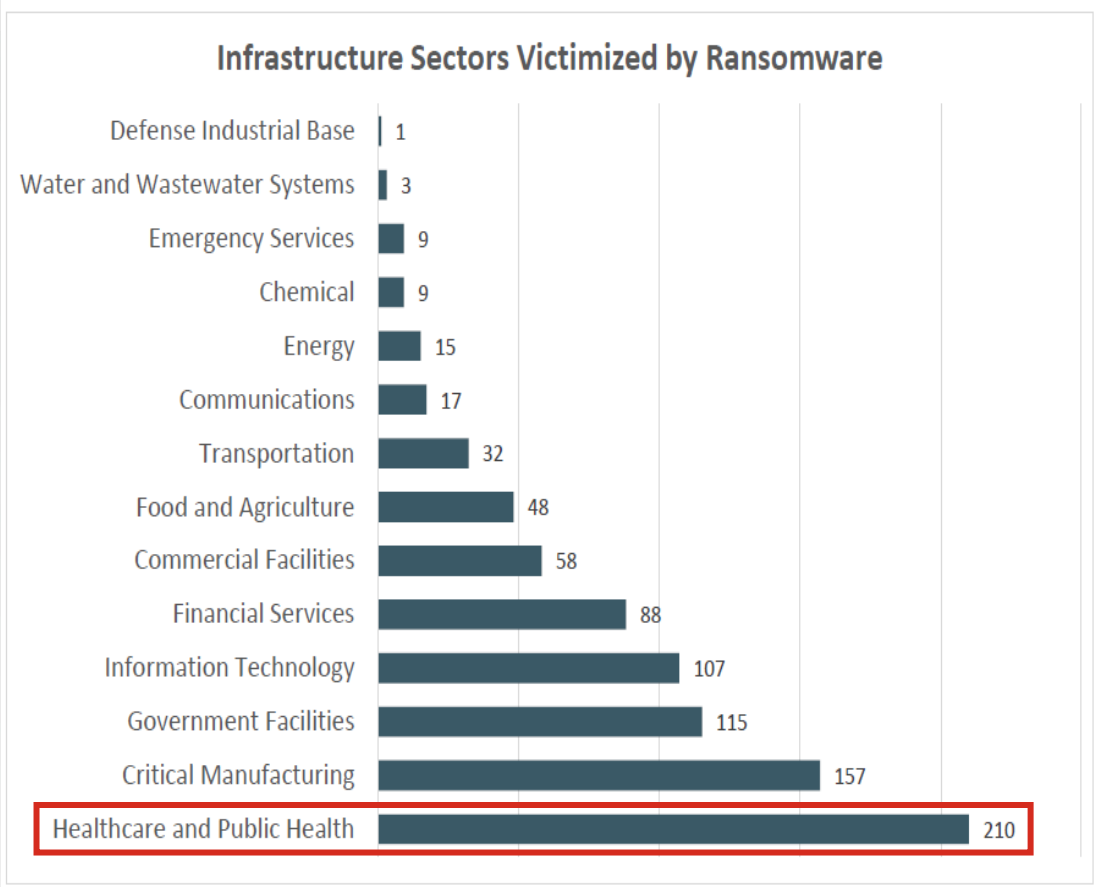
16-21 Days

The average downtime for a ransomware incident

$43 Billion

The total cost to organization over Business Email Compromise fraud since 2016

The IC3 anticipates an increase in critical infrastructure victimization in 2023.



Source:
2022 FBI Internet Crime Report
Committee of Homeland Security and Government Affairs

FORVIS

Responsibility to our **employees and customers**

When we equip people with new technology, we must equip them with the cybersecurity training and tools to safely and seamlessly integrate them into their workflow.

Cybersecurity is how we empower our people to make the most of digital investments.

The number of Internet devices worldwide is forecast to almost triple from **9.7 billion in 2020** to more than **29 billion in 2030**.

Source: Statista.com

The average hospital room contains from **fifteen to twenty connected medical devices.** Source: HIT Infrastructure

Digital transformation **promises better employee satisfaction** including enabling alternative workforce models.

85% of cybersecurity attacks attempted to **exploit the human element.**

Source: Verizon Data Breach Investigation Report 2021

FORVIS

Attack Vectors

FORVIS

Top Ransomware Infection Vector

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.

Best practices by vector to manage the risk of Ransomware

Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
- Regularly patch and update software and OSs to the latest available versions
- Employ best practices for use of Remote Desktop Protocols and other remote desktop services
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB.

Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Malware Infection

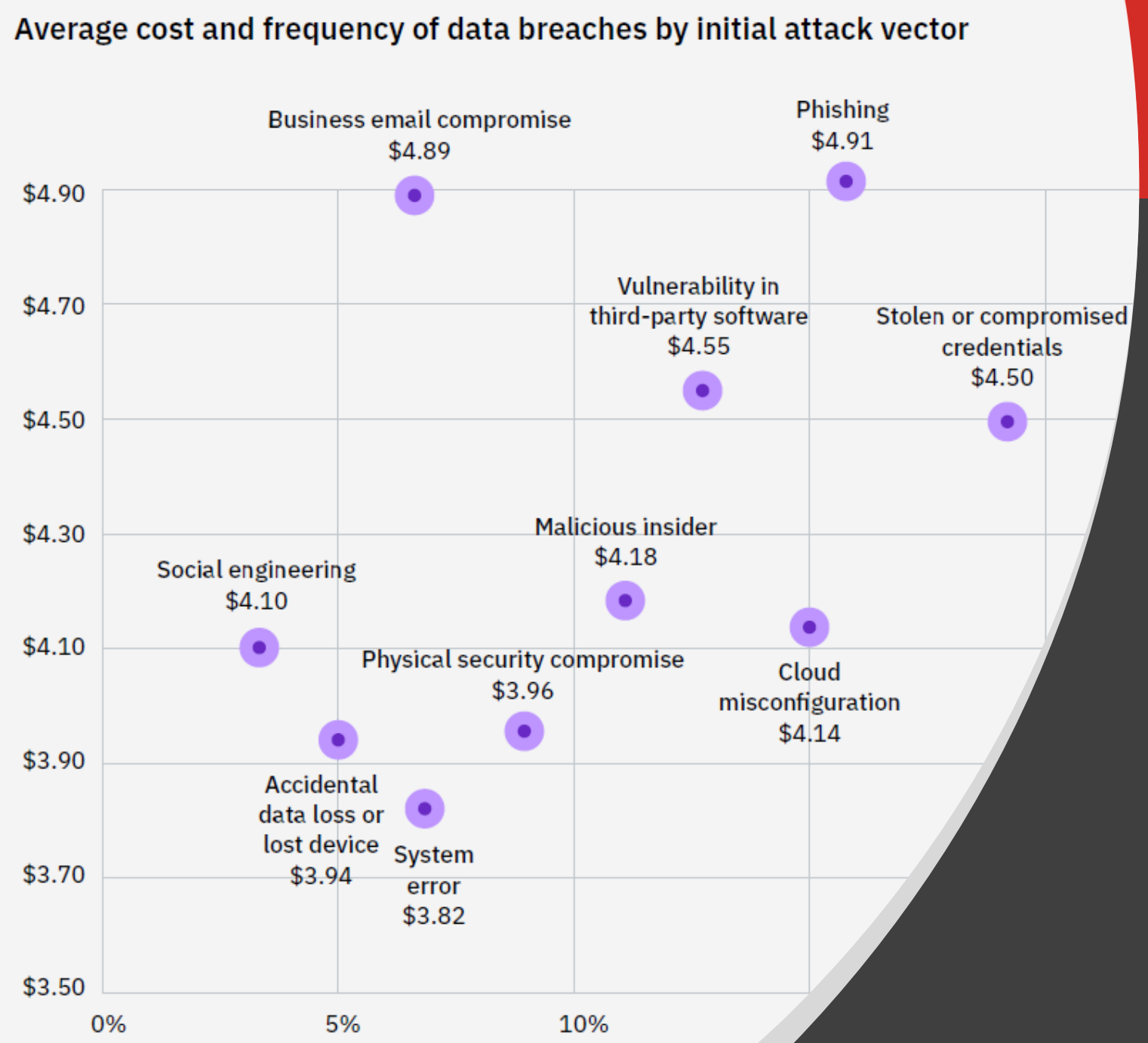
- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions.
- Use application directory allow listing on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs.

Source: CISA.gov, Ransomware Guide

Attack Vectors by the Numbers



The most common initial attack vector in 2022 was stolen or compromised credentials, responsible for 19% of breaches in the study, at an average cost of USD $4.50 million.

In 2022, the most common initial attack vectors were compromised credentials at 19% of breaches, phishing at 16% of breaches, cloud misconfiguration at 15% of breaches and vulnerability in third-party software at 13% of breaches.

The **costliest** initial attack vector in 2022 on average was phishing at USD $4.91 million. Followed by business email compromise at USD $4.89 million and 6% of breaches, vulnerability in third-party software at USD $4.55 million.

Source: IBM Security: Cost of a Data Breach Report 2022

FORV/S

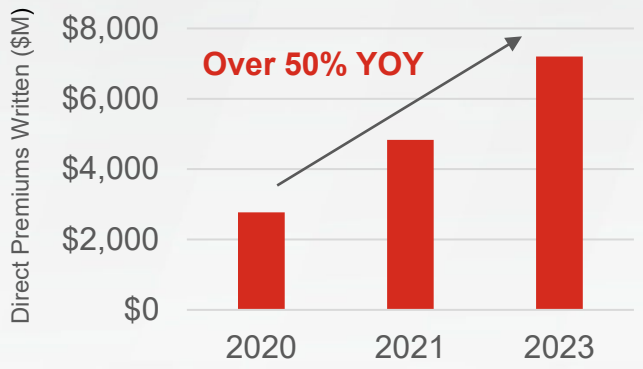
Cyber Insurance

FORVIS

Seismic Shift for Cyber Insurance

The cyber insurance market continues to grow with strong demand, but attackers have become more expensive which has increased the cost of cyber policies and claims.

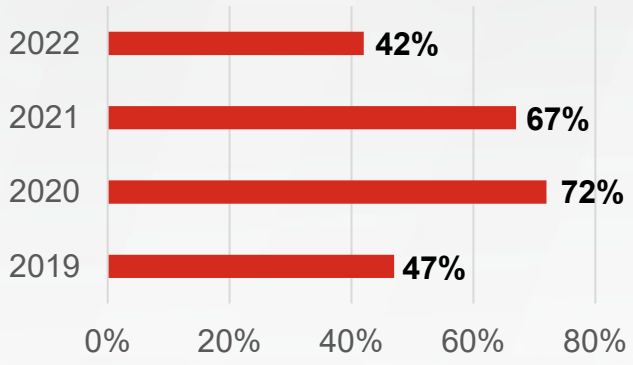
Total Cyber Policies increased to **$7.2 Billion** in 2022



100% ↑

Cyber insurance claims increased **100 percent** annually in each of the past three years over 2020, 2021 and 2022.

Direct loss ratios of US Cyber Insurers due to larger payouts



The rise in ransomware attacks over the past two years has led more organizations to seek cyber-insurance. **Ransomware insurance claims rose 35% in 2020, with the surge continuing in 2021**. As the cyber-insurance market hardens, insurers are looking for clients with security controls that meet higher standards.

Source:
S&P Global Market Intelligence
Fitch Ratings

FORVIS

Cyber Liability Insurance – Application Questions

Insurance underwriters assess the threat, business impact, and control effectiveness landscapes of the Applicant for the purposes of assessing overall cyber risk. Insurers want to know that your organization is taking steps to understand and act on cyber risks.

- Information security program
- Incident response program
- Business continuity, disaster recovery & vendor management policies & procedures address cybersecurity
- Cybersecurity awareness training
- Information sharing & analysis center (ISAC)
- Multifactor or two-factor for VPN, remote sessions, internet facing applications & privileged access
- Frequent cyber risk assessments, penetration tests, vulnerability assessments, & IT control audits
- Air gap backups to keep them out of reach of an attack
- Segment internal networks to isolate critical systems
- Data loss prevention

FORVIS

What can we do to not be the next News Headline?

FORVIS

Key Considerations: Focus on Governance Controls

- Maintain a strong **information security program**
- Maintain a strong **incident response program**
- Ensure **business continuity, disaster recovery** & **vendor management** policies & procedures address cybersecurity
- Consider how **cybersecurity insurance** should fit into your risk management program
- Ensure **cybersecurity awareness training** is performed regularly (educate & motivate)
- Join **an information sharing & analysis center (ISAC)** or other information sharing forums
- Perform **frequent cyber risk assessments**, penetration tests, vulnerability assessments, & IT control audits

FORV/S

Key Considerations: Focus on Technical Controls

- Use **multifactor** or **two-factor** for VPN, remote sessions, internet facing applications & privileged access
- Maintain accurate **asset inventories** for hardware & software, including **data classification**
- Implement strong cloud-based **data loss prevention** controls
- Enforce **application whitelisting** controls & **remove** unauthorized applications
- **Remove local administrator** rights to reduce malicious software installs
- **Tune existing security tools** – web content, email filtering, end point, etc.
- Deploy **cloud-based security** software & end-point protection.

FORV/S

Key Considerations: Focus on Operational Controls

- Track, report, independently test, & update security **patches** based on a risk priority schedule (Microsoft & non-Microsoft patches)
- Use **security information & event management (SIEM)** tools with **"defense in depth"** approach
- **Change** your passwords more frequently during this time
- Ensure **data encryption** is enforced to protect confidential data
- **Segment** internal networks to isolate critical systems
- **Air gap** your backups to keep them out of reach of an attack
- Make your air-gapped backups **immutable**!

FORV/S

Be Prepared through Best Practices

Backup and Recovery

It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization. Source: CISA.gov, Ransomware Guide

Incident Response Plan

Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident. Source: CISA.gov, Ransomware Guide

E-mail Security and Awareness

Scan all incoming and outgoing emails to detect and filter threats, such as phishing and spooking emails, and executable files. Implement training and awareness programs including regular phishing simulation exercises.

Configuration Hardening

- Restrict usage of PowerShell
- Disable Remote Desktop Protocol's
- Secure domain controllers including patching and updating
- Configure firewalls to block know malicious IP addresses.
- Restrict user permissions for installing and running software.
- Implement software restriction policies and application whitelisting.
- Network segmentation through virtualization and separation

Note: This is not meant to be a comprehensive list of ransomware best practices but rather an overview of key highlights to mitigate the risk of ransomware.

FORVIS

Implementing a Proactive Approach

Once an incident occurs and a regulatory inquiry is initiated – it's too late! It's important for organizations to establish a proactive approach to risk management and controls-based assessments. Assessments can be performed internally or externally in most cases.

Recommendations

Perform a Risk Assessment

A Risk Assessment can be framework-specific, entity-wide, or both. A Risk Assessment should evaluate inherent and residual risks to the organization. A risk score should be associated with each functional area of the Risk Assessment.

Perform a Controls-based Assessment

Utilize a well-developed framework (e.g. NIST) to assess the organization's security and/or privacy controls. Develop corrective action plans to formalize, assign, and track identified vulnerabilities to completion.

FORVIS

Incident Response

FORVIS

Case Study

Organization background:

- Community-based hospital with onsite outpatient medical offices
- 135+ bed hospital
- Approximately 1,150 employees

Recent security incidents led to the client reaching out with concerns regarding their incident response procedures. After discovery sessions, FORVIS developed a plan to perform a three-scenario table-top exercise to evaluate incident response at the entity level. The three scenarios were: ransomware, physical disaster, and business associate security incident. FORVIS performed its Ransomware Simulation service to identify results and impact of a successful attack, while the physical disaster and business associate-related scenarios were hypothetical.

FORVIS

Table-top Exercise

What is a table-top exercise?
A coordinated effort to discuss hypothetical emergency scenarios and how key stakeholders of an organization might react. The exercise should be guided by the organization's incident response plan and capture lessons learned from the discussions.

Goals and Objectives

1. Better understand roles
2. Create a safe space for critical thinking
3. Instill confidence
4. Education and training
5. Process improvement

FORVIS

Case Study Analysis

- Communication was a big issue
- Decision-making processes were unclear
- Defining roles was critical
- Collaboration is hard but key to success
- Hesitation to declare a disaster was prominent
- Education and training were desperately needed

FORVIS

Questions

forvis.com

FORVIS

Assurance / Tax / Advisory

Thank You!

forvis.com

FORVIS

Assurance / Tax / Advisory