Can HIPAA Really Save You?

A look at healthcare's 3 biggest threats.

Snowfensive

Snowfensive

President of Snowfensive

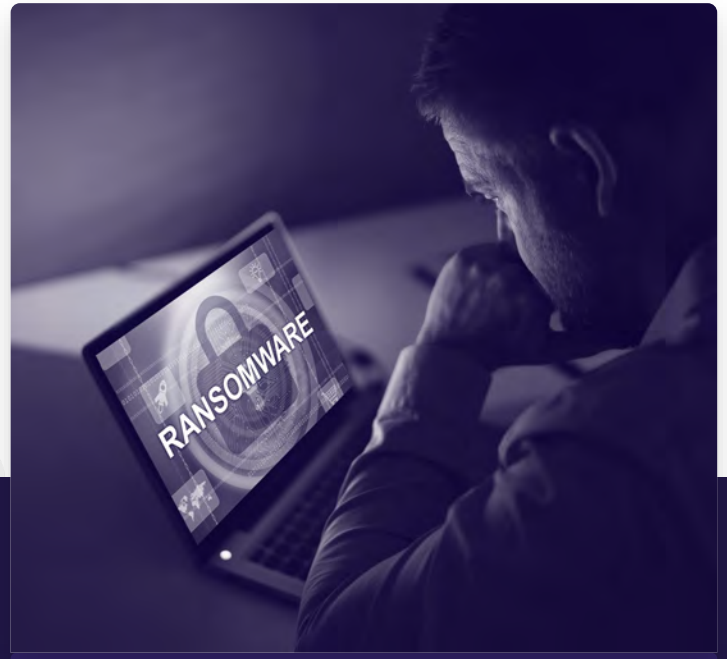
JC Carruthers

- Over 10 years of experience in Cybersecurity
- Penetration Testing and Incident Response
- USMC Veteran
- Salt Lake City, Utah

Snowfensive

3 Biggest Threats

Agenda



Ransomware

Cloud Security

Internet of Things

Snowfensive

WHY SHOULD YOU CARE?

- Organizations often associate being compliant with being secure.
- The healthcare industry has a great commodity to offer attackers: Data.
- As your organizations innovate and improve, so do attackers.

82% Percentage of healthcare companies that admitted to being attacked within the last 12 months.

2020 Vision Report – CyberMDX
https://www.cybermdx.com/news/vision-2020

Snowfensive

Ransomware

A look at:

- Ransomware Milestones
- How Ransomware Works
- Recommendations

TIMELINE

RANSOMWARE MILESTONES

AIDS Trojan

The virus was mailed to over 20,000 researchers promising to help identify an individual's risk of contracting AIDS. The virus would then encrypt the filenames and demand $189 via mail to a PO Box in Panama.

1989

The Renaissance

Ransomware started reappearing with a few variants including GPCode, Krotten, Cryzip, and Archievus. Some of these used their own implementation of cryptography and, as a result, were easy to fix without paying. However, all of them still had a payment problem.

2004-2008

Bitcoin Invented

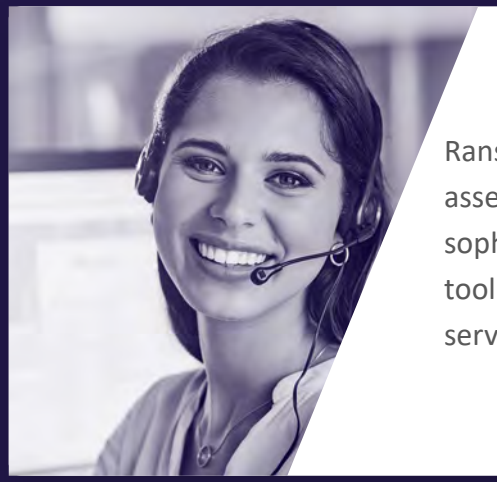
The decentralized cryptocurrency was invented and quickly adopted by black markets and cybercriminals.

2009

A Profitable Attack Model

With cryptocurrency and weak security postures still plaguing organizations, Ransomware became a very profitable attack model for cybercriminals. Variants started appearing such as TeslaCrypt, Citadel, CryptoLocker, and CryptoWall. These started using strong crypto libraries preventing the ability to decrypt.

2010-2015



RaaS

Ransomware-as-a-Service becomes an asset to cybercriminals who lack the sophistication in writing their own toolkit. Many offerings have customer service and tech support.

2015

The Surge

RaaS offerings start hitting the market with variants such as TOX, Fakben, Radamant, Ransom32, and Shark. The attack paradigm is also shifted, making a new market for attackers to find vulnerable systems and sell access for others to install ransomware kits.

2015-2019

Data Auctions

Ransomware such as REvil and Maze starts offering Data Auctions for stolen data taken during ransomware campaigns. This complicates the response process.

2019

Snowfensive

Death

Attackers were able to execute ransomware against 30 servers taking down some of a German hospital's infrastructure. Inside that hospital, a woman who was being prepped for an emergency surgery had to be turned away to another hospital and died in transit.

September
2020

Snowfensive

4 MAIN STEPS

How Ransomware Works

Step One

Compromise

The attacker executes code via some initial infection vector such as phishing or remote service such as RDP.

Step Two

Communication

The ransomware talks back to a Command & Control Server.

Step Three

Encryption

Files are targeted for encryption based on file extensions predetermined by the attacker.

Step Four

Spreading

Using vulnerabilities within the network, the ransomware tries to infect other systems.

Ransomware infections delivered via phishing.

https://www.idagent.com/blog/whats-behind-the-huge-rise-in-healthcare-data-breaches/

65%

IMPACT OF RANSOMWARE

01 Financial. Any ransom payments, costs from loss of productivity, remediation costs.

02 Loss of Data. In some cases, even if you pay the ransom, the data is corrupted, or the information is never decrypted.

03 Theft of Data. With the change in ransomware tactics, this is becoming more of a common threat.

04 Brand Reputation. Especially with the theft of data, this is an outcome that can cost you future business.

Snowfensive

FOCUS ON THE FOUR STEPS

RECOMMENDATIONS

1. **Compromise**
    - Ensure systems are running anti-virus. If budget allows, consider implementing an Endpoint Detection & Response ("EDR") solution instead.
    - Implement patch management policies and procedures for all workstations and servers.
    - Provide users with periodic security awareness training **and assessments**, such as phishing tests.
    - Perform **external** penetration testing at least annually to identify systems that may be remotely accessible and/or able to be compromised.
2. **Communication**
    - Implement an Intrusion Detection/Prevention System ("IDS/IPS").
    - If possible, restrict outbound communication. **Spoiler Alert: This is hard!**
3. **Encryption**
    - Ensure timely and valid backups are occurring of business-critical data.
    - Ransomware often targets backups. Ensure at least one copy of the backup is stored offsite.
    - Consider recovery timelines when creating backup plans.
4. **Spreading**
    - Segment your network! At a minimum, segment your workstations from servers.
    - Perform internal penetration testing at least annually to identify ways attacks can move within your network and compromise systems.

45 C.F.R.

HIPAA RULES

§164.308(a)(1)(ii)(A) – Risk Analysis

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

§164.308(a)(5)(ii)(A-D) -Security Awareness and Training

Implement:

- *Periodic security updates.*
- *Procedures for guarding against, detecting, and reporting malicious software.*
- *Procedures for monitoring log-in attempts and reporting discrepancies.*
- *Procedures for creating, changing, and safeguarding passwords.*

§ 164.308(a)(8) Evaluation

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security …

§164.308(a)(7) Contingency Plan

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Snowfensive

Cloud Security

A look at:

- Freedom Healthcare Case
- Risks in the Cloud
- Recommendations

Snowfensive

PASSWORDLESS DATABASE

Freedom Healthcare Staffing

A security researcher named Jeremiah Fowler identified an unprotected database belonging to Freedom Healthcare Staffing containing **957,000** records.

“In a sampling of the documents I read for verification purposes, I saw failed drug tests (without prescriptions for those drugs), a nurse being accused of taking a patient’s painkillers, complaints about a hospital’s illegal interference in nurses trying to unionize, and many more complicated situations,” Fowler wrote.

SEPTEMBER 2019

THE COMMON THREATS

CLOUD RISKS

Privileges

Depending on the product, there may not be significant levels of privilege assignment, making it challenging to implement the concept of “least privilege.” This may allow users access to data they shouldn’t have.

Lack of MFA

It’s very rare to find cloud-based software offerings that mandate MFA. However, some often include it, but the organization does not enable the feature.

Improper Configuration

Different cloud systems operate in different ways, especially with regards to security and default configurations. Additionally, the server software installed within the cloud instances sometimes come with minimal security enabled by default. Logging is also a concern.

Vendor Management

They say the cloud is just someone else’s computer. As such, many of the concerns organizations seek to remedy with cloud solutions don’t go away. Due diligence into the vendor’s security program and certifications is a minimum.

Snowfensive

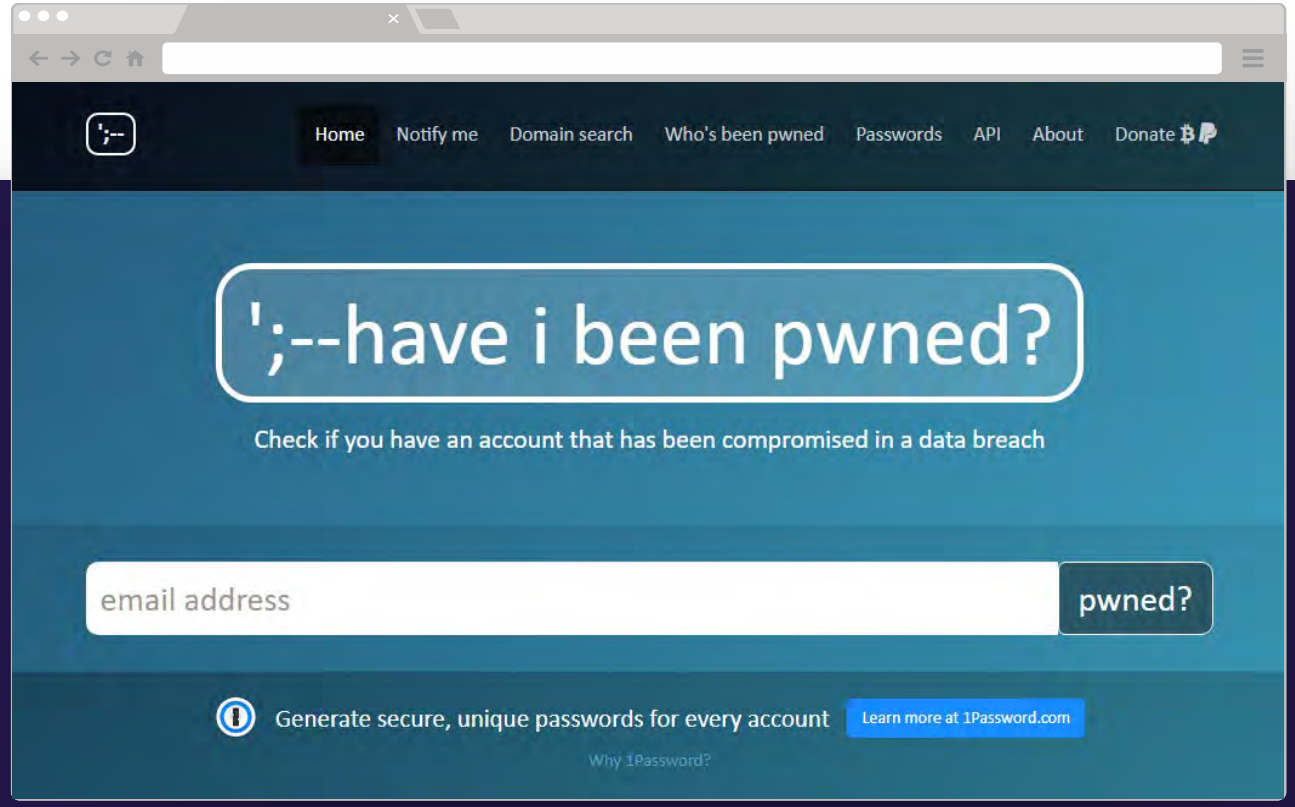
CREDENTIAL RISK

HAVEIBEENPWNED?

01 When web applications get breached such as LinkedIn, DropBox, Adobe, and even MySpace, user data is taken, including passwords.

02 Eventually, many of these breaches are publicly disclosed, including all of the sensitive data.

03 Attackers leverage this data using a concept called Password Reuse to attempt to gain access to your organization's user accounts.



https://haveibeenpwned.com

Breaches you were pwned in

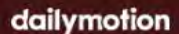
A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Baby Names: In approximately 2008, the site to help parents name their children known as Baby Names suffered a data breach. The incident exposed 846k email addresses and passwords stored as salted MD5 hashes. When contacted in October 2018, Baby Names advised that "the breach happened at least ten years ago" and that members were notified at the time.

Compromised data: Email addresses, Passwords

Chegg: In April 2018, the textbook rental service Chegg suffered a data breach that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Names, Passwords, Usernames



Dailymotion: In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames

Disqus: In October 2017, the blog commenting service Disqus announced they'd suffered a data breach. The breach dated back to July 2012 but wasn't identified until years later when the data finally surfaced. The breach contained over 17.5 million unique email addresses and usernames. Users who created logins on Disqus had salted SHA1 hashes of passwords whilst users who logged in via social providers only had references to those accounts.

Compromised data: Email addresses, Passwords, Usernames

Domino's: In June 2014, Domino's Pizza in France and Belgium was hacked by a group going by the name "Rex Mundi" and their customer data held to ransom. Domino's refused to pay the ransom and six months later, the attackers released the data along with troves of other hacked accounts. Amongst the customer data was passwords stored with a weak MD5 hashing algorithm and no salt.

Compromised data: Email addresses, Names, Passwords, Phone numbers, Physical addresses

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

Snowfensive

RECOMMENDATIONS

1. **Privileges**
    - Prevent account sharing. It often happens out of convenience or budget.
    - Remove excessive permissions (Capital One Breach).
    - Perform audits to review the permissions of both groups and users.
    - Tie job roles and functions to permission groups. Ensure these are changed if a user's job role changes.
2. **Credentials**
    - Ensure users use strong and complex passwords. Not Winter2020!
    - Enable & mandate MFA where possible. Use token applications over SMS.
    - Require user awareness training to discuss the benefits of MFA and warn about password reuse.
    - HIPAA requires the ability to "monitoring log-in attempts" – does the application provide this feature?
3. **Configuration**
    - Perform configuration reviews, assessments, or even penetration tests to evaluate configurations to find weaknesses that can be exploited.
    - If possible, ensure data is encrypted while at rest and in transmission.
    - Enable logging. The more logging, the better.
    - Ensure the logs are kept for retention.
4. **Vendor Management**
    - Expect, but Inspect. Validate your vendor's security posture by requesting their annual risk assessments. Independent assessments are preferred.

45 C.F.R.

HIPAA RULES

§164.312(b)(1)(ii)(A) – Audit Controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information …

§164.308(a)(5)(ii)(C-D) -Security Awareness and Training

Implement:

- *Procedures for monitoring log-in attempts and reporting discrepancies.*
- *Procedures for creating, changing, and safeguarding passwords.*

§ 164.308(a)(3)(i) Workforce Security

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information …

§164.308(b)(2) Business Associate Contracts

A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

Snowfensive

Internet of Things

A look at:

- Thermometer Hack Case
- Medtronic Insulin Pump Hack App Case
- IoT Security Challenges
- Recommendations

JACKPOT

Unnamed Casino

Attackers were able to hack an internet-connected thermometer used in the aquarium located in the casino lobby.

The attackers were able to access the database containing ‘high-rollers’ gambler information. They exfiltrated the data to the internet via the same thermometer.

APRIL 2018

Fatal FOB

Medtronic Insulin Pump

Security researchers Billy Rios and Jonathan Butts were able to reverse engineer the wireless protocol between the Medtronic Insulin Pump and its associated remote. The researchers were able to duplicate the commands and in order to reply them to nearby pumps.

As long as the attackers were in a somewhat close wireless range, they could withhold or overdose insulin to individuals with the pump.

JULY 2019

Snowfensive

THE BLACK BOX

DANGERS OF IoT DEVICES

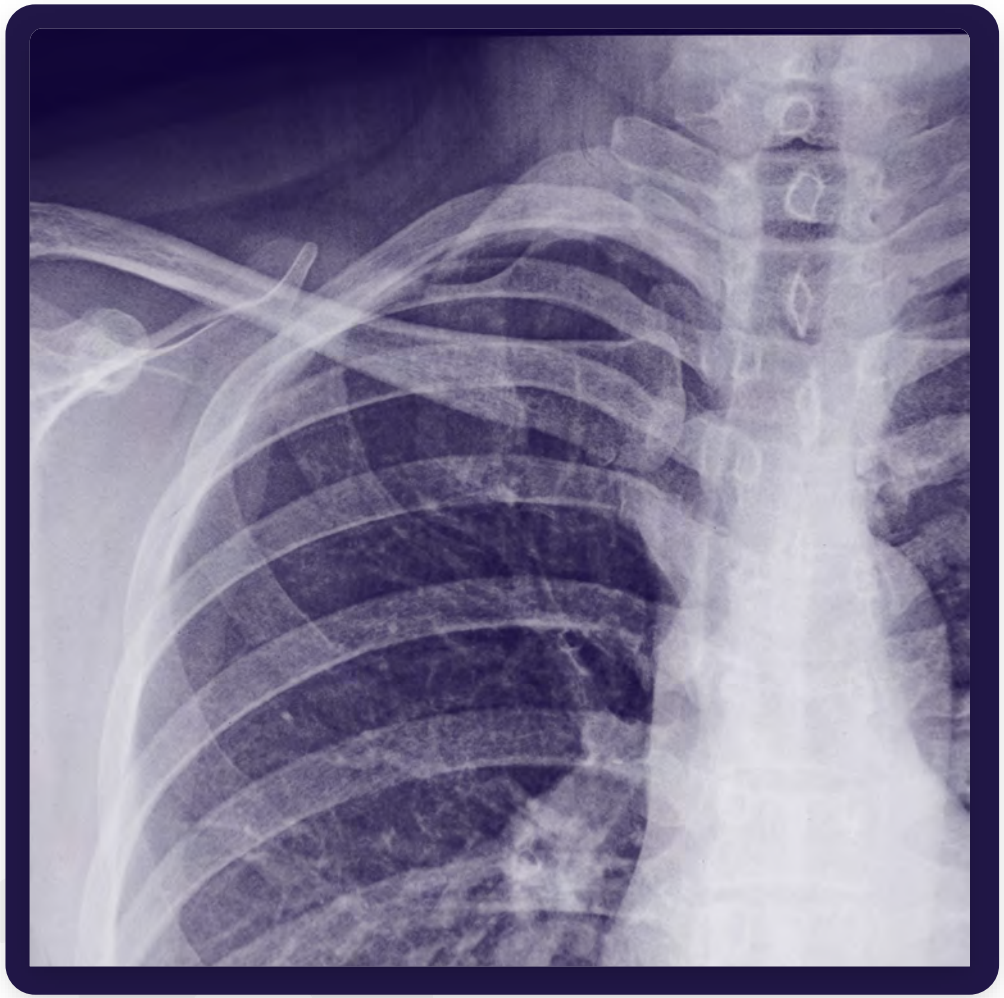
Operating System Market Share*:

- 42.02% - Android
- 34.57% - Windows
- 17.34% - iOS
- 3.72% - Mac OS
- 0.95% - Linux
- 0.29% - Unknown

IoT devices are not getting scrutiny from a security perspective the same way as larger operating systems are. As such, they're usually more at risk for vulnerabilities and other security issues including:

- Weak and sometimes hardcoded passwords
- Insecure Complex IoT Environments
- Vulnerable services and protocols

**https://netmarketshare.com/operating-system-market-share.aspx (last 12 months)*



I'M NOT A DOCTOR, BUT I PLAY ONE IN YOUR NETWORK

VULNERABLE X-RAY SYSTEM

Internal network penetration tests typically uncover many poor security practices, including ways to connect to systems like medical devices. In one case, our testing leads us to identify an x-ray system used to store patient x-rays and their identifiable information. The system contained the ability to remotely connect to the system protected by a very weak password.

The radiation technicians used this feature to connect to the system. However, as an attacker, we were able to as well. This access allowed us to see x-ray images and patient data from the system.

Snowfensive

THINGS TO PONDER

RECOMMENDATIONS

1. **Responsibility**
    - Who owns the device? Who **really** owns the device?
    - Where is the data stored?
        - Oh, look, we're back to the cloud.
    - Can it be patched? Who is responsible for patching?
2. **Secure Design**
    - Has the device been designed with security in mind? I doubt it …
    - Does it perform logging?
    - Is it sold in California? That may be a good thing!
        - Effective Jan 1, 2020, is the California Internet of Things Security Law.
        - The Act requires all "connected devices" sold or offered for sale in California to have "reasonable security" measures.
    - Is the data which is being transmitted encrypted? Probably …
3. **Vendor Management**
    - Are there reports to validate that security assessments have been performed?
    - Do you have the authorization to perform independent testing?
    - Are BAAs in place and consideration to HITRUST on who is responsible if there is a data breach?
    - How do you respond if there is a data breach?
4. **Disconnect**
    - Can it be disconnected? Either as part of incident response or because it really isn't needed online. Consider the insulin pump FOB.

45 C.F.R.

HIPAA RULES

§164.306(a)(1) – General Rules

Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

§164.312(a)(2)(i) – Unique user identification

Assign a unique name and/or number for identifying and tracking user identity.

§164.312(b) –Audit Controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Snowfensive

THE END

RECAP

Ransomware

Backup!

Test and ensure your critical business data is backed up, and you test that backup frequently.

Cloud

MFA, MFA, MFA

Ensure anything and everything that can support MFA has MFA turned on. Do it now.

IoT

Be Skeptical

The most dangerous paradigm shift is happening now and in the coming years. It won't go away, but that doesn't mean we trust it.

Q&A

Please prepare your questions during the recap.


THANK YOU
Snowfensive
2020

info@Snowfensive.com

2020