ISSN = 1377-7629

HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 24 • ISSUE 3 • € 22

ISSN = 1377-7629

Most Regrettable Business Decisions

ERRORS - MISSED OPPORTUNITIES - PITFALLS - TAKEAWAYS

Why Cybercriminals Target Healthcare Data and How Organisations Can Protect Themselves

Healthcare data garners significant value on the dark web. This article provides an overview of why cybercriminals specifically target healthcare organisations and how these organisations can better protect themselves.

ERROL WEISS

Chief Security Officer | Health-ISAC | USA

key points

- Humans are unchangeable, and the personal and medical data contained in EHRs remain perpetually valuable.
- EHRs are targeted primarily because of the prolonged usability of the data, which gives cybercriminals ample opportunity to sell and exploit the information.
- Beyond the immediate threat of ransomware, the comprehensive nature of EHRs makes them particularly appealing to cybercriminals.
- The massive appeal of healthcare data warrants additional cybersecurity measures to prevent sensitive information from falling into the wrong hands.
- Healthcare organisations must protect EHRs from cybercriminals by bolstering cybersecurity defences and making it much harder for a cyberattack to inhibit operations.

With the growing awareness of identity theft and other forms of cybercrime, the general public has become much more vigilant about protecting sensitive personal data like social security numbers, bank account numbers, and credit card information. However, this data isn't as valuable to cybercriminals as you might think. Healthcare data, by comparison, garners significantly more value on the dark web, where personal data – along with firearms, drugs, and other illegal items – are routinely sold and traded.

Just to give you an idea of how valuable healthcare data is on the dark web, a recent study found that electronic health records (EHRs) can sell for up to $1,000 each, compared to a mere $5 for a stolen credit card number and just $1 for a social security number. Why such a discrepancy? The main reason is that unlike credit cards and bank accounts, which can be closed and reissued, humans remain unchangeable, and the personal and medical data contained in EHRs, consequently, remain perpetually valuable.

While healthcare organisations understand the value of the data they are entrusted with, they may not have the support and resources to adequately fund the cybersecurity resources needed to properly protect that information. Data breaches in the healthcare sector are more frequent than in other industries and more financially damaging due to revenue losses, incident response and recovery costs, and large regulatory fines. The average cost of a breach in healthcare is $10 million, emphasising the urgent need for robust and comprehensive cybersecurity strategies. In light of the costs and reputational issues, this should serve as a catalyst for healthcare organisations to enhance their cybersecurity measures proactively.

Why are EHRs so Valuable?

EHRs are targeted primarily because of the prolonged usability of the data they hold, which gives cybercriminals ample opportunity to sell and exploit the information in various illicit ways. One common method that cybercriminals use is ransomware attacks, in which EHR data is held hostage. Healthcare organisations, under pressure to deliver uninterrupted life-saving patient care, often find themselves in a vulnerable position, making them more inclined to pay ransoms promptly.

Beyond the immediate threat of ransomware, the comprehensive nature of EHRs makes them particularly appealing to cybercriminals. These records are a repository of personal information, encompassing everything from patient addresses and insurance details to social security numbers and before and after surgery photos. The depth and variety of this data opens up multiple avenues for fraudulent schemes.

For instance, criminals might use detailed medical histories in EHRs to submit fake insurance claims or use that information to perpetrate financial fraud. Another example is prescription fraud, where perpetrators could use a patient's identity to obtain prescription medications, either for personal use or for illegal distribution. Medical insurance fraud can lead to financial loss and also poses significant risks to public health and safety.

Similarly, healthcare organisations should consider adopting stringent access controls to ensure that only authorised personnel can access EHRs or other private data. For instance, a role-based access control system should be used in which access to EHRs can only be granted to individuals with certain job responsibilities, as opposed to every registered employee.

In a larger sense, MFA and access control are two aspects of what's called zero-trust architecture, which should become the standard for cybersecurity models in healthcare. Zero-trust requires strict identity verification for every person and device trying to access an organisation's network, as opposed to implicitly trusting certain users and devices that have previously accessed the network time and time again.

Another key aspect of zero-trust architecture is least privilege access, in which users and devices are granted the minimum level of access required to complete their usual tasks. In healthcare, this could mean granting certain users permission to view the data in an EHR but restricting them from manipulating the data. Once the task is completed, the access rights are revoked, and the user and device must be verified again when access is needed.

> Data breaches in the healthcare sector are not only more frequent than in other industries but also more financially damaging

Boosting Cybersecurity in Healthcare

The massive appeal of healthcare data for cybercriminals clearly warrants additional cybersecurity measures to prevent sensitive information from falling into the wrong hands. Multi-factor authentication (MFA), for instance, adds another layer of security beyond passwords by only granting access to a website or application after the user has cleared two identification hurdles, often through the use of an out-of-band token, such as a six-digit number sent to a mobile phone.

While cybercriminals may be able to obtain a user's password, the second form of authentication is intended to be much harder to bypass: an attacker is very unlikely to be in possession of both a potential victim's password and their mobile phone, for example. MFA can be especially effective when that second step involves biometric authentication, which relies on the unique biological characteristics of an individual to verify their identity. Unlike a password, biometric information – such as an individual's fingerprints, face, or iris – is much harder to steal since it is inherently connected to the person.

Tools for Cyber Threat Intelligence

Advanced tools like honeytokens are crucial for enhancing cyber threat intelligence in healthcare organisations. Honeytokens act as digital decoys embedded within an organisation's digital infrastructure. They serve as traps for intruders attempting unauthorised access. When an adversary penetrates the system and interacts with a honeytoken, it distracts and misleads them and also triggers an alert to the security team, who can quickly identify and respond to the intrusion before a breach.

The use of honeytokens extends beyond immediate detection. When malicious actors engage with a honeytoken, it collects real-time data on the tactics used in an attack and reveals exactly what information the

hacker is attempting to exploit. This information is crucial in identifying specific vulnerabilities in the organisation's security framework and understanding the evolving nature of cyber threats.

Final Thoughts

Until the healthcare sector addresses its high vulnerability to cybercrime, cybercriminals and nation state threat actors will continue to target organisations that have yet to dedicate the necessary staff and resources to improving cybersecurity. Healthcare organisations must protect EHRs from cyber adversaries by bolstering their cybersecurity defences and making it much harder for a cyberattack to inhibit their operations.

> Healthcare organisations often find themselves in a vulnerable position, making them more inclined to pay ransom

Sharing first-hand experiences with cyberattacks throughout the healthcare community becomes a pivotal aspect of collective cybersecurity efforts. By exchanging insights gained from honeytoken engagements, healthcare organisations contribute to a broader understanding of cyber threats within the industry. This collaborative approach is essential to building a comprehensive picture of common attack patterns and tactics. Likewise, a deeper understanding of specific vulnerabilities and attack methods allows security teams to implement more robust cyber defence strategies.

The point is that a united front in sharing information and experiences plays a key role in fortifying the healthcare sector against cyberattacks.

Conflict of Interest

None.