Healthcare and Cyber security Practices

Protecting patient data, medical records and health-care systems from sophisticated cyber attacks

While innovation and developments in information technology is a cause for optimism, increasing sophistication in health care industry holds the promise to help address some of our most intractable problems, such-as in clinical care, fundamental research, population health or health system design. Technology will work for us only if it is secure. Information systems are crucial to present and future healthcare system. It is our responsibility to take complete precautions and proactive steps to ensure they are safe and protected.

Cyberattacks have become an increasing phenomenon across all verticals in an IT infrastructure of any industry. Healthcare is not ruled out here. It is a serious concern, especially in healthcare sector, where PHI, patient demographics and various diagnostic systems are compromised.

Who is a threat?

Health sector faces threats from multiple actors such as external attackers, malicious insiders and unsecure third-party data sharing and integration

What is the impact?

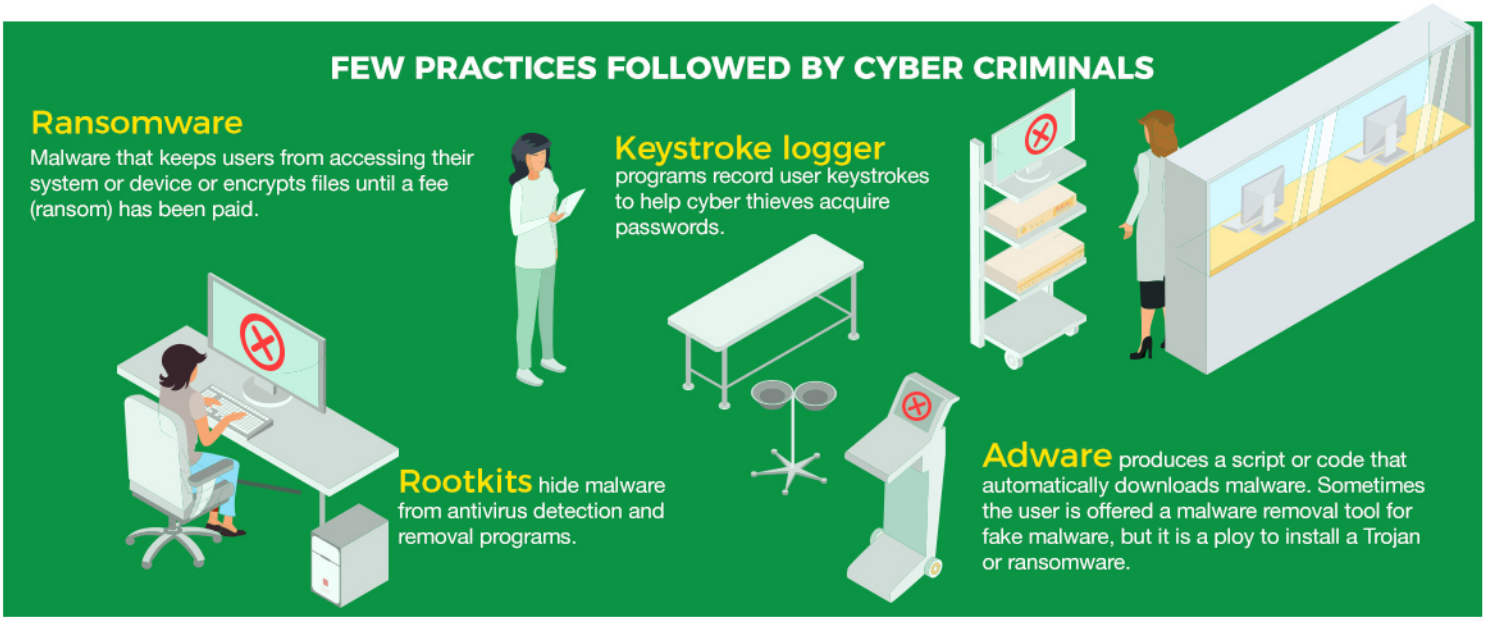
Cyber-attacks can cause operational lock downs, regulatory violations, Identity theft, medical device risks, inadequate security controls and misconfigured security devices

How will it affect you?

A cyber incident can have serious implications like HIPAA regulatory enforcement, litigation, financial losses, loss of trust and goodwill, over and above that wrong diagnosis.

Effects of cyber-attacks on the health care industry

The health care industry has become reliant on the digitization of data and automation of processes to maintain and share Patient Medical Information (PMI) and to deliver patient care more efficiently and effectively. With the benefits derived from the advancements in technology, health care organizations have become vulnerable to cyber-attacks on their IT systems and the data contained therein.



trixter

Info@trixter.in

trixter.in

The cost of security breaches

Cyber-incidents disrupt healthcare service provider's ability to provide life changing and life saving capabilities.

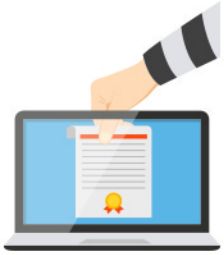
According to a study conducted by IBM Security and the Ponemon Institute, the cost of a data breach for health care organizations rose from $380 per breached record in 2017 to $408 per record in 2018. Across all industries, health care has the highest cost for data breaches.

Healthcare service providers are experts at identifying and eradicating viruses in patients, not computers. Cybersecurity has expanded the scope of patient wellness to include protecting the technology, networks, and databases that enable uninterrupted and accurate patient care. This includes securing computer systems, protecting data and training personnel to be cyber-vigilant.

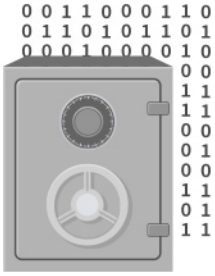
When electronic health record security is breached, hospitals and other organizations often pay hefty fines. Here are a few examples.

Advocate Health Care
Fine: $5.55 million
Why: Four stolen laptops with data from 4 million patients.

Oregon Health & Science University
Fine: $2.7 million
Why: Data breaches affecting 7,000 patients as the result of a stolen laptop and data stored in an unapproved Google Cloud.



Alaska Department of Health and Social Services
Fine: $1.7 million
Why: Stolen USB drive containing personal health information, and lack of adequate policies and procedures to safeguard electronic health information.



New York-Presbyterian Hospital and Columbia University
Fine: $4.8 million.
Why: Physician attempted to deactivate a personal computer, leaving data unsecured.

Anthem in Indiana
Fine: $115 million
Why: Breach affected nearly 80 million patients when a hacker accessed a database including names, birthdays, social security numbers, addresses, email addresses, and employment and income information.

Healthcare, pharmaceutical industries face a wide array of cyber threats which often can be prevented with the right plan of action.

That's where **trixter** comes in.

Identify
Identify the various information assets that could be affected by a cyber-attack and then identify the various risks that could affect those assets.

Remediate
Reduce a cyber-assetís susceptibility to cyber-attack over a range of attack Tactics, Techniques, and Proceduresassociated with the Advanced Persistent Threat.

Build Resilience
Build system within an organization to withstand, respond to, and recover from a cyber-attack or data breach in future.

Greatest Vulnerabilities In Data Security

65% External attackers
48% Sharing data
35% Wireless computing
35% Employee breaches/theft
27% Inadequate firewalls

Top Information Security Concerns

67% Malware Systems
57% Patient Privacy
40% Internal Vulnerabilities
32% Medical Device Security
31% Aging It Hardware

OUR SOLUTIONS

Business Intelligence and Investigations

Counterfeit products and lack in business intelligence are highly damaging to the brand, and profitability of organizations, and have tragic implications for patients. Trixter provides real-time intelligence for preventing, uncovering and disrupting criminal operations.

Compliance Risk and Diligence

Protecting against regulatory risks poses its own challenges where navigating third party risk can be confusing and complex. Trixter can help you take the first step towards establishing a risk-based compliance program.

Cyber Risk

Having a cyber-policy in place when hit with a data breach and not knowing whom to notify is a pressing concern. Trixter experts will come to help you rebuild that trust and meet all regulatory standards.

Managed endpoint protection program

Our managed endpoint protection program is designed to monitor and protect your endpoints from threats and malicious actors. We provide 24x7 monitoring if your endpoints to keep your data, patient data safe from malware and other threats.