Cyber Risks in the Healthcare Industry

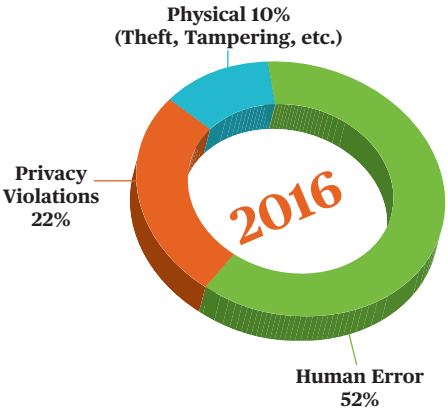
By the very nature of its business, the healthcare industry is privy to a large amount of personal data and records, making it extremely important for healthcare organizations to understand the importance of cyber security and privacy. Patients and businesses alike expect their private data to remain exactly that - private. However, our interconnected world often leaves open technology windows, increasing the exposure to cyber risk. In fact, the healthcare industry is one of the most attacked by cyber criminals.

Why?

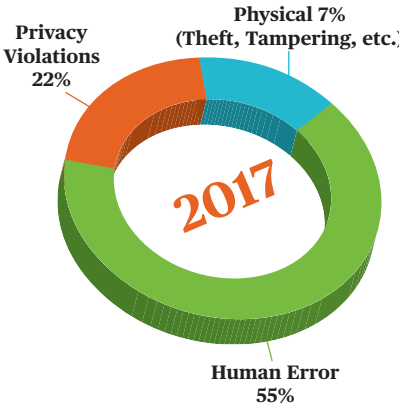
Cyber criminals may target healthcare institutions because there is an extraordinarily high incentive to become operational again if medical equipment is shut down. With patient's lives at stake there is a greater leverage for ransom.

Cyber risk in the healthcare industry continues to evolve with a high risk for human error:

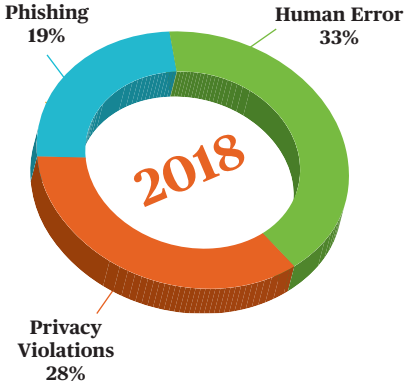
2016 Top Actions for Healthcare:



2017 Top Actions for Healthcare:

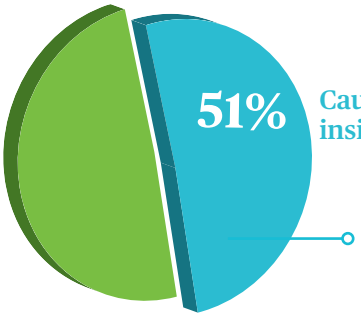


2018 Top Risks for Healthcare:



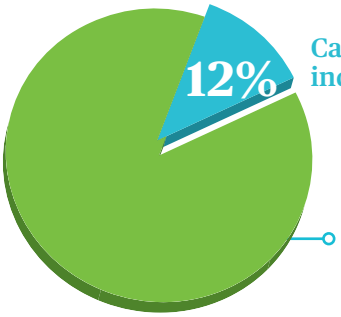
Fast Facts

More than 50% of the cyber incidents reported to Chubb by the healthcare institutions were caused by someone inside the organization. And an additional 12% of the incidents were caused by an industry partner. These actions compromised servers 39% of the time and people 29% of the time. Human error and privacy violations topped the risks healthcare institutions faced in 2018.



Caused by someone inside the organization

Accounted for **51%** of cyber incidents reported to Chubb by healthcare institutions in 2018



Caused by an industry partner

Accounted for an additional **12%** of cyber incidents reported to Chubb by healthcare institutions in 2018

*Data from the **Chubb Cyber Index℠**

What Can You Do?

The most critical service you can provide is employee education. When employees understand the risk factors they are less likely to make mistakes. Teach your employees how to:

- Identify potential cyber threats
- Protect sensitive data
- Escalate issues to the right people
- Ensure strong password hygiene

Services to Help Mitigate Cyber Risk:

Employee Education

Password Management Software

Claims Scenarios:

1. Dr. Imposter, M.D.

An Insured healthcare organization was notified by an outside firm that one of its doctors was being impersonated by an unlicensed physician posing as him. This imposter was able to review several medical files as part of a physician peer review process. Once the Insured became aware of the situation, it had to notify patients whose Personal Health Information (PHI) was inappropriately exposed to this person. Several of the affected individuals have brought third party claims against the Insured for failing to safeguard their PHI.

2. International Information Espionage

A healthcare organization was informed by law enforcement that its patients' information was found on the dark web. It is believed that criminals from outside the U.S. were able to exploit vulnerabilities in the Insured's system to access more than 200,000 patients' PHI. The Insured retained an incident response coach and a forensics firm from Chubb's cyber panel. Several governmental/regulatory agencies were notified with the assistance of the coach. A call center was established and credit monitoring was offered to the affected patients.

3. A Catfished CEO

An Insured was the victim of a spoofing attack whereby a bad actor contacted the company's payroll/HR manager impersonating the email address of the company's CEO. In the spoofing email, the bad actor requested the company's 2016 W2 forms, which included the names, addresses and social security numbers, of the company's current and former employees. Before the company discovered that it had been the victim of a spoofing attack, the W2 forms were transmitted to the bad actor. Approximately 4,000 current and former employees of the company were affected. Thereafter, a former employee of the Insured, whose personal information was compromised in the breach, filed a class action lawsuit against the Insured alleging that the Insured negligently failed to protect its current and former employees' personal information. As a result of this attack, approximately $70,000 was spent for credit monitoring and notification and call center services. Defense costs will also be covered under the terms of the Policy.

SOURCE: The Chubb Cyber Index℠ (June 2019)

Chubb. Insured.℠