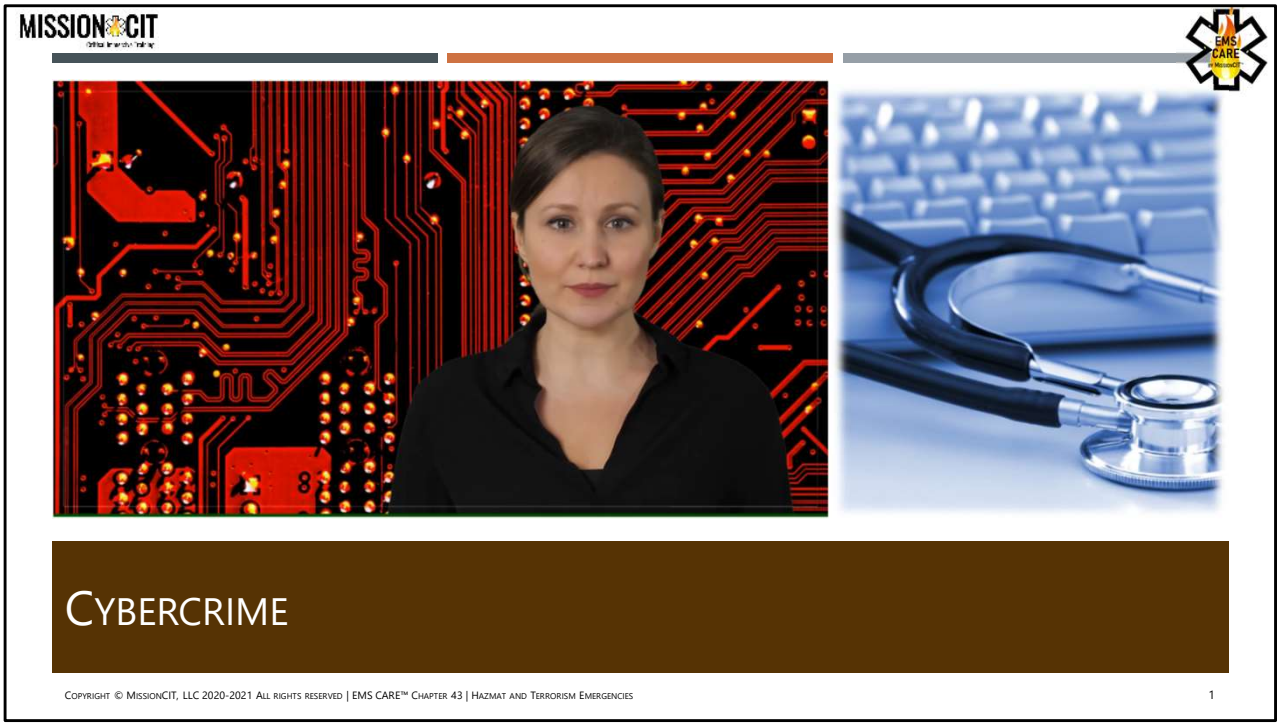


Cyber-attacks might also be launched in conjunction with more traditional forms of terrorist attacks to severely aggravate the consequences.

Today, cybercrime poses one of the largest risks in every sector that utilizes computer data-based operating systems. However, while other sectors have used the cloud for many years, the healthcare sector is still relatively new in this sensitive business.

Cybercriminals, or "hackers,“ prefer to target hospitals because they are more willing to pay ransom for the decryption of their crucial data after a cyber attack. Because hospitals perform sensitive activities, such attacks potentially damage not only the organization and its staff but its patients as well.

Welcome to the fourth lesson, where we will talk about cybercrime and its increased threat in Healthcare Industry.

Good Studying

Definition

- A crime that involves computers and a network
- Computer may be used in commission of crime or may be the target
- May threaten a person, company or a nation's security and financial health



Copyright © MissionCIT, LLC 2020-2021 All rights reserved | EMS CARE™ Chapter 43 | Hazmat and Terrorism Emergencies

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may threaten a person, company, or a nation's security and financial health. They can be carried out by cybercriminals, hacker, individuals, or an organization.

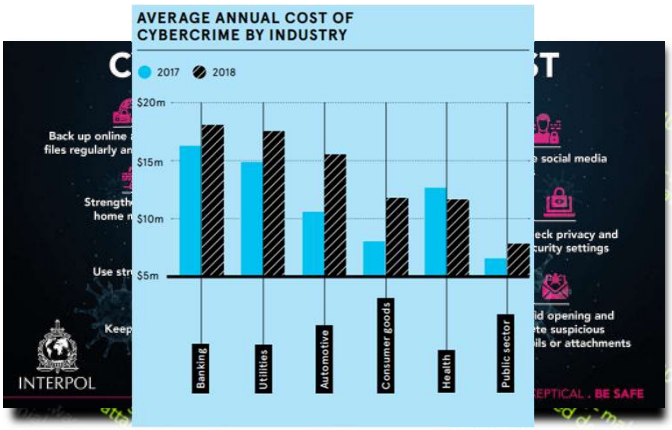
Apart from individual targeted crimes like email phishing, smishing, there are crimes on a larger scale. They are theft of company data, cyber extortion, which is demanding a ransom to prevent an attack;

cyberespionage, where the government or an organization's data is entirely under their access and denial of service, where the perpetuators of the crime block the network for communications and data access.

So, how vulnerable is healthcare to cyber-attack? Let's find out.

Threat to Healthcare

- Forms of cyber-attacks:
  - ✓ Ransomware
  - ✓ Data breaches
  - ✓ DDoS attacks
  - ✓ Insider threats
  - ✓ Computer fraud



Copyright © MissionCIT, LLC 2020-2021 All rights reserved | EMS CARE™ Chapter 43 | Hazmat and Terrorism Emergencies

Reports show that ransomware and other cyberattacks are on the rise — and health care is one of the biggest targets.

Breach of patient information can affect people in multiple ways. From the loss of patient information to a criminal stealing a patient's identity, cyber-attacks impact EMS patients in many ways. The potential forms of cyber-attacks shall be divided into six main groups:

ransomware;

data breaches;

D-D-o-S attacks;

insider threats; and.

computer fraud.

One of the most common cyber-attacks in the healthcare industry is ransomware. Ransomware is a type of malware that infects systems and files, making them inaccessible until a certain amount of ransom, stipulated by the hacker, is paid by the entity. This slows down all critical processes, and may go as far as to make them completely dysfunctional.

Data breach, the most widespread type of cyber-attack is a "loss or theft, or other unauthorized access to sensitive personally identifiable information, that could result in the potential compromise of the confidentiality or integrity of data. The goal of cybercriminals is either to sell the protected health information, or to use it for their gain.

"Distributed Denial of Service attacks", commonly known as D-D-o-S attacks, is a technique used by cybercriminals to overwhelm a network, so that it becomes inoperable. Given the interconnectedness of health systems in the United States, D-D-o-S attacks cause significant problems for healthcare providers.

Insider threats are defined as the potential for an individual, who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Due to the global nature of the Internet, the number of computer frauds is in constant growth.

With this, we have completed the lessons on Hazmat and Terrorism Emergencies, and in the next, Justin will take you through the chapter review.