Will Gignilliat

Dr. Lenry Lewis

CSCI 111 Introduction to Cybersecurity

25 February 2026

Ransomware

Ransomware is a highly relevant topic in cybersecurity and has been a large concern within the last five years. There has been an increase in attacks since around 2020 as technology continues to advance every day, and more organizations rely on digital systems. Large corporations and businesses have had their infrastructure attacked, which has caused financial losses and disruptions, making it a serious problem that the world is facing. The evolution of ransomware has led toward what is now called Ransomware-as-a-Service (RaaS), where cybercriminal groups create ransomware tools and allow others to use them for profit. In the last five years, ransomware has become more than just random cyberattacks, turning into an organized criminal business through Ransomware-as-a-Service and creating serious financial and security risks for companies and critical systems.

Most people wonder, “What is ransomware and how do attacks usually start”? According to the Cybersecurity and Infrastructure Security Agency (CISA), “Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption” (Cybersecurity and Infrastructure Security Agency). The attacker will lock the victim out of their own data and demand money to restore access. Most of these attacks start from phishing emails, downloading infected software, or something like a weak password. Once the system becomes infected, organizations can lose access to important files and operations, which creates pressure

to respond quickly. This is one reason ransomware has become such an effective cyber threat in recent years.

One of the biggest changes in ransomware in the last couple of years has been the development of Ransomware-as-a-Service (RaaS). It has made cyberattacks more organized and widespread. RaaS works by cybercriminal developers creating ransomware tools and then allowing other attackers, which are also known as affiliates, to use them in exchange for a share of profits. CISA explains that ransomware groups often operate using a Ransomware-as-a-Service model where developers create the tools and affiliates carry out the attacks (Cybersecurity and Infrastructure Security Agency). This means that attackers do not require a technological background to create ransomware attacks. There has been an increase of these types of incidents over the last five years. The criminal industry has become more structured because of the shift of ransomware causing more attacks to be more frequent and it harder for governments to prevent these attacks.

A recent known attack with the past several years was the Colonial Pipeline attack in 2021. This attack expresses how serious these cyber threats can be relating to the infrastructure. The company was forced to shut down temporarily after this attack, which lead to fuel shortages and panic across parts of the United States. According to the reports, “Colonial Pipeline's CEO on Wednesday acknowledged to the Wall Street Journal that his company paid a $4.4 million ransom to hackers as executives were unsure how badly its systems were breached or how long it would take to restore the pipeline.” (Bing and Satter). This indicates that not only do private companies get affected by ransomware, but also millions of people that depend on these essential services every day. Events like this are a major reason why ransomware has become cybersecurity concern within the last five years and why there needs to be better protection.

Healthcare organizations have taken a major hit from ransomware attacks and it proves that these ransomware attacks should be taken seriously. Hospitals and medical facilities rely on digital systems to manage patient records, equipment, and communication. This is a major target for attackers. CISA declares that healthcare and public health organizations are prime targets for ransomware attacks (Cybersecurity and Infrastructure Security Agency). Ransomware can disrupt these systems and force hospitals delaying procedures and operations without access to important medical information. Ransomware is affecting the common people in many different ways and hospitals one of the worst targets.

A lot of organizations will still choose to pay ransoms even though cybersecurity experts advise against it. Many companies feel pressured to restore operations as quickly as possible because too much downtown can result in financial loss and damage to their reputation. Sometimes attackers will threaten to release stolen data publicly and this will increase the likelihood of a victim to cooperate with the attacker. According to the FBI, paying a ransom does not guarantee that data will be recovered or that the systems will be restored safely (Federal Bureau of Investigation). Situations like these are prime examples of how ransomware attacks can put companies in a vulnerable state.

Ransomware attacks have been a major issue economically and socially, making them the most damaging cybersecurity threats today. Businesses face large financial losses from paying ransoms. These businesses also must face downtime, recovery costs, and damage of reputation. The FBI's Internet Crime Complaint Center reported $16.6 billion in total cybercrime losses for 2024, a 33% jump from the previous year. (Federal Bureau of Investigation). These attacks can also affect critical services such as healthcare, transportation, and energy systems. The consequences can extend beyond just businesses and impact an entire community. Organizations

rely heavily on digital data and technology. Ransomware continues to be a threat globally and there has to be some adaptations to keep up with the cybersecurity threats.

Ransomware prevention has become a major priority for organizations as threats continue to increase. CISA explains that the best way to protect against ransomware is to prevent it from happening in the first place (Cybersecurity and Infrastructure Security Agency). Companies are encouraged to use cybersecurity measures such as multi-factor authentication, regular data backups, software updates, and training the employees to reduce the risk of attacks. Prevention can still be challenging because cybercriminals develop new techniques and continue to target human error. Technological advances continue to have their advantages and disadvantages, where practicing protocols for preventing ransomware is essential.

Ransomware has become one of the most serious cybersecurity threats in the last five years as technology continues to advance and organizations depend more on digital systems for everyday operations. The development of Ransomware-as-a-Service has made these attacks more organized and more common, which increases the risks for businesses, healthcare organizations, and critical infrastructure. Real-world incidents such as the Colonial Pipeline attack and ransomware attacks on hospitals show how these cyber threats can impact not only companies but also everyday people who rely on essential services. The financial losses, operational disruptions, and risks to public safety demonstrate why ransomware continues to be a major global concern. Organizations are facing increasing pressure to improve cybersecurity practices because attackers are constantly developing new methods and taking advantage of human error. Prevention methods such as multi-factor authentication, employee training, regular backups, and system updates are important steps in reducing risks, but they require consistent effort and awareness. As technology continues to evolve, ransomware will likely remain a persistent threat,

which makes cybersecurity education and protection more important than ever. Overall, understanding how ransomware works and why it has grown so quickly helps show why stronger security measures are necessary to protect organizations and communities in the future.

References

Cybersecurity and Infrastructure Security Agency. *Stop Ransomware Guide*. CISA, 2023, https://www.cisa.gov/stopransomware.

Bing, Christopher, and Raphael Satter. "Colonial Pipeline CEO Admits Paying Hackers to Restore Pipeline." *Reuters*, 19 May 2021, https://www.reuters.com/business/energy/colonial-pipeline-ceo-admits-paying-hackers-restore-pipeline-wsj-2021-05-19/.

Federal Bureau of Investigation. *Internet Crime Report 2024*. FBI, 2025, https://www.ic3.gov