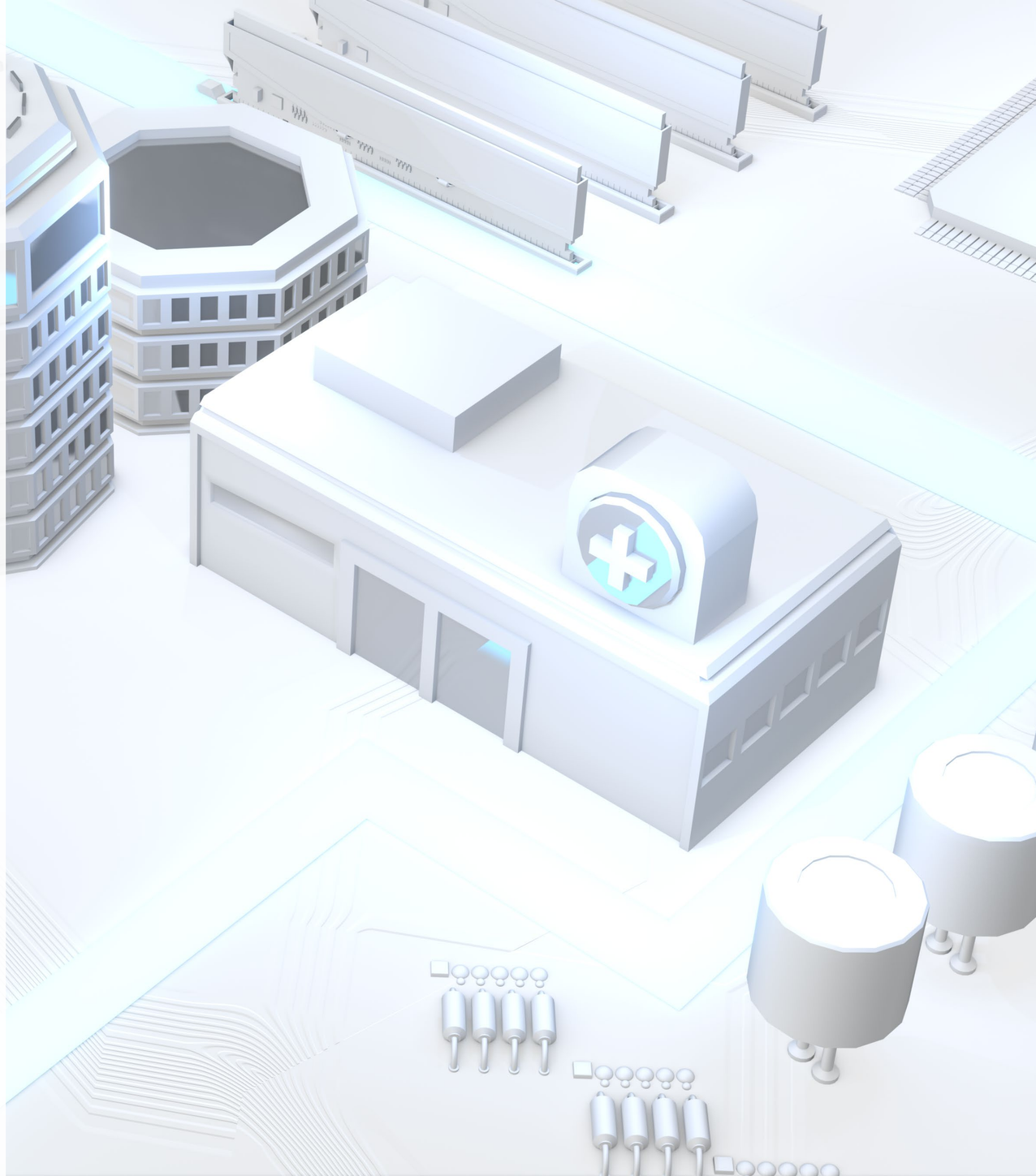
Cyber Case Study

provided by VantagePointe Benefit Solutions, Inc

Change Healthcare Cyberattack

In February 2024, hackers initiated a cyberattack against Change Healthcare, a leading health claims processing provider in North America that processes approximately 15 billion health care transactions annually. The attack created widespread disruption of health care claims, patient care and other technology-dependent services.

It also resulted in significant recovery costs, operational interruption, reputational damage and legal ramifications for the company. This cybersecurity event emphasized the severity of cybersecurity attacks (particularly in the health care sector) and offered valuable lessons on how businesses can prevent and respond to similar incidents. Here is what your organization needs to know.



The American Hospital Association referred to the cyberattack as **“the most significant and consequential incident of its kind against the U.S. health care system.”**

The Details

On Feb. 21, 2024, hacker group BlackCat, also known as ALPHV, accessed Change Healthcare’s network through compromised credentials, possibly including stolen passwords. The group was able to enter the system in part because the company’s server did not have multifactor authentication (MFA) protocols in place. Without multiple steps to verify a user’s identity, malicious actors could more readily access Change Healthcare’s data and move laterally within the company’s system.

Once the hackers compromised Change Healthcare’s network, they claimed to have stolen six terabytes of sensitive information, including personally identifiable information and medical records. The group then demanded a ransom to prevent the public release of the data.

To limit the damage, the leadership at Change Healthcare’s parent company, UnitedHealth Group, disconnected the affected systems. This forced pharmacies and health care providers to find alternative ways to continue providing services. For example, the disrupted transactions impacted billing, cash flow, electronic remittances, patient claims and other aspects of patient care, including clinical decision support, prior authorization submissions, medical group eligibility checks, pharmacy operations such as issuing and filling prescriptions, and clinical decision support.

The impacts of the attack were so immediate and widespread that the American Hospital Association, on behalf of its nearly 5,000 members, wrote a letter to the U.S. Department of Health and Human Services (HHS) requesting their support to resolve the situation. On Feb. 28, the Medical Group Management Association, which consists of over 60,000 medical practice administrators, executives and leaders, followed suit and penned a public letter to HHS requesting government assistance to address the impacts.

According to reports, the leadership team paid the 350 bitcoin ransom, valued at approximately $22 million, on March 1, and brought in multiple incident response firms and third-party cybersecurity experts. On March 7, services for payment services and prescription claim submissions were restored, and on March 15, the electronic payments platform was restored.

The criminal hacker group BlackCat or ALPHV operates as a ransomware-as-a-service model that enables affiliates to launch ransomware attacks using the ransomware code that BlackCat/ALPHV develops. The hacker group also agrees to pay a share of a ransom payment in exchange for executing these attacks. The Change Healthcare breach demonstrated how such attacks can significantly impact business operations, how health care functions can be disrupted, and why it is a necessity to have cybersecurity systems and procedures to prevent and respond to these types of attacks.

The Impact

Colonial Pipeline encountered numerous consequences from this ransomware attack, including the following:

Financial

The Change Healthcare cybersecurity incident resulted in significant financial losses. In addition to the $22 million ransom expenditure, UnitedHealth Group advanced nearly $4.7 billion to providers in need (as of April 3, 2024). Change Healthcare also experienced a multiday operational disruption resulting in a substantial business interruption and loss of income. Moreover, the company likely incurred expenses when it retained incident response firms and cybersecurity experts to investigate and respond to the ransomware attack. Other expenses in these situations typically include replacing damaged hardware or software and upgrading systems to strengthen cybersecurity. Implementing these updates can also contribute to productivity losses as the changes are processed. UnitedHealth Group reported that the cyberattack cost them over $870 million in the first quarter of 2024 and estimated that annual losses will exceed $1 billion.

Operational

The cyberattack resulted in major operation disruptions. After Change Healthcare shut down its systems, pharmacy services, claims processing, billing and other important health care services were disrupted. In fact, the American Hospital Association referred to the cyberattack as "the most significant and consequential incident of its kind against the U.S. health care system." The association said the disruption from the attack made it more difficult for hospitals to provide care to patients, submit insurance claims and receive payments for their services. Some new patients were also unable to see a provider since the provider was not able to verify insurance eligibility without the usual billing processes.

Reputational damage

Change Healthcare and UnitedHealth Group suffered reputation damage due to the cyber incident. The decision to pay the ransom was scrutinized as uncertainty arose regarding the security of the data after the company made the payment. Affected parties raised concerns that their information was still compromised and there was no guarantee the hackers would not disseminate it even after receiving the ransom. This is why the FBI encourages organizations not to make such payments. The bureau notes that paying a ransom can incentivize malicious actors to continue engaging in illegal behavior, and the ransom may be used to fund criminal activities. Additionally, the cyberattack and subsequent network shutdown resulted in a significant and lengthy disruption of services that called into question Change Healthcare's recovery process. Coupled with the media coverage of the attack and subsequent congressional hearings, this has created long-term reputational effects for the company.

Legal ramifications

The cyberattack on Change Healthcare resulted in multiple lawsuits being filed against the company. Ultimately, nearly 50 lawsuits were consolidated in Minnesota, the state where UnitedHealth Group is based. Among the suits are 19 consumer complaints with claims that personal information and health data were compromised. Another 30 were filed on behalf of providers who allege they had difficulties submitting claims and receiving payments due to the system shutdown following the cyberattack. In its Transfer Order, the U.S. Judicial Panel on Multidistrict Litigation noted that actions involved common questions of fact with allegations that Change Healthcare did not take adequate measures to stop the cyberattack or prevent its consequences. The panel noted there were overlapping class actions of individuals and health care providers that asserted similar claims for negligence, negligence per se, breach of contract or implied contract, violation of state consumer protection laws and unjust enrichment. Moreover, HHS initiated an investigation into whether the company violated the Health Insurance Portability and Accountability Act. Defending against and resolving these issues will likely require significant resources, and Change Healthcare may have to pay significant legal judgments, settlements or regulatory fines.

Lessons Learned

There are multiple takeaways about cybersecurity employers can glean from the Change Healthcare cyberattack. In particular, the incident highlighted these key lessons:

Assess third-party vendor risk.
This incident demonstrated how reliance on third-party vendors, like Change Healthcare, can increase cybersecurity risks. In this situation, thousands of health care organizations relied on Change Healthcare services and trusted them to safeguard sensitive data. This underscores how a breach of one company could have far-reaching consequences for an entire sector. To mitigate cybersecurity risks associated with third-party vendors, companies should thoroughly vet prospective partners and incorporate cyber risk management into vendor contracts; this may include adding clauses requiring vendors to secure cyber insurance, providing notification following a cyber incident, and establishing clear expectations concerning data destruction after the contract ends. Businesses should also minimize a third party's access to company data when possible and continually monitor the vendor's adherence to risk management best practices.

Establish robust cybersecurity measures.
The malicious actors in the Change Healthcare incident were able to carry out their attack by using compromised credentials to access the company's system. The business's server was more easily infiltrated without MFA access controls. Robust cybersecurity measures, such as proper password storage, network segmentation and MFA procedures, can help strengthen cyber defenses. It's essential to conduct regular risk assessments with penetration testing to identify vulnerabilities and prioritize addressing the ones that pose the most significant risks. Moreover, implementing executive-sponsored cybersecurity training and comprehensive cybersecurity awareness programs are also key to bolstering cyber defenses.

Implement proactive incident planning.
This cyberattack demonstrated the necessity of having a detailed incident response plan. This plan can help a company establish timely response procedures to mitigate losses and act appropriately amid a cyber event. Change Healthcare's handling of the cyberattack significantly impacted the business, its clients, the public and the company's reputation. Additionally, the organization has faced criticism for the length of its recovery process and deficient backup procedures. A successful incident response plan could have prepared leadership by outlining potential cyberattack scenarios and strategies for maintaining key functionality while noting individuals' roles during a cybersecurity incident. Such a plan also provides procedures for notifying relevant parties (e.g., government authorities, clients and shareholders) of an attack. An incident response plan should be regularly reviewed through activities such as tabletop exercises to identify its strengths and weaknesses. The plan should then be modified accordingly.

Financially protect against cyber risks with proper insurance coverage.
This cybersecurity incident clearly illustrated that cyber-related losses can substantially impact any organization, even large companies with extensive resources. Consequently, businesses should consider securing adequate financial protection against cyber incidents by obtaining proper coverage. Specifically, most organizations can benefit from a dedicated cyber insurance policy that offers both first-party and third-party coverage. First-party coverage typically provides financial protection for an organization's direct losses following a cyber incident. This includes costs associated with data recovery, incident response and notification obligations, as well as losses from business interruptions and cyber extortion. First-party coverage may also help pay for crisis management and public relations services after a cyberattack. A third-party cyber insurance offering generally may cover the costs associated with claims made against the business, fines it incurs and expenses connected to lawsuits filed against the company. It is advisable to consult a trusted insurance professional for assistance when navigating these coverage decisions.