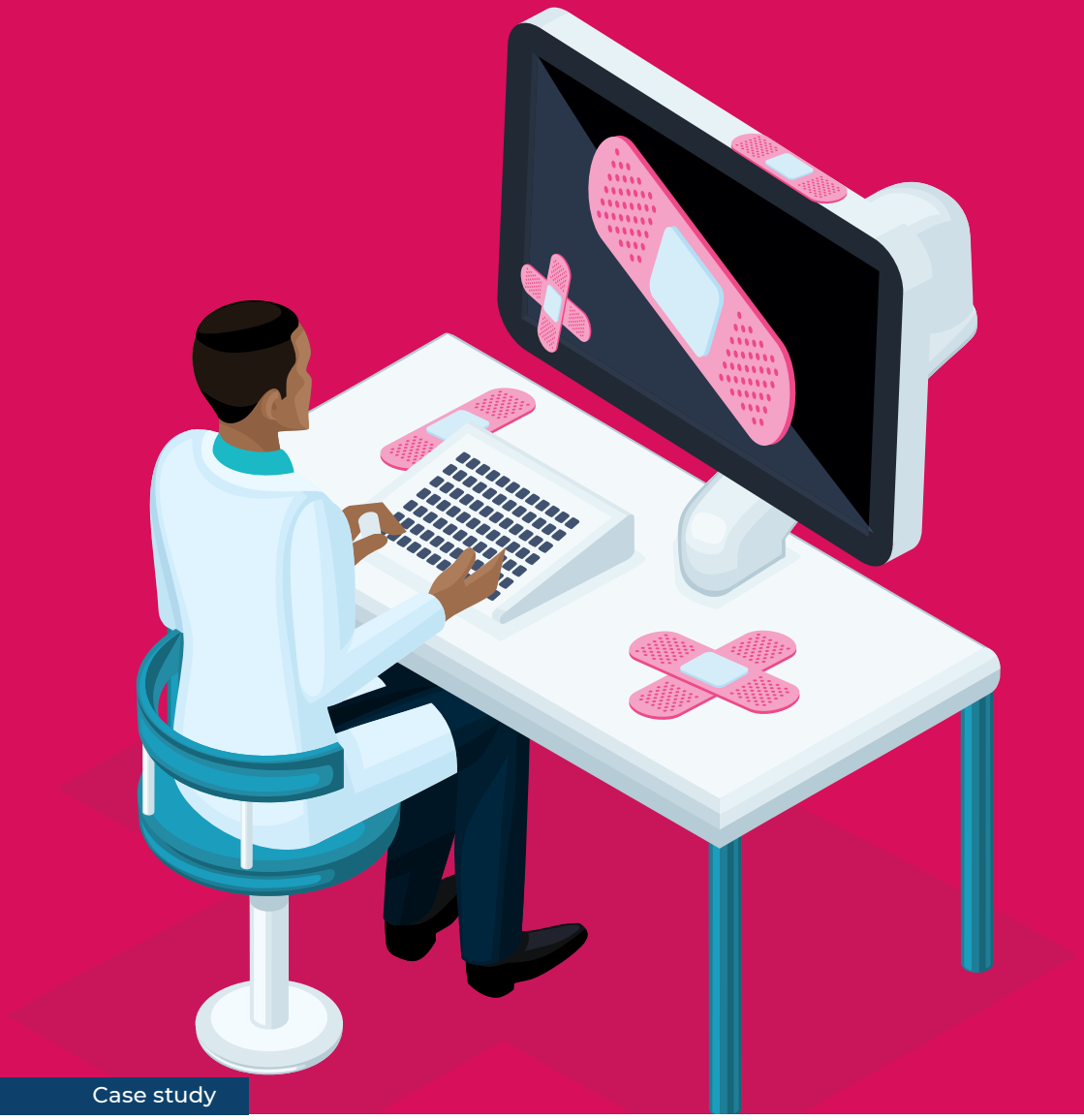
evolve



Case study

Quick fix complication

Healthcare provider avoids large-scale notification

Cyber insurance is projected to experience major growth in the years ahead and new carriers are regularly entering the market.

This is creating greater competition and providing more choice for customers. Businesses should be aware, however, that not all insurers are alike, and the skills and expertise that a well-established, experienced cyber insurer can bring can make a big difference to their buying experience and, most importantly, when making a claim.

System wipe out leads to larger issue

In the summer of 2017, a US-based medical service provider fell victim to a ransomware attack. The ransomware had spread throughout the organization's network, **encrypting 120 computer workstations and 15 servers**, rendering them useless, and making all patient management records and electronic medical records stored on the network inaccessible. Panicked and unable to conduct business as usual, the organization's first action was to promptly engage its IT vendor to fix the problem.

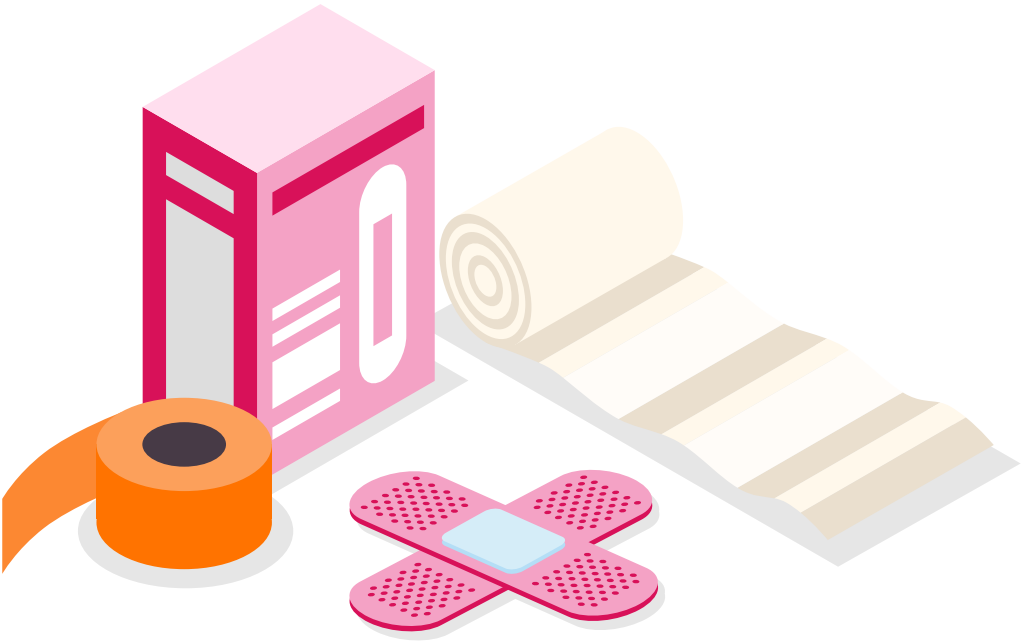
Did you know?

The number of reported major cyber events at healthcare institutions attributed to ransomware increased by 89% from 2016 to 2017.

Source: Cryptonite 2017 Health Care Cyber Research Report

The IT vendor responded quickly to the incident and managed to rebuild and reimage all of the affected workstations and servers from back-up, wiping any trace of the ransomware from the network. While the insured was up and running again quickly and avoided any substantial business interruption costs, removing the ransomware from its system did have a major drawback.

The main problem with wiping the system clean was its impact on the organization's breach notification requirements. As a US-based healthcare provider involved in the processing of Protected Healthcare Information (PHI), the organization fell under the remit of the Health Insurance Portability and Accountability Act (HIPAA). Under HIPAA and its associated legislation, patients whose PHI is compromised in a data breach must be notified within 60 days of the breach's discovery. The Office for Civil Rights (OCR), which is the entity responsible for enforcing HIPAA, has issued guidance on ransomware and has concluded that where a ransomware attack has resulted in PHI being encrypted, the organization must prove that there was a low probability that the PHI was viewed or stolen. Otherwise, the Breach Notification Rule is triggered. ▶



▶ Our policyholder's IT vendor was fairly sure that the ransomware variant was an automated attack that was not designed to access or steal data. But, having completely removed the ransomware from its network, it appeared nearly impossible to utilise forensics to analyse the attack vector, identify the ransomware variant, and establish whether or not any PHI was actually viewed or stolen.

The insured engaged their own legal counsel, who came to the conclusion that because it wouldn't be possible to determine if there was a low probability that the PHI had been compromised, **the insured would have to notify all 100,000 of their patients**, both past and present. Given the patient population size, **the cost to notify them all was likely to be in excess of $200,000**, and it would also trigger an OCR investigation. What's more, by notifying its patient base about a potential compromise of PHI, the organization was likely to see its reputation suffer serious harm as a result.

Incident response to the rescue

Having realised that they might have to notify their customers, it was at this point that the policyholder informed CFC of the incident. From the outset, CFC's specialist in-house cyber incident response team knew that it was essential to determine the variant of ransomware in order to understand whether PHI could have been viewed or stolen. They contacted both the insured and the IT vendor to see if either party had evidence of the ransom note itself. While no one in the senior management of the organisation or at the IT vendor had kept evidence of the attack, an employee had taken a photo of the ransom note during the event.

Analysis of the ransom note showed that it contained an email address that victims were supposed to contact in order to organize payment. Using this snippet of information, our in-house incident response team was able to identify the ransomware that had encrypted the company's computer systems as the variant known as LockCrypt. From here, our team engaged two forensic IT consultants to give their independent views as to whether LockCrypt was capable of viewing or exfiltrating data. Both consultants reported back that LockCrypt was an automated form of ransomware used by a group based in Australia that did not appear to have prior knowledge of the organizations it attacked or the data that these organisations held. They concluded that although PHI files were encrypted by the attack, the files themselves were unlikely to have been accessed or removed from the system by the attackers.

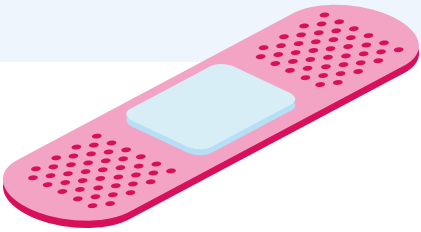
From the outset, CFC's specialist in-house cyber incident response team knew that it was essential to determine the variant of ransomware

Based on the forensic consultants' reports, the law firm reassessed the situation and determined that there was a low probability that PHI had been compromised, and therefore notifying the entire patient base was no longer required. This meant that a potentially very costly claim involving notification, a regulatory investigation, legal services and crisis communication fees was avoided. And perhaps most importantly for the insured, their reputation with current and future patients was still intact.

Experience in cyber claims is imperative

The situation faced by this healthcare provider highlights two important lessons. First, it is essential that when a ransomware attack or any other cyber event occurs, policyholders should engage their cyber insurance provider as soon as possible. By doing so, a coordinated response to the attack can be devised and any evidence that may become crucial later on can be preserved from the outset.

While cyber insurance is an increasingly competitive marketplace, having a well-seasoned cyber insurer that is experienced in handling cyber claims is key



Secondly, placing your cyber insurance with an experienced provider can make all the difference. By having our own in-house incident response team with specialist knowledge of cyber security and forensics, we were able to successfully prevent the policyholder's claim costs from escalating and ensured that the organisation's reputation didn't suffer unnecessarily. If they had been with a less experienced cyber insurer without a dedicated in-house incident response team, they may have gone ahead with the breach notification process. While cyber insurance is an increasingly competitive marketplace, having a well-seasoned cyber insurer that is experienced in handling cyber claims is key.