Case study

Beyond the breach

Small hospital faces huge operational disruption

Because healthcare providers typically hold large amounts of highly sensitive health-related information about their patients, it's widely assumed that their primary cyber exposure is data breach and the notification requirements, investigation costs, fines and penalties they may face as a result.

But healthcare providers, like any business, are exposed to a range of cyber exposures, including malware attacks, which can have a devastating impact on their operations, especially in relation to system damage and business interruption costs.

From malware to meltdown

Malware, or malicious software, is any software that has been designed specifically to cause damage to computer networks and recent events have shown malware attacks to be getting more and more destructive. The motives for such attacks can vary from attempting to extort money to inflicting damage for the sake of it but, either way, the impact on the victim organisation can be highly disruptive and, sometimes, catastrophic. Furthermore, malware is becoming easier to deploy with the continued rise of phishing campaigns acting as just one conduit to conduct attacks.

> All of the electronic data that the hospital held on its patients was now inaccessible

A number of high profile organisations have fallen victim to malware attacks in recent years. For example, back in 2012 Saudi Arabia's national oil firm Saudi Aramco was hit by a destructive malware variant known as Shamoon that resulted in some 35,000 computers being either completely destroyed or at least partly wiped.

In another attack in 2014, the American casino and resort company Las Vegas Sands had thousands of its servers wiped by a type of destructive malware that shut its websites down for a week.

However, it isn't just large corporations that are impacted by these kinds of malware attacks and much smaller entities can be affected too. One such victim was a mid-sized hospital based in America that provides a variety of surgical procedures for patients who have been referred via physicians and caters to a large volume of emergency admissions. ▶

▶ It was in late August 2017 that the hospital first noticed that something was wrong when employees arrived at work to find that all of the hospital's devices and servers were no longer functioning properly. This meant that all of the electronic data that the hospital held on its patients was now inaccessible. Staff at the hospital could now no longer look at their patients' medical histories, such as previous doctors' notes, allergies and drug prescriptions. Instead of being able to view electronic patient files as they normally would, doctors and nurses had to ask each individual patient about their medical history all over again. Electronic monitoring of patients was no longer possible and bed-side machines used for dispensing medication were rendered inoperable. This resulted in the hospital having to bring in an army of additional nurses to help ensure that patients were being monitored effectively.

Did you know?

There are 350,000 new malicious programmes discovered every day.

Source: AV-Test, It Security Institute

Getting back online

Despite the hospital's best efforts, these manual processes were causing significant delays to the service. By mid-afternoon, the hospital was forced to call a Red Alert. Red Alert is a state protocol that obliges ambulance staff to advise patients that although the hospital affected is still accepting patients, there will be **substantially longer** waiting times for procedures than usual. The patient can then choose whether to proceed to the affected hospital or to be taken to one of the other hospitals in the local area. With the Red Alert in place, patient numbers began to dwindle.

This destructive malware outbreak had rendered around 2,000 of the hospital's devices and servers inoperable, and getting those systems working again proved to be a significant task. The only way to return the hospital to normal operations was to **wipe and rebuild all of the servers and devices from scratch.** But wiping the devices and servers proved to be more expensive than just buying replacements.

Another complication the hospital faced was in relation to their electronic health records system. Like most healthcare organisations, this hospital was connected to a hosted, centralised electronic health records systems, which gave them access to patient records and details and allowed for the exchange of information with other healthcare facilities. But because of the malware outbreak on their system, the hospital was cut off by their service provider, who refused to reconnect them until their network was declared completely clean and malware free by an independent forensic consultant. In the meantime, the hospital had to connect to a separate cloud network to access the data that they needed **at an additional cost of $2,000 a day.**

It was only in late October 2017 that the hospital was able to call off Red Alert, and it would take until early November before normality was restored. In the meantime, the insured had incurred some $2.6 million in system damages costs, the bulk of which was to replace hard drives, servers, laptops, computers, printers, scanners, software licenses and the like, and a further $4.5 million in business interruption, which was primarily due to the drop-off in patient income following the Red Alert. Unfortunately for the insured, however, they only had a policy limit of $5 million.

While many cyber policies exclude physical property and hardware replacement costs, the hospital's cyber policy from CFC provides cover for these items when it is the most efficient way of making the insured operational again, as well as cover for the costs associated with business interruption.

Choosing the right cyber policy

Malware is one of many cyber risks that can have a destructive impact on any business, large or small. While organisations that handle large volumes of sensitive or personal data have long viewed their cyber risk in terms of data breach, **any business that relies on computer systems to operate can have a substantial exposure**, particularly when it comes to system damage and business interruption costs.

In this instance, the hospital had specifically purchased their cyber insurance policy with data breaches in mind and had only opted for a $5 million limit. They had calculated how many data subjects they had and what the likely cost would be to notify them and deal with any subsequent investigations or penalties, but they hadn't factored in the **huge operational interruption costs** that could be incurred by a destructive malware event, which left them terribly exposed when disaster struck. The insured suffered this enormous loss without a single patient record having been breached.

When purchasing a cyber policy, both insureds and their brokers should make sure that they **consider the full range of first and third party risks** that they might face and select an adequate limit accordingly.