"WE SHALL FIGHT ON THE BREACHES"

30 October 2018 | Global Insights

In May 2017 the WannaCry ransomware attack targeted computers running Microsoft Windows and was estimated to have affected over 230,000 computers in 150 different countries before Microsoft was able to issue emergency patches, and a kill switch was discovered that prevented further spread of the virus.

The ransomware encrypted computer files and displayed a message demanding payment to release those files. One of the most notable victims was the National Health Service in the UK, which saw up to 70,000 devices in its hospitals affected – leading to non-critical procedures being cancelled and ambulances turned away during the attack.

But this was just the tip of the iceberg. Such incidences are clearly on the rise, with viruses such as WYSIWYE, Osiris and Cerber just a few of the most troublesome, causing havoc in global IT and communication systems over the last couple of years.

The issue has only been compounded by the rapid rise of the IoT (Internet of Things). Its almost infinitely expanded connectivity has also expanded the potential for attacks in a whole new range of spaces.

The landscape has changed rapidly and cyber security has gone from being something of an IT afterthought to one of the most pressing concerns of the day.

Kwok Tang, Senior Associate, Technology, Media and Telecoms at Herbert Smith Freehills, believes this was inevitable. “Technology has now become all pervasive and is involved in pretty much every aspect of our lives. This has greatly enhanced our lives, but it also means the way people and companies can be potentially attacked by hackers has increased significantly.

“As risk of cyber threats increases, it is not coincidental that the amount of global regulation around security and data breaches and the fines connected to them have also increased.”

Fines are substantial and failure to comply with privacy acts and data breach notifications can cost up to $2.1 million in Australia, and up to the greater of 20 million euros or four percent of annual turnover in Europe.

“As a direct consequence of this, cyber security has slowly increased in importance and priority for companies,” says Kwok. “Almost each year there’s a new survey of priorities for boards and companies, what’s keeping them up at night, and invariably cyber security will be one of the top issues.”

How to avoid being a victim

Kwok explains that cyber security is at its core a cat and mouse game of hackers and victims always trying to keep ahead of each other. But it’s no game when the result is huge financial losses. An IBM Global study published in July estimated the average cost of a data breach globally is US$3.86 million.

So vigilance and proactiveness in cyber security is critically important. “The biggest issue is companies either not following their own security measures or failing to constantly review and update their security practices.”

One of the reasons WannaCry was so successful in its aims was because it targeted a vulnerable hole in Microsoft systems that the computer giant had already identified and issued a patch to plug. “The companies that were attacked just didn’t upload or update the patch in time,” reveals Kwok.

Despite the myriad of warnings and advice to constantly change or secure them, passwords remain one of the biggest danger spots. “In a 2018 report, Verizon estimated 80 to 90 percent of security breaches occur due to weak or compromised passwords,” explains Kwok. But as any IT professional will attest, trying to get company wide compliance without constant ‘I’ve forgotten my password, can you reset it?’ requests is an onerous task.

This is why the process needs to be automated, with regular reminders to staff to update their passwords. Training on how to create a secure password that can be easily remembered by user (and only that user) can also help. Kwok refers to “horror stories” he has heard where users have their login passwords on sticky notes and affixed to their screens because their company’s IT system self-generated passwords that were impossible for people to remember.

Company wide

From the micro to the macro, Kwok advises that there are a number of approaches companies need to take to ensure their safety in this area. First, they need to complete an appropriate risk assessment to understand exactly what assets need protecting – IT, financial data, customer and employee data – and which are less critical.

Then, it’s time to install robust anti-malware software and proper protection back-ups. Above all, he stresses, there should be regular and comprehensive staff training on the issue. “When the staff are on-board, they should have basic security training every year, as most security breaches arise from human error.”

He also advises external penetration testing. “You can hire a security team to actually try to attack your system, to check whether it’s secure.”

Finally, it’s vital that companies formulate a crisis management plan to enact should things go wrong. He has often seen companies spend the first day or two after a security breach simply trying to work out what to do next. “If you have a plan in place and know who to contact, when to contact them and who is responsible for doing what, that really helps.”

Crisis Prevention and Management app

At Herbert Smith Freehills we have decades of experience helping major corporations and governments take control of all aspects of crises, including cyber security breaches, defamation and reputation management, and safety, environmental, employee relations, human rights, insurance and competition issues.

We know that the first 24 hours of a crisis are critical, which is why we developed a Crisis Prevention app for our clients. The app provides high-level advice and outlines step-by-step processes on what to do in a series of emergency situations.