Cyber-Risks and Liabilities

May/June 2021

Understanding the Threat of Firmware Attacks

There are many different cyber-threats that organisations must be aware of in today's world. One specific type of cyber-attack that has become more common of late is firmware attacks.

Firmware is a specific type of software code that is used to control various hardware within a computer. For example, firmware within a motherboard can control basic commands, such as when the device should start up.

According to Microsoft's March 2021 Security Signals report—which surveyed over 1,000 organisations around the world—80 per cent of respondents said that they had experienced at least one firmware attack in the last two years. The study also found that only 29 per cent of cyber-security budgets allocated funds to protect firmware from attacks.

Attacks on firmware utilise malware in order to tamper with key components of a computer, such as the aforementioned motherboard or hardware drivers. These types of cyber-threats can be particularly difficult to detect due to the fact that firmware is at a layer within the device deeper than the operating system itself. As such, this type of attack may be able to bypass software designed to detect malware, as well as the entire operating system.

Firmware attacks are not often aimed at individuals, but larger firms should take the potential threat seriously. This method is more complicated for a cyber-criminal to utilise, but the coronavirus pandemic may have accelerated hackers' use of such attacks. In order to protect your organisation from a firmware attack, consider these steps:

- **Update**—Industry experts say that part of the reason for firmware vulnerabilities is that updating and patching potential security weaknesses is more complicated than doing so for software. Despite that hurdle, it's important for organisations to take this step.
- **Consider new equipment**—As the tactics of cyber-criminals continue to evolve, so too are defences. Given the recent rise in firmware attacks, some manufacturers are adding advanced security protocols to hardware that specifically address firmware security.
- **Be careful with USBs**—USB devices have their own firmware. Plugging an infected USB into a computer will provide the malware with an easy path to spread.

For more information on firmware attacks and other cyber-security solutions, contact us today.

The Rising Threat of Extortionware

Ransomware is a type of malware that holds a victim's data or devices hostage. While many organisations may already be familiar with this type of cyber-threat, it has now become more common for cyber-criminals to take this type of attack one step further.

Cyber-security organisations have begun to warn firms about the rise of 'extortionware'. Cyber-criminals use this type of attack to discover sensitive or embarrassing information that can then be used for extortion.

Victims of extortionware will not only face potential financial losses related to paying any ransom. There may also be severe reputational consequences at stake in the event that damaging information is released.

These attacks can be particularly difficult to defend against. Other ransomware attacks may have simply denied access to a device or data. As such, having thorough backups could be a potential solution. However, having a backup copy of data will not protect you if the hackers decide to release the information.

With the threat of extortionware in mind, employees must be trained and reminded not to store any potentially harmful information on an organisation's devices, servers or network. Other general cyber-security steps—such as strong passwords and avoiding phishing schemes—must also be re-emphasised in order to minimise the risk of an extortionware infection in the first place.

According to a global report by Emsisoft, ransomware attacks are estimated to have cost organisations around the world as much as £123 billion in 2019. This includes the costs of downtime and disruption related to the attack.

For more information on cyber-security and extortionware, contact us today.

The Importance of Sanitising Devices

Cyber-security practices for an electronic device must be considered at all times—even beyond the working life of the device itself. While computers, smartphones, tablets and other devices may eventually be retired from use, that does not mean that they cannot still present a potential cyber-risk for their owners.

A key cyber-security step that should not be taken lightly is understanding how to properly sanitise a device. Simply deleting data will not ensure security.

The National Cyber Security Centre (NCSC) defines sanitisation as 'the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level'. In other words, sanitisation is intended to minimise the chance that a cyber-criminal or other malicious party could acquire sensitive information using a device that has been passed on or disposed of.

Sanitising a device may be necessary for a number of reasons, such as:

- **Disposal**—Even when a device is being thrown out, it's possible that it could eventually fall into the wrong hands. As such, sanitise equipment prior to disposing of it.
- **Sale**—Organisations may wish to sell used equipment as a means of generating additional revenue, but it's important that the device's new owner not be able to recover any important information.
- **Maintenance**—If a device needs to be returned to a vendor or manufacturer, or left with a repair service, sanitisation may be a necessary precaution.
- **Re-use**—If a device previously used by one employee is now being issued to another, it may be advisable to sanitise it.

It's important that a device that has changed hands does not retain its previous permissions or access to organisational data. When sanitising, be sure to revoke all certificates associated with the device in question. In addition, any other credentials previously used on the device should be revoked or changed.

For additional guidance from the NCSC regarding the sanitisation process, click here.