Linklaters

May 2017

Cyber Crises: The WannaCry Attack

The WannaCry attack provides a stark example of the damage that can be caused by a cyber-attack and provides a wakeup call for all companies of the need to protect against these attacks.

This alert explains the background to the WannaCry attack, the steps you should take when managing a cyber-crisis and the governance measures needed to avoid such a crisis developing in the first place.

Contents

The WannaCry Attack

What is the aim of the attack?

The WannaCry virus is based on a ransomware attack. A user is tricked into running a malicious software virus on their computer. That virus encrypts the data on that computer and demands payment, normally in bitcoins, to decrypt that data. It is not clear how users were tricked into running the WannaCry virus, though it seems likely that they were sent phishing emails containing the virus as an attachment.

Once the user's computer is encrypted they are faced with a choice; pay the ransom and hope their computer is then unlocked, or wipe the computer and restore it from its last good back up.

Why was WannaCry so serious?

Ransomware attacks are well known and have been around for over twenty years. However, the WannaCry virus used the EternalBlue exploit to supercharge the attack.

EternalBlue is a remote code-execution bug. It allows the WannaCry virus to spread to other computers on the same network, encrypting them and demanding further ransom payments. This includes not only unprotected desktop computers but also equipment containing embedded software. In the case of the NHS, this includes equipment such as scanners and other medical devices.

In other words, it only takes one user to run the WannaCry virus to potentially compromise all the other computers on the same network.

Which computer systems were affected?

Microsoft issued a software patch on 14 March 2017 to protect against the EternalBlue exploit. Installing that patch will protect against the worst effects of this attack. However, a large number of computers had not been patched when the WannaCry attack was launched on 12 May 2017. There are two reasons why this patching might not have taken place:

> The process of patching computers was still underway (or worse still there was no process to apply the patch). In practice, patches need to be tested to check they don't create other problems and then need to be applied to each computer. This takes time.

> The computer is not supported and so no patch is available. Many of the computers affected by the WannaCry attack were running Windows XP, which ceased to be supported in April 2014 (though the NHS extended their XP support for a further year). The lack of support means no protection is provided against new exploits to that operating system.

The WannaCry attack was very serious. It affected computers around the world. In the UK, the NHS was most seriously affected with reports of disruption in over 40 hospitals.

What are the legal implications?

The hackers behind the WannaCry attack have clearly committed a wide range of criminal offences. In the UK, this is likely to include a breach of the newly introduced section 3ZA of the Computer Misuse Act 1990 which carries a life sentence. In practice, a successful prosecution is likely to turn on the identification of the hackers and enforcement in their home jurisdiction.

The organisations affected by the WannaCry attack are also exposed to a range of regulatory liability. Data protection laws impose an obligation on data controllers to take appropriate technical and organisational measures to protect personal data. This means protection against not just unauthorised disclosure but also unauthorised destruction, loss or alteration. This is likely to include ensuring the personal data is not inaccessible because of unauthorised encryption.

Other sector specific rules might apply. For example, financial services firms affected by the WannaCry attack will need to consider if this demonstrates a failure to ensure appropriate risk management systems.

Would I need to notify this type of attack to a regulator?

The need to notify regulators of the attack will depend on the sector and jurisdiction in which the organisation is based. In the UK, there is no current legal obligation to inform the Information Commissioner of security breaches but she has issued guidance indicating that she would like to be informed of serious breaches on a voluntary basis. Finally, other sector specific rules might apply. For example, the UK Financial Conduct Authority must be notified of anything of which they might reasonably expect notice. That is likely to include serious ransomware attacks.

Managing a cyber crisis

Governance and values - The difference between the success and failure of a company in dealing with a crisis is their ability to identify the core values they will apply in responding and to then stick to them.

Without core values, companies:

> risk losing public credibility;

> face increased internal and external scrutiny; and

> have no place of principle on which to ground quick, reliable decisions.

Ensuring a quick response - It is important to set out at the outset what you know and what you don't know – not all the facts will be clear initially. Strong external partners (lawyers/accountants) can be useful in this process:

> they can help establish a core narrative with consistent and reliable facts; and

> they can be a useful counterweight to the pressure to go public within the first 24 hours, as they will take a longer view of the situation in a fulsome way.

Mitigating the risk of litigation - Keep civil litigation at bay until facts are clear and don't put too much weight on it – it can be damaging to engage in legalistic arguments about liability to consumers. Consider wider brand risk.

Regulators - Regulators should be managed carefully and should be informed before there is a press release.

Internal communications - Prevent whistle-blowers and leaks by managing internal communications properly.

Preventing a cyber crisis

Compliance - Successful attacks often arise out of avoidable mistakes and poor housekeeping. Good governance can:

> create structures which enable executives and the Board to engage and understand risk and test the proposed strategy;

> allow oversight over the implementation of risk mitigation; and

> ensure that, in the event of an attack, there is a clear narrative as to how the Company's cyber strategy was agreed and deployed.

Culture - A secure operating environment comes from everyone in the business understanding that their responsibilities for system security are as important as for physical assets.

A robust approach is needed – a strong tone from the top, practical policies, training and enforcement.

Strategy - Specific strategies are needed in relation to cyber risk to:

> monitor and audit compliance; and

> monitor and respond to threats.

These strategies should be integrated in the company's day-to-day practices.

Incident response - Incident response should be rehearsed – important to be aware of what could happen, what is operationally realistic and your potential exposures. Resilience and speed of recovery will become differentiators.

Technical and organisational - Appropriate technical and organisational measures should also be taken both by the company and its supply chain. The measures include:

> Using supported equipment and adopting a patching policy.

> The use of appropriate technical measures including firewall configuration, email scanning, and anti-virus software.

> Conducting appropriate penetration testing on your systems.

> Considering the use of intrusion detection software and data loss prevention software to detect breaches.

> Restricting the ability of users within your organisation to run unauthorised programmes.

> Training employees to spot phishing emails.

> A robust process to back-up information.

Authors: Richard Cumbley, Tom Cassels, Vanessa Havard-Williams, Peter Church

Contacts

For further information please contact:

Richard Cumbley
Global Practice Head of TMT and IP

(+44) 20 7456 4681

richard.cumbley@linklaters.com

Tom Cassels
Partner

(+44) 20 7456 3755

tom.cassels@linklaters.com

Vanessa Havard-Williams
Partner

(+44) 20 7456 4280

vanessa.havard-williams@linklaters.com

Peter Church
Counsel

(+44) 20 7456 5495

peter.church@linklaters.com

Linklaters LLP
One Silk Street