LOCKTON
UNCOMMONLY INDEPENDENT

Cyber Ransomware Update

Sophisticated Targeting

Even someone with a passing acquaintance with cyber security will be aware of the dramatic surge in ransomware over the past couple of years. This has been coupled with a very distinct change in the nature of these invasions. Whereas earlier attacks were more "scatter-gun" in their approach, they are now likely to be far more sophisticated and targeted, with increased focus on businesses rather than individuals, partly due to companies' greater familiarity with Bitcoin and the scope for greater rewards.

Cyber-criminals are using every opportunity to gain access to an organisation's IT network. In many ransomware situations, the attack will start with a phishing attack – a "simple" email with an attachment which, when clicked on by a recipient, causes malware to infect a computer. That phish may provide remote access to an employee's computer or network, allowing the IT system to be monitored over a period of time and the criminal to determine the greatest vulnerabilities of the company's network – sensitive data, timing issues or other pinch points.

A Two-pronged Attack

Another worrying trend in the ransomware space that has been getting a significant amount of traction over the past few months, is the two-pronged ransomware attack: not only is data encrypted and a ransom demanded on the promise of decryption, but the data is also exfiltrated. Typically, the cybercriminals publish the victims' names with the threat that, unless a second ransom is paid, compromising stolen data will be released into the market place.

Whereas previously, a company might have been able to avoid payment of a ransom demand due to ability to recover data from back-ups, more organisations are being forced to confront the reality of paying a ransom to avoid the compromising publication of exfiltrated data.

Sky-rocketing Ransom Demands

Anecdotally, the ransom demands themselves have also increased substantially, such that the average demand has gone from $28,920 in 2018, to $302,539 (BakerHostetler, 2020 Data Security Incident Response Report).

Cyber-crime is big business. Further enhancing the viability of this "business model", some cyber-criminals are now operating "affiliate" programmes whereby they rent out their ransomware as a service to other attackers, widening the pool of those with access as well as their financial return.

Simply put, this illegal business model is booming and we don't anticipate any sign of it abating in the near future.

The message is clear. It is vital for every business to take the time to analyse the potential impact of a ransomware attack, including assessing the effects of downtime to the business as well as reputational harm. Officers and executives should ensure they have thoroughly discharged all responsibilities to their stakeholders, in terms of identifying and mitigating cyber risks in a manner appropriate to their businesses.

Claims Notifications Doubled/Claims Costs Increasing Ten-fold

The dramatic increase in frequency and severity of ransomware incidents has been evidenced in the claims statistics collated by Lockton's Cyber and Technology Team. The number of notifications in the first eight months of 2020 has been double the number in 2019, with average claims costs increasing ten-fold. Costs are only likely to increase further.

It is important to note that Lockton's claims experience is a portion of the wider cyber insurance market and therefore only a snapshot of the overall problem.

Of the 2020 declared incidents, the following is a breakdown of ransomware type.

Type	Description
Defray777	Targeted attack traditionally seen in the healthcare sector. Spreads via Microsoft word attachments in email and encrypts any data it finds. Increase in attacks outside of the traditional target industry.
Maze	Encrypts all files that it can in an infected system and then demands a ransom to recover the files. It also exfiltrates data with the attackers telling their victims that, if they do not pay, they will release the information.
Netwalker	Like Maze, it encrypts all files that it can in an infected system and then demands a ransom to recover the files. It also exfiltrates data and the attackers tell their victims that if they do not pay, they will release the information.
Robin Hood	Targeted attacks, where the threat actors make sure that essential files are encrypted so they can ask for large ransom amounts.
Ruyk	Targeted attacks, where the threat actors make sure that essential files are encrypted so they can ask for large ransom amounts.
.waiting	Ransomware which proliferates inside a work-station allowing bad actor to access the computer and lock files.
Vendor Incident (Blackbaud)	Ransomware attack on Blackbaud (cloud computing provider) that exfiltrated donor information of a significant number of not-for-profit organisations.
Vendor Incident (not specified)	Incident occurring at an insured's vendor without specific knowledge of the exact type of attack (variant).

Minimising Risk

There are several measures that businesses can take to minimise their ransomware risk. The following steps will certainly assist:

Governance

- Appoint individuals with clear responsibility for cyber security and develop a clear plan of reporting through to the board/management.
- Invest in an Incident Response Plan.
- Invest in a Business Continuity Plan.
- Consider the transfer of risk to a market-leading cyber insurer.

Security

- Invest in vulnerability assessments, including penetration testing and red teaming.
- Ensure additional procedures are put in place to counter increased network weaknesses involved in having a remote workforce, including MFA, the operation of remote desktops or VPNs, separation of employee and work data, safe use of portable devices, limited use of public wi-fi, security controls for video-conferencing etc.
- Install software updates, especially critical updates on a regular and prioritised basis.
- Back-up data to secure platforms, preferably off-line. Generate multiple back-ups.

Human Factors

- Invest in employee education, including the publication and distribution of policies and procedures covering phishing, transfer of funds, information security etc.
- Operate a "safe" work environment where employees feel comfortable sharing information regarding possible compromised security.

For more information, please contact the Global Cyber & Technology Team:

Vanessa Cathie
Vice President, Global
Professional & Financial Risks
T: +44 020 7933 2478
E:vanessa.cathie@uk.lockton.com

Liam Brown
Assistant Vice President, Global
Professional & Financial Risks
T: +44 020 7933 2719
E:liam.brown@uk.lockton.com

Peter Erceg
Senior Vice President, Global
Professional & Financial Risks
T: +44 020 7933 2608
E:peter.erceg@uk.lockton.com

LOCKTON
UNCOMMONLY INDEPENDENT