Ransomware guide: What you need to know
After ransomware again hit the headlines in 2017, it has fast become one of the top security concerns for businesses and organizations of all sizes.

The reality is that ransomware attacks are increasing, and thanks to increasingly sophisticated encryption technology, the threat is constantly evolving. This ebook will help you understand ransomware, how it could impact your business and what you can do to prevent it from damaging your operation.
Chapter 1: What is ransomware?

Ransomware is a type of malicious software that blocks access to a computer using an algorithm to encrypt your files and data.

It then demands a financial ransom, with a variety of tactics to compel you to pay up or lose your data forever. Payment is often requested in the form of an anonymous online currency such as Bitcoin, which makes tracking the criminals very difficult or impossible.

Ransomware is spread via spam or targeted campaigns, often arriving in an unsolicited phishing email or an attachment. Phishing attacks use emails disguised to look like they’re from someone you know and are more likely to trust. They typically ask you to click on a link or attachment to perform a routine task such as updating records or account details. Do this and the ‘worm’ or malware downloads and infects your computer, locking your system and encrypting your files. Ransomware can also infect a system using vulnerabilities in a computer’s browser or via malicious code hidden in online ads, an attack vector called ‘malvertising’.
The most notorious and dangerous families of ransomware currently active are **Locky, Cerber, WannaCrypt and CryptXXX**, though new variants are constantly appearing. The majority of these affect Windows-based systems but some, like Lockscreen, target the mobile Android operating system. The evolving nature of the threat makes ransomware very difficult to counter.

**Ransomware can affect businesses of all types and sizes.** Cybercriminals have shifted their focus to more lucrative commercial targets, such as large corporations and government agencies, that often have high-value data. **Small to medium business (SMBs) are also targets, and are particularly vulnerable to ransomware with their limited IT resources.** They are also more likely to pay the ransom in the hope they’ll get access to their data again, though this is not always the case.
Chapter 2: Counting the cost of ransomware

According to malware security firm Barkly, a company is hit with a ransomware attack every 40 seconds.

This is only likely to escalate as cybercriminals turn away from targeting individuals and focus on more lucrative victims, like corporations and government agencies. Barkly also identified ransomware as the most prevalent form of malware, with “4.3x new ransomware variants in Q1 2017 than in Q1 2016”.

And while attacks do generate revenue for cybercriminals, the real impact of ransomware is felt by smaller businesses, which often have limited IT resources and poor security protocols to deal with an attack. A study for security software provider Malwarebytes found that while ransom demands are typically small, **22 per cent of businesses were forced to cease operations immediately**—leading to a crucial loss in revenue. Organisations in the healthcare and education sectors are also attractive targets, as they too tend to have weaker security systems and hold valuable, sensitive personal information.
One of the highest profile cases of ransomware occurred in May 2017, when the WannaCry worm infected Great Britain’s National Health Service (NHS) in a ransomware attack that affected nearly 100 countries worldwide. Security experts believe an NHS user opened a file or clicked on a link they shouldn’t have. The NHS’s ageing IT infrastructure and outdated software were also factors that facilitated the spread of this ransomware variant, with many health trusts using an unsupported, unsecure version of Windows.

Cybersecurity experts are divided about paying a ransom to hackers. Firstly, there is no guarantee you’ll regain access to your encrypted files. Attackers have been known to demand multiple ransoms from the same business, while others have simply chosen not to reverse the encryption. Paying the ransom is also likely to encourage the cybercriminals to continue with their activities, which only serves to compound the problem.
Spotting ransomware can be difficult as cybercriminals fine-tune their tactics and become more sophisticated.

Chapter 3: Recognizing and recovering from a ransomware attack

Spotting ransomware can be difficult as cybercriminals fine-tune their tactics and become more sophisticated.

The leading cause of ransomware infections is a lack of awareness and cybersecurity training, especially in SMBs, which often don’t have the technical or financial resources to counter the threat. All it takes is one unsuspecting employee clicking on a link in a phishing email to unleash a ransomware infection.

Protecting your data can be as simple as educating your users, updating your systems and backing up your data. Best practice is to train your staff to look for anything that doesn’t seem quite right. This could be an email or social media message from strangers, where the link has a strange URL or the attached file has an unusual file extension.
Users should also be wary of ‘free’ downloads or clicking on links to unfamiliar websites. Microsoft suggests businesses look to protect, contain and isolate their high-value digital assets, and work on the assumption that they will suffer a breach. Protect your network by:

- Developing a detailed cyber-incident response plan.
- Training your staff to recognize malicious sites, social engineering tactics and phishing attacks.
- Having a clear security protocol that discourages users from clicking on suspicious links, attachments or emails.
- Ensuring technical staff have a rigorous security process.
- Installing the latest antivirus and anti-ransomware software applications.
- Backing up your systems regularly to physical sources and the cloud.
- Investing in hardware and software that’s up to the task of detecting and warding off ransomware threats.
- Constantly analyzing the traffic on your network for threats.
Ultimately, one of the most effective safeguards against a ransomware attack is to **backup data continually and keep multiple copies of your backups**. Malicious files can lay dormant on your system for some time before showing themselves, meaning recent backups could also contain corrupted files. This is why it’s paramount to keep older backups on hand, both online and off. 

**Make sure you keep multiple backups off-site on an isolated drive, as well as on the cloud to ensure your data is kept secure.**

If your network is compromised, look to isolate the infected machine(s) from the network and alert all staff, disable all shared drives and identify the source of the ransomware infection. You should then update your security software and run a full scan of your network. The infected machines can then be wiped and restored from backup.
Conclusion

Ransomware doesn’t discriminate.

Ignoring the threat could risk the loss of your data, compromise your ability to operate, damage your reputation, or worse. This is why it is critical your organization has a clear strategy to mitigate the threat, contain a breach and get back to business as usual ASAP.

Sources

https://blog.barkly.com/ransomware-statistics-2017
https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack
http://www.techadvisor.co.uk/feature/security/ransomware-pay-or-not-pay-get-your-files-back-3635730/