Top 5 cyber threats in 2019

How to protect your business from hackers

The cost of cybercrime

No business can afford to ignore the threat of cybercrime.

From ransomware and phishing scams to DDoS attacks, PUPs and cloud account hijacking, hackers employ a range of techniques to infiltrate business networks and steal private data.

In this ebook, we set out the top five most common cyber threats, what you can do to prevent them, and how to respond when an attack strikes your business.

The global cost of **cybercrime** is expected to **exceed $2 trillion** in 2019.

Ransomware attacks are predicted to cost the global economy **$11.5 billion** in 2019.

The global average cost of a **data breach** was **$3.86 million** in 2018 – **up 6.4 per cent** on 2017.

Threat 1: Malware/ransomware

Malware is a catch-all term for malicious software that hackers use to wreak various forms of havoc.

That may include monitoring keystrokes to steal passwords, infiltrating secure databases, and even taking control of your IT infrastructure. Ransomware is a type of malware that hackers use to block access to your private data. Hackers often demand a ransom payment from businesses to restore your seized data.

MALWARE IN PRACTICE

In May 2017, WannaCry malware infected 230,000 computers across 150 countries. Hackers exploited a security loophole in an old version of Windows, seized private data and requested ransom fees to unlock it.

Malware/ransomware:

What to do pre-hack

- Keep all your software up to date. That includes your OS, browsers, antivirus applications, firewalls, and spam filters.
- Ensure all your data is encrypted, and back up your data on secure servers as regularly as possible.
- Educate your staff about the dangers of clicking on suspicious email links, using unsecured mobile devices, and downloading software applications without IT approval.

What to do post-hack

- Immediately disconnect any infected terminals from your network and shut them down.
- Change all passwords used to access sensitive data.
- Communicate with your customers about any data that has potentially been exposed and keep them in the loop as you work to fix the problem.

Threat 2: Phishing attacks

Phishing is a set of tactics hackers use to encourage targets to unwittingly download malware or divulge passwords or financial information.

Tactics include phony emails that request personal data and fake websites that resemble official portals your staff frequently use, in order to steal login information.

PHISHING IN PRACTICE

In 2013, hackers gained access to retail chain Target's data centres via a phishing attack on a third-party vendor. They breached 40 million retail card accounts and stole data that affected 110 million users.

Phishing attacks:

What to do pre-hack

- Ensure all staff understand how to identify common phishing tactics.
- Regularly alert your employees about current phishing scams and what to look out for.
- Maintain up-to-date spam filters and monitor incoming email for suspicious links.

What to do post-hack

- If the phishing attack results in a malware download, follow the post-hack steps in the previous chapter.
- If the phishing attack steals login information, immediately contact your service providers and freeze accounts.
- If you suspect hackers are stealing employee or customer information for the purpose of identity fraud, contact your local authorities.

Threat 3: Distributed denial-of-service (DDoS)

DDoS attacks target your critical infrastructure, aiming to take your IT systems, network, or website offline for an extended period.

Hackers often use the combined processing power of multiple malware-infected computers to bring down major IT systems and disrupt mission-critical operations.

DDOS IN PRACTICE

In 2016 the Mirai botnet took down web app provider Dyn's servers in a DDoS attack that crashed clients' websites including Twitter, Netflix, Reddit and CNN. The attack flooded Dyn's servers with bot-based traffic until the company's network collapsed.

Distributed denial-of-service (DDoS):

What to do pre-hack

- Upgrade to security-enhanced server hardware and the latest operating system software to ensure your data center is protected.
- Use advanced threat identification, assessment, and filtering tools to monitor for potential DDoS attacks.
- Secure your network with firewalls, two-factor authentication, VPNs, and other intrusion-prevention systems.

What to do post-hack

- Restart your firewalls and restore your applications one by one to prevent a flood of traffic that could crash your network again.
- If your website has been attacked, you'll likely need to contact your provider to unblock your ISP.
- Gradually reconnect customer sessions to prevent all your customers from trying to connect to your network at the same time.

Threat 4: Potentially unwanted programs (PUPs)

Also known as Trojans, spyware, and adware, PUPs are unwanted programs, usually disguised in other software downloads, that infiltrate your terminals.

They may infect your system with inappropriate gambling or pornography content, advertising pop-ups, redirect your homepage to unsecured websites and generally slow down your system.

PUPS IN PRACTICE

CinemaPlus is a common PUP that tends to be bundled with other software or is downloaded from links in spam emails. It changes browser settings and may hijack homepages, redirect users to inappropriate websites, open browser tabs and display excessive advertising pop-ups.

Potentially unwanted programs (PUPs):

What to do pre-hack

- Ensure your employees are not downloading software apps without approval from your IT team.
- Install and auto-run antivirus software on your terminals to scan for PUPs.
- Always use custom installation options and opt-out of any bundled applications.

What to do post-hack

- Identify any PUPs in your ‘programs and features’ list and uninstall them.
- Run a full antivirus scan to ensure no unwanted applications are lingering in your system.
- Reset your browser settings and delete existing cookies.

Threat 5: Cloud account hijacking

Hackers use automated tools to ‘guess’ usernames and passwords to gain access to cloud accounts.

Bots are typically able to try thousands of passwords in seconds, and once they’ve entered a successful combination, give hackers complete access to the user account.

CLOUD ACCOUNT HIJACKING IN PRACTICE

Tesla’s Amazon Web Services cloud infrastructure was recently hijacked as part of a widespread cryptojacking attack. Tesla was able to lock down cloud access within the day to limit the data that was exposed to hackers.

Cloud account hijacking:

What to do pre-hack

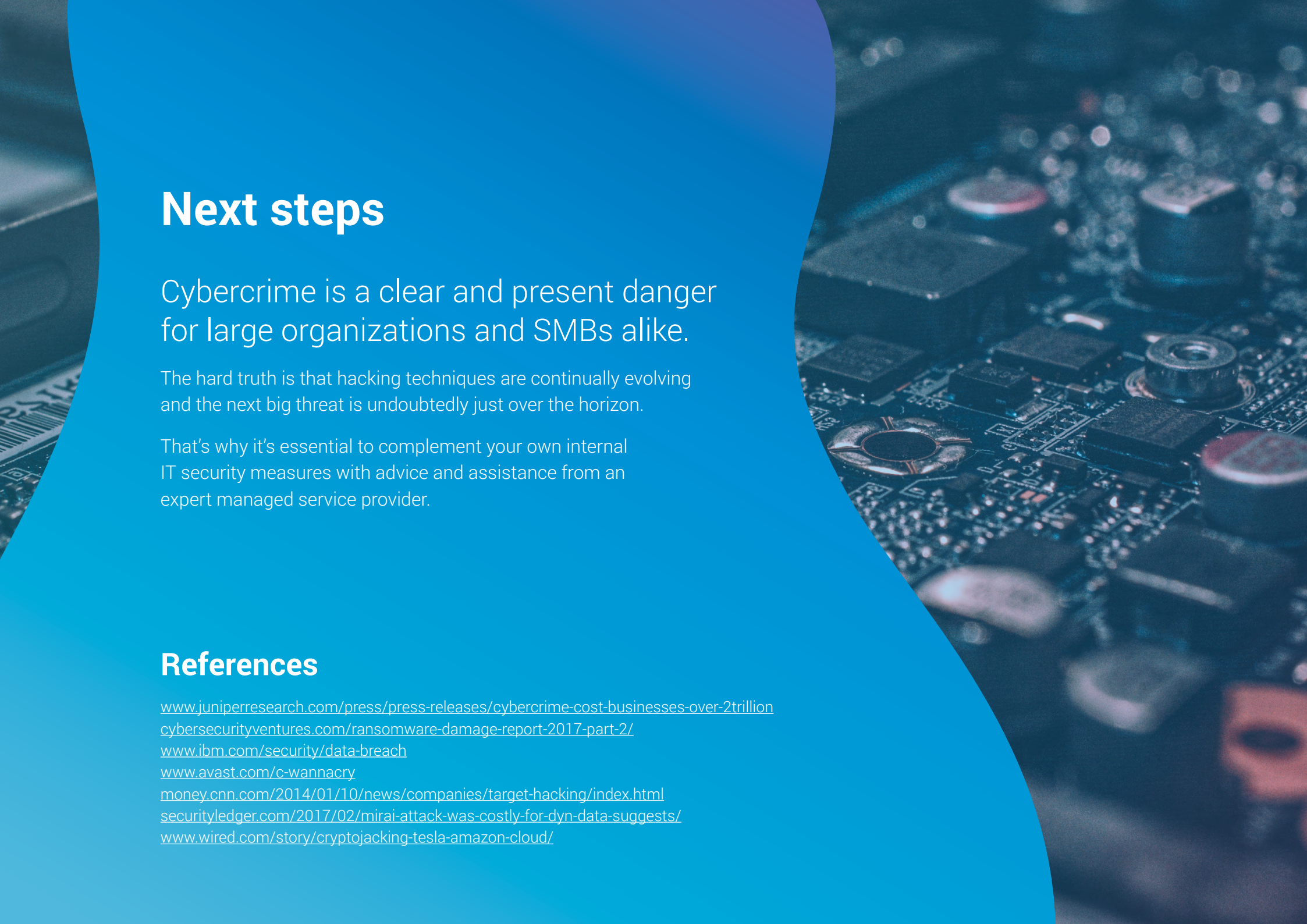
- Only use cloud vendors that automatically lock accounts after a specified number of unsuccessful login attempts, or use multi-factor authentication.
- Don't rely on your cloud vendors for data encryption. Always encrypt data before you upload it to the cloud, so you control the process.
- Restrict IP addresses that are authorized to access cloud platforms, and instruct staff not to share login information with colleagues.

What to do post-hack

- Immediately change the passwords for all your cloud accounts, not just for the hacked account as hackers may still be targeting your organization.
- Contact the cloud vendor to lock the account immediately and identify the data that has been compromised.
- Communicate with your customers about the breach and how it may affect them.

Threat protection and response checklist

THREAT	PRE-HACK ACTIONS	POST-HACK ACTIONS
1. Malware/ransomware	• Update your software • Encrypt and back up your data • Educate your staff	• Disconnect infected terminals • Change all account passwords • Communicate with your customers
2. Phishing	• Know how to identify common phishing tactics • Alert your employees about current phishing scams • Maintain up-to-date spam filters	• Follow malware post-hack actions • Contact your key service providers to freeze accounts • Contact local authorities to report possible identity fraud
3. DDoS	• Upgrade to security-enhanced server hardware • Use advanced threat identification tools • Use firewalls, two-factor authentication, and VPNs	• Restart your firewalls • Contact your provider to unblock your ISP • Gradually restore your applications
4. PUPs	• Don't download software without IT approval • Use antivirus software to scan for PUPs • Select custom installation options	• Uninstall PUPs from 'programs and features' • Run a full antivirus scan • Reset your browser settings and delete cookies
5. Cloud account hijacking	• Only use cloud vendors that automatically lock accounts or use multi-factor authentication • Encrypt your data in-house • Restrict internal access to cloud platforms	• Change the passwords for all your cloud accounts • Contact the cloud vendor immediately, to lock the account • Communicate with your customers about the breach



Next steps

Cybercrime is a clear and present danger for large organizations and SMBs alike.

The hard truth is that hacking techniques are continually evolving and the next big threat is undoubtedly just over the horizon.

That's why it's essential to complement your own internal IT security measures with advice and assistance from an expert managed service provider.

References

www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
cybersecurityventures.com/ransomware-damage-report-2017-part-2/
www.ibm.com/security/data-breach
www.avast.com/c-wannacry
money.cnn.com/2014/01/10/news/companies/target-hacking/index.html
securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/
www.wired.com/story/cryptojacking-tesla-amazon-cloud/