single point of contact

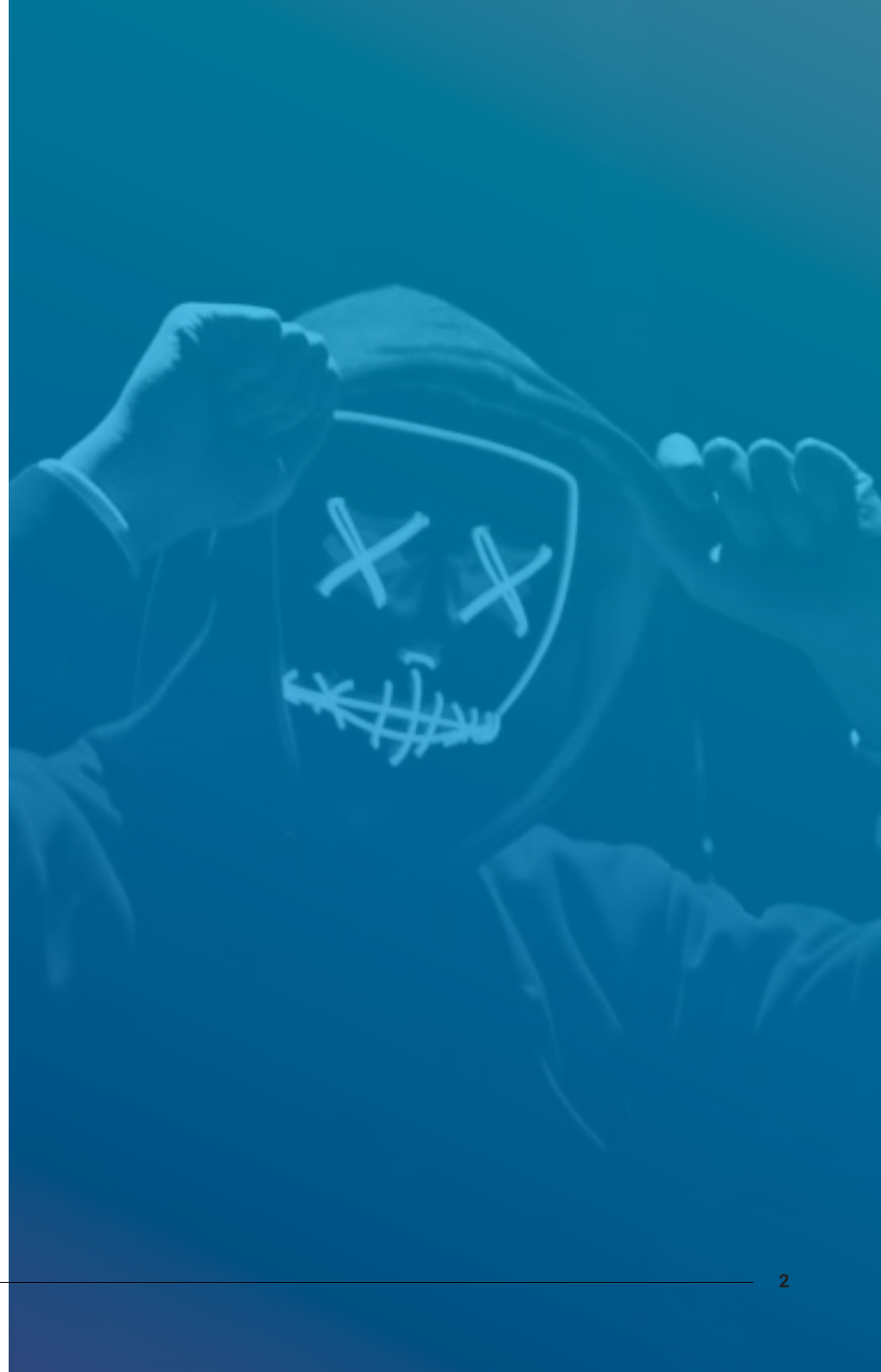
How to protect your business

Ransomware, human vulnerability and the IoT are rising threats

In the last year, cybersecurity breaches hit headlines like never before.

From cybercriminals penetrating Equifax and stealing the personal data of 145 million people to WannaCry ransomware locking down machines in more than 150 countries, the threat environment is rapidly evolving.

Huge violations like these make for great media fodder, but they're also symptomatic of a surge in sophisticated cyberattacks that's only going to get worse as the Internet of Things (IoT) connects millions of devices to the internet.

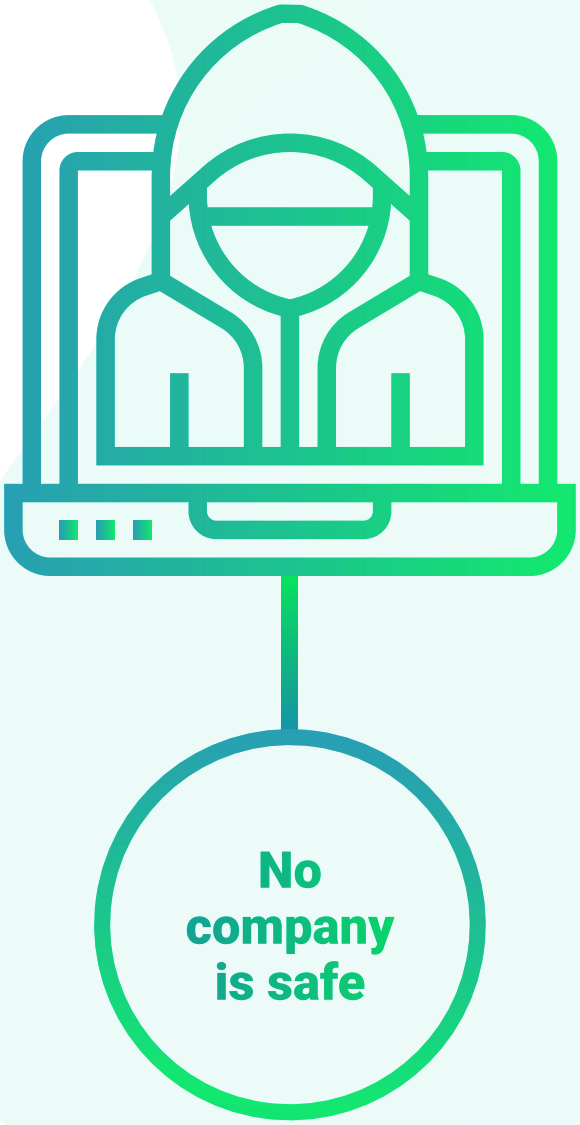


From big firms to small biz

Hacks on credit bureaus, healthcare systems and multinationals are the ones most publicised, but even small businesses are in the firing line for cybercriminals.

Equifax – one of the largest credit bureaus in the world – was attacked in July last year, with the personal data of more than 145 million people stolen. Largely considered among the worst security breaches in history, the fallout was made exponentially worse when it was revealed the company only announced the hack two months after the attack had occurred.

The effects will be felt for years to come, with such a major breach raising concerns around how information is collected and stored – no matter the size of the business.



Employee threat

Former Equifax CEO Richard Smith blamed the security failure on a single person. This should serve as a warning to small to medium business (SMB) owners that the number-one security concern is still the human factor.

Workers are the most vulnerable part of any business. They can be fooled by increasingly sophisticated phishing scams, they often bring their own (unsecured) devices onto a company network, and they may lack the education or skills to make good IT decisions.

Social media listening was once a tool for marketers who tracked mentions of their brand across social media channels for reputational analytics. But the same tool can be used to follow employees and identify those with financial woes, or to gather enough personal data to tailor phishing emails or hold workers to ransom.

Meanwhile, the growing mobile workforce, and the bring your own device (BYOD) revolution, have brought employees' devices under the purview of a company's cybersecurity measures, vastly increasing the complexity of securing the network. These are mostly smartphones and laptops, but thanks to the IoT, businesses will soon need to worry about connected cars, wearable devices and their smart management systems for lighting and heating.

It’s all about training

With regular cybersecurity training, employees can stay across new threats, and complex challenges can be met with intelligent solutions.

According to Crowd Research Partners’ Insider Threat 2018 Report, 90 per cent of organisations say they are vulnerable to insider threats – a massive 26 percentage-point jump from the 2016 survey. However, despite the headline -hitting breaches of last year, more than a quarter (27 per cent) still don’t have the appropriate controls in place. Whether maliciously or inadvertently, employees, contractors, clients and business partners can all allow hackers access to your network.

To stay vigilant, businesses must conduct ongoing security audits to uncover gaps in training or IT skills, and then move immediately to fill them. Beyond that, changing how workers access the network can lessen the impact of human vulnerability.

Modern protection methods

Businesses can employ various strategies to bolster their security:

- **Two-factor authentication:** Using single-use codes on mobiles or in emails to access the network.
- **Intrusion monitoring:** Intrusion detectors can monitor system and network activity, generating alarms – such as an email alert – based upon what it identifies as a potential security breach.
- **Biometrics:** Using facial recognition or fingerprint scanning in place of passwords. Voice recognition from AI assistants like Apple's Siri, Microsoft's Cortana and Google Home are increasingly being found in call centres in order to prevent fraud.
- **Access analytics:** Monitoring, and when necessary locking down, access based on behaviour. Examples include: checking when and where the person is logging in and whether that's typical; using keystroke assessment to watch for bot activity; and identifying what device are they using – only allowing access on certain devices.

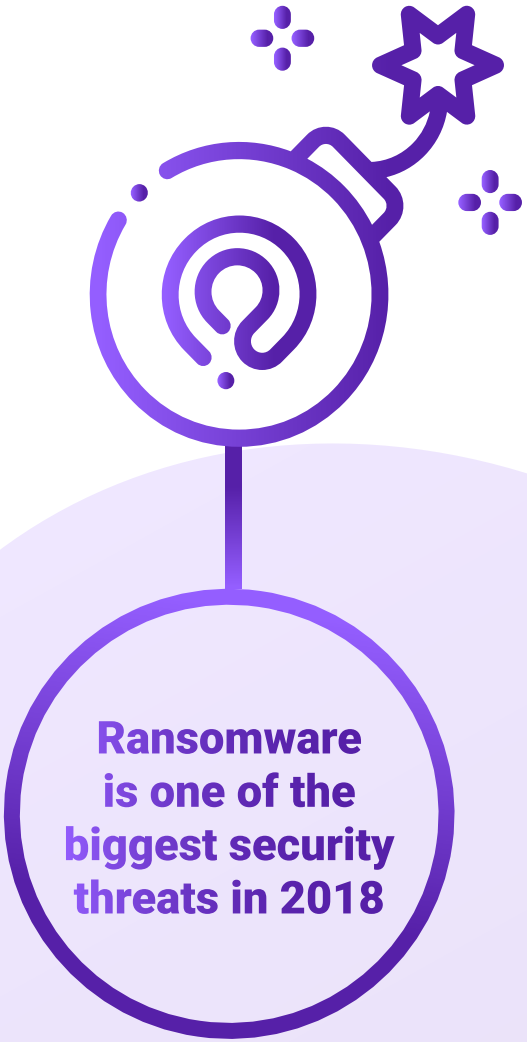
Modern-age ransom

Politically motivated breaches, such as alleged Russian state-sponsored cyberattacks on Australia, Britain and the United States, will always make headlines, but profit is always the motivator for criminals.

That's why ransomware is one of the five biggest cyber threats of 2018, according to *Forbes Technology Council*.

Not only is it a simple and effective way to get to profits, but holding a company's data to ransom has never been easier. Ransomware-as-a-service models have cropped up in cybercrime circles, and open-source ransomware programs are even being hosted on places like GitHub and hacking forums – meaning anyone can access them, often for free.

"We have 'freemium ransomware' – who wants to pay for a service in 2018?" said James Lyne, global head of security research at Sophos.

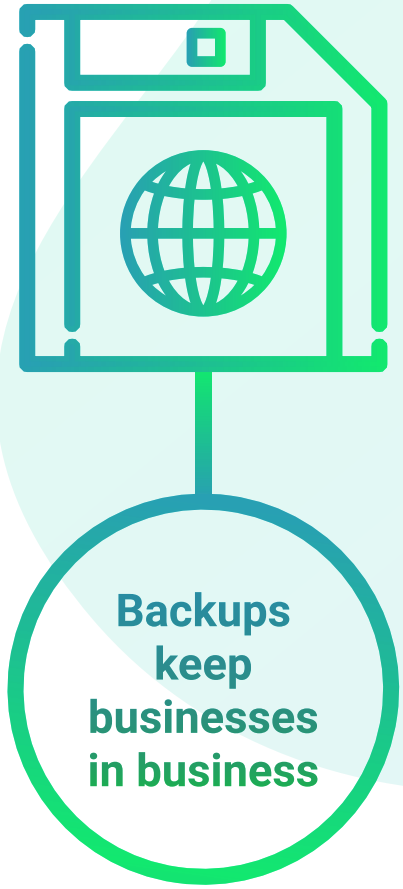


Protect your backups

Companies that pay the ransom often never see their data returned. There's only one way to protect against ransomware – stop it infecting your systems in the first place.

Firms must invest in good malware protection and regularly clean up email inboxes, as well as educate their employees on phishing scams and the dangers of clicking on unusual email links. On top of that, they need to invest in regular, offline backups of crucial data. While attackers can still threaten to expose breached data, backups mean businesses can at least continue to operate.

Security experts have long warned about the growing threat of the IoT, and in recent years they have been proven right. From the Mirai botnet exploiting major ISPs – like TalkTalk, Deutsche Telekom, KCOM and Irish telco Eir – to cybercriminals shutting down building heating in Finland to botnet barrages on university campuses, IoT-driven attacks can strike hard and fast – anywhere, anytime and in a variety of guises.



Securing the insecure

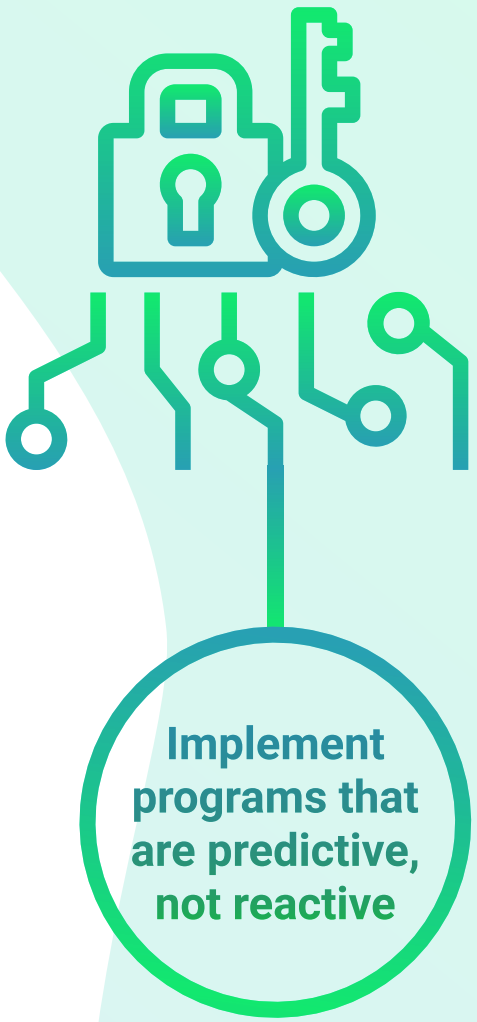
IoT attacks have become more intelligent and more focused – a trend that will continue.

Technavio predicts the sensors of IoT-connected devices will come under attack. Whether that's beaming infrared signals to cameras or using ultrasonic signals to penetrate voice-activated devices, security experts will need to develop functional solutions fast.

And with IoT security spending set to exceed $1.5 billion by the end of 2018, according to a *Gartner* survey (up 28 per cent from 2017 figures), businesses need to implement best practices and tools in the workplace to avoid becoming a statistic.

"Although IoT security is consistently referred to as a primary concern, most IoT security implementations have been planned, deployed and operated at the business-unit level, in cooperation with some IT departments" said Ruggero Contu, research director at Gartner.

"However, coordination via common architecture or a consistent security strategy is all but absent, and vendor product and service selection remains largely ad hoc."



Predict to protect

There are ways to ensure that all IoT-connected devices are as safe as possible for the enterprise.

Microsoft recommends a number of hardware strategies in its *Internet of Things security best practices*, including:

- Be specified to minimum requirements only, so it can't do more than required.
- Be tamper-proof, for example having no USB ports.
- Be built around secure hardware like a Trusted Platform Module (TPM).
- Have a secure method for firmware updates.

Companies deploying and operating IoT devices must:

- Ensure they are tamper-proof.
- Keep authentication keys safe after deployment.
- Keep systems up to date with the latest operating system (OS) versions and drivers.
- Secure the OS with anti-malware software.
- Protect cloud credentials by changing passwords frequently and not logging in from public machines.
- Audit the IoT infrastructure regularly.

As IoT threats multiply, the cybersecurity's focus must change, from deploying simple systems that meet specific challenges to adopting an intelligent, analytical and holistic approach.

Reactive programs are no longer enough. Firms must become predictive and able to adapt.

Seeking outside help

AI-based cybersecurity is a gargantuan task for SMBs.

Small firms are easy targets for cyberattacks because they frequently lack dedicated cybersecurity staff or relying on a tiny – and often under-resourced – IT team.

A managed security service provider (MSSP) could be the answer for SMBs. A recent survey conducted by Vanson Bourne suggests that "SMBs are beginning to realise the value of external security support", identifying new security resources to protect their assets.

"SMBs have begun to rely heavily on channel resellers and MSSPs for informed recommendations about the best security strategies and equipment," said Himanshu Verma, director of product management at WatchGuard.

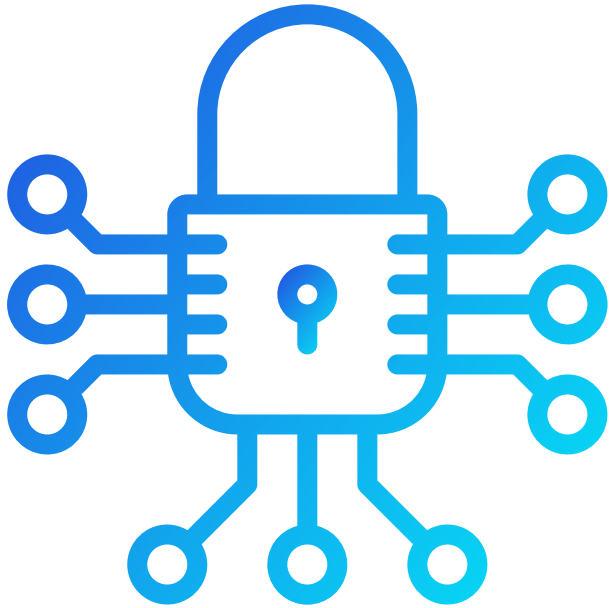
Securing today for a safer tomorrow

Whether SMBs employ an MSSP or an internal security team, they need to change their approach to cybersecurity, from reactionary programs to intelligence-driven, predictive solutions.

Skills and training must be top priorities for employees, and companies have to move away from passwords alone as a method of authentication.

Protecting crucial data is about more than just keeping it behind perimeter security; it also needs to be regularly backed up to mitigate the threat of ransomware.

Finally, the fast-evolving world of the IoT needs to be approached cautiously for businesses to reap the benefits without opening themselves up to new avenues of attack.



About Single Point of Contact

Single Point of Contact stays on top of everything related to cyber security and data protection. We are more than just a Managed Security Service Provider. We take swift and thorough action to ensure your business is protected around the clock and to remediate any security threats when they occur. Constant monitoring of any network is a requirement nowadays, and we are pleased to provide the most comprehensive security solution to our clients. To learn more about how we can help protect your business from cyber-attacks, contact us today.