White Paper

Cyber Security for SMEs: A Practical Guide to Protecting Your Business

nasstar

CONTENTS

Introduction

Think cyber threats only affect large enterprises? Think again. The FSB found last year that smaller UK firms are actually bearing the brunt of online threats – at a combined cost of nearly £5.3 billion. In fact, SMBs are attacked a staggering seven million times each year, despite the vast majority (93%) taking some steps to protect themselves.

It's clear that the volume and sophistication of threats have outstripped the ability of UK SMBs to effectively respond. And that has a very real cost. The impact of a major data breach or system outage could, in a worst-case scenario, lead to:

- Investigation, remediation and clean-up costs
- Legal fees
- Regulatory fines – especially the forthcoming European GDPR, which from May 2018 will levy maximum fines of up to €20m for serious infractions
- Lost customers
- Brand damage
- Share price slump
- Loss of IP as competitive differentiator
- Increased helpdesk/IT workload
- Service outages
- Staff productivity hit

PwC estimates the cost to a small business of between £75,000 and £311,000 per data breach, but it could go far higher in some cases. Financially motivated cybercriminals have calculated that SMBs sit at the sweet spot between consumers and large enterprises: in other words, they're a treasure trove of lucrative customer data and sensitive IP, but typically have fewer resources to mitigate the risk of attack. As such, SMBs can also be an attractive target for hackers looking to attack larger organisations which they may be partnered with. In the United States, the breach of major retailer Target, which affected up to 70 million people, occurred via a third party contractor with poor security.

The challenge for senior managers is where to begin. You're not only faced with a determined and agile online foe but also the threat of compromise stemming from deliberate or accidental employee actions. Often budgets are tight. And there's the ever-present risk of dialling up security too far, to the point where it starts to impede staff productivity. The good news is that help is at hand. We've put together this quick and easy guide to highlight the key threats facing your organisation. And most importantly, what you can do to protect mission critical data, mitigate risk and keep the business running smoothly. GCHQ reckons up to 80% of cyber attacks seen today can be prevented with basic risk management. Let's see how.

A world of threats

There's certainly no shortage of threats out there. And they affect all parts of your IT infrastructure: endpoint, network, servers and the cloud. Cybercriminals are spoiled for choice and they have the element of surprise. And as if that wasn't a big enough advantage, the dark web is bursting with underground forums where they can buy and sell hacking tools in pre-packaged exploit kits. It all means launching cyber attacks has never been easier – even for those with limited technical know-how. Then there's the ever-present risk posed by careless or malicious insiders.

Here are a few of the main threat types and key areas of vulnerability:

Social engineering: this is more of a technique than a distinct threat type. It's the practice of conning or manipulating the victim into bypassing security best practice without them even realising it, so that they divulge private details or download malware. It's used in many types of attack, particularly phishing and malware-borne emails.

Ransomware: malware that will usually work its way through all your networked systems, encrypting data as it goes. Unless you're lucky enough to be infected by a version for which there are keys available, the only way to regain access to your corporate data is by paying the ransom.

Phishing/Spearphishing: tried and tested technique designed to get victim to divulge sensitive information for use in follow-up attacks, or download malware. Spearphishing is aimed at a smaller number of employees and commonly contains malware as the first stage in a targeted attack.

Vishing/Smishing: These are effectively phishing attacks conducted over the phone, or in the latter case, via text, with the same end goals.

Targeted attacks: originally aimed at large organisations and the preserve of nation states and major cybercrime gangs, but now increasingly common. They use spearphishing emails to trick members of staff into clicking on a link or opening an attachment, triggering a secret malware download. Once inside your network, attackers can lie hidden for weeks, months or even years, stealing sensitive information.

Banking Trojans: malware designed to secretly steal corporate banking credentials, providing the cybercriminals with the keys to your company account.

DDoS: no organisation is too big or small to suffer a Distributed Denial of Service attack. It's designed to overwhelm your computer systems with traffic, effectively forcing your business offline. They can be launched by hacktivists out to generate publicity for their cause, blackmailers, or even data thieves looking to distract your IT team while the go after your sensitive data.

BYOD: Bring Your Own Device can provide a major productivity boost for any company, and reduce up-front expenditure on corporate-owned devices. But it introduces risks if devices are not suitably managed. They can be lost or stolen, raising the risk of data theft from the handset. And malware could be downloaded via innocent-looking apps or emails/websites viewed on the device. There's also a risk of hackers snooping on your staff from insecure public Wi-Fi networks. Any device which connects to the network may therefore also allow attackers to gain entry into key systems. The risk will only increase with wearables and other 'smart' devices.

Cloud computing: reputable, accredited cloud providers are usually a safe bet for securing your data. But organisations can't afford to be complacent. Various cloud models and providers require varying degrees of effort on the part of the customer to secure their data. Fail to read the small print and you could be in trouble.

Business Email Compromise (BEC): in these attacks a hacker will target someone in your finance or accounts payable department, with an email spoofed to appear as if coming from the CEO. It will ask for an urgent transfer of funds out of the business. These scams have landed cybercriminals over $2 billion in just two years, according to the FBI. Training staff is essential to stop the threat.

Your employees: any organisation is only as strong as its weakest link. And the truth is that your staff are exactly that. A Ponemon Institute poll of over 18,000 US IT staff found that 36% believe malicious insiders and 40% of negligent staff are the greatest risk to IT security. They could send data in error outside the company, or maintain easy-to-crack passwords which allow hackers to guess their way inside systems. And if your IT security is too restrictive then they may try to circumvent it via cloud-based services and consumer devices, presenting a major "shadow IT" risk. That's why training and awareness programmes are essential.

The fightback starts here

The threats are such today that no organisation can claim to be 100% protected. But if you put a few of the following controls in place, your organisation begins to become less appealing to hackers – most of whom are looking for the quickest and easiest RoI. If that fails, then make sure you have the right tools and processes in place to detect and respond as quickly as possible to an attack. The average time it takes for an organisation to identify a malicious attack on its network stands at 229 days. And it typically takes another 82 days to contain the threat. But the longer it's left on your network, the more damage it can do and the more expensive it will be in the long run.

The following controls will all reduce your cyber security risk:

Automated patch management: this will keep all key systems and software up-to-date with the latest security patches. In one swoop you will be safe from 90% of software exploits.

Back-up: vital to mitigating the risk of ransomware. Follow the 3-2-1 rule: at least three copies, in two different formats with at least one copy off-site.

Encrypt data: in transit and at rest, for maximum security. It means even if emailed in error, there is no risk of repercussions.

Anti-malware, anti-phishing, firewalls: these should all be implemented as standard, and from reputable vendors, i.e. not free AV with limited functionality.

Mobile device management: these tools will enable you to push policy and centrally manage any corporate and BYOD devices that connect to the network.

Secure authentication: consider two-factor authentication (2FA) to remove the risk of stolen passwords. Or a password manager which will securely store and generate almost impossible-to-crack, secure one-time passwords.

Secure collaboration: some 'sync and share' cloud-based tools can offer staff an easy way to share and collaborate on documents. Choose enterprise-grade versions rather than consumer tools.

Log inspection, file monitoring: tools like these continuously monitor your network to spot activity which could indicate a targeted attack.

Incident response: have a plan in place including key stakeholders from relevant departments (HR, IT, legal etc) so that if the worst happens, you know exactly what to do. Acting quickly can minimise the effect of an attack. Consider pen testing or regular exercises to test your preparedness.

Education and training

As mentioned, staff are your biggest weakness. But with the right training they can become your first line of defence against attackers. Training them in how to spot phishing emails, ransomware attempts and even BEC scams is a must, alongside the right technology tools.

Here are some key elements to consider:

- Start by drawing up an internet usage policy and enforce it with regular audits and education/ training sessions
- Teach your staff to be suspicious by default. Any unsolicited mail with links and attachments should be verified with the supposed sender. Staff should never click on a link in an email – always visit the website in question by typing the URL into the browser.
- Suspicious emails should be inspected for typos
- Hover your cursor over the "From" domain and any links to reveal discrepancies/true origin
- Staff should never divulge any personal/ corporate/financial details over email/phone

Quick Action Plan

1. **Find and classify your data.** What have you got and where is it?
2. **Assess the main threats to your organisation.** Decide on what your risk appetite is
3. **Draw up and enforce a security policy.** This must come from the top down

- Employees should be taught the repercussions of a misplaced click. A data breach/malware infection could lead to service outage; lost IP; legal costs; remediation and clean-up costs; lost customers; damage to brand/share price; and even job losses

- Try to create a culture from the top down where staff don't feel daft for reporting suspected incidents. It's always better to be safe than sorry
- Have a centralised reporting mechanism for any such incidents

Securing the recruitment industry

Don't assume just because you work in an industry like recruitment that you're not a target for cybercriminals. There have been notable high profile examples of incidents in the past. Michael Page was hacked last year in a massive global breach and the details of 700,000 jobseekers stolen.

The firm offered a cautionary tale of how not to handle such an incident, taking 11 days to notify those affected, which caused untold damage to the brand.

Recruitment firms, like many of their counterparts in other industries, are internet-connected, heavily reliant on technology and hold a great deal of sensitive personal information on their clients. That makes them an ideal target, especially those migrating data to the public cloud or using more automation in their systems without fully investigating the potential security implications. Keeping fingers crossed is not an acceptable response. Follow the steps in this guide to help mitigate risk.

Law firms: a goldmine for hackers

There are few companies which hold quite so much sensitive and highly monetisable data as those working in the legal industry. Many may have ticked what they think are the right boxes in terms of security. But firewalls and anti-spam filters do not cut the mustard.

Sophisticated targeted attacks combine social engineering with advanced malware to outwit most traditional defences. To respond you need improved staff awareness of the threats and behaviour-based tools and intrusion defences to stop both known and unknown threats. Why? Because law firms can be a goldmine for hackers looking for sensitive client data. M&A deals in particular can be a magnet both for state-sponsored operatives looking for intelligence which could help geopolitically and financially motivated cybercriminals. At the end of 2016, three Chinese men were charged after making over $4 million from inside information obtained illegally from law firms.

Be aware: you're a major target, so start off on the right foot and reassess your cyber security posture.

Managed services

A great option for SMBs keen to focus on growing the business is to outsource cyber security to an expert third party. It's an increasingly popular choice for smaller firms because they can benefit greatly from the fact that their provider is typically able to invest far more into cyber security processes and controls than they. At Nasstar we focus on building multiple layers of security, including the controls listed above (AV, firewalls, log-ins and monitoring, IDS etc).

We take a best-of-breed approach, investing in products from industry leading security vendors. And we ensure our datacentres are geographically dispersed and use multiple redundant connections, boosting BC/DR efforts. Just as importantly, we ensure staff are continuously trained in the latest cyber security skills.

Above and beyond this we get advanced warning of cyber threats thanks to our membership of the government's Cyber Security Information Sharing Partnership (CISP). And we're certified to ISO 27001 and with Cyber Essentials – a government-backed scheme designed to improve cyber security standards in organisations.

Nasstar also partners with experts Falanx to offer client services including Cyber Essentials training, policy writing, staff training, penetration testing and more. The Cyber Essentials 10 Steps to Cyber Security, encourages organisations to adopt best practices. Achieving certification provides a measured, baseline of security that can help set your organisation apart in the market and demonstrate to your clients your commitment to the safety of their data.

Nasstar offers **three** levels of service;

- **Cyber Essentials – SELF SERVICE:** If you want to acquire Cyber Essentials certification, and are confident that you know the questions you will be asked – and the correct answers – we have an online portal that you can use to self-certify quickly and easily.

- **Cyber Essentials – ASSISTED:** If you want to acquire Cyber Essentials certification but would like a little guidance and support with self-certification, we can assist you, walking you through the process to achieving certification.

- **Cyber Essentials+:** For this more demanding level of certification, we'll take you through a pre-assessment, perform a gap analysis, advise on any necessary remediation and help with your submission, including all evidence for verification and final vulnerability scans.

Nasstar will help you understand whether Cyber Essentials or Cyber Essentials+ is right for you. We'll help you prepare and if appropriate advise on how best to remediate issues that arise during the project and support you through to certification. Along the way, you'll gain the confidence that comes with knowing you are meeting an industry acknowledged standard for cyber security good practice and an important competitive differentiator.

Defence-in-depth is the future

In the end cyber security is not something you can do once and forget about. The advice presented in this guide is a good place to start, but it will only have a lasting impact if you create that all-important cyber-savvy culture in your organisation. That comes from the top down, and it spreads via effective training and regular updates to ensure best practice is always front of mind for staff. That's why as a managed service provider, Nasstar puts a major focus on education and training – of our own staff and those of our clients, in things like Cyber Essentials. Security is present at every layer of our organisation, and it can be in yours too.

 @Nasstar

 blog.nasstar.com

 Nasstar PLC

 info@nasstar.com

 nasstar.com

Headquarters

Datapoint House, 400 Queensway Business Park, Queensway, Telford, Shropshire TF1 7UL

Regional Offices

Victory House, 400 Pavilion Drive, Northampton NN4 7PA

Midland House, 2 Poole Road, Bournemouth, Dorset BH2 5QY

1G/5 Ceres Court, Rosedale, Auckland 0632

Registered number 05623736