sysnet global solutions

Why small businesses need to take cyber security seriously

It’s time to make the changes needed to protect your business

An outline of the risks your business faces that you may not have considered

Copyright © Sysnet Global Solutions

Cyber security and small business

Cyber security is not often high on the agenda of many small business owners in the face of other more pressing aspects of running their company. However, in recent times, both large and small businesses have experienced an unprecedented number of cyber security breaches. It's time for all businesses to sit up and take notice, regardless of size, location and industry; ignoring cyber security risks could have serious consequences.

Cyber security is a wide-ranging term linked to a plethora of issues that even the most technically savvy person can find daunting. However, a small business can take huge strides towards making itself more secure and resilient by understanding the risks involved and taking simple steps to secure their information and systems.

Now is the time

We regularly hear news stories about large corporations being hit with fines and suffering significant costs due to data breaches. Many small businesses believe themselves to be immune to this threat as they believe themselves to be "*too small to be a target*" or that they "*don't hold valuable data.*" Sadly, this is no longer the case. Opportunistic cyber criminals run large-scale, automated searches or launch mass-distributed email-based attacks to find and exploit the 'low hanging fruit'. Minimal time investment is needed to identify a business with weak defences, meaning no discrimination on business-size occurs.

In this paper, we outline why small businesses need to consider that the cyber threat is as real for them as it is for larger businesses.

Read on to learn how to strengthen your defences and protect your business.

Copyright © Sysnet Global Solutions

Data Loss

The act of an unauthorised person accessing your business files or data and removing or copying them without your permission for some kind of personal gain, is something that no one wants to experience. Imagine a criminal physically breaking into your office and stealing your filing cabinet – electronic data loss or theft is essentially the same thing. In the same way that you lock your doors at night and turn on the alarm to physically secure your business, you need to do the same for the data stored on your computers, laptops, tablets and mobile phones.

All data is valuable – in the wrong hands

What many people fail to realise is that nearly all data is valuable when in the wrong hands, as one way or another, most data can be monetised by criminals. Consider the following examples of information that you may have stored on your company's devices:

Customer information

Consider the details stored about your customers, such as phone numbers and email addresses. Cyber criminals can use this information to spam or worse, scam your customers, resulting in numerous negative effects on your business' reputation. There may be significant costs too, if you need to notify affected customers, make reparations or are found to be in breach of your legal obligations towards them.

Financial information

Consider the financial information available on your devices. Accounts, pricing and transaction data can be used for malicious purposes. This information could be valuable in the hands of your competitors, suppliers or even your customers. If your customers knew you were making 200% profit on a particular item, would they look for a discount? If your competitors knew what you were charging for your entire range of services, that would likely affect how they set their prices.

Staff information

As a business, you're responsible for protecting the information you hold on your staff, in the same way you are responsible for that of your customers. You hold personal information about your staff, for example their date of birth, details of their salary, sick leave or absences, or bank account details. How would your staff react if that highly personal information was accidentally or deliberately exposed to colleagues or to the wider world? Their personal information, such as address or employment history, date of birth, bank or tax information could all be leveraged to commit identity theft and fraud. You need to protect that information like it's your own.

Trade secrets

Consider the trade secrets you may store on your devices. If you're a bakery for example, would losing your secret recipes to the internet affect your ability to compete? Recipes, formulas and proprietary product information are all valuable information in the hands of your competitors – a cybercriminal can sell it to the highest bidder.

Loss of those trade secrets may not be a deliberate attack. Business critical information could be deleted by a virus or encrypted and lost to you if you are caught out by ransomware and don't have backups to be able to recover it. Whatever the secret sauce for your business is, you need to protect it and be able to recover if it is lost, stolen or even just accidentally erased.

Remember: Any breach of personal data of EU citizens may result in a fine under the EU's General Data Protection Regulation (GDPR) - 2% or 4% of turnover dependent on whether the breach was deemed as a result of failure to implement appropriate technical or operational measures or negligence in relation to the data subject's rights.

The evolution of the “hacker” – why would they target a small business?

Many people, quite rightly, ask the question: *“Why would a hacker target me?”*

“I’m just a small distributor or retailer, with nothing of value to cybercriminals”

In the past, you might have been right, however in the last few years, the world of the cybercriminal has evolved in four distinct ways:

1. “Hackers” aren’t always organised gangs

The term “hacker” is a broad one and refers to a spectrum of different levels of cybercriminal.

At one end, you have large state-sponsored, organised criminal groups working from office blocks, working to influence elections (allegedly!) and attack large conglomerates and influence share prices.

Somewhere in the middle, you have socially, or politically motivated groups known as “hacktivists”, looking to bring down the websites of organisations whose causes they don’t agree with or getting together to pool their efforts to further their cause.

At other end of the spectrum, you have the lone wolf – the individual sitting in their bedroom with the intention of making some easy money. Although the lone wolf lacks the resources of the other two groups, s/he is as dangerous as the other two if your business’ defences are not up to scratch.

Cybercriminals now come in a variety of shapes and sizes. So too, do their victims.

2. Risk vs reward is changing

Larger companies are now waking up to the threat posed by cybercriminals and malware and are investing heavily in their defensive efforts. This by no means makes them 100% safe from attack, but what it does mean is that cybercriminals need to devote more effort and time to get through these company’s defences.

This is leading to criminals using their skills and tools to widen the net and find companies that are still easy targets, whose data could still be as valuable to them, or whose resources could still be used for their gain.

3. It’s not always a manual process

The extraction of valuable information, does not have to be done manually by an individual. It can easily be performed by malicious software and viruses. For example, a common form of malware known as a rootkit can conceal its presence and gain administrative control of a computer system, slowly extracting data without the knowledge or consent of the owner. Once reported back to the source of the malicious software, this data can then be exploited for malicious purposes.

What this effectively means is, you can be targeted and exploited with little to no time investment by cybercriminals if your defences are inadequate.

4. It's not always a “hacker” doing the hacking

Malicious, effective malware can, these days, be purchased online for personal use. Known as malware-as-a-service, anyone with internet access and the financial resources (including bitcoin) can purchase what is known as an exploit kit.

As the name suggests, an exploit kit is a cocktail of malware or malicious software that the purchaser can use as they see fit. Exploit kits are often access to control dashboards where malware can be created and then distributed in a variety of ways.

Aside from the many applications of this technology, the cause for concern amongst small business is that the spreading and targeting of malware no longer needs to be performed by someone with the necessary skills. The only requirement is motivation.

Read more about rootkits, exploits and other forms of malware in our blog: Simple cyber security threats every small business owner should know about.

Real life case study* – how data loss can affect a small business

To facilitate growth, the management of a garden centre decided to begin selling their products online.

Unfortunately, the new website was open to a number of common web application security vulnerabilities. The website developers had not followed secure coding practices when developing the site.

A few months after going live, attackers exploited weaknesses in the website to obtain the garden centre's customer database (including email addresses).

Once the database was obtained, the attackers sent out emails to the customer list, advertising a 75% off sale. The emails claimed to be from the garden centre, used their branding and even pictures of real stock items advertised on their real website. Customers clicking on the link were then directed to the cybercriminal's website that looked just like centre's own site. When the customer placed an order, their card details were captured. The criminals then used these card details to fraudulently purchase expensive goods.

The company was inundated with complaints from angry customers and suffered immense reputational damage, including a social media backlash. They very nearly went out of business and took the decision never to trade online again.

*Identity of the real business has been removed for the purpose of this example

Disruption of daily operations

Although malicious, sophisticated strains of malware extract and compromise your data with the intention of making profit, often, malware and viruses simply disrupt and slow down your daily operations by interfering with the performance of your devices. Also, if your business is running with infected machines they may 'pass on' the malware and end up infecting your customers and business partners.

If not dealt with properly, this can have negative impacts on your ability to do business, especially if the problem persists over an elongated period of time.

Device and internet performance issues

Frequent crashes

Many strains of viruses and malware can sit undetected on your devices and use memory in order to run. This can slow the performance of your devices, often making them unworkable and causing them to crash as you open and run extra programs.

Often, a virus will cause intermittent crashes forcing a user to have to restart their device regularly, meaning they lose their unsaved work. Viruses can be programmed to crash machines randomly, making it difficult for a user to spot patterns and realise they are infected.

Adware

Adware (short for advertising-supported software) is a form of malware. Its purpose is to display advertisements. It commonly displays advertisements via pop ups on websites or in free versions of software. Adware often displays itself in ways that are intrusive to the user, causing a negative browsing experience and slowing the ability of the user to search and locate information online.

Internet performance

Overall Internet connection performance could also be impacted by malware infection. Malware is often programmed to communicate back with a server once a successful infection has occurred in order to exfiltrate data etc. If one device is infected, it may communicate with its servers, be searching for other devices to infect or be part of a cybercriminal's botnet (see below) etc. All of these activities can use up your company's bandwidth, having negative implications for your internet performance, further slowing down your operations.

These examples, although arguably not quite as harmful as a data breach can have serious effects on the productivity and personal performance of your staff. Especially if you consider that these examples can apply daily, to a number of employees, over a number of months, multiplying their effects, negatively impacting productivity over a longer period of time.

A **botnet** is a group of internet-connected devices that are being remotely controlled by a hacker. The intention of a botnet is to send spam, steal data or take part in a distributed denial of service (DDoS) attack. Read more

Copyright © Sysnet Global Solutions

Real life case study* – how viruses can affect machine performance and in turn, affect small business

After visiting a shopping site advertising discount clothing from China, Emma, a freelance graphic designer noticed her laptop began to freeze and had to be reset. She found this began happening about twice a week at first and then once or twice a day after a month or so. All work since the last save would be lost, not to mention her creative flow.

Two months later, Emma was working to a tight deadline for a client when her machine froze, and she lost all her work. As a result, she had to work late and all that weekend to catch up. The job was delivered two days late, leaving her embarrassed in front of her best client. Emma estimated she had lost an hour to two hours work per day over a three-month period - a huge amount of lost productivity time.

Eventually, Emma had to take the laptop to get fixed, resulting in a hefty bill and didn't receive work from that client again for a number of months, meaning an unmeasurable amount of lost business.

*Identity of the real business has been removed and that of the individual changed, for the purpose of this example

System crashes and downtime

While an individual malfunctioning laptop can be an issue for some, of potentially more concern to most small businesses is the prospect of business application system crashes, the inability to access critical files or website downtime.

Many risks exist to small businesses in terms of downtime. Under-protected applications on which the business relies for its revenue pose a potential business-ending risk.

Application attacks

Many of the applications businesses use in their day-to-day operations are, these days, hosted and accessed online. Examples include webmail, instant messaging, customer relationship management (CRM) or accounting platforms etc. As these business and web applications are accessed via and communicate across the Internet, they are vulnerable to cyber-attack. If they have not been coded in a secure manner, weaknesses may be present that could be exploited by common application attacks, such as SQL injection and cross-site scripting, or communications to/from these online systems could be the target of Man-in-the-Middle attacks[1]. Internet-facing web-based applications may also be subjected to Distributed Denial of Service (DDoS) attacks (see Website downtime below) making them unavailable to you while they are under attack.

If your business relies on a bespoke web-based application that has been developed for you or if you host an instance of a commercial off-the-shelf web-based application, to perform your daily operations, you need to consider the cyber security implications and the steps you can take to protect these applications.

You need to ensure that:

a) bespoke applications are securely coded to address known web application security risks,

b) all web-based applications, and the systems that support them, are securely configured and regularly

[1] An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other

updated with security updates designed to address known vulnerabilities, and
c) you have adequate protection against common forms of attacks in place. Your business can suffer irreparable damage if your vital applications are compromised or prevented from operating for a period of time (see our advice section below).

Although you may not have control over some of the applications you use (e.g. those offered as Software as a Service or fully hosted/managed by the provider), it's important to take all of the steps that you can to protect the Internet-facing business and web applications you rely on. For example, seek assurances from software developers of the secure coding practices they follow before engaging them for any custom development; make sure that third parties hosting and managing your applications have processes identifying and addressing new security vulnerabilities. The actions taken by you and your third-party providers can help you lessen the risk of a security breach, data compromise and downtime.

Ransomware and file encryption

Ransomware is a form of malware that infects a victim's system by encrypting or blocking access to all folders and files on the user's network. The victim must then pay money (i.e. a ransom) to the owner of the Ransomware for them to restore access to the blocked files.

This can be particularly troublesome for many businesses who rely on their computers and the files stored on them to operate. It is a favourite with organised cybercriminals as it gives them easy access to revenue to fund their extensive efforts. It can also be distributed via exploit kits (see above).

Website downtime

If you rely on your website to accept orders or even as a simple lead generation tool, ensuring your website is protected from attack and compromise can mean the difference between profit and loss for the quarter. Although you may outsource the hosting and management of your website and therefore also its protection, it is still your responsibility to ensure your web providers secure and protect your website from common forms of attack.

A common form of website attack is a Distributed Denial of Service (DDoS) attack. A DDoS attack is an attack on a website, whereby cybercriminals overload the site with fake web traffic with the intention of it crashing it due to an overload. This can be mitigated against with the implementation of a Web Application Firewall.

Real life case study* – how website downtime can affect a small business

One Saturday, James the staff supervisor at an online clothing retailer noticed no orders were coming in as usual. Upon investigation he found that the web server had crashed, and his browser was showing an error that the website could not be found. Not knowing what to do, and unable to contact Hannah, the manager, James went home for the weekend. When he returned on Monday, the website was still down.

Hannah had to engage an external consultant to investigate and resolve the issues at huge cost to the company. The consultant advised the website had been victim to what was known as a DDoS attack. On Tuesday, the problem was resolved, and the website was operational again. The company had lost 3.5 days' worth of business time.

Being a high-volume retailer, solely relying on its website for revenue, the 3.5 days of lost business was a lot more expensive than the cost of the consultant who repaired their website and a lot more expensive than the monthly cost of a Web Application Firewall (WAF).

*Identity of the real business and that of the individuals has been removed for the purpose of this example

Solutions to prevent, defend and respond to common cyber security threats

If you haven't already done so, consider some of the following defensive elements and apply them in your business. It's important as a business, not to rely on one security element. With so many different attack methods available for cyber criminals to exploit, no single cyber security protection method or defensive tool can be effective against them all. It's important to employ multiple forms of protection and continuously add protective layers to achieve defence-in-depth. Read more about this approach in our blog: How PCI DSS builds layers of protection.

Anti-virus

Anti-virus (AV) software is essential for any business and is an imperative first step in your defences. It's very important for small business to employ high AV protection and to scan your machines regularly. The use of free anti-virus packages is not recommended. For an AV package to be truly effective it must be regularly and constantly updated with information on the latest threats. Free packages are often not updated as regularly as the paid versions, making them less effective. This means you may be vulnerable to newer strains of malware for longer.

Host-based firewall

A host-based firewall is a form of protective barrier around your devices. At its simplest, the firewall examines incoming and outgoing network traffic, determining whether it should be allowed to pass or be blocked. A host-based firewall can allow safe applications and functions to communicate while alerting you to, or even blocking, any suspicious activity. Good host-based firewalls contain a Host Intrusion Prevention System (HIPS), meaning it can detect and prevent any unauthorised changes by malicious software on your device. This is a much-needed preventive element of any defence-in-depth approach.

Endpoint protection

Many businesses protect the main desktop computers used in their business but then neglect their other devices – mobiles, tablets etc. (i.e. Endpoints). As a business you need to consider Advanced Endpoint Protection to defend all types of business-critical devices from threats they may be exposed to when they surf the Internet, receive emails or interact with social media. Any device that does all of those things and connects to your business' network and internal systems is a potential weak point that could allow attackers in, introduce viruses or other malicious software or be a route out (data leakage/loss).

Web Application Firewall (WAF)

A WAF acts as a firewall for your website, defending it against common forms of online attack. As seen in our real-life example above, a WAF can be effective in defending against DDoS attacks. A WAF can also protect against other common attacks and known web application vulnerabilities (weaknesses) such as SQL Injections, Buffer Overflow and Cross Site Scripting (XSS) which can be used to gain access to sensitive data or gain privileged access to the website. Read more about these threats here.

Copyright © Sysnet Global Solutions

Awareness and education

Ensuring you and your staff are aware of the common risks and threats is a major step towards protecting your business. You need to ensure you have an Information Security Policy defined for your business, that is supported by processes and procedures for the handling and protection of sensitive data.

Establish other policies around the use of personal mobile phones, on the use of email so that users know how to recognise phishing emails and scams, and on the use of work computers for personal Internet browsing to limit risks. Your staff are often your first line of defence against scams, phishing, ransomware and malicious websites. Raising their cyber security awareness is one of the most effective ways to prevent data loss and cyber-attacks against your business.

Incident response

An incident response plan (IRP) should be in-place to help your business react quickly in the event of an attack to minimise the potentially damaging impact. An IRP provides detailed instructions on how to react to a range of incident scenarios such as data breaches, ransomware, denial of service attacks, virus outbreaks, etc. Your IRP should consider those incidents that could impact your valuable data and hinder your ability to operate your business. Planning ahead will help your company respond and recover as quickly and as safely as possible. The impact of the real-life website downtime example above could have been reduced if the business had a plan for reporting and dealing with security incidents.

There are many ways in which you can protect your business from cyber-attack, these are just some measures.

Ensure you have an understanding of all the common terms with The small business A – Z of Cyber security, a glossary of terms with definitions of common phrases relating to cyber security and the PCI DSS. Download it and keep it on your desktop to refer to when needed.

Copyright © Sysnet Global Solutions