Cyber security 101

Your guide to getting the basics right

FIELD EFFECT / Partners

Cyber attacks happen.

It may be easy to ignore cyber security and take the, “it will never happen to me or my business” stance. We get it - cyber security is an overwhelming topic. That’s why Field Effect exists.

We believe all businesses deserve powerful, cost-effective, and easy-to-use cyber security to protect their operations from cyber threats. No matter your security knowledge, resources, or budget, cyber security should be approachable and attainable for you.

But where do you start?

We created this eBook as a primer to help you understand the cyber threats that are targeting your business and how to proactively defend against them. More than anything, we want to stop cyber criminals from hurting businesses and people like you. We’ve got your back. If you have any questions, or if there’s anything further we can do to help, please reach out.

Table of Contents

INTRODUCTION

Why your small business **is a target**

When you think of the term "cyber attack," what comes to mind?

Chances are you've seen a movie or TV show that's given cyber attacks the Hollywood treatment: a scrappy group of hackers looking to take down a major corporation use smartphones to hack into everything from security cameras to fire sprinklers, throwing in all sorts of jargon as they steal data and upload it to the cloud.
Real-life hacking is far more mundane. For one, cyber criminals rely on human error as much as they do software tools. For another, big business isn't the only target, with criminals targeting small and mid-size businesses (SMBs) more and more often.

While SMEs account for nearly 30% of all data breaches,[1] cyber security remains a low priority for many of these businesses; a shocking 82% of SMBs underestimate the serious cyber risks they face.[2] On a daily basis, SMBs manage, share, and store valuable, confidential data. This includes everything from customer names, addresses, and financial information to confidential employee and company data, all of which are attractive targets for cyber criminals.

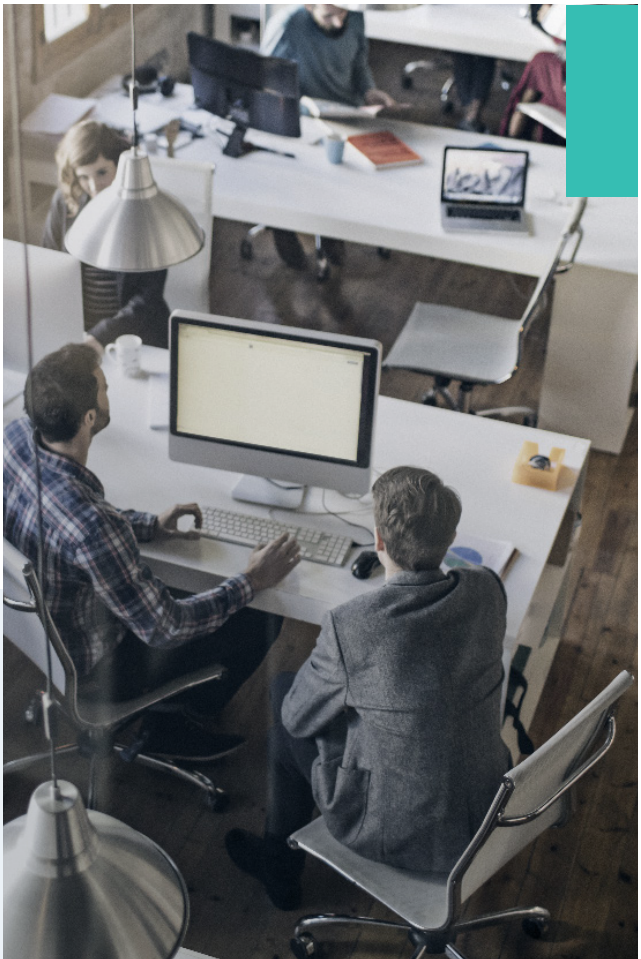
[1] https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

[2] https://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html

The internet and cloud-based services have allowed businesses of all sizes to scale their operations and gain efficiencies. But while this transformation has enabled smaller companies to grow their business (and in some cases, compete with large enterprise directly), it has also made it clear that cyber security must keep pace.

Unfortunately, most cyber security solutions are tailored to large enterprises, making it difficult for SMBs to easily put proactive security strategies in place.

While a real-life cyber attack might not be as flashy as in the movies, it's just as damaging, and could negatively impact the safety and security of your staff, customers, partners, and operations.



Protecting your **threat surface**

"Knowing is half the battle" is more than just a catchphrase from a Saturday morning cartoon – it's a great starting point for improving your cyber security. But before you can secure your IT network, you need to assess and understand the full scope of your threats.

> *Understanding and managing your threat surface are foundational steps in your organization's journey towards better cyber security.*

Threat surfaces are always changing and evolving as hardware or software is introduced or removed, or as employees connect to the network with new devices or from new locations, and more. Understanding all the elements of your threat surface is vital for building ongoing, proactive cyber security defences.

Definition: Threat Surface

All the parts of your IT network where cyber criminals could identify security gaps, holes, or other potential vulnerabilities, and gain access.

Familiarizing yourself with two key concepts can help:

NETWORK KNOWLEDGE

You have to know what you're securing in order to keep it safe. Mapping out your IT infrastructure is a great first step. Make a note of the tools and technology that drive data access and exchange between systems and users. Your network may include everything from on-premise servers and multiple workstations to cloud-based services and remote-access assets, in addition to internet-enabled devices. A solid understanding of every aspect of your IT operations will help you assess potential cyber risks facing the systems and technologies you rely on each day.

THREAT AWARENESS

Just like your network, threats are always evolving and changing, too. Unfortunately, this happens at a much faster pace; attackers are always looking for new ways to gain access to your network such as exploiting vulnerabilities, infecting systems with malware, and deceiving users into clicking malicious links or downloading compromised files.

The cyber threats facing **your business**

A quick glance at news headlines will reveal just how commonplace cyber attacks on SMBs have become. These attacks have impacted one in five businesses[3] since 2018 alone; coupled with the shift towards remote-first work policies and ever-evolving networks, the cyber threats facing small businesses continue to grow.

Understanding the major cyber threats facing your company can help you secure your operations.

RANSOMWARE

Ransomware is a common type of malicious software (or malware) designed to damage IT assets or steal data by encrypting the files on a device or network or otherwise prevent access to data or systems. Once this encryption takes place, an attacker will contact the victim with a ransom demand, promising to restore access once payment has been received. These attacks come from a variety of sources, most commonly phishing or other social engineering techniques where attackers attempt to lure users into clicking on a link or downloading a file that allows attackers to take control of the system.

While the overall volume of ransomware attacks is on the decline,[4] the attacks have become far more targeted and carry greater risks for businesses. Beyond the initial financial demands and potential costs incurred from operational downtime or repairing and replacing damaged systems, attackers may also threaten to expose the data on an infected system. Under the Personal Information Protection and Electronic Documents Act (PIPEDA) and General Data Protection Regulation (GDPR), data breaches that expose personal information (for example, of customers or employees) could also result in severe regulatory fines. A data breach also poses a serious risk to your company's reputation, impacting customer trust and potentially impacting your ability to retain existing customers and earn new business.

Definition: Cyber Attack

An attempt by cyber criminals to expose, alter, disable, damage, steal or otherwise gain unauthorized access to a computer system or network.

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC), sometimes known as CEO fraud, is a major cyber threat facing small businesses, and has cost North American businesses upwards of $3.13 billion[5] over a four-year period. BEC is a social engineering scam that typically targets a company's financial or procurement department. Attackers will impersonate the business' CEO or another executive by spoofing an email account or will use phishing attacks to seize the credentials they need.

Once they have these credentials, the attacker may email an employee, requesting they initiate a financial transfer to the attacker's account. These attacks may also use falsified invoices or requests from third-party vendors or clients. Defrauded vendors or clients may also pose a risk should they pursue legal action against a business that has been hit by a BEC attack.

[3] http://www.ibc.ca/on/resources/media-centre/media-releases/small-businesses-in-canada-vulnerable-to-cyber-attacks

[4] https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

[5] https://www.bennettjones.com/Blogs-Section/Business-Email-Compromise-Protect-Your-Company-From-This-Common-Scam

Cyber threats by the numbers:

28% of data breaches involve small businesses[6]

44% of small businesses have no cyber defences in place[7]

57% of cyber attacks on SMBs involve phishing[8]

PHISHING

Phishing attacks are the cause behind nearly a quarter of all data breaches[9] and continue to target businesses of all sizes. These attacks rely on social engineering techniques, much like BEC, to lure users into clicking a malicious link or downloading a malicious file. These attacks are incredibly common because of their relative ease and success rate. Even the most inexperienced attacker can acquire and use a phishing kit (a set of software tools used by cyber criminals) without much difficulty. Phishing attacks have also become more sophisticated, with harder-to-spot tools and techniques. Even with ongoing training for staff, your company may have difficulty identifying an attack.

Definition: Data Breach:
An incident where an organization's data is lost or stolen, most often resulting from a cyber attack.

THIRD PARTIES & INTERNAL THREATS

The growing use of third-party software and services in the day-to-day operations of a business poses another potential avenue of attack for cyber criminals. Even if you're taking steps to improve the security of your operations, new risks to your business are introduced if a software or service provider you rely on is compromised.

Your organization should take steps to ensure the partners and suppliers you work with are following cyber security best practices. This could include establishing a vendor management policy that sets expectations for the security measures these organizations have in place.

Additional threats may originate from within your organization. Either due to everyday human error, such as misplacing a USB drive or using weak passwords, or an intentional cyber security compromise from a disgruntled employee, these threats can also drastically impact the security of your operations.

[6] https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

[7] http://www.ibc.ca/on/resources/media-centre/media-releases/small-businesses-in-canada-vulnerable-to-cyber-attacks

[8] https://www.cpomagazine.com/cyber-security/cyber-attacks-on-smbs-are-once-again-on-the-rise-according-to-new-ponemon-report/

[9] https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

Getting the **basics right**

Cyber threats represent one of the greatest risks to your business. A single attack can have wide-ranging effects, impacting not only the day-to-day operations, financial health, and reputation of your company, but the safety of your staff and customers as well. The good news is you don't need to be an expert to take steps to secure your business.

Understanding a few cyber security basics will provide you with a foundation you can build on to protect your data and operations for the long term.

KNOW YOUR NETWORK

As discussed, you need to know your IT network inside and out. This working knowledge of your network can help you better understand where potential risks or entry points may exist, giving you an opportunity to close security gaps and improve your cyber security.

INVEST IN CYBER TRAINING

Do you know how to spot a phishing email? Nearly a quarter of all data breaches can be traced back to human error.[10] As remote-first work becomes increasingly common, it's likely that number will continue to rise. Educating and training your staff on cyber security basics and best practices can help reduce the chances of a successful attack.

Potential training topics include:

- What makes a strong password?
- How to spot a social engineering attack (such as a phishing email or BEC).
- What to do if you think you've been attacked.

UPDATE SOFTWARE & MANAGE PASSWORDS

How often do you click the "remind me later" button when your computer prompts you about a software update? It's a bad habit that too many users fall into, and it could have dire consequences for your business; one study found that 60% of reported breaches were linked to vulnerabilities where software patches were available but not applied.[11] Most software patches are provided specifically because a developer identified a risk, so it's worth taking the time to apply these patches.

[10] https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html

[11] https://securityboulevard.com/2019/10/60-of-breaches-in-2019-involved-unpatched-vulnerabilities/

Passwords are another easy fix. Shockingly, over half of all computer users reuse the same password across all their accounts;[12] all it takes is one cracked password for an attacker to gain access to a wide number of accounts and systems. For peace of mind, consider using a password management application to automate the creation and use of strong, hard-to-crack passwords.

USE SECURITY SERVICES

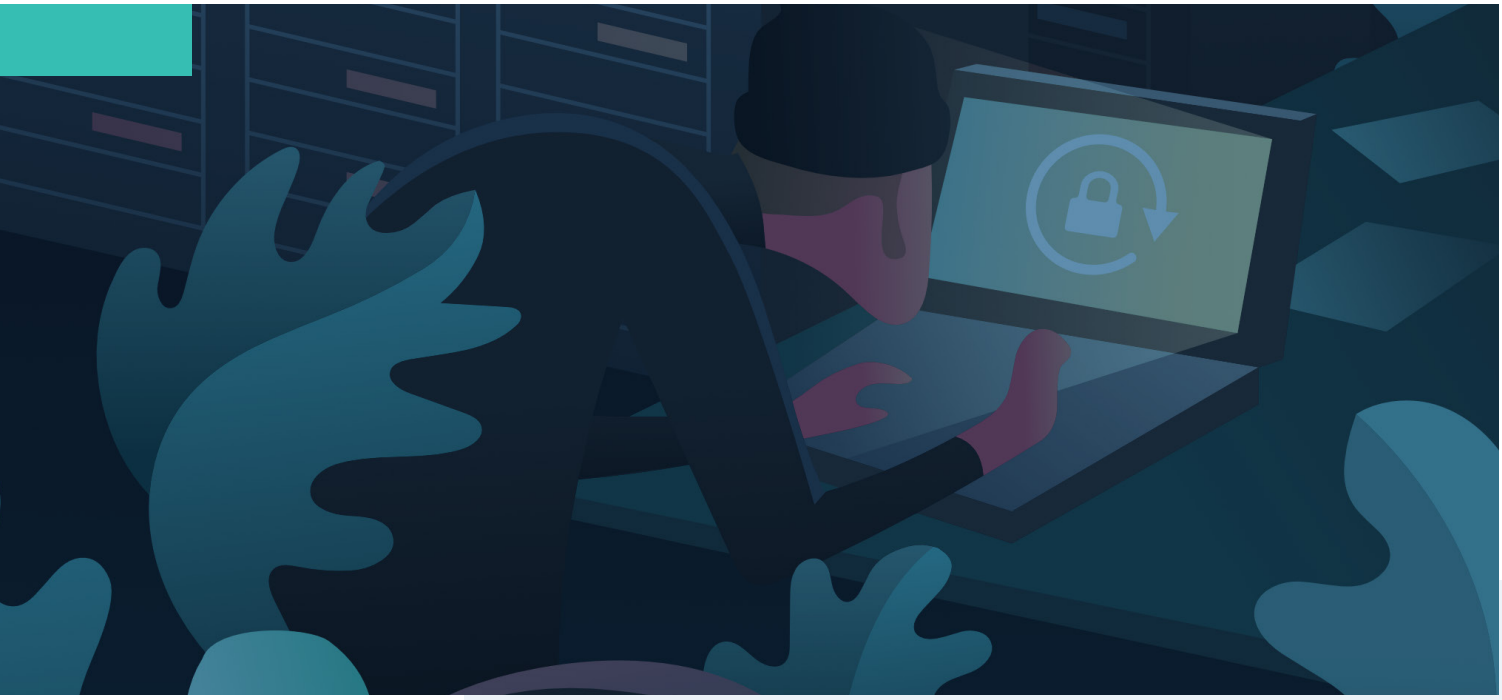
What steps are you currently taking to secure your IT network? Making use of antivirus software and a strong firewall can provide additional protection from these round-the-clock attacks and challenges facing your business, though additional defences are likely required. As an extra level of security, backup your data. While a backup cannot prevent an attack, it can ensure you have access to any data you have backed up so you can continue normal operations in the event of a cyber attack.

MONITORING & DETECTION

Without a view into your systems, staying informed and ahead of the threats facing your network will be challenging. After all, as we've touched on before, attackers aren't limited to the usual nine-to-five schedule when they target your systems. Attacks can happen at any time, so the ability to monitor all networks continually is key to protecting your business.

Cyber threat monitoring provides your company with the ability to detect suspicious or potentially malicious activity that could signal a future attack early on a 24-7 basis. Tools that detect and monitor all the activity happening in your IT environment can alert you to potential threats and risks before they become serious issues.

[12] https://services.google.com/fh/files/blogs/google_security_infographic.pdf



Threat monitoring & detection **done right**

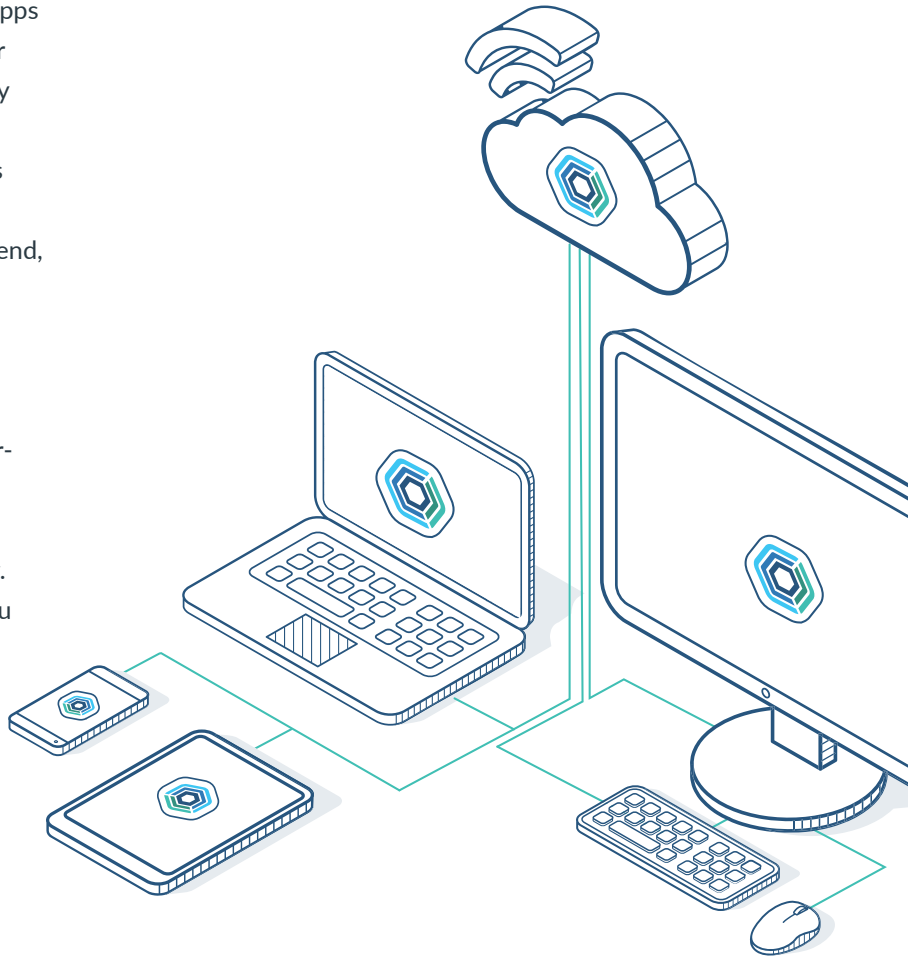
Cloud services and distributed, or remote, workforces have allowed even the smallest organizations to scale their operations and increase productivity, but security must keep pace with this growth. Small businesses frequently face challenges when approaching their cyber security needs, simply because the majority of solutions are geared towards much larger enterprises with greater resources. Small businesses often struggle to find tools for threat monitoring and detection that deliver continuous visibility into an IT network.

When looking for a monitoring solution, though, there are a few things that you should keep in mind:

It should cover your entire IT network. Ensure your cyber security solution provides monitoring and detection across all your systems, software, and devices. For example, if your business relies on Microsoft 365 or Google Workplace, or if your staff uses cloud-based apps to get their work done, continuous monitoring of your cloud services and infrastructure is a must. A company with a strong bring-your-own-device (BYOD) culture would require strong endpoint monitoring capabilities for smartphones and other devices connecting to the network. Look for solutions that provide that end-to-end, comprehensive monitoring.

It should be powerful, but easy to use. Setting up proactive threat monitoring and detection shouldn't be a process that takes weeks of fine-tuning and after-sales support; it should just work. Look for powerful, automated analytical capabilities in a user-friendly package that flags potentially suspicious activity early. This advanced notice of tomorrow's threats allows you to proactively address them before they become serious issues.

It should provide understandable, actionable information. Your monitoring and detection solution must be able to provide relevant insights into the threats facing your network. Not every business has an IT team, so a solution that cuts through the jargon and limits redundant threats with easy-to-understand notifications and actionable recommendations is vital for securing your IT network and infrastructure.



We hope this eBook has helped guide you on where to start when it comes to securing your business.

If you take only one thing away from what you've read, we hope it's that businesses like yours are facing very real cyber threats.

While it's very important to have cyber insurance and backups, you can't rely on these things to prevent an attack, resolve business interruption or keep your customer data safe. Taking a proactive approach to defending and securing your company against these risks can help prevent cyber attacks entirely and save your business.

Remember, you're not alone. It's our mission to protect companies like yours. If you have any questions, or need any help with your cyber security, please get in touch with our Field Effect team.

We've got your back.

About **Partner**

Boilerplate Copy : Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque varius iaculis enim in auctor. Pellentesque cursus volutpat augue non vehicula. Morbi interdum risus et metus vulputate sagittis. Phasellus suscipit enim vitae libero bibendum volutpat. Curabitur dignissim nulla purus, eget semper turpis volutpat nec. Suspendisse blandit, elit ut molestie convallis, mauris est aliquam odio, a blandit convallis faucibus lectus, rutrum ornare ante auctor smaximus sapien dignissim.

Partner Logo

Partner URL

About **Field Effect**

Field Effect believes that businesses of all sizes deserve powerful cyber security solutions to protect them. The company's threat detection, monitoring, and response solution, along with their training and compliance products and services are the result of years of research and development by the brightest talents in the cyber security industry. Field Effect's solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

fieldeffect.com

CONTACT US
+1 (800) 299-8986 (Canada and US)
+44(800) 0869176 (United Kingdom)
+61 (1800) 431418 (Australia)