Heimdal®

2023

CYBERSECURITY ADVICE FOR SMBS.

Understanding the Importance of Cybersecurity as an SMB Owner or Employee.

Author

Bianca Soare

WWW.HEIMDALSECURITY.COM

Author
Bianca Soare

TABLE OF CONTENTS

1.

INTRODUCTION

1. Introduction

Cybersecurity can feel overwhelming for SMBs, for they have to manage issues related to data security and integrity, avoid breaches, and understand and implement the protection measures required to efficiently deal with cyber threats. Sometimes, this responsibility falls on SMB owners, who often must fill several roles at once.

This whitepaper provides guidance on the latest cyber security dangers, defense strategies, and best practices, with a particular focus on prevention rather than remediation, that should be followed by SMB leaders and their employees from all over the world.

2.

DEFINING SMBS

2. Defining SMBs

2.1. SMB market overview

Small and Medium Businesses (SMBs), commonly referred to as Small and Medium Enterprises (SMEs), are often considered the backbone of economies, being a source of economic development and employment around the globe. The World Banks estimates they represent approximately 90% of businesses and over 50% of employment worldwide.[1] What's more, according to the same source, formal SMBs secure around 40% of GDP in emerging economies and create 7 out of 10 jobs.

A report released by Salesforce Research describes small and medium-sized business leaders as "hard-working, passionate entrepreneurs who face unique challenges, which change and evolve as their businesses grow."[2] Additionally, the SMB owners who participated in the study plan their investments in accordance with their customers' expectations, focusing on ensuring personalized experiences. Furthermore, developing SMBs have a greater likelihood of investing in CRM, marketing automation, and AI, which indicates the fact that digitalization is an important aspect for emerging companies, as well as a significant growth component.

2.2. SMBs in the context of the COVID-19 pandemic

The COVID-19 international crisis has impacted people's lives and the global economy. At the same time, the pandemic has also brought about a global economic downturn, impacting commerce, spending, productivity, and businesses. According to the World Trade Organization, the world merchandise trade will plummet somewhere in the range of 13% and 32%.[3] In addition, the International Trade Center (ITC) estimates that 1 in 5 small businesses are likely to go bankrupt within three months due to the current COVID-19 context.[4] Besides, the pandemic has strongly impacted 55% of SMBs, with almost two-thirds of micro and small firms having been affected, in contrast to almost 40% of large companies.[5]

Some of the participants in the ITC COVID-19 study have adopted various survival strategies, such as laying off employees, selling assets or taking on new debt. The majority of respondents attempted to maintain a state of resilience, extending their online sales channels, closing partnerships with new suppliers or opting for remote work. Simultaneously, the most agile SMBs fully adapted to the current situation, shifting their focus towards creating and providing essential supplies (such as masks, disinfectants, etc.).

[1] The World Bank, 2020.
[2] Salesforce Research, 2019.
[3] World Trade Organization, April 2020.
[4] International Trade Center, June 2020.
[5] Ibid.

How can small and medium-sized businesses continue their operations despite adversity? The ITC proposes four crucial aspects that SMBs should embrace during times of crises to ensure their stability and economic growth: resilience, digitalization, inclusiveness, and sustainable growth.

3.

CYBERSECURITY CHALLENGES FACED BY SMBS

3. Cybersecurity Challenges faced by SMBs

Generally, SMB owners are wearing many hats and are facing different types of challenges along their journey. Small and medium-sized business leaders are experiencing common impediments such as having limited access to capital (and thus, difficulty in maintaining financial growth), employee retention, creating and establishing internal processes, and scaling technology.[6]

43% of breaches in 2019 involved small businesses[7] and presently, cyber threats are still on the rise. Thus, cybersecurity must not be neglected, but treated as a priority by SMBs.[8]

3.1. What is cybersecurity and why does it matter for SMBs?

A Ponemon survey showed that almost 70% of all small companies witnessed a cyber-attack, while half having acknowledged that they have little knowledge on how to defend their company.[9] This raises the question: Do SMB owners understand what cybersecurity is – and more precisely, do they grasp its implications?

If we start by looking at the fundamentals, here is how NIST, an authority in cybersecurity defines it: "The ability to protect or defend the use of cyberspace from cyber-attacks." A more complex definition of cybersecurity provided by NIST is: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[10]

Simply put, cybersecurity refers to all technologies and procedures that aim to safeguard networks, devices, programs, and data from attacks and unauthorized access.

3.1.1. The importance of cybersecurity

Cybersecurity is a highly important aspect within any organization for several reasons. First of all, a company's data (regardless of the size of the organization) is of high importance since it may contain sensitive details, be it financial data, intellectual property, or the customers' and employees' personal information. Should all or segments of this data arrive in the wrong hands, its leakage could have devastating financial and reputational consequences.

[6] Salesforce Research, 2019.
[7] Ponemon Institute, 2018.
[8] NIST SP 800-37 Rev. 2
[9] Salesforce Research, 2019.
[10] Salesforce Research, 2018.

In terms of their relationship with their customers, first and foremost, 90% of SMB owners value trust.[11] Simultaneously, 63% of consumers believe their personal information is vulnerable to a security breach.[12] It is no wonder that this is the case, especially since security failures and data breaches are widespread and data protection regulations are now being enforced at large-scale. Therefore, gaining customers' trust becomes not only a necessity, but perhaps a strategic differentiating factor in today's competitive market. As a matter of fact, 87% of customers declared cybersecurity will transform their expectations of companies,[13] which validates the necessity for digital security.

Organizations large and small work with high volumes of data shared across their networks and devices. If these are not properly (or at all) secured, this means the company must undertake protective measures.

The rate of cyber-attacks and malware propagation is not showing any signs of slowdown – not even during the current COVID-19 pandemic. In fact, cybercriminals and scammers are still leveraging the ongoing crisis by widely spreading fake emails while posing as legitimate health organizations or government officials.[14] Usually, these messages contain infected attachments or malicious links, which infect the users' devices with malware or are aimed towards harvesting their credentials. The World Health Organization (WHO), for example, explicitly warned that cybercriminals are sending phishing emails related to COVID-19, and are impersonating WHO officials to steal confidential data and money.[15]

What's more, Heimdal™ Security's experts have noticed an increase of traffic to malicious websites during these times as employees started working remotely.[16] As always, panic-inducing events prove to be lucrative for online scammers, and unfortunately, the latest COVID-19 outbreak is no exception to the rule. Nowadays, cybercriminals are focusing on tricking people into giving away their credentials or transferring money to cybercriminals' accounts while using coronavirus-related materials as bait.[17]

3.2. Cyber security threats faced by SMBs

A popular belief is that smaller companies are too insignificant to be a priority for cyber attackers. However, this is not the case. Unfortunately, SMBs are appealing targets for cybercriminals not due to their financial attractiveness, but simply because of being well-known for their lack of experience and weak defense. This makes them easier and more attractive targets than larger organizations. In essence, they are operating in the same environment as developed businesses, but with fewer tools and financial resources. Therefore, SMBs are

11 Ibid.
12 "US Users Targeted with Corona Virus Phishing Attacks", 2020.
13 WHO (World Health Organization).
14 "Traffic to Malicious Websites Spiking as more Employees Take Up Work from Home", 2020.
15 CISA, 2020.
16 Switchfast Technologies, 2018.
17 PwC, 2018.

oftentimes vulnerable to malware and crippling cyber-attacks that can capture their customers' or their own sensitive information. Without proper training, their employees can easily become victims of social engineering campaigns. What's more, the extensive spread of the Internet of Things introduces even more security challenges that small business owners might not have even considered. The fact of the matter is there is a myriad of opportunities for cybercriminals to profit from - and SMBs lack the knowledge and preparation to stay safe.

3.2.1 SMBs' attitude towards cybersecurity

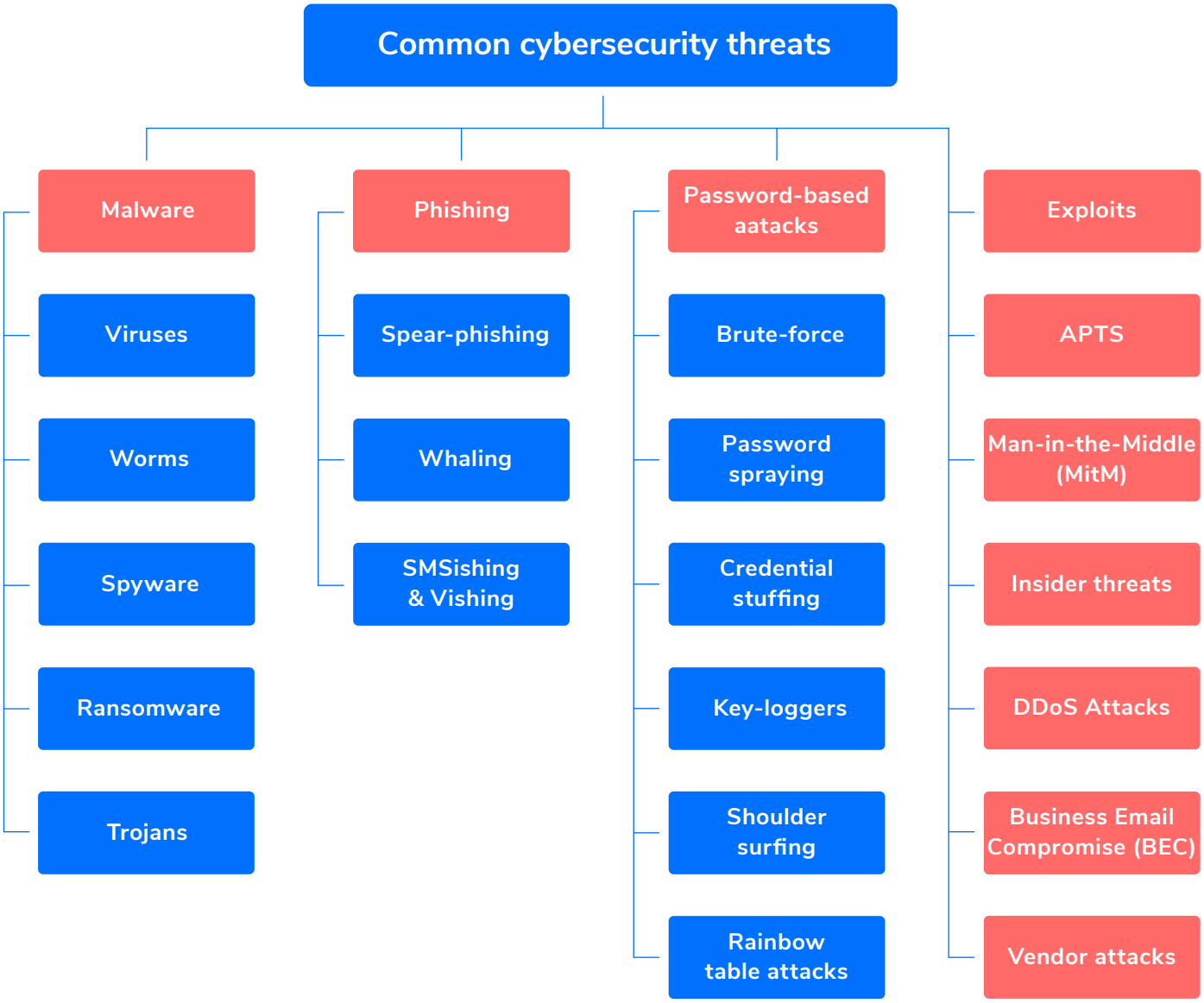
SMBs do not always have enough internal expertise to deal with cyberattacks and many times, due to budget constraints, their owners have to deal with cybersecurity issues themselves. Studies have shown that 51% of SMB leaders believe that their company cannot be targeted by cybercriminals.[18] What's more, according to the same report, one in three SMBs do not have any protections in place to combat a data breach. At the same time, another study has revealed that SMBs reduced their security budgets, even though the rate of cyber-attacks and subsequent losses have dramatically increased.[19]

As alarming as it may sound, many SMBs are not taking cybersecurity seriously. Yet another study proved that most SMBs struggle to properly tackle the dangers posed by cyber-attacks, with 60% of respondents placing cybersecurity in the bottom-half of their concerns.[20]

3.2.2 Examples of cybersecurity threats faced by SMBs

For the aforementioned reasons, SMB owners must be informed about basic types of e-threats, at minimum, and be capable of understanding how malicious hackers can gain entrance to a company's data and IT systems. Below are the most frequently encountered cyber risks that SMBs are likely to deal with, which their leaders and employees show be aware of.

[18] Ponemon Institute, 2018.
[19] PwC, 2018.
[20] Ponemon Institute, 2018.



1. Malware

Malware, the short term for “malicious software”, refers to all programs that have the capability of infecting endpoints (be them desktops or mobile devices - including Internet of Things devices). It's a term used for malicious code written to obtain entry to networks and capture or lock up data on machines. Malware typically emerges from downloading content from malicious webpages, spam emails or due to the communication with other compromised computers or apps. In short, malware is developed with the purpose of gaining unauthorized access to systems and wreaking havoc inside an organization’s IT environment. Such assaults are particularly dangerous for small companies as they can destroy equipment that would need to replaced or repaired, or jeopardize consumers’ and employees’ data. One of the most common types of malware are viruses, trojans, worms, spyware, and ransomware, to name a few. We will explain each of these terms further on.

The AV-TEST Institute registers over 350,000 new malware strains and potentially unwanted applications (PUA) daily.[21]

Viruses

Sometimes, the terms “viruses” and “malware” and used interchangeably - however, this is incorrect. A computer virus is a type of malware that injects itself into the code of legitimate software. As soon as the infected application is executed the virus code also runs along, producing damage on the machine. Viruses have the ability of reproducing; however, they require some form of user intervention.

Worms

Worms are types of malware that replicate themselves and propagate to other devices. They generally use a network to spread and take advantage of security mishaps on the host they are trying to access. Even if worms do not have the ability to alter the systems they infiltrate, they do produce at least some amount of damage such as increasing traffic on a network. Opposite to viruses, a worm does not require a host program to overwrite its code, yet it can run on its own and conduct attacks.

Spyware

Spyware is a form of malicious software that collects a user’s data without his or her prior consent and transmits the information to a third-party. Subtypes of spyware generally include adware, Trojans, key-loggers, and rootkits. Spyware may capture all sorts of data, such as a user’s personal details, Internet browsing history, login credentials, and banking details. Additionally, spyware may install more malware, redirect web browsers, change a device’s settings, slow down the Internet speed, etc. Spyware does not usually propagate in the same manner as a virus or worm, because compromised devices do not typically try to distribute or replicate the malware to other devices. Instead, spyware is installed by exploiting vulnerabilities found in software or by misleading the user into opening infected documents.

Ransomware

Ransomware is a type of malware intended to encrypt the victim’s files or system unless a certain amount of money is paid out to the attacker. This is a serious danger that is not to be neglected by both individuals and organizations, being one of the most prolific cyber threats that took the cyber world by storm. Companies,

[21] AV-TEST Institute.

universities, hospitals, and city governments have fallen prey to ransomware attacks that have demanded hundreds of thousands of dollars (in Bitcoin or other cryptocurrencies) in exchange for their information. Currently, the average ransomware demand is about $84,000, with one-third of victims paying the ransom.[22]

Trojans

The name comes from the mythological story of Greek warriors who hid themselves inside a giant wooden horse and managed to infiltrate the otherwise impenetrable city of Troy, which resulted in its fall. Thus, Trojans can be defined as types of malware who disguise themselves as legitimate software and appear to be harmless upon entering the device, until their true nature becomes revealed. Types of computer Trojans include banking Trojans (which steal a user's banking credentials in order to gain access to his/her financial account), ransomware Trojans, key-loggers, backdoors, etc. Unlike worms, they do not have the ability of replicating themselves.

2. Phishing

Phishing is the most common type of social engineering and refers to the process of gathering a user's confidential details, such as login credentials and credit card numbers. The attack is usually conducted through what may look like legitimate websites (like Amazon, Apple, Yahoo, etc.), which in reality are clones of the real webpages. Once malicious hackers obtain the target's credentials, they use it to access the company's network or transfer money into their accounts. According to Verizon's 2020 Data Breach Report, 32% of confirmed data breaches involved phishing.

Subtypes of **phishing attacks** include:

Spear-phishing

Spear-phishing is a form of phishing whereby malicious actors aim to obtain sensitive information from very specific individuals or organizations. These attacks usually take the shape of emails sent to employees that appear to be coming from vendors or other employees, asking them to hand over sensitive information or transfer money. Most commonly, C-level executives are the ones impersonated, as cyber criminals are attempting to take advantage of their status and authority and therefore, the recipients feel compelled to act promptly.

[22] Emsisoft, 2020.

Whaling

Spear-phishing turns into whaling when attackers target high-profile individuals, usually in the C-level suite. In other words, whaling occurs when scammers go after the big "fish". While standard phishing attacks are generic, spear-phishing and whaling attacks are extremely targeted and involve extensive research from the attackers' side. Traditionally, CEOs, for instance, might have more information about them publicly available that cybercriminals can leverage and also more access to sensitive company data, that's why they become enticing targets. Although in an organization the number of possible victims may be much more limited compared with the total number of other job functions, the stakes are far higher.

SMSishing and Vishing

Sometimes, phishing also takes the form of SMSishing: text messages used to trick individuals into providing sensitive information. In most cases, the SMS will include a link to a malicious website which the target will be lured into accessing. Vishing (voice phishing), on the other hand, is the phone version of phishing, through which scammers contact people via phone with the purpose of harvesting their data. Both of these, just like any types of phishing and social engineering attacks in general, are being crafted with a sense of urgency and are asking for the target's immediate attention.

3. Password-based attacks

Passwords are the frontline of user account protection, so naturally, they are sought after by cybercriminals. Attackers utilize various methods to find passwords, leveraging both technical and psychological aspects. Cyber-attacks based on password abuse include:

- Social engineering - usually conducted through phishing campaigns.
- Brute-force - the attackers are entering various username and passwords combinations until they finally guess them.
- Password spraying - while brute-force attacks usually concentrate on a single account, in password spraying attacks criminals attempt to crack thousands of accounts at once by trying a small number of frequently used passwords.
- Credential stuffing - this practice relies on users' tendency to recycle credentials on different accounts. In this type of attack, malicious hackers are using compromised databases of usernames and passwords on different websites where the victims might have signed up on until they successfully find matches.

- Key-loggers - malicious software that records each and every keystroke on a device, including usernames and passwords.
- Shoulder-surfing - this attack takes place when cybercriminals are literally looking over the victim's shoulder when they type in their credentials. This may also involve discovering insecurely held passwords (sticky notes placed next to a computer, credentials saved on devices, etc.)
- Rainbow table attacks - Password hashing is based on the process of translating databases of passwords into random, encrypted strings of characters to avoid their exploitation. However, when malicious actors are using a table of pre-matched hash values to possible plain text passwords (rainbow tables), they may be able to reverse the hashing function and obtain the passwords.

4. Exploits

All devices are inherently vulnerable to hacking and can become overridden by malicious actors through exploited vulnerabilities. The International Organization for Standardization provides a thorough definition of "vulnerabilities": [23]

"In the contexts of information technology and cybersecurity, a vulnerability is a behavior or set of conditions present in a system, product, component, or service that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence."

Exploits can either function remotely (when attackers exploit a vulnerability without having accessed the system beforehand) or locally (which requires previous access to the system and typically the elevation of user privileges). After vendors become aware of existing exploits, they release security updates to fix vulnerabilities. The process of vulnerability management and patch management is vital and must become the norm within any organization. In practice, 60% of breaches were related to unpatched vulnerabilities that were available, yet not applied.[24]

5. APTs

Short for "Advanced persistent threats", APTs are attacks through which cybercriminals break into a network using several stages to circumvent detection. When a target's network is breached by an intruder, cybercriminals operate in such a way to remain undetected whilst maintaining their presence. Should the breach be discovered and remediated, the attackers can still remain inside the network and reach very specific goals such as exfiltrating confidential information, gather intelligence, or disrupt the company's activity.

[23] ISO/IEC 29147:2018(en).

[24] Ponemon Institute and Service Now, 2019.

6. Man-in-the-Middle (MitM)

Attackers rely on the MitM intrusion method by installing malware which interrupts the communication between devices, with the ultimate purpose of capturing sensitive information. These attacks are typically successful when one or more individuals communicate through an unsecured public Wi-Fi network, where malware has been already installed by attackers.

7. Insider threats

Insider malfeasance is a somewhat disregarded, yet dangerous threat. Over the past two years, the number of insider threats incidents has increased by 47%.[25] On top of that, 30% of all data breaches happened as a result of insider threats.[26] These types of attacks take place when employees with elevated user privileges (intentionally or unintentionally) perform malicious actions in a company. Insider risks can be more difficult to recognize and avoid than external assaults, as they are immune to conventional defense measures such as firewalls and intrusion prevention systems that have been traditionally designed to deal with external threats.

8. DDoS attacks

A DDoS attack (Distributed Denial of Service attacks) is a malicious cyber activity meant to render an online service inaccessible by flooding it with traffic from multiple sources. In short, DDoS attacks take place when servers are overloaded with requests until a website or a network is shut down. In some cases, such an attack may also be coupled with a ransom demand.

9. Business Email Compromise (BEC)

In the cybersecurity industry, email phishing (and all email-based attacks, in general) targeting organizations are also commonly referred to as Business Email Compromise (BEC). Being one of the most financially destructive cyber offenses, BEC attackers prey on of the fact that email is the most commonly used medium in business operations. What's more, cybercriminals also leverage the innate tendency of humans to be helpful. When having to deal with urgent requests, individuals tend to be affected by the sense of urgency and disregard security protection measures.

[25] Ponemon Institute and Proofpoint, 2020.
[26] Verizon, 2020.

In BEC schemes, messages appear to be coming from genuine senders who seem to be making a legitimate request, however, the situation is different. Some examples may include an impersonated CEO asking someone from the financial department for an urgent money transfer. According to the FBI, BEC scams accounted for half of the cyber-crime losses in 2019, amounting to nearly $75,000, per complaint, on average.[27]

10. Vendor-facilitated attacks

In their never-ending pursuit of finding new entry points, cybersecurity criminals are targeting vendors through their service providers and business partners, resulting in a very specific type of BEC attack, also known as Vendor Email Compromise (VEC). These types of attacks prove to be highly elaborate and usually take place in several stages, frequently involving steps such as breaking into a vendor's account, so that cybercriminals are able to send fake requests to a customer.

[27] Cimpanu, "FBI: BEC scams accounted for half of the cyber-crime losses in 2019", February 2020.

4.

PROTECTING YOUR SMB AGAINST CYBER THREATS

4. Protecting your SMB against cyber threats

Even though the disparities between SMBs and enterprises are obvious, both types of companies are utilizing IT systems and tools which make them vulnerable to cyber-attacks by default. Thus, as far as cybersecurity is concerned, the lines between the two are blurring. In other words, as both SMBs and large corporations are operating in the same markets and digitalizing their business models, cybercriminals are keeping pace and adjusting their techniques to achieve the quickest and simplest routes towards them. Numerous times, small businesses may even represent a backdoor to large enterprises.

The emergence and increased availability of the Internet helps companies large and small from all over the world access different and wider audiences, now being able to enter new markets and improve their competitiveness and performance. Through technology, every organization is empowered to grow and achieve more, yet the risks that come along with the digitalization process must not be neglected. Therefore, along with an SMB's digital transformation journey (no matter how simple or sophisticated it may be), its owner must also incorporate cybersecurity in its overall business strategy.

Improving cybersecurity is expected to save businesses potentially over $5 trillion in the next five years, which implies that SMBs will greatly benefit from this practice and reduce risks. Below we will discuss some crucial aspects that need to be included in any cybersecurity strategy.

4.1. The basics of a successful cybersecurity strategy for SMBs

In cybersecurity, prevention will always be the best cure, as the consequences of a cyberattack can be catastrophic. In the past, it was common for organizations to follow a reactive approach as far as cybersecurity is concerned. However, a mitigation-only strategy can prove to be incredibly expensive in the long run, in a day and age where cyber threats are increasing in sophistication and size. Therefore, proactive measures such as ensuring your employees' cybersecurity education, safeguarding your data, and utilizing software that prevents rather than mitigates threats is key.

4.1.1 Cybersecurity awareness training

Cybersecurity training is an ongoing need that must not be neglected. SMBs need to provide their employees with continuous education in regards to security best practices and perform routine check-ins along the way. Once your employees become educated as cyber threats develop, your company avoids compromising your customer's

data and your sensitive information, intellectual property theft, reputational damage, etc. Keep in mind that a data breach may undermine your customer's confidence or even make them interrupt their business with you, whilst others may even seek legal action.

Your SMB should create common safety standards and procedures for your personnel to follow, such as having secure passwords, developing clear rules regarding the usage of the Internet, setting up processes in relation to how your customers' records and your company's details are managed and kept secure, etc. If your employees are engaged in rigorous and continuous cybersecurity training sessions, your customers will be confident that their data is being properly handled and therefore their trust will further increase.

4.1.2 Data backups

Another cybersecurity best practice is to back up your data periodically. Sensitive documents such as customer contracts, spreadsheets and reports, accounting and financial data, HR information, etc. must be safely kept through backups. This process should be conducted regularly, with copies of your data being stored either offline or in the cloud. Should your systems be infected with ransomware, this will be your quickest and safest return to business as usual. However, backing up your data to an off-site location may not be enough. Beyond the protection of the system that stores your archives, encrypting your files is equally important. In case you need to recover them, your data will remain unaltered.

4.1.3 The Zero Trust model and the Principle of Least Privilege

This brings us to the next item which is not to provide unnecessary IT privileges to your employees. Following a philosophy of Zero Trust does not mean you should not trust your employees, but instead keep in mind that malicious actions might as well be performed on their behalf without their knowledge or consent.

Furthermore, the Principle of Least Privilege is based on the concept that employees can only be granted access to IT systems they need for their work. They should never be able to install software on their own without receiving permission first, as unauthorized software can carry malware or allow intruders to access your data, modify and delete it as they please, and create additional users with administrative rights.

4.1.4 Password Policies

Your users may be using the same passwords for different business-related accounts - for instance, for their personal email account and an online third-party service where they registered using their corporate email address.

If any of these websites become breached, chances are that cyber-attackers will practice credential stuffing to break into your employees' company accounts. What's more, your employees' passwords must always remain confidential. They should never share them with other colleagues or members outside of your organization. Furthermore, encourage your users to start using password managers. This way, they will only need to remember one passphrase used to access their password manager. Last but not least, multi-factor authentication can dramatically reduce fraudulent login attempts, so make sure you have set up this option.

4.1.5 Cybersecurity software

Aim to always maintain high standards when it comes to the security software you are using. Seek for software alternatives that fit your needs, while also sticking to your budget. What's more, ensure that you invest in a strong protection against malware, ransomware, and other cyber risks. At the same time, always install the latest system and software updates as soon as they become available to avoid exploits.

Do not neglect mobile devices, as they do also pose serious risks. Mobile endpoints may be exposed to considerable security problems, especially if they carry sensitive details or connect to your company's network. Always require your staff to secure their devices through password protection and secure your own corporate network to prevent attackers from stealing sensitive information.

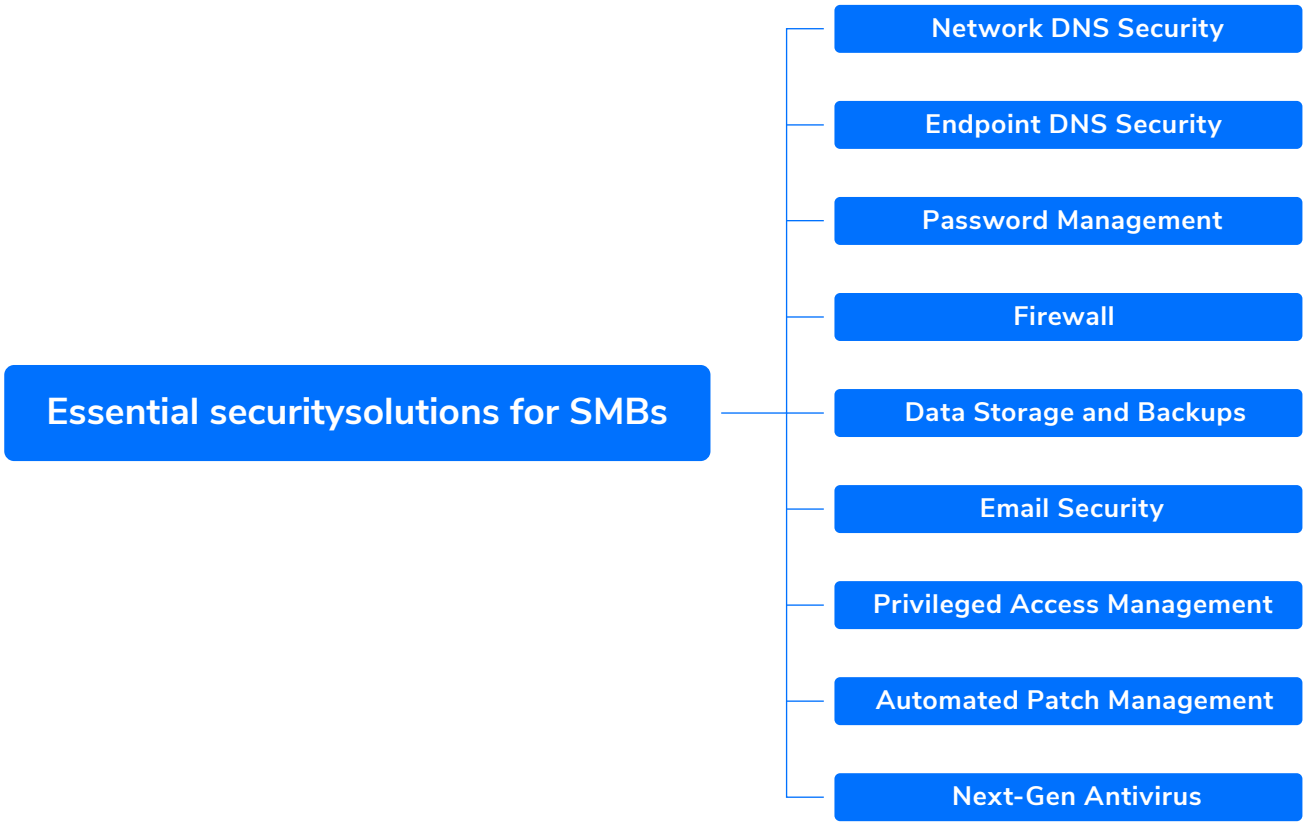
4.2. How to choose the right cybersecurity vendor

As we have already mentioned, it is vital to run your SMB in today's digital environment while being equipped with successful cyber protection and risk reduction tools to defend yourself against threats and safeguard your data. Regardless of the cybersecurity solution you end up choosing, it is imperative to keep in mind aspects like ensuring the safety of both of your networks and devices, impede unauthorized exposure of your confidential data to third-parties, guarantee your business continuity by avoiding unwanted downtime caused by service disruptions, and maintain (or even increase) your overall productivity.

The most efficient and powerful cyber defense should always come in multiple layers of protection.
A multi-layered cybersecurity approach encompasses software, employee training, policies and processes, and monitoring.

Below you can find a list of essential cybersecurity solutions that your SMB should not be missing:

- Network Security
- Endpoint Security (Anti-Malware/Anti-virus/DNS traffic filtering)
- Password Management
- Firewalls
- Data Storage and Backups
- Email Security
- Privileged Access Management



Key elements to consider when choosing your tools:

1. Automation

One key aspect to keep in mind is that you should automate your cybersecurity processes as much as possible, as this practice will save you time and financial resources. For instance, using an automated patch management solution will automatically install the latest updates you need to apply in a timely manner. Automating the most time-intensive tasks will certainly make a difference regardless if you are handling cybersecurity yourself, as an SMB owner, or if you have dedicated personnel in charge.

2. Availability

The cybersecurity software of your choice should work anywhere in the world. As telework is highly common for many organizations, you should ensure that your tools can be used and managed remotely.

3. Price

Compare alternatives and make sure you obtain the best value for money in regards to what the software can do for you. Almost 32% of small business owners are dependent on free security solutions.[28] Of course, utilizing several free cybersecurity solutions is not entirely wrong, as there are options that may suffice for small companies to some extent. Every organization needs to evaluate their alternatives and preferably search for security tools that have free trials and demos available, so they figure out if the solution would be a good fit for the company.

[28] BullGuard, 2020.

5.

CONCLUSION

5. Conclusion

For many businesses, data protection and safety are becoming differentiating factors in front of their customers when they are deciding if they want to spend their money at your business. Companies do have numerous possibilities to flourish in today's digital landscape, yet they must take precautionary measures as far as the safety and integrity of their data and systems is concerned. This implies that regardless of the size of a business, its leaders must not take cybersecurity lightly and should foster an organizational culture of Zero Trust, clear processes, continuous communication, and employee training in order to become a winner in cyber defense.

About Heimdal® Security

Heimdal Security is an emerging cybersecurity provider managed by world-renowned security experts, with an extensive experience in developing solutions that actively prevent, identify, and mitigate threats. We are one of the top go-to providers of valuable cyber intelligence and education for SMBs and large enterprises all over the world, providing AI-driven DNS-protection at the endpoint and network-levels, automated vulnerability and patch management, email security, and Next-gen Antivirus, with solutions that can be scaled up and tailored to fit your business's specific needs. Contact us for a free cybersecurity assessment and learn how you can enhance your company's security.

6.

BIBLIOGRAPHY

6. Bibliography

The World Bank, “Small and Medium Enterprises (SMEs) Finance”, 2020.
https://www.worldbank.org/en/topic/smefinance.

Salesforce Research, “Small & Medium Business Trends Report – Third Edition”, 2019.
https://www.wto.org/english/news_e/pres20_e/pr855_e.htm#:~:text=World%20merchandise%20trade%20is%20set,effectiveness%20of%20the%20policy%20responses.

International Trade Centre, “SME Competitiveness Outlook 2020: COVID-19: The Great Lockdown and its Impact on Small Business.”, Geneva, 2020.
https://www.intracen.org/uploadedFiles/intracenorg/Content/Publications/ITCSMECO2020.pdf

Verizon, “2019 Data Breach Investigations Report (Executive Summary)”, 2019.
https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

Kennedy, Carrie. "CYBERSECURITY AND CORONAVIRUS: Cyber Threats Are on The Rise". Otava (blog). April 8, 2020.
https://www.otava.com/blog/cybersecurity-and-coronavirus-cyber-threats-are-on-the-rise/

Ponemon Institute, “2018 State of Cybersecurity in Small & Medium Size Businesses”, 2018.
https://start.keeper.io/2018-ponemon-report

NIST (National Institute of Standards and Technology), CNSSI 4009-2015 NSPD-54/HSPD-23, NIST SP 800-37 Rev. 2, NISTIR 7621 Rev. 1 under Cybersecurity CNSSI 4009-2015
https://csrc.nist.gov/glossary/term/cybersecurity#:~:text=The%20ability%20to%20protect%20or,detecting%2C%20and%20responding%20to%20attacks.

Salesforce Research, “State of the Connected Customer” (Second Edition), 2018.
https://www.salesforce.com/content/dam/web/en_us/www/documents/e-books/state-of-the-connected-customer-report-second-edition2018.pdf

Cihodariu, Miriam. “SECURITY ALERT: US Users Targeted with Corona Virus Phishing Attacks”. Heimdal Security (Blog). February 6, 2020.
https://heimdalsecurity.com/blog/security-alert-corona-virus-phishing/

WHO (World Health Organization), "Beware of criminals pretending to be WHO", Accessed August 11, 2020.
https://www.who.int/about/communications/cyber-security

Unterfingher, Vladimir. "Traffic to Malicious Websites Spiking as more Employees Take Up Work from Home". Heimdal Security (Blog). March 24, 2020
https://heimdalsecurity.com/blog/malicious-websites-work-from-home/

CISA, "Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors", April 8, 2020.
https://us-cert.cisa.gov/ncas/alerts/aa20-099a

Switchfast Technologies, "Cybersecurity Mistakes All Small Business Employees Make, from Entry Level to the C-Suite", 2018.
https://us-cert.cisa.gov/ncas/alerts/aa20-099a

PWC, "The Global State of Information Security® Survey 2018"
https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

AV-TEST Institute, "Malware", Accessed August 12, 2020.
https://www.av-test.org/en/statistics/malware/

Emsisoft, "The cost of ransomware in 2020. A country-by-country analysis", 2020. February 11. 2020
https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/

International Organization for Standardization, "ISO/IEC 29147:2018(en) Information technology — Security techniques — Vulnerability disclosure", Accessed August 12, 2020.
https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en

Ponemon Institute, Service Now. "Costs and Consequences of Gaps in Vulnerability Response", 2019
https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

Ponemon Institute, Proofpoint. "2020 Cost of Insider Threats Global Report".
https://www.observeit.com/cost-of-insider-threats/

Cimpanu, Catalin. "FBI: BEC scams accounted for half of the cyber-crime losses in 2019". ZDNet. February 11, 2020.
https://www.zdnet.com/article/fbi-bec-scams-accounted-for-half-of-the-cyber-crime-losses-in-2019/

Accenture. “Ninth Annual Cost of Cybercrime Study”. March 6, 2019.
https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

BullGuard, “New Study Reveals One In Three SMBs Use Free Consumer Cybersecurity And One In Five Use No Endpoint Security At All”, 2020.
https://www.prweb.com/releases/new_study_reveals_one_in_three_smbs_use_free_consumer_cybersecurity_and_one_in_five_use_no_endpoint_security_at_all/prweb16921507.htm

Heimdal®

Leading the fight against cybercrime.

www.heimdalsecurity.com

Vat No. 35802495, Vester
Farimagsgade 1, 2 Sal, 1606 København V