Everything you ever wanted to know about cybersecurity

(but were too afraid to ask)

kaspersky

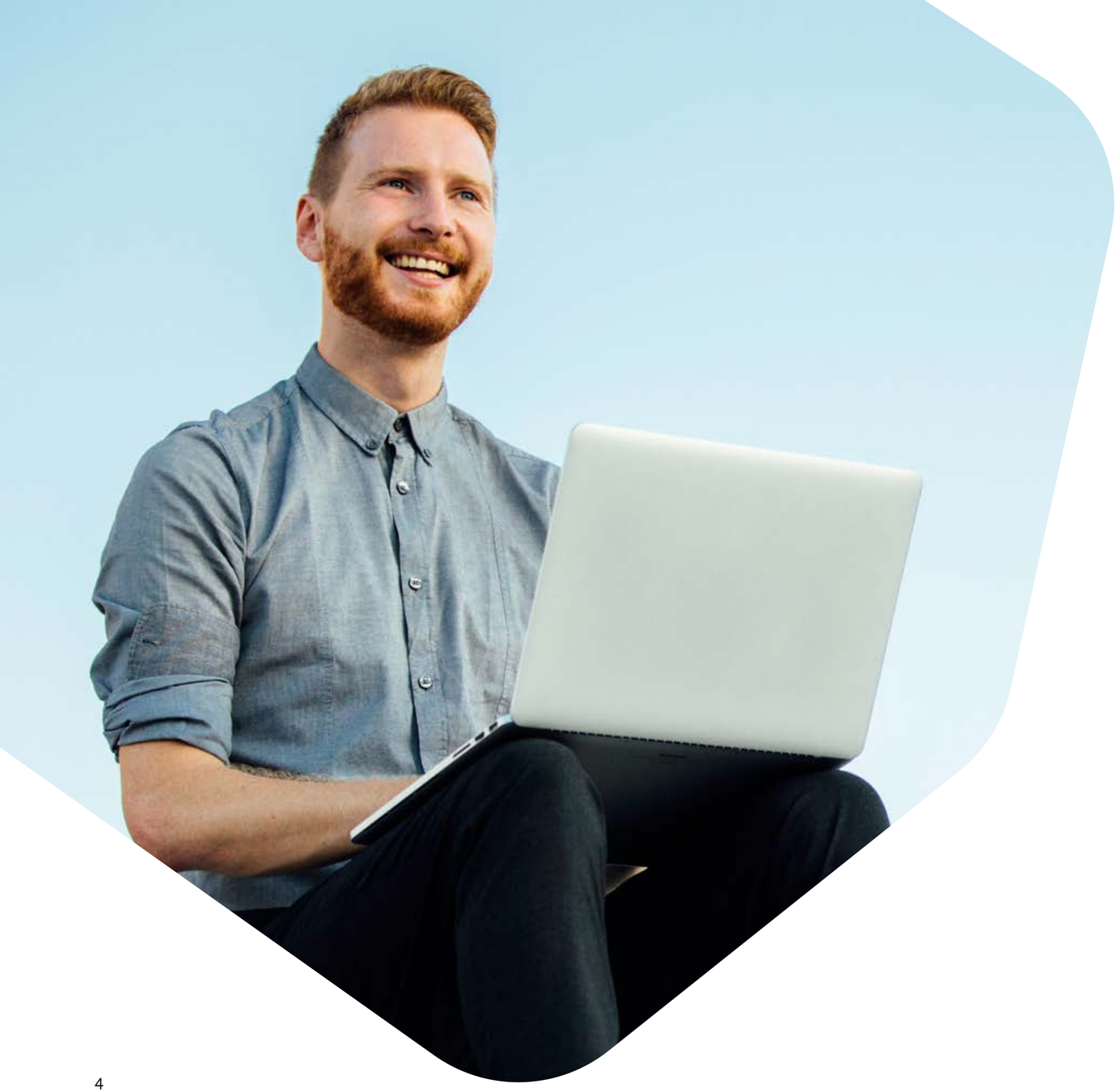
Hello!

This guide will tell you everything you need to know about how to keep your business safe for today (and tomorrow), without going broke (or nuts) in the process.

And, since your business is highly likely to be bigger tomorrow than it is today, we've dedicated a section to growth, so that you can be ready for the cyber risks that typically threaten larger businesses.

Before we tell you what you're going to get out of this guide, we want to explain why we believe that SMBs deserve a fuller and more dedicated resource for cyber defense.

It's simple:
All businesses are small to begin with; and there is no such thing as small.



This sounds obvious, not to mention oxymoronic, but the point is that SMBs are often overlooked by cybersecurity commentators because of their size, forgetting that the size of your business says nothing about its power, its importance, its growth, or its future.

When we talk about human beings and our own growth, we have no trouble identifying certain periods as either ‘formative years’ or as ‘critical periods’. And we take great care to steer, cultivate and – above all – defend our friends or our children (or ourselves) as they (or we) pass through these periods. This is not to compare SMBs to children — after all, just like with adults, there is no necessary correlation between size (or age) and maturity.

We feel that there has been a tendency in the cybersecurity industry to overlook the importance of cybersecurity for SMBs, perhaps because of their size, or because of the nature of the threats they might have been expected to face in the past.

Your business matters to you just as much (if not more) as a Fortune 500 company matters to its shareholders.

And now we're going to explain why we're publishing this guide at this particular moment in cyber security history:

The times, they are a'changing. (Newsflash: they've already changed).

Luckily, we can explain this one in precisely three lines, and seven lucky words:

New threats.

New culture.

New defensive technology.

7

We promise you these five key business-changing takeaways:

1 **This guide is about action.**

We promise not to deliver a single insight without an action you can take that accompanies it. Sometimes that will be a concrete action, other times it will be a way for you to actively change your way of thinking to bring about a more effective approach to defending your business.

2 **This guide deals in reality — your reality.**

We're going to make it easy for you to find and learn the insights and actions that matter to your business, so you can leave the chaff behind and keep moving.

3 **This guide will remove fear from the equation.**

We don't deal in fear-mongering. We'll tell you what risks to look out for, but we'll always show you how easy it is for you to defend against them without breaking sweat.

4 **This guide will speak to you expert-to-expert.**

So you're not a cybersecurity specialist? Doesn't matter. You're an expert in your business, and that's all that matters.

5 **This guide will give you mastery over your business' cybersecurity needs.**

Things have changed. You don't need a specialist IT team to stay informed or stay safe. You are in control, and you can do this.

How is cybersecurity like a car seatbelt?

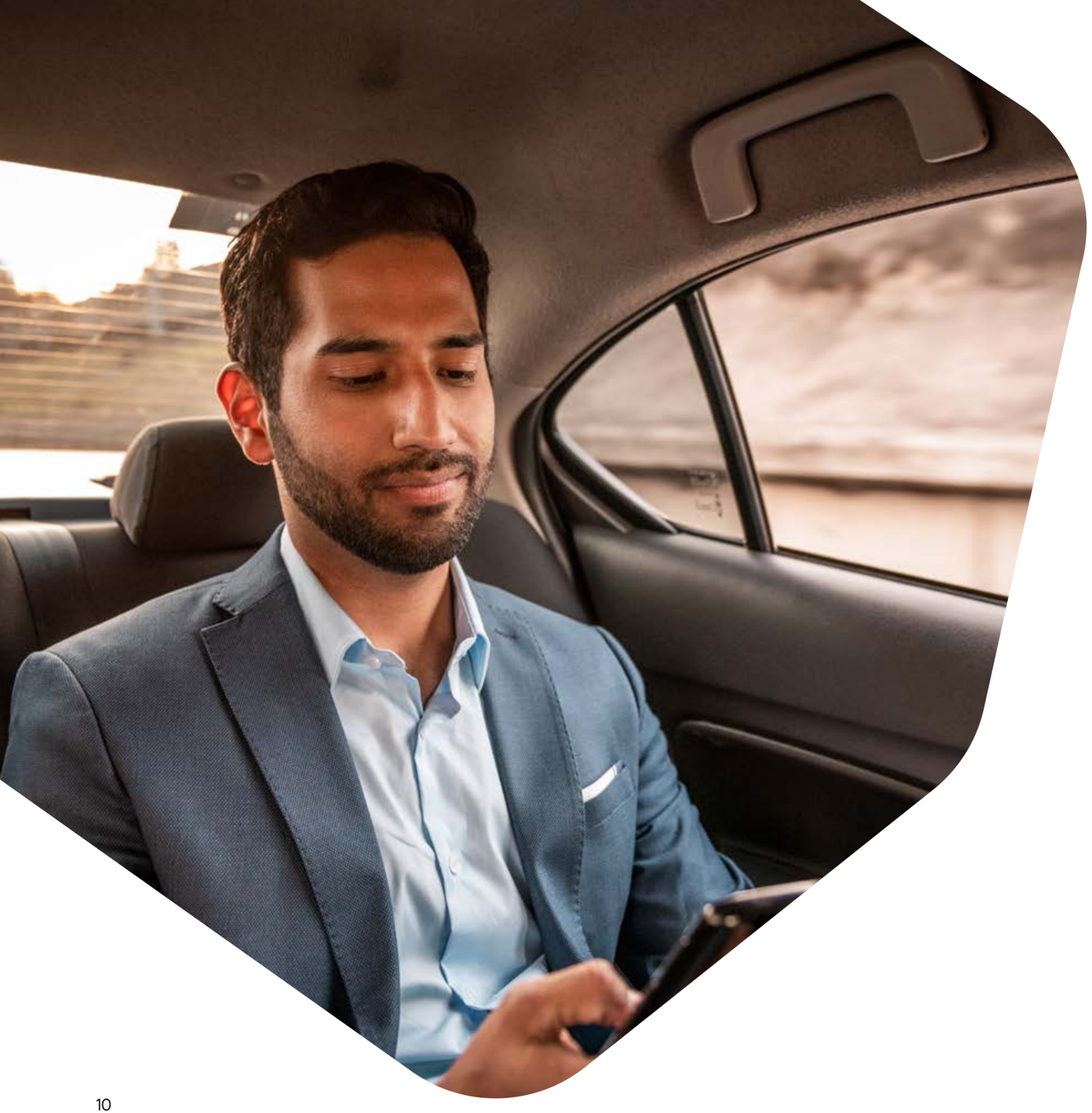
When you get into your car, you put your seatbelt on without a second thought. And, if you forget, most new cars have alarms that remind you.

Why do you put that seatbelt on? It's not because you think you're going to automatically crash and burn every time you drive to the supermarket. At the same time, you know exactly what the risks are.

Unless you are a particularly anxious driver, you don't put your seatbelt on because you enter your car each morning full of frightening thoughts about the various potential tragedies that lie ahead of you on your commute.

It's not fear that makes you put your seatbelt on. It's common sense.

You put your seatbelt on so that you don't have to give those risks a second thought.



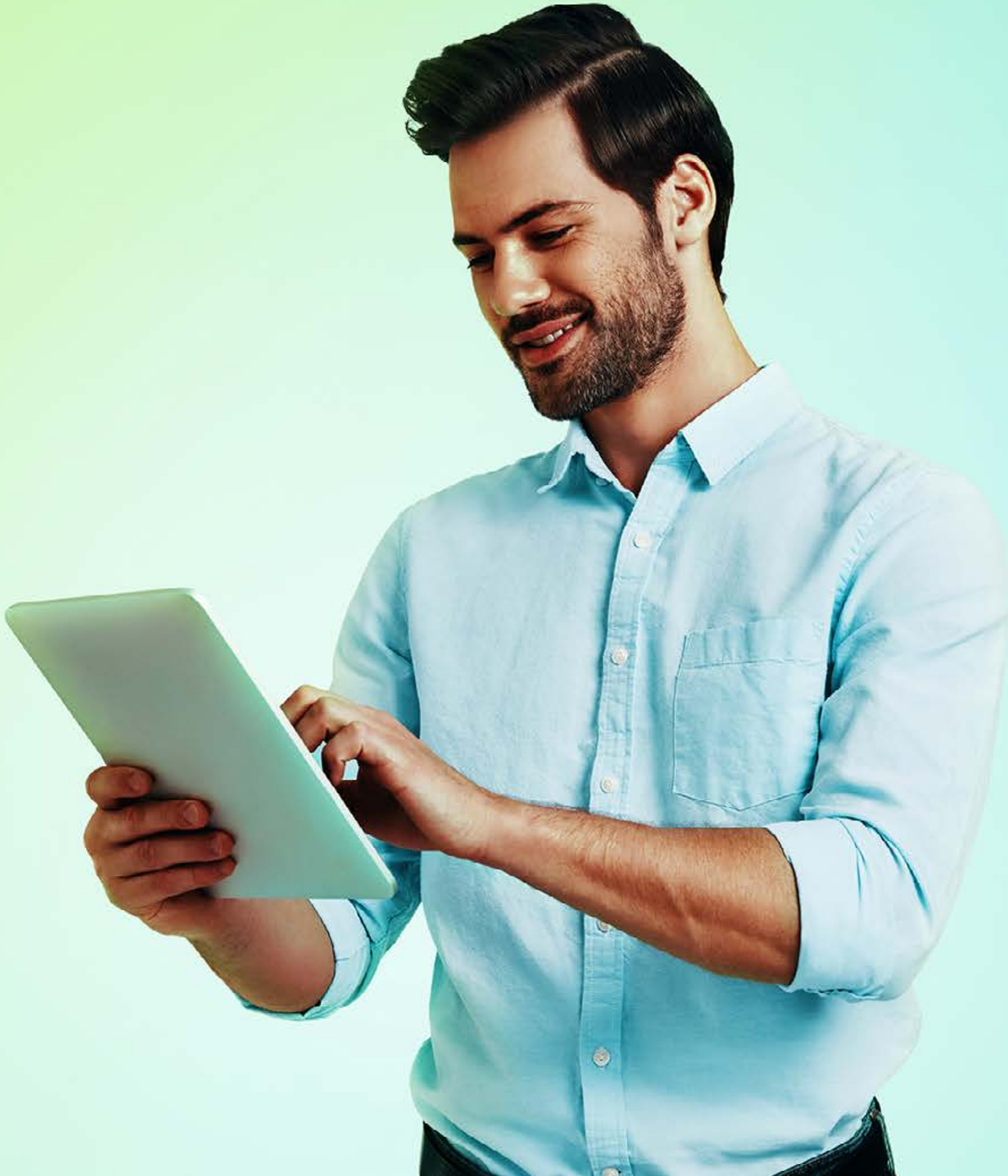
That’s exactly how cybersecurity should be, and that’s how we want you to think about it as you read this guide.

You (and your business), like the driver in the car, are going somewhere.

You can’t afford to focus on risks. That kind of mindset will slow you down. We’re going to show you how you can approach cybersecurity in exactly the same common sense matter-of-fact way as you approach putting on your seatbelt.

Buckled up?

Let’s go!



Contents

Chapter One

No such thing as small fry (Does size even matter?)

Let's start with the good news.

Your business is highly unlikely to become the target of an advanced persistent attack by a multi-million-dollar nation state enemy cyber-army. (Hmmm, that probably doesn't sound as comforting as it should. Besides, anyone can theoretically get caught in the crosshairs of an international state-sponsored attack).

So let's try that again.

As an SMB, you can absolutely still expect to have some natural immunity to the most horrific, complex and devious cyber-attacks. These usually involve a great deal of highly precise and diligently researched targeting, and the actors behind them probably won't be interested in investing significant time, funds and people in bringing your business to its knees.

However, the cybersecurity landscape has changed dramatically for SMBs over the last few years, and it's important that SMB leaders appreciate quite how dramatic that change has been.

Two factors lie behind this:

Malware for sale

Cybercriminals don't actually require very complex expertise in order to launch relatively complex attacks. Various forms of malware are now for sale on the Darknet, some for as little as a dollar (US). So the bar to entry has dropped, while the complexity (and quantity) of threats has risen.

Throwing a wide net

Increased connectivity (including cloud use), coupled with the proliferation in the number of devices businesses rely on, has made it easier for cybercriminals to 'throw a wide net' with the hope of catching (somewhat at random) those 'fish' who have failed to adequately defend their IT perimeters.

What hasn't changed (at least not fast enough), is that many SMBs still address cybersecurity from a pre-2016 standpoint.

What's so special about 2016?

Well, apart from the fact that Portugal won the Euros, it's also the year Pokémon Go and Google Cloud Platform were launched and – for the first time – more than half the world's population (4 billion people) was connected to the internet. Kind of a big deal.

Responsibility for this attention lag doesn't rest on the shoulders of SMBs. Regulatory requirements have been slow to catch up (these serve as helpful advisories as well as painstaking compliance points), and shared responsibility security arrangements with cloud providers have (forgive the pun) somewhat clouded the water.

But it does mean that cybercriminals often see SMBs as low-hanging fruit: poorly defended and easy to penetrate. Couple that with twin trends of malware for sale and 'wide net' tactics, and you have a tricky situation.

Back to the good news.

The cybercrime bar to entry isn't the only bar that has lowered considerably since the heady days of Pokémon Go mania. The cybersecurity bar to entry has also lowered, probably more so than that of cybercrime. And the cloud has played a huge role in this also.

We're not going to go into this in great depth until chapter five, but suffice to say that SMBs can now easily manage complex cybersecurity without the complexity. And by 'complexity', we're talking about a level of devilishness that requires a dedicated in-house IT security guru.

Anyone with a web browser can now keep their business safe, from anywhere – even if their staff are working remotely.

Part of what has made SMBs vulnerable is precisely the same false sense of security that comes from holding onto that pre-2016 mindset.

We've heard SMB leaders say things like:

"I don't need vulnerability scans or patch management, I'm a 20-person operation with a turnover of less than $1M."

"Why would anyone want to launch a ransomware attack on a business like ours?"

"We've never had any problems, our anti-virus works great."

If any of these statements sounds familiar to you, don't worry. We're not here to freak you out – that's not what we're about. This guide isn't about telling you to worry, it's about helping you transform any false sense of security into a real sense of security.

Trust us, you'll not only know, but **feel** the difference.

Lastly, and this is really the reason we've poured everything we know into this guide for SMB leaders, your business isn't small, no matter how small it is. Even if you're the only employee, maybe especially if you're the only employee. Your business isn't small to you, and it isn't small to your customers.

Business behemoths can and do bounce back from devastating nation-state attacks (albeit with some frightening stock fluctuations and a heavy investment in remediation and reputation management).

It's time that smaller businesses got the dedicated respect and support they deserve to stay safe no matter what.

Every business deserves the right to relegate cyber risk to where it belongs (under control), so that it doesn't threaten your operations or occupy too much of your precious bandwidth.

Chapter Two

Start where you are — but where is ‘where’ anyway?

Start where you are

Sounds straight forward enough.

But what does ‘where’ even mean?

Clearly, we can all say where we are in place and time, but where exactly is your business?

Let’s break down that ‘where’ into five parts and deal with them in turn:

1

Geographical jurisdiction

2

The distribution of your data storage and/or network (on-premicloud/ hybrid)

3

Your industry

4

Your office (if you have one)

5

Your mindset

1. The ‘where’ of geographical jurisdiction (otherwise known as the old-fashioned ‘where’)

This is easy — it’s just about which country (or region) your business is registered. Depending on geographical location, you’ll face different risks, as well as different regulations.

This is easy – it’s just about which country (or region) your business is registered. Depending on geographical location, you’ll face different risks, as well as different regulations.

A word on regulations:
It’s worth bearing in mind that regulations can sometimes lag behind the pace of technological change, not to mention the evolution of the cyber-threat horizon. While you should clearly ensure that your cybersecurity and data privacy configurations comply with local regulations, it’s a good idea to consider whether you might want to look beyond these, preparing for the future and protecting today.

You’re probably already aware of the regulations affecting your business but, if not, a good resource is the United Nations Conference on Trade and Development minisite on **Cybercrime Legislation Worldwide.**

For cyber risks affecting your geographical location, you're welcome to peruse Interpol's dedicated site, but it can sometimes be unnecessarily alarming; don't let it lead you down a pointless vortex of cyber horror.

Instead, try having a look at our animated Cyberthreat Real-Time Map that gives a depiction of cybercrime in your country at any given moment. But don't linger too long on it – we've got work to do.

For sure, you don't need to delve deeply into the precise risks affecting your country. Instead, provided you choose an award-winning globally recognized cybersecurity supplier — maybe one that starts with a 'K' and has won more top three places in independent tests than any other vendor — you can rely on them to make sure you're kept aware of everything you need to know about local risks without weighing you down unnecessarily.

2. The ‘where’ of data/ network distribution

Where is your data? How do you locate something you can’t touch?

Virtualization and cloud hosting have made it harder to pinpoint the exact location of businesses’ most precious assets — data.

Presumably you’ll find it quite easy to tell how much storage you have access to, where it’s hosted, and how much of it you’re using.

But it's important to pay attention to two key questions when surveying the lay of the data-land:

Is our most sensitive data being stored in the most highly protected location?

Only you know what your most sensitive data is – and it's important that it receives dedicated attention. It must be stored in the best possible location, with the best possible protection and access policies.

Who exactly is responsible for cloud storage? Is it Microsoft? Google? AWS? Me?

If you're not already using a hybrid cloud model, you probably will be soon. And in a sense, we all are, to some extent – even as consumers. While it's true that cloud providers share some of the responsibility for security, the true picture is a little more nuanced. Apart from anything else, there's the question of access: the business of passwords and permissions lies in your hands alone. Furthermore, some manufacturers' native cloud security solutions don't go far enough. For one thing, criminals are more than happy to spend time seeking out native cloud security vulnerabilities – it's highly rewarding to infect a service that millions of users rely on. Crack one lock and you've cracked them all, goes the sick logic of cloud service crime.

3. The ‘where’ of your industry

This is important, especially when it comes to considering risk. Unsurprisingly, the industry most attacked by cybercriminals is finance. But clearly no industry is completely immune.

What matters is that every industry is attractive (and vulnerable) in its own way, and it’s important to think about cybersecurity from an industry-informed perspective.

These are some of the factors you might want to think about in terms of your industry:

1 The perceived value of your data and that of your customers. Even small business can be targeted by data theft and other breaches, and such thefts aren’t restricted to financial data

2 The devices you use. For example, if you’re a retailer or hospitality provider, you’re more likely to rely on mobile POS devices (like Square, SumUp, or Zettle), so you’ll have specific security needs that address those devices

3 If you’re a disruptive startup, innovative product designer, or otherwise operating in a high-growth/high-innovation space, you may need to think about the possibility of intellectual theft, sabotage, or espionage from competitors

4 What degree of technological expertise do your staff have? Some industries (e.g. healthcare) require enormous expertise of their staff, but this by no means necessarily extends to IT knowledge. If your business operates in an industry that only uses technology for day-to-day operations, you’re going to have less tech-expertise to draw on among your staff than if your industry was already tech-oriented at its core.

4. The ‘where’ of your office (if you have one)

Kitchen table? Co-working space with bean-bags and ping-pong? An entire floor in a glass-encased CBD landmark? Anywhere and everywhere, and also, sometimes, nowhere?

Kitchen table? Co-working space with bean-bags and ping-pong? An entire floor in a glass-encased CBD landmark? Anywhere and everywhere, and also, sometimes, nowhere?

It matters. The first and most important thing to think about is the security of the network you’re using. Public WiFi is public – even if it’s password protected and only available to other business users. Home WiFi isn’t public (thankfully), but it comes with its own risks.

If you have a fixed office, you’re going to have a very high standard of access restrictions and other protections. It’s important to be able to replicate these wherever your employees are.

Thankfully, achieving that same high level of security isn’t too complicated anymore. You’ll obviously need to use a cybersecurity solution that recognizes the remote working reality, and makes it easy for you to set security policies to keep your business (and your employees) safe wherever they’re working.

Sometimes that will involve blocking personal devices from accessing the corporate network, but not always. A lot of businesses have Bring Your Own Device (BYOD) policies, under which employees use their personal devices for work. To some, it sounds like a security nightmare, but there are ways around the risks and – again – you'll need a cybersecurity solution that addresses BYOD.

Even if you don't have a specific BYOD policy, you're probably aware that employees are using their own devices for work at least some of the time. Staying on top of that is important but – again – there are ways to do it without losing sleep.

Education becomes increasingly important as the lines between the office desk and the kitchen table continue to blur.

Not to put too fine a point on it, but Gartner Inc. predict that, through 2023, more than 95% of cloud security incidents will result from human error. Many of those errors can be eliminated by educating your staff about cyber hygiene and awareness. We've got a whole section devoted to that, and you can skip ahead to it right now over <here>. The short story is that education is more important than ever before, but you can do it, and you can do it easily.

5. The ‘where’ of your mindset

If you’re an SMB leader, your mindset is naturally stunning. Innovation is your native language, and growth is your middle name. And if you’re reading this guide, you obviously care deeply about keeping your business safe.

These two questions will help you assess your cybersecurity mindset:

1 How much of a role does fear play in driving (or avoiding) your cybersecurity policies? Fear is pointless. It’s like the seatbelt we mentioned in the introduction. You take the right precautions for your business so that you can get on with your journey in confidence.

2 When you think about cybersecurity, which words come to mind? Do any of the following sound familiar?

a. Stressful

b. Irrelevant

c. Expensive

d. Time-consuming

e. Complicated

f. Boring

If so, we’ve (unsurprisingly) got news for you. We can knock down each of those misconceptions one by one, and help you shape the cybersecurity mindset that will set you free – not pin you down.

Misconception # 1:

Cybersecurity is stressful

Cybersecurity isn't stressful. What is stressful, is a cyberattack. So long as you choose solutions that take your specific needs and capacity into consideration, cybersecurity needn't be stressful at all. The same technological advances that have revolutionized how we live and work have revolutionized how we protect ourselves (and our businesses).

Misconception # 2:

Cybersecurity is irrelevant

This is common among businesses that operate outside of the confines of the office wall. The truth is that cybersecurity matters for every business (and every individual, come to think of it).

Misconception # 3:

Cybersecurity is expensive

Well, we'll be the first to admit that it's not free, but it's certainly cheaper than undoing the damage of an attack. And besides, with flexible subscription licensing that recognizes the unique needs of unique businesses, the right cybersecurity solution is more cost-efficient than ever before. In any case, cybersecurity is an essential cost that belongs on the same value sheet as IT as a whole – and it defends all your other investments.

Misconception # 4:

Cybersecurity is time-consuming

If cybersecurity is time-consuming then – firstly – you're doing it wrong, and – secondly – you've come to the right place. Our dedicated cloud-based security solution for SMBs delivers robust world-leading protection to your fingertips in just 15 minutes a week.

Misconception # 5:

Cybersecurity is complicated

Undoubtedly, cybersecurity technologies are complex. But that's our business, not yours. Cybersecurity technologies have to be complex because the risk profile today is complex – even for SMBs. However, this complexity is imperceptible to the user (unless you're that way inclined, in which case, hello fellow cyber-geek!). There's no point in delivering complex cybersecurity technologies that real business people can't operate. Our flagship SMB solution has a beautifully simple interface, and the option to choose between numerous preconfigured policies, or to configure your own. Either way, the experience is simple, no matter how complex the technologies that lie behind that crystal-clear pane of glass.

Misconception # 6:

Cybersecurity is boring

This is hard for us to understand because we're obsessed with cybersecurity and have been for over two decades. But I guess we can try to imagine a world where people don't eat, sleep and breathe cybersecurity... It's unlikely that you went into business because you couldn't wait to delve into the latest cybersecurity technologies, we'll give you that. But even so, the right cybersecurity solution for your business will be as attractive and as satisfying to use as any of the apps you rely on for your personal life (though there'll be less gossip and definitely no humble-boasting). And if you still find it boring, you needn't worry. It's so quick and easy to manage that you'll be able to move onto something far more interesting before you know it.

The ideal cybersecurity mindset is both hot and cool

Hopefully we've been able to slash through some common misconceptions that drain otherwise positive mindsets from effectively addressing their business' cyber needs.

The main takeaway is that the right cybersecurity mindset is two things at once:

Hot

Cybersecurity is a top priority, and I've got to face it, sort it and work it.

Cool

I've dealt so well with my business' cybersecurity needs that I don't sweat it, ever.

It's all about taking positive action to reduce the need for negative action. A bit like brushing your teeth, perhaps.

Chapter Three

People power — who can you count on?

Dolly Parton may not be the first person you think of when addressing cybersecurity, but bear with us just a moment — you won't regret it. Just consider these words of wisdom:

"Find out who you are and do it on purpose"

These words come from a highly successful self-made businesswoman and philanthropist, with a net worth of over 600 million USD.

We can’t overstress the importance of the guidance contained in this chapter.

In this chapter, we’re going to urge you to follow Dolly’s advice by conducting an easy-to-follow dedicated SWOT analysis to make sure that you’re using every ounce of people power to keep your business cybersecure.

Cybersecurity isn’t only about technology, it’s about people. We’re going to address this from a positive angle here – it’s always more productive that way. At the same time, it would be remiss not to mention that the majority of cyber incidents will occur as a result of human error.

Top industry analysts Gartner, Inc. spell this out in no uncertain terms:

“Through 2022, at least 95% of cloud security failures will be the customer’s fault.”

If that statistic sounds a bit ‘glass half empty’ to you then welcome to the club!

We read it like this: “Everything you need to keep your business secure is within your control.”

Technology is one piece of the puzzle (a vital one, obviously). Now we’re going to look at the person (or people) who are putting that puzzle together.

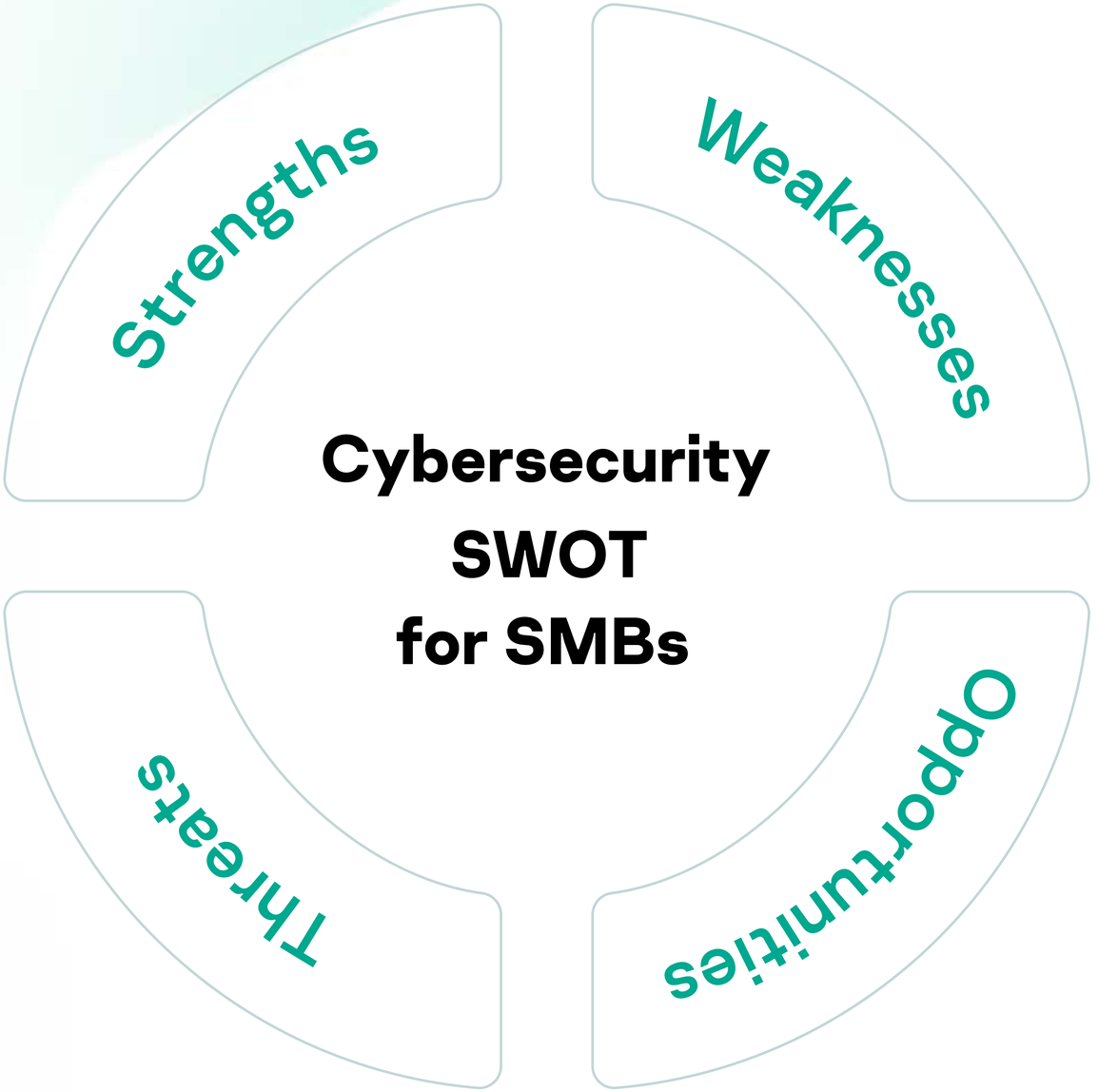
Cybersecurity SWOP for SMBs:

Strengths — Weaknesses — Opportunities — Threats

You're probably already familiar with the SWOT analysis process and – even if you're not – you probably already do it subconsciously all the time. Let's dive right in and see how you can use a simple process to make sure you're using all the people power available to you.

For each area, there are some key questions to consider. Make sure you keep an open mind and focus on what every SMB leader already knows: that people wear (or are capable of wearing) more than one hat; and skills can often be found in unexpected places.

- What experience do you have of dealing with cybersecurity (including personally?)
- What are some things that you do regularly to keep your devices secure?
- How do you protect customer information in your work?
- Tell me something about your IT knowledge in general



- Is everyone paying attention to basic cyber hygiene? (see our checklist below)
- What gaps (if any) are there in overall awareness that cybersecurity is everyone's business?
- How can we make sure that we're using our cybersecurity resources to the utmost?

- Which processes (or departments) are most vulnerable to cyber incidents?
- How can we use all our available people power to address weaknesses that expose us to the risk of human error?
- What might happen if we don't address these weaknesses?

- Does the thought of using innovative technologies to protect our business sound like something you'd be interested in?
- As part of your career development, how do you feel about taking on some more IT responsibilities?
- When you have an IT problem, who do you normally turn to for advice?

People power includes everyone

Keeping an open mind when going through the SWOT process above is absolutely crucial. With connected workplaces, anyone who has access to a device has a role to play in protecting your business. Conversely, this means that anyone could potentially introduce a cyber-risk.

This is why it's so important to be open to discovering cybersecurity talent or passion in your team, while also trying to uncover bad habits. This applies regardless of the individual/s official job titles. You have to use everything (and everyone) available to you. Don't leave anyone out (including contractors).

A cyber hygiene checklist any business can use

You don’t have to wait before harnessing the power of people to protect your business. You can do it right away by adopting our free cyber hygiene checklist below.

Why not print a few and keep them posted around your premises? It’s a good idea check in regularly to make sure everyone’s on board.

You can build also build the checklist into your human resources policies as a clear statement of the expectations and requirements your business has of everyone you employ.

We find that people often appreciate the clarity that such tools provide – demystifying the question of cyber risk, and giving clear steps to follow in the event of suspicious activity.

Cyber hygiene checklist

- **Shut down my computer if I'm away from my desk**
- **Cover up my webcam when I'm not using it**
- **Don't download attachments or click on links unless you trust the sender**
- **Only open emails from people you know and trust**
- **Follow the password rules:**
  - At least 8 characters
  - Mix numbers, letters (upper and lower case) and symbols
  - No sequences, words, or repetition
- **Change passwords regularly**
- **Use a different password for each account**
- **Use two-factor authentication wherever available**
- **If a password is stolen (or the account otherwise hacked), change it immediately and contact the relevant service**
- **Only use apps or online services (including social media) that have been approved by the company**
- **Don't use personal devices for business purposes unless approved in advance**
- **Use a PIN, touch or face ID to protect phones and tablets**
- **Never share your password with anyone else**

Cyberattack awareness checklist — fifteen signs anyone can spot

How sure are you that everyone on board knows how to spot signs of a cyber-incident? Unfortunately, awareness is often lacking, which leads to delays in response that can be critical.

Luckily, you can address this issue easily by making this list available to all your staff:

If you need an easy way to drive the message home, just make this sentence your mantra:

If my computer is slow, keeps crashing, or my email's behaving strangely, I will stop using it immediately and tell X.

In which 'X' is probably you – but it could be a team of people or someone else with responsibility for IT security.

Cyberattack awareness checklist

Email

- **You can't access an account**
- **You receive a notification that your account has been accessed from an unusual IP address**
- **You've received password reset requests that you didn't make**
- **Unusual activity (e.g. people report receiving suspicious mails from your account)**
- **You've received a ransomware demand or other threatening email**

Web

- **There's unusual content on the company website**
- **The company website is slow to load**
- **Your browser keeps redirecting you against your will**

System

- **Your computer is running slower than usual**
- **You're seeing unusual pop-ups or ads**
- **Your computer shuts down and/or restarts randomly**
- **You can't log on to the company network**

Network

- **You try to access a file or folder but it's unexpectedly encrypted**
- **The network is slower than usual**
- **Programs are opening, closing and crashing automatically and/or randomly**

Cybersecurity first-aid matters

Just as you need to have a physical first-aider to hand at all times, you also need to make sure that you have a cybersecurity first-aider. And just like a physical first-aider doesn't have to be a doctor or nurse, nor does your cybersecurity first-aider. It's just about knowing what to do if there are any signs of cyberattack or compromise — putting on the bandages until expert treatment is available.

You need clarity

SMBs often have to work harder to bring clarity of responsibility because job roles tend to be more flexible; this is a general point, and not restricted to cybersecurity alone.

You're unlikely to have a multi-tier IT support team, a Chief IT Security Officer, an IT Director, and perhaps you won't have a dedicated IT administrator.

Clarity is vital when it comes to cybersecurity—without it, your people could end up in a "somebody do something!" panic, in which nobody actually does anything.

Hopefully you will have uncovered some potential IT security talent during your SWOT analysis above. All you have to do now is bring those people together and have some discussions about what each of you can offer in terms of skills and responsibilities to support your company's cybersecurity efforts. Holding regular brief catch-ups with these people will also give you the chance to get new insights and ideas that will help your business stay safe.

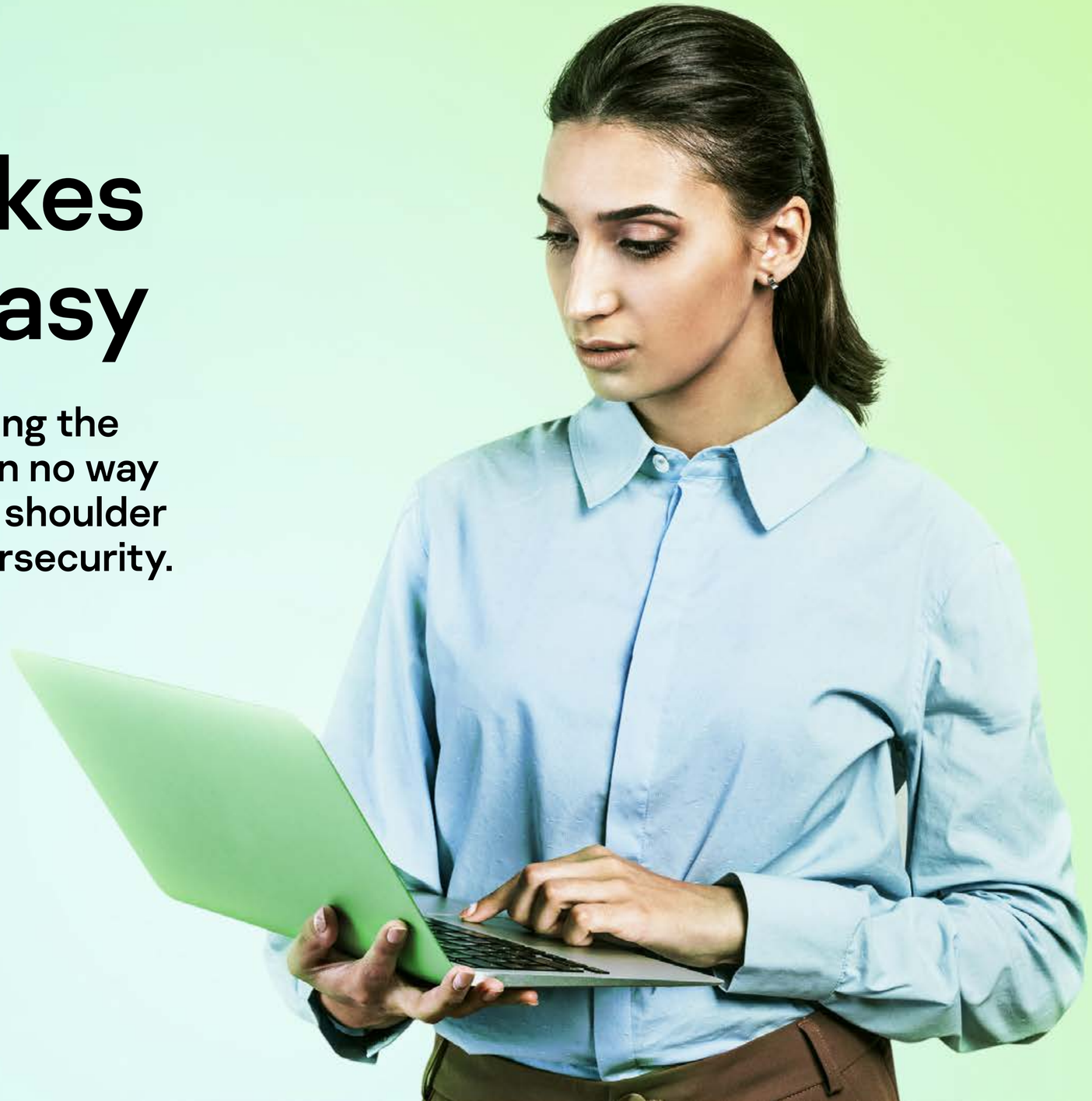
Your staff will appreciate this approach too—they'll feel valued and perform better because you're recognizing their skills, listening to them, and offering professional development opportunities.

Automation makes responsibility easy

We've made a huge point of emphasizing the importance of people power, but this in no way means that you (or your staff) have to shoulder a heavy weight when it comes to cybersecurity.

This relates back to some of the misconceptions we dealt with earlier: cybersecurity doesn't have to be stressful, complicated or time-consuming. We have automation to thank for that.

The right SMB cybersecurity solutions automate routine tasks (saving time), but they also make it easier than ever for users to master and control otherwise complex technologies.



Automation is more human than you think

Automation in cybersecurity is rather like being a human being.

We don't have to work consciously to control our heartbeat or our liver function, or our digestive systems — our autonomic nervous system takes care of that, so we're free to focus on the business of living.

At the same time, we can control what we do with our bodies. We're able to notice when we're not well, and seek medical attention if necessary.

Automation in cybersecurity does the exact same thing — it relieves the responsibility for conscious work where relevant, and frees businesses to focus on the business of, well, business.

Chapter Four

Understanding risk without fear

There's an obvious relationship between risk and fear. Getting the right balance is everything. We have to avoid the two traps that businesses can fall into when it comes to addressing cyber risk:

Fear can hold you back, and inaction is risky

Risk can be frightening, but ignoring risk is risky

This chapter is short, but important.

We believe SMB leaders deserve the solid comfort that comes from informed confidence. This is markedly difference from a happy-go-lucky approach.

You deserve to be able to address risk fearlessly. And the way to combat fear is with a balance of knowledge and action.

Cybersecurity confidence comes from being in control and knowing you're in control.

Risk: what you need to know, and how to get the info you need

Once you have the right cybersecurity tools in place, and the right person or people to manage them, you shouldn't need to invest much time in actively learning about risks. The tools will take care of that for you, backed by Threat Intelligence, analysis, and insights relevant to businesses like yours.

However, it's always good to have some awareness of any risks out there on the cyber horizon. After all, some of them will relate to human behavior (or error), and others to the devices your business runs on.

Do bear this in mind: if you find yourself up late at night scrolling through Threat Intelligence blogs instead of getting the R&R you need to be able to crush your business goals, then something's gone wrong. Either your cybersecurity tools aren't giving you the confidence your business deserves, or you've just tumbled into a vortex of endless tempting horrifying hyperlinks that won't help anyone.

Instead, try these resources for up-to-date information on cyber risks affecting your industry, sector or region.

- **ENISA** (European Union Agency for Cybersecurity)
- **NSC** (the UK's National Cybersecurity Centre)
- **CISA** (the US' Cybersecurity and Infrastructure Security Agency)
- **Kaspersky's blog** has a wealth of useful information on risk (and other areas) for SMBs
- **Forbes.com**
- **CSOonline.com**
- **Threatpost.com**

You should also check with your local industry body/ies to see if they offer information on any risks that businesses like yours should be aware of.

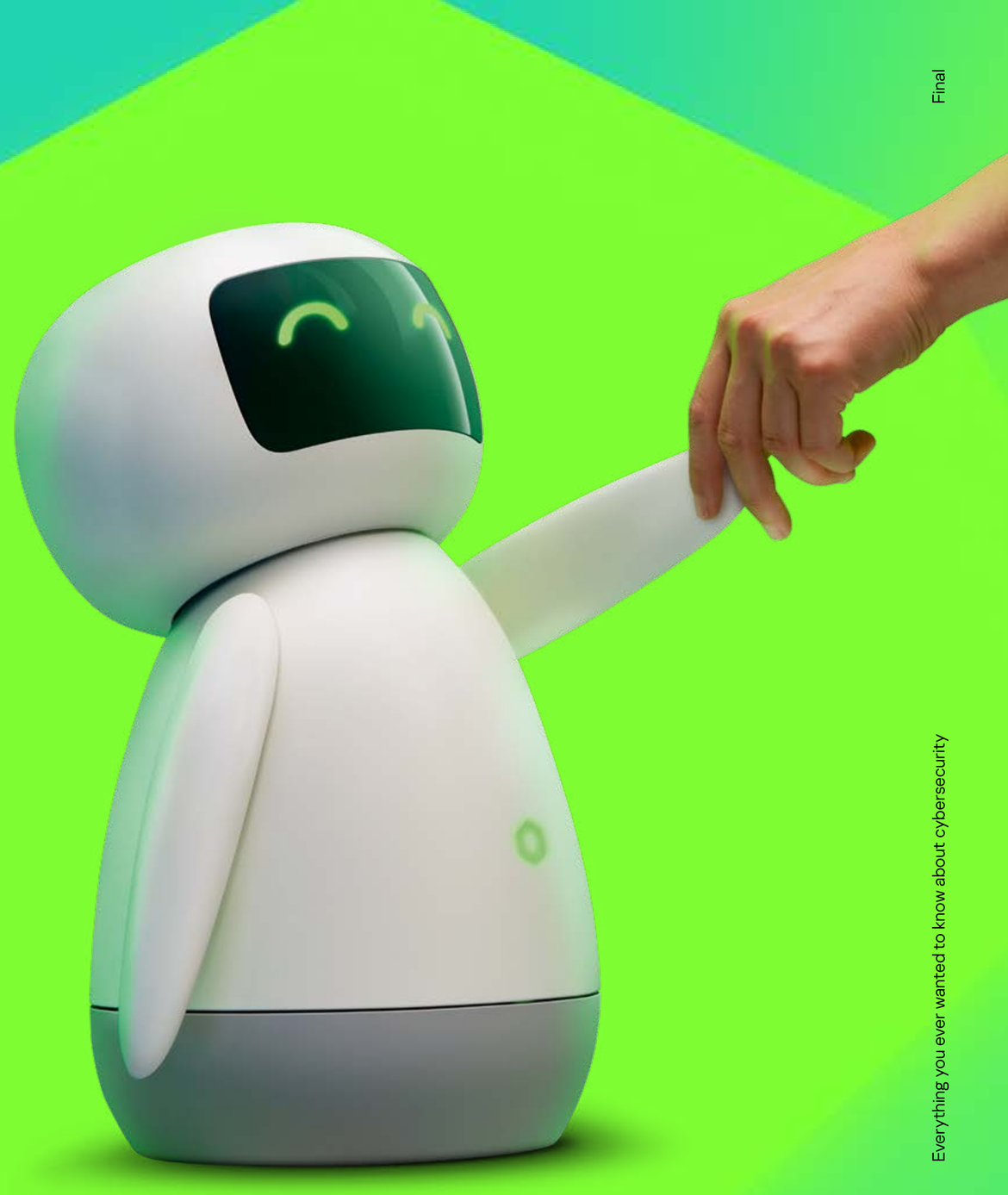
Just remember when you're reading up about cyber risks, try to focus on articles that are directly relevant to businesses like yours. Getting bogged down in irrelevant and potentially alarming details is stressful, not to mention time-consuming. The main point is to learn what you need to learn in order to build deep confidence that you are taking all the actions you need to take to protect your business.

A special note about legacy (or less common) devices

If your business relies on legacy devices, including less well-known networked devices developed for highly specialized tasks (this might include healthcare, facilities management or maintenance, for example), it's a good idea to check with the device manufacturer to see if there are any issues you need to be aware of, or any steps you can take to boost security (such as firmware or software updates).

Your relevant industry body could also be a source of information on legacy or highly specific connected devices, any associated risks and mitigation steps.

As always, the right cybersecurity vendor will also assist you in guaranteeing that your business can be protected across devices.

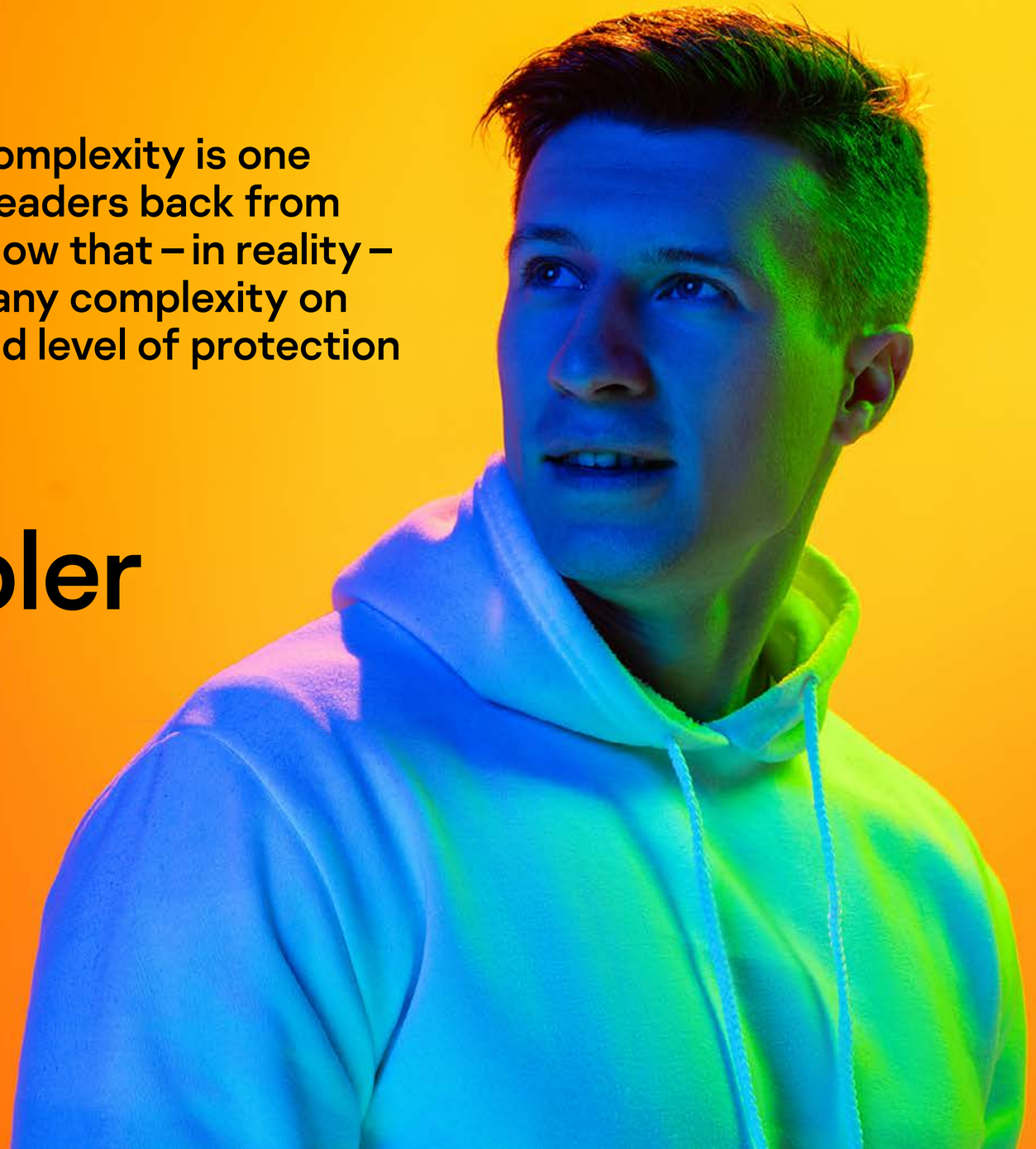


Chapter Five

A few notes on complexity

We've already looked at how the issue of complexity is one of the misconceptions that can hold SMB leaders back from decisively addressing cybersecurity. We know that – in reality – the right cybersecurity tools will deal with any complexity on your behalf, delivering a user experience and level of protection that could not be simpler.

"Things were simpler back then"



Nostalgia is big business these days, and it's not hard to understand why. The last couple of decades have completely changed the way we live and, while some things are more complex, many things are far easier today. Even Reader's Digest has resorted to publishing a list of 48 things that were way harder 'back in the day', in an attempt to correct rampant nostalgia for a past that never really was.

Nevertheless, complexity is a real issue when it comes to IT, and we're going to talk about why. This section is mostly about helping you build wider situational awareness about what complexity actually means for your business. We hope to leave you with a level of reassurance that can only come from understanding.

Cyberspace is complex by definition

Cyberspace itself is defined by ISO/IEC 27032:2012 as a “complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

Three layers of complexity

In protecting your business, you're dealing with three layers of complexity: cyberspace, your IT environment, and any cyber threats. These three layers interact with each other, resulting in layers of complexity. Let's break it down:

1 Cyberspace

An increasing reliance on interconnected devices, systems and processes, which support daily business and leisure life, leading to an increasingly complex business IT environment.

2 The business IT environment

The more interconnected devices, systems, and processes your business has, the larger (and more complex) the potential attack surface. In response, cybercriminals devise increasingly complex methods of attack, and your business must adopt cybersecurity tools that are fit to deal with that complexity.

3 The threat landscape and the actors within it

Cybercriminals have to adopt methods of greater complexity to launch attacks on increasingly complex environments. Going further, they also try to leverage that complexity, because they know that some businesses are still relying on cybersecurity tools from 'simpler' times; exposing vulnerabilities.

Finding simplicity in complexity

Even though your business is coming into contact with these interconnected layers of complexity, its position remains clear and simple—provided that you put certain measures in place.

Think of it this way: you may be a citizen of a sprawling metropolis (London, Tokyo, Nairobi—anywhere), but at no point are you called upon to delve deep into the complex systems, processes, hardware, technologies or institutions that keep it running.

In order to interact with the complex city you call home, all you need to do is follow the guidelines for each specific context.

You want to travel on the metro? Go ahead: buy a ticket and get on board. The system will take care of the rest.

You don't need to understand the workings of the trains, nor the mechanics of the contactless barriers, nor the ticket machines and their payment technologies. You can use a highly complex system without having to invest any time in understanding the complexity (unless that's a passion of yours!).

The same applies to cybersecurity, and to other IT technologies. You — and your business — are a part of a multi-layered complex system, there's no getting away from that.

The way you interface with complexity can be as easy as buying a metro ticket.

Chapter Six

WHY? The forensic psychology of cybercrime, and why it matters

Do you find it more motivating to defend yourself and your business against human adversaries rather than against amorphous or invisible groups? If so, you're definitely not alone, and this chapter is for you!

The psychology of crime matters: it's a crucial aspect of prevention, from the perspective of the judicial authorities, as well as from that of any potential victim.

There is something different in the aesthetic quality of cybercrime in this respect. It's not like a bank robbery; with human beings, and guns, suddenly right in front of you on a banal Saturday afternoon.

The cybercriminals themselves are so completely removed from their victims in a physical sense. For potential victims, it's almost as though the threat actors themselves only exist in the virtual realm. But the people behind cybercrime are human beings.

Fighting bad guys is easier when you can ‘see’ them

Thinking about the criminals themselves can really help motivate you to defend your business. The formulation below might sound a bit basic, but it’s worth thinking about which of the two approaches you find more motivating:

Bad guys

Somewhere out there, someone is trying to out-wit me and steal from or destroy my business and there’s no way I’m going to let them get away with it!

Bad stuff

There are some threats out there that could hurt my business, and that could be really damaging, so I’d better look into it and take some action.

There's a reason why movies consistently focus on 'bad guys' rather than 'bad stuff': the psychology of it is endlessly fascinating. The same type of fascination can be leveraged in your efforts to keep your business safe from cybercrime — by understanding that you are defending your business from actual bad guys who are intent on destruction.

The three hacker 'hats' — black, white, and gray

Many people divide hackers into three ‘hat’ categories, according to their activities:

Black hat hackers

These are the outright bad guys — causing harm, stealing, destroying, devastating, and even killing, for political and/or financial profit and enjoyment (which includes plain old-fashioned schadenfreude)

White hat hackers

These are the good guys, often known as ‘ethical hackers,’ who use their expertise to help make the world safer, with efforts such as penetration testing: using hacking techniques to test security.

Gray hat hackers

There’s obviously a huge amount of overlap between black hats and white hats (including high profile individuals such as Kevin Mitnick – more about him below). Gray hat hackers might use illegal or unethical means for ethical ends; bending the rules, in other words. Or they might ‘diversify’ their approach by carrying out legal and illegal hacking activities simultaneously. Perhaps, in many cases, the end goal is less important than the fact of having achieved that goal — of surmounting barriers that would confound the majority of people on this earth...

Another way of looking at cybercrime psychology is to consider the hackers' intentions:

Utopians

Utopian hackers believe that they're making the world a better place. However, their ideas of 'better' might not always coincide with everyone else's — least of all their victims. Utopians were identified all the way back in 1993 by Lawrence Young. Things have come a long way since then, with highly formalized (and respected) initiatives that reward Utopian hackers for contributing to cybersecurity. HackerOne is a great example of this — according to their website, over 600,000 'ethical hackers' have contributed to identifying security vulnerabilities, and are rewarded for their efforts with bug bounty programs, and similar. The interesting thing about utopians is that individuals and groups might combine ethical hacking with unethical and/or illegal hacking. After all it is the same inquisitive, persistent and ingenious mindset that drives hackers to learn, master, and ultimately outwit complex systems.

Cyberpunks

These are hackers who commit cybercrime for ideological and/or political reasons. The most famous group is Anonymous, but there are countless others. All share the desire to outwit, disrupt and overthrow selected businesses, institutions, industries, governments and even individuals.

Cyber-spies (or cyber-terrorists)

This category includes both lone-wolf actors as well as state-sponsored or group-sponsored actors, and even mercenaries. In some cases, cyber-terrorists don't really care who they attack — they just want to spread a wide net and see who they can catch. The victims' identity is less important than the sadistic joy of knowing systems that they have caused harm.

“Insatiable curiosity”

Kevin Mitnick’s path from black hat to white hat

Kevin Mitnick is a notorious former hacker who went from being on the FBI’s most wanted list to being a highly respected consultant to Fortune 500 companies and governments alike.

People like Kevin are very different from simple ‘snitches’ who escape prosecution by becoming police informants.

By switching hats from black to white, Kevin was able to continue using the exact same skills and passion for good as he did for bad.

In his own words, he has been driven by ‘an insatiable curiosity, a passion for seemingly impossible challenges and an unstoppable sense of humor.’

Mitnick’s case is a fascinating example of the type of mind that leads a person to engage in cybercrime.

Remembering that cybercriminals are human can help us look at cybersecurity in a more effective and grounded way.

Without this focus, cybercrime can sometimes seem unreal, or invisible. The motivating power of learning about the human element is worthwhile from a business perspective, but it's also extremely fascinating. There's also an exciting challenge within that fascination: how can I overcome these fiendish minds that are out to get me? Many people find that ruminating on the forensic psychology of cybercrime can help them take security more seriously, leading to greater resilience. But (of course) there are challenges.

According to experts, there's simply not enough research on the forensic psychology of cybercrime, and it's easy to understand why. Cybercrime is both highly complex and relatively new, and requires a multi-disciplinary approach, as the authors of the Palgrave Handbook of International Cybercrime and Cyber Deviance (2020) explain below:

Imagine a criminologist, computer scientist, engineer, information scientist, and philosopher coming together to talk about cybercrime. Each of them would have received intense academic training within their discipline. They would each have different definitions of crime, different views about the causes of crime, different perspectives about what the term "cyber" means, and different views about how to use the academic discourse to address, prevent, and respond to cybercrime. In many ways, they are trained to speak different languages. In the end, these different languages would result in differing definitions of cybercrime.

Chapter Seven

Eight types of cybercrime affecting SMBs

The old days of simple viruses and worms are far behind us. The spectrum of cybercrime is immense. These are the seven types of cybercrime that SMBs need to know about:

1 Phishing

Phishing is a sophisticated form of malicious attack, whereby cybercriminals create a fake version of a genuine website, email or sms — purporting to come from a genuine service; such as a bank or social network.

When the victim visits the fake site, the site will use social engineering methods in order to obtain valuable information from the victim. Phishing is often used for identity theft scams and to steal money from bank accounts and credit cards, as well as a way to gain entry to networks and devices.

Amazingly, phishing is still one of the top forms of 'initial access' methods, even for the most high-level state-sponsored Advanced Persistent Threats (APTs).

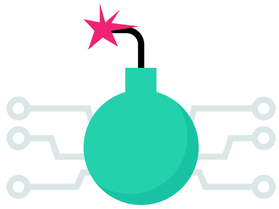
2 Ransomware

You're busy working away and suddenly your computer screen goes red; flashing up a ransom demand: pay us or you will lose your data!

Ransomware actors will either encrypt data that's on the computer hard drive — so the victim cannot access their data — or will totally block all access to the victim's computer.

Ransomware can be spread via phishing emails, or can occur if a user simply visits a website or uses a cloud service that contains a malicious program.

The problem is that criminals sometimes infiltrate legitimate sites and services to infect them with ransomware. The risks of picking up a ransomware infection are by no means limited to visits to suspicious websites.



3 DDoS (Distributed Denial of Service) attacks

Cybercriminals use Distributed Denial of Service (DDoS) Attacks in order to make a computer or network unavailable for its intended use.

The targets for these attacks can vary. However, a business's website is often the prime focus for an attack. There are many different forms of DDoS attack. In one example, cybercriminals will infect vast quantities of innocent users' computers and then use those 'infected hosts' to bombard the target business's website with a massive volume of useless traffic. This can overwhelm the computers/servers that run the victim business's website and cause the site to run slowly or crash altogether. With most businesses depending on their website to attract and interact with customers, anything that makes the site malfunction, run slowly or fail to let customers access it can be very damaging to the business.

4 Malware vs Viruses

This distinction is important to understand, particularly for SMBs – many of whom are stuck with outdated understandings of cyber risks that still center viruses (and therefore only adopt simply antivirus solutions).

This perception can be damaging and is highly risky. Most people are familiar with the types of computer viruses that can spread from computer to computer.

However, malware – which is short for malicious software – is the name given to a much wider range of hostile software. Malware includes computer viruses, worms, Trojan horses, ransomware, keyloggers, spyware and many other threats.

A software product that offers anti-malware capabilities will protect your computers and information from far more than viruses alone.

5 Backdoor Trojans

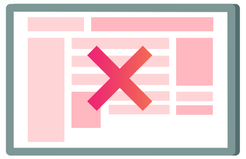
Cybercriminals use backdoors for remotely controlling machines that they have infected. Typically, compromised computers become part of a malicious network – known as a botnet – that can be used for a wide variety of cybercriminal purposes.

6 Keyloggers

Keyloggers are malicious programs that record the keys that you press on your computer keyboard.

Cybercriminals use keyloggers to capture confidential data; including passwords, bank account numbers and access codes, credit card details, and more. Keyloggers often leverage the technologies that are essential to the running of vital software and devices, such as Javascript, and they are freely available in open source forums such as GitHub.

These often work in conjunction with backdoor Trojans, as a way of obtaining and maintaining access to victims' devices and networks.



7 Firmware attacks

Firmware is a specific and normally permanent type of software that controls how hardware components work.

It's different from your operating system — e.g. if you're using Windows as your OS, you'll be used to receiving reminders to update it in order to get the latest bug fixes or other important updates.

Firmware has traditionally not benefited from regular updates, because it's been seen as low-level basic control software.

Unfortunately, for this very reason, cybercriminals are increasingly targeting outdated legacy firmware as a way of launching attacks. Firmware attacks can bypass your operating system, so it's important to build awareness of the risks, and take measures to prevent them.

8 Supply Chain attacks

Your business relies on devices, components and equipment from multiple suppliers, and each of those suppliers in turn is relying on its own chain of suppliers.

In a supply chain attack, criminals target just one component in a supply chain, with the goal of making that component carry the infection further up the chain until it reaches its target (or targets). It's a bit like genealogy in that sense — where a gene is carried through the generations.

As of early 2022, supply chain attacks are more likely to target enterprise-level organizations (and governments) than SMBs, but it's still important to bear in mind that cybersecurity is not only about 'locking your own door' — it's about being aware of the security of your vendors and suppliers (both offline and online).

Chapter Eight

Avoiding common mistakes

We've already covered some of the most important mistakes that SMBs need to avoid if they are to keep their businesses safe — these are the misconceptions we tackled in chapter two.

This chapter is short, but important.

Let's start with this stunning fact from industry analysts, Gartner, Inc.:

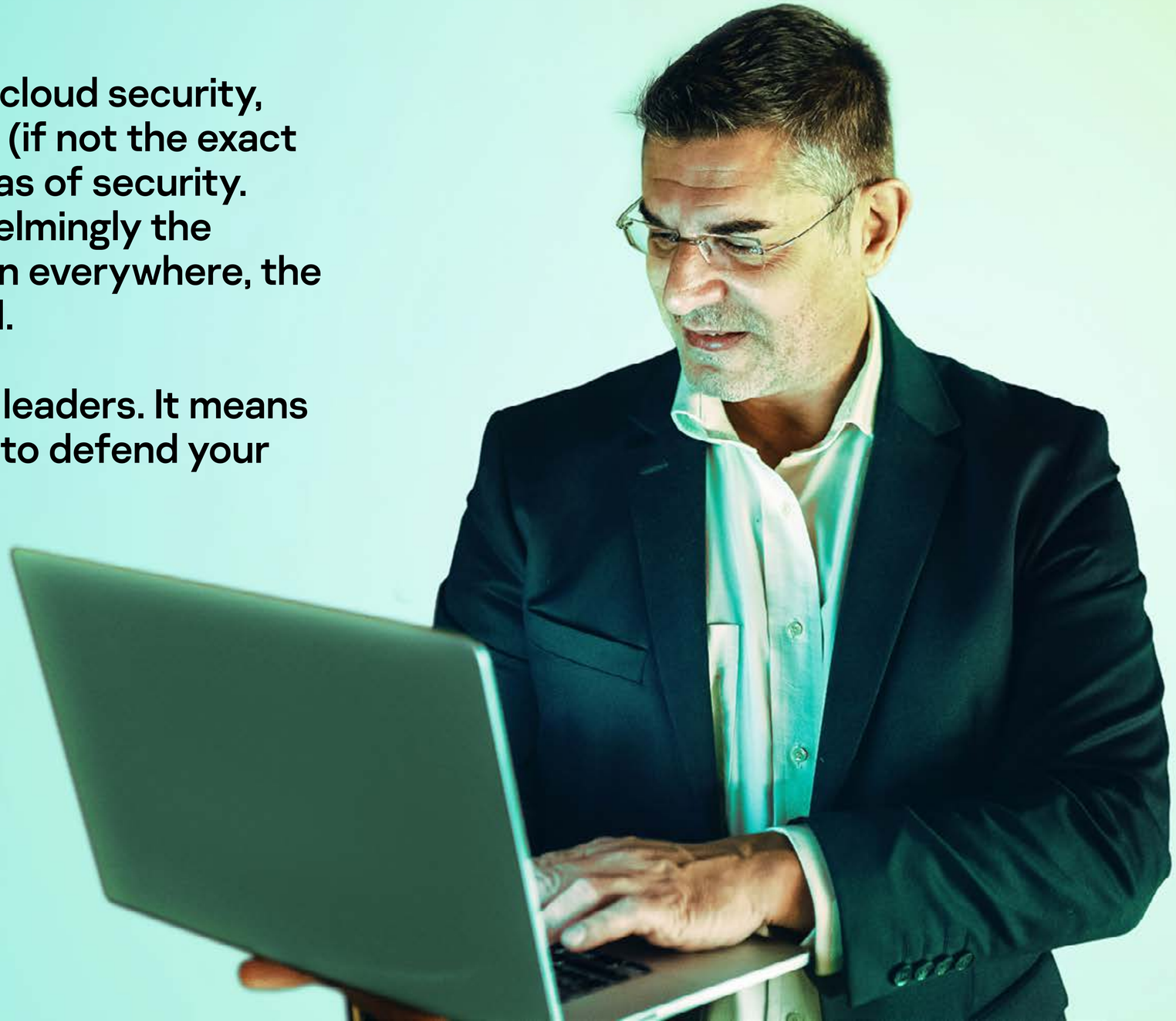
At least 95% of cloud security breaches will be caused by human error through 2023.

And now let's turn that stat on its head:

You can prevent 95% of cloud breaches by eliminating human error.

While this statistic focuses on cloud security, we can apply a similar principle (if not the exact same percentage) to other areas of security. And, any case, cloud is overwhelmingly the course of digital transformation everywhere, the principle is absolutely universal.

This is excellent news for SMB leaders. It means that it's well within your power to defend your business from cyberattacks.



You just have to take action.

Education, education, education

Right off the bat, we'll say that the reason we've invested so much into this cybersecurity guide for SMB leaders is because education stands at the center of everything we're trying to achieve in making the world a better place. So if you're reading this guide, you are already taking powerful steps to protect your business.

If you don't have much time to read, we urge you to pay special attention to chapters **two** and **three** (if you haven't already). You should also dedicate time to understanding and mitigating the risk of human error in the following areas:

Devices

Devices are now both so numerous, commonplace, and diverse, that the risks associated with them are often overlooked.

If your employees are using personal devices for work, the risk is even more critical.

What's more, if you're not aware that they are using their personal devices, the risks are even greater, because you won't be able to implement security measures, or to educate your staff accordingly.

Remote working

Simple human error can occur when employees are working over private/personal or public WiFi networks that lack the high level of security, visibility, and control that you apply to your corporate network.

Cloud service use – and Shadow IT

Your business likely relies on a wide range of cloud services; from social media to CRM or accounting solutions and (in most cases), making sure these are secure is more straightforward. However, the growing problem of 'Shadow IT' makes this trickier if you don't have the right security solutions. Shadow IT is when you're not aware of exactly which cloud services your employees are using. Sometimes individuals or teams might adopt a cloud service for business purposes, with purely good intentions in mind. After all, it's hard for businesses to compete without the use of these highly efficient solutions. However, if (like many businesses) you don't have total visibility and control over the exact services your employees are using, this can create enormous problems, because you won't be able to mitigate any risks. Compounding this is the fact that employees often use seemingly innocent cloud services (like social media) for personal reasons, on devices that they also use for work, or on personal devices connected to the corporate WiFi. Shadow IT is a key way for human error to creep in, leading to devastating cyber incidents.

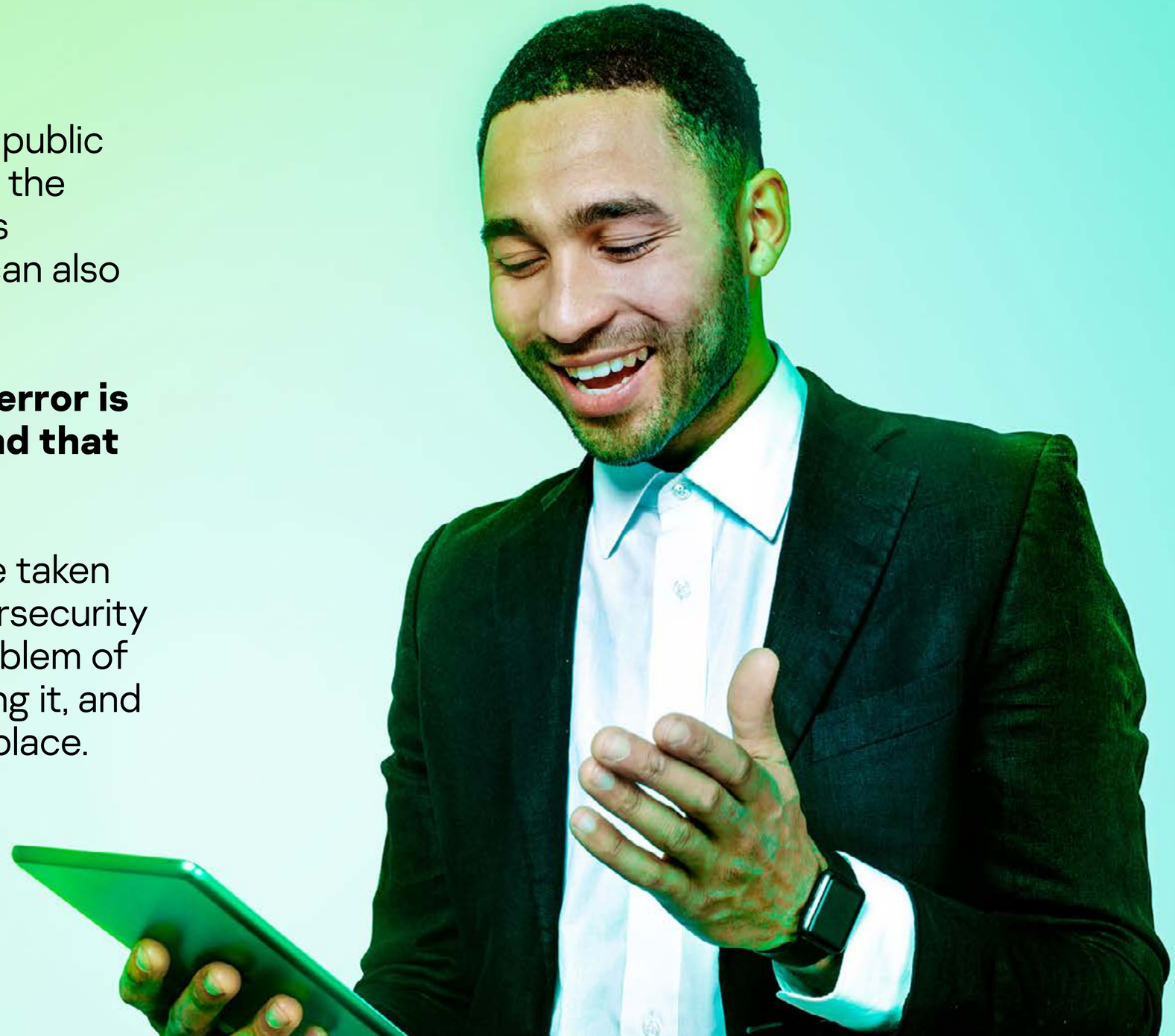
“We must accept that human error is inevitable — and design around that fact”

Cybersecurity is a bit like medicine, but more so. Estimates vary, but official bodies such as the Center for Disease Control in the US have said that some 40% of deaths from the top fatal diseases are preventable. If you’re interested, you can find statistics on avoidable deaths in the European Union here. Compare that 40% with the 95% projected by Gartner, Inc. above, and you’ll understand why we say ‘more so!’

Donald Berwick, the doctor and public health expert who served under the Obama administration made this important plea, which we think can also be applied to cybersecurity:

We must accept that human error is inevitable — and design around that fact.

This is the exact approach we've taken at Kaspersky, by designing cybersecurity solutions that recognize the problem of human error; spotting it, removing it, and making it impossible in the first place.



SMBs are in a better position than larger businesses

Because SMBs are still largely unaffected by the most devious, ingenious and cunning state-sponsored attacks (such as Advanced Persistent Threats), it means you're in a great position to be able to protect your business by using technology that removes the risk posed by human error. In the overwhelming number of cases, defending against cyberattack is well within your reach – provided you take education seriously, and adopt technologies like ours that deal with the problem of human error head-on.

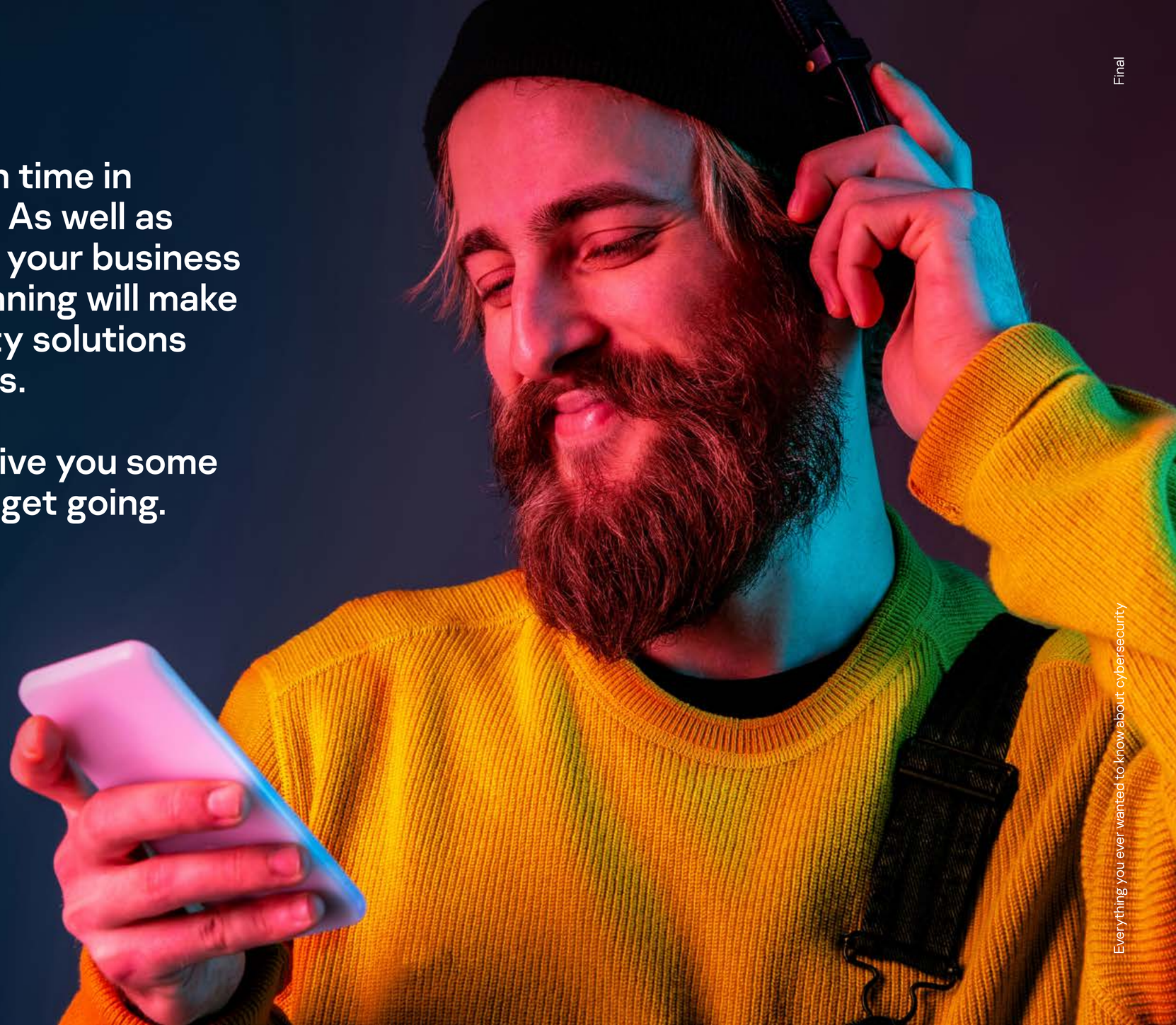
Chapter Nine

Plan for the worst, expect the best

You don’t have to invest too much time in planning, but you do have to plan. As well as helping you take steps to protect your business (such as education), the right planning will make sure you choose the cybersecurity solutions your business needs and deserves.

We’re going to jump right in and give you some action points that you can use to get going.

You can’t protect your business unless you know what the risks are, so here’s a simple and thorough risk assessment you can do right now.



We wrote this risk assessment expressly for SMBs, but it's adapted from the highly respected NIST Privacy Risk Assessment Methodology (PRAM), which is available on the open source platform, GitHub. Below each question we've written examples of answers that SMBs might give to these questions.

1 Why are security and privacy important to my business?

a. We can't afford downtime, we'd lose revenue

b. Our customers wouldn't trust us if we suffered a breach

c. If we lost access to our data, we wouldn't be able to operate

2 What regulations and standards affect my business?

a. Specific legal regulations for our region — we'll be fined if we fail to comply

b. Our sector has specific standards that must be met

c. Laws regarding the handling of financial information

d. Personal data on our employees

3 Which systems and products do we rely on?

a. Microsoft Office 365

b. Google Cloud

c. Social networks

4 Do our cybersecurity solutions protect the systems and products we rely on?

a. No, there's no specific protection for the cloud services we use

b. We've chosen a provider that protects the cloud services that hold our most sensitive data

Above all, it's important to think about cybersecurity as being about far more than protecting your business from viruses or malware.

It's about understanding the much broader value of remaining safe: protecting your reputation, maintaining trust, and avoiding regulatory penalties.

5 How are we controlling credentials and access privileges?

a. Everyone has more or less the same access to the corporate network or the files on it

b. We have cybersecurity that restricts access with specific rules to protect us

6 Which risks would cause the worst impact on our business?

a. Losing access to customer data

b. Damage to our reputation

c. Being fined for regulatory non-compliance

7 How is a lack of control putting us at risk?

a. We don't know which devices our employees are using (e.g. USBs or smartphones)

b. We can't see which websites our employees are visiting

c. We don't know which cloud services our employees are using

Planning will give you confidence that you can convey to your customers

The confidence that comes from knowing that you have put enough thought into protecting your business will have a ripple effect that goes far beyond cybersecurity.

You can use that confidence to power your communications with your customers and target market.

Running a successful business in an age of continuing digital transformation means that you are constantly asking your customers to entrust you with their data; both personal and financial. At the same time, customers are becoming more cynical towards 'hollow' promises about customer privacy respect.

When you communicate from a place of informed confidence that you have invested careful time and planning in defending your business and its customers, your trust rating and reputation will go up, having a positive impact on revenue.

Planning which cloud services to use

Sometimes it's hard to resist immediately and enthusiastically adopting new cloud services that promise to revolutionize your business. In an ideal world, all services would be safe, and you would be free to pick and choose as and when you need.

However, it's important not to lose track of the cloud services your business adopts.

Our Cloud Discovery (and Blocking) technology removes the uncertainty and risk from the equation by uncovering cloud service use, giving you easy risk ratings for each one, and making it easy to block any that might bring risk.

Chapter Ten

Time and Timing (and the difference between the two)

Time is limited, and timing is everything

Both are connected.

Let’s explain.

Time

Time is arguably your most precious asset; who wouldn't want an extra hour in the day? And, with so many competing priorities, it can be hard to accurately assess how much you should invest in each task. As we said earlier, there's a misconception that cybersecurity is time-consuming. The only thing that's really time-consuming is the work involved in repairing a cyber-attack. That's where timing comes in.

Timing

You have to lock the stable door before the horse bolts. As well as using your time effectively, you need to time your decisions effectively. In fact, the relationship between time and timing is even deeper. If you choose the right cybersecurity solutions early on in your journey, you won't end up wasting time either dealing with the results of attacks, or trying to fight them off using inadequate tools.

That said, it's never 'too late in the day' to implement a time-saving cybersecurity solution. You'll start to benefit as soon as you adopt cybersecurity that's designed specifically for SMBs, with your time pressures in mind.

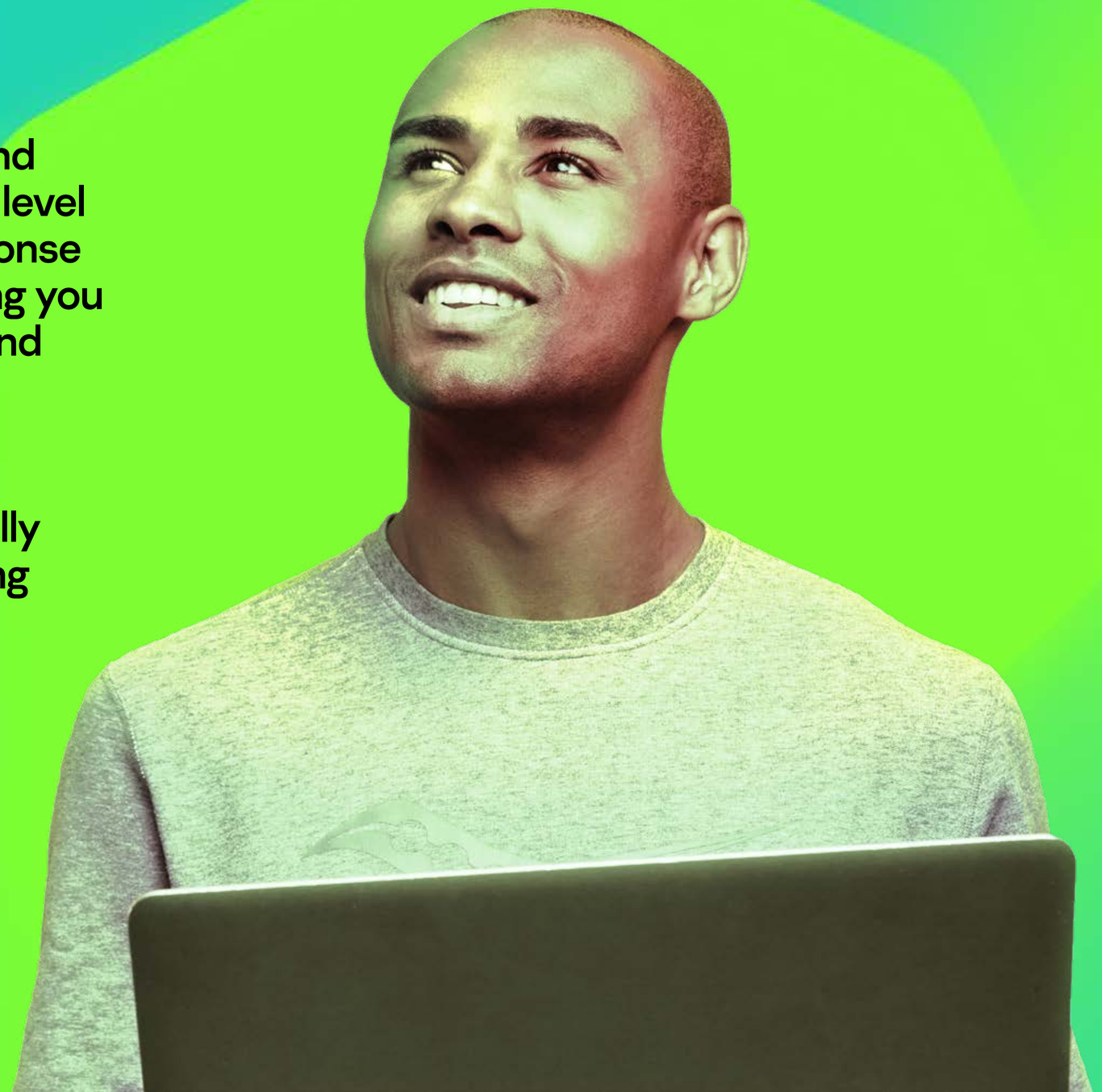
Our flagship SMB security solution can be managed in just 15 minutes a week from anywhere, and all you need is a web browser. Deployment is immediate, and in those 15 minutes a week, you'll be able to deal with every single one of the risks and challenges we've addressed in this guide.

With Kaspersky Endpoint Security Cloud, you can do all this in just 15 minutes a week:

- Uncover the cloud services your employees are using and block any that are risky
- Control which devices they're using to connect to the corporate network (including USBs, headphones, smartphones and more)
- Protect desktops and servers
- Secure geographically separated offices, home or field-based workers; at their desks, at home, or on the go - regardless of device type
- Control which websites your employees can access
- Protect your businesses from risks associated with using Microsoft Office 365
- Prevent ransomware and other exploits
- Control firewalls and network attack blockers
- Protect 2 mobile devices per user
- Encrypt employees' devices remotely so that corporate data is protected if a device is stolen
- Automate patching so that you always have the latest versions of all your applications

You can even access Endpoint Detection and Response (EDR) functionality that offers a level of incident visibility, investigation and response normally only offered to enterprises; helping you detect threats and reveal their full scope and origins.

It's tailored specifically to SMBs, removing much of the complexity that has traditionally prevented smaller operators from accessing the security they deserve.



Chapter Eleven

Choosing the right cybersecurity

Here's a straightforward checklist to help you identify the right cybersecurity solution

You can use it to assess Kaspersky products, as well as those of our competitors.

YES or NO

Essential questions: does this solution allow my business to...

- [ ] Uncover and control cloud service use?
- [ ] Control which devices my employees use?
- [ ] Control which websites my employees access?
- [ ] Offer crucial protection for file-sharing (e.g. SharePoint)?
- [ ] Manage cybersecurity simply and quickly?
- [ ] Allow me to manage cybersecurity from anywhere?
- [ ] Help me protect my customers' data?
- [ ] Help us comply with regulatory requirements?
- [ ] Make it easy to encrypt data in case devices are lost?
- [ ] Give me risk ratings for cloud services so that I know which to allow/block?
- [ ] Give me enhanced visibility and control (e.g. through EDR functionality)?
- [ ] Protect my employees wherever they are (e.g. remote working)

Lastly, there is a simple question you can ask to help assess the right cybersecurity vendor for you:

Has this vendor demonstrated sustained success in independent tests and ratings?

Don’t overlook this aspect. Hype about shiny new features can be very enticing, but it’s important to consider sustained performance when choosing a vendor – rather than looking at what might be ‘flashes in the pan.’ You don’t want to have to end up switching vendors because they’ve failed to address new and emerging risks or working realities. Cybersecurity shouldn’t occupy too much of your time as a small business leader. It needs to have a high level of set-and-forget capability, and this is only possible when you can rely on your vendor to keep supporting you well into the future.

It probably won’t surprise you to learn that Kaspersky is the most tested, most awarded security vendor, or that we’ve maintained a consistent top 3 ranking in aggregate scores from the security industry’s most respected, independent tests and reviews. You can read all about our sustained performance here.

Will this vendor support my business as it grows?

You don’t want to have to switch vendors simply because your business has grown. You deserve a vendor that is able to meet you right now where you are, as well as grow with you throughout your journey.

After all, even Amazon started in a garage; so there’s no knowing what tomorrow will bring.

Ask these questions to assess a vendor's capacity to support your growth:

YES or NO

Does this vendor...

- [ ] Offer elastic, user-based licensing?
- [ ] Offer different tiers of protection so that we get exactly what we need?
- [ ] Demonstrate deep expertise in enterprise solutions (1000+ employees)?
- [ ] Have a proven track record in identifying risks across business size? (e.g. research and analysis)
- [ ] Provide enhanced levels of control for security needs and expertise that develop as we grow?

Further sources of insights into cybersecurity solution performance

If you want to do more of your own research into the cybersecurity solutions you're considering, we recommend the following independent research and testing sources:

- SE Labs
- AV Comparatives
- AV Test

Chapter Twelve

Action stations: Yes, yes, yes!

If you're ready to get going, we're offering a free test drive of Kaspersky Endpoint Security Cloud, so that you can experience an easy-to-use solution that will solve every challenge we've addressed in this guide without draining your time (or budget).

We hope you've found this guide useful, and that you'll continue to return to it to help you build insights and confidence in getting the protection your business deserves.

Here's your pre-test-drive checklist — if you can answer yes to these three questions then you're ready:

1

Do you want to protect your business immediately without the need for training?

2

Do you have access to a web browser?

3

Can you spare 15 minutes a week to protect your business, its reputation, and your customers?

Yes, yes, yes?

Then what are you waiting for?

Try for free now