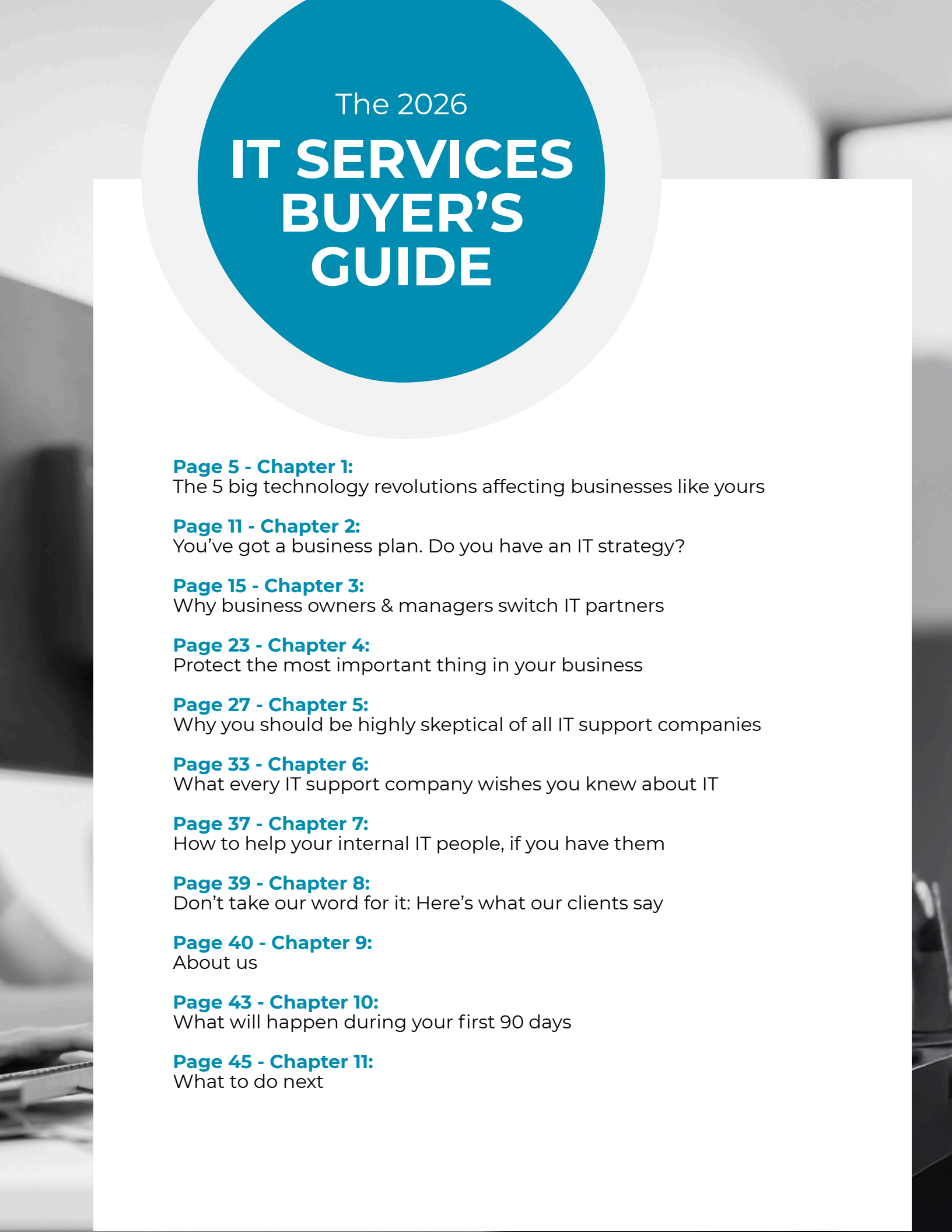
The 2026

CYBER SECURITY SERVICES BUYER'S GUIDE

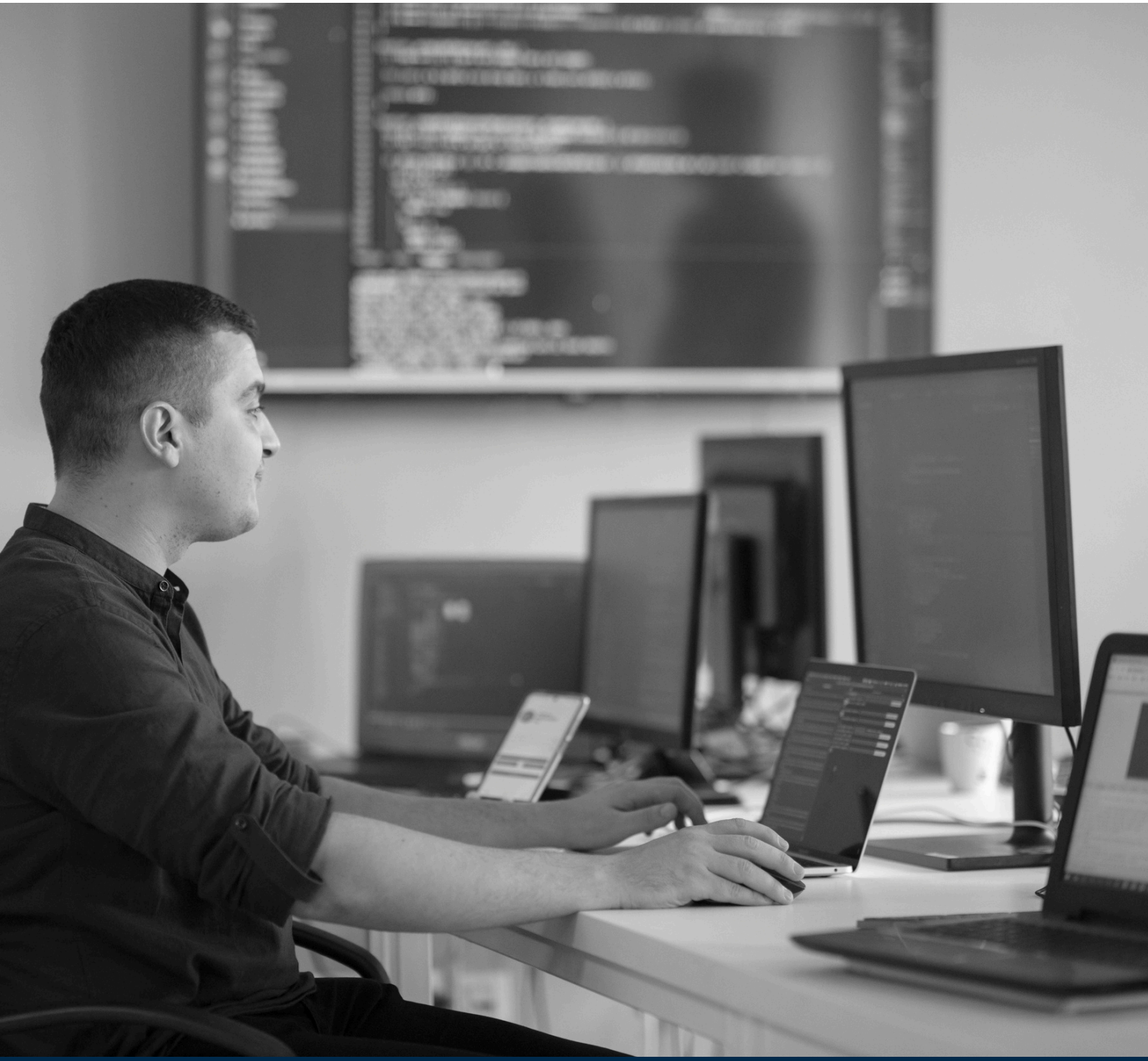
An easy-to-follow guide showing you how to pick a new cyber security services support partner.
Discover what to look for, what to beware of and the right questions to ask.

www.nsecurity.ca



The 2026

IT SERVICES BUYER'S GUIDE



Chapter 1:
The 5 big technology revolutions affecting businesses like yours

Hello, my name is Prathab Kanagasingham and I'm the owner of NCI.

Wow... what a crazy few years it's been for business owners and managers like you and me.

Whether you're doing well today or fighting for every bit of new business, you can't have missed the dramatic changes in the technology we all rely on.

I believe we're in the middle of a series of massive and interrelated technological revolutions. **There are 5 areas that I see are directly affecting the businesses my team and I look after:**

Revolution 1) AI

Go back a few years to late 2022. And to most people, AI was still a science fiction concept... something that would happen "in the future". Then ChatGPT was released to the public, and the AI race started.

AI tools have been in development for many years. But it's only been recently that many people have become aware of them – and have been able to directly access them through their browsers.

You're using Microsoft's Copilot, ChatGPT, or Google's Gemini, right? 90% of businesses now use AI tools.

Perhaps you use them for research, to find answers more easily, generate images or create documents?

Or maybe you rely on AI to summarize calls or pull meeting notes together. Many people are benefiting from AI built into the tools they use every day.

It's been an exciting start to this revolution. And just wait till the tools can figure out what needs to be done, then do it without being asked.

This is known as agentic AI. It's like giving a smart robot its own task list. It can decide what steps to take, then get jobs done without needing help.

How could that improve your business?

Revolution 2) Hybrid Working

The big shift back in 2020 accelerated something that was already gaining huge traction: People want the option to work from home or the office. Or Starbucks.

Technology makes it so easy to work from anywhere. You just need to be very aware of the security implications, and make sure your people can communicate well and be productive wherever they choose to work.

The tools for this are developing at an astonishing rate. So, it's always worth reviewing how your business communicates and collaborates.

Revolution 3) The Cloud

The idea of being able to work anywhere, any time, on any device, is so easy because of the cloud. Can you remember the bad old days when you couldn't access data unless you were in the office? Unthinkable now.

But as the data has been freed, so we must take greater care of it. The cloud both liberates us and puts us at a hugely increased risk of crime. More on that later.

Revolution 4) Internet of Things

The day your refrigerator was allowed to go online was surely the day you realized eventually EVERYTHING will be online. Experts predict there'll be 30 billion devices online by 2030.

Great for helping us check how many eggs we have left while we're at the store. But there are huge security implications too, which affect any business that allows devices to be connected to its network.

Revolution 5) The greatest security risk ever known

This is the revolution that weaves through all the other revolutions... because any time there is change, it creates an opportunity for cybercriminals. And change is constant right now.

I've never seen as many threats to normal businesses like yours as I see today. It's increasing year after year. If you saw everything I saw, you'd be forgiven for not sleeping well at night.

I'm not exaggerating. Cybercriminals are getting smarter. They're using automated tools to target all businesses, all the time. It really does only take one person to click one bad link in a fake email, and you've unwittingly let them in to your entire business. You won't even know they're there until they strike, often weeks later.

There is a very clear and solid security 'best practice' that you should make sure everyone in your team sticks to. And I'm constantly assessing new cybersecurity tools to keep my clients safe. I'd be happy to talk these through with you.

Things are changing at such a pace, it's too easy to feel you are falling behind. Even as technology experts, my team and I work hard to stay on top of everything that's happening.

Let me make it easy for you with a simple technology strategy I believe you should focus on: **Defend and Invest.**

Defend is about protecting your business from cyber criminals

Invest is about making sure technology is powering your business forward, not holding it back

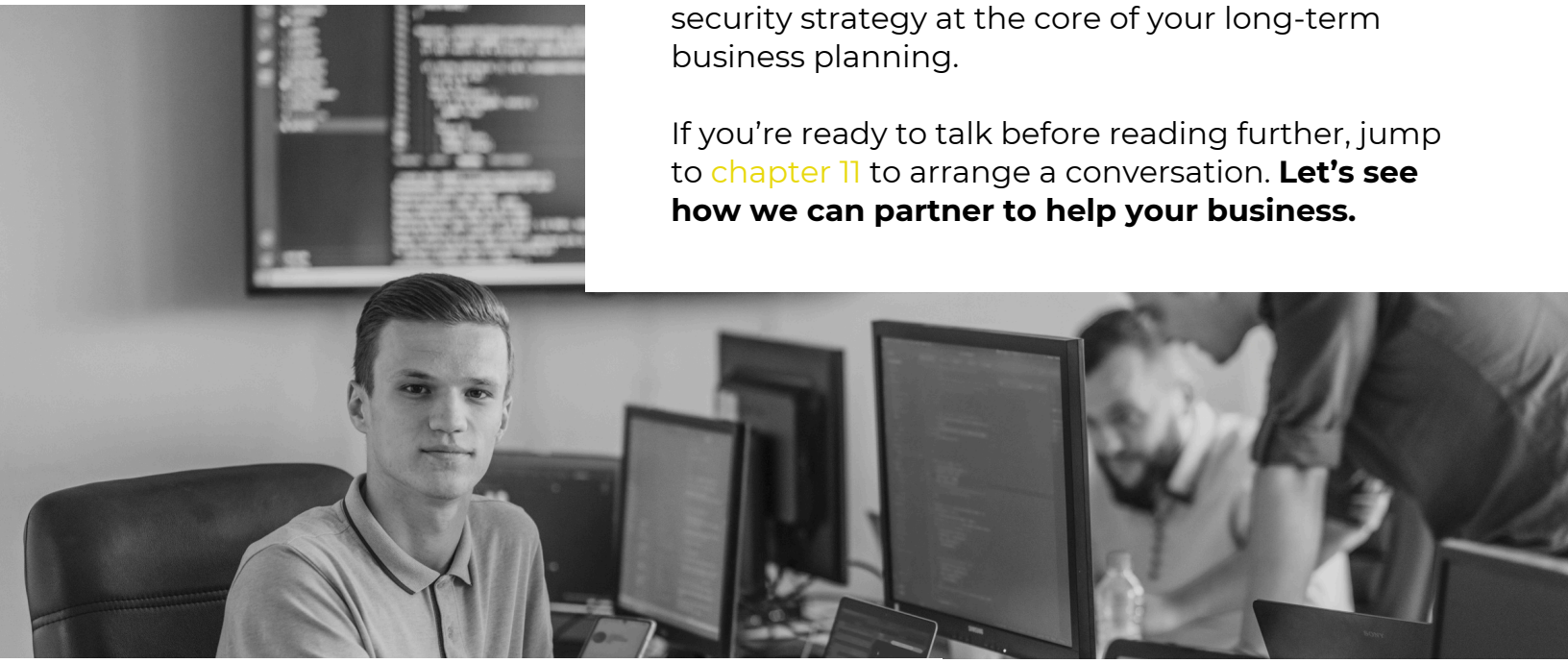
I suspect you're reading this guide because you're not 100% happy with your current cyber security support company and are thinking of changing.

Of course, I'd like you to switch to us!

I've written this guide to help you understand how a trusted cybersecurity support partner behaves, and what great cybersecurity support looks like.

I'll explain why we genuinely partner with our clients and refuse to become just a supplier. I'll also explain why it's critical you put your cyber security strategy at the core of your long-term business planning.

If you're ready to talk before reading further, jump to chapter 11 to arrange a conversation. **Let's see how we can partner to help your business.**



Prathab Kanagasingham
Director of Cyber Security Services
prathabk@nsecurity.ca
1 800 826 8102

Chapter 2:
You've got a business plan.
Do you have a cybersecurity strategy?

When did you last update your cybersecurity strategy?

If you don't have one, or you haven't given it much thought over the last few years, now's the time to develop one.

If you use any technology in your business – whether that's something as simple as a cash register, or it's a full-blown network for 5 locations – a proper cybersecurity strategy will be your best friend. It's the foundation for growing your business. It can mean the difference between surviving a period of uncertainty and thriving through it.

OK, I'm biased! But I cannot stress enough how important a well thought out cybersecurity strategy is for any successful business. Your cybersecurity strategy should work alongside your business plan, detailing the ways your technology will accelerate progress towards your goals and objectives. It should consider both long and short term targets and leave room for change where necessary.

And while it's called an cybersecurity strategy, it's not actually about your technology. Sure, you'll have plans for the technology and devices that you use, and those you want to use in future. But really, the strategy is about your business, and how your technology can help you to achieve everything you'd like to, in the easiest possible way.

A great starting point is to look at your current cybersecurity policy.

- What works well?
- What would you like to improve?
- As your business grows, will your technology grow with you, or will you need to look at new ways to address cybersecurity?

Speak to your people. What do they think works well, and what would they change if they could? Are there parts of your infrastructure that hold them back? Could you save time if you switched over to different software, or if one application could communicate with another one?

When you partner with a proactive cybersecurity services provider, they help you identify the right technology stack for your environment. They make tailored recommendations based on how your organization operates today—and how you plan to operate in the future. They can also uncover potential gaps you may not have noticed and propose more efficient, secure ways of doing things.

A cybersecurity roadmap as part of your strategy will help you to budget better and know what you'll need to invest in, and when. It'll stop surprise costs and random invoices you weren't expecting.

It can seem complicated to do this yourself. But if you're working with an cybersecurity services partner, this is something they should be involved with.

Now, more than ever, every spend needs to be justified. Every investment needs to work hard for your business. You want value for money from everything you do.

Create a range of metrics to help you track how well your infrastructure is working for you. Your team might like the way a certain system works. But if you're not getting a return on your investment then it's not working as well as you might think.

Your cybersecurity services partner should also get involved with regular strategic reviews. It's up to you how often you do these, but I would recommend every 6 months. You should look at what's going well and what's taking longer than you'd like it to.

And this is why I keep talking about an cybersecurity services partner. Not an cybersecurity services company. Not an cybersecurity services provider. **A partner.**

Imagine an office building. It has a janitor who comes in every evening and cleans up the mess that people make.

That's how lots of cybersecurity services companies work. They just clean up the mess.

We prefer to work as a facilities manager. This person is constantly thinking and planning. They schedule what maintenance the building needs. They look at what they can proactively do to stop it falling into any level of disrepair.

Yes, there's still an element of managing the janitors and making sure they've done their job. But a facilities manager is proactive enough to stop most of the problems happening in the first place.

That's what an cybersecurity services partner does. We take a proactive approach. We do as much as we can in the background to stop things from going wrong in the first place.

Of course, some things will still go wrong. Unfortunately, that's inevitable when it comes to fast moving technology and data. But that's when the clean-up work happens, and things get fixed. All the proactive work means that we need to clean up a lot less than an cybersecurity services company which doesn't work proactively.

What my team and I like to do for our clients is to be a partner in securing the future of your business. It means that both you and I know exactly:

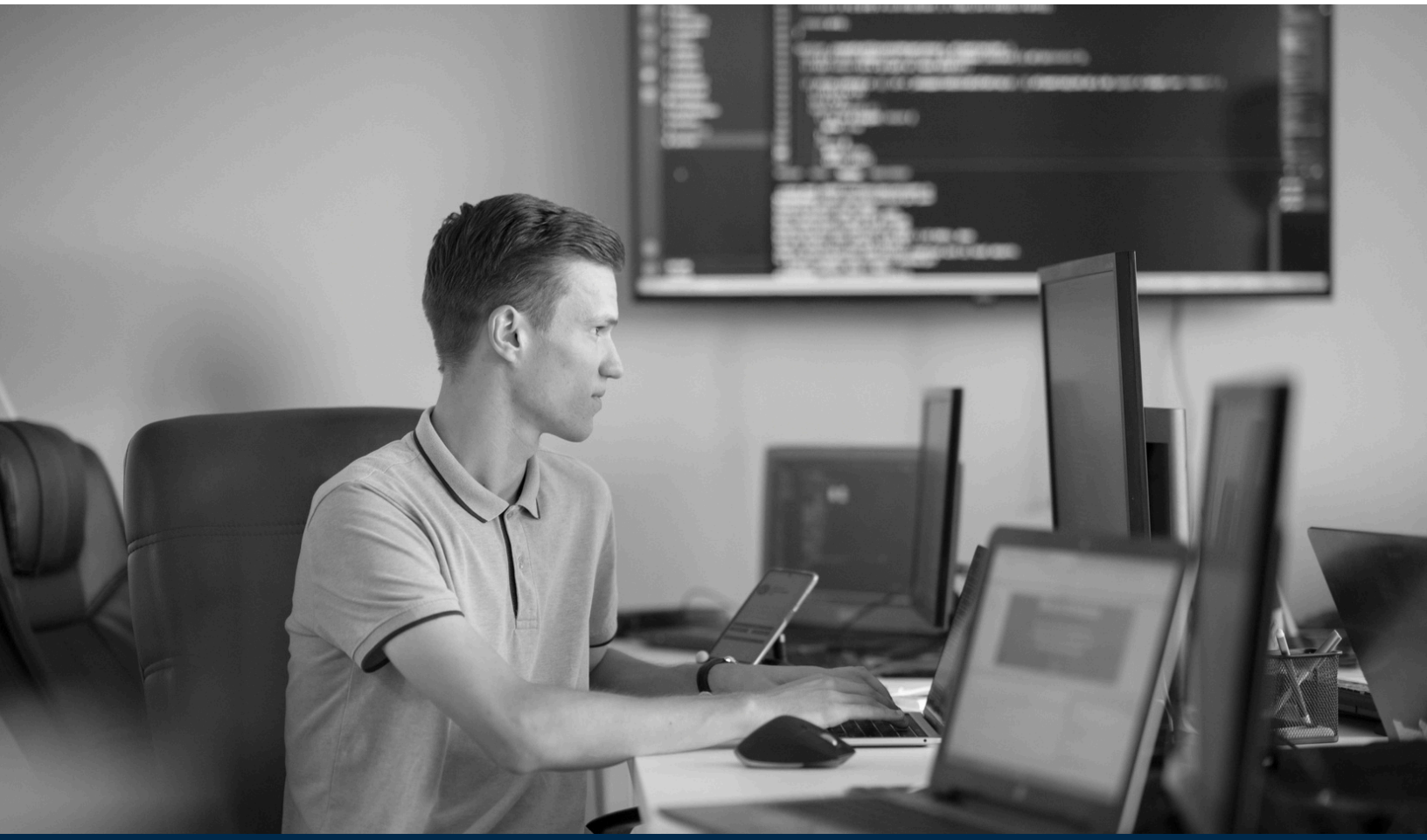
- What will be happening over the next 2 to 3 years
- What cybersecurity investments you need to make

And there are no surprises. It's all planned with regular strategic reviews to help us both move in the right direction.

This roadmap also allows us to see what can be delayed (if there's a problem), what investments are critical and, if you're ahead financially, what can be brought forward.

In large part, it's our partnership that allows this in-depth planning to take place. We get to know your business as if it's our own. We're constantly working with you on your business and learning about you and your team.

This commitment makes it easy for my team and I to help you because we know (just as well as you do) where your business is going.



Chapter 3:
Why business owners & managers switch cybersecurity partners

I hear from a lot of businesses who are unhappy with their current cybersecurity services provider.

These are the top 10 reasons people want to make the switch to a new and improved cybersecurity support partner:

#1

Reason to switch 1) You're not seeing business results

Return on investment is everything. Especially right now. You need to be able to see immediately exactly how hard your cybersecurity partner is working for you, and what benefit that work is bringing to your business.

A cybersecurity support partner should not only provide a detailed cybersecurity strategy for the long and short term, but they should also give you a set of metrics which you can measure results by.

And these metrics should be relevant and important to your business. Not a standard set issued by the cybersecurity support partner, not made difficult with jargon. I've heard too many stories of cybersecurity companies providing vague metrics that are impossible to decipher. Avoid!

#2

Reason to switch 2) Poor communication

This can cover a whole range of issues... from taking too long for them to acknowledge problems... to them not following proper escalation procedures... or not getting back to you when they say they will...

If we were talking about any other kind of supplier, these gripes might seem petty. But as we know, without working technology, your business can't run as it's supposed to, and these little gripes become huge issues.

Again, this is another way for you to distinguish an cybersecurity support provider from an cybersecurity support partner.

You need a responsive cybersecurity support partner who:

- **Acknowledges issues in good time**
- **Keeps you in the loop of everything you need to know, and**
- **Does what they say they'll do, when they say they'll do it**

Just as your success is their success, your failure is their failure. So, the faster an issue can be resolved, the better it is for both parties.

#3

Reason to switch 3) They don't take data security seriously

Yes, you read that correctly.

There are some cybersecurity services providers – whose job is to keep your data safe and secure – that don't do the same thing within their own business.

They don't make it a priority to keep themselves educated on the latest scams and threats. They can't keep you fully protected.

And they won't go out of their way to ensure every part of your data is as safe as it can be. Or that your software is 100% up to date all the time.

I know... this scares me too...

Is this really a company you'd want to be responsible for keeping your business safe from the growing number of attacks and data breaches?

#4

Reason to switch 4) They won't go outside of their contract

"Sorry, we don't cover that."

Ever heard that from your cybersecurity services provider? Lots of businesses have. But so long as the request relates to your technology, it should be a red flag.

"We don't cover that" suggests a real lack of concern for your business, and that's not how a partner behaves.

A partner actively spends time looking at new ways to improve your network, your data security and your infrastructure. They won't be working rigidly to a one-size fits all contract.

And that's the point. One size doesn't fit all, because every business is unique. Even two businesses in the same street, selling the same product or service will have a different way of working. They'll use different software and devices, have different people working with them and, importantly, have different goals.

You need an cybersecurity services partner who will take your goals as their own and do as much as they can to help you reach them.

#5

Reason to switch 5) Things take too long to fix

Some problems can't always be fixed immediately. Now and then issues take a while to get to the bottom of. Other problems are rare and may demand more diagnostic work.

But in these situations, good communication is key.
It might take you a while to see a resolution. But if your cybersecurity services partner is keeping you updated at each step, you're confident it's in hand.

Whereas if your support request is still waiting for a response three days later... you've got a problem.

And what if some issues never get fixed at all? Or that one thing gets fixed only to break something else?

This is technology we're talking about. It goes wrong. It doesn't always work the way we want it to.

But you absolutely should not be facing issue after issue, waiting days to have problems resolved. You should not face silence when you need help.

All that waiting means downtime for your business. Where's the value for money in that?

#6

Reason to switch 6) They never accept responsibility

When you take on an cybersecurity services partner, it's vital that both businesses take responsibility for their side of the agreement.

Failing to do so causes a huge lack of trust. And means the relationship is going nowhere.

I've heard from business owners who have reported an issue to their cybersecurity services provider, only to be told that it's their fault that the issue arose!

(despite them following advice and instruction from that company)

I've also heard from business owners who reported issues to their cybersecurity services provider, only to be told that they need to contact someone else (such as a software supplier) about the problem.

The idea of an cybersecurity services partner is that you trust them to deal with their area of expertise, while you get on with yours. If they're passing the buck when you face a problem, you're not getting the benefit of a support partner at all.

#7

Reason to switch 7) They confuse you with tech talk

If technology wasn't complicated, everyone would be able to take care of their own business infrastructure without a problem.

However, the truth is quite the opposite. It's full of strange words and concepts, and everything changes every 7 minutes! (it seems that way anyway).

It's a minefield if you don't know what you're doing.

The hallmark of a good cybersecurity services partner is that they take this complication and make it look easy. Better still, they make it sound easy. They explain things to you without sounding like they're speaking a foreign language.

Again, it all comes down to your connection as partners. If you can't communicate properly with each other, how fruitful is this relationship really going to be? The likelihood is that it'll leave both sides frustrated, and your business won't be able to make the most of the technology it has.

#8

Reason to switch 8) You're not learning

We're not expecting your cybersecurity services partner to teach you their job. You don't need to be an expert in cybersecurity – that's what you're paying someone else for. However, there should be an element of learning when you partner with an cybersecurity services company.

For example, you need to learn about cybersecurity, how to avoid scams, and how to protect your data.

If you're told "let us worry about that", it should ring alarm bells. You can't expect to keep your organization safe from a data breach or data theft if you don't know what you're trying to protect yourself from.

It's also important that your cybersecurity services partner explains what they're doing. You want to have a basic understanding of how your infrastructure works or is set up for you. This will help you to help yourself when a minor issue occurs.

#9

Reason to switch 9) They're always pushing new hardware

Some of our clients complain that their previous cybersecurity services providers spent more time pushing new equipment than they did on the fundamentals.

Of course, last year was a big upgrade year with Windows 10 reaching end of life.

And it's nice to have the very latest technology in your business. But it's certainly not vital. There are lots of other things to consider before upgrading equipment and devices. Especially today when you expect value for money and a return on investment.

Yes, your business will need a certain level of equipment for you to operate the way you need to, but you probably already have most of the technology you need. I find that for most businesses, it's far more important to get the infrastructure right before we consider your hardware. Additional devices, for example, are sometimes nice to have rather than crucial.

A good cybersecurity services partner will help you create an cybersecurity strategy, which should detail when in the years ahead you need to plan for protecting your business.

#10

Reason to switch 10) You've outgrown them

This last one isn't necessarily a bad reason to switch cybersecurity services partners. Sometimes, your business just grows too big for a smaller cybersecurity services company to deal with.

That's great news for you. The difficult part can be knowing when to make the switch. Especially when you're working with a company that you like.

It's worth keeping in mind that if:

- **If your support requests aren't being responded to as quickly as you need them to be**
- **Or the recommendations on how best to use technology to grow your business have stopped**
- **Or you need a higher level of support**

... it's in your best interest to find a new cybersecurity services partner.

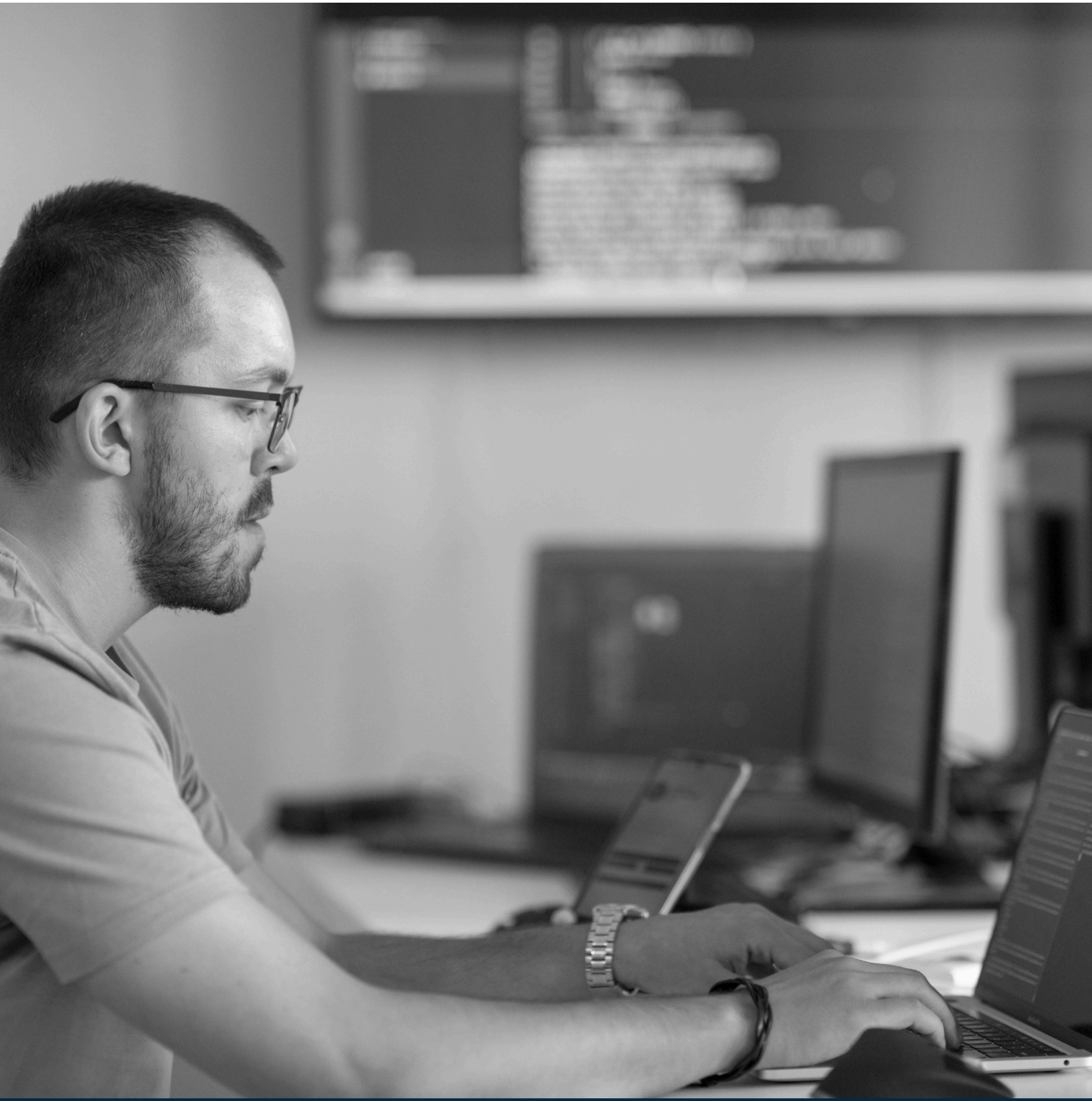
If you've noticed you need more support, your cybersecurity services partner has probably noticed too. In fact, if they're good partners, they may even discuss this with you first. Trust me when I say there'll be no hard feelings. No company wants to be out of its depth with clients.

If you've ever felt any of these issues, maybe now is the right time for you to make the switch too?

When you place your technology at the heart of your business growth strategy, you see why it's important to have a partner you can trust.

No business is perfect. Inevitably we get some things wrong for our clients some of the time, because we're human too.

But because my team and I have partnerships with our clients, we're able to have adult conversations and change course quickly. We don't have to spend unnecessary time repairing relationships. Instead, we can set the correct expectations and resolve issues quickly.



Chapter 4:
Protect the most important thing in your business

As we've seen over the past few years, being able to work anywhere, any time, on any device is liberating.

Working flexibly like this means that businesses can reduce their costs, attract the best candidates for jobs and have a happier workforce too.

But as our devices get smarter and more powerful, they're also becoming more disposable. You can do most things on your phone now, right? And how often do we lose or break them?

The thing is, because everything is stored safely in the cloud (the huge servers where you store your data in multiple locations across the globe), if you lose your phone, it's no big deal. You simply get a new one and restore your files from your backup. Just like magic, you have a new handset that contains all the data your old one had.

A lost phone is now merely a minor inconvenience and a small financial cost. And it's not just phones this applies to; your tablet and laptop work the same way.

This flexibility is amazing. However, it also has its risks; number one being that any time you take your device away from the office, you're potentially opening your data to anybody. The sad and scary truth is that there are many cybercriminals who are trying very, very hard to access your data. And even take it away from you.

You've probably heard about malware before. Malware, or malicious software, is code placed on a device or network with the aim of infecting, stealing, or corrupting your data.

Essentially, a hacker can create malware to do exactly what they want, once it's within your network. Once it's there, it can take you some time to notice what's happened. And it can be very difficult to remove.

But there's something scarier: Ransomware. This is the fastest growing cybercrime right now. And if you're not taking all the right precautions, it's likely that you'll fall victim to this devastating form of cyberattack at some point.

As the name suggests, ransomware is a kind of malicious software that encrypts your data so you can't access it. The hackers then hold you to ransom - to regain access you must pay a fee.

For example, they might ask for $10,000 – in cryptocurrency, of course – within 3 days. If you fail to pay, this fee doubles. If a week goes by, you can kiss your data goodbye forever.

Ransomware is terrifying. Trust me when I say you want to avoid this at all costs.

And while absolutely anyone can become a victim of ransomware, it's usually small and medium sized businesses that are targeted. Cybercriminals know this is a group that typically doesn't spend enough time or money on cybersecurity.

I don't want to bore (or scare) you with statistics, but it's estimated that up to two thirds of all businesses have been attacked with ransomware. That figure is rising every year.

The most common way for ransomware to get on your device or network is by someone clicking a link in a suspicious email.

And before your jaw drops that someone – especially someone in your own business – would be naive enough to click a link in a scam email, you need to know how sophisticated these emails are nowadays. AI has changed the game for scammers, too.

These emails will look just like genuine emails from someone you know or expect messages from – the IRS, your bank, even a department within your own company. And they not only look like the real deal, but the email address may be a close copy too.

These emails work because they ask you to do something relatively simple; click to update your details, for example. Even looking with a suspicious eye, it can be hard to spot that something is wrong.

Once that ransomware is installed, there's not always an immediate attack. In fact, it can take between 60 to 100 days for anything to happen; sometimes even longer. That's for several reasons.

Firstly, the longer a hacker lurks within your network, the harder it is for you to detect them. Usually, hackers enter through one device that's connected to a network. Then they investigate your network for other weaknesses. Better for them to have control over as many devices as they can. This can make it virtually impossible to kick them out once the attack has started.

That's what makes ransomware so difficult to deal with. And it's why prevention is always better than cure.

You need to be aware of the signs of a hacker in your network. Both you and your cybersecurity services partner should look out for:

- Unexpected new administrators appearing on your network
- Software being disabled
- New software being downloaded
- Remote access sessions lasting for days at a time

A great cybersecurity services partner will always recommend everyone in your business has regular cybersecurity training. After all, your people are your first line of defense from cyberattack. Software alone won't offer a good level of protection. You need software and humans.

It's important to understand this: You can never be 100% protected from malware, ransomware, and other forms of attack. That's impossible, because it's a non-stop game where the criminals are always inventing something new, and the data security world must catch up.

It is possible to be 99.99% protected, but you may be surprised to learn that we don't always agree with going that far.

You see, when you lock down **everything** to make your data security watertight, you can accidentally frustrate and annoy your staff. They'll have lots of extra layers of protection to go through, more steps in an already busy workload. And more to remember.

What that means in the real world is that they'll skip steps and look for ways to bypass security. Which puts your business at greater risk. Think of it like a door to an office. If you have seven big locks and a biometric scan just to open it, eventually people will get frustrated and just prop the door open!

To remove the frustration and hassle, we use what's called "blended security". We combine several products and services, which work together to protect you. It means fewer codes and passwords for your people, and a better level of security for your data.

And the clever part is that every blend will be different, depending on the business it's for. That way we can customize security perfectly for each client, based on their specific requirements.

Chapter 5:
Why you should be highly skeptical of all cybersecurity services companies

You probably don't know what you don't know about cybersecurity services.

Does that make sense? I think that's a fair assumption for me to make.

And why should you concern yourself with the latest tech news, software, and support updates? You're too busy doing what you do best.

You probably read your industry magazines, blogs, visit trade shows, go to conferences, and attend training... you're an expert in your field. That's what experts do. You certainly don't have the time to do all of that for your IT as well.

Would you expect your clients to know as much about your area of expertise as you do? Of course not. That's why they hire you, right?

The same goes for us.

We totally absorb ourselves in the highly technical, high speed, rapidly changing world of technology. We genuinely love it and pride ourselves on having a level of expertise that most people don't.

You'd be shocked how many people consider themselves cybersecurity experts, simply because they know their way around computers. However, great cybersecurity services partners operate on a completely different level – with better knowledge, tools, and systems.

Ask them: *"How quickly will problems be fixed?"*

Obviously, this will depend on the scale of the problem, but you need to know time frames based on severity. How long will it take your proposed cybersecurity services partner to acknowledge your issue in the first place? How long do they expect it'll take to get someone working on the problem?

Look at different scenarios. If you can't access your software, how long should it take to get you logged in? How long could it take to get your business up and running if you suffer a ransomware attack?

You also need to understand the approach your potential new partner will take.

Do they have processes and procedures they stick to when issues arise, or are they winging it? Can they tell you about the worst problem they've encountered and how they dealt with it?

Remember, it's not the problem that you're judging them on, but how they responded to it. This can tell you a lot about their professionalism, knowledge, and ability to remain calm in a crisis.

Ask them: *"What do you do proactively, to make sure my team has fewer interruptions?"*

Downtime is a business killer.

You'll have seen it for yourself at some point, either in your own business or one you were working for. The internet goes down, for example, and people can't access the software they need to do their jobs.

The office descends into chaos. Even those who aren't reliant on the internet stop doing what they're doing. The coffee machine goes into overdrive. Everyone forgets about their job for a while and makes the most of an unofficial break.

The biggest problem with cybersecurity services is that it's an unregulated industry. There's no governing body that people must pass through to be allowed to call themselves a cybersecurity services company. No industry standard that must be met. No guidelines on how the business must operate.

Just about anybody ...*literally anybody*... can set themselves up and say they're a cybersecurity services company.

This is why I say you should be highly skeptical of all cybersecurity services companies.

Without asking the right questions, you don't know if you're putting your trust – and the security of your business data – in the hands of a reputable, honest company... or someone working alone out of a bedroom in their parents' house. A bedroom warrior as I like to call those guys.

Now don't get me wrong, there's nothing wrong with bedroom warriors. Everyone must start somewhere, and if you're a one-man band with minimal IT requirements, that could be the most cost-effective solution for you.

However, if you own or manage an established, growing business, with staff and more than one computer, you'll need more than one person working from their bedroom can provide.

So how do you avoid choosing the wrong cybersecurity services company?

Firstly, look for solidity. You need to check they have the right qualifications, accreditation, and experience. Remember, it's an unregulated industry, so you really need to do the research if you want to end up with the best cybersecurity services partner.

Next, ask them some difficult questions.

You don't want to see your potential new cybersecurity services squirm. But you do want to make sure that they are going to deliver what you need. **And asking difficult questions is the only way to be sure that you're making the right choice.**

But then when things are up and running again, people don't immediately get back to business. Conversations are finished, systems are rebooted, everyone needs to regain their focus. And that often takes more time. What should have been a 15 minute interruption loses you 90 minutes of work.

And that's if it's a minor problem.

So, what can your cybersecurity services partner do to minimize this downtime? Will they be working away in the background, making the necessary checks to ensure that most of these little blips don't arise? Can they assure you that most updates and maintenance will be done outside of working hours?

Do they have any other solutions that will mean your business maintains productivity while essential work is taking place?

Ask them: *"Tell me about the specific people who'll be looking after us."*

Though it's an important question, many businesses overlook this side of things when it comes to working with a partner.

It's good to know about the people you'll be working with.

How does your proposed cybersecurity services partner assign your account manager, for example? Do account managers have an area of sector expertise? Do they match you on how your personalities may work together? Or do you simply get assigned to the person with the smallest current workload?

Will you always be speaking to the same person? What happens if that person is on vacation or sick? Who will be doing your strategic cybersecurity reviews and building your cybersecurity roadmap? Who do you talk to if you're not happy?

This question is a great way for you to get to know more about the company you're hoping to work with. But it's also a great way for you to figure out if their people are the right match for yours.

Ask them: *"Can you explain something deeply technical to me in a way I'll understand?"*

With this question, I'm not suggesting that you try to learn the ins and outs of building an IT infrastructure from the ground up. Instead, it demonstrates your potential cybersecurity services partner's ability to explain things to you in English, not tech-speak.

Can they explain a really complicated, technical process to you in a way that you can understand? Do they get frustrated if you ask too many questions? Do they brush you off with 'you don't need to know the technicalities of that'?

If you are partnering with someone, it's vital that you can communicate with each other clearly, without any confusion or breakdown.

It also demonstrates their ability to educate you about the things that matter.

Ask them: *"How will you keep on top of the constant changes in my business?"*

It's no secret that successful businesses deal with a lot of change. From adding new staff members, to tweaking the product or service you offer, it's likely that your business is forever changing things.

It's the way we grow.

In fact, your business probably looks very different now to how it looked 12 months ago.

So how will your proposed cybersecurity services partner cope with that? How much do they need to know about these changes? Will it affect what they're doing for you?

It should. Remember, you're looking for a partner here, not just another supplier. It's part of their role to be able to make

recommendations based on how you're working. To suggest better software to use, a smoother network, more appropriate security.

If they can't keep track of how many people are working for you, or the ways you deliver your service, how can they suggest ways to grow, improve – and especially, stay secure?

Look for a new partner who takes an active interest in the changes happening within your business. Perhaps even arrange regular catch-up sessions to ensure they're on top of everything that's going on.

There are lots of other questions that you should be asking. But I feel these are the 5 that tell you the most about your potential partner.

Chapter 6:
What every cybersecurity services company wishes you knew about cybersecurity.

Before you glaze over and flip past this chapter, I'll add my disclaimer here: I'm not about to bore you with technical jargon or tech speak. Please don't panic!

What I am going to talk about are the basic things that – if every client knew them – would make our lives a lot easier.

#1

Your setup needs constant monitoring and maintenance. It's not a one-off job

Computers and other devices ask you to update them all the time. And that's because things are constantly changing.

The same applies to your network and infrastructure. Software is always changing, operating systems are being tweaked, and hardware deteriorates. It never ends!

It's virtually unheard of in professional cybersecurity circles that an cybersecurity services isn't about constantly monitoring and protecting your business. If you're not offered 24/7 monitoring and maintenance as part of your cybersecurity services contract, run a mile. You will start seeing issues before the ink on the contract is dry.

Most cybersecurity services support companies do it all in the background and you never hear about it. In fact, a great cybersecurity services support partner will spend a lot of its time monitoring what's going on within your system, and fixing issues before you know you have a problem.

#2

The support triangle is like the hardware triangle

This is a fun concept to learn about buying hardware.

Picture a triangle in your mind. The three equal sides of the triangle represent quality, speed, and price.

If you make one side longer, then all the sides will lengthen to keep the triangle together. For example, if you pick a faster computer, typically the quality and price will also increase.

cybersecurity services has an identical triangle with the same three sides: Quality, speed, and price.

If you buy cheap cybersecurity services support, it'll be slow and lower quality. And vice versa.

Ideally, you'll look at what you can afford to spend on cybersecurity services support and go with the top of your budget. That's because you understand cybersecurity services support is an investment in your business. Get your cybersecurity services setup and your business cybersecurity strategy right, and it makes hitting business goals so much easier.

#3

Beware the bedroom warriors

Let's go back to them for a moment.

Picture a guy, sitting in his bedroom, carrying out your cybersecurity service. He hasn't got the overheads we have, so of course his service will be a lot cheaper.

But remember the triangle – his speed will be slow, and he won't have access to the professional cybersecurity tools, because they're expensive.

If you choose a bedroom warrior to provide your cybersecurity services support, doing everything himself – that's fine. Providing you're his only client. One person should be able to carry out the cybersecurity services support, maintenance, and monitoring that a business like yours requires.

But what happens when he gets another client?

And another? And then realizes, because he's cheap, he needs even more clients just to make a decent living?

The quality of the service you receive falls, as does the speed in which he reacts to your problems. It's possible he'll stop doing the proactive work for you, because one person cannot service many clients properly.

Yes, you pay more for a larger business with an office, team and all the tools. But you also know that they're set up to keep service levels high, no matter how many clients they take on.

We ask for a long-term partnership to protect you more than us

We don't want to work with people short-term.

We refuse to do ad-hoc work, and one-off crisis management.

We only work with businesses as part of a long-term partnership.

Why?

Well, obviously, it's good for us to build our own business around long-term clients. It's a great business model, if we're honest.

But the real benefit for us of long-term partnerships for us comes from the investment we're able to make in our clients, so that we know you inside out. It means we can:

- **Work more closely with you**
- **Learn about your priorities and take an active part in getting you closer to your goals**
- **Customize our cybersecurity offering around where you're heading, rather than where you currently are**
- **Build an infrastructure that grows with your business**
- **Keep you better protected, because we can take an honest and strategic approach when we work in a trusting partnership**

When you work with someone on a short-term basis, it's impossible to do this.

A long-term partnership means we'll be as invested as you will be. Because we genuinely care about your business. If you're doing well, we are too.

#5

Outsourced is better value for money. And helps you access better expertise than the same spend in-house

As you're reviewing your cybersecurity services support, it's probably crossed your mind that you could build an in-house infosec capabilities .

There's a big downside to be aware of. When you have an in-house infosec capability, it comes with significant operational, financial, and strategic challenges. Understanding these hurdles helps leadership make informed decisions about whether to build internally, outsource, or adopt a hybrid model.you're asking them to do several different specialized jobs, and support a huge number of people, all at the same time.

Someone who can do that without having some kind of breakdown would be hard to find! Certainly, they'd soon learn to cut corners, just to get home on time each day.

When you outsource this work, you might pay a little more than an in-house person. But you're gaining access to multiple people, with a broad range of skills and specialties. And they don't go home until the work is done.

Chapter 7:
Protect the most important thing in your business

Sometimes, the businesses we work with have internal cybersecurity people. And a senior member of staff who takes on responsibility for cybersecurity, without having a background in cybersecurity themselves.

If that's you, then you should be scared. Terrified in fact.

Not because you don't have the skillset, but because if your measure are don't adequately address the threat conditions – I'm talking ransomware attacks or similar large-scale problems – the responsibility rests with you.

Luckily, there is a solution to protect both you and the business. It's called co-managed cybersecurity support.

You retain your in-house cybersecurity people. And we help them with whatever support they need, at whatever level.

The best way to describe our help is to imagine a ring donut, with your internal cybersecurity person in the middle.

Yes, it's a big donut!

They benefit from support all round:

- **At the bottom:** Help with handling the low-level stuff that's important but can be overwhelming, such as being the help desk for your staff, monitoring the network, rolling out updates
- **At the sides:** Support at their skill level to help them cope with their workload, and to have direct access to an experienced IT team to bounce ideas off
- **From above:** High level strategic advice and long-term planning

Our job is to complement your internal cybersecurity people, adding in the partnership and strategic overview. So, there's plenty of high-level thinking and support on tap.

This gets the most out of your internal resource, and fully protects you, as the person with ultimate responsibility.

Some cybersecurity managers see outsourced cybersecurity services partners as a threat.

*We are **not a threat***

Our job is to make you, and your internal IT people look great and operate seamlessly. When you look great, so do we – everyone wins!

Chapter 8:
Don’t take our word for it:
Here’s what our clients say

I’ve spent a long time in this guide educating you how to buy an cybersecurity service. I’ve covered all the bases. And by now you should know what you want and need in your cybersecurity services partner.

But it’s all very well me, the owner of the business, telling you how a great cybersecurity services partner will change your business.

It’s time you heard from some of my clients about the reality of working with us.

“NSecurity Consulting transformed our SOC operations. Their focus on automation and streamlined processes significantly improved our response times and reduced analyst fatigue. Highly recommend their expertise.”

“The team at NSecurity Consulting provided top-notch service and truly understood our needs. Their solutions were customized and effective, leading to enhanced security and operational efficiency.”

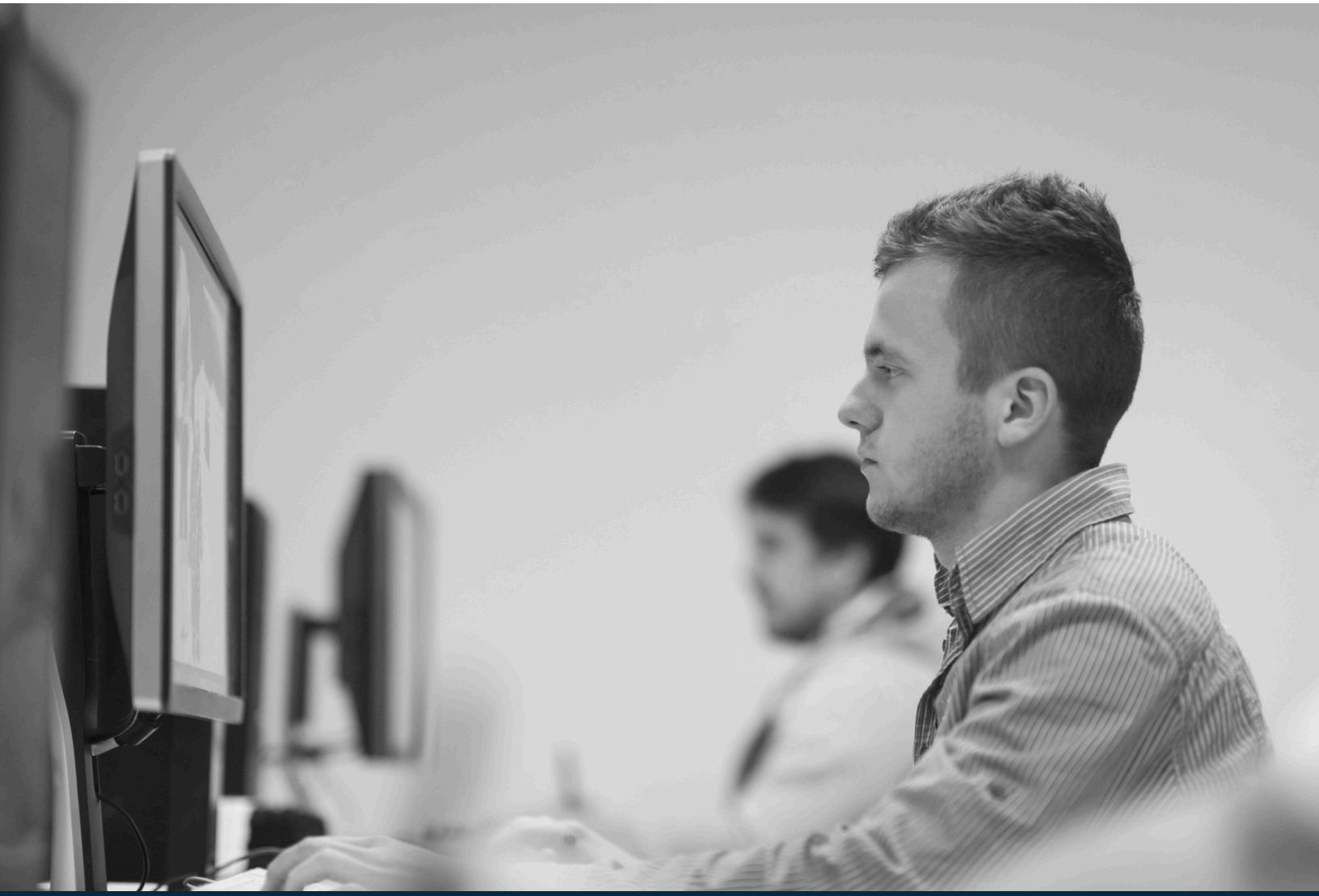
Real Estate Firm boosts SOC efficiency with SOAR (Security Orchestration and Response). NSecurity Consulting helped us automate key parts of our SOC operations through SOAR playbooks. We’ve cut response times dramatically and our analysts can now focus on strategic threats instead of repetitive tasks.”
– SOC Manager

Mid-sized law firm modernizes security and achieves compliance “The move to NSecurity’s managed security services was a game-changer. Not only did we feel more secure, but the level of detail and automation provided by their SIEM and SOC made our recent compliance audit a smooth, uneventful process.”
— Managing Partner, Legal Services Firm

Chapter 9:
About us

I love our clients. They always have such wonderful things to say about us.

Let me now properly introduce me, my team and our business.



I've always loved computers. Some of my earliest memories are of me working on Windows 3.1 to help my dad's printing business (if you're too young, or too cool to know, that's an old computer, and it was the first one my family owned).

As the years went by, the computers got more sophisticated, and my obsession grew. Any free time I had was spent either using a computer or learning about them. I even built my own when I was 16.

When the internet became commonplace, my interest in technology deepened. The world opened to me, and I loved all the new things to learn and practice.

You could say a career in technology was an obvious choice for me.

After studying computer engineering at Wichita State University of Wichita, KS, I started off working as an cybersecurity analyst. After a few years I joint ArcSight Inc, the then market leader in SIEM technology. I really enjoyed the job. Problem solving, creative solutions, seeing the difference I was making to the companies I worked with; it was so rewarding.

But while I loved my job and the clients I worked with, I found I was becoming really frustrated with the way that the company did things. It didn't put the clients first. It wasn't part of the role to help our clients grow and improve. The client wasn't at the heart of everything that was being done. ***And to me that was wrong.***

One day, something just clicked inside me. I realized that I needed to go and do this for myself. To find my own clients and help them in the same way that I would help my own business. To really make a difference to what they did.

In 2014, I quit and took the step to set up NCI. I haven't looked back since!

Since 2014 we've grown in exactly the way I'd hoped for. I have my own team now, and dozens of businesses see us as their trusted cybersecurity services partner.

My whole team are personally invested in every business we work with, celebrating their success as if it were our own. Because really, it is.

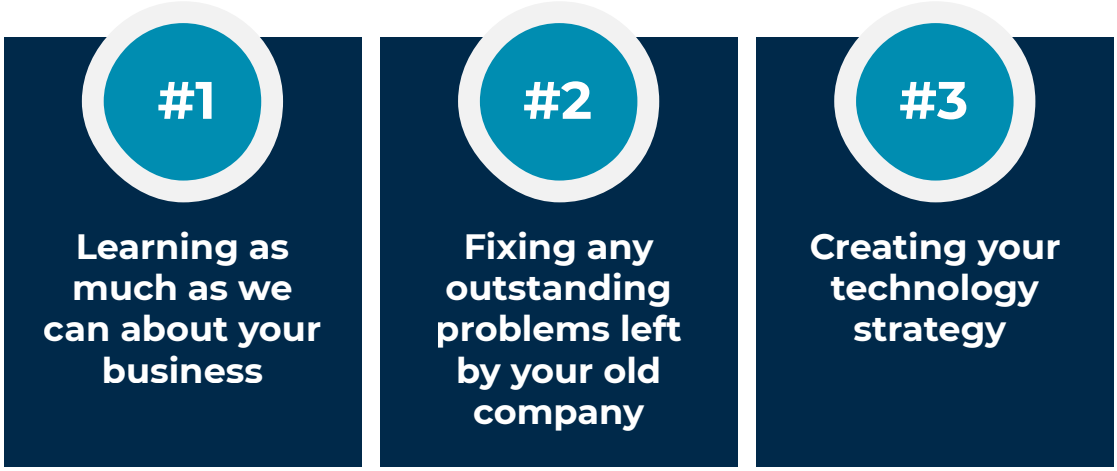
We know that we've played a part in helping each business to reach their goals and hit their targets. And that's a great feeling.

Chapter 10:
What will happen during your first 90 days

If you're ready to explore working with us, here's some important information you need to know.

When we begin to work together, the first 90 days are the most critical.

My team and I will be working on three key areas:



I hope and expect to work with you for years to come in our partnership. So, my goal in these first 90 days is to set you up for success.

You'll know:

- **What we can and can't do, with realistic expectations**
- **What we need from you and**
- **How to be a great partner**

We'll survey everything and examine every tiny part of your current cybersecurity setup. The more we know the better. All the answers are fully documented in our secure systems.

We'll even ask about your website hosting and examine any specialist software you use. Even if we're not directly supporting these things, we still want to know how it works and who's supporting it. At some stage in our relationship, you're going to ask us about it, so, we need to know about every single service or third-party vendor you're currently using.

Of course, it will mean there's a little work for you and your team, but I promise it will be worthwhile. And you'll only need to do it once.

Once my team has all the information, they'll strategically analyze it to make sure they understand every aspect of your technology. Any cybersecurity services company that doesn't do this is not doing their job properly.

Then we're going to talk to your team. Every single person.

We'll find out what their existing cybersecurity problems are, what frustrates them and what makes their job more difficult. We'll also review anything your previous cybersecurity services provider told them couldn't be done, fixed, or created. There's no promise we can make it happen, but of course, we'll try.

Your first 90 days are going to reset everything. And then get your entire cybersecurity setup back up to the high level it needs to be (and where it will stay).

Then – and only then – you and I begin our strategic, forward-thinking work together. This is a unique process for every client. I can tell you more about it when we talk.

Here's what to do next.

Chapter 11:
What to do next

I hope you've found this guide useful, and it's covered many of the questions you've had about choosing a new cybersecurity services partner.

Perhaps it's made you look at your cybersecurity program in a different way?

Good news – we're currently taking on new clients again. That's why I wrote this guide.

I'd really love to talk to you about your business.

If you're serious about working with a new cybersecurity services partner to improve your business and contribute to long-term growth, this is your next step:

Contact us for a no obligation video call with me at https://nsecurity.ca/contact-us/

You and I can check that our businesses are a good fit and arrange a longer video call, or physical meeting (whichever is most appropriate).

Of course there's no obligation to buy anything, ever.

I'm looking forward to speaking with you and learning about your business.

This is how you can get in touch with us:

CALL: (800) 826-8102
EMAIL: prathabk@nsecurity.ca
www.nsecurity.ca
https://www.linkedin.com/in/prathab-k-b13b59145/