CYBER SECURITY

STRATEGY GUIDE

A COMPREHENSIVE APPROACH TO CYBER SECURITY

PRIORITISE YOUR ACTIONS, DEVELOP A PLAN, AND SECURE YOUR SUPPLY CHAIN

Softcat

Threats, risks, pressures, fears, uncertainties, mistakes…

Isn't it time to change the way we talk about cyber security?

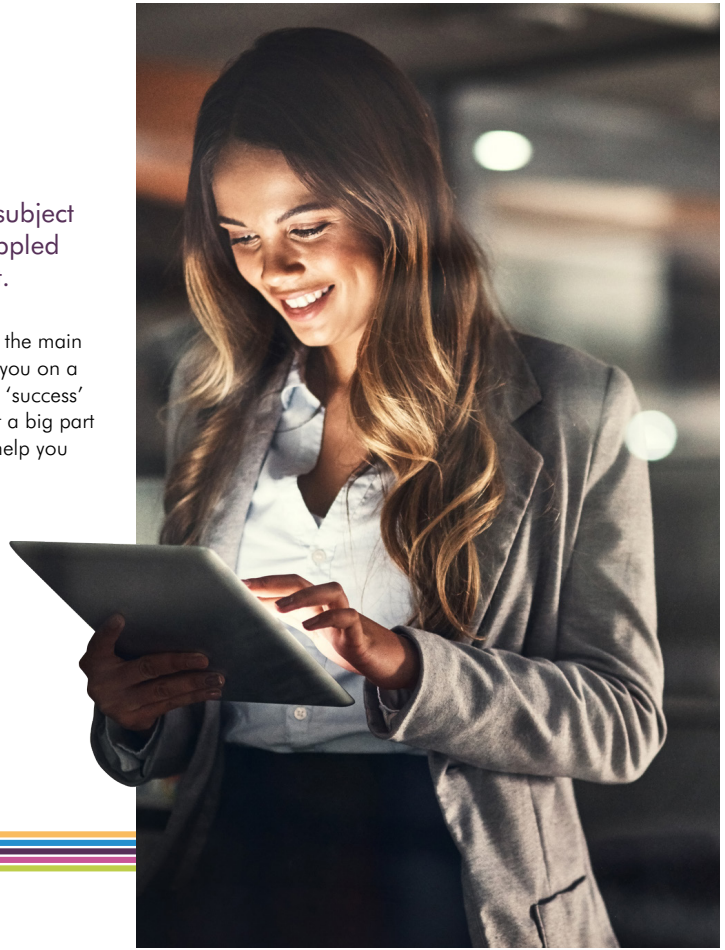
Almost every report, paper or guide based on the issue of cyber security approaches the subject negatively. It's all about what you're not doing right, how many businesses have been crippled due to breaches, and why you're in grave danger of losing everything if you don't act fast.

While there are certainly things to be cautious about, at Softcat we're more interested in focusing on what our customers are already doing well but could be doing better. Cyber security is now a common enough theme that there's less of a need to strike fear into businesses. And most businesses will have already implemented some form of security measures anyway, which no matter how basic, are a step in the right direction.

Businesses today are interested in knowing what 'good' looks like, as opposed to what's 'bad', and rightly so. We understand that you have a high level of responsibility to deliver consistently reliable security within your organisation. So, it's more beneficial to help you build a strategy for success, rather than point out the things that you might not be doing so well.

Therefore, this guide has been created to highlight the main areas that'll help you make improvements and set you on a path to continued cyber security success. What this 'success' looks like is clearly individual to each business, but a big part of what we do is clearly define your goals to then help you achieve them.

Matthew Helling
Head of Cyber Security Services, Softcat



INTRODUCING OUR APPROACH

Prioritising your cyber security actions

The first step towards improving your cyber security is the process of prioritisation. It's almost impossible to achieve everything all at once, so it's good to define and focus on what's most important to your business.

Developing a tangible plan

Once you understand where you should concentrate your efforts, you'll need a structure to be able to make progress. Plan to optimise your existing systems, bridge any skills gaps you might have, and attain any resources you may need.

Securing the supply chain

You've got your own security measures in place, but what about everyone else in the supply chain? We'll explain why it's key to understand who all your customers and suppliers are, and work with them to tighten up your data sharing.

We've held in-depth conversations with three of our experts to talk about the key areas required to build a solid cyber security strategy. All three offer a wealth of experience when it comes to working with clients of all sizes to improve their security outcomes. And over the coming pages, we've shared their insight, opinion and expertise in order to help guide you on your own cyber security journey.

Adam Louca

Chief Technologist, Softcat

Adam focuses on developing, engaging and transforming Softcat's strategic customers' cyber security approach. In addition, he also runs Softcat's cyber assessment services business, which helps customers understand and improve their cyber security.

Alexander Lewis

Security Consultant, Softcat

Alexander works with Softcat customers to identify, categorise and prioritise their cyber security risks and collaboratively develop a bespoke transformation project to best enable them to operate as a business with confidence.

Sean Huggett

GRC Consultant, Softcat

Sean specialises in governance, risk and compliance, including data protection, security risk management and ISO 27001. He has helped Softcat customers prepare for GDPR, NIS, ISO 27001 certification and other industry security standards.

You're doing great; keep going

Introduction: the state of cyber security today

Cyber security threats are rising. Attackers are using new and increasingly sophisticated methods. More organisations are going out of business as a result of attacks. The media makes us aware of all of these things, but what about the positives?

Today's businesses are more self-aware than ever when it comes to their cyber security. Indeed, 50% of large enterprises (with over 10,000 employees) are spending $1 million or more annually on security, with 43% spending $250,000 to $999,999, and just 7% spending under $250,000[1].

The market itself is poised for rapid expansion, with cyber security sales expected to reach $248.3 billion by 2023, up from $152.7 billion in 2018, representing a compound annual growth rate of 10.2 percent[2]. This can only be a good thing, and proves that measures are being taken to make improvements. What's more, the cyber security unemployment rate is currently 0% and projected to remain there until 2021[3].

EXPECTED CYBER SECURITY SALES

Huge action is also being taken towards regulatory concerns. $9 billion was spent by companies preparing for the introduction of GDPR[4] – with 88% of companies spending more than $1 million each on preparations[5].

Many businesses are doing things right. We just don't always get to hear about it because it's easier to employ scare tactics to encourage solutions sales. Threats will always evolve, but so will the approaches being used by businesses to protect themselves. Therefore, at Softcat, we believe it's best to help our customers create effective strategies based on a realistic, but positive outlook.

FOCUSING ON THE POSITIVES

It was reported in 2019 that 90% of all security breaches were due to human error[6], implying that businesses should fear the competency of their own staff – and to look to automation as the answer.

However, it's also been reported that 97% of companies with the best cyber security measures utilise an extensive staff training programme[7]. The lesson here is that, to strengthen cyber security efforts, it's better to raise awareness and teach employees about their responsibilities – a far more positive approach to the issue.

[1] https://www.cisco.com/c/en/us/products/security/security-reports.html
[2] https://www.crn.com/cybersecurity-week-2019
[3] https://www.csoonline.com/article/3120998/zero-percent-cybersecurity-unemployment-1-million-jobs-unfilled.html
[4] https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#4beb956934a2
[5] https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[6] https://www.smallbizgenius.net/by-the-numbers/cyber-security-statistics/
[7] http://business.itbusinessnet.com/2019/11/10-cybersecurity-statistics-in-2019-that-every-business-should-know/

Using findings taken from a cross section of Softcat customers, we've been able to establish the areas of cyber security that businesses are currently doing well in – and which ones can be improved upon.

INSIGHTS

You'll notice that data recovery scores particularly high, telling us that businesses have perhaps been prioritising their backup capabilities. Email and web browser protection also scores well, as does wireless access control and security skills assessment.

But it's areas such as the control of ports, protocols and segmenting networks where we can focus our attention on to help improve things.

THE AREAS OF CYBER SECURITY THAT BUSINESSES ARE CURRENTLY DOING WELL IN (average score/100)

Prioritising your cyber security actions

How to set the rules of the game

AUTHOR

Adam Louca

Chief Technologist, Softcat

When it comes to cyber security, as with most areas of IT, every business inevitably has an ongoing list of to-dos. This could include process-related tasks, problems to fix, regulatory hoops to jump, and business goals to accomplish. Therefore, in my opinion, prioritising your cyber security actions is vital in order to make any meaningful progress.

I like to think of it as setting the rules of the game. You need to know how to play before you start. And you need to be aware of the order in which your actions will impact your business. The thing is, there are many different ways to approach prioritisation and it's sometimes hard to know where to start. For example, you could prioritise your actions by:

- **The likelihood of issues occurring** – starting with the ones that you think will happen most frequently
- **Worst case scenarios** – prioritising higher level threats to prevent the worst from happening
- **Best case scenarios** – beginning with the easiest issues first to work through your list faster
- **Operational efficiency** – focusing on consolidating disparate tools to eliminate operational silos, and ensuring you're getting the most out of your existing technologies
- **Taking a firefighting approach** – reducing immediate risks by prioritising the most pressing issues

Each of these approaches has its own pros and cons, and they will differ from business to business. For example, a start-up may have more of a tendency to address and remediate problems as they present themselves. So, we often see a 'firefighting strategy' being used as a default option, with money only spent when it's really necessary. The business is probably willing to accept higher risks, as available budget is more likely to go towards growing the business. Having a comprehensive security strategy, with a full action plan on day one, may not be a priority.

On the other hand, for a hospital, it's critical to stay operational while working with limited budgets and resources; so it's far more likely to operate in the opposite way. The hospital might start by addressing the issues that are expected to occur first. But at the same time it will also take great care to ensure its processes meet all the relevant regulatory standards required to avoid large fines and bad press.

Every business is different. So, what are your priorities? Let me explain how I like to guide clients who are looking to get things in order…

BE PROACTIVE

In my experience, a proactive mindset is essential. And the very first thing to realise is that while you can't solve everything all at once, you can certainly start somewhere – and work through things one at a time in an order that creates the greatest impact both in the short and long term.

What defines this 'impact' is down to the individual business, the market it operates in and the sector it is part of. So, it's important to work out what matters most to you in order to maximise your outcomes. I like to determine this by asking clients a number of questions right at the start of their cyber security journey, based on a set of internal and external criteria.

Internal impact

Individual impact – what will make your life better?

How easy is it to use the applications, solutions and systems (tools) you currently have in place? If they're too complex, you may not be able to make best use of them, so you might want to consider prioritising your investments in tooling to make your life easier. Or do you need to boost your skillset in order to make the most of your current setup – in which case, is training required?

Team impact – what will make your team better?

Think about actions that can be taken for the greater good of the team, and what impact they might have on other teams within the business. For instance, if you were to update an aspect of cyber security within the IT department, would it suddenly mean that the finance department couldn't complete the monthly payroll?

The key here is to consider how any investment made may help or hinder others and ensure any new platforms integrate seamlessly with your existing infrastructure. But, of course, try not to overly simplify or consolidate things as you may end up with gaps in your security. In my experience, it's definitely a balancing act – but very much achievable with the right support.

Business impact – what will make the business better?

Risk management is always a key priority for businesses, as is the operational and financial impact of any security actions taken. As key drivers for almost all organisations, I think it's well worth getting into the boardroom to understand these areas first-hand. Therefore, I'd encourage IT leaders to get a feel for the business leaders' fears and aspirations, and build a relationship to make future communications as simple and straightforward as possible.

External impact

Environmental context – knowing who you are and what's around you

Consider the external factors surrounding your business, such as the sector you work in, the profile of your business and the type of customers you have. Pragmatism is key here – to the point where I'd strongly suggest choosing the most naturally pragmatic member of your team to take responsibility for assessing your environmental context.

By focusing on reality first, over and above any fantasy scenarios, you'll be able to concentrate on the most pressing risks. Then you can work out a way to deal with the everyday occurrences that you simply shouldn't avoid. You'll be able to make meaningful progress quickly and reduce many of the issues that could trip your business up.

Threat intelligence is important and it needs to be realistic. So, it's best not to spend too much time worrying about stories in the media of one-off incidents and freak attacks. Focus instead on who you are, what your business has to regularly face, and what happens on a daily basis.

THE FINAL WORD ON PRIORITISATION

It's important to remember that you can't prepare, protect and defend against everything all at once. But you can be more effective in prioritising your actions, and more confident that you're covering more bases.

Perhaps the biggest challenge for the majority of businesses is moving away from a reactive footing. Being in a reactive situation makes it very difficult to take the time to stop and look at things on a wider level. In this position, it's unlikely for anyone to be confident that they've got everything covered; are resourced to the right level; and are being effective with budgets. So, ensure your key people are aligned to your proactive approach as you start to become more priority-driven.

Prioritisation shouldn't cause friction when everyone is pulling in the same direction, or when changes are communicated up front. When everyone knows the rules of the game, everyone feels comfortable playing the game. And with this in mind, I'd also advise allocating clear responsibilities for key members of your team, because in times of crisis the rule book may need ripping up in order to save the day. The person responsible for responding, in this instance, will feel supported in their decisions, and empowered to act quickly.

Prioritisation shouldn't cause friction when everyone is pulling in the same direction, or when changes are communicated up front.

Developing a tangible plan

Why you need to devise a winning strategy

AUTHOR

Alexander Lewis

Security Consultant, Softcat

You've got your priorities in order, so now it's time to develop a tangible plan. Why 'tangible' specifically? Well, when it comes to security planning, many businesses focus on the fundamentals to be covered in terms of regulations, which looks good on paper and covers them if they're audited. But it doesn't necessarily mean they're confident in operating their business, or knowing they are doing the right things at the right times. So, the aim is to craft a plan that you can really hang your hat off – a set of real actions that lead to real outcomes.

When working with my clients, one of the first things I try to ascertain is whether they are confident they're covered against common threats. And secondly, whether they're covered against common threats specific to their business type. For instance, if you're the IT leader of a utilities company, you'll need to consider the threat of potential attacks from activists looking to thwart your operations. Whereas, if you work within a bank, you'll obviously need to focus on criminals looking to get hold of your customers' bank details.

However, the behaviour I see most often in clients is comparative to that of a housing tenant who spends huge amounts of time and effort frantically tidying up ahead of a landlord inspection every quarter! A lot of stress could be avoided if there was a change in their approach, and if they kept things organised all year round…

Keeping your engine running

Having a sensible, ongoing plan means that when something new crops up, you're you're prepared. It also means that you're keeping pace with the rest of the cyber security world, rather than constantly chasing your tail.

One example of this is with resourcing. Skills gaps are much easier to solve with a plan, rather than frantically finding people at the point you're desperate for them. With a plan, you have a clear view of the extent of the effort required and the all-important business case to take to the board.

It's the same concept as owning a car. Yes, insurance and breakdown cover give you an element of confidence should anything go wrong. But to know you've got working brakes, clean oil and a fresh service gives you the added confidence that you've reduced the chances of anything going wrong in the first place; and you can keep your engine running when you need it most.

Knowing the speed of your business

I believe that the very best cyber security plans are created by the organisations who truly understand the speed of their business. And what I mean by this is having a good understanding of how quickly things can get done. For example, while an endpoint solution implementation for some could take a few weeks, for others it could take 18 months. Either of these timeframes is perfectly acceptable; it's simply a case of being realistic so that any planning can be as accurate as possible.

I'll ask things such as: 'How long does it take for you to attain board sign-off?' 'Are there any skills gaps in your team that will hold things up while we train them?' 'Are we looking to achieve one step of a plan per month, or will each one take several months?' I like to try and help my clients learn the speed of their business as early as possible. And if they come to the realisation that things are happening slower than they'd like, we can work together to speed things up over time to become more agile.

Automate, or accept your fate

Many businesses want to achieve lots of things – usually all at once – and today, they might look towards automation as being the silver bullet solution. But it's firstly important to be realistic about how much you can do with your current resources and people. While enterprises might have the budget to hire in the talent they need to manage automation, smaller businesses sometimes can't. So, new technologies, systems and processes have to fit in to the existing infrastructure.

I suggest thinking about which of these three levels your requirement belongs in:

- **Level 1**: A simple task or process that can and should be automated
- **Level 2**: A task or process that can be automated in part, but human assistance is required
- **Level 3**: A task or process that requires human involvement throughout

While you might believe that automating a task can help you get it done more efficiently, it may not always be the case. So, you need to really think about whether human involvement is necessary, and whether you've got someone skilled enough to handle the responsibility if required. Once you've got this figured out, you can then start planning your approach.

A TWO-TIER APPROACH TO CYBER SECURITY PLANNING

It's easy to get bogged down in the complexities that can arise when creating a cyber security plan, so I recommend following this simple, two-tier approach as a baseline to getting things right:

Tier 1: Where have you already invested?

What solutions or technologies do you already have in place? How can you maximise them? Chances are you've already invested in some form of security in an attempt to shore up your cyber safety. It therefore makes sense to see if you can make the most of it, as opposed to starting from scratch.

Tier 2: What does operational confidence feel like to you?

What does 'good' look like to your individual business? And how does 'good' map to your budgeting? It's easy as a business to peer over the garden fence and see what's going on with your neighbours, but it's more important to focus on your own unique needs first and foremost.

THE FINAL WORD ON PLANNING

Creating a solid cyber security plan is all about combining the necessary processes, policies, governance, technology and your people – all under the lens of your business's unique priorities – and turning them into a clear strategy. You need to understand what your specific threat landscape looks like. And you need to be realistic about the speed in which you can get things done.

The plan itself should be a clear working document that all the relevant stakeholders can contribute to. The board should have sight of it. And any consultants you work with should have ownership over it too. The number of people who are involved obviously all depends on the strategic outcome required. But It'd say it's important to allocate key people who are directly responsible for delivering the plan over time.

The last thing I'll say is that, in my experience, there's a lot of scaremongering when it comes to cyber security, but it doesn't need to be like this. Crime, threat and risk will always exist, yes, but I like to focus on the good things that people are already doing, instead of what they're not. For me, it's all about optimising existing systems, getting the most out of your people, and planning to put security measures in place that constantly provide a good level of reassurance today, and into the future.

The plan itself should be a clear working document that all the relevant stakeholders can contribute to. The board should have sight of it.

Securing the supply chain

What it means to lock down suppliers, customers and everyone in between

AUTHOR

Sean Huggett

GRC Consultant, Softcat

Life used be simpler. At least it did regarding security. At one time of day, it used to be that a business would manage all its data by itself and keep everything secure by itself. But digitisation changed all of this. Businesses now rely on third parties who have access to their information, and this makes everything more complicated to manage.

Think of a castle with a moat. That's how things used to be for businesses. Everything was safe in one place, with one point of restricted access to trusted suppliers. In this analogy, a drawbridge could be opened and shut as required to let information in and out. Today, however, the situation looks more like the London underground map! It's open, multi-layered and accessible everywhere. New suppliers are onboarding all the time. Systems are increasingly accessible by, or connected to, supplier systems. Sensitive data is shared more than ever, including payment information, medical data and other personal data. It's exciting, highly convenient and entirely necessary, but it can obviously create potential cyber security issues.

The supply chain has subsequently become an easier way into organisations for cyber attackers. And small businesses, which typically tend to take greater risks and cut more corners in order to disrupt the market and grow at speed, are usually the most susceptible to these kinds of attacks.

However, big businesses suffer too and just one of their suppliers can end up affecting everyone in the chain. 'Island hopping' criminals use small suppliers with poor security as platforms to leap into otherwise secure large organisations and take what they can. This unsurprisingly makes financial and retail companies a key target, as well as manufacturers who have valuable intellectual property.

What should you do, then?

The supply chain needs to be prioritised better in order to ensure greater security. So, start by asking yourself who your key suppliers are. Who do you deal with on a regular basis? Put these names at the top of your list, and find out whether you've checked their security recently.

As a minimum, I'd recommend an annual review for all of your suppliers to ensure no new threats have emerged. And conduct reviews when things change, such as when your relationship with a certain supplier develops and you have to give them greater access to your data.

This applies to longstanding suppliers too, even if things have been 'fine' for years. It's now increasingly common to establish cyber security practices between businesses, so don't feel awkward for asking.

What about new suppliers?

If anything, I think that working with new suppliers can be simpler because it gives you the opportunity to set a precedent from the start; and define your new relationship when it comes to security. So, be sure to set a pre-qualification requirement for any new suppliers as part of your RFP, and include one or more of the following elements as a minimum standard:

- **Cyber Essentials or Cyber Essentials Plus** – certification that helps guard against the most common cyber threats and demonstrates a commitment to security
- **ISO 27001** – an information security management system that includes a framework of policies and procedures to help reduce risk
- **Independent verification** – an assessment of the business from an independent source, detailed within a full report

In the past, being set up as a supplier simply meant being asked a few questions around policies and processes, and in many cases just answering 'yes' was enough. Today, however, suppliers have to deal with an increased number of requests from customers for evidence that their business is secure.

It's now not unusual for the customer to demand the full policy and process details. Or, in some cases, they may send an auditor out to check they're true to their word.

With this in mind, extra validation on top of the essential elements listed above is frequently required. And many new contracts now include a data rider, or a schedule of controls to ensure cyber security is adhered to for the duration of the business relationship.

KEY REQUIREMENTS

Large organisations

- **Preventative measures** – ensuring that standards are in place to guard against threats, i.e. ISO 27001
- **Detective measures** – detecting and reporting issues before, during and after they happen
- **Corrective measures** – adding indemnity and liability clauses into contracts to prevent recurring issues

Small suppliers

- **Process focus** – setting up data procedures and policies, and keeping them up to date
- **HR focus** – establishing confidentiality clauses, completing security awareness training and keeping records
- **Testing focus** – undertaking independent penetration tests and sharing the findings

THE FINAL WORD ON SECURING THE SUPPLY CHAIN

Today, cyber security is a prominent and constant consideration for any business, which is a good thing. Threats will always exist, so businesses should regularly ask themselves questions like: 'Where's my risk?'; 'Am I going to invalidate my insurance by missing something?' These issues then filter through the business, with more people consequently seeing security as a priority.

As soon as the question of 'where's my weak link?' is asked, suppliers become a focus, so adding a minimum baseline in any contract agreement is critical. Data sharing is a common and fundamental part of partnerships today; combine this with the ease that data can be transferred – and the subsequent ease of access and loss – and it's clear why more organisations are striving to make sure they're covered.

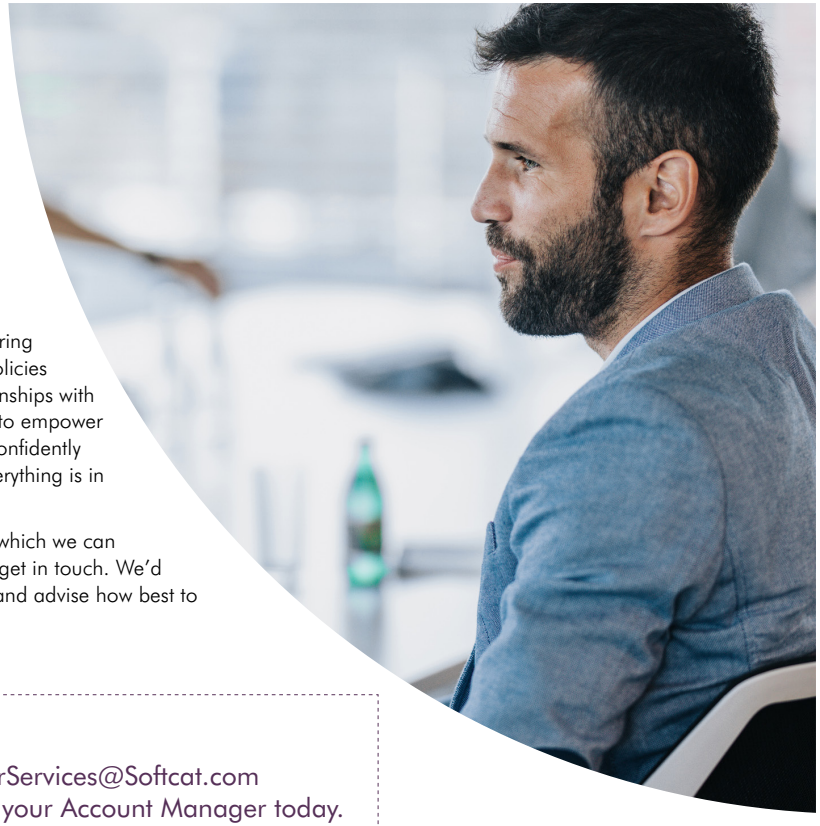
However, over the years, I've seen that very few businesses actually know their full supply chain. So, my key piece of advice is to understand who has access to your data no matter how big or small, no matter how regular or sporadic, and then prioritise them accordingly. Once you've got an order for your actions, you can create a plan that everyone's on board with, and then you can begin to secure your supply chain.

In my experience, it's often the smaller businesses who aren't sure of their priorities, and with not enough budget to hire an IT specialist, usually require support in this area. However, bigger businesses need guidance too, which is why, at Softcat, we have the expertise to be able to help all kinds of organisations regardless of size.

As soon as the question of 'where's my weak link?' is asked, suppliers become a focus, so adding a minimum baseline in any contract agreement is critical.

Creating your own cyber security strategy

Start your own journey to improved cyber security, with Softcat



Now you've seen the elements that comprise a well-rounded cyber security strategy, it's time to take a look at your own operations and devise your own approach. And if that still feels somewhat daunting, don't worry; help is at hand.

The first step is prioritisation. Define and focus on what's most important to you. Consider the internal and external impacts on your business and act accordingly. At Softcat, we work closely with clients to establish this key phase of their strategy and use our cyber assessment service to continually monitor their situation.

When you understand where to concentrate your efforts, it's time to create a structure that takes into account the speed of your business. Again, we support our clients in creating this tangible plan, to ensure that they cover every aspect required to optimise existing systems, bridge skills gaps, and attain necessary resources.

With a plan in place, you can start securing the supply chain; putting in place the policies and processes to tighten up your relationships with both suppliers and customers. We help to empower IT staff in this area, meaning they can confidently reassure the rest of the business that everything is in place to limit cyber threats and risk.

If you're interested in the many ways in which we can support your business, don't hesitate to get in touch. We'd love to learn about your current setup, and advise how best to improve upon it.

Contact Us

Email: CyberServices@Softcat.com
Or speak to your Account Manager today.