CYBER SECURITY

SMALL BUSINESS GUIDE

A PRAGMATIC APPROACH TO CYBER SECURITY

A SMALL BUSINESS GUIDE

Softcat

Cyber Security can seem like a huge challenge.

Especially for a business just starting out.

But it doesn't have to be. Cyber security recommendations are often focused on enterprise businesses, leaving smaller businesses unsure of what to do; Softcat is looking to change that.

Whilst threats, vulnerabilities and hackers are nothing new in this industry, Softcat looks to approach the challenge of cyber differently. Rather than follow the norm of fear, doubt and uncertainty, we help our customers understand their risks, how to control them, and how to accept them.

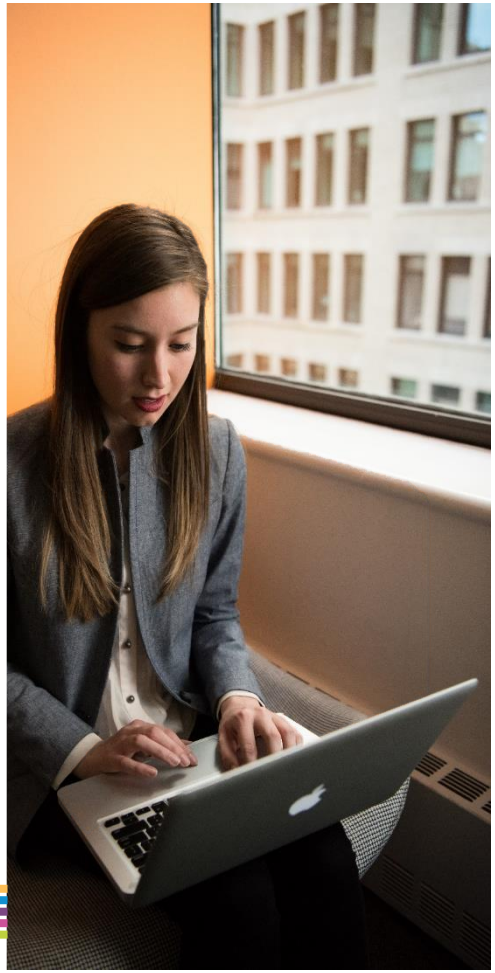
Small businesses are the backbone of our economy. Last year there were 5.8 million small businesses accounting for around half of the turnover in the UK private sector. These businesses, however, don't necessarily have a full-time member of IT, and even less likely a security specific head. Sadly, the resource an organisation has available is ignored by malicious threat actors.

Over recent years there has been a 424% increase in breaches of small businesses in the SMB category, accounting for just under half of all identified breaches. It's not all doom and gloom, however. We believe our experience of assessing organisations of all sizes and our extensive understanding of the security market identifies some basic steps small businesses can take to stop the most common cyber-attacks.

It is important to note, that these steps don't have to break the bank and should be achievable for all businesses. As your business then grows, these steps can be matured into wider operations and become the reliable security foundation your business can built on for the future.

Couple this with the traditional account management, expertise and resources available to you through Softcat, and you've got a long-standing partnership to keep you secure.

Alexander Lewis
Cyber Security Consultant, Softcat



INTRODUCING OUR THREE STEP APPROACH

Understand your Assets

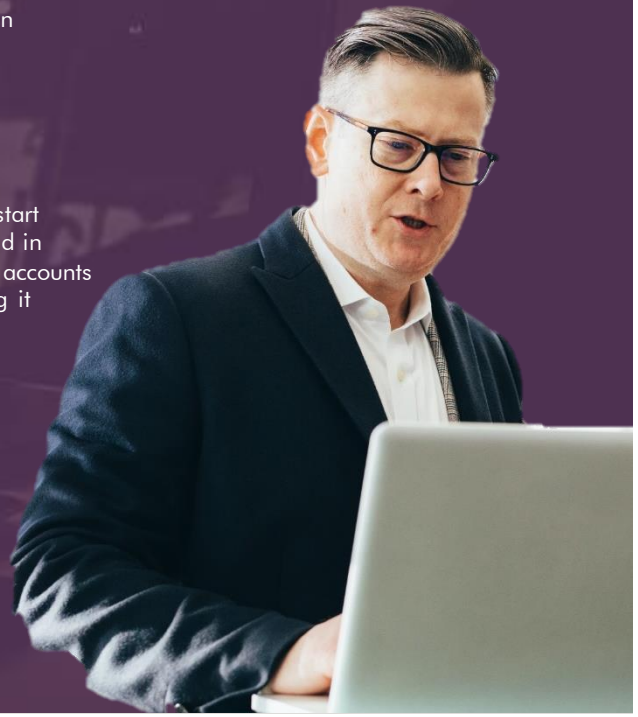
The Number one task towards improving cyber security involves getting to know your assets. Keeping track of them, whose using them and their vulnerabilities, will keep you best informed and best protected against the most common cyber-attack scenarios, plus provides invaluable insight in the event of an investigation.

Control your Permissions

Once we know all we can about your organisation's assets, it's time to start looking at the user. Understanding where and how privileges are applied in your business allows you to start off on the right foot, ensuring elevated accounts are only assigned to those with a legitimate business reason and making it harder for an attacker to make changes.

Store your Logs

System Logs, which are essentially the minute-takers of a particular system, allow security professionals to have the ability to go back and understand events occurring on devices, as well as identify malicious activities. Regardless of whether or not these can be interpreted in-house, collecting and storing these are of huge benefit in the event of an incident.



Through the expertise of our cyber assessment services and the networking and security division, we've provided a commentary of the approach for small businesses through three of our experts. Each have extensive experience in working with a broad level of organisations and they have specific cyber security knowledge through working with small businesses.
The following pages shares their insight, expertise and opinions.

Ella Watson

Networking & Security Specialist, Softcat

Ella provides networking and security expertise to both customers directly and to Softcat account managers. She balances industry and vendor knowledge, solution architecture and commercial ownership.

David Hewson

Cyber Security Assessor, Softcat

David focuses on providing organisations with a holistic view of the 'point in time' security posture and subsequently provides bespoke remediation advice, working across all industries and business sizes.

Alexander Lewis

Cyber 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.

Understand your assets

Get to know your technology

AUTHOR

Ella Watson

Networking & Security Specialist, Softcat

An IT asset is any data, device, or other components that sit within the information technology environment of an organisation. These generally include hardware such as computers, switches and various Internet of Things (IoT) devices. Software is another example of an IT asset which includes mission-critical applications and support systems. With this in mind, why is it so important to understand and manage these assets?

There are new vulnerabilities and attacks identified every day and it can be difficult to keep up with them all; from social engineering and phishing, to zero-day exploits and advanced persistent threats. Although as businesses we can focus on protecting these by considering potential attacks vulnerabilities and planning on deploying technological solutions to hopefully mitigate these, we often overlook what needs protecting in the first place – our assets.

Uncertainty around security threats and unpredictable events are much worse when organisations fail to understand where their assets are located, how they are managed, and if they are vulnerable. Therefore, the foundation of having an effective cyber security strategy is understanding your current environment. Undertaking an inventory of your organisations' digital valuables enables you to scrutinise what they are and where they are located, lowering the security risk of misplaced or misconfigured assets.

There are multiple benefits associated with understanding your assets which are invaluable in mitigating risk concerns. The sections below highlight how asset management can improve your cyber-security posture:

Updated Software and Latest Security Patches

With an accurate understanding of current assets, your organisation can ensure that software remains up to date. Old versions of software or assets that haven't been properly patched can pose a security risk to your organisation.

Vulnerability Scanning

System vulnerabilities represent gaps in security that can be abused by attackers who are constantly searching for new exploits. Ensuring that you are aware of what assets are connecting to your network, means you can easily implement vulnerability management strategies that can identify the weaknesses of assets on your network.
Scanning tools that regularly check for new vulnerabilities are crucial in preventing cyber security breaches, especially as vulnerabilities can be left un-patched for long periods without regular scans. Asset management brings considerable benefits to vulnerability scanning. If you aren't aware of all your assets within your organisation, how can you know every vulnerability is patched?

Assets Connecting to the Network

Unauthorised or unknown assets can introduce security risks to a network, so tools including network visibility help to provide transparency to all the devices that are connecting to your network. This allows you to put checks in place to verify that assets are compliant with security updates and controls. Having these measures in place to track and manage assets allows you to be notified if an asset fails to report into your network, allowing you to investigate missing assets that may have been misplaced or stolen.

The key to understanding IT assets and keeping track starts with your organisation; by considering the whole enterprise and then prioritising critical risks. By anticipating attacks, responding to them in real-time and protecting assets according to their value, your organisation can enhance abilities to stop sophisticated cybercriminals.

Understanding Security Measures for Each Asset

Managing your IT assets enables your organisation to understand which departments and purpose is associated with each asset. This provides you with vital information on the security measures you need to put in place. For example, within a testing environment of a datacentre network, servers for this need may require different security policies to servers that provide web services within a live environment. Furthermore, establishing which employees are using certain assets, allows you to understand who has access to sensitive data, meaning organisations can restrict user permission where needed.

Standardisation of Assets

Asset management can provide uniformity and transparency to your organisation's cyber security strategy by utilising standardisation practices. In doing so, you can ensure all IT assets on the network follow a standardised build process to provide uniformity in configuration. As a result, your organisation can adhere to certain practices and regulations concerning your cybersecurity strategies. Standardising assets also helps to reduce the overall system complexity and maintains consistency across the network.

Criticality of Assets

Assessing the criticality of assets on your network is crucial, as some assets are more exposed by potential adversaries than others. This allows you to determine which assets must be prioritised for protection, how likely it is that these assets will be infiltrated and what can be done to protect them.

The following guidelines provide a unified approach that you can take to managing and prioritising your IT assets and risk for a more reliable cyber security strategy. One of the basic controls includes identifying all devices, documenting your inventory and keeping your inventory current and up to date.

Discovery Tools

For security conscious organisations, implementing tools created by market leaders to specifically discover and track both hardware and software assets on the network is often advised and can be easier than doing it yourself. By utilising active and passive discovery tools, these can help to identify devices that are connected to your network. These tools ensure that only authorised devices are given access to a network, and any unauthorised devices are discovered and prevented from gaining access. In addition to this, actively managing all software on the network is equally as important, to ensure that only authorised software is installed, and that any unauthorised software can be found and prevented from installation and execution.

Creating an Asset Inventory

However, for some smaller organisations, implementing these tools can often be quite costly. With so many different technologies helping to automate processes, how can we manage our IT assets in a cost-efficient way? One simple method is to track assets yourself through implementing an ongoing strategy. It's important to mention that this step is not a one-time thing – it's a process that is dynamic and ongoing for the entire lifecycle of all devices on your network. You can track the assets by using documents such as Microsoft Excel, without relying on the aid of discovery tools, but this is more manual and reliant on individuals to keep this inventory up to date as opposed to automated software solutions. It is, however, important to mention that you can document any information that you find necessary for that asset within your asset inventory and this can vary from organisation to organisation.

THE FINAL WORD ON UNDERSTANDING YOUR ASSETS

Understanding and tracking assets that you have on your network can bring you huge benefits while allowing you to establish a more effective cyber security strategy within your organisation. Although the steps highlighted above can often be overlooked by many, these actions can be easily achieved to ensure your cyber security strategy remains effective. Taking appropriate measures means that you can be certain only authorised, secure devices are connecting to your trusted network.

Being aware of what assets are connecting to your network, and what to do if an unauthorised asset is on your network is the best possible way to mitigate any threats to your organisation. There are multiple benefits to understanding the assets you have on your network. Putting the right measures in place provides you with much better scope to being proactive and mitigating risk before an attack happens. While taking the steps described are advised, understanding and tracking your assets most effectively will vary depending on your organisation. Setting expectations of what you want to accomplish through successful asset management will ensure that you achieve your cyber security objectives within this particular element.

Following an asset management strategy, whether this is using discovery tools or by tracking assets yourself, will help to radically improve your security posture. It will also provide you with a solid foundation of transparency to those assets on your network and how best to protect these accordingly.

Asset management is one of the most basic things an organisation can do that will mitigate the most risk.

Control your permissions

Be aware of who has access to what

AUTHOR

David Hewson

Cyber Security Assessor, Softcat

Permissions, put simply, determine who has access to what. Being aware of who has access to what and having a high level of control over this is important, especially over those accounts which are given administrative privileges. To a malicious threat, these administrator accounts are a high priority target due to their plethora of access.

Admin privileges are often only given to select users who ultimately require these permissions to function in their day-to-day job. However, the level of access can still vary, therefore it is important that we monitor these accounts effectively.

Automated tools exist to help maintain an up to date inventory of administrative accounts. These Privileged Access Management solutions not only store the required information but will also assist with the management of these to secure, control and monitor privileges, working most effectively alongside an existing Active Directory. Having access to this information means you can make sure only the authorised users have access, thus decreasing the size of your attack surface.

Even if your organisation is 'small', it's still important that these privileges are controlled and monitored. Anyone with privileged access, who doesn't require it, acts as an important target for malicious threats who could use these privileges or the account to move laterally around the network or access to critical information.

Some users may require certain administrative privileges dependent on their role. Other users may require only access to the tools or data but do not require any control over it. A basic example of this is, you may provide a user with Microsoft Word training documents and its crucial the user has access to these documents, but you don't want them plagiarised or edited. Therefore the user receives the documents in a locked 'Read Only' mode.

However, a Learning and Development team requires access to these documents to keep them up to date and relevant. As a result, they would have full access privilege to these documents. Picture this on a much larger scale - files with highly critical information, servers with critical software.

Having strong visibility and control over account permissions is highly beneficial. Initially we want to be limiting these permissions as much as possible where achievable, making sure only those who absolutely require admin privileges have it and restricting those that don't. These also allow for better control as we'd be able to more effectively monitor if anything changes, as only limited accounts would be able to action such change.

As with many security areas, having the correct visibility and control is invaluable. It allows for quick and effective responses if a malicious event takes place in turn, reducing the damage that could be done and even the potential to stop it happening in general.

It's worth noting that some accounts need the privileges and they will always act as a risk, but as always, steps can be taken to make sure you have reduced the risk and putting in place controls. It's all about making sure only those that need it have it and those that have the permissions have a good business purpose. It's important not to fret over every permission each user has but ultimately to make sure the permissions they do have are correctly given. Let's run through some steps that can be taken to assist with this.

Have the Tools for the Job

Ideally acquire a Privileged Access Management tool as these help automate the process and store those crucial details including, administrative accounts, domain and local accounts. If an automated tool is out of reach, basic tools such as excel can be used, detailing the above information and having regular checks to make sure the details are correct, much more manual and not as effective but 100% better than nothing.

Default Password

A simple first step, but still an area many skip over or add to is the 'I'll sort that later' list. Make sure all default passwords are changed before any new assets are deployed, as lists of these default passwords can often be sourced online, so as much as your default password may sound unique, it may not be secure as it seems and acts as an easy in for malicious attacks.

Dedicated Accounts for Admin Users

A user with an administrative account should use a dedicated or secondary account for admin tasks. This account should be used strictly for admin tasks and not any day to day activity. This again reduces that attack surface, meaning less points of entry for those with malicious intent. It also means that in the case of an incident, narrowing down the point of entry is that bit simpler.

Dedicated machines

Dedicated accounts are great, and dedicated machines, even better! This machine should be segmented from the organisations primary network and not allowed internet access. You'll hear it crop up over and over, but this allows you to further reduce that attack surface.

Multifactor Authentication

Using multifactor authentication is a great tool to implement, as MFA acts as a great extra layer of security with the user having to prove they have access to a device they own, as well as knowing their own personal credentials. Even if not feasible company wide, it is even more important to get MFA for administrative accounts so this may be a manageable goal.

Encrypted Channels

Very similar to the MFA section, encrypted channels such as SSH or VPN would be great deployed across the organisation but if more manageable, use them for your administrative accounts only and grow out from there.

Unique Passwords

In an ideal world Multifactor authentication is in place, but for those for whom that just isn't an option, make sure that passwords are unique to each system and ideally follow a strong security policy with set standards. Weak, easily guessed, regularly used passwords such as Password1234 shouldn't be an option.

Scripting tools

Scripting tools such as PowerShell or Bash should only be accessible from administrative accounts or users that require access to these tools such as development teams. Should a malicious user have the ability to access these tools running a malicious script becomes very simple.

Login Alerts

If a privileged access management tool is in place, ensure systems are configured to ping over alerts if unsuccessful logins attempts to admin accounts are made. This will also hold logs of when the attempts were made and on which account. This allows for better visibility and control.

KEY REQUIREMENTS

Whilst it's easy to think managing permissions is complicated, keep it simple by coming back to these key points:

Justify the business need

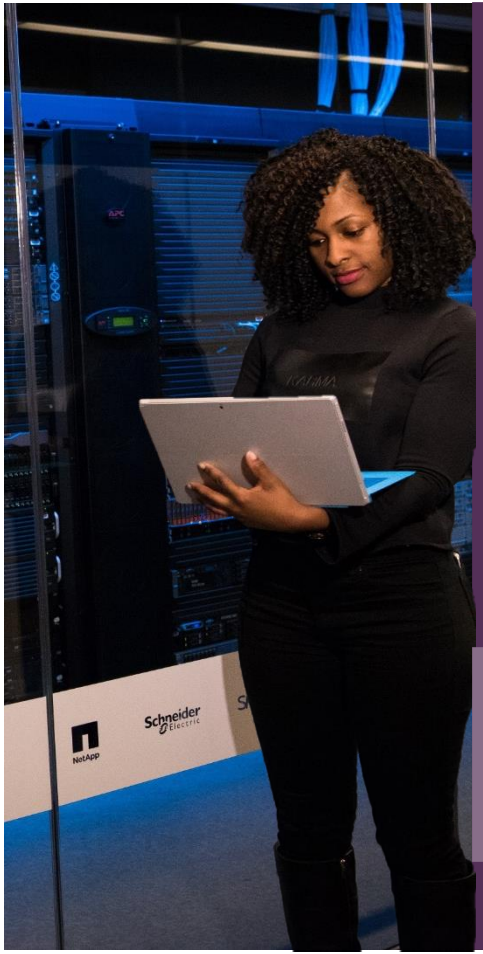
Does this user *have* to have this access? Just because they've always had it, or because they want it is not worth opening the organisation to unnecessary risk.

Minimise the risk

Whether elevating privileges temporarily, or creating a second account, ensure if administrative permissions are given, your organisation has controls deployed to minimise the risk, such as the ones identified in this guide.

Review regularly

Ensuring users permissions, the business need, and the relevant controls are regularly reviewed will make sure nothing slips the net.



THE FINAL WORD ON CONTROLLING YOUR PERMISSIONS

It's an ongoing battle and may sound like a lot of work (with the potential for moaning users), but simple steps taken can help massively reduce that attack surface and gain that extra control over your network via effective, controlled use of administrative privileges. Simple questions to ask yourself can seriously reduce your risk: Does the user need access? Do they need full access? Do they need access all the time? Could we use dedicated account/machines for admin tasks? Is MFA/encrypted channels for at least admin users an option (if we limit those admin accounts and machine)? Do we have strong security standards in place for password management? Are all default passwords changed on devices?

Privileged access management tools would be great and help automate a lot of these tasks. It doesn't have to cost a chunk of your budget and there is most certainly initial considerations and steps that can be taken. Ensuring we work on keeping the attack surface as low as possible, by minimising the potential footholds a malicious user could use to access those critical tools and that vital data.

Make key decisions around the implementation of tools that would assist with the management, as well as those important access/restriction decisions. An employee who is a bit upset that they can no longer type random assortments of things into PowerShell to see what happens, or are not impressed that logging on takes slightly longer with MFA in place, or that they don't want to have to log on to a separate account or machine, is the better alternative than if a malicious user gained access and is able to exploit these areas.

Privileges sound scary and difficult to manage, but in reality, having a small bit of control and enforcing some basic security steps can ensure that high level access to your sensitive systems and data is something that remains firmly in the hands of your organisation, and away from malicious threat actors.

Store your logs

Keep a record of all systems in operation

AUTHOR

Alexander Lewis

Cyber Security Consultant, Softcat

System logs, which are essentially the 'minute takers' of a given technology, record what a system did, when, and why, and can be an invaluable source of information both before and during a cyber incident. Keeping these logs can be your 'break glass in case of emergency' resource.

System logs, often referred to as 'syslogs' continuously and chronologically record the events a given technology asset has interacted with. Regularly collecting and storing these logs are invaluable in multiple ways.

The first benefit of storing system logs is that we can look retrospectively in the event of an incident. Being able to interrogate the logs of a potentially compromised system means we can ascertain the technical events leading up to the incident. Additionally, this information assists in establishing the scope, as the information supplied can help in narrowing the search for the root cause of the incident.

Whether or not your organisation has resource in-house to interrogate these systems, it is still worth storing these logs, should your business decide to invoke an incident response service. These logs can aid the efforts of these services and also ensure an efficient use of time.

Another benefit of system logging is that we can review logs to identify anomalies. Take for example a business that has two sites, one in Glasgow, and one in Southampton. A user successfully swipes into the Glasgow office, but then 30 seconds later logs onto the company's CRM using a device in Southampton. Whilst both individually are acceptable events, a user cannot be in both locations in such a short space of time.

Identifying these sort of events can allow for earlier notification of an incident and in many cases the prevention of malicious events. A word of caution on this point is that it is very easy to become overwhelmed with the number of 'events' that occur on certain systems, and this anomaly detection can quickly become an insurmountable challenge for smaller businesses, if attempted at all.

The best advice here for security conscious small businesses, would be to utilise the expertise of service providers who already have a process and technology to achieve this.

But what if anomaly detection isn't for you – either being too expensive, too complicated, or not achievable for other reasons? As mentioned before, simply storing these logs can be a huge help. See below some key considerations when looking to store logs:

Consider where to store logs

Log storage, as with property, is all about location, location, location. Whether on premise or in the cloud, thinking about how to control the access to your logs, how to keep on top of the storage, and ease of access during an incident are crucial considerations at this point.

Ensure logs are useful

Sounds obvious, but ensuring logs actually contain relevant and detailed information is of key importance. Information such as event source, date, timestamp, user and relevant source/destination addresses actually deliver on the context elements a log should provide.

Manage the storage closely

As mentioned, logs can quickly grow and create an exponential storage problem if not monitored and certain controls set. Ensuring your storage location has adequate capacity is the first consideration here, as losing logs due to insufficient available storage can be a real headache, when those lost logs happen to be crucial to the resolve an investigation.

Keeping logs on all devices sounds great, but only adds to this storage problem. Confirming you are collecting all *relevant* system logs, allows you to minimise unnecessary used space. Whilst it could be useful to collect everything, it may not be feasible to store everything.

Setting the right retention period for your organisation can aid with handling this issue. In principle, the best advice is to retain for as long as is feasible, but pragmatically have a think about realistically how far back you'd want to look during an incident, that providing this doesn't create a ridiculous storage problem, either by size, cost or both, and work with that.

Enforcing your retention is then the final step here, either through manual or technological means. Once a logs date hits past a certain figure, it needs archiving, moving, or deleting, to make room for newer ones. Nobody is expected to log everything forever, and smaller businesses may not have the bottomless pit of cloud storage a larger organisation could be happy to pay for.

Know how to interact with your logs

Once we know where, how, when and why we are storing our logs, it is imperative to understand how we as an organisation interact with them.

Understanding who has access, how they achieve this access and when this access is required is the first step here. Controlling this, but also ensuring when required it is able to be accessed can be a difficult medium to strike. Keeping the users limited but the access simple can be one way to achieve this.

If examining logs in-house, build an escalation process to clarify when something is simply a weird event that someone wants to confirm is benign, and the relevant process to handle that, versus something significant which likely indicates compromise. These two scenarios should be handled differently to ensure the right information gets in front of the right people ASAP.

If you don't have security resource internally, and only want to ensure this information is available for a third party, then knowing this interaction is your port of call. Sounds simple, but knowing who that third party is can save a surprising amount of time. Having up to date, and out of hours contact details for this organisation gets the ball rolling faster.

KEY FOCUSES TO SECURITY BASED LOGGING

It's easy to get bogged down in the complexities of logging and feel like you're out of your depth. Keep yourself true to what you want to achieve with these two key questions:

Question 1: What are you hoping to achieve?

If you're simply looking to find a place to store your logs, attempting to build a process to regularly review them isn't feasible. When reading this question keep the context to which you want to apply this learning in the forefront of your mind to get the most from it.

Question 2: Is it realistic?

Whilst wanting to analyse everything going on in your world is commendable, if you have an IT team of one, this may not be possible. Focusing on your ability to execute any new process, technology or solution you aspire to implement will allow you to achieve your objectives, whereas idealistic overengineering will hold you back.

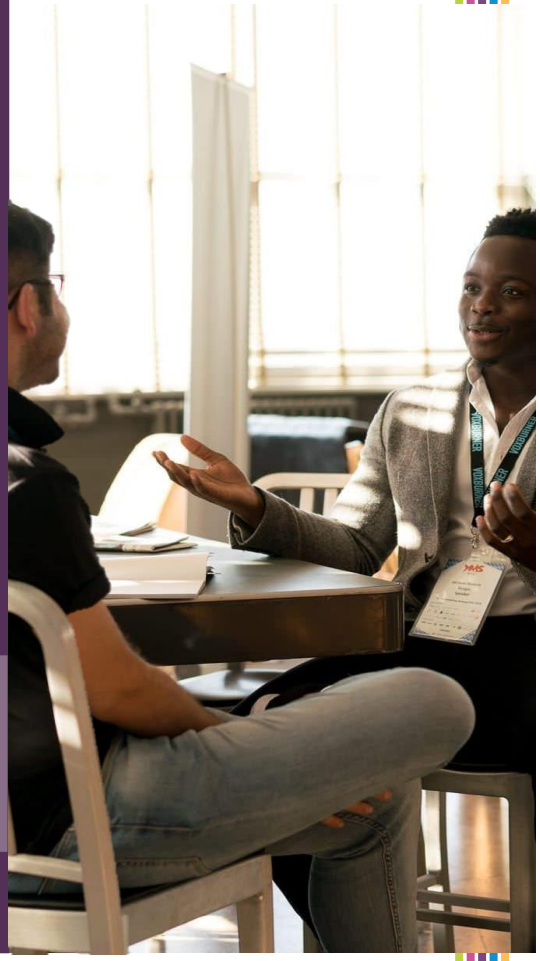
THE FINAL WORD ON STORING YOUR LOGS

Having logs available when you need them, can be a huge resource to any customer of any size. Being able to retrospectively look at the events that occurred can provide invaluable context and prove/disprove a suspicion of a user. Whilst arguably the most complex section of this guide, this is still achievable with the help of security experts, or through a trusted service provider.

Ensuring your organisation knows what is going on with its logs, what is being collected, how it is stored and the relevant interactions with them, not only puts you in the best place for security investigation, it also looks great on supplier questionnaires and more generally in the security industry. Being realistic with what you're looking to achieve and knowing when to call upon external help, can be your best escalation points during this process. Making sure the governance and controls are relevant and realistic for your organisation means this will actually work.

If part of your pragmatic view is that you want to utilise a service provider, then ensure this provider is held to the same, if not higher standard than you'd expect for yourself. Do your due diligence, understand the service contract, and ensure details are kept up to date. A great service provider can take the headache away completely when it comes to log management.

Log management, when done correctly, can do a chunk of the heavy lifting when it comes to security investigation. Whether delivered by you, or a third party, ensure you are getting the most from this investment.



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.