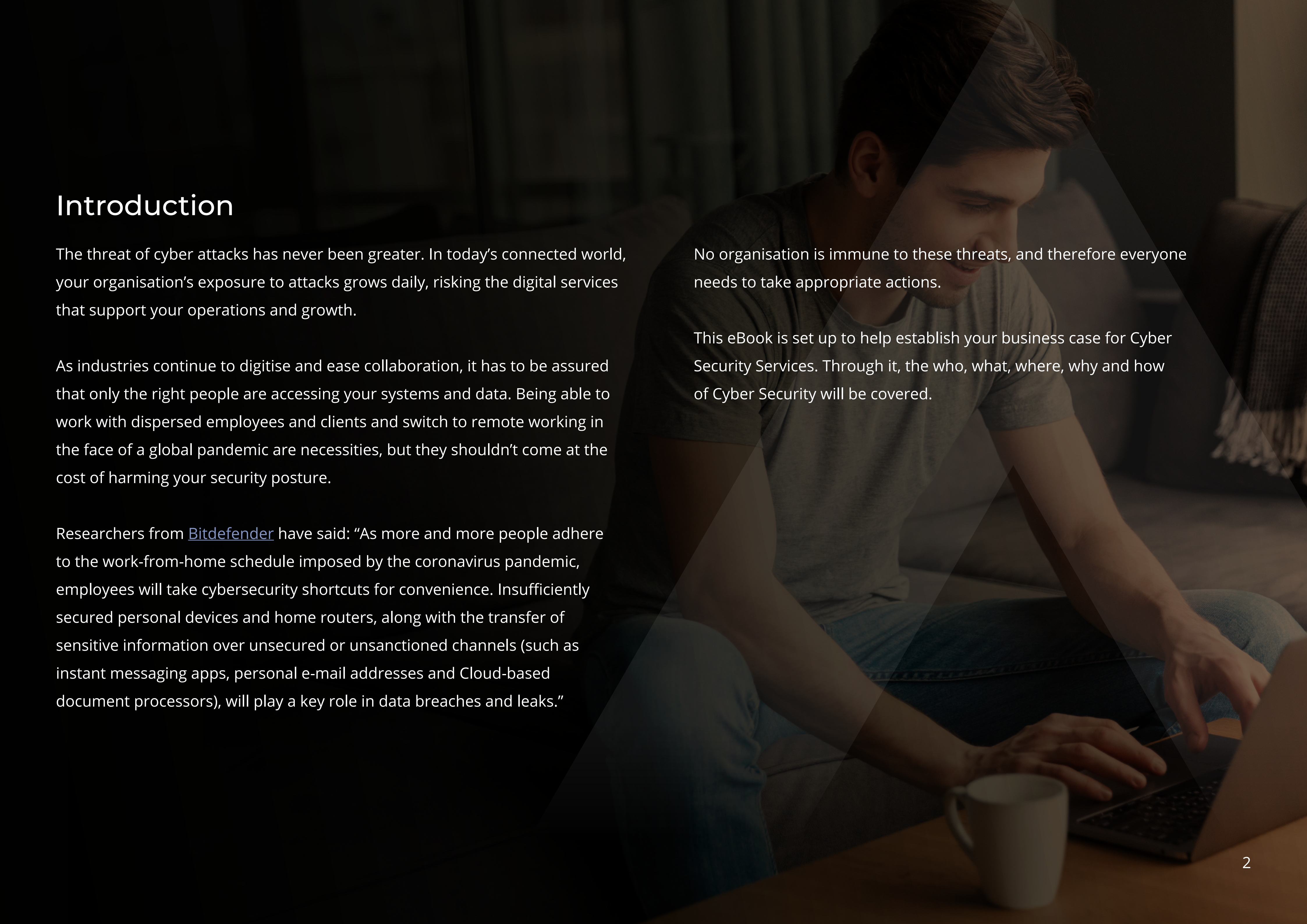
advanced

Cyber Security

The business case for Cyber Security Services

EBOOK



Introduction

The threat of cyber attacks has never been greater. In today's connected world, your organisation's exposure to attacks grows daily, risking the digital services that support your operations and growth.

As industries continue to digitise and ease collaboration, it has to be assured that only the right people are accessing your systems and data. Being able to work with dispersed employees and clients and switch to remote working in the face of a global pandemic are necessities, but they shouldn't come at the cost of harming your security posture.

Researchers from Bitdefender have said: "As more and more people adhere to the work-from-home schedule imposed by the coronavirus pandemic, employees will take cybersecurity shortcuts for convenience. Insufficiently secured personal devices and home routers, along with the transfer of sensitive information over unsecured or unsanctioned channels (such as instant messaging apps, personal e-mail addresses and Cloud-based document processors), will play a key role in data breaches and leaks."

No organisation is immune to these threats, and therefore everyone needs to take appropriate actions.

This eBook is set up to help establish your business case for Cyber Security Services. Through it, the who, what, where, why and how of Cyber Security will be covered.

Contents

Who are you securing?

This may seem a simple question with a very obvious answer. Your initial response to it may have been, 'I'm protecting my organisation'. But do you truly understand the full extent of what that means?

To protect your organisation means to look externally as well as internally. Particularly as remote working becomes more commonplace, the exposure of your devices and servers outside of standard operating hours needs to be taken in to account when assessing your security posture. No longer is equipment locked away in your offices, behind doors with codes and security personnel keeping an eye. Now, laptops containing data in need of protecting are in people's homes and networks are needing to reach more places that ever before. This can mean that it is no longer a case of trusting employees within working their hours and in their office, but also educating them so that their home environment is as secure as it can be.

For many organisations, it is not only internal employees that need to be thought of on this level, but also external clients and service users. Previously, those who use your services may also have been in their own offices and corporately secure environments, but now they are working from home. Again, this is opening up your networks and necessitating a greater reliance on the security practices of your customers.

This also extends to any providers that you may have. At the very least, they will hold data of yours and if they suffer a breach, that can put your organisation at risk. As the saying goes, 'it doesn't matter how good the locks on your doors are if you leave the windows open'.

60% of data breaches involve a third party, but only 52% of companies have security standards in place regarding such third parties.

Risk Management Monitor

There needs to be collaborative efforts across your whole supply chain, between your practices as an organisation and those of your providers, clients and service users. With such an approach, you can ensure that none are the weak link in the chain of operations and be confident in maintaining strong security postures.

This can work to strengthen your relationships through working together and be a great opportunity for developing best practice, establishing yourselves as technology leaders and sharing helpful insight across industries.

Ultimately, when looking at your Cyber Security strategy, you need to think about all of the access points to your data and systems. It is not simply a case of securing the actions of the people who work for your organisation and protecting them from attacks. You also must consider everybody that your company works with. Doing this properly will not only improve security now, but the sharing of information and ideas can lead to better preventative measures being put in place in the future.

What are you securing against?

The greatest success is often found in being proactive as opposed to reactive. Sorting things out once a problem has occurred is one thing, but stopping a negative active action before it takes hold is far more beneficial. If you can know what's coming and prevent it, you will be ahead of threats and keep ahead of your competitors.

The National Cyber Security Centre's (NCSC) Annual Report in 2020 identified key trends in the types of attack and their prevalence across UK organisations. They are as follows:

- Since 2017 there have been, among those identifying breaches or attacks, a rise in organisations experiencing phishing attacks (from 72% to 86%), and a fall in attacks involving viruses or other malware (from 33% to 16%).
- There has been a 10% rise in the number of incidents (723 v 658), and a 33% increase in the number of victims (<1200 v c900) this year compare to 2019
- Around a quarter of incidents the NCSC responded to in 2020 related to coronavirus
- The NCSC also handled more than three times as many ransomware incidents than last year

Phishing attacks are the practice of sending fraudulent communications, appearing to come from a reputable source. Often, these communications come through email, directly to the inboxes of your employees. The goal tends to be to steal sensitive data or to install malware on the victim's machine. This is one area in particular where the practices of your employees, suppliers and clients are vital to your security. If they engage with one of these emails then your organisation can be breached and your data stolen.

The other key attach the NCSC found is ransomware. An example of this is the WannaCry incident in 2017. Ransomware is malicious software that infects a computer and displays messages that demand a fee be paid to get the system working again or to have stolen data returned, it can lock a computer screen or encrypt important, predetermined files with a password. This type of attack requires technical services and tools that proactively work against the possibility of it.

86% organisations experiencing phishing attacks in 2017

The cost of doing nothing vs the cost of doing something

An incident can cause several types of loss. The 4 types are:

Productivity

This type of loss is relatively easy to quantify. It can be seen in a number of way, including the time an end user cannot complete a task because the app or site they were using to do so is down. Taking the average salary of that user and multiplying it by the number of hours the system is down and then multiplying that by the number of users affected calculates the productivity loss.
By reviewing past help desk tickets, an Annual Rate of Occurrence (ARO) can be produced which can be taken into account as a cost when purchasing fixes and/or new systems/software.

Rework

These events cause data corruption or data loss. The value of the data itself can be simple enough to quantify through how much it cost to obtain along with the worth of having it, though the amount of data that could be damaged would depend upon the event itself.

Legal

Legal fees are of high variability and are difficult to predict, however it is guaranteed that they will be present in any incident that results in a lawsuits, with additional liability costs a potential as well. Even if a lawsuit is won by the organisation that suffered the breach, fees will still need paying and this could get very expensive.

Business loss due to residual impact

Security incidents are often well-publicised incidents. The impact of this can be that potential customers/service users will decide against your organisation causing a loss of business. This is difficult to quantify, but the potential severity cannot be ignored.

To then make a decision about purchasing services or software related to protecting your organisation, other costs also need to be calculated and taken in to account alongside the costs of the software and/or services. This provides the true value and monetary impact of a project.

What needs to be factored in to a project as a cost includes:

IT costs
Server hardware and software costs

Implementation labour
Including any consulting hours necessary

Ongoing labour
The continued work of those managing systems

ARO
The number of virus infections that result in user downtime every year, which can be based on historical data from help tickets from previous years

SLE
The estimated cost to your organisation for each instance of an incident, this will likely derive from the calculations done in relation to the types of loss above

ALE
Determined through multiplying the ARO and SLE which determines the annual loss due to the incident

mARO
An estimation of the ARO once the security software/services have been implemented

mALE
An estimation of the ALE once the security software/services have been implemented

Productivity cost savings per year
This is mALE minus the mARO which shows the value of the software/services in decreasing productivity loss

Employees are still falling victim to social attacks

Financial pretexting and phishing represent **98%** of social incidents and **93%** of all breaches investigated

Security Magazine*

Source: Security Magazine

Where is your organisation weakest?

Cyber attackers will discover and exploit vulnerabilities in an IT system using a variety of techniques and tools. As the way we use technology develops, so too do the skills and knowledge of hackers.

Hackers were originally individuals with highly specialised knowledge of computer systems, consequently meaning that there were not many of them. However, some of these early hackers decided to make their knowledge available to others through software packages that include hacking tools.

The availability of such packages has significantly increased the number of people capable of performing sophisticated hacking. This in itself increases the vulnerability of your organisation, because more people doing the hacking means more chances of your being attacked.

However, there are key entry points for hackers that, once you know about them, can be specifically looked at to be secured and reduce successful attacks.

The 7 main points of entry are:

Compromised credentials

These tend to cover usernames and passwords and can often fall in to the hands of an intruder through phishing attacks, though it is not always humans who hold the credentials. Servers, network devices and security tools can as well. Any credential being shared with an unauthorised user can open your organisation up to attackers.

Weak and stolen credentials

Continuing with credentials, they do not have to be compromised for hackers to gain access to your systems and data. Weak passwords and obvious usernames can make it a simple guessing game for attackers that leads to success for them and damage for you.

Malicious insiders

Often, these are unhappy employees who expose private company information and/or exploits an organisation's vulnerabilities. Those with access to sensitive data and networks can inflict extensive damage through privileged misuse and malicious intent.

Missing or poor encryption

Without strong encryption being applied to data at rest, in-motion, and in-processing, sensitive information can be transmitted, meaning an attacker could intercept data storage, communication orprocessing and get access to sensitive data.

Misconfiguration

When a system is misconfigured or not fully configured, such as when default passwords are still in place, the devices and applications can present an easy entry point for an attacker to exploit.

Emails

Phishing attacks in particular are successful due to the lax email practices that many people have. They work by appearing legitimate, but often there will be something that gives them away. Employees need to be aware of these tells to ensure they do not open these sorts of emails.

Poor patching Patch

management that is inadequate can mean create loopholes in your IT infrastructure which act as invites for hackers who can exploit them to access your systems. Though patching can be a manual, time consuming process, it is necessary to protect your IT.

> “The need for cutting-edge cyber security has never been greater”
>
> Matt Warman, Digital Minister, UK Government*

Source: Matt Warman, Digital Minister, UK Government

Why now?

Cyber Security encompasses everything connected to protecting sensitive data – personally identifiable information, protected health information, personal information, intellectual property are some of those key things. Malicious agents understand the value of these things and are exploiting vulnerabilities to get to them at a rapid rate.

- A PricewaterhouseCooper survey of 3000 business executives from at least 80 countries showed that more than half of the world's companies are ill-prepared to handle a cyber-attack.

- Manufacturing, healthcare, transportation, government, and financial service are the five topmost industries targeted by cybercriminals.

- Hacking kits and tools used for ransomware, malware, identity theft, and other types of cybercrime are available in various online platforms retailing for as low as $1.

Why not now?

The ability to commit cybercrime has become more widely available with digitisation offering more opportunities to hack in to organisations as well. Adopting technology is coin with two sides. On the one hand, there are an abundance of benefits to be gained and grow from. Without technology the recent enforcing of mass remote working would be impossible, many processes would still be performed manually which takes up time and can cause problems when paper goes missing or is misfiled. However, on the other side, having your technology infrastructure underpin your organisation means that all it can take is one successful hack to have an incredibly negative impact.

As the effects of the COVID-19 pandemic have enforced, technology is now relied upon by more organisations in more major ways than ever before. Not only is the Internet of Things presenting more benefits in tandem with more threats, scalable platforming like the Public Cloud has increased in necessity which alters and expands an IT estate, adding more entry point opportunities for attackers. This does not mean that technology should be avoided at all, it means that cyber security has to be considered as a priority and invested in appropriately.

The cost of doing nothing in regards to Cyber Security is on the increase. The General Data Protection Regulation, as of March 2018, can fine up to a maximum fine of €20 million (about £18 million) or 4% of annual global turnover – whichever is greater – for infringements. If your data is stolen, this is only one of the costs you could be facing. If it is stolen as part of a ransomware attack, you could also be look at having to pay that ransom.

Other costs are covered in Ponemon Institute's Cost of a Data Breach Report 2020. These include, organisations spending $3.86 million (about £2.9 million) recovering from security incident with 52% of data breaches are caused by cyber attacks, and that malware is the costliest form of attack, with organisations spending $4.52 million (about £3.4 million) on average responding to such incidents.

Suddenly the costs associated with world class Cyber Security Services that can be proactive and reactive to such incidents seem more reasonable, don't they? Cyber attacks are not going away, they are only growing in prevalence which means your efforts against them need to grow in significance. Now.

Communicating cross-business value

It's not that long ago that Cyber Security was considered an IT job, but now, it's a job for everyone.

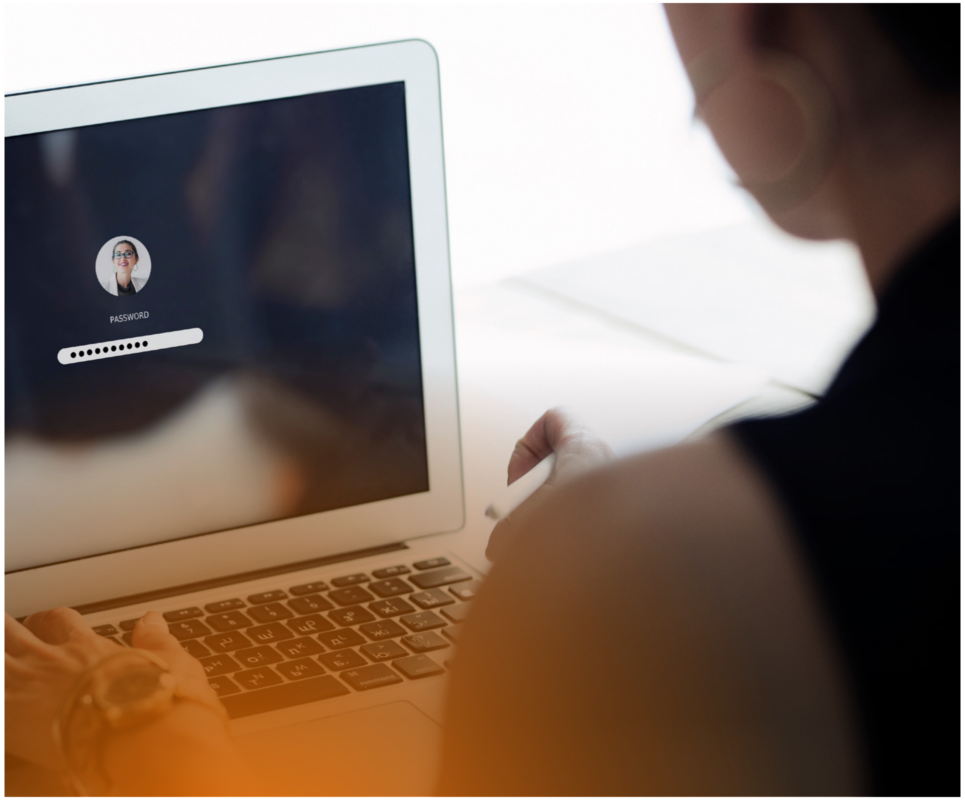
Much like how safe driving takes care of all passengers, developing and maintaining an effective Cyber Security strategy effects an organisation as a whole, and it ought to. Such strategies work their best when they start at an individual level. A whole organisation can be made vulnerable by one person connecting their infected personal device to the company network, or the system can infect other systems.

Using weak passwords for email or social media accounts and allowing insecure practices for storing passwords, such as post it notes stuck to computer screens, are easy ways for hackers to break in to accounts. From this, they can access personal information of other users that communicate through the account. One incident can grow exponentially in a short space of time and cause a lot of damage.

To combat this, Cyber Security practices should be developed in such a way that they can be followed easily and they adequately protect all. Though policies may be able to vary from one department to another due to the data handled and possible vulnerabilities, none can be ignored or determined to not be important.
A comprehensive Cyber Security program is required to ensure that every users needs are addressed in a way that does not compromise the needs of others.

This can be difficult to achieve, and there is certainly a lot to think about, so working with an expert partner can help a lot.

Without making these efforts, you can lose customers, suppliers, money, intellectual property, as well as the ability to function. It's worth it.



To the CEO

Your organisation needs to be secure to maintain its current status and to have any chance at growing in the future. The reputations of companies that have suffered breaches and lost the data of customers have been permanently tarnished, taking a lot to recover from. Due to this, there have been a significant number of organisation leaders that have resigned or been fired after a breach because they are ultimately held responsible. An effective Cyber Security strategy needs your sign off and support in orchestrating its requirements across the company. With a top down approach and consideration for all departments, new practices are better enforced and produce better results.

To the Procurement/Operations Lead

In regards to Cyber Security, how an organisation is operating and procuring are two vital elements to getting it right. This is not only for the Cyber Security Services themselves – providers you engage with should reference the NIST best practice framework, show awareness of the advice and work of the NCSC and be ISO 27001 accredited – but for all other operations and procurements. As has been made clear, there are multiple ways in which hackers can attack an organisation and maliciously enter a system. If technology erroneously procured, or operatively there are not secure enough processes in place, then an organisation will be left vulnerable. For a Chief Operating Officer to ensure financial strength and operating efficiency, Cyber Security Services need to be a priority focus.

To the CFO

Cyber Security Services can be a relatively small scanning project that does not require your specific sign off, or they can be large projects that span from scanning for awareness to responding to threats that would need your input. Also, practices such as having an incident response team, using encryption and having board-level involvement in risk management can result in big cost savings during breach incidents. Really, all projects should be brought to your attention, the financial implications of poor Cyber Security are too great for them not to be. Investing in Cyber Security Services doesn't only protect your organisation on a technical level, it all takes care of your revenue as well.

To the HR Lead

There are two main sides to why a HR lead should invest themselves in Cyber Security conversations and be a decision-maker in practices. The first is that the HR department, along with the Finance department, probably hold the most sensitive data out of all functions in an organisation. If your organisation is breached, the reputation won't only be damaged in a way that reduces customers, it will also be damaged in a way that puts talent off from joining. No one wants to work for somewhere that gets hacked. The other side, is that the HR departments plays a large role in the education of employees. Employees need continuous Cyber Security education that keeps they up to date with best practice and lets them know what to do in the event of a potential breach.

Summary

Facing an ever-evolving threat landscape can be incredible daunting. That is why we have developed a portfolio of Cyber Security Services that works with you from initial vulnerability scanning for awareness, right up to an end-to-end Managed Detection and Response offering, all forming part of our commitment to be the fastest to find and fix problems.

Justin Young, Director of Security & Compliance, Advanced

Our experience across numerous sectors, with organisations of all sizes, means we have a depth of knowledge that has led to a breadth of capabilities that are market-leading. Also, alongside frameworks built from our experience, we align ourselves to best practice from NIST and the NCSC, and are ISO 27001 accredited. We want to work with you, utilising industry-leading technology from partners including Alert Logic, McAfee and SureCloud alongside our world-class services to ensure your organisation can securely operate at its best, whatever the

In partnership with

ALERT LOGIC™ McAfee Microsoft Defender SureCloud.

advanced

We would love to hear from you

Find out more about how our Cyber Security services can help safeguard your business so you can focus on running your business.

Contact us

☎ +44(0) 330 343 8000

www.oneadvanced.com

✉ hello@oneadvanced.com