FROM RISK TO RESILIENCE

PROTECTING YOUR DATA UNDERSTANDING AND OVERCOMING TODAY'S CYBERSECURITY CONCERNS WITH HARBOR.

harbor

TAKING THE FEAR OUT OF CYBERSECURITY

Cybersecurity can understandably feel like a daunting topic. From the financial impact of cyber-attacks to the reputational damage they can cause, the consequences are well documented.

Fears are compounded by the inevitable media frenzy that accompanies high-profile attacks, and as a result of continually being exposed to the consequences, the cybersecurity industry can sell based on fear. Without realising it, we're now used to being unnerved into buying the latest solutions or products. But it doesn't have to be this way.

There are immediate things you can do to protect your organisation and we'd like to introduce you to some of them in this guide. We are going to look at the complexities of cybersecurity because they shouldn't be ignored. We will also explore how simple steps can make a big difference

So, let's take the heat out of the situation, take a step back, and without trivialising it, bring some practical, operational clarity to cybersecurity.

82%
of boards within UK businesses rate cybersecurity as a 'very high' or 'fairly high' priority[1]

THE TRUTH BEHIND THE TALES

76%
of customers said that cybercriminals succeeded in encrypting their organisation's data during a ransomware attack[2]

Today, there is a lot of talk about ransomware and its impact on organisations of all sizes. That's because an increasingly common output of someone gaining access to your environment and deploying ransomware is some form of data breach – most likely resulting in a threat actor being able to:

01 ENCRYPT YOUR DATA AND ASK FOR MONEY

02 DELETE YOUR DATA TO INTERRUPT OR STOP YOU FROM DOING BUSINESS

03 EXFILTRATE YOUR DATA TO USE IT FOR SOMETHING UNETHICAL OR MOST LIKELY, MAKE MONEY FROM IT

There are a lot of products on the market that promise to mitigate these ransomware threats in some way. The problem is that many of them are perhaps not as simplistic as the technology providers promote them to be. Providers will sell the dream of being able to recover data from a ransomware attack in a few simple clicks – but this isn't always the case. There is also a lot of confusion and misinformation about both the powers and capability of the products, and about the ransomware attacks themselves.

While ransomware is becoming increasingly prevalent, and its effects can be seismic, the reality is that there are different types of attacks, and we only hear about the ones that work. Rarely is there a headline in the news about an organisation being hit with ransomware and successfully recovering with no disruption to their operations.

Furthermore, ransomware attacks are not quite as common as some studies or reports would have you believe. For example, one vendor told us that they see, on average, just two successful attacks a week from around 6,000 customers. Consequently, we are not saying that you will be attacked, but our advice would be to prepare for one and work out how to recover from it.

Most organisations have a data recovery plan that will cover things like fire, flood or hardware failure and it is important to strategise for such events, but a ransomware attack is potentially more likely and something you should also have an approach for. Starting simple, like having a copy of your cyber recovery plan somewhere that can't be attacked, is the best place to begin.

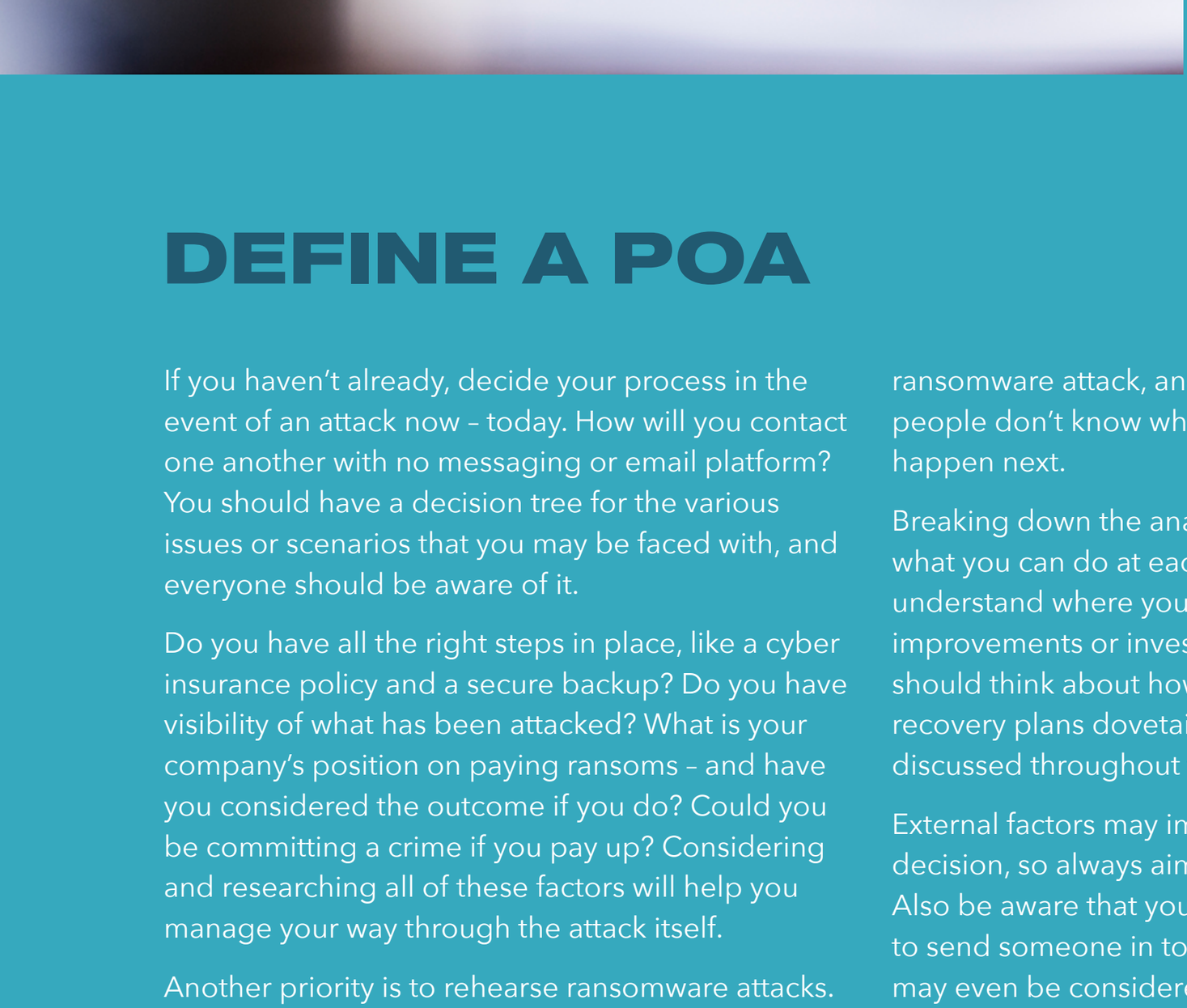
Remember that cyber criminals operate like businesses. If they believe the reward is large enough, they will concentrate more resources and effort on ensuring the attack is a success. Whereas, if the prize is small, they will often do the bare minimum, merely chancing their arm at a hit. Who you are and what business you are in should therefore be an important factor when calculating risk.

Root Causes of Ransomware Attacks:

36%
Exploited Vulnerability

29%
Compromised credentials

18%
Malicious Email



PRACTICAL WAYS TO PROTECT YOUR DATA

We are only human, and sometimes that means clicking on things that we shouldn't. Yet even though most organisations are aware of how phishing attacks work, a surprising amount only take minimal mitigation steps against it.

By being more switched onto the risks and looking at user activity, you can easily prevent, stop or minimise the likelihood of an attack. It's important to secure and manage your endpoints. Things like up-to-date anti-virus, web filtering and email link click protection can all help. Even the basic tools in Office 365 will help alert your users to a risk.

Educating your end users on the basics is vital because most will probably want to do the right thing but might not know what that looks like. You can help them with this and there are tools available to support with their education. The key is to communicate to the business why these things are important and what they will prevent. Teaching a company about cybersecurity might be the IT department's job – but everyone is responsible for doing their bit.

Housekeeping and the effectiveness of an admin access password rotation policy shouldn't be underestimated either. There are a number of simple good-hygiene factors that most people in IT know about, but simply don't get the time to do. In most cases, the only reason an attacker has achieved success is because of these little lapses; hackers aren't out there cracking AES256 encryption, they are mere opportunists looking to see if the admin account password is still 'admin'.

These small measures remain some of the best ways to guard against attacks. If you get the basics right, you can use your IT budget more effectively – rather than trying to buy your way out of a problem.

DEFINE A POA

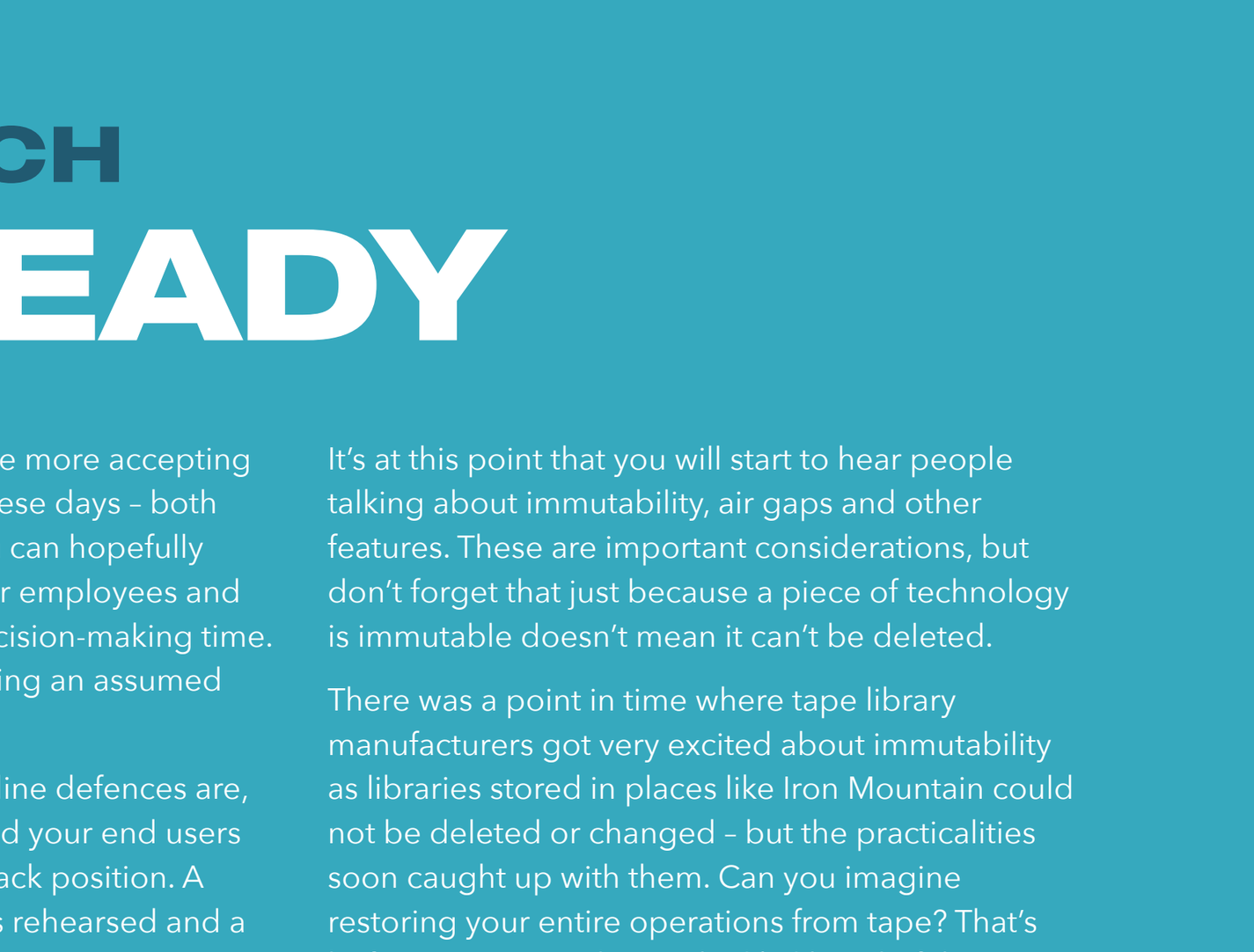
If you haven't already, decide your process in the event of an attack now – today. How will you contact one another with no messaging or email platform? You should have a decision tree for the various issues or scenarios that you may be faced with, and everyone should be aware of it.

Do you have all the right steps in place, like a cyber insurance policy and a secure backup? Do you have visibility of what has been attacked? What is your company's position on paying ransoms – and have you considered the outcome if you do? Could you be committing a crime if you pay up? Considering and researching all of these factors will help you manage your way through the attack itself.

Another priority is to rehearse ransomware attacks. Do it as a tabletop exercise with your board – go through it step-by-step and then look back at the decisions you made. At Harbor, we spend a lot of time educating people on what happens in a ransomware attack, and it is surprising how many people don't know what to expect, or what will happen next.

Breaking down the anatomy of a cyber-attack, and what you can do at each stage, helps you better understand where you need to make process improvements or investments. Additionally, you should think about how your existing disaster recovery plans dovetail into what we have discussed throughout this document.

External factors may impact your ability to make a decision, so always aim to 'expect the unexpected'. Also be aware that your cyber insurer might want to send someone in to take over. Your infrastructure may even be considered a crime scene depending on your line of business. Furthermore, there could be legislative or legal requirements in your sector that put time pressure on certain decisions you need to make. Put it all in your plan.



68%
of customers took between 1 week and 1 month to recover their data

BE BREACH READY

The good news is that people are more accepting of having a ransomware issue these days – both internally and externally – so you can hopefully rely on some good will from your employees and customers to buy you critical decision-making time. But we still strongly advise defining an assumed breach position.

No matter how good your front-line defences are, and no matter how well-educated your end users are, you should still have a fall-back position. A mindset of 'what if'. A plan that is rehearsed and a copy of your data somewhere secure.

It's at this point that you will start to hear people talking about immutability, air gaps and other features. These are important considerations, but don't forget that just because a piece of technology is immutable doesn't mean it can't be deleted.

There was a point in time where tape library manufacturers got very excited about immutability as libraries stored in places like Iron Mountain could not be deleted or changed – but the practicalities soon caught up with them. Can you imagine restoring your entire operations from tape? That's before even considering the likelihood of the tape still being readable. Here, it is clear to see that returning to normal operations as quickly as possible is crucial.

TECHNOLOGY, PEOPLE AND PROCESS

AS WITH MOST THINGS IN IT, PROTECTING YOUR DATA COMES DOWN TO THREE KEY ASPECTS: TECHNOLOGY, PEOPLE AND PROCESS. LET'S EXPLORE THEIR IMPORTANCE HERE.

THE RIGHT TECH YOU NEED

Technology is important, but it is not guaranteed to magically give you the outcomes you desire.

At Harbor, we work with industry-leading technologies in the data protection space – and we are highly experienced in optimising tailored services for our customers' unique environments. Working closely alongside you, we can make sure you are using the technology correctly, and that your people are responding efficiently to what the tools are telling them.

IT departments are always short on resource and backups can fail for any number of reasons. Keeping on top of the situation may seem dull, but it is fundamental in achieving peace of mind. The basic questions are the best ones: 'What do you classify as a failed backup job?'; 'How many failed backups have you had?'; 'How old is the last backup of your most crucial server?' We can help at this management level and take the stress away.

TECHNOLOGY

Technology is usually the first thing an organisation focuses on as it is easy to issue an RFP with a series of requirements and problems that need solving. The RFP will include key points like it must have 'X' feature or 'Y' reporting capability, but rarely will it state the goals and outcomes they are trying to achieve. Many vendors also focus on features, selling things like 'automatic ransomware detection'. But what does that actually mean and what do you need to do to make it work?

Twenty years ago, the spotlight was on protecting your data centre from a high impact yet ultimately low likelihood event. Around ten years ago, cost savings were key ("x86 servers and virtualisation are cheap, so why not re-utilise the assets you already have?"). Now though, hardened, custom-built backup appliances are very much in vogue and for the reasons we have outlined, you can see why.

There is a lot more software as a service (SaaS) based technology now too, such as Rubrik and Druva. Being SaaS means they can quickly remove an attack vector as they are cloud native. They also come with handy features like automatic deployment of new features and single panes of glass.

Additionally, there is a continued rise of intelligent services, with artificial intelligence (AI) and machine learning (ML) being used on the metadata that the platform garners to enrich offerings. Examples include storage arrays that can provide you with insights on what you are using and how you are using them to improve performance or service; and applications that provide threat hunting in your backup data. They all have built-in capabilities that can be shared across your wider IT landscape, enriching your experience and oversight into your IT landscape.

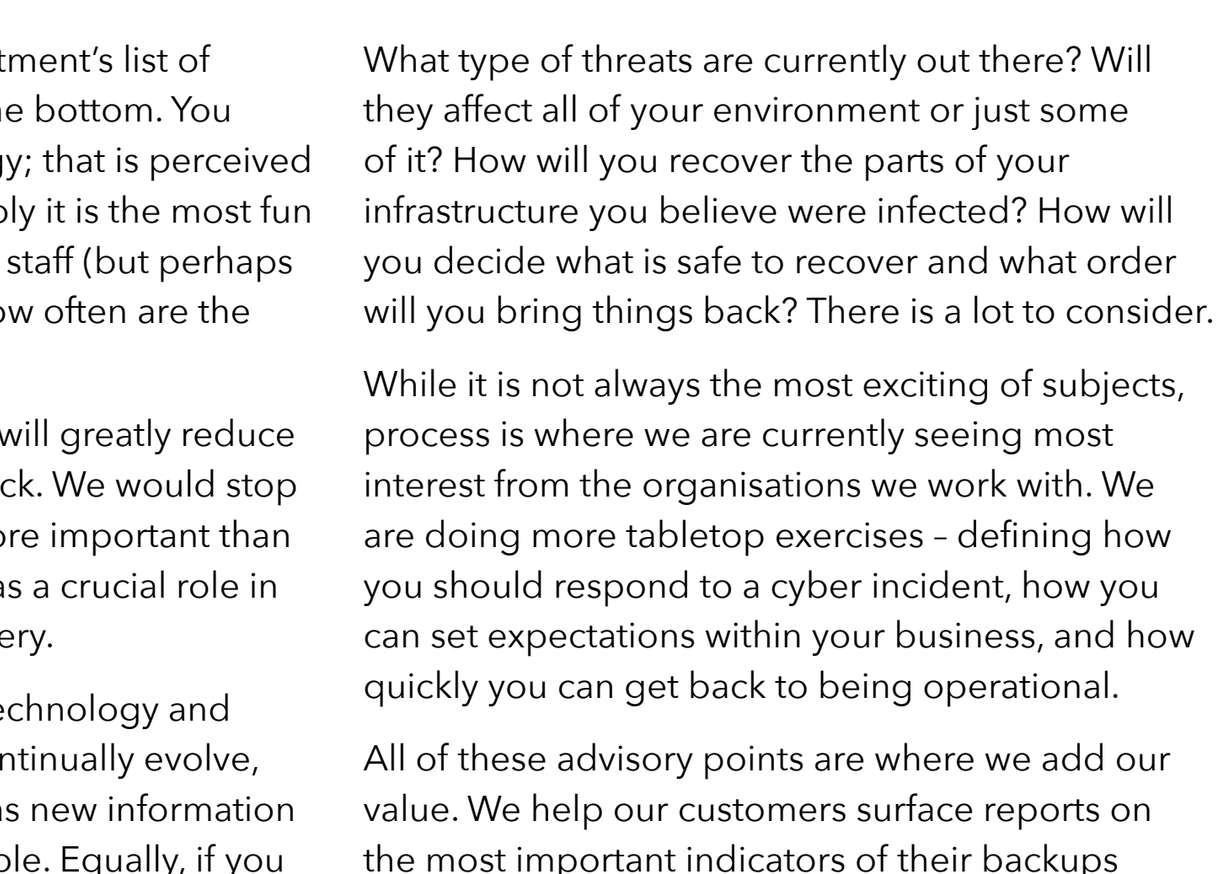
PEOPLE

Adopting new technology is not just about the cost of the technology itself, it is also about bringing your teams up to speed with the changes. It is the time required to become confident in using the tools, so that when you find yourself in a situation where you are relying on them, your people can deliver.

On top of this, maintaining a dedicated team is challenging. Experience is everything, so you need to find people who have been there before – and the more diverse their experience the better.

To help remove some of this pressure, we help customers daily. Not only with the basics like ensuring backup jobs are running smoothly and that solutions are patched and up to date. But also with cyber recovery, best practices, deploying new apps and services into new environments, and making sure they are properly protected.

We make sure you can recover. We provide support in those boardroom conversations about what to do in the event of an attack, and we provide an agnostic, experienced voice.



PROCESS

As you go through your IT department's list of priorities, process often falls to the bottom. You always review and buy technology; that is perceived as the most important bit (arguably it is the most fun too!). You train and educate your staff (but perhaps not as much as you need). Yet, how often are the supporting processes updated?

Having good processes in place will greatly reduce the risk of a successful cyber-attack. We would stop short of saying that process is more important than the technology, but it certainly has a crucial role in getting you to a successful recovery.

Therefore, if you have the right technology and people in place, it is critical to continually evolve, update and test your processes as new information and intelligence becomes available. Equally, if you don't have access to the latest technology, or you are short on people, the processes you have can still go a long way to protecting your business from an attack.

What type of threats are currently out there? Will they affect all of your environment or just some of it? How will you recover the parts of your infrastructure you believe were infected? How will you decide what is safe to recover and what order will you bring things back? There is a lot to consider.

While it is not always the most exciting of subjects, process is where we are currently seeing most interest from the organisations we work with. We are doing more tabletop exercises – defining how you should respond to a cyber incident, how you can set expectations within your business, and how quickly you can get back to being operational.

All of these advisory points are where we add our value. We help our customers surface reports on the most important indicators of their backups – and more.

THE HARBOR APPROACH TO CYBERSECURITY

The responsibility to protect your organisation's data can feel overwhelming. Aside from dealing with the threat of increasingly sophisticated attacks, finding the right technology, people and processes to suit your needs can seem like an insurmountable challenge.

However, what we have taken you through here hopefully shows that ransomware is not necessarily something to fear. Instead, there are a number of simple things you can do to mitigate much of the risk. Like any kind of IT incident, the more prepared you are, the more successful you will be. Having someone with experience to support you will greatly help the outcome.

If you want to make a start now, follow this simple checklist to start improving your cyber resilience posture today:

OUR SIMPLE DE-STRESS CHECKLIST

01 REHEARSE A RANSOMWARE INCIDENT WITH YOUR BOARD

Get all your key stakeholders and decision makers in a room together and take them through what will – and what can – happen and how the business should respond. This is also a great time to test your recovery plans work!

02 REVIEW THE INTELLIGENCE OF YOUR BACKUP AND RECOVERY PLATFORMS

Firstly, are all of your backup jobs running successfully? Unless your team is ignoring failed job notifications, everything usually backs up. It's important to be able to intelligently recover in the event of an attack. Carry out periodical practice restores to test the process and ensure that you are able to recover 'clean' data in a safe environment.

03 MAKE SURE THE RIGHT PEOPLE CAN ALL COMMUNICATE CLEARLY -IN ANY EVENT

It's crucial to be able to keep in close contact during the event of a ransomware attack that takes out your corporate messaging systems. Decide how you will do this.

04 HAVE A COPY OF YOUR PLAN SOMEWHERE THAT WON'T BE ENCRYPTED

If you don't know how to do this, there are many providers that offer this kind of service.

05 REVIEW YOUR BACKUP TECHNOLOGY

What protection does your current technology offer against cyber-attacks? Is it immutable and air-gapped from your environment? Can it help to tell you what you can recover and what has been compromised? Are all your key workloads protected – and how easy is it to bring them back?

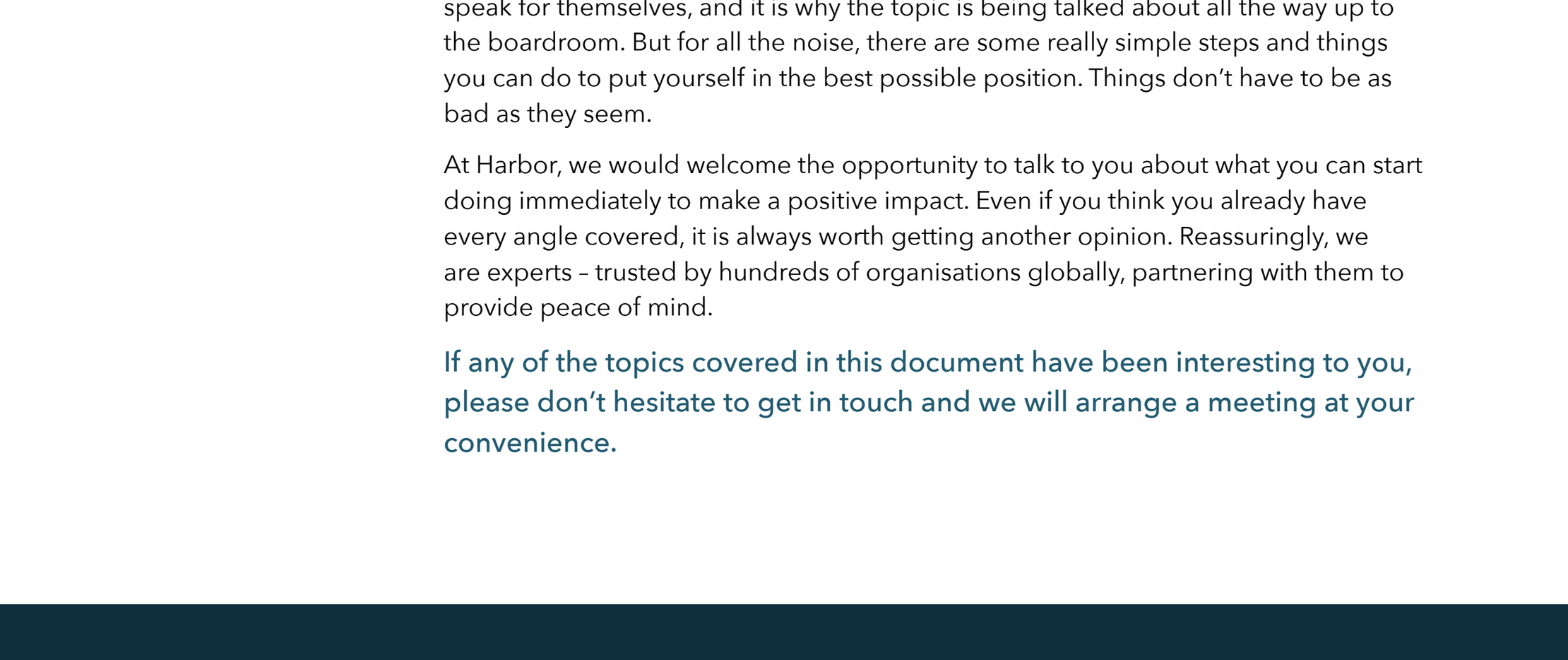
06 ENABLE 2FA ON ALL ADMINISTRATIVE ACCOUNTS

If you haven't already, ensuring all administrative accounts have either 2FA (2 Factor Authentication) or ToTP (Time-based one-time password) enabled is a simple yet highly effective way to better protect yourself.

"From the first meeting, there was a reassurance about the approachability and competence of the team involved in the sales-pitch process. Harbor had clearly spent the time to understand our RFP. They weren't giving us boilerplate responses to the questions, but instead came prepared to challenge some of our assumptions and requirements. Harbor stood out from the competition, because they proved themselves as true experts and told us exactly what we needed to improve on.

There's certainly a feeling of transparency, openness and an affability about the team we met – this reassured us that Harbor are the right company to work with."

Knight Frank



WHERE TO NEXT?

There's no doubt that the potential impact of a cyberattack is alarming. The figures speak for themselves, and it is why the topic is being talked about all the way up to the boardroom. But for all the noise, there are some really simple steps and things you can do to put yourself in the best possible position. Things don't have to be as bad as they seem.

At Harbor, we would welcome the opportunity to talk to you about what you can start doing immediately to make a positive impact. Even if you think you already have every angle covered, it is always worth getting another opinion. Reassuringly, we are experts – trusted by hundreds of organisations globally, partnering with them to provide peace of mind.

If any of the topics covered in this document have been interesting to you, please don't hesitate to get in touch and we will arrange a meeting at your convenience.

WE CAN BE YOUR TRUSTED ADVISOR. TALK TO US TODAY.

harbor

REACH OUT TO US AT: SALES@HARBORSOLUTIONS.COM
FOR MORE INFORMATION, VISIT OUR WEBSITE.

REFERENCES

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
[2] Sophos Ransomware Report 2023