CSI

CELEBRATING 40 YEARS

MAXIMISE CYBER SECURITY AND DATA STORAGE CAPABILITIES

IBM

Platinum Partner

Cyber attacks are frequently making headlines and damaging organisational reputations. Targets vary by industry, size and scale, but they all aim to cause disruption, steal data - and even hold it to ransom. To combat the problem, businesses are facing rising cyber insurance premiums and the need to build robust business continuity and operational resilience plans to remediate fast, should the worst case scenario become a reality.

The destructive impact a cyber attack can have, with costs in the millions proves why investment in cyber security is so important – both in terms of detection and mitigation of cyber attacks, but equally in data storage and restoration in the event of an incident.

In this whitepaper, our experts share insights to further understand some of these challenges and how we can get the most out of our cyber security and data storage efforts.

Organisations face cyber threats daily, of differing types and severities, and the volume of some have been significantly increasing in recent months. This is partly encouraged by the greater digital shift we've seen as a result of the pandemic and wider adoption of remote, hybrid and digital working.

It is a very interesting area in terms of data security. The rise and acceleration in attacks – malicious attacks – which we're hearing about is frightening, across all industries.

For complex and regulated industries including financial services and public sector, with the personal information and services, it can be even more frightening in terms of what could happen, if the worst happens.

Businesses are turning to specialists such as CSI, and technology vendors like IBM, for help to find and implement solutions to combat threats and protect customers' data.

Ultimately, the big difference right now is that it's not just about the protection. It's about how you recover, because there has to be an acceptance that you may get hit with a cyber attack and organisations need to know that they can recover properly.

It is a pattern backed by comments by Jeremy Fleming, Director of GCHQ: "This year (2021) we have seen countless examples of cyber security threats: from state sponsored activity to criminal ransomware attacks.

"It all serves to remind us that what happens online doesn't stay online – there are real consequences of virtual activity."

Reaching that position where an organisation can work not only to reliably detect and counteract cyber threats, but also to have confidence in its ability to recover quickly and safely should something manage to breach the defences, requires an open attitude (often, it requires identifying risks and weaknesses, not as a shortcoming with which to bemoan the organisation but as a way of addressing points of risk) and collaboration with industry.

It is an area where CSI has been able to help a number of customers. We've done a lot of consultative work within regulated industries around advisory services. This has been identifying gaps and analysing areas of an organisations' risk, and what they see as their crown jewels in terms of data, systems or intellectual property.

From there, the risk assessment can identify what is a high or low priority, and what additional services may be needed to bolster security, including training employees on best practices.

We can see where you could address some of those gaps through technology, with CSI's team of experts able to offer a managed services partnership to our clients to fill gaps if needed.

ENABLING YOUR WORKFORCE

That partnership also helps provide organisations with solutions to one of the few big challenges it needs for effective cyber security and data storage: an appropriately skilled workforce.

In many sectors there is a shortage of qualified, experienced IT professionals, with competition from the private sector often ratcheting up salaries and working in conflict with often tight public sector budgets.

As such, introducing the expertise of a third party provider can be an effective way of adding these capabilities into the organisation without significant or unsustainable salaried outlays.

Another big challenge for cyber security is the always-on nature of today's digital systems. While employees may typically work a standard 9-5 work day, cyber security systems do not - and nor do cyber criminals.

Security capabilities and monitoring need to be on hand 24-hours a day, often requiring the support of specialist IT organisations, like CSI, who operate a 24/7 security operation centre (SOC) to offer this assurance.

Cyber security is not about 'if' but about 'when'. People are quite accepting of that fact, but one of the challenges we see regularly is the skills shortage.

In order to understand what risk your organisation is susceptible to; you need to have visibility. If you haven't got visibility to see what's going on, then you haven't got the intelligence you need to make a decision to act on.

The technology and tools are out there. Services are available. But in order to have that intelligence and understanding of what the problem is, it's really important to identify the issues and bringing in security experts can be key where there is such as a skills shortage internally.

This is where the value-add comes in from resellers and suppliers, to come in and deliver that high level of service, and help businesses get access to all the same skillsets.

Having an external set of eyes look and cast a second opinion, because the people in the organisation are looking at their infrastructure every day and may not see the gaping issue that an external party could identify - could make a big difference.

PROCEDURAL BEST PRACTICE & IMPROVING THE TECHNOLOGY

With that said however, addressing the staffing side of cyber security is only going to be effective if organisations ensure that they are implementing procedural best practice across their organisation, as well.

This can include staff-related steps, such as training employees to remain vigilant to cyber threats and to feel comfortable to report incidents or concerns if and when they do occur, allowing a quick response.

But equally, it can be steps involving the way organisations handle their team and responsibilities, to protect the data. It can't be overlooked that some cyber attacks can also involve internal actors playing a role, either intentionally or not.

It is crucial to maintain a separation of different duties, making sure there is no single person in control of everything that is going on.

It is not just about building up walls and stopping things from happening. People are going to get through those walls with malicious intent, but equally people inside the walls might have that same bad intent.

We're seeing 'ransomware as a service' these days. Anybody with a bit of money can come up with the idea and go attack someone.

As such, measures to spread responsibility around the team can help safeguard the business from internal actions leaving the organisation vulnerable. As well as helping guarantee that in the event of an incident – an often high pressure environment – responsibility for reacting and restoring normal service doesn't funnel down to a single point or individual who could become easily overwhelmed.

There are many different aspects to think of in terms of your data protection strategy. Accepting the fact something might go wrong, whether malicious or not, is important in creating a clear strategy.

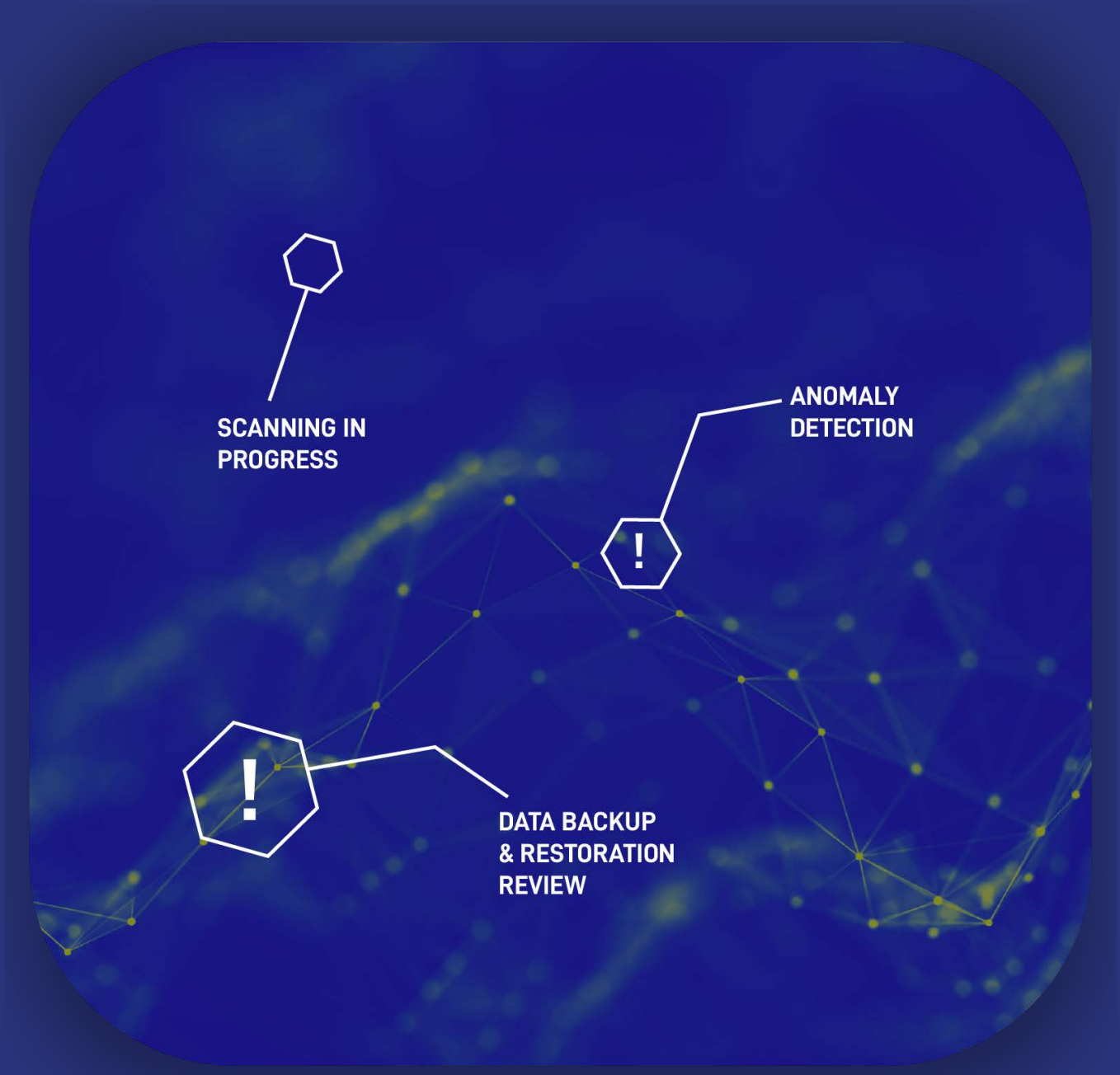
A clear plan on how you recover after an incident is absolutely critical.

We work closely with partners like IBM to bring technology into the mix which makes it easy to safely store data and give our clients options to be able to recover. The technology is there, but it is very complicated and bespoke for every single organisation.

Budgets are not growing, and likely most organisations are not awash with technology, people or skills. We're trying to make it as easy as possible by adding a consultative approach.

Introducing external skills and expertise also allows businesses to benefit from the innovations and stress-testing of systems and processes. For example, the financial services industry is regularly at the forefront of tech innovation – perfectly understandable, given the sensitivity of the information they hold – and as the technology becomes more commonplace in other sectors, demand increases and is able to facilitate a fall in pricing.

Things have been developing for decades. More recently, there's been a movement from a dual site setup to a three site, and now a four site setup with the big banks. For them, it has to also include immutable storage and ways to protect against ransomware.



THE POWER OF EFFECTIVE DATA STORAGE

A robust, effective defence against cyber threats is only attainable if the data storage, recovery and resilience pieces are also given equal attention. This is where CSI and IBM have been able to make particular strides, helping to educate people about the importance of storage in the conversation and support those organisations to deliver it.

With data backup and data security, you see so many organisations back up their data, even in some instances to third party clouds, but how many organisations test recoveries on those backups? It's likely a very small proportion.

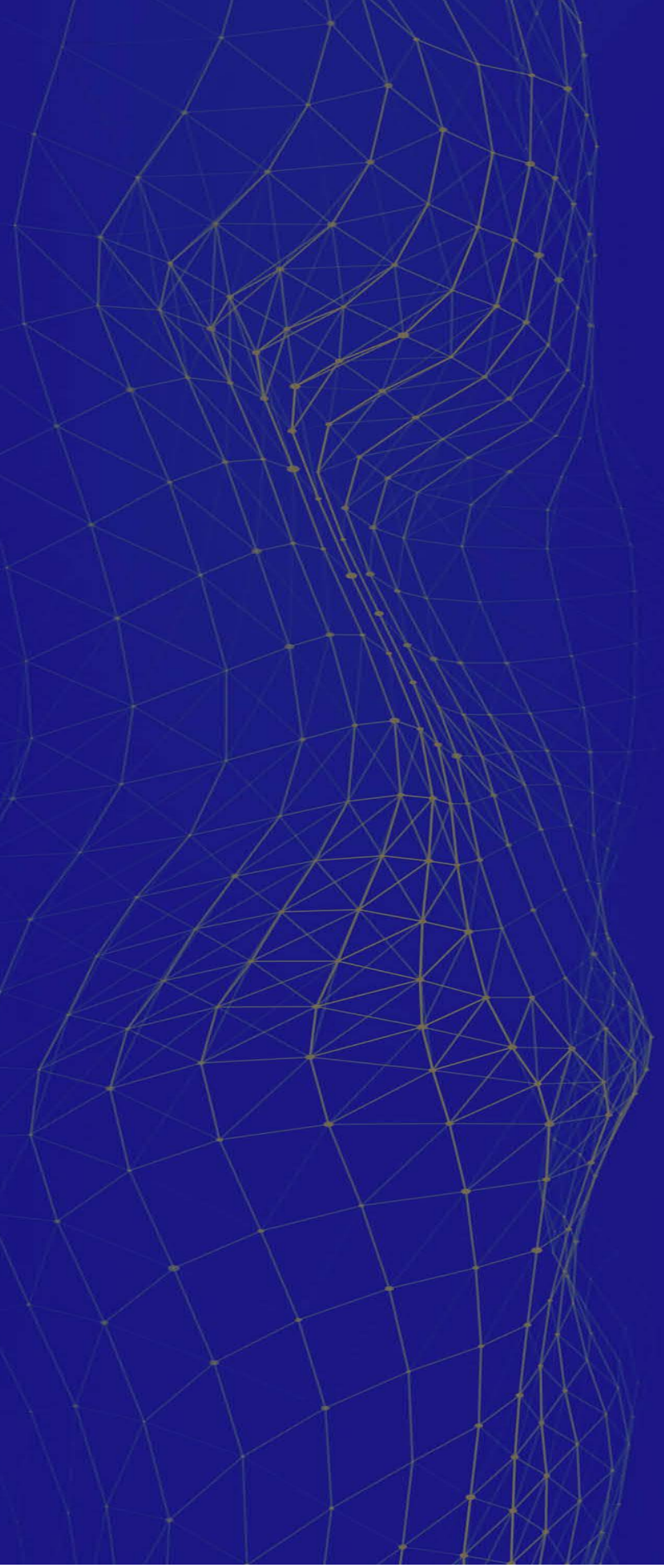
That is part of the problem with ransomware. Organisations are doing their backups in increments – scheduled daily, weekly, monthly – and with today's ransomware you can have a type of attack which is 'slow and low' in the sense it comes in, sits for a while, propagates around the network, then detonates and formally downloads the payload to try and carry out the infection.

By that point in time, your backups include malicious software in the backup data that you need to restore from.

Having an 'air gap' type solution to remediate those recoveries of backups is really important.

Data recovery can help address ransomware breaches and attacks by having it completely separated and having a separation of duties in terms of who controls that data.

Then there are the steps to recover, which includes things like a clean room to check and validate you don't have a problem, or clean it out if there is a problem in the data. It needs a lot of thought and consideration around the whole process.



FROM RECOVERY TO FUTURE PREVENTION

As concerning and vast a task as it sounds though, if put in place correctly, then an organisation can continue its operations with the confidence that not only is it doing all that it can to protect against cyber threats, but in the event that an attack is successful, services can be resumed quickly and safely.

It can also improve early response with those recovery capabilities being fed back into proactive monitoring and earlier responses going forward.

From a data storage perspective, clean-up and remediation after you've been hit by a cyber attack and are looking to get things restored is key.

With that data, we can start to see trends. A lot of the IBM products we utilise have built in alerts which will say something doesn't quite seem right. Or that there has been a big change in the amount of data in a specific location. The greater the visibility the better protected the data will be in the future.

With advances in technology we hope to see more detection capabilities to make cyber security easy.

CSI UK Head Office

CSI House
2940 Trident Court
Birmingham Business Park
Solihull Parkway
Birmingham B37 7YN

CONTACT

info@csiltd.co.uk
www.csiltd.co.uk

CSI
YOUR PERPETUAL EDGE