Building Cyber Resilience for 2023 and beyond

A guide for business leaders

- Cyber resilience defined
- The current threat landscape
- Barriers to resilience
- Building resilience: steps to take

Millennium Consulting

There was a time when cyber was seen almost exclusively as an IT concern. These days, cyber security and risk management need to be viewed as a board-level issue, directly impacting finance, compliance, operations, customer relations - and indeed, every corner of the business.

The cyber security basics - measures such as systems protection, security infrastructure, user controls and safe data handling - are as crucial as ever. And as threat actors and their methods evolve, there will always be the need to ensure your cyber security toolkit is fit for purpose.

But alongside cyber *security*, it is also vital to focus on cyber *resilience*. This is the realisation that - try as you might - not every threat can be stopped and not every risk can be entirely mitigated. Resilience describes your ability to anticipate, prepare for, withstand, respond to and recover from whatever may be around the corner.

Here's a closer look at the need for resilience in the context of the current threat landscape, the barriers to it, and the steps required to build it.

Millennium Consulting

Cyber resilience defined

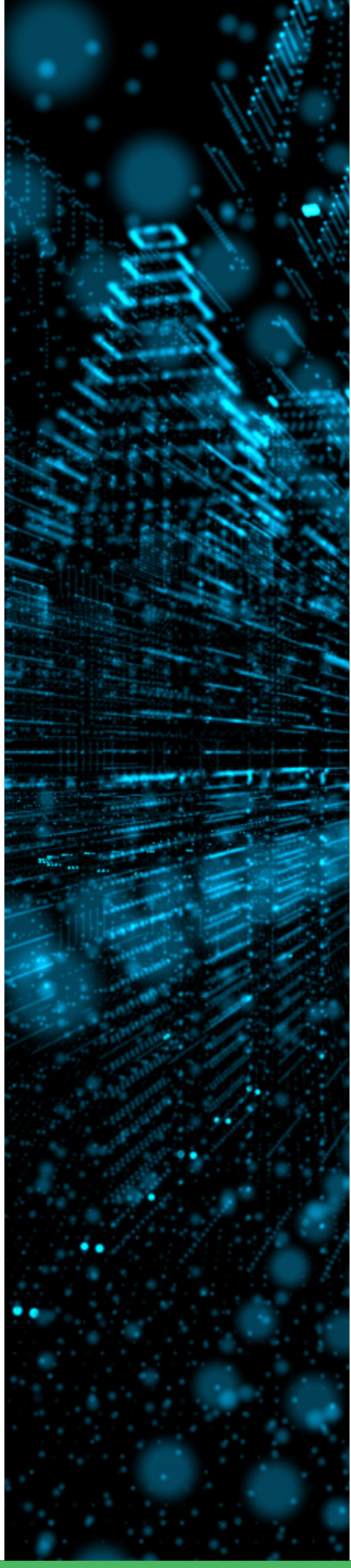
Almost 75% of organisations have experienced cyberattacks (Marsh and Microsoft, The State of Cyber Resilience report, 2022).

In late 2021, 81% of CISOs said “staying ahead of attackers is a constant battle and the cost is unsustainable”, compared to 69% a year earlier (Accenture).

The standard approach to cyber security is often compared to a kind of cat-and-mouse or whack-a-mole. As operating models change (through remote and hybrid working, for instance) or as business strategies shift (e.g. through digital transformation, new product offerings, markets or supply chain arrangements), threat actors hone their tactics and try to exploit new vectors. It’s the job of security teams to try and keep up.

The cyber resilience approach recognises the fact that even with state-of-the-art prevention measures in play, no organisation can ever expect to thwart all of the threats out there, all of the time. You should, of course, still invest in measures such as threat-detection software, employee cyber training and addressing software vulnerabilities. But it’s also important to take an ‘assume breach stance. This involves the following:

- Accept that a breach is not just possible, but likely
- Assess how and where a breach could cause impact or loss to the business
- Enact measures to ensure any impact or loss is minimised
- Ensure essential functions remain viable during and after a breach
- Consider how business functionality can be restored as quickly as possible following an attack



The current threat landscape

These are some of the most commonly encountered cyber threats that businesses need to be aware of:

Ransomware attacks

Ransomware attacks - i.e. malware designed to deny victims access to files unless a ransom is paid - remains an ever-evolving threat. Recent research from NordLocker suggests that UK businesses currently suffer the third highest rate of ransomware attacks globally, behind the US and Canada. More than a third of UK attacks are the responsibility of two major gangs: Conti and LockBit.

Businesses can increase resilience and security against this form of threat through a combination of robust perimeter shield measures (e.g. malicious URL blocking, email server filters and systems monitoring). A backup and recovery plan is essential, as is user training to educate users to spot and avoid dangerous links and attachments.

Phishing and social engineering

Phishing is a very common attack route for gaining sensitive information and for launching ransomware and other types of malware attack, including spyware: software capable of logging user activity and accessing credentials, without the victim being aware of any breach.

Typically with phishing, fraudsters disguise themselves as legitimate organisations and recipients are invited to disclose information, open attachments or click on links. With social engineering and so-called 'spear phishing', criminals will do their homework, - e.g. carefully researching the details of key insiders, perhaps researching clients and suppliers, enabling them to craft much more convincing bogus communications.

Anti-phishing strategies include filters and anti-spam capable of blocking traffic from untrusted sources, training and enforcement of robust policies governing disclosure of sensitive information.

Hybrid and remote working

Post-pandemic, many organisations have decided to retain a hybrid working model, with employees splitting their time between home and the office. From a cyber perspective, this means a much wider and more fluid perimeter to manage.

Measures to adopt include mobile device management (MDM) software, which makes it easier to deploy, secure and monitor scattered endpoints, including remote backups and updates. The use of virtual private networks (VPNs) may also be appropriate, to provide encrypted access between remote users and the company network. Careful consideration also needs to be given to hardening access against unauthorised users, while still enabling employees to do their jobs. This may involve use of internal firewalls to cordon off externally accessed systems from particularly sensitive areas of the network and multi-factor authentication.
From a resilience perspective, one of the biggest risks of remote working is to drift into an 'out of sight, out of mind' mentality. Employees need to know that wherever they are based, the same rules on cyber hygiene - e.g. use of unauthorised apps on hardware used for work, password sharing and opening emails and links from unfamiliar sources - are always adhered to.

Cloud security

Around three quarters of enterprises and half of smaller businesses use cloud infrastructure or hosting services. 94% of businesses use at least one cloud service. Key security benefits of the cloud include automatic deployment of security updates by cloud providers, 'failsafe' solutions for disaster recovery, and less risk of downtime.

However, greater reliance on cloud infrastructure and software does not negate the need to secure your own network. Most breaches - including cloud-related ones - occur as a result of human error, particularly misconfiguration of solutions at administer level, and failure to enable the various access and identity control tools that come with the solution. Careful choice of cloud service provider is crucial, too. Look at factors such as verified uptime statistics, resilience measures in place around backup and recovery, as well as the supplier's reputation within your industry.

Supply chain attacks and breaches

From manufacturing partners through to potentially large web of logistics suppliers, most large organisations rely on a network of third parties in order to deliver their core offerings. The benefits of this in terms of cost and efficiency are clear. The flipside however, is that a cyber breach involving one or more of your partners can have significant consequences for your business. The risk can be categorised in three ways:

- A cyber attack is suffered by a core supplier, impacting their operations, and preventing you from delivering essential products and services.
- An attacker exploits a vulnerability in one of your supplier's networks, thereby allowing the attacker to move laterally from that network and into your own.
- If you are using third-party products in your own operations (IoT or M2M devices, for instance), a vulnerability embedded in such a product may compromise your network.

To build true cyber resilience, you need to go beyond the boundaries of your own organisation to consider the entire supply chain. This includes putting in place cyber assurance processes; notably, by ensuring that your partners' cybersecurity strategies are aligned with industry standards (e.g. ISO27001 or NIST) and that they have credible and verifiable plans in place to mitigate risk and ensure operational continuity.

Barriers to resilience

People as the weakest link

Around 80% of successful cyber attacks involve criminals taking advantage of human error. Training is essential, but the fact is that not even the most tech-savvy employees are immune to inadvertently sending a file to the wrong recipient, or falling for a sophisticated spear-phishing attack.

Automating processes (routine invoicing processes that involve disclosure of sensitive financial information, for instance) can significantly reduce these human risks. However, you need to be careful with your choice of solutions used, to avoid merely shifting risk from the human level and centralising it in your systems architecture. N.B. when you are planning a major software implementation such as finance management or enterprise resource planning (ERP), your implementation partner should always take into account your cyber resilience priorities to ensure a best-fit solution for your needs.

Interdependency and connectivity

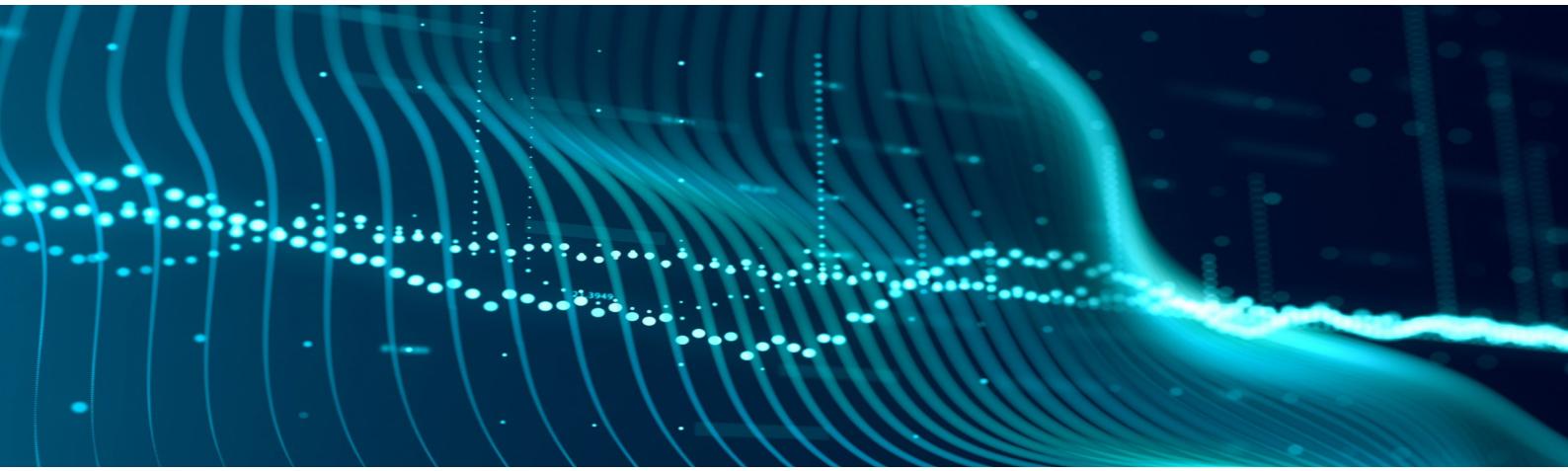
The number of new devices in play across your business, the location of those devices, the applications used, systems deployed and the sheer amount of data you control: in all likelihood, these have all increased significantly over recent years. The evolution of a complex and interdependent ecosystem makes it increasingly difficult to manage your cyber risks.

These risks can be mitigated by developing a coherent data strategy; one where data is stored, processed and shared in an efficient and secure way.

Talent shortage

A recent survey by the UK's National Cyber Security Centre suggests that 51% of private sector businesses have identified a shortage of technical cybersecurity skills. More than a third of businesses struggle with the basics of cyber, such as firewall configuration and malware detection. Cyber security can, of course, be outsourced. However, the perceived loss of control (and expense) that full outsourcing involves may mean that this is not a particularly attractive long-term option for many organisations.

As a long-term solution to scale up your in-house capacity and reduce reliance on third parties, start thinking now about onboarding junior employees through training programmes, apprenticeship schemes and targeted professional development.



Building true resilience: 3 steps that the entire business should be taking

1. Look at cyber resilience in the context of wider organisational resilience

Too often in the past, cyber has been treated as a distinct set of technical problems that non-specialist board members are quite happy to leave solely to technical managers and information security specialists.

Events of the last few years have led many business leaders to widen their perspective. In fact, Gartner estimates that by 2025, 70% of CEOs will be mandating a culture of organisational resilience to survive coincident threats from cybercrime, severe weather events, civil unrest and political instabilities. After all, if there's one thing we've learned recently, it's that big events rarely happen in isolation - and it's even more rare for their consequences to be confined to distinct pockets of the organisation.

To build this resilience, organisations firstly need to define what resilience means in the context of their own operations. What are your 'must have' functions to ensure core continuity in the event that an emergency hits? Based on these priorities, what level of protection should be afforded to different categories of assets, and in what order should they be restored during any recovery procedure?

Businesses also need the ability to ask 'what if?' and get answers they can trust. For instance, what if customer-facing systems were disabled for an hour, week or month? What would be the operational and financial implications of this? It's only through looking at cyber in the context of the wider business can you start to produce an effective, resilience-focused response and recovery plan.

2. Start building cyber into your wider decision-making processes

Some of you may have come across the concept of secure by design. It's the idea that you shouldn't develop a product and then add security mechanisms later on as an afterthought. Rather, security should be hardwired into it on a foundational level.

Cyber-aware business leaders, finance officers and procurement are taking a similar 'secure by design' approach to commercial decision making. Gartner estimates that by 2025, 60% of organisations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements. For things like mergers and acquisitions and vendor contracts, it's important to look carefully at potential partners' cybersecurity procedures as an integral part of the opportunity assessment process: a deal breaker, rather than an ancillary concern.

3. Turn cyber into a team concern

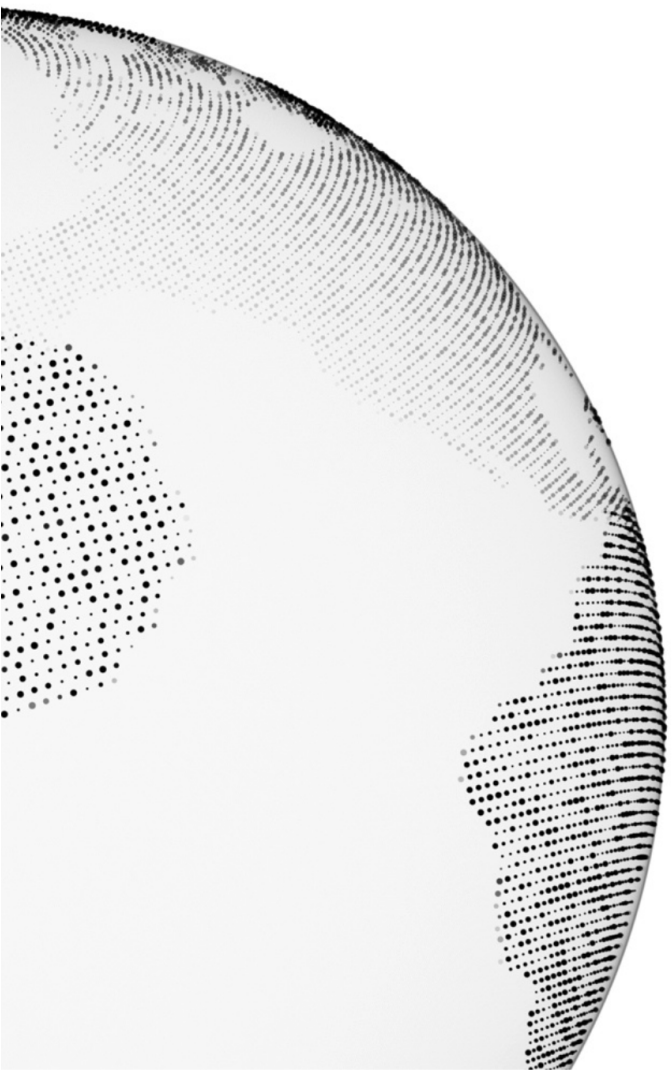
Why does 'human error' persistently come top of the list of cyber breach causes? In part it's because too many employees still pay lip service to the idea of cyber hygiene. They see things like safe usage policies and password management as a hindrance rather than a help. IT managers need to change this narrative; to communicate clearly that operating safely is crucial to organisational resilience, and to the company's future financial health. Try to make cyber training as relevant to individual roles and as engaging as possible. Invite suggestions for improvement from the wider business; make it clear that if anyone has any viable suggestions for making cyber management more user-friendly, you would be happy to consider them.

In turn, key business insiders - including finance leaders need to be more closely involved in conversations around cyber resilience and risk management. According to Marsh and Microsoft's 2022 cyber resilience report, just 26% of organisations use financial measures for evaluating financial risk. If true cyber resilience is to be achieved in the future, businesses should consider placing greater focus on analysing the potential impact of different cyber events in financial terms. This might involve tiering different categories of events based on forecasted potential losses, integrating business interruption into the calculations. This can give you a much more accurate picture of what level of risks - and what risks - you can afford, and where to focus your cyber security resources so they are aligned as closely as possible with the priorities of the business. Your organisation's finance leaders can and should bring their forecasting and data analytics capabilities front and centre to help achieve this.

Business transformation delivered securely

In most businesses, the cyber resilience imperative coexists with a desire to move forward with digital transformation; to find new ways to drive efficiency, reduce cost and deliver a more compelling customer experience. The two need to be considered hand in hand.

To transform your processes, while ensuring cyber resilience is hardwired into the changes you make, speak to **Millennium Consulting** today.



Contact Millennium Consulting at
assist@millenniumconsulting.com