LOGICALIS | CISCO

Stop the panic buying

A future-focused approach to building cyber resilience

Contents

Executive summary

In the constantly evolving cybersecurity landscape, it is the future-focused tech leader who foresees disruptions, harnesses the potential of new trends and builds resilient strategies.

This includes prioritising sustainability, a pragmatic approach to assessing legacy technology and processes, and ensuring resilience beyond cyber threats.

While immediate threats, such as cyberattacks, pose significant challenges, tech leaders must not lose sight of the broader horizon. However, a spate of high profile cyber attacks in Australia has triggered a buying frenzy for cybersecurity products and consulting services.

The hysteria around cybersecurity has fuelled panic buying, in addition to over-resourcing, with many companies taking on solutions requiring highly paid personnel that can otherwise be automated.

This whitepaper sets out a practical approach to building cyber resilience within your organisation, which is applicable no matter the size, industry or whether you are enterprise, SME, government or a not-for-profit organisation.

Certainly the scale of the cyber risk continues to grow for many, and it's natural that organisations would escalate their response to meet this ever present threat.

Data privacy and customer trust are fundamental principles to consider in developing your cybersecurity strategy.

While losing customer trust is difficult to measure, it can range from mild to severe across organisations.

This is before penalties are imposed by regulators in Australia and other markets.

What's important in this context is to return to first principles.

Basic hygiene measures can protect against 98% of attacks.

In fact, complexity is the enemy of security in that the unbridled addition of possibly superfluous security controls can actually increase the cyber risk when you consider the size of the attack surface and the privileges involved.

Logicalis can work with your organisation to leverage our global cybersecurity expertise, managed services track record and breadth and depth of talent, to "right size" your cybersecurity strategy, implementation and monitoring so that sensibility, not fear, underpins your cybersecurity approach and investment.

Cisco's extensive portfolio can provide end-to-end secure networking, delivering seamless secure user experiences. As one of only five Global Gold partners, Logicalis have partnered with Cisco for almost 25 years to create outcome-led solutions for the digital era.

Not only could this save your organisation time and money, but a pragmatic approach to cybersecurity may actually be the key to improving overall cyber resilience.

Understanding the cybersecurity landscape

Cyber resilience doesn't start with your technology stack, it starts with your people.

They are your greatest asset, but they can be your organisation's biggest potential weakness.

Cybercriminals routinely exploit simple human error to gain access to systems and data.

82% of data breaches are from human error

Source: Verizon's 2022 Data Breaches Investigations Report

Phishing

1h 42m

The median time for an attacker to begin moving laterally within your corporate network once a device is compromised.

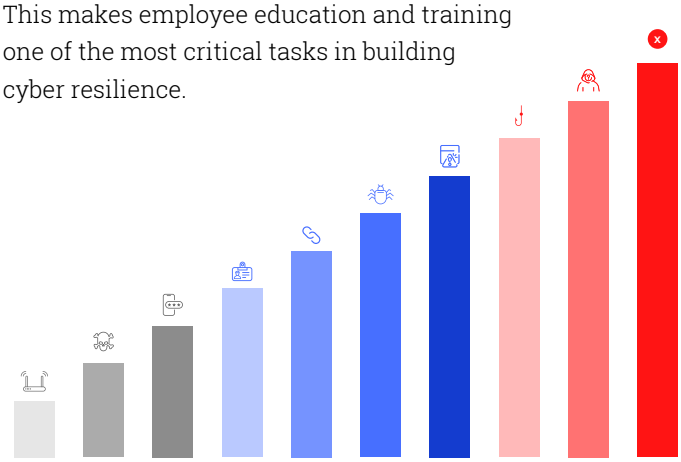
1h 12m

The median time it takes for an attacker to access your private data if you fall victim to a phishing email.

Where are cyber threats coming from?

The overwhelming majority of cyber attacks are the result of human error, namely phishing and social engineering. These can all lead to a ransomware attack or other more subtle attacks.

This makes employee education and training one of the most critical tasks in building cyber resilience.



ADAPT Security Edge April 2023: 79 CISOs, 18 with remediation

- Human error
- External threat
- Phishing and social engineering attacks
- System vulnerabilities (unpatched or vulnerable software and systems)
- Malware or ransomware
- Third-party vendors or supply chain attacks
- Stolen credentials or identity breach
- Unsecured BYOD / mobile devices
- Advanced Persistent Threats (APTs) or nation-state attacks
- Unsecured Internet of Things (IoT) devices

Remote working and device targeting

Rogue access to legitimate accounts in remote-work environments increased more than six-fold over the past three years according to the graph below.

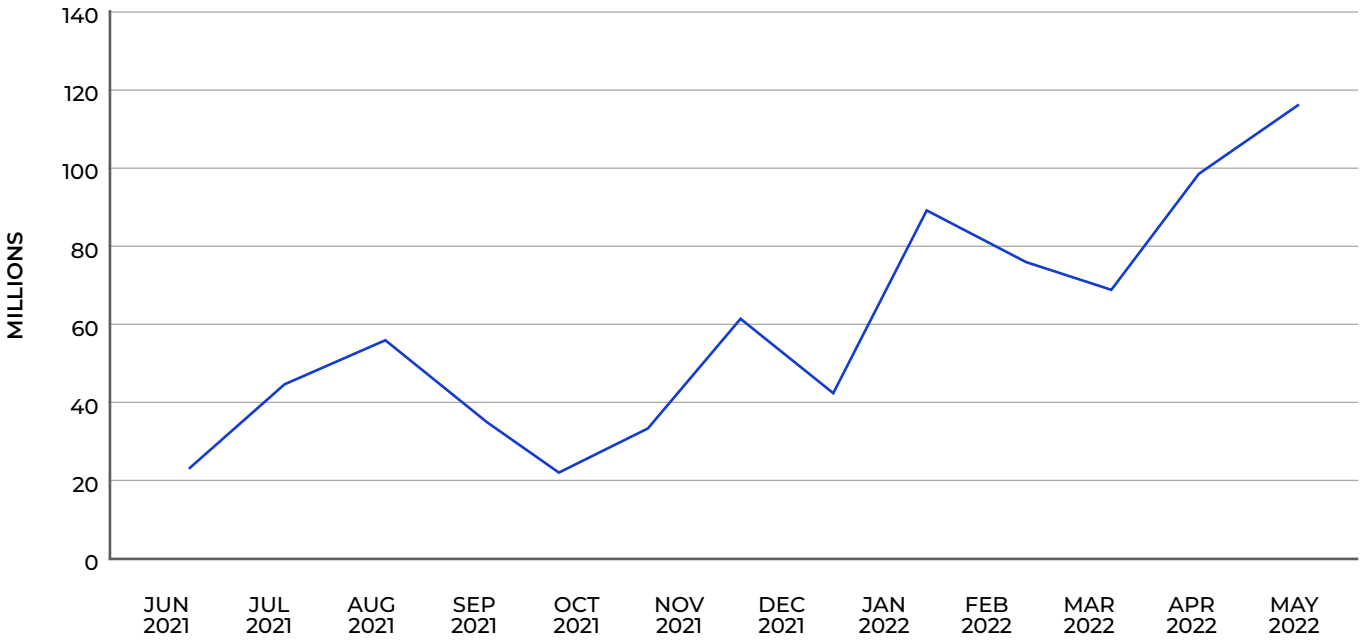
With remote working, sensitive data may be stored on personal computers that may not have adequate security measures in place.

Or worse, employee devices may be an implicitly trusted remote link back to the company's core technology assets.

Will you be held to ransom?

Ransomware is now a distinct identifiable risk with its own characteristics, including response processes, and can have indiscriminate and disruptive effects on customers.

Attacks against remote management devices



Increasing attacks on remote management ports over time, as seen through the MSTIC sensor network.

Source: Microsoft Digital Defense Report 2022

The reality from the frontline

The hierarchy of cybersecurity needs

There is a hierarchy of cybersecurity priorities. Similar to Maslow's Hierarchy of Needs, the most important factors for ongoing survival are at the base of the pyramid.

In Maslow's model, food and sleep are essential for human survival. In the cybersecurity context, understanding the size and scope of the potential attack surface is at the core of the foundation.

Companies firstly need to go back to basics — there is no point investing in next-gen solutions if basic cybersecurity needs are not being met.

Understand your risk

Company-wide risk assessment

Conduct a complete audit of the company's infrastructure, applications, data, devices and digital assets.

You can't protect what you don't understand.

Importantly, risk assessment is a continuous process, not something that's done at a single moment in time.

Secure by design

Start by reducing your attack surface, which means implementing a "Zero Trust" or "least-privilege" model for systems design and access.

Zero Trust is a security framework requiring all users, whether in or outside the organisation's network, to be authenticated, authorised, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

For example, a smart controller for an air conditioner, or a smart TV, could be dual-homed on a network and may be several firmware releases behind. Should such devices retain their original trust assignment or should they be at least periodically reassessed?

By reducing the attack surface, you are beginning your cyber resilience from a solid foundation.

End-to-end visibility

Before you can begin protecting something, you need to be able to see what you need to protect.

Comprehensively understand your environment by collecting data from your environment.

Know your devices, who uses them and who makes decisions about access and privileges.

Logicalis can help to build real-real-time security dashboards that give you visibility about what exactly you are trying to protect.

Appropriate, sensible protective measures

Advancements in technology have meant that many protective measures can now be automated.

For example, advancements in AI can assess cyber risks in minutes, instead of hours or days and can then trigger remediation for identified issues if desired.

Developments with technology allow companies to recalibrate their cyber spending to "right-size" solutions and mitigate a quantified threat risk, rather than implementing blanket protection against a threat that hasn't been clearly defined.

The reality from the frontline

Tim Davoren

Logicalis Head of Cybersecurity

Cyber criminals only need to be right once, but companies need to be right every time.

"The traditional security approach has been to make the outside a hard shell, but then once you crack that shell and get in, a threat actor can take it all. If you do zero trust well, you can rethink resource allocation because you're strong internally."

The victories are silent and the defeats are resounding. Davoren uses a risk assessment framework to implement cybersecurity strategies for Logicalis' clients.

Firstly, understand the risk which includes uncovering vulnerabilities and assessing the consequences of a potential cyber attack.

"If the probability is extremely low and the impact is low, this is probably a threat that doesn't warrant mitigating."

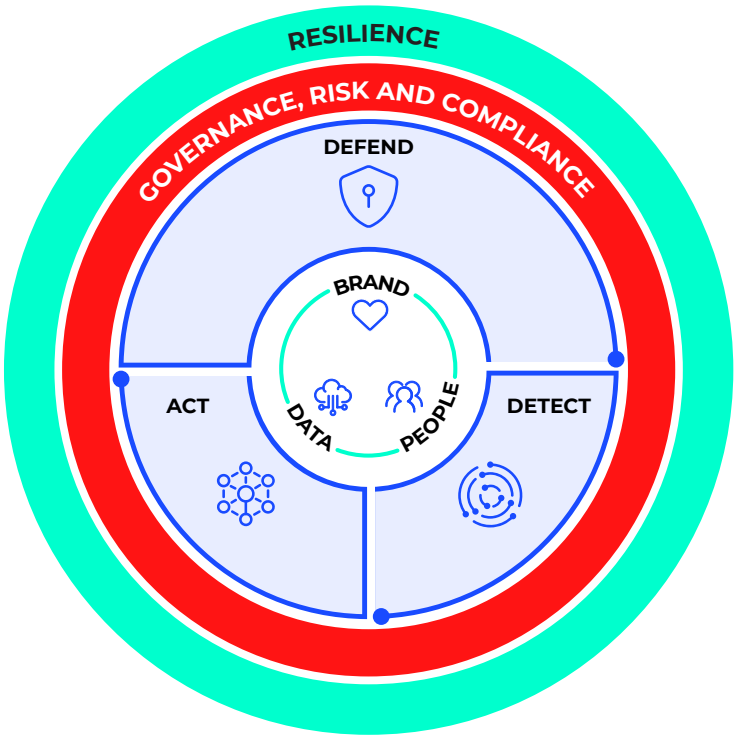
Then reduce the size of the target.

"Does everyone in the organisation need access to particular folders, or need devices with remote access?"

It's Davoren's view that the risk of cyber threats can be minimised significantly by implementing a "Zero Trust" or "least-privilege" model for security and access.

Key takeaways

- Always start with evaluating and prioritising your organisation's cyber risks and then create or allocate budget accordingly.
- Pursue comprehensive visibility of your assets. Security decisions made without reference to situational data about your environment can lead to wasteful, mis-matched investments and your incident response capability will be limited
- Be pragmatic about your solutions and work with the tools and controls you already have in the first instance. Over-engineering a solution may not reduce your risks, but it will almost certainly increase your operating expenses.



Logicalis' Adaptive Asset Protection Approach

The reality from the frontline

Rob Mattlin

Logicalis Product Owner
Digital Workplace COE, Security COE

Organisations need to be cyber resilient, but the reality is that many either can't afford it, or are wasting money on unnecessary products and FTEs.

"Nobody wants to be on the front page of a newspaper, but you could potentially be throwing away millions of dollars and getting nothing in return. Fear has been driving sub-optimal spending on cybersecurity."

As one of Australia's leading cybersecurity consulting firms, Logicalis has developed a holistic approach which includes a mix of strategy, planning, and managed services with deep automation to bring down the cost of cybersecurity and make it a "no-brainer" for every organisation..

"Automation has helped to bring down response times to some incidents from 20 minutes to 20 seconds."

Logicalis is utilising vendor software including Cisco's XDR - Extended Detection and Response.

The aim is to reduce human labour, increase accuracy and speed and all for a price that is more cost effective at scale.

Key takeaways

- Automation has completely changed the cybersecurity game, so try to automate as much as possible.
- Automation needs to be implemented responsibly, by cybersecurity experts, so that you don't start triggering false positives. There simply is no plug-and-play solution that exists anywhere in the world.
- Automation has greatly brought down the cost of being cyber secure, which is democratising access to cybersecurity for companies of all sizes.

A holistic approach to cybersecurity

Your people are your greatest asset in developing your cyber resilience strategy.

The key is to align people, systems and technologies with your business objectives so that your cybersecurity posture is embedded into everything you do.

This means accountability for cybersecurity isn't assigned to the IT team, it's a whole-of-business, holistic approach to building end-to-end organisational resilience.

The circle of trust

Governance, risk management, and compliance (GRC) are three critical areas that organisations must address in order to operate efficiently and effectively.

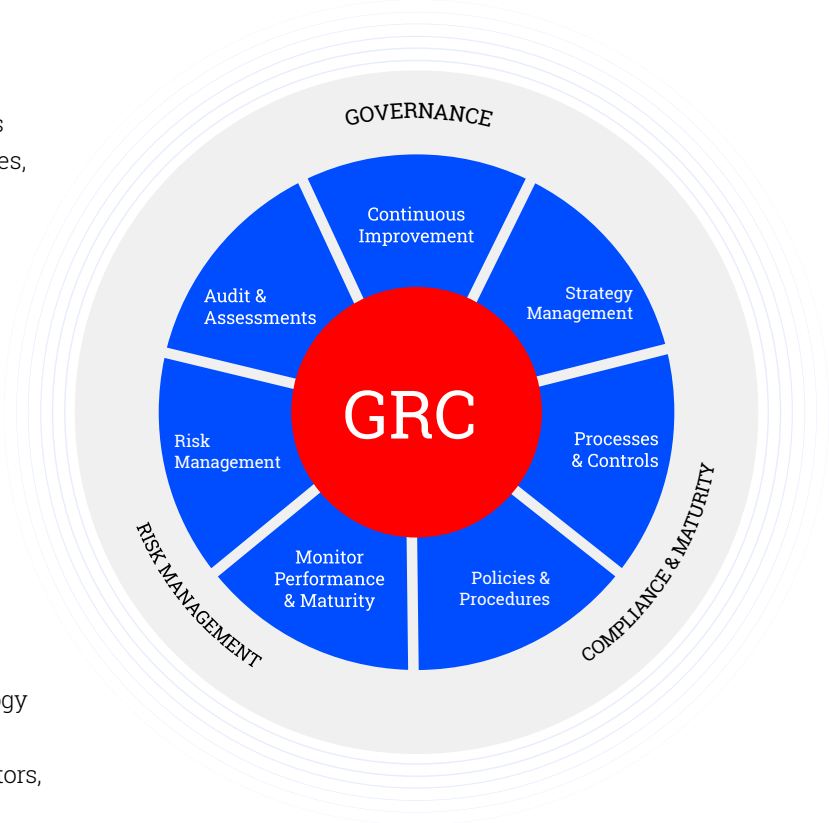
GRC has become the starting point for implementing a holistic cybersecurity approach, mostly because it helps organisations avoid silos, which can lead to inefficiencies, inconsistencies and consequently - weaknesses.

One of the key benefits of GRC is the ability to identify risks most relevant to your business and manage these proactively.

The benefits simply cannot be overstated. A GRC approach allows organisations to identify and prioritise risks that may not be immediately obvious when looking at individual risks in isolation.

The circle of trust also implies that the process is a continuous journey, ever evolving and that everything is interconnected.

Your internal staff, external contractors and your technology team all work together to strengthen the company to maintain and build trust with key stakeholders like regulators, investors and most importantly, your customers.



Governance, Risk and Compliance (GRC) in depth

Let's make it simple

Cybersecurity is a key focus for most organisations, yet it can be overwhelming. Don't overthink it. There's a checklist you can work towards, and it has four basic components.

There's a checklist you can work towards, and it has four basic components.

Strategy

This is your plan for how you are going to identify and protect your information assets and detect and respond to cyberthreats within your business. Start by identifying the relevant risks, and match them with your plan to mitigate them.

Using the GRC model, your strategy with continue to evolve and allow you to operate and innovate with confidence.

Processes

Using the GRC model, build a process and competencies (internal and external) to meet your core objectives outlined in your cyber strategy.

Once you've built your processes, embed them into the business both from a policy, technology and people perspective in terms of training and acceptance.

Technology

Technology partners are critical in developing your end-to-end approach. Logicalis can help you with advice about off-the-shelf technology solutions from major suppliers, as well as provide advice and insights about how to implement technology solutions within your existing data and IT infrastructure.

People

While your employees are your biggest risk for cybercriminals, this risk is mitigated if your people understand and have a process for reporting phishing attempts or suspicious activity.

We find that a lot of organisations we work with are either not fully comfortable that they understand their compliance obligations, or how they may impact their security.

The board of the organisation owns the cybersecurity risk. As a technology professional it's your job to make sure that board and executive management has full visibility in making decisions about budgets, resourcing and which gaps to fill.

Top considerations

- GRC is continuous, it doesn't matter at which point you start, the most important thing is to make a start.
- It's not the job of IT to manage the entire risk, it's their job to understand and quantify the risk and give visibility to the board to make decisions.
- The boring hygiene factors are more important than you might realise. Start with a process for reducing risk, not the software for countering attacks.

Accountability for cybersecurity risk ultimately rests with a company's board.

As the head of IT, you might be trying to get rid of every risk, but it's not up to you to eliminate every risk, it's your job to identify the risk and present the information to the board and executive management.

In developing a comprehensive risk assessment, companies need to consider the sector in which it operates, the legislative and regulatory obligations and the risk appetite for the business.

Think of cybersecurity like building blocks. You need all the different building blocks, and in terms of strategy, you don't need to do a particular thing first, you just need to start because the process is circular and it's continual.

Too many companies are failing to address the basic hygiene factors.

Data is an asset, but it can also become a liability.

Have you actually cleaned up all the data from your old computers and phones? It's tough and it's not fun and it's not glamorous, but rather than just putting new stuff and the shiny new toys in place, make sure you take out the rubbish.

It's also important to articulate what you are trying to do, and deliver the plan to your organisation in a way they understand.

You don't run a business without writing something down. Give the instructions to the organisation in a meaningful and relevant format that they can consume.

GRC is something every company needs to own, you can outsource the development of the strategy, but ultimately you can't outsource the risk.

The power of partnership: vendor perspectives

There is simply no plug and play solution, or silver bullet that solves the cybersecurity challenge.

As one of only five Global Gold partners Logicalis has partnered with Cisco for almost 25 years to create outcome-led solutions for the digital era.

Logicalis is one of the leading Cisco partners in providing Managed next generation connectivity including Managed SD Wan and SASE, in addition to Managed Private 5G for Enterprise.

With 130+ Cisco certified Internetwork Experts and a range of global Cisco powered solutions, Logicalis is trusted around the world to deliver expertise clients can count on.

The problem is complex and constantly evolving.

The vendors are creating the tools to fight the cyber criminals and their implementation partners are helping you to face the threat.

Logicalis is a leading, award-winning implementation partner for Cisco, with strong relationships with many other leading vendors.

The reality is that most organisations will need a range of solutions from one or more vendors. And importantly, that the vendor solutions and implementation partners are generally agnostic to your tech stack.

LOGICALIS
Architects of Change

CISCO

Cisco's Cloud Security platform protects all aspects of your business. One of the flagship products is "Cisco Extended Detection and Response" or "Cisco XDR" which is the foundation of Cisco's Breach Protection Suite.

"If an organisation carries a Cisco-verified partner gold badge, or cybersecurity badge, these are things that clients can trust because we put our partners through a rigorous program over decades. Start with a verified Cisco partner because they will really optimise your budget."

Top tips

- ✓ If you don't have an internal cyber team yet, start by finding an implementation partner, like Logicalis, and work through them to develop and implement your cybersecurity strategy.
- ✓ Don't get distracted by shiny new software, instead spend your time fixing your hygiene factors.
- ✓ Pick projects where you can achieve an outcome, for example decide to reduce the number of endpoints with a vulnerability down from 90% to 5%.

Contextual Security

Cisco XDR allows for visibility across the network and endpoint and simplifies security operations in today's hybrid, multi-vendor, multi-threat landscape.

The platform prioritises and remediates security incidents more efficiently using evidence-based automation.

According to Corien Vermaak, Cisco's Director of Cybersecurity, Cisco XDR's platform can process data from disparate sources to qualify threats in near real time.

"Let's say you have a CCTV camera at your front door, a laser beam at your gates and a door lock. If someone approaches the property, the laser beam will be tripped off.

The laser beam reports movement in the garden. Then the CCTV camera will say, "I see a perpetrator we don't know".

And the lock will say "somebody is tampering with me, but I'm not allowing them access because they don't have a key."

Now, you can immediately see how the three pieces of information are vastly different.

However, put together in context, the platform can predict that this is a perpetrator. So that's exactly how you can think about Cisco XDR - it takes different viewpoints from traditional security tools," said Vermaak.

The hybrid workforce has changed the game

Cisco recognises that people will continuously work remotely and the way they access data will be dispersed across multiple clouds.

According to Vermaak, protecting the user endpoint is a critical first line of defence.

"Protecting the user endpoint is at the core of everything we do. For example, the user endpoint needs to be patched at the right level, and we need to check the user's chrome is updated from all security vulnerabilities."

In addition to endpoints, the concept of "multi-cloud defence" is also critical.

"This is still underpinned by old methods of securing office infrastructure. In some cases we still have servers and they sit within the fortress and we need to secure the fortress."

Finding the right partner

Right now in this industry there are more positions available than people who are qualified, according to Vermaak.

"We need to be smarter and do things quicker and be able to respond faster and smarter with the tools we already have," said Vermaak.

For Cisco, implementation partners are an essential piece of the cybersecurity matrix.

"It's always very sad to me when I get to a site and the client has all of my tools but they're not optimally using them. Cisco relies on our implementation partners, like Logicalis, to optimise our technology."

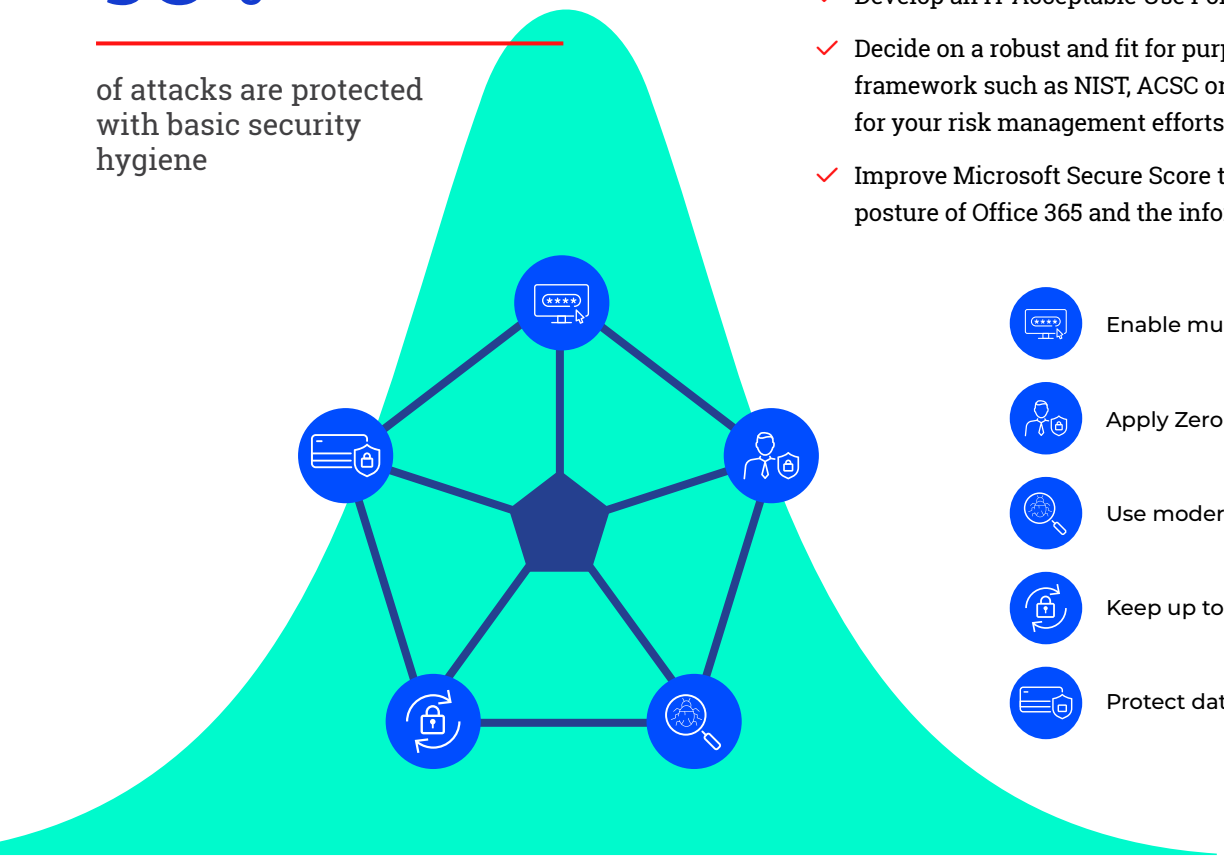
Driving cyber resilience and business performance

The good news is that 98% of cyberthreats can be addressed with basic hygiene measures.

Most of these require discipline and communication across the organisation.

98%

of attacks are protected with basic security hygiene



Logicalis has some quick wins

- ✓ Whole-of- business cybersecurity education and training as a critical first step in improving your cybersecurity posture and effectiveness.
- ✓ Implement Cisco's zero trust access with multi-factor authentication (MFA) across all applications to reduce identity based attacks.
- ✓ Have defined and implemented data retention and disposal policies in place.
- ✓ Document offboarding process for system users to ensure this is followed consistently.
- ✓ Develop an IT Acceptable Use Policy.
- ✓ Decide on a robust and fit for purpose controls framework such as NIST, ACSC or ISO to provide context for your risk management efforts.
- ✓ Improve Microsoft Secure Score to uplift the security posture of Office 365 and the information this contains.

- Enable multifactor authentication
- Apply Zero Trust principles
- Use modern anti-malware
- Keep up to date
- Protect data

Source: Microsoft Digital Defense Report 2022

Seizing opportunity in the cyber age

In an era of rapid technological advancement, the measure of a future-focused tech leader is the ability to anticipate, adapt, and align strategies with a changing landscape.

Rather than reactively addressing immediate threats, these leaders proactively shape their cybersecurity approach with foresight, balancing innovation with foundational principles.

This vision extends beyond defending against threats; it encompasses leveraging cybersecurity as a tool for trust-building, strategic advantage, and organisational growth.

Importantly, cybersecurity is an accountability of the board and a potential financial and reputational risk for the organisation.

But while the cybersecurity challenge is growing in size and complexity, that doesn't necessarily mean the budget for the response needs to grow in proportion.

With increased budgets, the temptation has been to simply throw money at the problem. However, there is no silver bullet and money alone won't resolve the cyber threat.

Cybercriminal activity is a threat that is best countered through a partnership between your organisation, a cybertechnology vendor, or a range of vendors, and a trusted advisory and implementation partner.

As an experienced, award-winning partner leading cybersecurity vendors such as Cisco, engaging with Logicalis is an opportunity for you to ensure a comprehensive and informed approach to your organisation's cyber resilience.

We empower you to manage complex operating challenges and confidently pursue opportunities with a flexible and robust defence system for your most valued organisational assets.

Our proven track record as a leading systems integrator and managed services provider gives you the confidence to transform with complete confidence.

Speak to a Logicalis cybersecurity expert today

www.au.logicalis.com/cyber-security