BLUEREEF
TECHNOLOGY

The Cybersecurity Crisis

The Cybersecurity Threat No Small Business Can Ignore

What Every Small Business Must Do Now to Avoid the Financial and Reputational Fallout of Cybercrime

Cyber Threats Are Growing Fast — And No Business Is Immune
The rise in cybercrime, ransomware, and targeted attacks has reached alarming levels.

Business owners and leaders can no longer afford to think,
“It won’t happen to us.”

Whether you're running a small local business or a large operation, you will be targeted — and without the right protections in place, your systems, data, and reputation are at serious risk.

This report outlines essential, up-to-date cybersecurity measures that every business must implement to stay protected in today’s threat landscape.

Provided as an educational service by:

Daniel Ladlow, Managing Director
BlueReef Technology
bluereef.tech
08 8922 0000

About The Author

Daniel Ladlow is the Managing Director of BlueReef Technology, a 100% founder-owned Managed Service Provider (MSP) delivering proactive IT support to growth-focused SMEs across Darwin, Alice Springs, and Brisbane. Since founding the business in 2008, Daniel has grown BlueReef into a trusted local partner for all things tech—cloud, cybersecurity, communications, and beyond.

With nearly two decades of hands-on experience in the technology space, Daniel has helped countless regional businesses overcome complex challenges—whether it's navigating cloud migration, improving cybersecurity, or replacing slow, outdated IT support. His leadership combines a deep love for technology with a practical, outcomes-focused mindset. At the heart of BlueReef's culture is Daniel's commitment to transparency, integrity, and long-term partnerships.

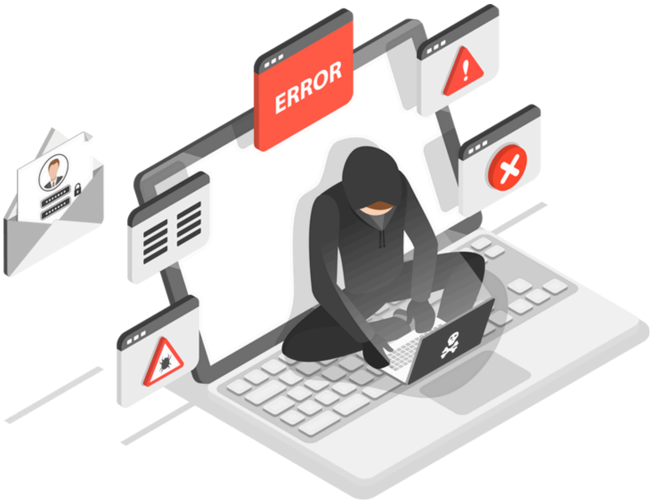
Under his guidance, BlueReef has introduced customer-first initiatives like 24/7 monitoring, regular monthly check-ins, and a 60-day "Thrilled Today or You Don't Have to Stay" guarantee. It's all part of Daniel's mission to simplify IT for regional businesses, cut through the jargon, and deliver real results.

When he's not leading the team, you'll find Daniel collecting vinyl records, riding his motorbike, or heading out for a fish—interests that reflect his hands-on nature and love for balance.

Daniel's vision is clear: to become the leading MSP for regional Australia—empowering local businesses with smarter tech, stronger security, and a team that genuinely has their back.

After a Cyber-Attack, Will You Be Blamed — Even If It Wasn't Your Fault?

It doesn't seem fair — and in many ways, it isn't. If you're the victim of a physical crime like a break-in or theft, you'll likely receive support and sympathy. But if your business suffers a cyberattack that compromises sensitive client or patient data, the reaction is very different. Instead of support, you could be labeled careless or negligent.



Your business may be investigated, and clients will demand answers. If you can't demonstrate that you took reasonable steps to prevent the breach, you could face legal action, hefty fines, and lasting damage to your reputation — even if you were relying on an outsourced IT provider.

Unfortunately, "I didn't know" is not a valid excuse. As a business owner, the responsibility ultimately falls on your shoulders.

But it doesn't stop there.
Under Australian data protection and privacy laws, you may be legally required to notify your clients or patients that their information was exposed in a breach — and that your systems were the source. The reputational fallout can be severe. Competitors may take advantage, clients may leave, and staff morale can take a serious hit as the blame lands squarely on your shoulders.

Worse still, your bank isn't obligated to reimburse funds lost through cybercrime, and unless you hold a specific type of cyber liability insurance, your policy likely won't cover the damages. The financial and reputational costs can be devastating.

This is not something to take lightly. Many business owners assume their current IT provider is "handling everything," but in reality, many are cutting corners, missing critical protections, or simply not keeping up with today's cybersecurity standards. We can prove this — with your permission — through a quick, no-obligation Cybersecurity Risk Assessment.
But before we get into that, let me properly introduce myself and explain why I created this report in the first place.

Why We Are So PASSIONATE About Informing And Protecting YOU

My name is Daniel Ladlow, Managing Director of BlueReef Technology. We specialise in being the outsourced IT department for businesses across Australia, with local expertise in Darwin, Brisbane, and beyond. No matter where you're located, we provide trusted, expert IT services designed to protect your business from the rising tide of cyber threats.

Over the past few years, my team and I have seen a sharp rise in calls from business owners urgently seeking help after ransomware attacks, data breaches, or other cybercrime incidents.

When they reach out, they're often overwhelmed and desperate, scrambling to find anyone who can help put the pieces back together. Many have their entire business on lockdown—critical data corrupted or held hostage—making it impossible to meet their client obligations. Years of hard work and vital information, all at risk or lost.

Along with the technical crisis, they're scared and frustrated. They feel violated and helpless, even embarrassed. How could money be stolen from their bank account without their knowledge? Why didn't their IT company or internal team stop this? How will they break the news to their clients or patients that they've been exposed to cybercriminals? Many are in disbelief they fell victim at all—after all, they thought "we weren't a target."

What makes this all the more unforgivable is that every CEO who comes to us after a serious cyberattack had trusted an IT company to protect their business — only to discover too late that the company wasn't doing the job they were paid to do.

As a business owner who built my company from the ground up, I deeply understand the hard work, risks, and personal sacrifices involved in making your business succeed. It's a profound insult to have everything jeopardized or taken away by cybercriminals operating with impunity from across the globe.

What frustrates me even more is how many so-called "IT experts" fail to fulfill their responsibilities. As a CEO, you must trust that your IT provider is doing everything necessary to safeguard your organization — and when they don't, the fallout lands squarely on your shoulders: costly, devastating, and disruptive.

That's why we've launched a "one-company revolution" to educate and empower as many business owners as possible. We want to help you avoid the stress, anxiety, and losses caused by cyberattacks — so you're prepared and protected, not caught off guard.

Yes, It CAN Happen To YOU And The Damages Are VERY Real

You're probably aware of the growing threats—from ransomware to hackers—but there's a good chance you're underestimating how vulnerable your business really is. It's also possible that you're not fully protected, operating with a false sense of security, and unfortunately being underserved by your current IT provider.

If your IT provider hasn't discussed the protections outlined in this report or the need for a cyber "disaster recovery" plan, you are at risk and not getting the proper advice.

This is not a matter to take lightly. If a breach happens, your reputation, finances, business, and personal liability could all be on the line. That's why you need to take an active role in ensuring your company is prepared and properly protected—not just leave it to someone else.

QUESTION: When did your IT provider last discuss these cyber threats with you? If they haven't, read this report and act now.

"It Won't Happen to Us — We're Too Small" — Think Again

Don't think you're at risk because you're "small" and not a big company like Commonwealth Bank, Qantas, or Woolworths? Believe you have "good" people and enough protections in place? That it won't happen to you?

That's exactly what cybercriminals are counting on. It makes you easy prey because you have little to no proper protection in place.

Right now, there are over 980 million malware programs in circulation—and that number keeps growing (source: AV-Test Institute). Around 70% of cyber-attacks target small businesses (source: National Cybersecurity Alliance). You might not hear about these attacks because the media focuses on big breaches, or companies keep quiet to avoid bad PR, lawsuits, fines, and embarrassment.

In fact, the National Cybersecurity Alliance reports that one in five small businesses have fallen victim to cybercrime in the past year—and that only counts reported incidents. Many small businesses don't report breaches, so the real number is likely much higher.

Are you "too small" to suffer serious damage from ransomware that locks your files for days? Too small to worry about a hacker using your company's server to infect clients, vendors, and employees with malware? Or too small to be targeted for payroll theft?

According to Osterman Research, the average ransomware demand now sits at $84,000 (source: MSSP Alert). Small businesses lose over $100,000 per ransomware incident on average, plus more than 25 hours of downtime.

Is this a risk you're willing to take?

How Bad Can It Be?
My Insurance Will Cover Me, Won't It?

Insurance companies are in business to make money, not to pay out claims.

A few years ago, cyber insurers kept about 70% of premiums as profit and only paid out 30% in claims. Today, that ratio has flipped — forcing insurers to tighten requirements and change how cyber-liability coverage is offered and paid.

Now, even to get a basic cyber-liability or crime policy, you often must prove you have essential security measures in place — like multi-factor authentication, strong password management, advanced endpoint protection, and tested, reliable data backups.

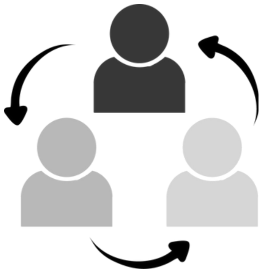
Insurance carriers expect you to have phishing and cybersecurity awareness training in place, and many require a Written Information Security Program (WISP) or a Business Continuity Plan. Depending on the insurer, your specific business, and the coverage sought, this list of requirements may be even longer.

The biggest risk often overlooked is the proper enforcement of these critical security protocols that insurance policies and data protection laws mandate. If you fail to implement these measures, your insurance claim can be denied. When a breach occurs, insurers will investigate the cause and assess whether negligence played a role before approving any payout.

Saying, "I thought my IT company was handling this," won't protect you. IT providers typically disclaim responsibility for insurance procurement and don't guarantee your security (check your contract). They may also document if you declined advanced security services, distancing themselves further. Without thorough documentation proving you took reasonable steps to secure your network and avoid willful negligence, you will be personally responsible for the costly fallout of a breach.

It's NOT Just Cybercriminals Who Are The Problem

Many business owners mistakenly believe cybercrime only comes from hackers in places like China or Russia. However, the reality is that disgruntled employees—whether from within your own company or among your vendors—pose a serious threat. Because they understand your systems and have access to sensitive data, they can cause significant damage. So, what kind of harm could insiders really do?

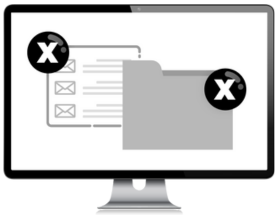


When employees leave, they often take your company's files, client data, and confidential information with them—sometimes stored on personal devices. They may also retain access to cloud services like social media accounts or file-sharing platforms (such as Dropbox or OneDrive), especially if your IT team isn't aware or forgets to update passwords.

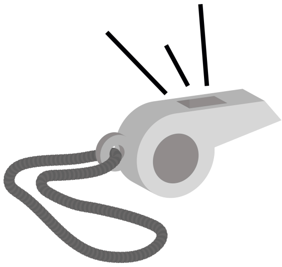
In fact, a detailed study by Osterman Research found that 69% of businesses suffer data loss due to employee turnover, and 87% of departing employees take company data with them. What happens to that information? It can be sold to competitors, used to start a competing business, or retained for use at their next job.

Funds, inventory, trade secrets, client lists, and countless work hours are stolen every day—and it's happening far more often than most businesses realize. According to StatisticBrain, 75% of employees have stolen from their employers at some point. Theft can range from pilfering inventory to check and credit card fraud. Often, these losses add up slowly in small amounts that go unnoticed.

The most common form of "theft" is time theft: employees spending work hours on personal errands, shopping, gaming, browsing social media, gambling, reading news, or other non-work activities. You pay them for a full 40-hour week but might only be getting half of that. Then, these same employees complain about being "overwhelmed" and "overworked," urging you to hire more staff—costing your business even more. If your IT provider isn't monitoring or restricting employee internet activity, employees might also visit high-risk sites—like those hosting illegal downloads, adult content, gambling, or gaming—which can expose your network to viruses and phishing attacks.



Some employees, when leaving or fired, will delete critical emails and files before they go. If you don't have reliable backups, you risk losing everything. Even if you successfully sue the employee, the legal costs, time, and distractions usually outweigh any compensation you might receive.



Disgruntled employees, vendors, and even clients can also become whistleblowers. For example, most HIPAA violation complaints against medical practices come from inside the organization—often from unhappy staff or patients, not auditors. Protected under whistleblower laws, these individuals can receive financial rewards for reporting wrongdoing. This trend is growing as government agencies strengthen cybersecurity laws and enforcement. Ambulance-chasing attorneys are even advertising to represent whistleblowers, with websites like www.CorporateWhistleBlower.com encouraging people to report Medicare fraud or corporate wrongdoing.

This is just the beginning of a wave of whistleblower actions impacting all industries.

Take a moment to review the risks we've just outlined. Do you truly believe these things couldn't happen to you?

Beyond your own employees, vendor theft is another serious threat. Payroll, HR, and accounting firms often have direct access to your most sensitive data and financial information.

It's not just their leadership teams you need to worry about—sometimes, part-time or temporary staff, such as seasonal data entry workers who may work remotely with little supervision, can exploit this access. They might steal money, sell confidential data, or siphon funds from your accounts without your knowledge.

To Request Your FREE Assessment,
please visit **bluetech.tech** or call our office at 08 8922 0000

Read On To Hear What Our Clients Have To Say:

"BlueReef Have The Knowledge And Expertise To Get It Right The First Time
Streamlining our software and cloud services has been significantly beneficial in terms of productivity by creating access to shared documents immediately. Having one central source is also beneficial to our field engineers and keeps the Project running efficiently.
The IT Support we receive is extremely efficient and professional. Turnaround time for troubleshooting and solutions are virtually immediate, and all staff have access to support. BlueReef provide a prompt service for the delivery and setup of new equipment, even in remote locations.
BlueReef have great customer service. All calls and emails are answered, and turnaround time is well above what we've experienced with other companies. Being local, they understand the environment we work in and make our IT straightforward. We've recommended BlueReef to other firms and continue to do so. I would recommend having a conversation with them—that's how simple they make it!"

-Lisa Chapman

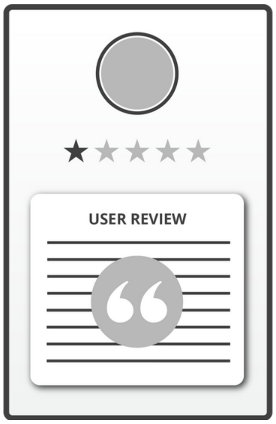
"Very friendly and helpful above and beyond. Quick effective solving of my problem when others were unreliable and unhelpful."

-Fiona Douglas

To Request Your FREE Assessment,
please visit **bluetech.tech** or call our office at 08 8922 0000

Exactly How Can Cybercrime Harm Your Business? Let's Count the Ways:

1. Reputational Damages:



What's worse than a data breach? Trying to cover it up. Companies like Yahoo! found this out the hard way, facing major lawsuits for not informing users quickly after a breach. These days, dark web monitoring and forensic tools can easily trace where the breach started — so you can't hide it.

When your business is breached, do you think your clients or patients will be understanding? Or will they demand answers?
Will you be able to confidently say you took the right precautions — or will you have to admit, "We didn't think it would happen to us," or "We didn't want to spend the money"?

News spreads fast. A breach can seriously damage your reputation — and once trust is lost, it's hard (and expensive) to win back.

2. Government Fines, Legal Fees, Lawsuits:

Governments here in Australia and around the world are tightening cybersecurity and privacy legislation. Enforcement is ramping up, and the penalties for non-compliance are getting steeper.
This isn't just a big business problem. If your organisation collects or stores personal information — even just names and emails — you're responsible for protecting it. And if a data breach occurs, you're legally required to notify affected individuals. Fail to do that, and you could be facing serious fines, legal consequences, and long-term damage to your reputation.

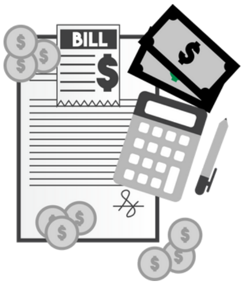
In certain industries, like healthcare, finance, and law, have even stricter obligations. Under Australia's Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme, any organisation covered by the Act must notify both the Office of the Australian Information Commissioner (OAIC) and the individuals affected if the breach is likely to cause serious harm.
If you operate under international compliance frameworks like HIPAA, PCI DSS, or ISO 27001, your reporting requirements are even more extensive — including notifying regulators, clients, and sometimes even the media.

And if you're working with government or defence contracts, the bar is even higher.
You may need to meet security standards under the Protective Security Policy Framework (PSPF) or the Defence Industry Security Program (DISP). These frameworks require strict cybersecurity controls, personnel checks, and formal incident reporting processes. A breach can result in more than just fines — it can jeopardise your contracts.
Cyber regulations are evolving rapidly. There's a good chance what kept you compliant last year isn't enough today.

So here's the real question: Is your current IT provider keeping you informed and protected?

To Request Your FREE Assessment,
please visit **bluetech.tech** or call our office at 08 8922 0000

3. Cost, After Cost, After Cost:



It only takes one breach, one ransomware attack, or one rogue employee to send your business into chaos.
Your already stretched team is suddenly swamped with urgent tasks. Projects are delayed. Operations grind to a halt. Clients are frustrated. Sales opportunities slip through the cracks.

Then come the unexpected costs:

- Forensics to figure out what happened and what data was stolen
- Emergency IT restoration, often at premium rates
- Ransom payments — with no guarantee you'll get your data back
- Legal fees to manage client communications and media fallout
- Credit monitoring services for affected clients (often required under law)
- Cash flow disruption and budget blowouts

The financial impact can be devastating — and for some businesses, it's the beginning of the end.

4. Bank Fraud:

If cybercriminals gain access to your business bank account and steal funds, your bank is not obligated to reimburse you.

Take the real-life case of Verne Harnish, a successful CEO and author, who lost $400,000 after hackers accessed his computer and intercepted internal emails. Impersonating him, the hackers instructed his assistant to wire money to three accounts — and she did, thinking the request was legitimate. The hackers even disabled his bank alerts to cover their tracks. By the time anyone realised, the money was long gone — and the bank refused to cover the loss.

Think this couldn't happen in your business?

Many Australian business owners believe, "Not my staff. Not my company." But even the most trusted team member can fall for a convincing scam. It only takes one error in judgment, one fake email, one overlooked detail — and the damage is done.

You wouldn't drive without a seatbelt just because you don't expect a crash. Cybercrime is no different.

Claiming ignorance or shifting blame to your IT provider won't hold up. In the eyes of the law and your clients, you are responsible.

5. Using YOU As The Means To Infect Your Clients:

Not all cybercriminals are after your money or data — sometimes, they want your systems.

Hackers can hijack your server, website or email accounts to spread malware, send spam, or quietly infect your clients and vendors. Your compromised website could be used to host phishing pages, run SEO scams, or even promote extremist content — all under your business's name.

This kind of attack doesn't just damage your brand — it puts your reputation, client trust and potential legal standing at serious risk.

That's why robust protections like advanced endpoint security, spam filtering, threat monitoring, and web gateway controls aren't optional extras — they're essential.
Are you comfortable being the reason one of your clients gets hacked?

You May Want To Believe You're "Safe" But Are You Sure?

It's very possible you're being ill-advised by your current IT company.

When was the last time they sat down with you — proactively — to talk about emerging cyber threats, updated security protocols, and the latest tools you need to stay protected today, not six months ago?
If that conversation hasn't happened recently, there could be a few concerning reasons:

- They don't know how. Many IT providers are great at keeping systems running but lack the expertise to deal with today's advanced cybersecurity landscape.
- They're too busy or unwilling to upgrade you. It's not uncommon for IT companies to avoid recommending better protection because it means admitting their current setup is now outdated — or because they don't want to wear the cost of upgrading their own systems and tools.
- They won't admit they're out of their depth. Nobody wants to say, "We can't handle this," especially not the people you've trusted with your business-critical technology.

To be fair, your provider might have you fully covered — but here's the real question: How do you know?

Have they provided clear documentation, shown evidence of regular updates, or offered an independent assessment? If not, it might be time to get a second opinion before it's too late.

Think Your IT Company Has You Covered? Take the Quiz to See If They're Really Doing Their Job.

If your current IT company doesn't score a **"Yes"** on every item in this checklist, they are NOT adequately protecting your business. Don't let them "explain it away," and do not give them a pass on even a single point — each one is critical.

Just as important: get verification. Asking, "Do you have insurance to cover us if you make a mistake?" is a good start — but don't stop there.
Request a copy of their insurance policy or written confirmation.
When things go wrong, verbal assurances won't hold up. Documentation will.

To Request Your FREE Assessment,
please visit **bluetech.tech** or call our office at 08 8922 0000

If your current IT company does not score a "YES" on every point, they are NOT adequately protecting you.

Have they met with you recently — within the last 3 months — to review how they're protecting your business right now?

Do they proactively monitor, patch, and update your network's critical security settings daily? Weekly? At all?

Have they ever urged you to talk with your insurance company to confirm you have the right coverage for cyber liability and fraud?

Do they have adequate insurance to protect YOU if their mistake compromises your network?

Have you been fully and honestly briefed on what to do if your business is compromised?

Have they told you if your IT support is outsourced to a third party?

Are their technicians properly trained on the latest cybersecurity threats and technologies, or are they learning on the job?

Do they have a ransomware-proof backup system in place?

Do they have a written mobile and remote device security policy?
Do they enforce strong password policies for your employees?
Have they discussed replacing traditional antivirus with advanced endpoint security?
Have they talked to you about or set up multifactor authentication (MFA) for accessing sensitive data?
Have they recommended or completed a full risk assessment every year?
Have they set up web-filtering to block harmful or inappropriate websites?
Have they provided cybersecurity training for you and your employees?
Is your email system set up to block sending or receiving confidential data?
Do they allow remote access through tools like GoToMyPC, LogMeIn, or TeamViewer? If yes, that’s a red flag—remote access should only be through a secure VPN.
Have they offered or discussed dark web ID monitoring with you?

Get Real Assurance with an Independent Risk Assessment

A security assessment is exactly what it sounds like — a thorough review and evaluation of your company's network designed to identify weaknesses and vulnerabilities before a cyber-attack happens.

Think of it like a cancer screening: catching problems early when they're small means they're much easier and less costly to fix, less disruptive to your business, and gives you a far better chance of surviving a cyber incident.

An assessment should always be performed by a qualified third party—not your current IT team or provider. Fresh eyes can spot issues that might be overlooked by those who see your systems every day.

You want a skilled "Sherlock Holmes" working on your behalf—someone who won't cover up problems or make excuses, but instead delivers a confidential report you can use to address vulnerabilities before others discover and exploit them.

Our Free Cybersecurity Risk Assessment: Get the Answers You Need and the Confidence You Deserve

For a limited time, we're offering a Free Cybersecurity Risk Assessment to a select group of businesses. This is completely free and comes with no obligation.

Everything we find and discuss will be kept strictly confidential.

This assessment provides an independent, expert verification of whether your current IT company is doing everything needed to keep your network running smoothly and safe from cyber threats.

How It Works:

At no cost or obligation, one of my lead consultants and I will visit your office to perform a non-invasive, confidential review of your computer network, backups, and security measures.

Your current IT provider does not need to know about this assessment. Your time commitment is minimal — about one hour for the initial meeting and another hour for a follow-up to review our detailed Report of Findings.

To Request Your FREE Assessment,

please visit **bluetech.tech** or call our office at 08 8922 0000

When This Risk Assessment IS Complete, You Will Know:

- Whether your employees' login credentials are being sold on the dark web. We'll run a live scan on your company right in your office (results are confidential and only shared with you). It's rare not to find compromised credentials—and what we find will likely surprise you.
- If your IT systems and data are truly secured against hackers, cybercriminals, viruses, worms, and even sabotage by rogue employees.
- Whether your current backups would allow you to quickly restore operations if ransomware locked all your files. In 99% of networks we've reviewed, owners were shocked to learn their backups wouldn't survive such an attack.
- How well your employees can spot phishing emails. We actually put them to the test—and no company has ever scored 100%.

If we do find any issues—like security gaps, weak backups, compromised passwords, outdated firewall or antivirus software, or even malware on any of your computers—we'll put together a straightforward Action Plan to fix them. And if you want, we can handle the whole fix for you.

Just so you know, everything we talk about and find during this process will stay completely confidential.

Why Free?

Simply put, we want the chance to show you why BlueReef Technology is the most competent, responsive, and trusted IT services provider for small businesses across Australia.

We also understand you might be fed up with poor service, bad advice, or feeling sold to by other IT companies. That's completely fair — trust is earned, not given.

That's why this assessment is 100% free, with no strings attached. Our goal is to earn your trust by sharing honest, fact-based insights so you can make an informed decision.

If it feels like a good fit, then we can talk about working together — no pressure, no gimmicks, no hard sell.

To Request Your FREE Assessment,
please visit **bluetech.tech** or call our office at 08 8922 0000

Please...Do NOT Just Shrug This Off
What you should do next...

I know you're incredibly busy, and it's tempting to set this aside or tell yourself you'll worry about it later. That might be the easy choice, but easy rarely means right.

Here's the truth:
sooner or later, your business WILL face a cybersecurity event.

If you're prepared, it might only be a minor disruption. But if you wait and do nothing, the attack could be costly, damaging, and deeply disruptive.

You've worked hard to build your business—don't let some faceless cybercriminal take that away. And don't just hope your IT provider has everything covered.

Get the facts. Take action. Be certain your business is protected.

Contact Us And Schedule Your Free, CONFIDENTIAL Cybersecurity Risk Assessment Today!

To Request Your FREE Assessment,
please visit **bluetech.tech** or call
our office at 08 8922 0000

Dedicated to serving you,

Daniel Ladlow
Managing Director, BlueReef Technology
Web: bluereef.tech
Phone: 08 8922 0000
E-mail: daniell@bluereef.tech

P.S. From my conversations with IT pros and CEOs who've been hit by cyber-attacks, almost every one believed their IT provider "had things covered."

I'm connected with IT firms across Australia and beyond, and I can tell you that most simply haven't dealt with the kind of sophisticated, relentless attacks we're seeing today. That means it's very likely your current IT provider isn't fully protecting you—and that's why I'm offering this independent, no-obligation risk assessment.

As someone who leads BlueReef Technology and understands the challenges of running a business, I know you have to trust your team and vendors. But it's crucial to verify they're doing everything they should. Remember, it's YOUR reputation, YOUR money, and YOUR business on the line. If they slip up, it's YOUR nightmare to deal with.

Read On To Hear What Our Clients Have To Say:

"The single biggest benefit of using BlueReef Technology is they do what they say they are going to do. Period. An amazing concept!
With their support and the new Office 365, our technology is no longer a roadblock in our business.
If someone were on the fence about choosing BlueReef Technology as their IT firm, I say, get off the fence. BlueReef is giving us the support that other IT firms haven't.
That is a game changer in working with BlueReef Technology."

-Meegan Chandler

"Amazing service from the team at BlueReef. Fast set up of all our IT/Communications needs as well as getting our business website for ShieldTech Locksmiths & Security up and running. Professional and reliable."

-Damien Carey

"Always very professional and goes the extra mile to assist."

-Jeanette Green

To Request Your FREE Assessment,
please visit **bluetech.tech** or call our office at 08 8922 0000