Cyber Audit TEAM

INVESTING IN YOUR FUTURE:

THE BUSINESS CASE FOR A MANAGED DETECTION AND RESPONSE SOLUTION

CYBER AUDIT TEAM

Preface

Information and data security aren't just IT issues — they're core Governance, Risk and Compliance (GRC) organisational issues that if not adequately addressed and managed, can have a serious negative impact on your business, its brand, and reputation. Up to 90% of Australian businesses faced some sort of breach in the last year[1], and most didn't even know it. For businesses without Managed Security Services, the average time before a data breach is discovered and contained is 281 days[2].

So, what can happen in those 281 days? In addition to the loss of valuable company-owned IP, customer data, and productivity disruption, organisations can also face expensive regulatory compliance fines. Many organisations will also face damage — not only to their IT systems — but also to their brand reputation, resulting in a very costly outcome.

The uptick in the volume and sophistication of threats attacking businesses has only been increasing in recent years — and this is why Managed Detection & Response (MDR) is becoming more critical. MDR provides organisations with both a proactive and reactive response to information and data security threats. Without MDR, attacks will go unnoticed and have the potential to damage an organisation irreversibly.

We, at Cyber Audit Team, exist because we genuinely want to protect businesses from the pervasive cybersecurity threats that exist across every industry. This guide is designed to provide you with a framework to understand why MDR is critical to the success of your business, and how the return on investment can be quickly realised and maximised as a key differentiator for your business.

[1] Australian Cyber Security Centre

[2] 2019 Cost of a Data Breach Report, IBM & Ponemon

Why Data Protection & Privacy Matter

Data is the world's new natural resource and the lifeblood of every organisation in our digital age. We store employee data, financials, transactions, customer details, intellectual property, source code, and more. In doing so, we must acknowledge the information security risks and compliance factors at play in how we store, manage, process, retain, and transfer such data.

So, what happens to your business in the case of a security incident or data breach?

Your system becomes infected

With the significant escalation of targeted ransomware attacks, the breach will most likely result in your system becoming infected. Threat Actors have devised methods enabling them to identify your company's digital back-ups, exfiltrate your company's valuable data and IP, before encrypting your entire digital infrastructure (including online back-ups), locking you out of your own systems, and rendering your planned recovery efforts futile unless a digital ransom — such as Bitcoin — is paid.

Reactively remedying an attack costs money and time

Considering most attacks go unnoticed for 200+ days, retrospectively trying to remedy the attack can prove extremely costly for your organisation. In fact, $3m is the average cost of a data breach to Australian businesses[2]. Many businesses also face long bouts of productivity downtime when employees are locked out or customers unable to access their systems.

[2] 2019 Cost of a Data Breach Report, IBM & Ponemon

Personal data is leaked

Given that the majority[3] of security incidents and breaches are financially motivated, Personally Identifiable Information (PII) such as email addresses, phone numbers, addresses, and other sensitive data including customer credit card details, are often sold to malicious third parties. Organisations are now required by Australian law to disclose data breaches to the privacy regulator as soon as practicable, and to all affected persons within 30 days of discovery of the breach — failure to do so may result in major financial implications, with penalties up to $10m or 10% of an organisation's annual turnover[4].

Your brand reputation is damaged

A data breach of any kind negatively affects brand reputation and lost consumer trust that can be hard to recover from — 85% of Australians would stop dealing with an organisation if their data was breached[5]. Case in point — a series of data breaches and leaks **cost** Australian valuation firm Landmark White an estimated $8m, and the loss of numerous large **contracts**.

When organisations fail to incorporate data protection and privacy into their business strategy, there is a major financial and reputational cost to their brand. Organisations must ensure they have appropriate cybersecurity measures in place to deal with these issues.

[3] 2020 Data Breach Investigations Report, Verizon

[4] Part 4: Notifiable Data Breach (NDB) Scheme, Office of The Australian Information Commissioner

[5] 2019 Security Index Australia, Unisys

Could Managed Detection and Response be the Answer?

Protecting your data can be difficult, especially when you don't have visibility over your digital environment or active threats. Compounding this, the technologies used for threat detection and response are complicated and sometimes costly. But when your brand reputation and future is at stake, protecting your data should be a top priority.

Threat detection and response solutions

There are a number of threat detection and response solutions available, each with their own risks and benefits:

Do nothing: Sadly, aside from some minor IT security enhancements, most organisations opt to do nothing when it comes to their information security. When this is the action taken, you should anticipate a big bill for a data breach and recovery.

Build internal capabilities: In-house teams and solutions are costly, time consuming, and complex, and are best suited to larger organisations with the budget and resources to spare.

Partner with an MDR provider: This option enables speed to deploy, is affordable, and simpler to manage. It's suited to everyone from SMEs to large enterprises.

The benefits of MDR

While an MDR solution is fast to deploy, more affordable, and simpler to manage, it is also a long-term investment into the success of your organisation. MDR has a myriad of other benefits to your business including:

- MDR becomes your trusted "eyes and ears" throughout your digital infrastructure, actively investigating anything suspicious or abnormal. Those with MDR see **40% fewer security incidents per year[6].**

- MDR helps to improve cybersecurity maturity and risk management, without the need to invest in major resources, technology, or headcount. In fact, organisations with MDR are **4.6 times more likely to have improved security posture after two years[6].**

- MDR proactively monitors your landscape, which minimises risks and downtime for your organisation by **reducing security incident detection time by 80%[7].**

- If remediation efforts are required, they will be less costly and easier to fix. **82% of organisations with a strong cyber security posture report they are very effective with incident response[6].**

[6] The Relationship between Security Maturity and Business Enablement Infographic, AT&T Cybersecurity

[7] The Total Economic ImpactTM Of AlienVault® Unified Security Management®, Forrester Report

Justifying the Investment: How MDR can Transform your Business

Cyber Audit Team's Managed Detection and Response (MDR) is an advanced managed security service that is focused on security information and event management (SIEM), 24/7 incident analysis and response, threat intelligence, and threat hunting to ensure a proactive and mature information security posture.

MDR is an investment into the success of your organisation. In fact, 79% of organisations with a strong cyber security posture draw a direct line from security to business acumen[8]. Quantifying the ROI is possible, as well as creating points of difference for your business — however, it's the long-term protection and support provided by MDR that is the key to your success[9].

With Cyber Audit Team's MDR solution, your organisation will benefit from:

- Ongoing protection of your high-value, company-owned and customer data
- Peace of mind for the Board, your directors and your customers
- Protection of your brand reputation
- Reduced downtime and disruptions to the workings of your business in the case of a breach
- Compliance with laws and regulations
- Support with building customer and supply chain trust in your organisation
- Supported cybersecurity maturity and growth for the future

[8] The Relationship Between Security Maturity and Business Enablement Report, AT&T Cybersecurity
[9] ASIC Cyber Security Survey 2016

What others have to say about our MDR

It's not only the research that points to the relationship between business success and cybersecurity acumen[9], it's our clients who have seen the benefits first-hand.

"As one of Australia's largest charities, our Executive along with our Risk Committee made a determination to invest in preventive cybersecurity measures. We engaged Cyber Audit Team to secure corporate information systems and online fundraising platforms as well as mitigate corporate sponsors' brand and reputation risk. By taking a proactive approach to Managed Detection and Response, we aim to ensure critical donation website vulnerabilities or a possible data breach don't disrupt the success of our organisation."

CFO & Company Secretary, Fast-growing NFP

"Our ICT team have found Cyber Audit Team's service, skills and experience to be unquestionable. With their hands-on partnership, we've been able to continually grow our security posture with them by our side. They've helped us implement a vast number of cybersecurity maturity improvements including to the minute security information and event monitoring for all of our servers and systems. We've prioritised these based on proactive risk reduction, vulnerability detection, incident response and compliance to ensure we protect the data and privacy of our customers and 3rd parties as well as enhance trust in our brand."

GM ICT, Leading Travel Retailer

"We are a medium-size business that operates in financial services — so data security is paramount. Essentially, we face the same data risks as big business but have a smaller budget. We needed a solution that provided scalable security outcomes in a streamlined and concise package. Cyber Audit Team have been able to deliver this solution giving us confidence around our security posture and delivering ongoing surveillance services. We highly recommend Cyber Audit Team."

COO, Private Wealth Management Firm

[9] ASIC Cyber Security Survey 2016

Cyber Audit TEAM

Want to learn more about how our Managed Detection & Response solution could benefit your company? Get in touch with one of our specialists today.

enquiries@cyberauditteam.com

Cyber Audit Team is an independent, Australian owned and operated, Managed Detection and Response service provider. The multi-disciplinary team of highly experienced industry specialists provide simplified end-to-end Information security solutions as well as support and guidance to businesses of all sizes across various industries.

Cyber Audit Team
4 Helensvale Road
Helensvale QLD 4212
Australia

P: 1300 077 022

E: enquiries@cyberauditteam.com

W: cyberauditteam.com

Follow us on LinkedIn & Twitter
@cyberauditteam