+44 345 094 0945
www.waterstons.com

Article

Oct 2023

# Cracking the Cybersecurity ROI Code: Why It's More Vital Than Ever

For years, there has been a consistent notion in Australia that cybersecurity rarely delivers a 'worthy' ROI. Scepticism often takes form in asking "Why invest when we have never been breached?" or "It won't happen to us, hackers aren't interested in us?"

**Cyber Security and Return on Investment (ROI)**

For years, there has been a consistent notion in Australia that cybersecurity rarely delivers a 'worthy' ROI. Scepticism often takes form in asking "Why invest when we have never been breached?" or "It won't happen to us, hackers aren't interested in us?" Historically, it has been difficult to quantify the ROI on cybersecurity. However, the landscape is evolving rapidly and examples like OPTUS, Medibank and others have demonstrated front and centre the devastating impacts on business. The repercussions, encompassing reputational damage and financial loss can be catastrophic. Especially if you're not financially equipped to bounce back.

**Security Manager as a Service and ROI**

Opting for a service like SMaaS (Security Manager as a Service) offers substantial value into bolstering your organisation's security. It also lays the groundwork for building a compelling ROI business case, as SMaaS experts not only possess the technical know-how to protect your organisation but also the invaluable ability to convey the significance of security measures to senior leadership and boards. We've categorised the ROI into seven essential components.

**Cost Avoidance**

Could you answer this question: *How much would downtime cost you per day, per week or even per month if you were to be breached?* If this is a question that stumps you, your Security Manager will collaborate with you to understand the potential financial implications.

For context, the average cost of a cyber breach is rising annually at a rate of 15%. Global statistics indicate that on average, a breach alarmingly costs organisations USD 4.45 million.

Understanding the costs to your organisation and the financial loss you may incur can help provide valuable insight into the money you invest and why.

**Reputation**

There are positive and negatives to this one, let us explain.

A data breach or the inability to fulfill contracts and client expectations can tarnish your reputation. It takes only one breach to destroy the hard work and dedication necessary to build strong client relationships.

Conversely, enhancing your security posture is an appealing quality and, in some cases, a prerequisite for winning new business. As an example, certain sectors must comply with frameworks such as ISO27001 (and whilst a fantastic target to aim for), is not necessarily the best option for all organisations.

The recent Australian Community Attitudes to Privacy Survey showcases the increasing importance places on data privacy and security by consumers. A key finding in the survey is that consumers now value data privacy as their 3rd most important factor when choosing a product and service. Click here to learn more about this survey.

Utilising SMaaS demonstrates to clients and the market that you stand out among your competitors and are committed to security.

**Data Protection and Compliance**

The aftermath of the Optus breach prompted the Australian government to impose heavier fines for repeated privacy breaches, up to $50 million or 30% of a company's turnover, aligning Australia with global standards.

Further regulations are on the horizon and legislation is changing to reflect today's evolving cyber-conscious economy, aiming to fortify the nation's security by 2030. This presents opportunities and challenges that businesses must address promptly to stay ahead.

**Reduced Business Risk**

In a world where businesses aspire to minimise risks, it's essential to include mitigating cyber security risks. With more companies operating online and remotely, the risk landscape has expanded.

A Security Manager will employ a rigorous risk assessment methodology to uncover vulnerabilities in organisational data and identify avenues for improvement.

**Recruitment and Retention**

While SMaaS mitigates the risks associated with the Security Manager role, it also enhances the overall work environment, safeguarding all employees.

The survey above highlights that people now expect this level of protection, potentially saving the cost of future hires.

With over 17,000 cyber security vacancies projected by AustCyber by 2026, SMaaS is an invaluable resource to removes several obstacles to tackle this challenge. We've covered more of this in another article. Click here to learn more.

**Rapidly Evolving Security Landscape**

In the face of a rapidly changing security landscape, maintaining an in-house Security Manager can be challenging. SMaaS offers numerous benefits through its extensive team that keeps abreast of evolving trends, ultimately saving you both time and money.

**Training and Awareness**

A significant portion of breaches have been incited by the human element. Addressing this issue in your organisation is imperative, as even incidents categorised as 'cyber incidents' often stem from phishing e-mails or stolen/compromised credentials.

Training your employees is crucial, and SMaaS can incorporate gamification in their training/awareness regime to ensure the message resonates, cultivating a cyber-aware culture across your organisation. Learn more about our cybersecurity game, Udder Disaster here.

**Insurance**

The landscape for Cyber Insurance is evolving rapidly. Renewing your policies have become increasingly challenging as the number of claims surge year on year. Investing in cybersecurity and good cyber hygiene can not only enable you to obtain insurance but also significantly reduce your organisations premiums.

A win-win for security and your bottom line.

**Summary of Cyber ROI**

Embracing cybersecurity measures can be a strategic benefit for Australian businesses seeking a substantial Return on Investment (ROI).

For too long, scepticism prevailed, with doubts about the necessity of cybersecurity investments when "it won't happen to us." However, evolving dynamics underscore the critical role of cybersecurity.

Recent high-profile breaches, including those experienced by OPTUS and Medibank, have demonstrated the dire consequences, from reputational damage to financial turmoil. Security Manager as a Service (SMaaS) emerges as a potent solution, offering not just technical expertise but also the ability to articulate the significance of security to senior leadership.

The ROI components encompass cost avoidance, reputation safeguarding, data protection and compliance, risk reduction, recruitment and retention advantages, and staying attuned to the rapidly evolving security landscape.

The bottom line? Investing in cybersecurity enhances not only security but also financial stability – a win-win for your organisation's future.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today’s cyber conscious economy.

**Empower your organisation today, get in touch with one of our team members - 24/7**

**info@waterstons.com.au | 02 9160 8430**