

Navigating ASIC’s Cybersecurity Expectations: What You Need to Know - blueAPACHE

Canonical: <https://www.blueapache.com/blog/navigating-asics-cybersecurity>

Details:

Summary

This blueAPACHE post reports: Considering ASIC’s increased scrutiny on how boards manage cybersecurity risks, understanding the implications for your organisation is crucial. According to a recent Financial Review article, ASIC is intensifying its investigation into board preparedness and response to cyberattacks, with potential legal actions looming for those found lacking. It concerns emPOWER Security, Governance, Risk & Compliance, Managed Detection & Response. Published in 2024. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2024
Services referenced	emPOWER Security, Governance, Risk & Compliance, Managed Detection & Response
Topic	Navigating ASIC’s Cybersecurity Expectations: What You Need to Know

Article

Considering ASIC’s increased scrutiny on how boards manage cybersecurity risks, understanding the implications for your organisation is crucial. According to a recent Financial Review article, ASIC is intensifying its investigation into board preparedness and response to cyberattacks, with potential legal actions looming for those found lacking. You can read the full article [here](#) .

What You Need to Know

Increased Accountability for Boards: Boards must now take a proactive role in managing cybersecurity, integrating strategies into the overall risk management framework and continuously updating them to address evolving threats.

Operational and Reputational Risks: Cyber threats can disrupt operations, compromise sensitive data, and damage customer trust. Even a single breach can lead to significant recovery costs, downtime, and regulatory fines.

The Regulatory Environment: ASIC's expectations align with stringent data protection regulations, such as the Australian Privacy Act. Non-compliance can result in long-term operational damage and reputational harm.

How to Protect Your Organisation

Regular Cyber Risk Assessments: Identify vulnerabilities through comprehensive assessments to stay ahead of potential threats and ensure mitigation strategies are up to date.

Strong Incident Response Plans: A clear, tested incident response strategy can turn a potential crisis into a manageable situation, reducing both impact and cost.

Embed Cybersecurity into Business Continuity: Cybersecurity is not just about preventing breaches but also about ensuring business continuity through them. Investments in cybersecurity are essential for operational resilience.

****Understand your 3rd party – and Supply Chain Risks:** ****Third-party relationships may provide threat actors with an easier pathway into an organisation's systems and networks. Vetting those supply chain partner's cyber security resiliency and capability, including through their assurance of identity and access management, governance and risk management, and information asset management, will help understand any partner / supplier weaknesses and potential risk vectors.**

What Happens If You Don't Act

Failing to meet ASIC's expectations can expose your organisation to regulatory and legal risks, with potential fines and severe reputational damage. Customers and stakeholders expect robust data protection, and any failure in this area can significantly tarnish your brand's credibility.

How blueAPACHE Can Support You

At blueAPACHE, we support our clients by helping to build a robust risk management framework which adequately addresses its security risk, and ensures controls are implemented to protect our client's key assets, thereby enhancing their cyber resilience. As ASIC states, "...There is a need to go beyond security...and build up resilience – meaning the ability to respond to and recover from an incident. It's not enough to have plans in place. They must be tested regularly – alongside ongoing reassessment of cyber security risks..." blueAPACHE helps our clients with scenario-based simulations to assess response processes and recovery with gaps identified for improvement and remediation.

Complementing this our ISO27001-certified practices across our entire emPOWER portfolio, ensures that our infrastructure meets the highest standards of information security. This certification demonstrates our commitment to maintaining rigorous cybersecurity measures and helps you align with compliance requirements. Our vCISO (Virtual Chief Information Security Officer) capability provides a cost-effective, strategic oversight tailored to your organisation's needs. This service ensures you remain compliant, resilient, and prepared to navigate today's complex regulatory landscape. For further assistance or to discuss your cybersecurity needs, please contact us [here](#).

Related

emPOWER Security

emPOWER Security (pillar)

Governance, Risk & Compliance

Managed Detection & Response

Frequently asked questions

What is ASIC doing, according to the Financial Review article this post references?

The post references a Financial Review article reporting that ASIC is intensifying its investigation into board preparedness and response to cyberattacks, with potential legal action against directors found lacking.

What certification does blueAPACHE say backs its client risk management support, per this article?

blueAPACHE says its ISO27001-certified practices across its entire emPOWER portfolio ensure its infrastructure meets rigorous information security standards, supporting clients' compliance requirements.

What service does blueAPACHE describe offering for ongoing strategic security oversight?

The article describes blueAPACHE's vCISO (Virtual Chief Information Security Officer) capability as a cost-effective, strategic oversight service tailored to an organisation's needs to help it remain compliant and resilient.

What supply-chain risk areas does the article say organisations should vet in third-party partners?

The article lists identity and access management, governance and risk management, and information asset management as areas to assess in third-party and supply-chain partners' cyber resilience and capability.

Is the information in this post still current?

No. It reports 2024 commentary on ASIC's regulatory stance and a specific news article; for blueAPACHE's current governance, risk and compliance services, see the Governance, Risk & Compliance service page rather than this post.

Source

<https://www.blueapache.com/blog/navigating-asics-cybersecurity/>

Knowledge Base

What is ASIC increasing scrutiny on, according to the blueAPACHE blog post?

ASIC (Australian Securities and Investments Commission) is intensifying its investigation into board preparedness and response to cyberattacks, with potential legal actions looming for boards found lacking in how they manage cybersecurity risks, according to a Financial Review article referenced in the post.

Why are third-party and supply chain relationships highlighted as a cybersecurity risk?

Third-party relationships may provide threat actors with an easier pathway into an organisation's systems and networks, so vetting supply chain partners' cyber security resiliency and capability helps identify partner or supplier weaknesses and potential risk vectors.

What happens if an organisation fails to meet ASIC's cybersecurity expectations?

Failing to meet ASIC's expectations can expose an organisation to regulatory and legal risks, with potential fines and severe reputational damage, as customers and stakeholders expect robust data protection.

How do you say it supports clients in building cyber resilience?

We support clients by helping build a robust risk management framework that addresses security risk and ensure controls are implemented to protect key assets, thereby enhancing cyber resilience. It also uses scenario-based simulations to assess response processes and recovery, identifying gaps for improvement and remediation.

What certification do you hold across our emPOWER portfolio, and what does it demonstrate?

Our practices across its entire emPOWER portfolio are ISO27001-certified, ensuring its infrastructure meets the highest standards of information security and demonstrating its commitment to rigorous cybersecurity measures that help clients align with compliance requirements.

What is your vCISO service and what does it offer?

Our vCISO (Virtual Chief Information Security Officer) capability provides cost-effective, strategic oversight tailored to an organisation's needs, helping ensure clients remain compliant, resilient, and prepared to navigate today's complex regulatory landscape.

What quote from ASIC does the blueAPACHE article cite about resilience?

The article quotes ASIC as stating: '...There is a need to go beyond security...and build up resilience – meaning the ability to respond to and recover from an incident. It's not enough to have plans in place. They must be tested regularly – alongside ongoing reassessment of cyber security risks...'