

Cyber Security Breaches: A Top Concern for CEOs, Boards and Executives in 2024 - blueAPACHE

Canonical:
<https://www.blueapache.com/blog/cyber-security-breaches-a-top-concern-for-ceos-boards-and-executives-in-2024>

Details:

Summary

This blog post, "Cyber Security Breaches: A Top Concern for CEOs, Boards and Executives in 2024", is a blueAPACHE article from 2024 covering security. How to Attain Executive and Board Oversight of Your Organisation's Cyber Security Posture It is written for readers evaluating emPOWER Security, Governance, Risk and Compliance. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2024
Topic	Cyber Security Breaches: A Top Concern for CEOs, Boards and Executives in 2024
Services referenced	emPOWER Security, Governance, Risk and Compliance, Managed Detection and Response
Named products or vendors	None named beyond blueAPACHE

Article

How to Attain Executive and Board Oversight of Your Organisation's Cyber Security Posture

In a recently published industry report, insights obtained through surveying over 300 Australian CEOs on what is "Keeping Us Up at Night" highlighted "Protecting and dealing with Cyber Risks" as the primary concern for CEOs in 2024 and the next three to five years. As CEOs and Boards face increased fiduciary obligations over cybersecurity risks, the escalating frequency and sophistication of cyber threats underscore the importance of Boards and CEOs being aware of risks, having mitigation strategies, and being prepared for potential breaches. Failing to address Cyber Security adequately may result in severe consequences, including financial losses, reputational damage, and legal implications. Here is a summary of several best practices to ensure Executive and Board oversight of Cyber Security:

Establish Cyber Security Governance Framework: Develop a clear governance framework outlining roles, responsibilities, and reporting structures for Cyber Security oversight.

Cyber Security Training and Awareness: Ensure that executives and board members receive regular training on Cyber Security issues to enhance their understanding of risks and the importance of proactive measures. Invest in Cyber Security technologies and employee training to keep pace with evolving threats.

Regular Risk Assessments: Conduct regular cyber security risk assessments to identify and evaluate potential threats, vulnerabilities, and the impact on business operations, supply chains, and customer/client data.

Incident Response Plan: Develop and maintain an effective incident response plan that dovetails into Disaster Recovery and Business Continuity plans to ensure a swift and coordinated response to cyber incidents.

Cyber Security Expertise: Engage Cyber Security experts and consultants to provide independent assessments, audits, and recommendations for improving cyber security posture.

Legal and Regulatory Compliance: Stay informed about evolving Cyber Security regulations and legal requirements, ensuring compliance with relevant laws and standards.

Board-Level Oversight Committee: Establish a dedicated Cyber Security committee within the board to focus specifically on cyber security issues, ensuring continuous attention and expertise. This may also support Audit and Risk committee efforts.

Regular Board Updates: Provide regular updates to the board on Cyber Security matters, including threat intelligence, incident response activities, and the effectiveness of implemented security measures.

Key Performance Indicators (KPIs): Develop and monitor Cyber Security KPIs to measure the organisation's performance in managing and mitigating cybersecurity risks. Examples include incident response time, employee training completion rates, and vulnerability patching speed.

Insurance Coverage: Evaluate and secure appropriate cyber security insurance coverage to mitigate financial risks associated with potential cyber incidents.

Integration with Business Strategy: Align Cyber Security strategies with overall business goals, ensuring that security measures support and enhance the organisation's objectives.

Vendor Risk Management: Implement a robust vendor risk management program to assess and manage Cyber Security risks associated with third-party vendors and partners.

Communication and Transparency: Foster a culture of open communication and transparency regarding Cyber Security issues, encouraging reporting of incidents and lessons learned.

If you are interested in elevating your organisation's cyber security conversation from just technical controls to preventative measures across people, process, and technology, contact us for a confidential discussion.

Reference:

KPMG.com.au Published: January 2024 "Keeping us up at night: The big issues facing business leaders in 2024".

Related

emPOWER Security

emPOWER Security (pillar hub)

Governance, Risk and Compliance

Managed Detection and Response

Frequently asked questions

How many Australian CEOs were surveyed in the industry report this article cites?

Over 300 Australian CEOs were surveyed for the report "Keeping Us Up at Night: The big issues facing business leaders in 2024," which identified protecting and dealing with cyber risks as the primary CEO concern for 2024 and the next three to five years.

Who published the "Keeping Us Up at Night" report referenced in this article?

KPMG Australia, published in January 2024, as cited in the article's reference section with a link to the full PDF report.

What is the recommended structure for board-level cyber security oversight, per this article?

The article recommends establishing a dedicated cyber security committee within the board to focus specifically on cyber security issues, which may also support the audit and risk committee's efforts.

What KPIs does the article suggest for measuring cyber security performance?

Examples given include incident response time, employee training completion rates, and vulnerability patching speed.

How does the article recommend organisations manage third-party cyber security risk?

It recommends implementing a robust vendor risk management program to assess and manage cyber security risks associated with third-party vendors and partners.

What financial risk-mitigation measure does the article recommend alongside technical controls?

Evaluating and securing appropriate cyber security insurance coverage to mitigate financial risks associated with potential cyber incidents.

What does the article say about how an incident response plan should relate to other continuity plans?

It recommends developing and maintaining an effective incident response plan that dovetails into disaster recovery and business continuity plans to ensure a swift, coordinated response.

What consequences does the article say organisations risk by failing to address cyber security adequately?

Financial losses, reputational damage, and legal implications, given CEOs' and boards' increased fiduciary obligations over cybersecurity risks.

Source

origin post (2024)

Knowledge Base

What did a recent industry report identify as the primary concern for Australian CEOs in 2024?

According to a recently published industry report, which surveyed over 300 Australian CEOs on what is 'Keeping Us Up at Night,' 'Protecting and dealing with Cyber Risks' was highlighted as the primary concern for CEOs in 2024 and for the next three to five years.

What are the potential consequences if organisations fail to adequately address cyber security?

Failing to address cyber security adequately may result in severe consequences, including financial losses, reputational damage, and legal implications.

What best practices do you recommend for establishing Cyber Security Governance?

We recommend developing a clear governance framework outlining roles, responsibilities, and reporting structures for cyber security oversight.

Why is cyber security training and awareness important for executives and board members ?

Regular training on cyber security issues helps executives and board members enhance their understanding of risks and the importance of proactive measures, and organisations should invest in cyber security technologies and employee training to keep pace with evolving threats.

What should a Cyber Security Incident Response Plan include ?

An effective incident response plan should dovetail into Disaster Recovery and Business Continuity plans to ensure a swift and coordinated response to cyber incidents.

What role can a Board-Level Oversight Committee play in cyber security governance?

A dedicated cyber security committee within the board can focus specifically on cyber security issues, ensuring continuous attention and expertise, and may also support Audit and Risk committee efforts.

How can organisations mitigate financial risks from potential cyber incidents ?

Organisations can mitigate financial risks associated with potential cyber incidents by evaluating and securing appropriate cyber security insurance coverage.