CISO PLAYBOOK SERIES

CYBER LEADERSHIP INSTITUTE
KNOW YOU'RE READY

CISO PLAYBOOK:
CYBER RESILIENCE GOVERNANCE

Developing lean, efficient and effective cyber governance structures

CISO PLAYBOOK:

CYBER RESILIENCE GOVERNANCE

Developing lean, efficient and effective cyber governance structures

EXECUTIVE SUMMARY 4

INTRODUCTION AND PURPOSE 7

MAJOR BUSINESS PAIN POINTS 8

ACTION PLAN 10

1. CLOSE THE EXPECTATIONS GAP 11
2. ESTABLISH A CYBER-RISK GOVERNANCE COMMITTEE 11
3. ESTABLISH OPERATIONAL GOVERNANCE FORUMS 13
4. ENCOURAGE DEEPER BOARD-LEVEL CYBERSECURITY CONVERSATIONS 14
5. EMPOWER THE CHIEF INFORMATION SECURITY OFFICER (CISO) 15
6. CLEARLY ARTICULATE YOUR CYBER-RISK APPETITE 16
7. INVEST IN CYBERSECURITY INSURANCE 18
8. BOARD CYBER-RISK METRICS 18

CONCLUSION 20

APPENDIX 21

ABOUT CYBER LEADERSHIP INSTITUTE 22

THE CYBER LEADERSHIP INSTITUTE 22
ABOUT THE CYBER LEADERSHIP INSTITUTE 22
JOIN THE CYBER LEADERSHIP HUB 22
CONTACT US 22

REFERENCES 23

EXECUTIVE SUMMARY

This playbook proposes a series of recommendations for implementation of an effective cyber governance strategy through the following approach:

- Create tone at the top, pushing cyber security accountability to the most senior business executives, and keeping the board fully informed of the cyber risk profile and their fiduciary responsibilities.
- Maintain a comprehensive cyber risk profile, enabling the enterprise to direct limited resources towards areas of highest risk exposure, thus eliminating waste.
- Awareness of the cyber threat landscape and understanding the advanced persistent threats that need to be identified and managed
- Enabling good practices to ensure the business operates in a highly adaptive and responsive way with such a rapidly changing cyber environment
- Teach organisations to become cyber resilient through embedding cyber-risk governance into the bloodstream of their enterprises, making it an inevitable and inconspicuous part of strategic and operational decision-making, fostering transparency and accountability
- Implement lean and efficient structures that can rapidly and flexibly adapt to reflect changing market needs or business circumstances

Through these recommendations, you can expect the following benefits:

- Diffuse common tensions between security and business teams, reinforce business buy-in for important cybersecurity initiatives and promote the articulation of cybersecurity issues in business terms. Most importantly, you will be able to align the cybersecurity strategy with enterprise goals.
- Ensure senior executives are not mired in day-to-day technology operations and free up time for them to run the business and focus on the strategic aspects of cyber risk.
- Create deep and open relationships of trust, align board and management agendas,
- Give the board insight into how the board and management of how similar organisations are addressing cyber risk.
- Promote business agility and efficiency as cybersecurity teams can make risk decisions faster, balancing the need to protect critical assets and speed to market.

Consider the analysis in this book to help frame the understanding effective cyber governance for your enterprise. The recommendations and the nine-phased approach are supported by the analysis. Detail on the nine-phased approach can be found in the Action Plan section of this book.

Below are the top 10 recommendations both organisations can benefit and gain value from:

RECOMMENDATIONS

1 Align cyber strategy and risk management to corporate goals

The cyber resilience strategy and risk management frameworks must be rooted in the corporate strategy, regulatory environment. Only that way can the cyber governance framework support, not impede on, corporate goals.

2 Establish a Cyber Risk Governance Committee

Develop a clear understanding of data privacy laws applicable to jurisdictions where your enterprise operates, as well as other external data protection obligations, such as the SWIFT Mandatory Security Controls, PCI DSS, or other contractual obligations.

3 Establish Operational Governance Forums

Used to report key matters to the cyber risk committee and support consistent implementation of security controls across the enterprise. Operational risk registers must be rigorously maintained to track detailed cyber risks, which aggregate into the corporate cyber risk register.

4 Encourage board level cyber security conversations

The board should challenge the adequacy of risk measures against business appetite and business strategy, through the appropriate and important questions. Bring the outside in by inviting management consultants with proven ability to inform the board if they are over or underspending on cyber security. The CISO must have direct access to the board to enable candid conversations and ensure key messages are not lost in translation or needless hierarchies.

5 Create Appropriate Reporting Lines

Ideally, the CISO must report to the CEO, especially for companies whose survival depends on the protection of digital assets. We however acknowledge this is not feasible in most circumstances. The CISO must not report to the CIO as that creates a material conflict of interest. An alternative is for the CISO to report to the Chief Risk Officer.

6 Ensure your Cyber Risk Appetite is Clearly Articulated

Clearly articulate the cyber risk appetite so risks are clearly understood and effectively managed, thus enabling the business to make critical decisions faster without exposing the organisation to risks beyond its capital capacity.

7 Simulate Cyber Incident Response Exercises

Business leaders have a responsibility to take deliberate steps to anticipate major cyber breach scenarios and assess the adequacy of response measures through 'drills' or risk simulation exercises to identify major impact from plausible cyber scenarios.

8 Purchase cyber security insurance

Covering both internal and external losses resulting from a cyber-attack, insulating the business from plausible, high-impact cyber breach scenarios.

9 Use board cyber risk metrics

An essential tool to inform an enterprise's board of directors of the organisation's vulnerabilities and strength of its defences, two factors that an organisation can influence.

10 Ensure you have a secure cyber governance strategy

Implementing the recommendations in this playbook while tailoring the strategy to suit your business will guarantee your organisation to be one step ahead.

INTRODUCTION AND **PURPOSE**

Throughout this playbook, you will find practical guidelines to identify and implement effective cyber governance strategies to develop a highly focused cyber resilient organisation.

The role of corporate directors in cyber risk oversight has been cast into spotlight by a succession of high-profile cyber risk events, including recent hacker incursions at Equifax, Uber, Facebook, Google and several other well-regarded corporations. Regulators are also tightening the squeeze, seeking positive affirmation from boards that their cyber risk governance structures are effective and fit for purpose.

The rising customer, investor, shareholder and regulatory expectations have merit; most data breaches have their roots in profound lapses in corporate governance, not technology, as commonly perceived. Given the stakes are so high, an increasing number of corporate directors are seeking deeper insight into cyber risk and its potential impact on their strategic priorities and regulatory compliance.

Cyber-resilient enterprises acknowledge now widely that board oversight and C-suite leadership are essential to driving any transformational change, and that cybersecurity is no exception. Their most senior business officers and the board of directors provide unwavering support for cybersecurity programs. They role model expected behaviours and uphold the virtues of their cyber- risk appetite. They embed cyber-risk governance into the bloodstream of their enterprises, making it an inevitable and inconspicuous part of strategic and operational decision-making, and, as a result, foster transparency and accountability. Cyber-resilient enterprises reject needlessly complex and rigid decision-making structures that impede prompt strategy execution. Instead, they favour lean and efficient structures that can rapidly and flexibly adapt to reflect changing market needs or business circumstances.

Given the stakes are so high, the board and senior business officers should be closely involved in cybersecurity issues. This sentiment was echoed by the Committee of Sponsoring Organisations for the Treadway Commission (COSO), which stated, 'Today, more than ever, boards of directors need to demonstrate their understanding of cyber trends that could impact the organisation's ability to achieve its objectives. The board plays a fundamental role in being secure, vigilant, and resilient by understanding cyber risks, confirming preventative and detective controls are in place to manage such risks'. Simply put, totally delegating the issue of cyber risk to middle management is a risky business.

MAJOR BUSINESS PAIN POINTS

Boards of directors now widely appreciate the significance of cyber risk and are seeking deeper insight into cybersecurity issues and their business implications. But despite the growing enthusiasm, most corporate directors still find cyber security highly cryptic and existing frameworks tedious. Predictably, a recent Deloitte study painted a grim picture regarding CEOs and directors' involvement in cyber security, with only 38 percent of polled CEOs and 23 percent of board members identifying themselves as "highly engaged" in the subject.

Despite the significance of cybersecurity and growing enthusiasm from senior executives, a serious obstacle exists. Compounding this challenge, cybersecurity professionals often provide highly ambiguous cybersecurity reports, accompanied by low level, detailed metrics to senior business executives. Such information leaves senior business leaders frustrated or unclear about key threats targeting their businesses, the strength of their existing defences or what investment is required. Most business leaders have long perceived cybersecurity as too complex. The excessive use of security jargon – some unfathomable even to other technology professionals – further reinforces this opinion.

A wide range of cybersecurity metrics exist, including vulnerabilities, misconfigurations, and threat intelligence, but translating these into useful knowledge for business leaders remains a significant challenge. No wonder that 91 percent of the directors polled by NASDAQ and security firm Tanium in 2016 conceded that they don't understand cybersecurity reports.

Some of the key challenges identified by enterprises are listed below:

CURRENT BUSINESS CHALLENGES

a

Limited executive buy-in into cybersecurity programs. Most business executives and boards simply don't care about cyber security until something goes horribly wrong, such as a major data breach, loss of a major potential deal or a regulatory undertaking.

b

A growing list of poorly secured business partners without proper governance framework to oversight that risk and ensure operational effectiveness of key controls.

c

Expansive cyber security governance frameworks often impractical for SME enterprises to implement given limited budgets.

d

Heavily diluted, one-size-fits-all strategies. Attempts to implement equal governance measures over hundreds of systems and processes, each of varying business significance spells failure from the start.

e

The widespread use of vain metrics that have their roots in technologies, not business risk, leaves senior management unclear of their cyber blind spots.

f

Majority of CISOs / Head of Cyber Security hail from technical background and often struggle to implement risk-based governance frameworks and report up to the board in business terms. Consequently, securing buy-in is an uphill task.

ACTION PLAN

How can an enterprise encourage executive leadership and improve board oversight of this vital business risk? What should enterprises do to improve their management's level of engagement with cybersecurity and cybersecurity professionals? The next steps offer solutions to these important questions.

1 CLOSE THE EXPECTATIONS GAP

To address this enduring challenge, CISOs should raise their game, move away from numbing cybersecurity vocabulary, and learn to speak the language of the businesses they work with. Boards of directors have very limited time at their disposal and are not comfortable discussing ISO 27001 reports or NIST standards. Rather, they are concerned about how cyber risk will impact new product success, business growth, the cost of capital, innovation, customer trust, profitability and other crucial business priorities.

Doing so requires:

- Linking cyber risk to corporate objectives through developing an in-depth understanding of business operations, value chain, strategic priorities, risk appetite and regulatory environment.
- CISOs to become provocative storytellers to persuade the board and executive management to act. Risk maps and detailed metrics are not enough, sustained governance requires CISOs to simplify cyber risk in business terms, enlisting board and executive support.
- Effective leadership includes role modelling, active participation by c-level executives in cyber drills and holding personnel accountable for maintaining robust cybersecurity controls.
- Business leaders are to embed cybersecurity into vital business processes, such as product development, digital transformation or acquisitions.

For too long, cybersecurity professionals have advocated for greater business visibility and influence. But they also need to play their part, particularly by articulating this crucial business risk in ways non-IT business leaders find relatable and understandable.

2 ESTABLISH A CYBER-RISK GOVERNANCE COMMITTEE

Underpinning any cyber-resilient environment is a strong governance framework. To that end, the board should establish a dedicated cyber-risk committee comprised of senior business, technology and risk executives tasked with ensuring the business maintains strong defences against current and emerging cybersecurity threats. They should also ensure that the business is not exposed to risks outside its determined risk tolerances. The cyber-risk committee should be chaired by the Chief Information Security Officer (CISO). Acceptance of this responsibility by the CISO naturally elevates this critical role within the business. Senior business officers, such as the Chief Executive Officer, Chief Information Officer, General Counsel, Public Relations Officer, Chief Customer Officer, Chief Operations Officer and the Chief Financial Officer should all be part of the cyber-risk committee.

BOARD OF DIRECTORS		
CYBER-RISK GOVERNANCE COMMITTEE (CHAIRED BY THE CISO)		
Monthly cyber security governance forums (Chaired by CISO)	**Monthly third party cyber security governance forums (Chaired by CISO)**	**Business unit level operational risk forums (Chaired by BU CRO)**
Chief Information Officer Chief Information Security Officer Cyber Security Managers Business operations Legal Technology Risk Managers	Chief Information Security Officer Commercial vendor management Business operations Legal	BU Chief risk officer BU aligned security managers BU enterprise risk managers Senior BU business and technology management

Above: Suggested structure for cybersecurity operational governance forums

Source: The Five Anchors of Cyber Resilience

The committee should be responsible for:

a. Ensuring the enterprise has a strong grasp on its most valuable digital assets, revalidates this grasp frequently and implements a mandatory set of non-negotiable controls around each asset

b. Keeping an eye on emerging threats, regulatory changes, key stakeholder expectations (of customers, business partners, shareholders and investors) and adjusting management priorities as required

c. Ensuring that the business maintains a fine balance between customer digital trust and convenience, and that cybersecurity acts as a key business enabler, not an inhibitor of innovation or agility

d. Reviewing and communicating the enterprise's cyber-risk appetite and ensuring its intent is clearly understood and institutionalised into critical decision-making processes

e. Keeping the board of directors fully informed about the enterprise's cybersecurity posture (challenges, capabilities and key initiatives to improve the risk profile)

f. Maintaining a pragmatic, business-aligned cyber-risk scorecard to measure the operating effectiveness of critical controls

g. Ensuring the business maintains a highly engaging program to promote positive risk-aware behaviours across employees, customers and business partners

h. Engaging external consultants to benchmark the maturity of the enterprise's cyber-risk profile against similar enterprises to identify key improvement opportunities

i. Ensuring the enterprise maintains a suitably qualified, motivated and well-funded cybersecurity team with appropriate reporting structures

j. Reviewing and challenging the enterprise's cyber assurance program to ensure areas of high risk are subject to independent reviews and all findings rated 'high' are promptly addressed

k. Actively participating in cyber-risk drills, ensuring all plausible scenarios are regularly tested and the enterprise maintains enough capital reserves to absorb cyber incident management activities

l. Ensuring critical responsibilities are clearly understood. This includes authorising disconnection of transactional systems from the internet in the event of a breach or contacting key customer segments and the media when required.

The advantages of establishing a cross-functional cyber-risk committee are clear – it helps diffuse common tensions between security and business teams, reinforces business buy-in for important cybersecurity initiatives and promotes the articulation of cybersecurity issues in business terms. Most importantly, it aligns the cybersecurity strategy with enterprise goals. The cyberthreat landscape and technology landscape are changing at breathtaking speeds. Accordingly, the cyber-risk committee should provide detailed cybersecurity updates to the board on a regular basis.

3 ESTABLISH A CYBER-RISK GOVERNANCE COMMITTEE

To maximise the value of the cyber-risk committee, enterprises should establish operational cyber-risk governance forums to support consistent implementation of cybersecurity controls across the enterprise and report key matters to the cyber-risk committee. This approach ensures senior executives are not mired in day-to-day technology operations and frees up time for them to run the business and focus on the strategic aspects of cyber risk. Operational governance forums may include, but are not limited to:

a. Monthly cybersecurity governance forums to track progress against key strategic initiatives, operational scorecards, material incidents and assurance programs.

b. Monthly third-party governance forums to track cybersecurity service level agreements (SLAs), operational scorecards and assurance processes over high-risk service providers and partners.

c. Business-unit-level cyber-governance forums comprised of senior business unit (BU) business and technology management. The forums should include cybersecurity managers, be chaired by the BU Chief Risk Officer (CRO) and oversee the effectiveness of security controls and improvement initiatives.

4 ENCOURAGE DEEPER BOARD-LEVEL CYBERSECURITY CONVERSATIONS

Despite the importance of technology to corporate strategies, most board members still lack technology experience. It's no longer enough for the board to 'note' cybersecurity reports on a quarterly basis. Effective cyber-risk management requires the board to challenge the adequacy of risk measures against business appetite and business strategy.

To have a good grasp of the enterprise cyber-risk posture, the board needs to ask several important questions:

a. What are our high-risk information assets, and do they have appropriate cybersecurity defences? (For example, are they running on vendor-supported infrastructure updated with the latest security patches?)

b. How do our cybersecurity capabilities, resourcing and spending compare with industry peers?

c. What are our current cybersecurity strategic initiatives and how do they support the overall mission? Are they aligned with enterprise goals to account for current and future needs?

d. How effective are our cyber breach response capabilities and have they been tested?

e. How effective are our cybersecurity assurance procedures of key business partners (especially those charged with handling sensitive information or connecting to the corporate network)?

f. How does the residual enterprise-level cyber-risk rating compare with our board-approved risk appetite, and what activities are in place to reduce our business risk exposure?

g. What were the top data breaches and other cyber-attacks in our industry and how has the business applied lessons learnt from those incidents?

The board should also consider inviting management consultants with proven ability who work across multiple customers to join the board in order to 'bring the outside in'. These external advisors can offer insight into how similar enterprises are tackling rising cyberthreats and anticipated regulation changes or could inform the board if they are over or underspending on cybersecurity.

These interactions must be handled with care for three key reasons:

- External consultants without a nuanced understanding of the enterprise's technology landscape and constraints can fuel board- management mistrust.
- Several consultants promise 'no obligations' advisory. But obligation- free consultancy is a fallacy – the reality is these consultants hope to sell a broad range of technologies or advisory services to fix the discussed cybersecurity concerns. Sidestepping the CISO therefore increases the odds that external consultants may exaggerate the enterprise's cyber-risk exposure, persuading the board to invest in valueless initiatives.
- There is also a slight possibility that management consultants themselves may be interested in the CISO role. This significantly affects their objectivity and can result in needless restructures, derailing key cybersecurity programs.

External advisors should therefore complement, rather than replace, internal governance and reporting structures. The key to navigating this challenge is having external advisors present their insights to the board in the presence of the CISO. This approach has two benefits: it creates open relationships of trust, where the board and management have mutual agendas, and doubly informs the board and management of how similar organisations are addressing cyber risk.

The board should develop a positive but skeptical attitude when interacting with management, as management may be inherently biased to overstate the effectiveness of controls and downplay the organisation's vulnerabilities, especially when management incentives are tied to cyber-risk metrics.

5 ENCOURAGE DEEPER BOARD-LEVEL CYBERSECURITY CONVERSATIONS

No matter how good a cyber resilience framework is, it's bound to get better if it is regularly tested and refined. The board has a responsibility for ensuring that a comprehensive cyber crisis management plan is in place and response capabilities are regularly tested against high-impact scenarios. Stress testing cyber response capabilities in controlled environments validates key assumptions, uncovers defective procedures and clarifies key responsibilities - reinforcing muscle memory and instilling business confidence.

Furthermore, cyber scenario drills answer some important questions:

- Who makes critical decisions during a cyber crisis event, such paying ransom if vital business files are rendered inaccessible without up-to-date backups?
- Does the organisation have up to date, offline backups to recover essential business processes if production systems are rendered inoperable or corrupted?
- Does the enterprise have cyber incident response retainer to ensure prompt access to incident response and forensics experts in the event of a data breach?
- Who is authorized to speak to the media, regulators, key customers or shareholders in the event of a major data breach?
- Which business functions are a priority if IT resources are significantly constrained by a cyber-attack?
- Does the enterprise have pre-canned messages for call center staff to provide consistent messages to customers in the event of a data breach?
- What has been the extent of incident response tests, e.g. has the organisation conducted full blown red teaming exercises to validate the capabilities of the blue team?

Attempting to make these critical decisions during a cyber emergency can lead to significant missteps, conflicted messages or internal squabbles, aggravating an already dire situation.

6 CLEARLY ARTICULATE YOUR CYBER-RISK APPETITE

Enterprises thrive by taking measured business risk, but stumble if these risks are not clearly understood and effectively managed. Business leaders are constantly making intelligent trade-offs between how much risk they are willing to take in pursuit of enterprise goals. A clearly articulated cyber-risk appetite statement – a formal articulation of the organisation's willingness to accept cyber risk – is a vital tool to enable an enterprise to make critical decisions faster without exposing the organisation to risks beyond its capital capacity. The cyber-risk governance committee should formulate the cyber- risk appetite and the board should ratify it, at a minimum, annually.

An effective cyber-risk appetite is one that's clearly understood by all employees, is actionable, measurable and supported by clear roles and responsibilities. The board of directors have ultimate responsibility to ratify the cyber-risk appetite, ensuring it supports the enterprise's objective and doesn't constrain innovation. This necessity was emphasised by a report by the Senior Supervisors Group, which stated, 'The board of directors should ensure that senior management establishes strong accountability structures to translate the RAF [risk appetite statement] into clear incentives and constraints for business lines.'205

Most cyber-risk appetite statements, however, are vague and don't provide any meaningful guidance to operational teams. For instance, a cyber-risk appetite that states that the enterprise has a low risk appetite for the loss of its business and customer data only stimulates boredom.

When formulating the enterprise's cyber-risk appetite, business leaders should be guided by two factors: the enterprise's capacity to absorb the accepted risks should they materialise, and its enterprise mission. An effective cyber-risk appetite is also tightly linked to an organisation's high-value digital assets, and takes into consideration external obligations to customers, investors, shareholders and regulators.

Below are some practical examples that illustrate a variety of risk appetites.

ILLUSTRATIVE EXAMPLES

HAS APPETITE

- Connecting employee owned devices to a corporate network if they undergo required security procedures.
- Partnering with third-party business or technology providers that have been assessed as having medium or low cyber-risk exposure to pursue unique capabilities, provided enough governance and monitoring processes are implemented to ensure the firm is not exposed to risks outside its tolerance.

HAS LIMITED APPETITE

- Partnering with third parties whose cyber-risk exposure has been assessed as 'medium', provided there is a solid commitment to address associated issues within a specific time frame.
- Acquiring new digital solutions with known vulnerabilities provided the vendor has reasonable, contractually enforceable commitments to address them.

HAS NO APPETITE

- Partnering with third-party suppliers whose cybersecurity risk exposure has been assessed as 'high'.
- Using public cloud environments to host high-risk information assets, such as intellectual property that underpins the enterprise's mission.
- Deliberate breach of security policies and associated procedures by employees.
- Taking the organisation's digital assets to high-cyber-risk countries that have not been certified by the cybersecurity team.
- Putting new digital offerings with known high-rated vulnerabilities into production.
- Allowing line managers to neglect validating access rights for their direct reports within a stipulated time frame.
- Exempting any non-negotiable cybersecurity control on high-risk systems, e.g. storing sensitive customer records in unencrypted form.
- Unjustified delay in applying critical vendor patches on high-risk applications

Technology, cyber risk and the business environment are all evolving at breathtaking speed. An enterprise cyber-risk appetite statement should therefore be constantly tightened or relaxed in line with evolving circumstances.

7 INVEST IN CYBERSECURITY INSURANCE

The board of directors, in exercising their fiduciary responsibilities, should ensure that the organisation maintains a comprehensive cyber insurance plan covering both internal and external losses resulting from a cyber-attack. Insurance companies have already started including cyber-risk exclusions on traditional covers, making it clear that businesses can experience severe shocks in the event of a significant breach.

The prevalence of high-profile cyber-attacks has prompted many businesses to complement existing cyber defences with cyber insurance cover, fueling the growth of the cyber insurance market. Consulting giant PwC predicts that the cyber insurance industry will triple to approximately US$7.5 billion by 2020 . Cyber related insurance claims are also on the rise. CFC Underwriting, the largest independent specialty Managing General Agent (MGA) in the UK, revealed that it handled more than 400 cyber-related claims in 2016, a 78 percent increase from 2015, underscoring the growing frequency of impactful cyber-attacks.

8 BOARD CYBER-RISK METRICS

Business-aligned and understandable cyber-risk metrics are an essential tool to inform an enterprise's board of directors of the organisation's vulnerabilities and strength of its defences, two factors that an organisation can influence. They establish a consistent mechanism to gauge management's commitment to cyber resilience, reinforcing discipline and accountability.

For them to be valuable to the board, cyber-risk metrics should:

a. Be unambiguous and be relatable to senior business officers and the board of directors

b. Be centered on an enterprise's high-value digital assets, critical suppliers and business strategy

c. Span across people, process and technology domains to provide a complete picture of the cyber-risk profile

d. Refrain from reporting on vain measures, whose aim is to arouse emotions without driving real change. For example, telling the board that the cybersecurity team stopped 7 million spam emails last month may not provide any value; advising the board that the organisation is running outdated email threat prevention technologies will prompt them to fund the modernisation of cybersecurity capabilities.

e. Inform the board, via brief and clear commentary, of current management initiatives to address measures that are outside of tolerance, including specific target dates. Metrics identified as red should be accompanied by a brief commentary articulating the plausible business impacts, the likelihood of the risk materialising and existing compensating controls, if any.

f. Be continuously revised to remain insightful to the board and relevant to the business environment.

The list below provides examples that illustrate some key cybersecurity metrics that can be reported to the board. Consistent with our message, these examples are not conclusive. The right metrics depend on several factors, such as enterprise mission, unique cyberthreats, the enterprise's cyber-risk appetite and the judgement of management. Here are some examples:

A. **CYBERSECURITY INITIATIVES** - The percentage of key cybersecurity initiatives tracking to plan.

B. **PROTECTION OF HIGH- RISK ASSETS** - The percentage of high-risk systems with non-negotiable cybersecurity controls.

C. **IDENTITY AND ACCESS MANAGEMENT** - The number of employees with local administrator rights

D. **VULNERABILITY MANAGEMENT** - The number of open system vulnerabilities (age of vulnerabilities and risk ratings).

E. **SECURITY ASSURANCE** - The number of overdue audit findings (e.g. penetration testing, external audits or ISAE 3402/SSAE 16 reviews).

F. **INCIDENT MANAGEMENT** - The number of cybersecurity incidents reported and resolved within the defined timeframe, including root causes for high rated incidents

G. **HOST AND DEVICE SECURITY** – Percentage of servers and end user devices with endpoint security – personal firewalls, intrusion prevention, hard drive encryption, anti-malware etc.

H. **SECURITY AWARENESS** – Percentage of staff falling victim to phishing simulation tests, improvements of behaviour against previous tests etc.

I. **SUPPLIER SECURITY** - Percentage of new supplier contracts that have undergone cybersecurity reviews, including high and critical rated suppliers.

CONCLUSION

Despite the billions of dollars invested in cyber security solutions every year, not much has changed. The bad guys keep outsmarting enterprises - pilfering billions of sensitive records, manipulating stock markets, stealing trade secrets and committing several other egregious acts. It's become clear that change driven solely by technology will not suffice; real transformation needs to start up higher, with the board holding management accountable for maintaining strong cyber defence and response measures.

APPENDIX

THE CYBER LEADERSHIP INSTITUTE

Develop and grow your cyber skills

We provide capability development and training programs to accelerate the development of cyber strategy, leadership and risk management skills.

https://cyberleadershipinstitute.com/what-we-do/

ABOUT THE CYBER LEADERSHIP INSTITUTE

Our mission is to empower cyber leaders to embrace the technological revolution and improve the way we all live, work and interact.

Our purpose is to give business leaders the skills to confidently lead their organizations in the digital economy.

We strive to:

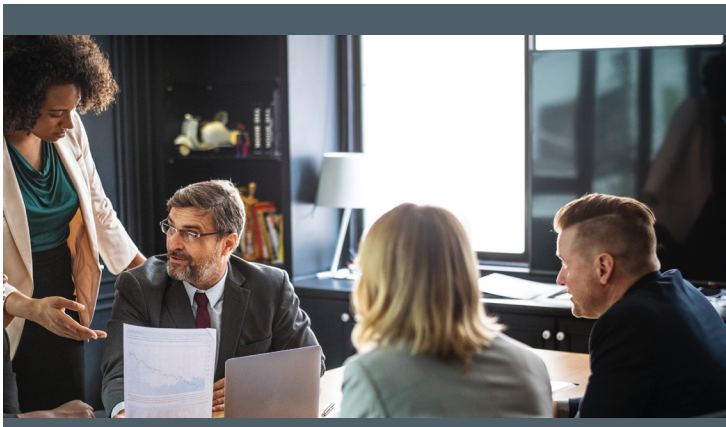
- Develop cyber leaders who build resilience into business strategy
- Empower business leaders to develop sustainable cyber strategies
- Inspire leaders to work together to secure our digital world

JOIN THE CYBER LEADERSHIP HUB

Stronger together – co-create cyber resilience solutions

There is strength in collaboration. Join a community of business, technology and cyber leaders who co-create solutions to cyber challenges, and develop and share business ready templates, methodologies and tools via a digital platform – the Cyber Leadership Hub.

https://cyberleadershipinstitute.com/cyber-leadership-hub/



CONTACT US

CYBER LEADERSHIP INSTITUTE
Level 17 Angel Place
123 Pitt Street
Sydney NSW 2000 Australia
contact@cyberleadershipinstitute.com

REFERENCES

The Five Anchors of Cyber Resilience

https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

https://cyberleadershipinstitute.com/enhancing-board-oversight-of-cyber-risk/

https://www.tanium.com/blog/cybersecurity-accountability-gap/

https://insuranceasianews.com/cyber-insurance-markets-size-to-triple-by-2020-to-us7-5bn/

https://www.insurancejournal.com/news/international/2017/03/06/443623.htm

CYBER LEADERSHIP INSTITUTE

KNOW YOU'RE READY