THREAT INTELLIGENCE FOR EXECUTIVE DECISION MAKING: TURNING DATA INTO ACTION

CYJAX Whitepaper

Executive Summary

As cybersecurity threats grow in complexity and impact, the ability to translate technical threat intelligence into strategic business insights becomes essential. This whitepaper guides Chief Information Security Officers (CISOs) in using threat intelligence to inform executive-level decision-making and shape organisational risk management strategies. It provides practical advice on presenting technical data as risk metrics and communicating with non-technical stakeholders, ensuring the board understands how threat intelligence supports business resilience and growth.

"The real value of threat intelligence lies in what you do with it. Turning insight into action is where resilience is built."

Jonathan Bennett
Chief Executive Officer at CYJAX

Only 2% of executives say their company has implemented cyber resilience actions across all areas of their organisation

Table of Contents

The business value of threat intelligence

"As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture."

Britney Hommertzheim
Global CIO at Cardinal Health

As cybersecurity threats continue to become more varied and destructive, the role of threat intelligence in executive decision-making has become indispensable. With businesses facing a growing array of cyber risks, threat intelligence provides the necessary insights to help organisations identify potential vulnerabilities, allocate resources effectively, and safeguard against escalating risks.

Only 15% of executives are measuring the financial impact of cyber risks to a significant extent

For Chief Information Security Officers (CISOs), a core challenge lies in making technical threat intelligence understandable to non-technical stakeholders, such as the board and senior executives. Translating complex data into relevant business risks enables leaders to view cybersecurity not as an isolated IT issue, but as a critical component of the broader strategic landscape. When presented in terms that speak to the organisation's objectives, risk appetite, and business priorities, threat intelligence becomes a vital tool in steering the company towards informed, proactive decision-making.

Harnessing threat intelligence to guide executive decisions not only mitigates the likelihood of cyber incidents but also enhances the organisation's resilience. By aligning threat intelligence with the organisation's risk management framework, businesses are better equipped to respond to emerging threats, optimise their security investments, and minimise operational impact, all while strengthening the company's competitive position in an increasingly hostile environment.

Less than 50% of CISOs report being involved in key business activities including cyber investment and tech deployments

Defining threat intelligence in a business context

48% of business executives report data protection and data trust as a top cyber investment

To fully realise the value of threat intelligence, it is essential to move beyond technical data and focus on transforming that information into actionable insights that can drive informed business decisions. For Chief Information Security Officers (CISOs), this requires translating complex threat data into a language that resonates with non-technical stakeholders, such as board members and executives.

In its raw form, threat intelligence can be highly specialised and challenging to interpret without a clear understanding of its broader business implications. However, when translated effectively, it becomes a powerful tool for strengthening an organisation's security posture and guiding executive decision-making.

Threat intelligence comes in several distinct forms, each serving a different purpose: strategic, operational, and tactical. Strategic threat intelligence offers long-term insights into broader trends, such as shifts in cybercriminal activity or geopolitical developments that could affect the business. This type of intelligence is crucial for guiding executives in the development of organisational strategy.

Operational and tactical intelligence provide more granular, immediate insights into specific threats. Operational intelligence might reveal ongoing attacks or vulnerabilities in real-time, while tactical intelligence focuses on actionable data, such as IP addresses and malware signatures. This stark statistic underscores the need for organisations to respond quickly to emerging threats.

By aligning the different types of threat intelligence with the company's risk management framework, organisations can more effectively assess their exposure to potential risks, allocate resources accordingly, and make strategic decisions based on clear, data-driven insights. The goal is to ensure that threat intelligence is integrated into the business strategy, not only as a protective measure but as a tool that enhances organisational resilience and drives long-term success.

”We’re investing resources toward integrated response and recovery capabilities to enhance physical security and cybersecurity. Threat actors don’t differentiate. We need to be prepared at every level with our business continuity and resilience programs.”

Dr. Georg Stamatelopoulos
CEO of EnBW AG

Translating technical data into risk metrics

One of the most important tasks for CISOs in leveraging threat intelligence is to effectively translate complex technical data into risk metrics that are meaningful to business leaders. This process enables executives to grasp the relevance of cybersecurity risks and prioritise resources accordingly, aligning security efforts with broader business goals.

Step 1: Identify key risk indicators from threat intelligence data

The initial step involves extracting key risk indicators (KRIs) from threat intelligence data. KRIs serve as early warning signals, highlighting vulnerabilities that could be exploited by cyber threats. For instance, compromised emails and data theft are among the most common causes of cyberattacks, accounting for 20% and 18% of cases, respectively.

Additionally, the World Economic Forum reported in 2022 that as much as 95% of cybersecurity incidents are due to human error, despite two-thirds of board members believing this is not their greatest vulnerability. Identifying KRIs related to such attacks can help businesses proactively address potential threats.

Step 2: Quantify the potential impact on business operations

Once KRIs are identified, it's crucial to assess their potential impact on business operations. Cyberattacks can lead to significant financial losses, operational disruptions, and reputational harm. In 2024, the average cost of a data breach reached $4.88 million, marking the highest average on record.

Moreover, cybercrime damage is projected to reach $1 trillion a month by 2031, underscoring the escalating financial threat to businesses. A study by the National Cybersecurity Institute even revealed that 50% of small to medium-sized businesses have fallen victim to cyberattacks, with over 60% of those attacked going out of business.

Understanding these potential impacts aids in prioritising security measures based on their potential return on investment.

Step 3: Use risk scores and metrics to prioritise security investments

Utilising risk scores and metrics derived from identified KRIs and quantified impacts enables businesses to prioritise security investments effectively. A report by Howden indicates that cyberattacks have cost British businesses approximately £44 billion in lost revenue over the past five years, with larger companies more likely to be targeted.

"You can have all of the fancy tools, but if [your] data quality is not good, you're nowhere."

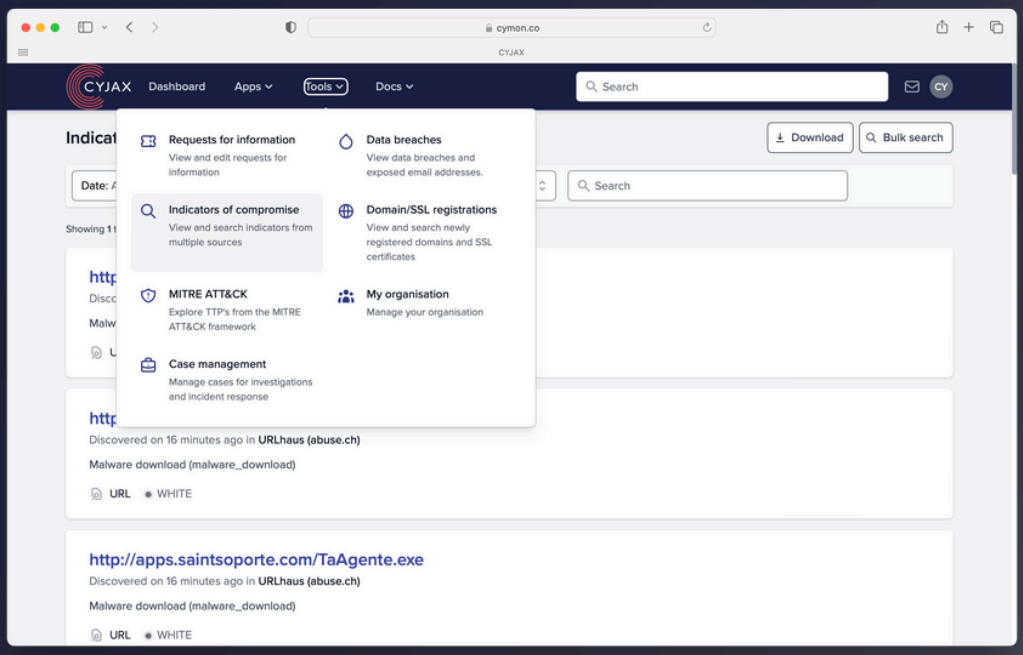
Veda Bawo,
Director of Data Governance at Raymond James

By assigning numerical values to various threats based on their likelihood and potential impact, organisations can present executives with clear, data-driven priorities for security measures. This approach ensures that resources are allocated to address the most pressing threats, enhancing the organisation's security posture and aligning with strategic business objectives.

Communicating with Non-Technical Stakeholders

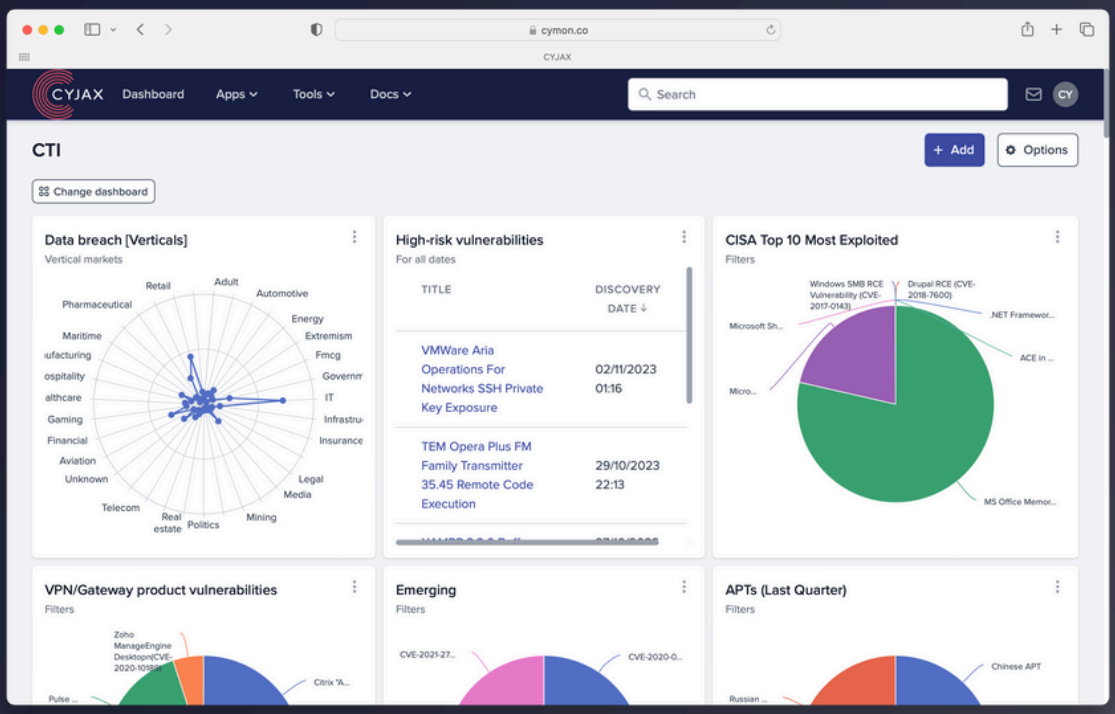
Effectively communicating threat intelligence to non-technical stakeholders, such as the board and executive teams, is critical for ensuring that cybersecurity is viewed as a strategic priority. This group is primarily concerned with the financial, operational, and reputational risks posed by cyber threats, rather than the technical details. Therefore, the challenge lies in presenting technical information in a way that aligns with their business objectives and helps them understand the potential impact on the organisation.

One of the most effective approaches is to tailor the messaging by focusing on how cyber risks affect the organisation's bottom line. Instead of delving into the complexities of attack vectors or malware signatures, it's important to frame the discussion in terms of business outcomes, such as potential financial losses, damage to brand reputation, and regulatory penalties. For example, a data breach that compromises customer information can lead to significant financial costs, operational disruptions, and a loss of consumer trust. This messaging approach helps board members and executives quickly assess the severity of the threat without becoming bogged down in technical jargon.



EVisualisation tools, such as dashboards and reports, can further enhance the clarity of this messaging. Using clear, simple visuals like charts, graphs, and colour-coded risk levels, organisations can present key threat data in a way that is easy to digest. Real-time threat monitoring dashboards can highlight critical risks, track mitigation progress, and display vulnerabilities in a user-friendly format. These visual tools make it easier for non-technical stakeholders to understand the risks at a glance and monitor the effectiveness of security measures.

Additionally, real-world examples of cybersecurity incidents can drive home the importance of proactive measures. Case studies, such as the Target breach of 2013, which resulted in over $200 million in direct costs and long-term reputational damage, can illustrate the tangible consequences of security lapses. By using examples relevant to the organisation's industry, cybersecurity leaders can make the risks feel more immediate and relatable, helping executives understand the potential for similar impacts on their own business.



Top tips for communicating cybersecurity to non-technical stakeholders

Focus on Business Impact: Frame cybersecurity risks in terms of financial losses, brand damage, and operational disruptions rather than technical details. 01

Use Visualisation Tools: Present data in an easy-to-understand format using charts, graphs, and colour-coded dashboards to highlight risks and progress 02

Tailor Messaging to Business Priorities: Align cybersecurity discussions with the organisation's strategic goals, such as protecting customer trust, compliance, and competitive advantage. 03

Leverage Real-World Examples: Use relevant case studies and incidents to demonstrate the real-world impact of cyber threats on business operations. 04

Simplify Complex Data: Avoid technical jargon and instead focus on clear, actionable insights that resonate with executives' core concerns. 05

By focusing on business outcomes, using visual tools, and providing relevant case studies, CISOs can ensure that non-technical stakeholders fully understand the importance of cybersecurity and are equipped to make informed decisions that support the organisation's overall strategy.

Building a threat intelligence strategy for executive engagement

A successful threat intelligence strategy is essential for engaging executives and ensuring that cybersecurity is aligned with business priorities. By establishing clear objectives, developing a tailored communication framework, and ensuring continuous improvement, CISOs can effectively demonstrate the value of threat intelligence to the organisation's leadership.

Establish clear objectives and success metrics

The foundation of an effective threat intelligence strategy lies in defining clear objectives that align with business goals. These objectives should focus on risk mitigation, business continuity, and improving decision-making. To track success, measurable outcomes such as response time to incidents, vulnerability mitigation, and risk prioritisation should be established. Research by Accenture found that organisations with clear objectives are 30% more effective in mitigating cyber risks.

Develop a communication framework for different stakeholders

Communication is key to a successful strategy. Tailoring the messaging for different stakeholders ensures that the information is both relevant and understandable. Executives and board members need high-level, business-focused insights, such as the potential financial and reputational impact of cyber risks. Visual tools like dashboards and risk metrics can help make these insights clearer. In contrast, technical teams require detailed, actionable intelligence for immediate mitigation.

Ensuring continuous improvement and adaptability

Threat intelligence is an ongoing process that requires constant refinement. Regular assessments of tools, processes, and stakeholder feedback help ensure the strategy adapts to emerging threats. Regular reviews and adjustments based on feedback ensure that the strategy remains relevant and effective.

Integrating threat intelligence into organisational risk management

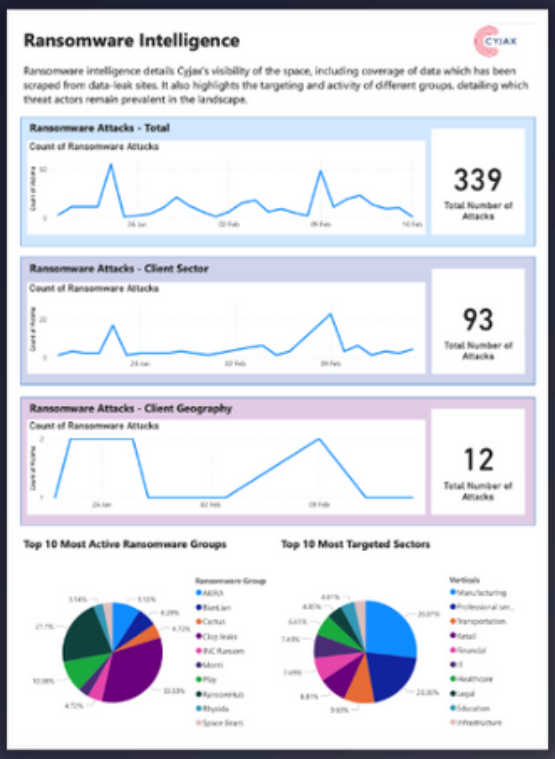
Integrating threat intelligence into the broader risk management strategy ensures alignment with business objectives. By linking threat intelligence with risk assessments, businesses can proactively address risks and align cybersecurity with overall strategy.

Strengthening business Decisions with Intelligence

As this whitepaper has demonstrated, threat intelligence provides business leaders with the insights necessary to anticipate, assess, and mitigate risks effectively. However, to maximise its value, organisations must bridge the gap between technical data and strategic business objectives.

By translating raw threat intelligence into meaningful risk metrics, aligning security priorities with business goals, and fostering clear communication with non-technical stakeholders, CISOs can ensure that cybersecurity is recognised as a fundamental component of organisational resilience. A well-structured threat intelligence strategy enables executives to make proactive, data-driven decisions that not only protect against cyber risks but also support long-term business growth.

Ultimately, the organisations that succeed in embedding threat intelligence into their decision-making processes will be best positioned to navigate the evolving threat landscape, minimise financial and reputational damage, and maintain a competitive edge in an increasingly digital world. Take the next step in integrating threat intelligence into board-level discussions now.



Endnotes

1. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
2. https://www.reuters.com/technology/cybersecurity/cyberattacks-cost-british-businesses-55-billion-past-five-years-broker-says-2024-11-25/
3. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
4. https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity
5. https://www.securitymagazine.com/articles/101321-488m-was-the-average-cost-of-a-data-breach-in-2024
6. https://cybersecurityventures.com/cybercrime-will-cost-the-world-1-trillion-usd-per-month-by-2031/
7. https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial1.pdf
8. https://www.reuters.com/technology/cybersecurity/cyberattacks-cost-british-businesses-55-billion-past-five-years-broker-says-2024-11-25/
9. https://mitsloan.mit.edu/ideas-made-to-matter/3-challenges-chief-data-officers-finance
10. https://www.cyjax.com/resources/blog/the-need-for-contextualised-threat-intelligence/
11. https://www.cyjax.com/cymon/
12. https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883
13. https://www.cyjax.com/resources/blog/the-roi-of-threat-intelligence-measuring-the-value-beyond-detection/

About CYJAX

CYJAX is an award-winning technology company and provider of digital threat intelligence services to international corporations, law enforcement agencies and the public sector.

Using our state of the art technology and our world-class team of analysts, CYJAX monitors the Internet to identify the digital risks to your organisation from cyber threats, reputational risk, and the Darknet.

CYJAX provides an Incident Response and Investigation service that provides a calming and structured approach in helping organisations when a breach does occur.

Our proactive methodologies make sense of the noise and help make intelligence decisions, securing the future for our customers.

2025 Winner Global Business Tech Awards

FSQS REGISTERED

Crown Commercial Service Supplier

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Trusted by enterprises like AstraZeneca, Disney, UK Power Networks, Viatris, HM Revenue & Customs, and more...

SEE CYJAX IN ACTION NOW