ALLIANCES
PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

ALLIANCES PROJECT

EXECUTIVE SUMMARY

IN PARTNERSHIP WITH

Trustwave®

Alliances

www.alliances.global

ALLIANCES MARKET INTELLIGENCE

ALLIANCES INTERVIEWS

ALLIANCES CONVERSATIONS PODCAST

DIGITAL ALLIANCES CHAPTERS

ALLIANCES CHAPTERS

ALLIANCES INSIGHTS

Executive Summary

This comprehensive report delves into the multifaceted realm of cybersecurity governance and communication between Chief Information Security Officers (CISOs) and the board. The findings reveal the intricate challenges faced by cybersecurity professionals and underscore the pivotal importance of practicality, clear communication, and relationship building to effectively address cybersecurity concerns and investments.

Tailored Cybersecurity Strategies:

One of the key takeaways from this report is the necessity of tailoring cybersecurity strategies to specific risk profiles, industries, and evolving threat landscapes. This highlights the significance of ongoing risk assessment, proactive threat intelligence, and the imperative to adapt security measures continuously to stay ahead of an ever-evolving threat landscape. This adaptability is central to a robust cybersecurity posture in an era where digital resilience is of paramount importance.

Diverse Perceptions of Readiness:

The report brings forth the diverse perceptions of breach readiness among organizations, which sheds light on the need for continuous improvement in cybersecurity governance. It strongly advocates for organizations to revisit and enhance their incident response plans, invest substantially in proactive threat intelligence, and conduct regular exercises to rigorously test and refine their response capabilities.

Effective Communication with the Board:

A significant challenge highlighted is the difficulty in communicating the value of cybersecurity investments to the board. To bridge this gap, CISOs are advised not only to articulate Return on Investment (ROI) clearly but also to align these investments meticulously with overarching business strategies. Additionally, mastering the art of storytelling to engage non-technical stakeholders effectively is a skill set that is highly emphasized.

Board's Understanding of Cybersecurity Risks:

The report indicates that while a majority of board members exhibit a moderate to high understanding of cybersecurity risks, there exists ample room for improvement. Effective education and communication are identified as pivotal factors in enhancing board members' awareness and comprehension of these risks.

Challenging Questions from the Board:

Board members often pose challenging questions to CISOs, which require thoughtful and nuanced responses. The complexity of these questions varies significantly, touching upon diverse facets such as the organization's security posture, measurement of effectiveness, recovery capabilities, quantification of risk, budget allocation, data governance, and preparedness for emerging technologies. Effectively addressing these questions involves translating intricate technical details into accessible business language, providing quantifiable data where possible, and aligning cybersecurity efforts cohesively with broader organizational goals.

Strategic Role of the Board:

The report underscores the pivotal role played by the board in cybersecurity governance. The board's inquiry into various facets of cybersecurity investments, accountability, talent availability, control coverage, security awareness, alignment with strategic goals, and more provides a comprehensive understanding of the organization's cybersecurity strategy and preparedness. This underlines the significance of aligning cybersecurity initiatives with the overarching business strategy.

Elevating Cybersecurity to the Board Agenda:

Elevating cybersecurity to the board's agenda is a strategic endeavor that requires a deep understanding of the organization's current situation, astute alignment of cybersecurity considerations with business risks, and effective non-technical communication. Additionally, having an executive sponsor, political acumen, and fostering collaboration with like-minded individuals can considerably strengthen the position of cybersecurity on the board's agenda.

Cybersecurity and Business Continuity Committees:

The establishment of cybersecurity and business continuity committees is identified as vital for effective cybersecurity risk management and ensuring business resilience. These committees serve as forums that bring together experts with diverse expertise to tackle cybersecurity challenges, align cybersecurity strategies cohesively with business objectives, and respond to emerging threats effectively. Clear delineation of roles and responsibilities within these committees, coupled with regular meetings, significantly enhances an organization's cybersecurity posture and readiness for unforeseen disruptions.

Holistic Approach for CISOs:

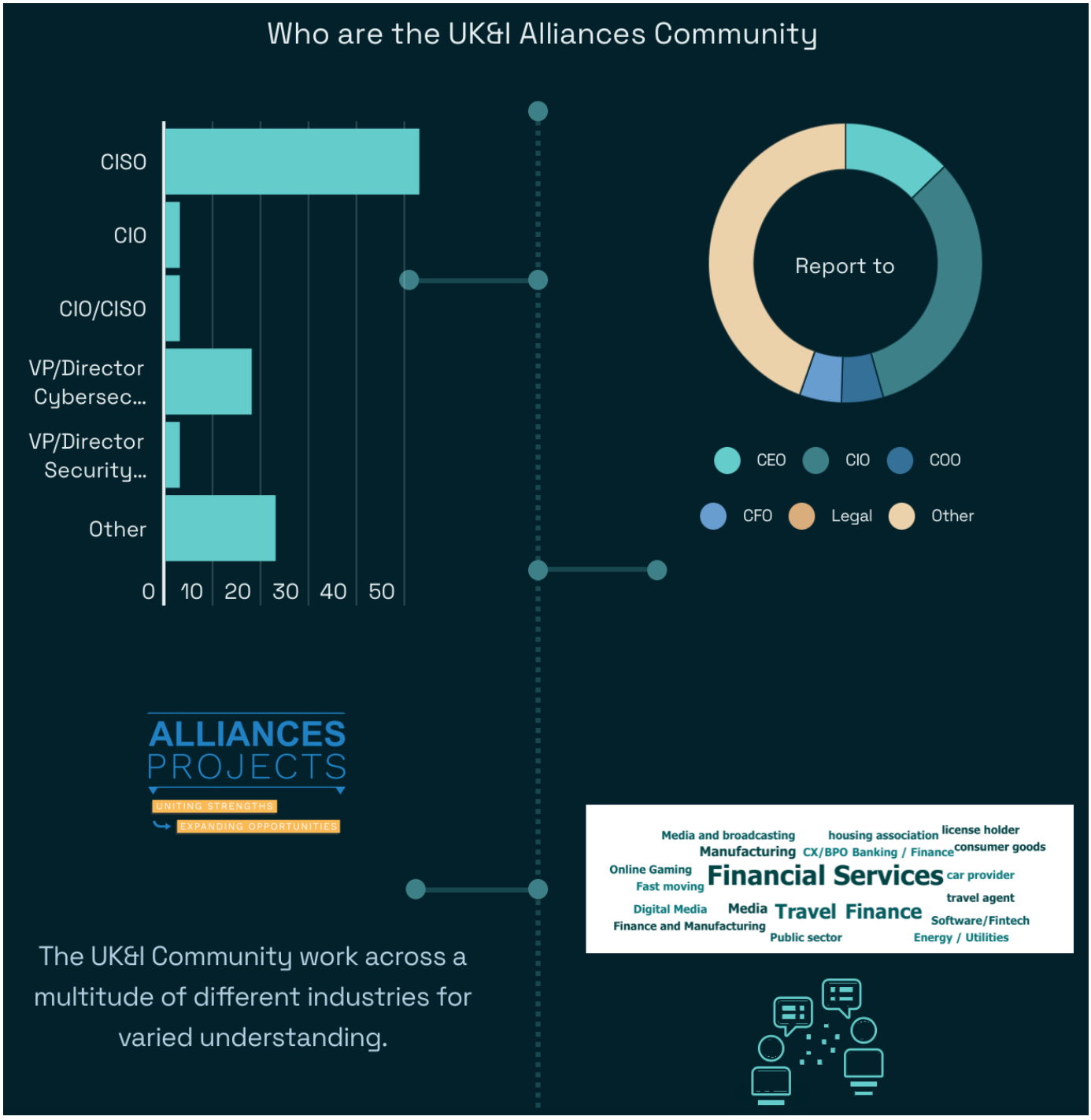
CISOs are encouraged to adopt a holistic approach that transcends technical expertise. This broader perspective entails comprehending the business value of cybersecurity, mastering the art of communication, and aligning security strategies seamlessly with organizational goals. By doing so, CISOs can establish themselves as invaluable strategic partners in the boardroom, ensuring that cybersecurity remains a top-tier priority across the entire organization.

Effective Communication:

Effectively conveying the significance of cybersecurity matters to the board is a multidimensional challenge that involves translating complex technical jargon into accessible business terms, weaving language intricately with overarching business objectives, conversing fluently in the language of finance, storytelling, comprehending industry dynamics, adhering to standards, and fostering collaborative partnerships. CISOs who excel in mastering these languages and strategies are well-equipped to effectively articulate the value of cybersecurity and ensure that it remains a strategic priority intricately aligned with the organization's overarching business goals and objectives.

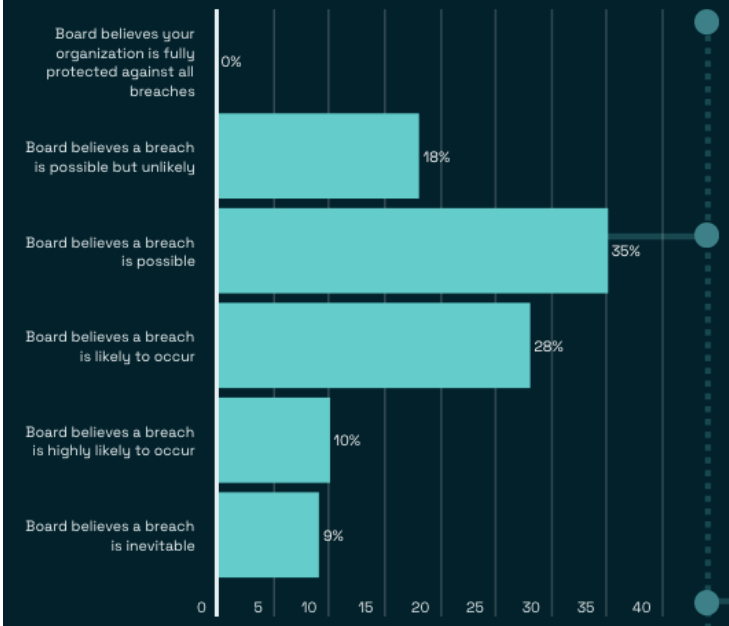
Creating a Culture of Cybersecurity:

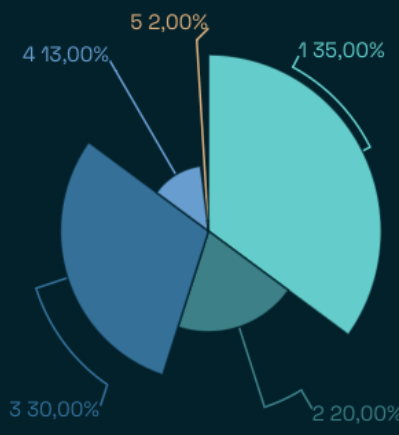
Engaging the entire organization in cybersecurity transcends mere technology and policies; it's about nurturing a culture wherein every member of the organization recognizes their integral role in safeguarding the organization's digital assets. This culture-focused approach revolves around aspects such as fostering a sense of ownership, nurturing awareness, exhibiting leadership, encouraging feedback, and promoting active participation by employees. This approach collectively fortifies the organization against cyber threats and minimizes risks.


Who are the UK&I Alliances Community
CISO
CIO
CIO/CISO
VP/Director Cybersec...
VP/Director Security...
Other
0
10
20
30
40
50
Report to
CEO
CIO
COO
CFO
Legal
Other
ALLIANCES PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES
Media and broadcasting
housing association
license holder
Manufacturing
CX/BPO
Banking / Finance
consumer goods
Online Gaming
Fast moving
Financial Services
car provider
travel agent
Digital Media
Media
Travel
Finance
Software/Fintech
Finance and Manufacturing
Public sector
Energy / Utilities
The UK&I Community work across a multitude of different industries for varied understanding.

Risk, Resilience & Reputation: CISO & The Board

A view of the Board

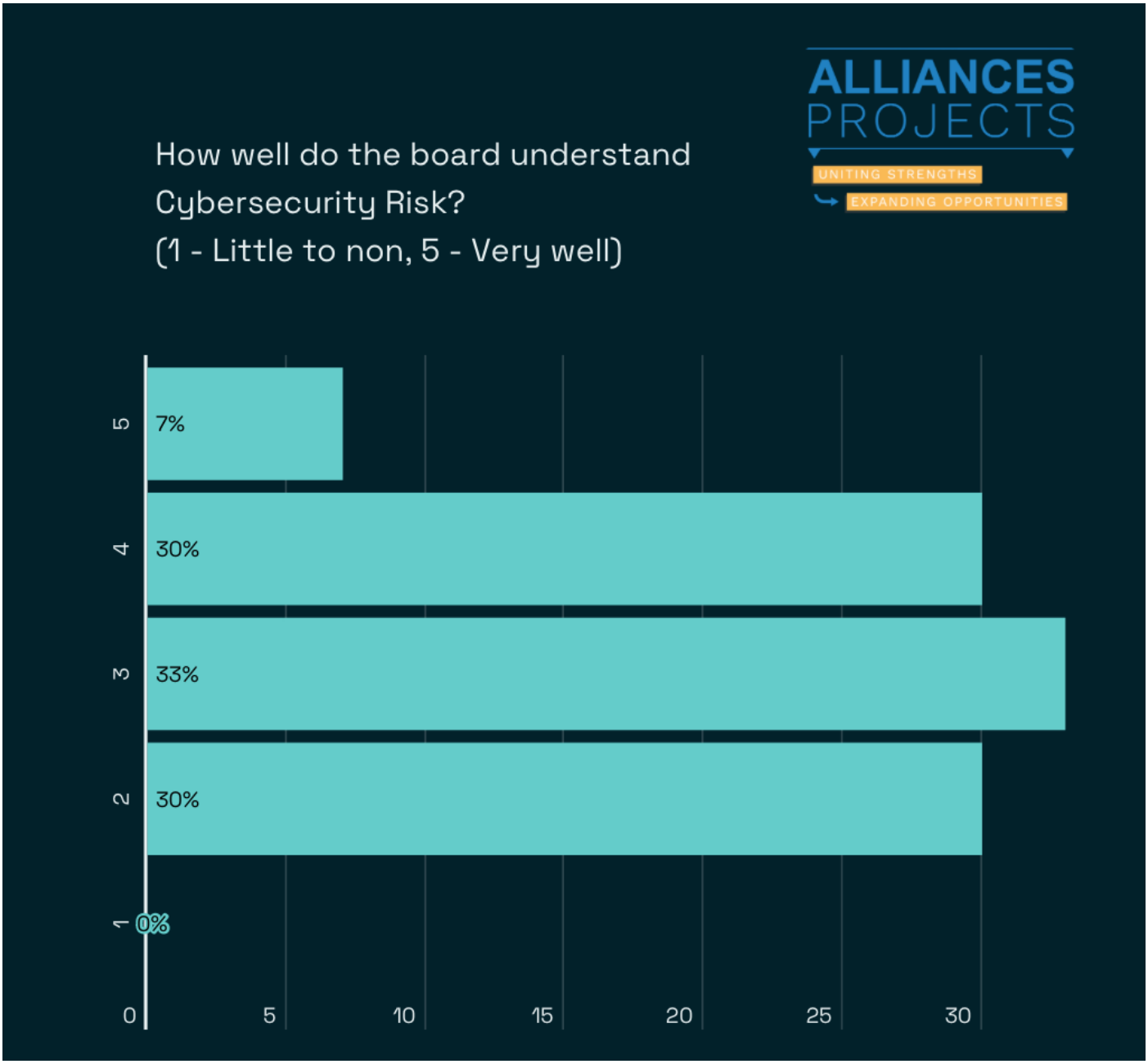


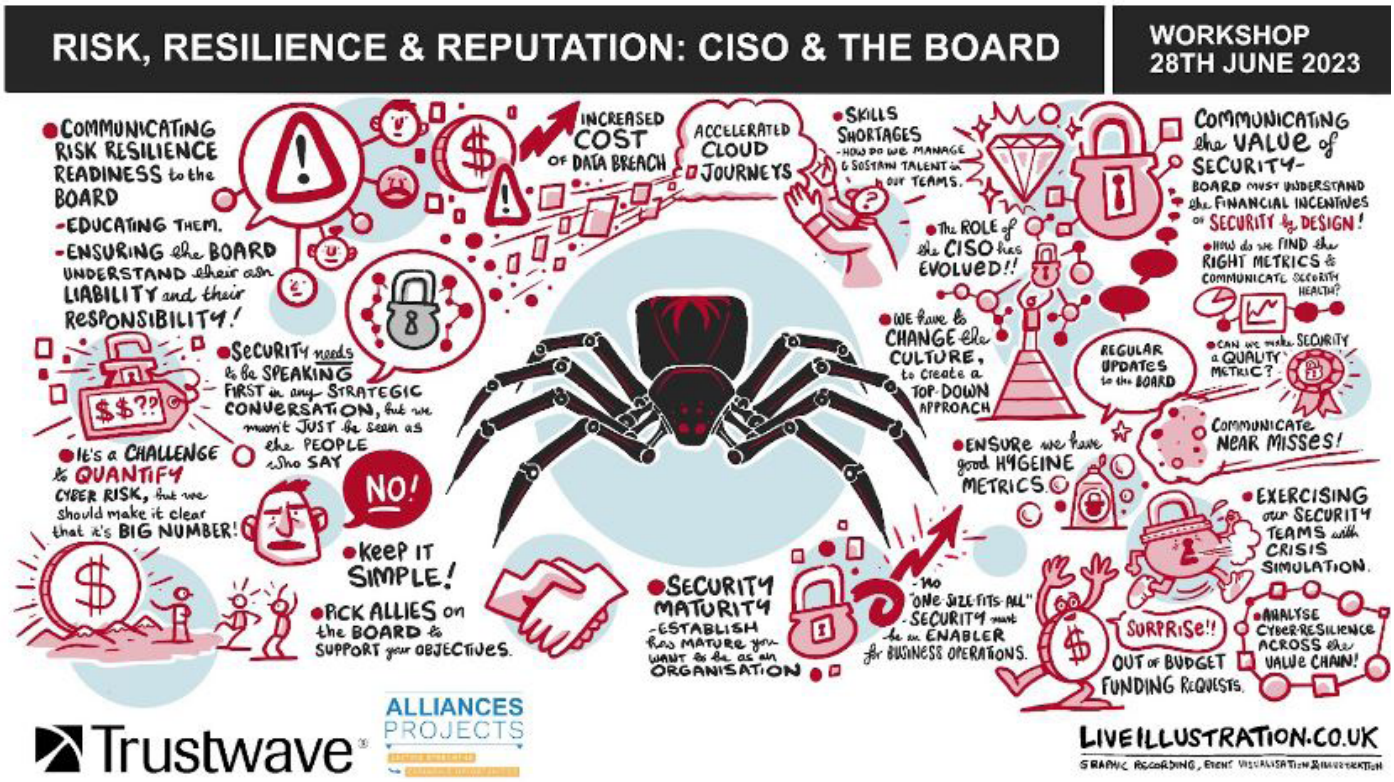


Board Effectiveness to a breach, 1 - Adhoc - 5 - very effective

ALLIANCES PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES

Only 6 members of UK&I Community have a cybersecurity NED on the board


ALLIANCES
PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES
How well do the board understand
Cybersecurity Risk?
(1 - Little to non, 5 - Very well)
5
4
3
2
1
0
7%
30%
33%
30%
0%
0
5
10
15
20
25
30


RISK, RESILIENCE & REPUTATION: CISO & THE BOARD
WORKSHOP 28TH JUNE 2023
COMMUNICATING RISK RESILIENCE READINESS to the BOARD
-EDUCATING THEM.
-ENSURING the BOARD UNDERSTAND their own LIABILITY and their RESPONSIBILITY!
INCREASED COST OF DATA BREACH
ACCELERATED CLOUD JOURNEYS
SKILLS SHORTAGES
-HOW DO WE MANAGE & SUSTAIN TALENT in our TEAMS.
The ROLE of the CISO has EVOLVED!!
COMMUNICATING the VALUE of SECURITY-
BOARD must UNDERSTAND the FINANCIAL INCENTIVES of SECURITY by DESIGN!
HOW do we FIND the RIGHT METRICS & COMMUNICATE SECURITY HEALTH?
CAN we make SECURITY a QUALITY METRIC?
SECURITY needs to be SPEAKING FIRST in any STRATEGIC CONVERSATION, but we mustn't JUST be seen as the PEOPLE who SAY
NO!
IT's a CHALLENGE to QUANTIFY CYBER RISK, but we should make it clear that it's BIG NUMBER!
KEEP IT SIMPLE!
PICK ALLIES on the BOARD to SUPPORT your OBJECTIVES.
WE have to CHANGE the CULTURE, to create a TOP-DOWN APPROACH
REGULAR UPDATES to the BOARD
ENSURE we have good HYGEINE METRICS.
COMMUNICATE NEAR MISSES!
EXERCISING our SECURITY TEAMS with CRISIS SIMULATION.
SECURITY MATURITY
-ESTABLISH how MATURE you WANT to be as an ORGANISATION
-no "ONE SIZE FITS ALL" SECURITY must be an ENABLER for BUSINESS OPERATIONS.
SURPRISE!!
OUT OF BUDGET FUNDING REQUESTS.
ANALYSE CYBER-RESILIENCE ACROSS the VALUE CHAIN!
Trustwave
ALLIANCES PROJECTS
LIVEILLUSTRATION.CO.UK
GRAPHIC RECORDING, EVENT VISUALISATION & ILLUSTRATION


RISK, RESILIENCE & REPUTATION: SECURITY LEADERS & THE BOARD
PREPARING THE BOARD
HOW do YOU GET CYBERSECURITY on the AGENDA?
COMMUNICATE the RISK & the BUSINESS
-UNDERSTAND what STYLE of BOARD you are TALKING to
USE NON-TECHNICAL LANGUAGE!
TALK about BUSINESS CONTINUITY
IT's about CRISIS MANAGEMENT!
UNDERSTAND BUSINESS MATURITY.
ESTABLISH SPONSORS in the EXEC
BRING the THREAT to LIFE!
-USE EXAMPLES from INDUSTRY
-TELL STORIES!
IT's about BUILDING RELATIONSHIPS!
WHAT are the QUESTIONS YOU NEED to be ASKING the BOARD?
LONG TERM vs SHORT TERM PRIORITIES
WHAT KEEPS YOU awake at NIGHT?
WHAT are the BIGGEST RISKS FOR THE BUSINESS?
-AND HOW can we HELP ADDRESS THESE?
WHAT are the SIGNIFICANT METRICS?
WHAT CULTURE do you want to HAVE?
WHAT KIND OF BOARD is it? - GOVERNANCE or BUSINESS?
WHO are YOUR MAIN COMPETITORS?
SECURITY INTEGRATED into BUSINESS CULTURE.
WHAT are your SECURITY GOALS?
WHAT are the COMMITTEES needed to ADDRESS CYBERSECURITY?
CYBER SECURITY & RISK COMMITTEE
-CISO, ITSM, LEGAL, DPO, CFO/CTO/CIO, COO, CRO/CCO, -HR MANAGER & ENCOURAGE GOOD BEHAVIOURS
-QUARTERLY REPORTING
BUSINESS CONTINUITY COMMITTEE
-COO, OPERATION RM, CFO, SECURITY OPERATIONS MANAGER, ITSM, BCM, PEOPLE x CULTURE.
-QUARTERLY REPORTING.
-EVENT DRIVEN.
-IMPLEMENTATION REPORTING.
Trustwave
ALLIANCES PROJECTS
LIVEILLUSTRATION.CO.UK
GRAPHIC RECORDING, EVENT VISUALISATION & ILLUSTRATION

Conclusion

In conclusion, this report serves as a rich resource for organizations navigating the intricate terrain of cybersecurity. By embracing diverse perspectives and acknowledging the complexity of cyber risks, organizations can craft agile, effective, and resilient cybersecurity strategies that steadfastly protect their operations, preserve their reputation, and nurture stakeholder trust. These findings collectively underscore the significance of continuous improvement in cybersecurity governance, proactive risk management, and a relentless commitment to safeguarding digital assets in a landscape where cyber threats evolve incessantly.

ALLIANCES PROJECTS

UNITING STRENGTHS

EXPANDING OPPORTUNITIES

Trustwave

ALLIANCES PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES

ALLIANCES PROJECT OVERVIEW

ALLIANCES PROJECTS Trustwave®