CYBERSECURITY EVOLVED:

INCREASE VALUE, IMPROVE ALIGNMENT WITH THE BUSINESS & ENGAGE THE BOARD OF DIRECTORS

Prepared by

TDI

MARCH 2022

CYBERSECURITY EVOLVED:
INCREASE VALUE, IMPROVE ALIGNMENT WITH THE BUSINESS & ENGAGE THE BOARD OF DIRECTORS




TABLE OF CONTENTS

INTRODUCTION

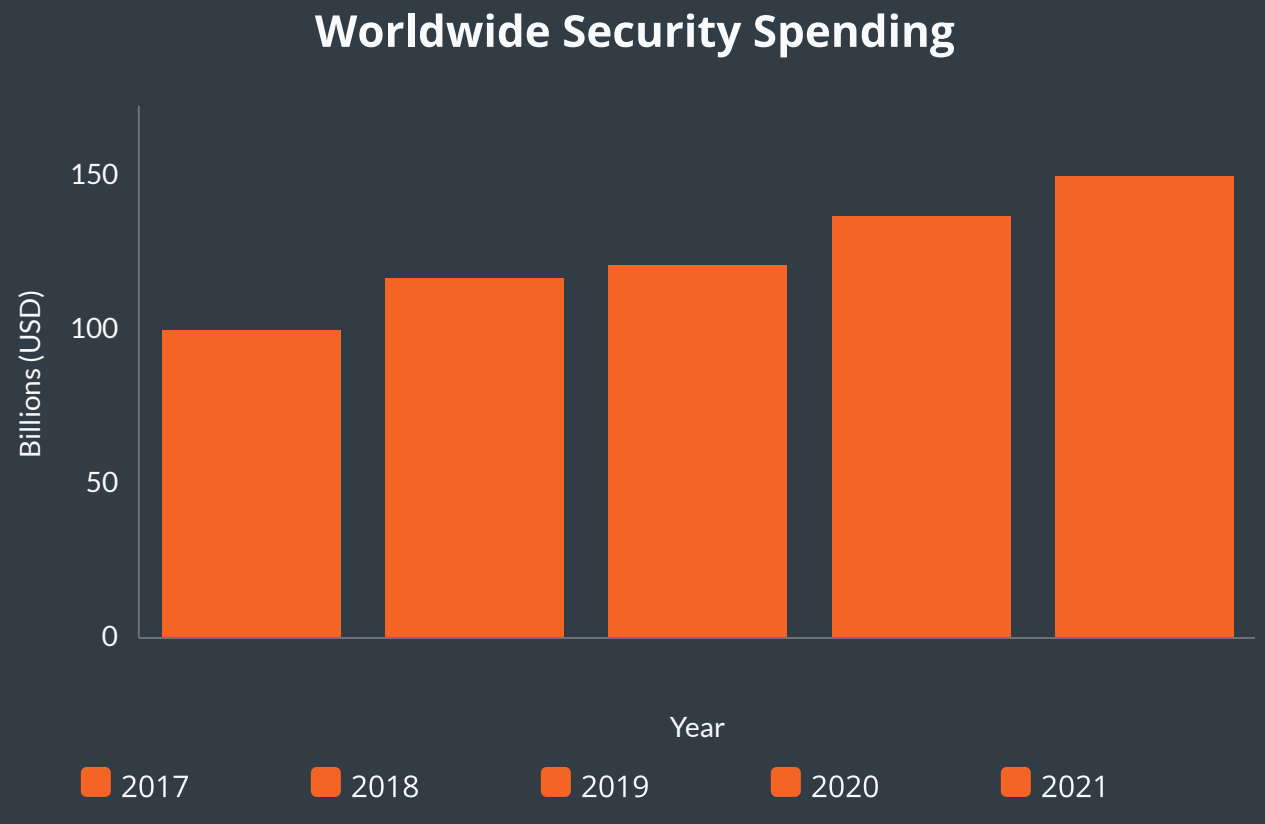
TDI has dedicated the last 20+ years working with organizations of all sizes to improve and mature their cybersecurity practices. This nSight Report draws on that deep expertise, new data, and scientific research, to lay out a proven and practical approach companies can use to accelerate their cybersecurity journey towards increasing value and alignment to the business and Board of Directors.

> "This report highlights the critical need for companies to start reporting to the board when it comes to navigating the esoteric and dynamic field of cybersecurity. Now more than ever, working together to up-level board transparency with tangible measures and a common lexicon is what will increasingly differentiate foward-leaning companies from those looking in the rearview mirror."

Craig Rosen
Chief Security & Trust Officer at ASAPP
and Former VP & CISO at AppDynamics
and VP & CSO at FireEye

BACKGROUND

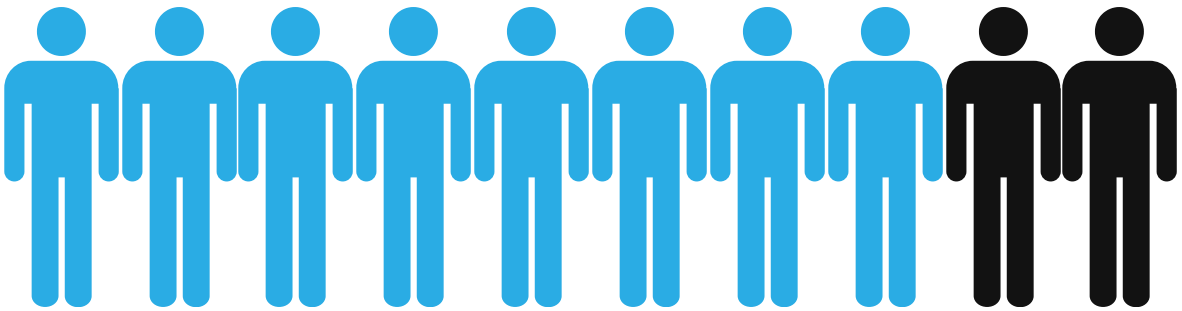
The data is clear, cyber spend is higher than ever, yet so are the number of attacks and incidents faced by organizations across the globe. Compliance and regulatory drivers continue to evolve and add further burden to overtaxed security teams. Liability concerns are becoming too real with increased data privacy requirements (GDPR, HIPAA, FCRA, FERPA, GLBA, etc.) and pressure from cyber insurance carriers as organizations look to demonstrate due care. In the 2021 annual Fortune poll of Fortune 500 CEOs, two-thirds responded that the biggest risk to their business was cybersecurity risk. Given these realities, it's no wonder the board is increasingly more involved in organizational cyber security practices.



*Data source: Gartner[1]

BACKGROUND

For years there has been an understandable tension between security leaders and corporate boards working towards an equilibrium. Understandable because cybersecurity is not only complex but is a relatively new practice in business as compared to financial management, which has well-defined and established linkage to the overall health of the business. Effectively and efficiently being able to communicate how cybersecurity spending and performance supports the business and translates to risk and the bottom line continues to elude many organizations. According to Insight's "*Cybersecurity at a Crossroads: The Insight 2021 Report,*" nearly 80% of senior IT and security leaders lack confidence in their organization's protection against cyber-attacks.



80% of senior IT and security leaders lack confidence in their organization's protection against cyber attacks

*Data source: Insight's "*Cybersecurity at a Crossroads: The Insight 2021 Report*"[2]

BACKGROUND

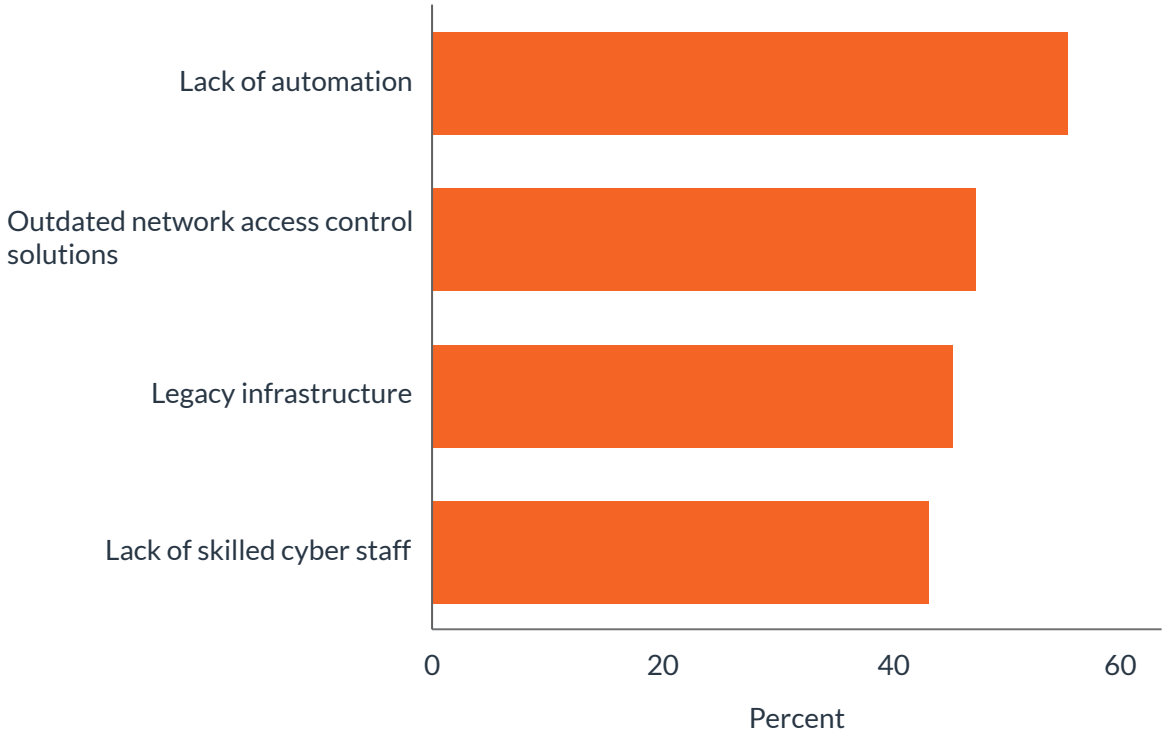
The report further details the lack of confidence in an organization's overall strategy and roadmap as well as a large concern around lack of automation. This has resulted in board members becoming more interested and involved. In fact, every single one of the respondents said their boards and executive teams are more focused on their organization's cyber program than before.

Q: What aspects of your security posture do you feel the least confident about?

*Data source: Insight's "*Cybersecurity at a Crossroads: The Insight 2021 Report*"

BACKGROUND

Q: What are your organization's major security operations and management challenges?



All told, it's now more critical than ever to be able to accurately report to senior management and the board how well the cyber program is performing. However, this is easier said than done since few boards have members with the cybersecurity expertise to contextualize the metrics that matter most, and security teams don't always have the necessary data readily available to communicate in a way that senior management and the board will understand. As we've observed, cybersecurity and business alignment varies greatly across organizations today and can be found at various stages of team development (forming, storming, norming, but rarely performing).

*Data source: Insight's "*Cybersecurity at a Crossroads: The Insight 2021 Report*"

OUR THESIS

Undoubtedly organizations could be achieving more with respect to cybersecurity. To bring a semblance of order from the chaos, it's important for us to define and baseline what is a complex and evolving problem - that has no regard for industry or market vertical - and propose an encompassing thesis from which we can smartly mature the state of cybersecurity programs.

Cybersecurity must be elevated to the highest level

Cybersecurity is as critical and interrelated to the success of a business as any other resource or component (e.g., labor, material, knowledge, technology, pricing, innovation, agility, communication). As such, the topic of cybersecurity must be elevated to the highest level of the organization in an appropriate manner whereby its holistic impact is known, understood, measured, visually reported, and managed.

KEY CHALLENGES

To that end, we begin by distilling the concerns mentioned earlier into three chief issues which we see as the crux of the overarching dilemma: most Boards and senior executives are unaware of how their respective organization fares in the fight to be cyber-secure. Each individual issue manifests into an array of cascading challenges that are typically difficult to identify and correct such as inefficiencies and overspending. Corralling the tentacles of this beast into three tangible challenges – those we call the Organizational Obstacles to Cyber Success - provides us a substantial structure to build a plan to overcome. Let's examine them in turn:

1. Misalignment in understanding of risk tolerance between the board and security teams

2. Disparity in technical understanding and industry terminology

3. Lack of meaningful and timely visibility into the day-to-day cybersecurity performance of the organization

KEY CHALLENGES

Misalignment in understanding of risk tolerance between the board and security teams

Oftentimes referred to as "*risk appetite*," this misalignment – or oftentimes undefined tolerance - creates a mismatch in the amount of risk the team and board see as acceptable and sets the stage for not working towards the same objectives. To attain alignment is theoretically simple, yet practically quite difficult and rare to see in practice. Risk management frameworks such as NIST SP800-37, ISO 27001 and others lay out critical aspects of prioritizing the mitigation of high-consequence risks within an organization. The key is having an end-to-end program that manages cybersecurity risk like any other business risk; specifically, measuring cyber risk in terms of impact to the business and associated investment and not by how many high vulnerabilities the organization quelled in a given month or what the Splunk team may have worked on.

> "Having buy-in from the board is critical for company-wide security initiatives. There needs to be a greater level of accountability by the board in overseeing cybersecurity operations, since failing to do so can have such dire consequences on business operations. This report is a great primer on the issue."
>
> Cynthia Nustad
>
> Former EVP, Chief Strategy Officer of HMS Holdings &
> Board Director at Brightfin, WPAS, and NextHealth

KEY CHALLENGES

Disparity in technical understanding and industry terminology

While there are a number of reasons why executive teams and the board speak a different language than cybersecurity practitioners, there are two focal points we must address. The first being that board members can be new to cybersecurity and, unlike reading a financial report which is uniform and learned consistently in business school, cybersecurity reports on the other hand, are both foreign and vary wildly from one place to another. Another major issue stems from the lack of a shared lexicon that carries meaning across any level of an organization. While a board member might support an organization in Singapore, New Zealand or Canada, they will always intimately understand a P&L Statement or Pro Forma Sales Projections no matter where they sit – the same is not true for cybersecurity reporting.

As an example, conversations of zero-day critical CVSS 9.8 vulnerability impacting a domain controller likely means little to most board members and would be reported differently in nearly every organization on the planet.

Board members are new to cyber and reporting varies from organization to organization

Cyber needs a shared lexicon, in every market and in every organization

KEY CHALLENGES

Disparity in technical understanding and industry terminology

What is really needed is shared terminology across all verticals, mapped to the business in terms of impact and risk (as illustrated in the figure below).

*Source: CnSight's Cybersecurity Board Report[3]

Details of this lexicon are further described in a later section entitled, "*A GPS to Find Success*."

KEY CHALLENGES

Lack of meaningful & timely visibility into the day-to-day cybersecurity performance of the organization

Ask an average CEO or Board member how well their organization is performing in terms of its cybersecurity program and experience coupled with statistics indicate the answer will be the same, they are unsure. Much of this issue currently rests in the ability of the Chief Information Security Officer (CISO) to simplify complex and nuanced security topics to a high-level summary that adequately contextualizes the issue for the board. Their interpretation of the always evolving status and performance of an organization's security posture needs to be as accurate as possible; at the end of the day, it's their interpretation that the board will be hearing and acting upon. How CISO's seek to accomplish this translation varies greatly along with the resulting impact of their efforts.

Manual data gathering from spreadsheets, disparate tools and teams, manual correlation, bespoke solutions, and interpretation transcribed further into reporting is a common theme. While the efforts are heroic, none are continuous, efficient, or scale, and they are typically far from optimal. Often these well intended solutions are not enterprise ready, difficult to maintain, have questionable data integrity, and include labor intensive manual processes that add reporting burdens to the team.

Oftentimes these challenges are exposed only during a security breach or incident that sheds light into a particular problem area. This is part and parcel of the security whack-a-mole culture that this report seeks to address.

KEY CHALLENGES

Lack of meaningful & timely visibility into the day-to-day cybersecurity performance of the organization

CISO's are consumed by fighting fires and implementing more and more tools from the nearly 10,000 now available on the market. Combined, they have limited capacity to effectively view and manage their program's cybersecurity performance more strategically. Until teams take a different approach, the priority will continue to favor the urgent over the important. As too many organizations know all too well, when a successful attack does occur, it is incredibly time-consuming, deprioritizes other ongoing important initiatives, and is expensive to recover from – the average cost of a successful breach is 4.24M[4].

$4.24 million
average cost of a successful data breach

It is crucial for the board to have insights into how well their cyber program is performing, identify performance gaps, and create a unified strategy for mediating identified issues before it is too late.

The current trend is positive in that there is consensus that the problem is real and needs to be addressed if organizations want to get ahead of the curve and maximize their cybersecurity spend through greater effectiveness. This is evident by survey data and an increase in published principles for boards from notable organizations such as The National Association of Corporate Directors (NACD)[5], Internet Security Alliance (ISA)[6], and Organization of American States (OAS).

A GLIMMER OF HOPE

These oversight organizations have established key principles that aim to inform and progress how boards can better understand and incorporate digital risk into their planning and decision making. Below are examples of these principles that are especially germane to the topic of this report.

OAS[7] & ISA CYBER-RISK OVERSIGHT HANDBOOK FOR CORPORATE BOARDS	NACD[8] & ISA Principles for Board Governance of Cyber Risk Insight Report
PRINCIPLE 4: Board directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget. **PRINCIPLE 5:** Board-management discussion about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.	**Principle 2.1:** Cybersecurity is a strategic business enabler. **Principle 2.2:** Understand the economic drivers and impact of cyber risk. **Principle 2.3:** Align cyber-risk management with business needs. **Principle 2.4:** Ensure organizational design supports cybersecurity.

A GLIMMER OF HOPE

Armed with a clear understanding of the challenges facing them, organizations have embraced security frameworks and taken heed of guidance from NACD, ISA, and others on how best to evolve and mature cybersecurity programs. This, coupled with the tremendous amount of security data available to organizations, creates an opportunity to truly transform how security is managed and integrated into the fabric of the business such that its value and effectiveness becomes evident across all levels of the organization. The stage is set for next level performance and understanding. Now, the question which still seems to elude many organizations is the how – how exactly do we ensure our organization is continuously performing well and reporting, timely, accurately, and effectively, to senior executives and the board. We endeavor to tackle this next.

> “Boards need assurance that finite resources are being prudently used where they are needed the most, resulting in improved cyber resiliency and operating within pragmatic risk tolerances. This all requires data, KPIs, KRIs, to report performance of cyber investments.”
>
> Jayesh Panchal
> Former CISO of IMF

A GPS TO FIND SUCCESS

The journey to achieving an evolved and highly aligned state of cybersecurity performance and optimization should be a business imperative that helps establish a competitive advantage through risk and cost reduction. Put another way, organizations will benefit financially - and in their entirety - if they consistently and continuously measure, manage, and report on their cybersecurity performance, speaking the same language all the way thru to the board. Experience shows this is easier said than done. Practically speaking, implementing, and managing what is essentially a high-performing cybersecurity program is a universal challenge across all market verticals.

Based on our analysis, with consideration of the principles outlined by NACD and guidance offered by NIST, ISO, CIS, and other frameworks, we established eight tenets that govern how organizations can successfully accelerate their cyber journey to achieve efficiencies and better effectiveness while avoiding common pitfalls along the way. Simply stated, this is the path to effectively achieve our defined thesis statement: "*…the topic of cybersecurity must be elevated to the highest level of the organization in an appropriate manner whereby its holistic impact is known, understood, measured, visually reported, and managed.*"

A GPS TO FIND SUCCESS

We recommend these tenets be considered as part of board conversations, enterprise strategic planning and budgeting activities, and at the operational level when considering alignment of security functions with business stakeholders, risk and compliance functions, and IT.

8 Tenets to increase cybersecurity value & alignment with the business & board of directors

1

Automated & Efficient

Data collection, analysis, and reporting should be highly streamlined and automated with the lowest amount of human intervention and labor. This includes developing and maintaining the automation as well (refer to Tenet #8).

2

Interoperability & Scalability

Data should be available through a REST API when possible, methods or systems used to collect, analyze, and report should be transparent and not be viewed as a “black box”. These systems should easily scale to accommodate multiple data integrations, areas of security, systems, data types, data volume, and work across hybrid and cloud environments.

A GPS TO FIND SUCCESS

3

Contextualized Meaningful Visibility & Availability

Meaningful and actionable information reporting must be available on demand at various levels (tiers) of the organization. Based on roles, information should contain the proper contextualized visibility to derive value and impact.

4

Business Decision Support

Reporting should provide necessary insights to inform and baseline an integrated cybersecurity strategy and provide measures to gauge effectiveness and progress over the course of the organization's journey.

5

Performance Centric

This approach fosters accountability using metrics aligned to Cybersecurity Performance Indicators (CPIs) that benefit multiple areas of the business, providing the bedrock foundation upon which high performance cybersecurity programs are built (refer to Tenet #6).

A GPS TO FIND SUCCESS

6

Mapping & Unification of Adjacencies

Performance objectives must be linked to related security, business, and risk functions to provide the most complete and impactful view of organizational performance. These functions include at a minimum: Compliance, Business Value, Risk, and Maturity (refer to next page for additional detail).

7

Timeliness & Accuracy

To facilitate data-driven agility, information and reporting must have a high degree of data integrity and represent the current operational view.

8

Cost-Effective

Solutions cannot be cost-prohibitive due to data throughput and operation & maintenance (O&M) costs. Instead, implantation and associated operations should be cost-effective throughout the lifecycle (acquisition, customization, O&M, and even retirement).

A GPS TO FIND SUCCESS

With these eight tenets as a guide, effective board reporting becomes a natural outcome such that organizations can understand performance against strategic cybersecurity objectives that are wholly centered on the measurement of five critical components that are paramount in achieving high performance business-centric cybersecurity:

Our effectiveness in meeting our strategic cyber objectives →

Performance

How well are we doing?

Our exposure to threats / danger →

Risk

What is our risk?

Our ability to respond to the environment at-hand, knowing when & how to act →

Maturity

Are we consistent & continuously improving?

Our adherence to relevant guidelines, frameworks, & regulations →

Compliance

Are we compliant?

Our investment over the relevant period compared to how we performed →

Business Value

What is our ROI?

A GPS TO FIND SUCCESS

More specially, these critical components provide the timely operational detail necessary to satisfy board reporting that is meaningful, actionable, and aligned to the business in a manner that organizations have only dreamt about.

Performance

At the core, these are measurements of effectiveness against defined goals. Stemming from a risk assessment and threat analysis, mission of the business, regulatory drivers, and overall risk appetite - every organization must define acceptable goals around security. These are measured in the form of cybersecurity performance indicators (CPIs), key risk indicators (KRIs), key control indicators (KCIs), etc. to provide needed visibility to inform the other complementary components as described below.

Risk

Risk in part is a measure of an organization's current understanding of the operational reality in which it resides. Through measure of performance, more is known about this reality, minimizing “unknown-unknowns” as well as “known-unknowns”. With fewer blind spots, organizations know where they stand in terms of risks and how to best prioritize finite resources ahead of the storm.

A GPS TO FIND SUCCESS

Maturity

Capability is important; however, consistency is king, especially – and critically – over time. Measures of maturity answer questions about consistency and repeatability of tools, teams, and processes. How resilient are the systems we have in place and where might we have areas to improve such that we have the coverage appropriate for our risk appetite?

Compliance

Point in time compliance against one or many frameworks has little utility in a DevSecOps world. Organizations need to understand where they stand continuously - across the entirety of the enterprise. With measures of performance linked to existing security frameworks and controls, it's possible to have a continuous view into compliance efforts.

Business Value

Perhaps the ultimate goal of every business is to be able to readily understand if they are receiving the best value for all their cyber spend and efforts. Measuring the impact of events that are never realized is difficult. Using performance metrics as a guide, business value can be derived into something akin to ROI when coupled with spend in a particular area of security.

A GPS TO FIND SUCCESS

While there are several overarching guiding principles to help organizations, our clients have found the devil is often in the details. Organizations are stretched thin and competing operational priorities often take centerstage, pushing strategy to the arena of, "*other duties as assigned*" and "*as time permits*." Forged in operations and practice, our 8 tenets and 5 critical components provide organizations a roadmap to effectively transform the esoteric to a reality in which the espoused value becomes realized. This is achieved with a practical and proven approach to improve communication and transparency, providing a holistic understanding of the underlying cyber-health of the business to internal stakeholders as it aligns with the company's mission and goals.

WELCOMED PROVISIONS FOR YOUR JOURNEY: CYBERSECURITY PERFORMANCE MANAGEMENT

While studying and hoping to improve organizations and how they conduct the business of cyber, we developed an innovative, comprehensive, and practical approach to cybersecurity risk, effectiveness, and performance management. Our methodology is security tool agnostic and conforms to the 8 tenets and 5 components of a board report outlined above and addresses the challenges identified in this paper. The overarching framework we designed for effective cybersecurity management is called Cybersecurity Performance Management (CPM). CPM consists of cyber KPIs or what we refer to as CPIs, cybersecurity performance indicators. We've applied research out of Stanford University by Nicolas Bloom[9] et al. asserting that management practices account for more than 20 percent of productivity variations. The research states that this is a similar, or greater percentage as that accounted for by R&D, information and communication technologies, or human capital. The researchers focused on the degree to which KPIs were established, visible, reviewed, and embedded as part of employee performance conversations and incentives. Simply put, using KPIs can make a team more effective than buying another tool or hiring more staff.

CPM can and should be automated to integrate with an organization's existing cyber tools and collect valuable data points to inform key metrics in the form of CPIs which are then charted to the 5 critical components of Performance, Risk, Maturity, Compliance, and Business Value.

WELCOMED PROVISIONS FOR YOUR JOURNEY: CYBERSECURITY PERFORMANCE MANAGEMENT

Finally, this information can be contextualized even further to produce meaningful board reporting that speaks to what boards need to know most. The figure below illustrates how elements of our approach work in concert to provide the visibility needed to drive value across the enterprise.

*Source: CnSight's Cybersecurity Board Report[3]

CPM can and should be automated to integrate with an organization's existing cyber tools and collect valuable data points to inform key metrics in the form of CPIs which are then charted to the 5 critical components of Performance, Risk, Maturity, Compliance, and Business Value. Finally, this information can be contextualized even further to produce meaningful board reporting that speaks to what boards need to know most. The figure below illustrates how elements of our approach work in concert to provide the visibility needed to drive value across the enterprise.

CONCLUSION

> As an Independent Board Director and C-Suite Executive, it is critical that we assess how cyber impacts our business growth. There are 5 key components that are essential to assess and provide over-site of strategic cyber posture: Business Value, Performance, Risk, Maturity, and Compliance.

Deborah Dunie

Former EVP & CTO of CACI, Deputy Under Secretary of Defense, Counterintelligence & Security, and Board of Directors SAIC. Presently Board of Directors at National Association of Corporate Directors, Axient, Leonardo, Sigma Defense, Arcfield, Babel Street, Code-X, and Peraton

A fortunate product of having supported projects around the globe for more than two decades is the remarkable viewpoint gained by working with agencies across the government, Fortune 50 boards, onboard ships at sea, stock and metal exchanges, and systems under the water and sometimes in space. The one constant we have recognized and studied, thus forming the basis of this paper, is the manifestation of the same paradigmatic dilemma – the focus on what we are doing vice how well we are doing.

CONCLUSION

The data is clear, organizations need to make a step-change and evolve how they think about and manage cybersecurity within their organizations. Succinctly, when divisions within an organization are unified in mission and approach to cybersecurity, it vastly increases the effectiveness and efficiency of security improvement initiatives, drives process maturity, and better informs understanding of risk. This paper set out to deliver the five critical components to measure an organization's success with eight tenets to implement such a system – the endeavor to implement is now in your hands. It's time to move our focus from our activities in cyber to our achievement and value as it relates to the business.

> "The ability to present cyber program status to the board is one of the most challenging issues facing CISO's today. Often CISO's havent been exposed to the language the board uses, nor do we really understand what the board wants and needs to know. This report is a great starting point for CISOs to begin the critical task of transforming cyber from a technology problem to a business problem in their companies."
>
> Stan Lowe
> Former Global CISO for Zscaler & PerkinElmer and
> Deputy Assistant Secretary for Information Security &
> CISO U.S. Department of Veterans Affairs

AUTHORS

CEO

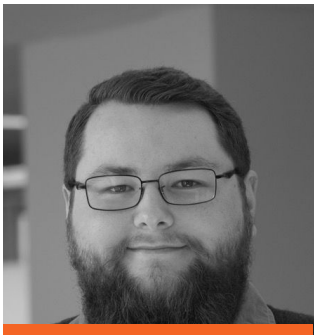
Paul Innella

Paul Innella, TDI's CEO, has over 25 years of executive and cybersecurity experience. He founded and built TDI which offers cybersecurity services to hundreds of government agencies and commercial clients. He is a recognized cybersecurity SME and corporate executive who has published articles, lectured, and conducted interviews (ABC, Fox News, Forbes, MSNBC). He established and chairs the charitable cyber-focused "White Hat USA" which raises money for Children's Hospital. He is a Board Member in many private companies, JMU, Children's Hospital, WashingtonExec's Cyber Security Council, and Chair of Children's Corporate Advisory Council. He graduated from JMU, attended graduate courses at Johns Hopkins, and Executive Programs at Cambridge, IMD, U. of Edinburgh, and U. College of Dublin.

VP, Solutions

Jesse Dean

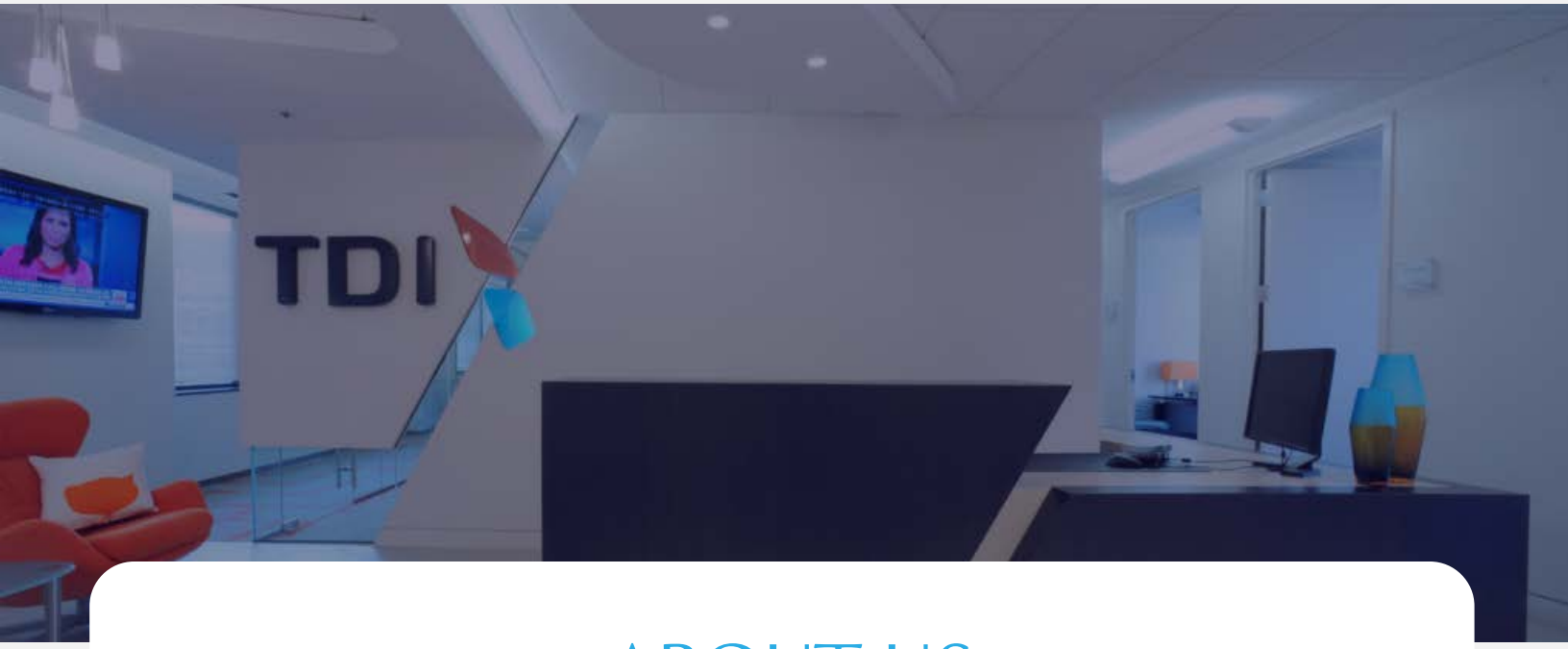
Jesse K. Dean is the Vice President of Solutions at TDI. He has over 20 years' experience across multiple market sectors as a practitioner and leader in both cybersecurity (audit, policy, compliance) and technology (software development, IT ops, DevOps, cloud migration). He holds a master's degree in Information Technology, with a concentration in Information Systems Project Management from the George Washington University and maintains the CISSP and PMP certifications.



Cyber Engineer

Tristan Hinsley

Tristan Hinsley is a Cybersecurity Engineer at TDI, specializing in providing GRC services for TDI clients, industry research, content generation and more. Tristan is an outgoing individual with a diligent work ethic, passion and drive, and cybersecurity experience within compliance with NIST-800-171 and NIST 800-53 specifications and using his technical knowledge to support technical control remediation. He graduated from George Mason University's Volgenau School of Engineering with a BS in Information Technology and a concentraction in Cybersecurity.



ABOUT US

CnSight is powered by TDI, one of the longest practicing cybersecurity firms in the field. We've taken our million hours plus of experience across defense, intelligence, and commercial markets to develop an innovative solution to solve the challenges faced by today's security and business leaders.

Founded in 2001, TDI secures our clients around the globe against threats thru innovative tech-enabled services and our cybersecurity management performance platform - CnSight - to effectively manage cyber and risk across the enterprise.

www.cnsight.io

1 866 CNSIGHT

hello@cnsight.io

1718 Connecticut Ave NW, Suite 350, Washington, DC 20009

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021

Cyber Security Awards
Finalist 2020

REFERENCES

[1]https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem &
https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem &
https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[2]https://www.insight.com/en_US/content-and-resources/2021/cybersecurity-at-a-crossroads--the-insight-2021-report.html

[3]https://cnsight.io/board-report-waitlist/

[4]https://securityintelligence.com/posts/whats-new-2021-cost-of-a-data-breach-report/

[5]https://www.nacdonline.org/insights/board_resources.cfm

[6]https://isalliance.org/nacd-and-isa-to-expand-collaboration-internationally-on-cybersecurity-for-boards-of-directors/

[7]https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf

[8]https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71795

[9]https://www.gsb.stanford.edu/faculty-research/publications/what-drives-differences-management-practices