Cyber Talk

EXECUTING A SUCCESSFUL

CYBER SECURITY TRANSFORMATION

Sponsored by Cyber Talk

Introduction

The race to digitally transform is on. Although organizations are eager to transition to digital models, transformation efforts fail 90% of the time.[1] Regardless of your stage within the digital transformation process, as your organization's cyber security leader, you need to develop a clear digital transformation mindset.

You need to develop a clear digital transformation mindset.

It's tempting for many organizations to hastily latch onto the nearest solutions without a strong vision, a thorough evaluation of risk and corresponding safeguards, and a detailed list of capabilities to ensure the long-term success of a secure transformation.

[1] "Competitive Landscape — Threat Intelligence Services," page 7, Gartner, October 2014

Vision: Eyes on the Prize

Your vision can carry your organization forward, making it more competitive and more profitable. However, the first major obstacle to clear before moving ahead with ideas consists of engaging leadership, and building trust in the approach. Without the support of board members and high-level internal leaders, your intended plans may stagnate, or worse, invite criticism.

> Although companies are often eager and enthusiastic about the endeavor, transformation efforts fail 90% of the time.

VOTE OF CONFIDENCE FROM THE BOARD

When it comes to cyber risk, boards of directors are more informed than ever before. In 2015, 22% of board members stated that they had little or no knowledge of cyber security. By 2019, that number dipped to 15%.[2] Nonetheless, this means that a significant number of board members (three out of every twenty) are still receiving a failing grade when it comes to understanding cyber security essentials.

Because board members are responsible for the financial calculations and risk tolerance of the organization, and because these two themes heavily impact CIOs and CISOs, they should feel motivated to educate the board about cyber security.[3] The less board members know about cyber security, the tighter the caps on CISO spending.

Too often, cyber security can be viewed by stakeholders as an obligation rather than an investment in reducing corporate risk and driving business value.

HAVING THE RIGHT CONVERSATIONS

More than one third of cyber teams are unaware of how to converse in business terms.[4] This is inability to communicate well can hinder progress in achieving current and future team objectives.

Board members speak the language of finance and risk. When speaking with your board, broadly paint a picture of the risk, and the financial resources that you require to offset it. Ensure that everyone is aware of the largest cyber threats to the business, and which facets of the company contribute to porous perimeters. In addition, "A critical early step is to ensure the board and senior leadership agree on the 'crown jewels'" of the company; the data and assets that are most in need of protection".[5] This helps set priorities and offers lower risk profile for your business.

---

[2] "5 Security Questions Your Board Will Inevitably Ask," Gartner, Kasey Panetta, October 23, 2019

[3] Ibid

[4] "Digital Trust Insights 2019," PwC South Africa

[5] "CISOs Need to Unleash the Power of Storytelling to make Cybersecurity Real to Boards, Leadership: Report," FierceHealthcare, Heather Landi, May 22, 2019

Evaluating Risks and Moving Forward

A successful digital transformation depends on a thorough evaluation of the risks and a corresponding roadmap. Here, we examine three core areas of cyber risk, and relevant benchmarks that signal an improved security posture.

THE ARCHITECTURE ITSELF

A CISO's role is to lead in developing and strengthening an organization's foundational security architecture.

A critical means of improving operational management while simultaneously simplifying architecture consists of implementing a consolidated security solution. A consolidated solution presents security professionals with a common risk language that includes consistent alert indicators, a uniform set of response protocols, and standardized terminology, enabling viewers to move from analysis to action more quickly than ever before.

An average security operations center (SOC) contends with 10,000 inbound alerts each day.[6] Security analysts are often overwhelmed by the volume of alerts, and consequently can't devote as much time as needed to actually remediate and resolve issues. And occasionally, an alert is mis-categorized due to bleary eyes and alert fatigue.

A well-orchestrated and cohesive consolidated approach can cut the noise, heighten categorization accuracy, transform staffing needs, and help you stop attacks at the start, improving your organization's overall security outcomes.

An average security operations center contends with 10,000 inbound alerts each day.

AUTOMATION

It's likely that you're using automated processes, but are there other processes that can become part of your automated architecture?

Although you may have functional operational processes in place, there's often room for improvement. For example, in one organization, a CISO felt proud of employing seven different marquee threat detection tools. However, when probed about how he used all of the tools, he replied, *"I focus on the one that's giving me the most actionable data."* In other words, he only used one tool at a time, while the data from the other six tools languished, unattended.[7] This CISO's operational system functioned, but for timely threat management, you'll need a different configuration.

[6] "Security Analysts Are Only Human," Roselle Safran, Utpal Desai, February 21, 2019

With automated tools, you don't need more hours in a day or additional staff to stay on top of threats. Real-time threat information gives you both high-level and granular visibility that enables you to expeditiously maintain and restore systems. In addition, automated tools can also trim costs, and increase efficiency within your accounting department. Your organization will pay a single vendor once, rather than paying an ever-growing list of vendors at varying intervals.

Real-time threat information gives you both high-level and granular visibility that enables you to expeditiously maintain and restore systems.

THREAT INTELLIGENCE: KNOW THY ENEMY

Without insights into attackers' methods and motives, combatting insidious cyber threats feels nearly impossible. Cyber threat intelligence is of particular import to organizations that rely on diverse devices and platforms with asymmetrical attack surfaces

By 2025, the threat intelligence market is predicted to surpass 13 billion USD, pointing to the value of credible threat intelligence resources.[8] As you might imagine, some vendors offer more expansive threat intelligence options than others. When searching for an intelligence platform, seek out those that offer:

1. Alignment with your organization's unique needs.
2. Integrated architecture, and can pull information from both internal and external sources.
3. Predictive architecture, warning you about imminent events before they occur.
4. Customized insights to fit the needs of your organization.
5. Rapid-fire responses, giving you all the info you need at lightning speed.

Threat intelligence can help your organization make better decisions and can measurably demonstrate value by blocking an increased volume of threats.

Examine and reexamine your cyber risks, and apply forward-thinking solutions in order to improve your long-term business outcomes.

[7] "Missing the Forest for the Trees: Top 5 CISO Pitfalls in Cybersecurity," Security Boulevard, Aaron Pritz, June 20, 2019

[8] "Threat Intelligence Market Size Analysis by Key Players Trends, Growth Till 2025," MarketWatch, April 4, 2019

The Long-term Impact: Where There's Security, There's Trust

Bake security into your service/organization and address customers' potential security concerns up front. Cite newly implemented frameworks within your roadmap and show that security is a significant focal point within your organization. In this way, you'll be able to show that customer concerns are your highest priority.

DEVELOPING TRUST WITH B2B CUSTOMERS

In PwC's 20th global CEO survey, 69% of CEOs reported that earning and retaining trust in the digital age can be a challenge.[9] To earn and retain trust, be upfront with your customers. Ask your sales team to highlight security during early stage conversations, rather than waiting for it to come up at signing. Security and privacy are competitive factors when organizations evaluate suppliers. If your customers feel that your organization is neglecting cyber security, they'll move on to another vendor. Demonstrating strong and impenetrable cyber safeguards works in your favor, helping to retain and expand your customer base.

BUILDING TRUST WITH B2C CUSTOMERS

Among B2C customers, your security and privacy image matters greatly. In a survey, only 25% of consumers stated that they believe companies responsibly handle their personal data.[10] Current levels of consumer trust are not much to speak of, but the security safeguards that your company implements can effectively help reshape negative perceptions.

Regardless of how many years your organization has been in existence, or its precise history, when your security is strong, you improve brand trust, and in the long run, it pays off.

Being a Rule Follower Makes You a Better Leader

For organizations subject to regulations like SOX, GLBA, HIPAA and/or GDPR, the stakes are especially high. Get security that fosters a culture of compliance, and that continues to build trust. Although compliance with regulatory mandates doesn't automatically add up to good security, it can help insulate your organization from legal, financial, and client backlash in the event of a breach.

---

[9] "How Consumers See Cybersecurity and Privacy Risks and What to do About it," PwC, August/September 2017

[10] Ibid

Conclusion

With a strong vision, a thorough evaluation of your architecture, and a refreshed roadmap, you can revamp your cyber security approach, and execute a clean digital transformation. Following the steps outlined in this paper, you can achieve macro and micro-level business improvements. Your executives, shareholders, and clients will appreciate the steps you've implemented to protect high- value assets.

For more information on how a single, consolidated architecture can enrich your organization, please visit the Check Point Infinity webpage, or reach out to your local Check Point representative.

A Case in Point

PGNiG Termika, a leading energy supplier in Poland, wanted to transform its cyber security to better protect employees and to better understand the threats targeting the rapidly evolving business.

In partnership with Check Point, the business successfully limited architectural complexity, and enhanced threat management capabilities. From the big ticket items to the small stuff, network engineer Konrad Sobczak says, "Check Point makes my daily duties easier…it is easy to manage and provides insights into what's happening in the network," improving cyber safety for everyone.[11]

Read their story here.

[11] PGNiG Termika Strengthens Security to Protect Energy Supplies," Check Point Software Technologies

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com