Cybersecurity Is All About People

White Paper

A call for fostering a strong cybersecurity culture that extends beyond mere awareness

Authors:

Dr. Jetzabel Maritza Serna Olvera
Leonie Bader

CYBER4PEOPLE

The projected annual damage caused by cybercrime worldwide is expected to reach a staggering USD 10.5 trillion by 2025.[1] While cybersecurity is being recognized as one of the top global business risks,[2] the human factor remains the primary source of attack in many cases.[3] This highlights the critical need for businesses to prioritize cybersecurity efforts that account for the human aspects.

The importance of addressing cybersecurity holistically is undeniable. However, the human aspect of security has often been neglected, and essentially been reduced to traditional cybersecurity awareness programs which have proven to be insufficient in keeping up with the evolving threat landscape. Forward-thinking organizations must move beyond simple awareness[4] and foster a strong cybersecurity culture.

In the subsequent sections of this whitepaper, we will:

- Delve into what is cybersecurity culture.
- Uncover common misconceptions surrounding cybersecurity culture.
- Define the key components essential for cultivating a positive and engaged cybersecurity culture.
- Explore strategies for transforming a negative mindset into a proactive one.
- Discuss the significance of ownership in fostering a collective responsibility for cybersecurity.
- Address the challenge of competencies, offering insights into innovative training and education programs.
- Examine the pivotal role of transparent communication and effective leadership in shaping cybersecurity culture.
- Delve into the importance of incentives and recognition in driving the widespread adoption of best cybersecurity practices.

This whitepaper aims to provide actionable insights, practical strategies, and a holistic understanding of cybersecurity culture for organizations looking to enhance their overall security posture.

Top 1

Business Risk: Cybersecurity

$10.5T

Projected Cybercrime Impact by 2025

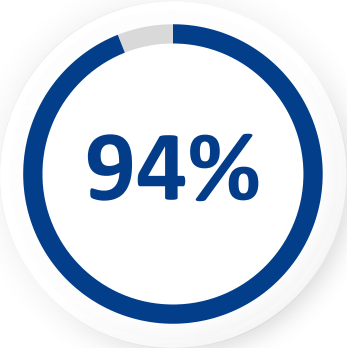
82%

Breaches Involving the Human Element

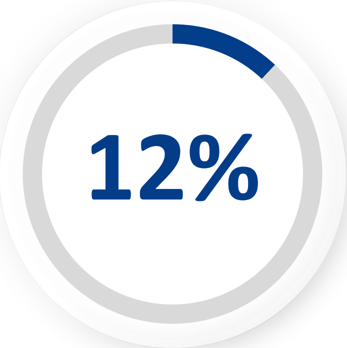
The cybersecurity culture misconception

Discussions about cybersecurity culture with experts can often result in varying interpretations of the topic due to a lack of a universally accepted definition. This can make implementation and agreement on what it entails difficult. This has been referred to as the[5] "problem of definition" by Perry Carpenter and Kai Roer in their "Security Culture Playbook". The authors noted that, despite 94% of 1,161 cybersecurity leaders surveyed recognizing the significance of cybersecurity culture for business success, only 12% defined it as "security being integrated into the organization".

The common misconception of equating cybersecurity culture with security awareness is a recurring challenge. Additionally, while awareness is crucial, it is merely a small component of what shapes cybersecurity culture.



94% of 1,161 Cybersecurity Leaders Recognize Cybersecurity Culture's Key Role in Business Success



Only 12% of Cybersecurity Leaders Defined Cybersecurity Culture as 'Security Integrated into the Organization

What is cybersecurity culture?

Cybersecurity culture is made up of more than just training and awareness initiatives. It also involves established policies and procedures, strong leadership, and efficient communication.

As defined by ENISA’s Cyber Security Culture in organizations report,[6] the cybersecurity culture of an organization encompasses the collective understanding, beliefs, attitudes, norms, and values of its employees regarding cybersecurity and their behavior towards information and communications technology. It involves making cybersecurity an integral aspect of daily operations and incorporating it into employees' job responsibilities, habits, and actions.

Key Components for Cultivating a Positive and Engaged Cybersecurity Culture

Positive Mindset

- Emphasize cybersecurity as vital for digital success.
- Showcase personal impacts, making it relatable.
- Simplify policies and automate processes.

Ownership

- Cultivate cybersecurity as everyone's duty.
- Leaders model good behavior.
- Clearly define roles for protection.

Competencies

- Address expert shortage with tailored programs.
- Tailor training for effective implementation.
- Extend competency throughout the organization.

Communication

- Create open dialogue.
- Use understandable language.

Leadership

- Leaders make cybersecurity a priority.
- Reflect on incidents, and emphasize learning.

Incentives

- Acknowledge proactive practices.
- Deal with those falling short.

With a clearer grasp of cybersecurity culture, let us now outline the desired outcomes, determine the driving forces behind them, and explore the path to realizing them.

Positive mindset

Cybersecurity poses a challenge, often perceived as difficult, restrictive, and frustrating. Individuals may resist engaging in it, viewing it as an obstacle hindering productivity. The negative perception of cybersecurity stems partly from the notion that it requires additional effort without immediate tangible benefits.

To transform this mindset, leaders should actively emphasize cybersecurity's importance beyond risk mitigation, framing it as a critical aspect of digital product or service quality. Shifting the perception of cybersecurity from a bothersome duty to a vital element of success is essential.

Making cybersecurity more relatable is a key strategy in this shift. Colleagues need to understand that good cybersecurity practices not only safeguard company assets but also protect their personal digital lives. From securing personal email accounts to preserving sensitive information, adopting strong security habits positively impacts individual well-being.

Another challenge lies in the length and complexity of security policies, often daunting for non-security professionals. Simplifying policies, providing user-friendly guidelines, and automating cybersecurity processes can address this issue. Equipping employees with the necessary cybersecurity skills and tools is crucial for seamlessly integrating cybersecurity into daily tasks.

Additionally, addressing communication, collaboration, and trust issues, as highlighted in the study "Why IT security needs therapy?" by Angela Sasse et al[7] can improve relationships between cybersecurity experts and the organization.

Ownership

The ideal state should be one where cybersecurity is viewed as everyone’s responsibility. Employees should understand the role they play in maintaining the organization's security, perceive cybersecurity as a collective effort, and be motivated to actively participate. Leaders play a crucial role; they should model good cybersecurity behavior and follow the same practices they expect from their employees.

To foster a strong cybersecurity culture, it is crucial to clearly define and assign cybersecurity roles and responsibilities within the organization. This helps to ensure that all employees understand their part in protecting the organization's digital assets from both external and internal threats.

Further, it is essential to identify and address any gaps in processes and communication between teams that may lead to a lack of accountability. It is equally important to empower employees with the autonomy and authority to make informed decisions.

Competencies

Cybersecurity cannot be solely reliant on a limited pool of cybersecurity experts, as the shortage of such professionals is well-known, and recruitment can be challenging. The challenge of staying ahead of rapidly advancing technologies and the mismatch between employees' cybersecurity skills and organizational needs must be addressed.

Developing cybersecurity competency is a critical component, requiring innovative and tailored awareness, training, and education programs. Outdated methods such as phishing awareness campaigns are no longer effective and do not contribute to a healthy cybersecurity culture as most of these campaigns induce fear in employees. Similarly, one-size-fits-all approaches are insufficient for enabling employees to implement cybersecurity processes and handle any incidents effectively.

Effective training must be tailored, considering employee roles, responsibilities, and skills. Skills-based training needs to consider the current knowledge and experience levels of employees and ensure a proper understanding and implementation of cybersecurity processes throughout the organization, including sales, purchasing, management, engineering, and all aspects of the supply chain.

Communication

Bringing together employees and managers with diverse backgrounds, teams, and functions can be a daunting task, but effective communication is essential to the success of any cybersecurity effort.

Transparent, trustworthy, and open communication forms the cornerstone of effective cybersecurity communication. Empowering employees to openly discuss cybersecurity issues, even if they are the cause, is crucial as it leads to greater awareness and preparedness against potential threats.

Effective communication also involves using language that is accessible and understandable to all employees.

Leadership

Leaders have the power to make cybersecurity a priority and promote open discussions about the topic across the organization while maintaining a balance between the need-to-know principle for specific cases, like ongoing incidents, and facilitating transparent communication about security-related matters. By discussing the current cybersecurity posture, reflecting on past incidents, and stressing the significance of learning from mistakes, leaders can continuously enhance the organization's security culture.

Incentives

Finally, proper incentives for following best cybersecurity practices are key for widespread adoption. You should acknowledge and reward those who take cybersecurity ownership (those who actively report incidents, engage in cybersecurity initiatives, adopt, and use cybersecurity tools, proactively seek out information about cybersecurity, etc.), along with addressing those who fall short in their commitment to these practices.

Strategies for Cultivating a Robust Cybersecurity Culture

So, what can you do to move beyond awareness and focus on building a robust cybersecurity culture?

Get leadership buy-in

Forge a direct link between cybersecurity and business objectives by showcasing how cybersecurity practices contribute to organizational goals, including asset and reputation protection, ensuring business continuity, and meeting regulatory requirements. Quantify cybersecurity risks, presenting management with concrete data on potential impacts in the event of breaches.

It is also critical to provide ongoing training to management, educating them on the evolving threat landscape, making threats relatable to the organization, and enhancing their understanding of cybersecurity risks, best practices, and their role in fostering a robust cybersecurity culture.

Streamline cybersecurity processes

Establish a routine for regular reviews and updates of cybersecurity policies, ensuring clarity and ease of understanding for all employees. Integrate automation tools to streamline processes, reducing manual effort and enhancing the overall efficiency of cybersecurity measures. Additionally, embed cybersecurity features by default in systems and processes whenever feasible, simplifying adherence to best practices for employees.

Promote continuous learning

Create customized and innovative awareness, training, and education programs tailored to address the specific cybersecurity skills and organizational needs of employees. Illustrate the significance of cybersecurity as a critical element in digital products, services, and infrastructure, making it relatable to daily operations. Foster engagement through gamified hands-on learning experiences, incorporating activities like jeopardy-style capture-the-flag events to enhance practical understanding and retention.

Encourage transparent, trustworthy, and open communication throughout the organization.

Establishing effective communication channels and dedicated cybersecurity communities is crucial. Organizing events focused on cybersecurity and integrating related topics into existing events ensures widespread awareness. Regularly including cybersecurity discussions in meeting agendas fosters a culture of vigilance. Cultivating a blame-free environment prioritizes learning from mistakes over assigning blame, promoting a positive error culture.

Additionally, offering training and support to managers and cybersecurity professionals enhances their communication skills, enabling them to convey security-related information clearly and empathetically. Moreover, recruiting cybersecurity champions can act as conduits, fostering trust and further enhancing communication within the organization.

Acknowledge and reward excellent cybersecurity practices.

Implementing a recognition program, like a hall of fame, encourages employees to engage in cybersecurity initiatives and report issues. Providing tangible incentives linked to achievements such as completing cybersecurity training or contributing to policy improvements motivates proactive participation. Incorporating cybersecurity performance into evaluations ensures a comprehensive approach to assessing employees' commitment to maintaining a secure environment.

Cybersecurity Leadership Checklist

1

Align Strategy

Ensure cybersecurity efforts are strategically aligned with overall business objectives.

2

Risk Quantification

Quantify cybersecurity risks and present tangible data to leadership.

3

Continuous Education

Implement ongoing, role-specific cybersecurity training programs for all employees.

4

Policy Streamlining

Conduct regular reviews to simplify and update cybersecurity policies for clarity.

5

Transparent Communication Channels

Establish open communication channels dedicated to cybersecurity discussions.

6

Recognition and Rewards Framework

Ensure cybersecurity efforts are strategically aligned with overall business objectives.

Institute a structured recognition program with tangible incentives for cybersecurity excellence.

Conclusion

The imperative shift towards a robust cybersecurity culture is evident in the face of escalating cyber threats. Recognizing the human factor as a primary source of vulnerabilities, organizations must adopt a holistic approach to cybersecurity, moving beyond misconceptions that equate it solely with awareness.

Key strategies for this cultural shift include:

- Fostering a positive mindset that views cybersecurity as a vital element of success.
- Promoting ownership and clearly defining cybersecurity roles and responsibilities.
- Developing competencies through tailored training programs and addressing skill gaps.
- Enhancing transparent communication and effective leadership at all organizational levels.
- Providing proper incentives to acknowledge and reward cybersecurity practices.

In a strong cybersecurity culture, all members understand their roles, possess the necessary knowledge, and feel empowered to contribute collectively to the defense against cyber threats. As businesses strive for resilience and success in the digital age, the cultivation of a cybersecurity culture emerges as an indispensable strategic imperative, transcending the limitations of mere awareness.

Authors:

Dr. Jetzabel Maritza Serna Olvera

Leonie Bader

References:

1. Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybercrime Magazine https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
2. Allianz Risk Barometer Report 2023, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
3. Verizon Data Breach Investigation Report 2023, https://www.verizon.com/business/de-de/resources/reports/dbir/
4. Gartner Top 7 trends in Cybersecurity 2022, https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022
5. The Security Culture Playbook. 1st edn. Carpenter, P. and Roer, K. (2022) Wiley.
6. ENISA Cyber Security Culture in Organisations Report 2018, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
7. Why IT Security Needs Therapy. Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M. Angela Sasse, CyberICPS/SECPRE/ADIoT/SPOSE/CPS4CIP/CDT&SECOMANE@ESORICS 2021: 335-356