WISP 2023 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-10-2023

Cybersecurity in Contemporary Organizations: A leadership challenge

Gurpreet Dhillon
University of North Texas, gurpreet.dhillon@unt.edu

Rajiv Kohli
William & Mary

Recommended Citation

Dhillon, Gurpreet and Kohli, Rajiv, "Cybersecurity in Contemporary Organizations: A leadership challenge" (2023). *WISP 2023 Proceedings*. 7.
https://aisel.aisnet.org/wisp2023/7

Cybersecurity in Contemporary Organizations: A leadership challenge

Gurpreet Dhillon[1]
University of North Texas,
Denton, TX, USA

Rajiv Kohli
College of William and Mary,
Williamsburg, VA, USA

ABSTRACT

This paper addresses narrowing the gap between business executives and cybersecurity technologists for cybersecurity preparedness within organizations. Without a common understanding of cybersecurity risks, organizations become vulnerable to data breaches. To manage cybersecurity effectively, leaders must stay informed about evolving threats and adopt a proactive approach. We draw upon interviews with senior business and cybersecurity executives and propose three action items to narrow the gap -- engage with cybersecurity professionals, establish cyber governance, and counter social engineering, which will prepare organizations to protect against cyber threats and become resilient when a cyber breach occurs.

Keywords: Cyber resilience, Cybersecurity, Leadership, Alignment.

INTRODUCTION

A World Economic Forum report[2] notes a substantial disparity between corporate executives and information security professionals, particularly in how they assess the effectiveness of cybersecurity measures within organizational settings. 92% of surveyed business leaders agreed that cyber resilience represents a foundational element within their comprehensive enterprise risk management strategies. This finding underscores the commitment to protecting organizations from cyber threats and addressing potential incidents to prevent disruption.

[1] Corresponding author. gurpreet.dhillon@unt.edu +1 940 369 7076
[2] https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

Nonetheless, it is noteworthy that only 55% of security-focused executives believe that cyber resilience is fully integrated into their risk management strategies, revealing the gap in cybersecurity readiness that can make organizations vulnerable to cyberattacks.

The management of cyber security in contemporary organizations may seem daunting, but with an adaptive approach, leaders can effectively navigate the complexities of cyber security management. Taking on this multifaceted challenge requires a confident and proactive mindset at all levels of the organization. It's particularly crucial for leaders to stay informed of the evolving challenges and remain up to date with the steps to counter potential threats. By doing so, they can help their organization stay safe in the growing digital footprint where new threats are certain to emerge.

In this paper, we present action items derived from in-depth interviews with senior executives from business functions and cybersecurity. Our recommendations will prepare organizations to safeguard against cyber threats through three primary actions – (i) engage with cybersecurity professionals, (ii) establish cyber governance, and (iii) counter social engineering.

ENGAGE WITH CYBERSECURITY PROFESSIONALS

Cybersecurity knowledge gaps between senior managers and technology professionals continue to persist. As more sophisticated technologies emerge, so will the cyber risks. Given that future cybersecurity risks will require a deeper understanding, this gap will likely widen.

Several contributing factors exacerbate this divide, with one of the most prominent being the inadequate engagement of business leaders with cybersecurity professionals. This lack of proper engagement can manifest in diverse ways. For instance, senior management might make key business decisions regarding adopting new technologies that cause changes in business processes without seeking input from their cybersecurity team. The result is a lack of senior management awareness of the organizational risks and their tolerance levels (Abraham et al. 2019). Such decisions can lead to implementing novel technologies or processes that inadvertently introduce heightened security vulnerabilities (Leventhal 2018).

The budget allocation also bears the imprint of an engagement deficit. Senior management may either allocate insufficient resources to cybersecurity efforts or restrict the cybersecurity team's autonomy in resource allocation, hindering the team's ability to execute its duties effectively. Additionally, the absence of proper engagement results in a dearth of cybersecurity awareness among senior management about the nature of emergent cyber threats. This knowledge gap can impede informed decision-making on other matters, such as vendor selection and acquisitions, that expose the organization to indirect cybersecurity risks.

The absence of engagement frequently forces cybersecurity professionals to make compromises in talent and resource acquisitions that jeopardize their organization's security. Therefore, cybersecurity measures are deployed *ad hoc* rather than designed into the fabric of the organization’s processes and information systems. The ramifications of compromising on cybersecurity can be severe, ranging from financial losses, operational disruptions, reputational damage, and, in extreme cases, to physical harm, particularly when critical safety infrastructure is compromised.

Lack of cybersecurity engagement on the part of business executives can have devastating impacts before, during, or after a cyber breach incident. During a cyber-attack in Atlanta, USA, a journalist inquired about the scope of the attack's impact, specifically questioning its effects on permits for new homes, Department of Motor Vehicles (DMV) operations, or whether it was merely an outage. Mayor Keisha Lance Bottoms suggested that individuals should monitor their bank accounts due to potential threat actors. While it was good advice, the mayor’s comments inadvertently generated public panic, highlighting the disconnect between senior executives of her office and cyber professionals leading to a lack of awareness within the leadership.

So, what can organizations do? They must engage with their cybersecurity professionals, learn about the necessary support and resources, and make necessary investments in cybersecurity. This involves seeking input from cybersecurity professionals on all major decisions that impact security. In practical terms, assigning a cybersecurity professional to a C-level role can ensure that cybersecurity becomes an integral part of the planning conversation.

ESTABLISH CYBER GOVERNANCE

The intersection of data governance and cybersecurity governance is salient, as data ranks among a corporation's most valuable assets (Thuraisingham 2019). The assets encompass raw data, information, and insights gained from analysis. Together, these constitute an organization’s digital assets and intellectual capital that must nurtured, shared, and protected. Together, these constitute an organization’s digital assets and intellectual capital that must be nurtured, shared, and protected. In spite of the fact that the Chief Information Officer (CIO) plays a pivotal role in overseeing data and digital assets, most of these activities take place outside of the IT department. Therefore, a governance structure clearly defining roles and responsibilities is necessary to safeguard digital assets.

In this context, essential questions arise: What constitutes the critical data that must be secured? Where does the data originate, who handles it, and where is it stored? As data assets differ in their importance (e.g., office picnic data vs. product design data), the governance structure must identify who is responsible for identifying the security level of digital assets. How is it integrated and analyzed, and what protocols guide sharing, alteration, and deletion? Who has the authority to allocate sharing and deletion rights?

In 2021, Securitas[3], a Swedish company offering customized security and guarding solutions, experienced a data breach exposing 1.5 million files. Insufficient data governance practices primarily caused the breach. Specifically, the company left one of its Amazon S3 buckets open to the public. This oversight exposed sensitive company data and the Personally Identifiable Information (PII) of employees at airports in Colombia and Peru. Many other high-profile incidents reported in recent years also involve public S3 buckets. These permission issues are not just a concern for Amazon S3 but can jeopardize data in most storage systems. Thus, maintaining proper data governance, clear roles, and defined responsibilities becomes crucial.

To ensure effective cybersecurity governance, it is imperative to identify and allocate tasks and responsibilities appropriately (see (Dhillon et al. 2021). While defining roles and responsibilities is not a new concept, and was highlighted by (Backhouse and Dhillon 1996), it remains crucial in cybersecurity. They argue that organizations should be viewed as structures of responsibility, with responsible agents assigned specific tasks and substantive actions of the business, a characterization that enhances information security.

However, in today's landscape characterized by increased reliance on data and the pervasive use of technology in work processes, the focus on cybersecurity governance and delineating roles and responsibilities takes on heightened urgency.

[3] https://www.securitymagazine.com/articles/96996-security-firm-securitas-exposed-airports-employees-in-data-breach

COUNTER SOCIAL ENGINEERING

As organizations become more aware of cybersecurity risks and implement governance structures to fortify data assets, cyber criminals recognize that human fallibility remains the weak link. They use social engineering[4] to trick people into letting them access the organization's data assets. They often use psychological manipulation techniques to deceive customers or employees, compelling them to disclose confidential or sensitive information. The primary objective is to exert influence, manipulate, or deceive individuals, leading them to surrender critical information or access within an organization. These attacks can take place through various communication channels, including face-to-face interactions, phone calls, and electronic mail, provided the attacker possesses skill in deception.

Our interviews uncovered the deleterious effects of social engineering that sometimes go undetected for a long time because the cyber breach appears to be a legitimate activity. Employee education is the most effective antidote to social engineering cyber breaches. Over the years, the attack types have increased and become more sophisticated. For example, phishing attacks and vishing, in which cybercriminals combine voice calls with phishing tactics, have experienced a significant increase. Recently, vishing banking scams have also become more widespread. In such cases, an attacker assumes the role of a representative from a bank or another financial institution. They may warn that there is an issue with your account or a late payment and ask to transfer funds to an account to resolve the purported problem. However, their true intent is simply to steal money.

[4] Krombholz et al (2015) define social engineering as the act of "manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion" (p. 114).

Among numerous instances of social engineering, one prominent case is the 2016 US Presidential Election Email Leak[5]. In this incident, malicious actors executed a series of spear-phishing attacks by sending deceptive emails to various individuals within The Democratic National Convention's network. The emails were disguised as warnings from Google, alerting recipients to suspicious activities on their Google accounts. To conceal the true redirect path, the email employed a Bitly URL to shorten the link. Once recipients clicked on the shortened link, they were directed to a webpage that prompted them to reset their password. When targets fell for the deception and entered the login credentials, the cybercriminals accessed their Google accounts. Cybercriminals purged thousands of emails containing sensitive information about the Democratic party candidate Hillary Clinton's campaign.

To address attempts to compromise cybersecurity through social engineering, organizations have turned to security awareness training. Originating from the Federal Computer Security Act of 1987, the significance of user awareness and security controls was recognized to address cybersecurity threats. As a result, the practice of annual training requirements was established. Recently, ISACA's 2021 Privacy in Practice Report[6] found that 67% of the 1,873 surveyed security and technology leaders provide privacy training annually, with only 14% offering it quarterly. Additionally, 52% incorporate training in their onboarding process, and 18% deliver training in response to significant events. However, despite the increasing use of technologies in digital transformation, training methods have remained largely unchanged.

Scholars have frequently emphasized the need for training (e.g., (Bulgurcu et al. 2010) or focused on how to deliver such training (e.g., (Dincelli and Chengalur-Smith 2020), but they

[5] https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

[6] https://www.isaca.org/go/privacy-in-practice-2021-survey

have rarely delved into the content of the training. Even organizations that value training to enhance enterprise security often discover their programs are not as robust as desired.

CONCLUSION

As cyber breach threats have increased, keeping organizations secure is everyone's business. Our findings indicate that, in addition to building technical barriers, senior business executives must engage with cybersecurity professionals to learn about new challenges and solutions. Second, cyber governance structure ensures that roles and responsibilities are assigned that make it difficult for hackers to breach digital assets. Finally, we find that organizations must educate employees and partners about how to counter social engineering efforts. Together, these three actions will prepare organizations to protect against cyber threats and become resilient.

REFERENCES

Abraham, C., Chatterjee, D., and Sims, R. R. 2019. "Muddling through Cybersecurity: Insights from the Us Healthcare Industry," *Business Horizons* (62:4), pp. 539-548.

Backhouse, J., and Dhillon, G. 1996. "Structures of Responsibility and Security of Information Systems," *European Journal of Information Systems* (5:1), pp. 2-9.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Dhillon, G., Smith, K., and Dissanayaka, I. 2021. "Information Systems Security Research Agenda: Exploring the Gap between Research and Practice," *The Journal of Strategic Information Systems* (30:4), pp. 101693.

Dincelli, E., and Chengalur-Smith, I. 2020. "Choose Your Own Training Adventure: Designing a Gamified Seta Artefact for Improving Information Security and Privacy through Interactive Storytelling," *European Journal of Information Systems* (29:6), pp. 669-687.

Krombholz, K., et al. 2015. "Advanced social engineering attacks." *Journal of Information Security and Applications* 22: pp.113-122.

Leventhal, R. 2018. "Cyber Attacks Increase as IT Security Budgeting Remains Static, Report Finds," *Healthcare Innovation*. Accessed October 4, 2023. https://www.hcinnovationgroup.com/cybersecurity/news/13030218/cyber-attacks-increase-as-it-security-budgeting-remains-static-report-finds

Thuraisingham, B. 2019. "Cyber Security and Data Governance Roles and Responsibilities at the C-Level and the Board," *IEEE International Conference on Intelligence and Security Informatics (ISI)*: IEEE, pp. 231-236.