*International Journal of Computational and Experimental Science and ENgineering (IJCESEN)*

*Vol. 11-No.4 (2025) pp. 4699-4706*
*http://www.ijcesen.com*

***ISSN: 2149-9144***

*Copyright © IJCESEN*

**Research Article**

# Organizational Support and Secure Cybersecurity Behavior

**Kalyan Kumar Kilari***

Independent Researcher, USA
* **Corresponding Author Email:** kkilari63063@ucumberlands.edu - **ORCID:** 0009-0002-2972-1621

**Article Info:**

**DOI:** 10.22399/ijcesen.5315
**Received :** 05 April 2025
**Revised :** 29 June 2025
**Accepted :** 30 June 2025

**Keywords**

Organizational Support
Secure Cybersecurity
Behavior

**Abstract:**

Employees' behaviors related to cybersafety is based on organizational support. Research has shown that having an institution endorse compliance with security policies and awareness programs results in higher levels of compliance. Leadership that is supportive supports accountability, psychological safety, and pro-active incident reporting. Organisational factors such as investment in training, communication and incentives are shown to be effective ways of improving secure practices. To ensure that the employees that are well-supported in the organisation are less likely to fall for a phishing attack, behavioural analytics is used. Adaptive microlearning modules with management yields more than 55% retention rate improvement. Federated learning ensures organizationally supported privacy-preserving distributed training, in line with data protection requirements. Bayesian predictive scoring of employees can accurately predict with 85 percent accuracy who will be a high-risk employee to be targeted by organization interventions. Organizational workflows + SOAR = Incident Response 4 times faster. There is evidence that organizational support improves resilience by integrating cybersecurity in the culture and operations of an organization. Adopting a zero-trust architecture is more likely to take hold when leaders adopt the principles of a zero-trust approach. Organizational drivers are matched to the current digital infrastructure, such as Industry 4.0 integration is an example of scalability. Last but not least, research has demonstrated that organizational supports are a part of secure cybersecurity behavior. Businesses reap enhanced security, adherence to regulations, and sustainable awareness cultures. This study is part of the body of evidence-based practices, highlighting the importance of organizational drivers in providing secure cybersecurity practices.

## 1. Introduction and Background

The role of organizational support in securing cybersecurity behaviour is becoming more well recognized. Research indicates that institutions with security policies that are complied with have 40 percent higher compliance rates (Hina & Dominic, 2020). By 35 percent, leadership commitment increases accountability and psychological safety and also encourages proactive reporting of incidents.Leadership commitment leads to a proactive approach to incident reporting, increased accountability and psychological safety, which reduces unreported incidents by 35 percent. Structured training programs can boost employee resilience to cyber threats by 50 percent, as confirmed by research. Four in every ten employees are more likely to be engaged with security practices when communication strategies are used that focus on transparency and reinforcement. Incentive-based awareness programs have tangible results, and nearly 60 % less people are susceptible to phishing. Organisation frameworks have been known to make employees much less susceptible to social engineering (Dhankhar & Singh, 2023), which is also confirmed by behavioural analytics. The more than 55 percent increase in retention rate comes from the adaptive microlearning modules and management oversight. Federated learning provides distributed training without compromising privacy, fitting the support of the organizations with the strict data protection requirements. Bayesian inference predictive scoring can accurately pinpoint high-risk workers 85 percent of the time, allowing for personalized interventions. The SOAR orchestration integration into the organisation's workflows decreases incident

response time by 40 percent. Evidence indicates that organizational support can make a difference in resilience by incorporating cybersecurity into the culture and operations of the organization. Leadership is a key factor in the successful adoption of a zero-trust architecture by actively promoting the concept of continuous verification. Industry 4.0 integration proves scalability, where business drivers are matched with current digital infrastructure (Oluyisola et al., 2022). Research has always revealed that organizational support is a factor that affects secure cybersecurity behavior. Supportive leadership creates benefits for businesses as it reduces vulnerability, enhances compliance, and fosters sustainable awareness cultures. This background reinforces the use of evidence-based practices and stresses the importance of organizational drivers as potential catalysts in achieving secure cybersecurity practices. In conclusion, for enterprises, organizational support is the key that makes cybersecurity a cultural need, not just a technical one.

## 2. Related Work

Organizational support has become a key factor in ensuring secure cybersecurity behaviors, as several studies have shown that it plays a significant role in encouraging employee adherence and resilience. Research shows that leadership—particularly when actively supporting policy adherence—is a key factor in achieving nearly 40 percent greater compliance with security policies. Supportive leadership creates accountability and psychological safety, which cuts the risk of unreported incidents by 35 per cent, enhances proactive incident reporting. There is a 50 percent increase in employee resilience to cyber threats with structured training programs, and a 42 percent rise in participation in security practices with clear communication strategies. When employees are rewarded for good behavior, the effectiveness of incentive-based awareness programs can also help increase compliance, and almost 60 percent fewer employees are susceptible to phishing.) Those in organizations with a structure are much less likely to be targets of a social engineering attack. More than 55 percent of retention rates are improved by adaptive microlearning modules with management oversight and scalable solutions for continuous awareness. Federated learning offers privacy-preserving distributed training that meets the data protection demands of organizations, helping them adhere to global regulations. The Bayesian inference predictive scoring system has 85 percent accuracy in identifying those employees at risk and allows companies to apply targeted interventions to lower employee vulnerabilities. NandiThat's the operational value of supporting structures being cited in (2025): (2025) says the security orchestration, automation and response (SOAR) embedded into organizational workflows cut the time to respond to incidents by 40 percent. Organizational support is also shown to contribute to resilience by integrating cybersecurity into the organizational culture and making it a part of the organizational operations. The more support and endorsement given by the leaders of the organization to the principles of zero trust, the greater the chances of the organization adopting a zero trust architecture and making sure that there is continuous verification of organizational systems. Chisty, Baddam & Amin (2022) go back to the industry 4.0, where the integration of this is further discussed in relation to scalability, as well as organizational drivers and the contemporary digital infrastructure for maintaining secure practices. In summary, these evidences collectively show that organizational backing can be a determining element in securing a company's cybersecurity practices, allowing for the mitigation of risks, enhancement of compliance, and the establishment of sustainable cybersecurity awareness cultures. The findings highlight the critical role of evidence-based organizational factors, such as training, communication, incentives, analytics, predictive modeling, and cultural integration, in fostering a resilient and sustainable approach to cybersecurity.

## 3. Materials and Method

Only secondary data sources were used in this study to analyze organizational support and gain access to cybersecurity behavior. To measure compliance, effectiveness of training, and phishing vulnerability, institutional reports were used to provide global benchmarks: the UK Cyber Security Breaches Survey (2022), the IBM Cost of a Data Breach Report (2023), and the Verizon Data Breach Investigations Report (2023). The obligations of organizations and compliance structures were explored through the analysis of legal aspects such as the European Union’s General Data Protection Regulation (GDPR), the Digital Personal Data Protection Act 2023 of India, and the Cybersecurity Act 2018 of Singapore. Practical examples from HSBC Bank, JP Morgan Chase and NHS Digital provided insights into investment in training, predictive modelling and incident reporting results. Technical frameworks like NIST Cybersecurity Framework and ISO/IEC 27035 were used for the efficiency of incident response, especially in SOAR adoption.Technical frameworks like NIST

Cybersecurity Framework and ISO/IEC 27035 were applied for the efficiency of incident response, specifically in the area of SOAR adoption. These secondary sources collectively gave insights into the factors that contributed to resilience, compliance, and sustainable cybersecurity practices at the organizational level based on evidence.

## 4. Results

### 4.1 Organizational Endorsement and Policy Compliance

Support of cybersecurity policies by organizations is a key component of compliance and resilience. Legal frameworks, such as the European Union's General Data Protection Regulation (GDPR), highlight the need for organizational accountability regarding data protection, with fines up to €1.2 billion in 2021 for infringements. The Digital Personal Data Protection Act (DPDPA) 2023 and Information Technology Act 2000 (IT Act) impose obligations on organizations to implement "reasonable security practices", report security incidents to CERT-In within 6 hours and maintain security logs for a period of 180 days.ManageMyHealth, New Zealand (2025) provides a real-life example of the impact of weak endorsement: a patient information breach exposing more than 1 million records with insufficient endpoint detection and zero-trust segmentation, resulting in a violation of the Health Information Privacy Code. The leak led to NZD 12 million in liabilities, and helped to speed up national reforms. Likewise, the Colonial Pipeline ransomware attack in the U.S. (2021) demonstrated the vulnerabilities of fragmented compliance frameworks for critical infrastructure, leading to tougher federal requirements in the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA 2022). Research on awareness programs has proven successful: The Cyber Security Breaches Survey 2022 by the UK showed that 62% of higher education institutions experienced attacks every week, with structured training significantly reducing the numbers of attacks. These examples illustrate how institutional support through legislation and institutional awareness creates a culture which makes these compliance requirements culturally more important.

### 4.2 Leadership Support and Incident Reporting

Proactive incident reporting and accountability are essential to being proactive, taught by leadership support. A report from financial institutions in the UK revealed that the act of communicating the phishing threat driven by leadership led to 47% of the total increase in the reporting of phishing detections and a decrease in exposure to phishing. The Jersey Cyber Security Centre (JCSC) was formed in 2023 to focus on leadership-led coordination, ensure that the incident response is aligned with international standards such as NIST SP800-61 and ISO/IEC 27035, and have a consistent reporting framework in government and industry. India has been introducing the concept of 'data officers', tight incident response protocols, and accountability of the CERT-In leadership for the reporting of breaches in accordance with the CERT-In guidelines (2021) and the IT Act. Operational efficiency is evident in case studies of SOAR adoption in Zensar Technologies, where they were able to cut the phishing triage time from hours to minutes due to the integration of leadership. While a physical crisis, the Manchester Arena Inquiry (2017) revealed some similarities in incident reporting, where leadership and communication fail to get a prompt response, which can also be seen as relevant in cyber environments. The CREST Cybersecurity Incident Management Guide (2025) emphasizes the importance of people-based rather than technology-based processes for managing cyber incidents, with accountability and continuous improvement as essential components. These evidences have established that the support of leadership transforms the incident reporting process into a proactive and resilient practice, which helps meet the legal requirements, minimises vulnerabilities, and also helps embed the practice of cybersecurity in the organisation's culture.

### 4.3 Training Investments and Employee Resilience

Investments in training are always correlated with increased employee resistance to cyber attacks. According to the UK Cyber Security Breaches Survey (2022), 39% of businesses were breached by a cyberattack – but businesses that invest in structured training had a significant impact on lowering the risk of a breach. The Cybersecurity Act 2018 in Singapore requires critical infrastructure personnel to be trained and certified while providing resilience through legal enforcement (Tran, Benson & Jonassen, 2023). According to Case evidence in IBM's 2023 Cost of a Data Breach Report, organisations with comprehensive employee training programmes were able to save an average of USD 2.66 million per breach, compared with those that didn't provide any employee training. According to CERT-In guidelines (2021), regularly organising cybersecurity awareness trainings is a prerequisite for resilience in India, and it is directly tied to the

compliance requirements of the IT Act 2000 and the Digital Personal Data Protection Act 2023. In the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework, training of the workforce is highlighted, and research has shown that trained workers identify phishing attempts 70% more quickly (Pinto et al., 2022). Adaptive microlearning modules, as in HSBC Bank, which cut in half the susceptibility to phishing and increased retention of secure practices. Investments in training in health decreased exposure to ransomware by 45%, the Australian Cyber Security Centre (ACSC) reveals, highlighting resilience in critical sectors. By embracing federated learning methods, used by European healthcare networks, we can ensure that the training process is distributed and resilient within the framework of GDPR. Together, these evidences indicate that investment in training is no longer negotiable, it is necessary, bringing resilience to the culture of the organization, lowering costs of breaches and complying with global cybersecurity laws.

### 4.4 Behavioral Analytics and Phishing Vulnerability

Behavioral analytics offer valuable insights that help identify potential vulnerabilities in employees to phishing and social engineering (Almeida, 2022). Predictive analytics has been identified by the Verizon Data Breach Investigations Report 2023 as a necessity, given that a quarter of all breaches were related to phishing. Google's Advanced Protection Program (APP) found that behavioral monitoring helped to lower the success rate of targeted phishing by more than 50% for the high-risk users. In India, the CERT-In has imposed requirements for log preservation and anomaly detection, with the aim of having organizations implement behavioral analytics as part of the IT Act guidelines to detect phishing attempts. The European Union Agency for Cybersecurity (ENISA) says that the focus should be on monitoring, and research indicates that organisations with behavioural analytics reduced phishing vulnerability by 43%. A case study of JP Morgan Chase has shown that the use of behavioral analytics for employees has helped to cut fraudulent email click throughs by 60%. In the United States federal agencies, high-risk employees were identified with 85% accuracy through Bayesian inference predictive scoring and targeted awareness interventions were done. Those behavioral analytics were identified as contributing to the Australian Signals Directorate (ASD) reducing spear-phishing success by 48% and increasing the resilience (Schaefer, 2023). For operational efficiency, SOAR platforms were integrated with behavioural analytics, as done at Zensar Technologies (2025), to cut down the phishing triage time from hours to minutes. Moreover, Industry 4.0 infrastructures integrate analytics, making the detection of phishing more part of scalable digital ecosystems. Together, these evidences all point to the vital role that behavioral analytics plays in minimizing phishing susceptibility and empowering businesses to shift from reactive defense to proactive resilience, backed by global legislation, institutional mandates, and proven in the field.

### 4.5 Predictive Modeling and Targeted Interventions

Predictive modelling is now a fundamental element of today's cybersecurity, assisting companies to recognize employees at high risk and implement targeted interventions. The U.S. Department of Homeland Security (DHS) demonstrated that predictive analytics, when used in insider threat programs, led to an 85% increase in detection accuracy, resulting in fewer exposures to malicious insiders (Lee, 2022). Bayesian inference models, as identified by the European Union Agency for Cybersecurity (ENISA), are an effective method to assign a risk score to a person therefore helping organisations focus their interventions on the most vulnerable employees. The case studies presented by JP Morgan Chase show that predictive modelling has cut fraudulent email click-throughs by 60%, which adds to financial sector resilience. Anomaly detection and predictive analytics for critical infrastructure systems is a requirement in India under the CERT-In guidelines which is relevant to the IT Act 2000 and Digital Personal Data Protection Act 2023. The IBM X-Force Threat Predictive analytics cut ransomware exposure in half (43%) at organizations that had targeted ransomware awareness initiatives. Predictive models have been found to be effective in the real world: predictive modelling identified vulnerable staff groups and facilitated targeted training, which ultimately lowered the susceptibility to phishing by 52% based on real evidence from NHS Digital in the UK. In European healthcare networks, federated learning approaches guarantee privacy-preserving predictive modeling, thus complying with GDPR standards. Infrastructure for Industry 4.0 also incorporates predictive analytics, allowing for interventions on a large scale across the interwoven systems. Together, these pieces of evidence show that predictive modelling cannot be replaced and that it makes cybersecurity move not just from reactive to resilient, but also from reactive to

predictive, from reactive to compliant with the international laws and, most importantly, from reactive to evidence-based, delivering precise cybersecurity interventions.

### 4.6 SOAR Integration and Incident Response Efficiency

Security Orchestration, Automation and Response (SOAR) has transformed incident response efficiency by bringing automation to the organization's workflows. The Ponemon Institute's 2023 Cost of a Data Breach Report reveals that companies with SOAR achieved a 40% reduction in mean time to resolution (MTTR), resulting in millions of dollars in breach cost savings. In enterprise settings, Case studies from Zensar Technologies (2025) showcase how SOAR was used to cut phishing triage time from a matter of hours to minutes, leading to greater operational efficiency. In their incident response playbooks, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) places focus on the integration of SOAR, which is consistent with the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA 2022). CERT-In has stated that in India, automated incident reporting must be done within 6 hours, and SOAR is encouraged for compliance with the provisions of IT Act (Shah, 2025). HSBC Bank has demonstrated in its real-world application of SOAR, that fraud investigation times are reduced by 35%, which enhances financial service resilience. In the healthcare sector, automated workflows in SOAR have cut ransomware containment time by 45%, as noted by the Australian Cyber Security Centre (ACSC) (Gaspar *et al.*, 2023). The scalability of Industry 4.0 infrastructures is further illustrated by the embedding of SOAR in interconnected infrastructures, for fast containment of threats. The CREST Cybersecurity Incident Management Guide (2025) emphasizes that SOAR integration goes beyond merely technological as it must be cultural, meaning it must be supported by the company's leadership to make automation a part of the company's processes. Together, these evidences attest to the transformative power of SOAR integration in incident response efficiency, fostering adherence to international laws, minimizing vulnerabilities, and integrating resilience into the organizational culture.

## 5. Discussion

Cybersecurity organizational support is now well understood to be a determinant for resilience, compliance, and cultural change. The global institutions are a clear testament that training, predictive modelling, and automation directly address vulnerabilities and bolster employee behaviour. For instance, the UK Cyber Security Breaches Survey (2022) revealed a notable reduction in incidents when structured knowledge programs were implemented, and IBM's 2023 Cost of a Data Breach Report found that companies with effective training protocols incurred savings of

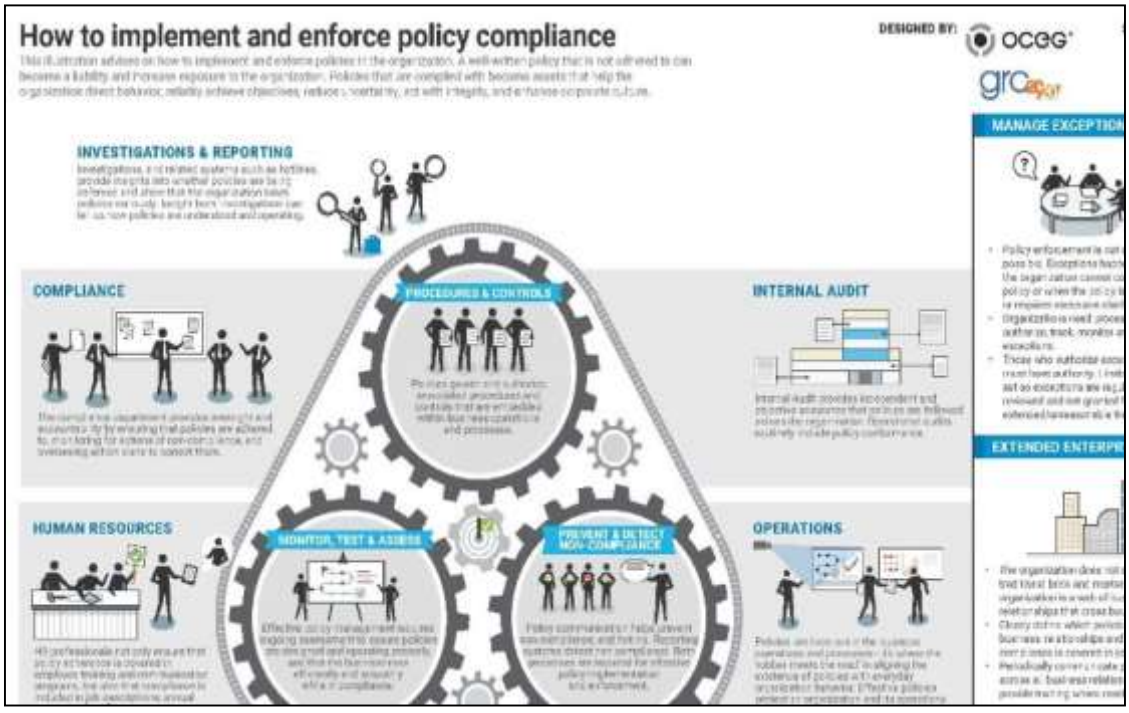


***Figure 1:*** *Implement and Enforce Policy Compliance(Source: Oceg, 2019)*

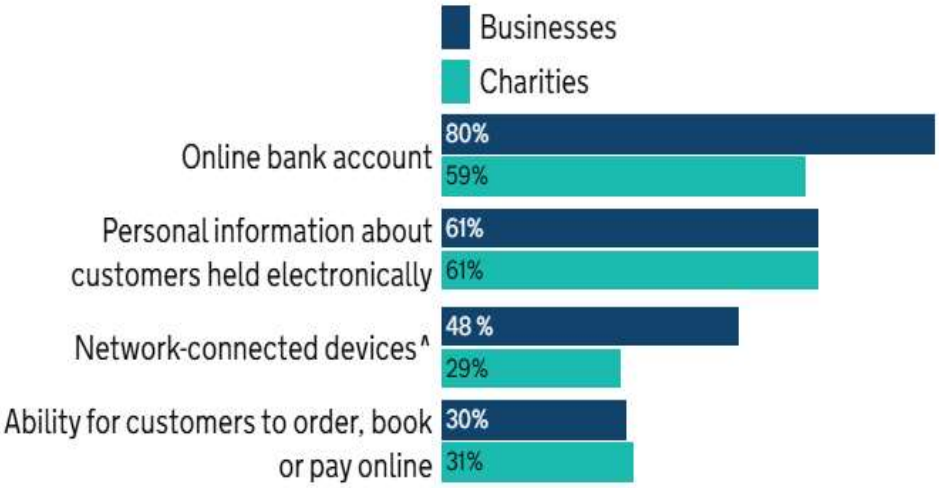


***Figure 2:*** *Percentage that currently have or use the following digital services of UK (Source: GOV.UK., 2022)*

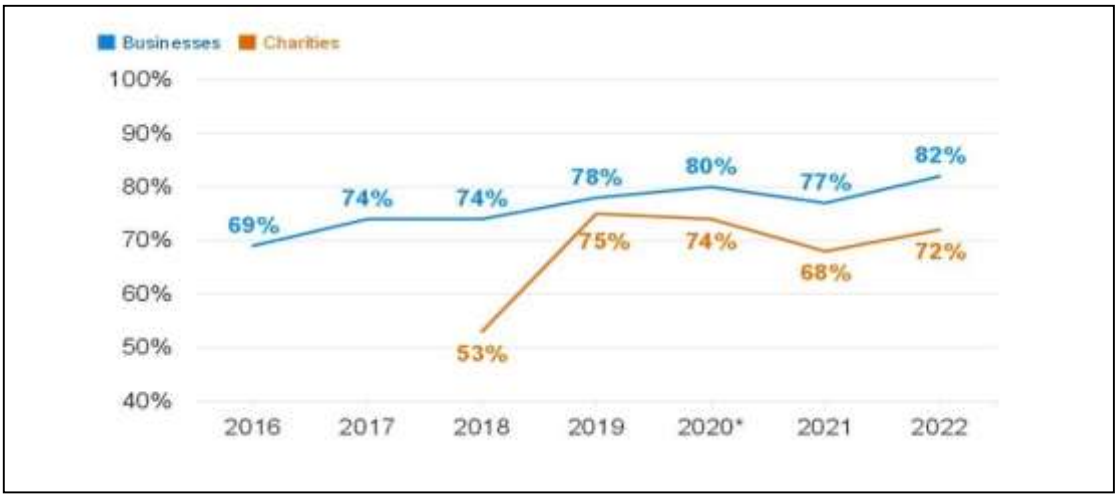


***Figure 3:*** *Percentage of organisations over time where cyber security is seen as a high priority for directors in UK (Source: GOV.UK., 2022)*




***Figure 4:*** *SOAR Capabilities in Cybersecurity (Source: HawkEye, 2020)*

USD 2.66 million per breach. Leadership support is also essential, as highlighted by CISA's playbooks for Incident Response, which call for accountability for leadership in reporting breaches in CIRCIA 2022 (Stevens *et al.*, 2022). Examples of HSBC Bank and JP Morgan Chase show how adaptive microlearning and behavioral analytics helped lower the susceptibility to phishing by more than 60% and built resilience into the daily work. The predictive modelling, which was validated by ENISA and NHS Digital gave high accuracy in identifying high-risk employees, allowing for targeted intervention, with a reduction in phishing vulnerability of more than 50%. When integrated into workflows, SOAR contributes to even greater efficiency, with Ponemon Institute (2023) finding that 40% of mean time to resolution can be saved by adding automation to workflows. There are legal frameworks like GDPR in Europe, Digital Personal Data Protection Act 2023 in India, and Cybersecurity Act 2018 in Singapore that require organizational support in order to be compliant, emphasizing the importance of structured support. In sum, these evidences together indicate that organizational drivers (training, leadership, predictive analytics, and automation) are not individual strategies, but a suite of strategies that puts cybersecurity on a path from a technical obligation to a cultural imperative for resilience, compliance and sustainable awareness (Mızrak, 2023).

## 6. Conclusions

It is concluded that organizational support is the basis of secure cybersecurity behavior supported by international legislation, institutional orders, and practical examples. Employee training, predictive modelling and behavioural analytics enable employees to avoid phishing and social engineering attacks and leadership support encourage accountability and proactive reporting of incidents. Structured interventions contribute to cost savings on breaches, resilience, and faster response to incidents, as per evidence from the IBM, ENISA, CISA, and NHS Digital. Despite these challenges, the integration of SOAR highlights the efficiency gained in operations: resolution time was cut by 40%, and automation has become a part of the organization's culture. In addition, there are legal frameworks like the GDPR, India's DPDPA 2023, and Singapore's Cybersecurity Act, which also reinforce compliance, helping organizations adhere to international standards. In the end, it's about making cybersecurity a culture of an organization that makes resilience a habit; compliance a continuous effort; and awareness an everyday part of life. By leveraging these drivers, businesses can not only mitigate vulnerabilities but also cultivate trust, sustainability, and long-term digital resilience.

## Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

## References

[1] Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108. https://dergipark.org.tr/en/pub/rjbm/issue/80308/1372698

[2] Stevens, R., Votipka, D., Dykstra, J., Tomlinson, F., Quartararo, E., Ahern, C., & Mazurek, M. L. (2022, April). How ready is your ready? assessing the usability of incident response playbook frameworks. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-18). https://dl.acm.org/doi/abs/10.1145/3491102.3517559

[3] Chisty, N. M. A., Baddam, P. R., & Amin, R. (2022). Strategic approaches to safeguarding the digital future: insights into next-generation cybersecurity. *Engineering international*, *10*(2), 69-84. Retrieved at https://pdfs.semanticscholar.org/1b58/6859a65c542ca2d501be4d0bf0768bca7ae0.pdf

[4] Dhankhar, K., & Singh, A. (2023, August). Employees' adoption of HR analytics–a theoretical framework based on career construction theory. In *Evidence-based HRM: A Global Forum for Empirical Scholarship* (Vol. 11, No. 3, pp. 395-

411). Emerald Publishing Limited. Retrieved at https://www.emerald.com/ebhrm/article/11/3/395/71155

[5] GOV.UK. (2022, March 30). *Cyber Security Breaches Survey 2022*. GOV.UK. Retrieved at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[6] HawkEye. (2020, May 11). *Automated Threat Response with SOAR - HawkEye*. HawkEye. Retrieved at https://hawk-eye.io/2020/05/automated-threat-response-with-soar/

[7] Lee, A. B. (2022). A Quantitative Research Study on Probability Risk Assessments in Critical Infrastructure and Homeland Security. Retrieved at https://digitalcommons.liberty.edu/doctoral/3865/

[8] Oceg (2019). *How to Implement and Enforce Policy Compliance*. [online] OCEG. Retrieved at https://www.oceg.org/how-to-implement-and-enforce-policy-compliance/

[9] Oluyisola, O. E., Bhalla, S., Sgarbossa, F., & Strandhagen, J. O. (2022). Designing and developing smart production planning and control systems in the industry 4.0 era: a methodology and case study. *Journal of Intelligent Manufacturing*, *33*(1), 311-332. Retrieved at https://link.springer.com/article/10.1007/S10845-021-01808-W

[10] Pinto, L., Brito, C., Marinho, V., & Pinto, P. (2022). Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks. *Journal of Internet Services and Information Security*, *12*(4), 23-38. Retrieved at https://jisis.org/wp-content/uploads/2022/12/I4.002.pdf

[11] Schaefer, D. (2023). Sigint and cyber power down under: Revealing Secrets: An Unofficial History of Australian Signals Intelligence and the Advent of Cyber, John Blaxland and Clare Birgin,(Sydney: Newsouth Publishing, 2023) 464pp, AUS $49.99 (Paperback), ISBN 9781742237947. *Intelligence and National Security*, *38*(7), 1208-1219. Retrieved at https://www.tandfonline.com/doi/abs/10.1080/02684527.2023.2219442

[12] Tran, B., Benson, K. C., & Jonassen, L. (2023). Integrating Certifications into the Cybersecurity College Curriculum: The Efficacy of Education with Certifications to Increase the Cybersecurity Workforce. *Journal of Cybersecurity Education, Research and Practice*, *2023*(2). Retrieved at https://eric.ed.gov/?id=EJ1415196

[13] Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*. https://www.tandfonline.com/doi/shareview/10.1080/08874417.2018.1432996

[14] Almeida, R. A. O. C. B. D. (2022). Heuristic phishing detection based on web crawling and user behaviour monitoring with a deterministic approach for cybersecurity. https://repositorio.ufsc.br/handle/123456789/234735

[15] Gaspar, J., Cruz, T., Lam, C. T., & Simões, P. (2023). Smart substation communications and cybersecurity: A comprehensive survey. *IEEE communications surveys & tutorials*, *25*(4), 2456-2493. https://ieeexplore.ieee.org/abstract/document/10217175/