BUSINESS PROCESS OUTSOURCING 14 CYBERSECURITY KPIS TOWARDS A STRATEGIC INFORMATION SECURITY

WARREN MARK M. SILVA, Ph.D.
http://orcid.org./0009-0002-8460-9501
wmsilva@gmail.com
Philippine Christian University
Manila, Philippines

DOI: https://doi.org/10.54476/ioer-imrj/027433

ABSTRACT

In an age where digital threats are escalating, the Business Process Outsourcing (BPO) sector is intensifying its focus on information security. This research delves into how BPO firms employ cybersecurity Key Performance Indicators (KPIs) among 14 identified measures to bolster their defenses. Employing a dual-method approach, it combines the depth of thematic analysis from interviews with the breadth of statistical evaluation from surveys. More so, it uncovers the key components of strategic security approaches within the BPO field, detailing how risks are assessed, defenses are implemented, staff is trained, incidents are managed, and regulations are met. The results offer actionable guidance for BPOs to fortify their security in a way that's congruent with their unique environment and goals. Additionally, this work enriches the body of knowledge on security management, underlining the essential role of cybersecurity KPIs in maintaining vigilant and effective security postures.

Keywords: cybersecurity, information security, KPI, business process outsourcing industry, information security management.

INTRODUCTION

In today's rapidly advancing technological landscape, ensuring the security of sensitive information has emerged as a paramount concern for businesses. The escalation of cyber threats necessitates organizations to fortify their defenses against unauthorized access, disclosure, and destruction of their vital data.

The Business Process Outsourcing (BPO) industry has witnessed exponential growth in recent decades, propelled by globalization and the escalating demand for cost-effective business solutions. However, this surge in demand has also underscored the criticality of information security within the BPO domain. BPO companies handle substantial volumes of sensitive data, encompassing personal information, financial records, and intellectual property. Consequently, they become lucrative targets for cybercriminals seeking to exploit vulnerabilities and gain illicit access to valuable data.

The intricacies of BPO operations present unique challenges to information security. The risk of

data breaches, cyber-attacks, and various security threats looms significantly, bearing potentially severe consequences for BPO companies, their clients, and their clientele. With the rapidly evolving threat landscape and the emergence of sophisticated attack vectors, BPO entities must remain vigilant and continually adapt their information security strategies. Cybercriminals employ intricate techniques such as social engineering, malware, ransomware, and advanced persistent threats (APTs) to infiltrate organizational systems and exploit vulnerabilities. To counteract these threats, BPO companies must proactively identify and implement robust security measures to protect their infrastructure, data, and reputation.

Maintaining a robust information security posture is not only vital for safeguarding client data but also indispensable for the overall sustainability and growth of BPO firms. Clients entrust their confidential information to BPO service providers with the expectation that it will be handled securely and confidentially. A breach in data security can result in severe financial repercussions, reputation damage, and legal liabilities. For instance, a data breach in a BPO company tasked with credit card processing for a major retailer can lead to significant financial losses, reputational damage, and legal entanglements. A survey of BPO providers revealed that 78% of respondents reported experiencing a security breach in the previous year, with an average cost of $1.2 million per breach (Ponemon Institute, 2020).

Given the criticality of information security in the BPO industry, the development of a strategic plan becomes imperative. A strategic development plan offers a roadmap for BPO companies to align their information security objectives with their overall business goals. It delineates the requisite policies, procedures, technologies, and resources necessary to mitigate information security risks effectively.

However, formulating and executing a strategic development plan in the BPO industry poses considerable challenges. BPO companies must meticulously assess their specific information security needs and ascertain the most effective strategies to address them. Factors such as risk assessment, regulatory compliance, incident response, employee awareness, vendor management, and ongoing monitoring and evaluation of security measures must be taken into account.

Employee training programs in information security are identified as a critical aspect, as employees are considered a significant threat to information security within a business (Experian, 2016). Comprehensive cybersecurity programs covering fundamental information security practices, advanced topics like threat detection and incident response, and best practices for password management, email security, and data handling are deemed essential for BPO companies.

This research endeavors to make a substantial contribution by developing a comprehensive strategic development plan for information security in the BPO industry. It aims to identify the pivotal information security challenges BPO companies face and explore effective strategies to mitigate these risks. Additionally, the research aims to establish a set of cybersecurity Key Performance Indicators (KPIs) that can be leveraged to track and monitor the progress and efficacy of the strategic development plan. These 14 metrics serve as strategic signposts, encompassing various dimensions of cybersecurity readiness, response, and risk mitigation. From assessing preparedness and detecting unidentified network devices to measuring response times and evaluating vendor security, each KPI offers a crucial lens into an organization's resilience against evolving threats. This suite of metrics empowers stakeholders to make informed decisions, prioritize resources, and

drive continual improvements in cybersecurity practices:

1. Level of Preparedness: Proactive measures to anticipate and address threats.
2. Unidentified Devices in Internal Networks: Monitoring and addressing potential security risks.
3. Intrusion Attempts: Detecting and responding to unauthorized access activities.
4. Security Incidents: Events compromising system integrity or data confidentiality.
5. Mean Time to Detect (MTTD): Average time to identify security incidents.
6. Mean Time to Resolve (MTTR): Average time to resolve security incidents.
7. Mean Time to Contain (MTTC): Average time to limit the impact of incidents.
8. First Party Security Ratings: Evaluating an organization's internal security posture.
9. Average Vendor Security Rating: Assessing third-party vendor security practices.
10. Patching Cadence: Frequency of software updates to address vulnerabilities.
11. Access Management: Controlling user access to mitigate unauthorized entry.
12. Company vs Peer Performance: Benchmarking cybersecurity strategies against industry peers.
13. Vendor Patching Cadence: Evaluating third-party vendor update timeliness.
14. Mean Time For Vendors Incident Response: Assessing vendor incident resolution efficiency.

The findings of this research will furnish BPO companies, decision-makers, and researchers with invaluable insights to enhance industry information security procedures and decrease the likelihood of security breaches.

OBJECTIVES OF THE STUDY

The objectives of this study are to assess the current landscape of Information Security practices, policies, systems, and procedures within BPO organizations, identify areas for improvement, and ultimately develop a comprehensive Information Security development plan and handbook tailored to their needs.

1. Identify existing Information Security practices, policies, systems, procedures, and programs within the BPO organizations covered by the research.

2. Identify the presence or absence of Information Security practices, policies, systems, procedures, and programs within the BPO organizations covered by the research.

3. Identify and recommend non-existing Information Security practices, policies, systems, procedures, or programs, that should be adopted by the BPO organizations.

4. Formulate a comprehensive Information Security development plan and handbook.

METHODOLOGY

A mixed-methods strategy is used in the study, integrating qualitative and quantitative techniques. This approach allows for a comprehensive exploration of the research objectives, capturing both the depth and breadth of the information security landscape in the BPO sector.

The qualitative component involves thematic analysis of key informant interviews, while the quantitative component entails the analysis of Likert-scale questionnaires and numerical data.

Key informant interviews were conducted with cybersecurity subject matter experts and IT professionals within BPO organizations to obtain in-depth insights and expert opinions on cybersecurity practices.

Table 1
Likert Scale and Response Interpretation (Degree of Agreement)

Rating Scale	Degree of Agreement
5	Strongly Agree
4	Agree
3	Neither Agree nor Disagree
2	Disagree
1	Strongly Disagree

Likert-scale questionnaires were administered to participants to measure their perceptions regarding specific cybersecurity key performance indicators (KPIs).

Table 2
Weighted Mean and Degree of Agreement

Rate	Range	Degree of Agreement
5	4.20 - 5.00	Strongly Agree
4	3.40 - 4.19	Agree
3	2.60 - 3.39	Neither Agree nor Disagree
2	1.80 - 2.59	Disagree
1	1.00 - 1.79	Strongly Disagree

The following table shows the rating of numerical weight assigned to the corresponding value of measurements.

RESULTS AND DISCUSSION

In the landscape of the Business Process Outsourcing (BPO) industry, strategic development plans in information security are significant. These plans involve the formulation and execution of long-term strategies aimed at safeguarding an organization's invaluable information assets from an array of potential threats (Safa, Von Solms, & Futcher, 2016). These threats encompass a broad spectrum, ranging from cyber-attacks and data breaches to internal vulnerabilities arising from human behaviors (Ulsamer et al., 2021).

Amidst this intricate landscape, cybersecurity Key Performance Indicators (KPIs) emerge as vital tools. These metrics serve multifaceted purposes:

Assessment of Security Posture. KPIs enable organizations to measure incident response times, patching rates, and vulnerability remediation, providing insights into strengths and weaknesses (Accenture, 2019).

Compliance Demonstration. KPIs aligned with regulatory guidelines showcase adherence to standards like PCI DSS, bolstering organizational credibility (PCI DSS, 2021).

Incident Response Evaluation: Metrics like the mean time to detect and respond aid in evaluating incident response capabilities, and minimizing impact (Ponemon Institute, 2018).

Accountability and Decision-Making Support. Establishing KPIs reinforces accountability and facilitates informed decisions based on incident trends and audit findings (Gartner, 2019).

The outlined 14 cybersecurity KPIs encompass critical areas like incident response, access management, and vendor security ratings. These metrics provide a comprehensive framework for tracking and evaluating security measures, ensuring proactive risk mitigation and continuous improvement.

The assessment of Key Performance Indicators (KPIs) pertaining to information security practices within the organization revealed a nuanced landscape. Across various domains such as vendor security, patching cadence, access management, and comparison with peer performance, there exist areas of strength and notable weaknesses.

1. The organization's current information security practices contribute to the overall security posture

Table 3
Identified existing KPIs

KPI	Mean	Interpretation
Access Management	3.45	Agree
Level Of Preparedness	3.06	Neither Agree or Disagree
Unidentified Devices in Internal Networks	3.17	Neither Agree or Disagree
Intrusion Attempts	3.03	Neither Agree or Disagree
Security Incidents	2.96	Neither Agree or Disagree
First Party security ratings	3.22	Neither Agree or Disagree
General Weighted Mean	**3.15**	**Neither Agree or Disagree**

Based on the general weighted mean of 3.15, the overall interpretation organization's existing security practices is “Neither Agree or Disagree“. This indicates that there is room for improvement in various areas as indicated by KPIs.

The organization's performance in managing access to its systems and resources is considered satisfactory and meets the agreed-upon standards. Hence, the others need to be further assessed, identify areas that need attention, and implement more measures to enhance security posture.

2. Extent of the presence or absence of Information Security practices, policies, systems, procedures, and programs within BPO organizations

The overall weighted mean of 2.55 suggests a general disagreement when considering all the 14 KPIs collectively. It indicates that the organization is falling short in terms of its information security strategies.

This finding highlights the need for improvement in various aspects of the concern that require attention and remediation. It is beneficial for the organization to conduct a detailed analysis of the individual KPIs to identify specific weaknesses and develop an information security strategy.

Addressing the specific areas of disagreement identified by the KPIs, organizations can work towards improving their cybersecurity posture, enhancing incident detection and response capabilities, and reducing potential vulnerabilities. Regular monitoring and reassessment of these KPIs can help track progress over time and ensure that the organization is moving towards a more secure and resilient state.

Table 4
14 KPIs overall weighted mean

KPI	Mean	Interpretation
Level Of Preparedness	3.06	Neither Agree or Disagree
Unidentified Devices in Internal Networks	3.17	Neither Agree or Disagree
Intrusion Attempts	3.03	Neither Agree or Disagree
Security Incidents	2.96	Neither Agree or Disagree
Mean time to Detect	2.47	Disagree
Mean time to Resolve	2.48	Disagree
Mean time to Contain	2.43	Disagree
First Party security ratings	3.22	Neither Agree or Disagree
Average Vendor Security Rating	1.21	Strongly Disagree
Patching Cadence	2.41	Disagree
Access Management	3.45	Agree
Company vs Peer performance	1.57	Strongly Disagree
Vendor Patching Cadence	1.87	Disagree
Mean Time for Vendors Incident Response	2.31	Disagree
Overall Weighted Mean	**2.55**	**Disagree**

3. Implementation strategies and considerations should be taken into account when adopting these non-existing information security measures within BPO organizations

Table 5
Non-existing KPIs weighted mean

KPI	Mean	Interpretation
Mean time to Detect	2.47	Disagree
Mean time to Resolve	2.48	Disagree
Mean time to Contain	2.43	Disagree
Average Vendor Security Rating	1.21	Strongly Disagree
Patching Cadence	2.41	Disagree
Company vs Peer performance	1.57	Strongly Disagree
Vendor Patching Cadence	1.87	Disagree
Mean Time for Vendors Incident Response	2.31	Disagree
General Weighted Mean	**2.09**	**Disagree**

Across various KPIs, the mean scores fall below expected or desired levels, leading to the overall conclusion of "Disagree" in the general weighted mean of 2.09. The organization must take these findings seriously and prioritize improving its security measures, incident response times, vendor security ratings, and patching processes.

Addressing these issues will help the organization enhance its security posture and better protect itself against potential threats and risks. Regular monitoring, proactive measures, and continuous improvement efforts will be crucial to closing the performance gaps and achieving a more secure environment.

5. Comprehensive Information Security plan should an organization consider to strengthen its security posture

The comprehensive Information Security Development Plan and Handbook aims to strengthen the organization's security posture by addressing various aspects of information security. The plan is divided into several sections, each focusing on specific areas of improvement. Here are the key findings and action items from each section:

Introduction. The introduction communicates the importance of information security as a shared responsibility throughout the organization. The objectives and scope of the plan are defined to guide the development and implementation process.

Overview of Information Security. The section emphasizes the importance of information security in protecting sensitive data and outlines key principles such as confidentiality, integrity, availability, and user awareness.

Current State Assessment. The organization should conduct a comprehensive risk assessment, gap analysis, vulnerability assessment, and incident and breach analysis to identify potential threats, vulnerabilities, and risks. Involving key stakeholders from various departments ensures a comprehensive understanding of security posture.

Information Security Policy and Governance. The plan recommends developing a comprehensive set of policies and procedures covering various aspects of information security. Roles and responsibilities should be clearly defined, and compliance with regulatory requirements should be ensured.

Information Security Controls. The plan emphasizes implementing strong access controls, network, and perimeter security, data protection measures, incident response, and management. Vendor and third-party risk management are also critical.

Security Incident Response Plan. The organization should establish an incident response team structure, detailed procedures, and workflows for handling security incidents. Regular testing and post-incident analysis are essential for continuous improvement.

Security Awareness and Training. Developing a comprehensive security awareness program tailored to the specific needs and roles of different employee groups is essential. Regular phishing simulations and social engineering tests reinforce good security practices.

Security Monitoring and Auditing. Implementing a centralized log management system, intrusion detection and prevention systems, and conducting regular security audits and compliance assessments are essential for proactive security monitoring.

Continuous Improvement and Performance Measurement. Defining Key Performance Indicators (KPIs) and metrics to measure the effectiveness of security controls, incident response, and training programs is crucial. Regularly assessing the organization's security posture using KPIs and sharing lessons learned are essential for continuous improvement.

Documentation and Policy Templates. Developing comprehensive policy templates, incident response plan templates, security awareness program templates, and standardized security incident report templates ensures consistency and effective implementation.

By implementing the action items outlined in the plan, the organization can significantly enhance its information security practices, minimize vulnerabilities, and improve incident response capabilities. Regular monitoring and continuous improvement efforts will ensure the organization maintains a strong and resilient security posture over time.

CONCLUSION

The evaluation of the organization's information security practices identifies strengths in Access Management policies but also emphasizes the need for regular access control assessments. Level of Preparedness calls for refining security policies, bolstering training, and improving incident response strategies, underlining the significance of routine security control updates. Unidentified devices within internal networks require frequent updates and comprehensive scans, advocating for automated device management tools and robust access controls. Intrusion Attempts and Security Incidents highlight the necessity for enhanced intrusion detection, incident response procedures, and collaborative efforts with security experts. The organization's security rating and vendor management practices indicate potential enhancements through improved data protection, risk assessment, compliance, and incident response strategies. A comprehensive Information Security Development Plan and Handbook are proposed to effectively address these areas, encompassing aspects like access management, policy development, incident response, training, and continuous improvement. By embracing a proactive and continuously improving stance on information security, the organization can uphold industry standards, cultivate stakeholder trust, and fortify its systems, data, and reputation against evolving threats in the digital landscape, ensuring long-term resilience and success.

RECOMMENDATION

The following recommendations are provided to further enhance the organization's cybersecurity posture:

1. Strengthen the Identification and Mitigation of Unidentified Devices. Implement robust network access controls and regular device scanning to identify and address unidentified devices. Enhance network visibility.
2. Enhance Intrusion Detection and Prevention. Investigate and deploy advanced intrusion detection and prevention systems to proactively identify and prevent intrusion attempts.
3. Enhance Incident Response Capability. Establish an incident response team, define clear incident response procedures, and conduct regular incident response drills and

simulations. Ensure that incident response plans are regularly updated to address emerging threats and vulnerabilities.

4. Improve Mean Time to Detect and Resolve. Implement advanced security monitoring and detection mechanisms to reduce the mean time to detect security incidents. Enhance incident response processes, collaboration, and automation to expedite the meantime to resolve security incidents, minimizing the potential impact on business operations.
5. Enhance Patch Management Practices. Implement a robust patch management process that includes regular vulnerability and risk assessments, prioritization of critical patches, and timely deployment across all systems and applications.
6. Strengthen Access Management. Continuous review and enhance access management practices by implementing strong authentication mechanisms, role-based access controls, and regular access reviews.
7. Foster a Culture of Security Awareness. Invest in ongoing security awareness and training programs to educate employees about cybersecurity risks and best practices. Regularly communicate security policies, conduct phishing simulations and IT campaigns.
8. Foster Vendor Relationships. Regularly audit and evaluate vendor security ratings and assess their incident response capabilities. Closed collaboration with vendors to ensure they adhere to strong security practices.
9. Benchmark Against Industry Standards. Regular benchmarking organization's cybersecurity performance against industry standards, best practices, and peer organizations.
10. Continuously Monitor and Evaluate. Establish a robust cybersecurity monitoring and evaluation to continuously assess the organization's cybersecurity posture. Implement security metrics and use 14 key performance indicators, regularly track and report on them, and use the insights gained to drive continuous improvement.

REFERENCES

Accenture. (2019). Securing the digital economy: Reinventing the internet for trust. https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Reinventing-Internet-for-Trust.pdf

Experian. (2016). Third annual 2016 data breach industry forecast. Experian Data Breach Resolution. http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf

Furnell, S., Papadaki, M., & Dowland, P. (2006). Organizational culture and information security: An assessment of theory and current practice. Information Management & Computer Security, 14(2), 86-96.

Gartner. (2019). Metrics for Cybersecurity Investment. https://www.gartner.com/en/documents/3980977/metrics-for-cybersecurity-investment

Harbert, T. (2021, October 25). The weakest link in cybersecurity. SHRM. https://www.shrm.org/hr-today/news/all-things-work/pages/the-weakest-link-in-cybersecurity.aspx

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.

ISACA. (n.d.). https://www.isaca.org/resources/cobit

ISO/IEC 27001 Standard – Information Security Management Systems. (n.d.). https://www.iso.org/standard/27001

Kim, D., & Solomon, M. G. (2018). Fundamentals of information systems security (3rd ed.). Jones & Bartlett Learning.

Nathan, A. (2021, November 4). What is cybersecurity metrics & 14 Cybersecurity Metrics KPIs to Track. The Tech Trend. https://the-tech-

trend.com/security/what-is-cybersecurity-metrics-14-cybersecurity-metrics-kpis-to-track/

National Institute of Standards and Technology (NIST). (2012). Computer Security Incident Handling Guide (NIST SP 800-61).

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework

Ofori, K., Anyigba, H., Ampong, A., Omoregie, O., Nyamadi, M., & Fianu, E. (2022). Factors influencing information security policy compliance behavior. In Handbook of Research on Security Considerations in Cloud Computing (pp. 211-225). IGI Global.

Payment Card Industry Security Standards Council. (2021). PCI DSS. https://www.pcisecuritystandards.org/pci-security-standards/pci-dss

Ponemon Institute. (2018). Cost of Cyber Crime Study. https://www.accenture.com/us-en/insights/security/cost-of-cyber-crime-study

Ponemon Institute. (2020). 2020 Cost of a Data Breach Study: Global Analysis. https://www.ibm.com/security/data-breach

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. Computer Fraud & Security, 2016(2), 15-18.

Shayan, A., Soheili, K., & Abdi, B. (2009). Human excellence in information security: A complexity theory perspective. In Proceedings of the International Symposium on Human Aspects of Information Security and Assurance (pp. 32-41).

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41. https://doi.org/10.1108/09685220010371394

Sulabo, K., Serrano, M., Balarbar, A., & Macaraeg, P. (2016). Cyber crime effects to businesses in Philippines. https://doi.org/10.13140/RG.2.2.16219.77607

Ulsamer, P., Schütz, A., Fertig, T., & Keller, L. (2021). Immersive storytelling for information security awareness training in virtual reality. https://doi.org/10.24251/HICSS.2021.861

AUTHOR'S PROFILE

Engr. Warren Mark M. Silva, holder of multiple IT certifications with significant exposure in analysis, solution, service delivery, project management, vendor and facility management, and administration and support of systems and networks. Adept at interacting with clients, understanding their requisites, and accordingly developing solutions utilizing vast knowledge of technologies and tools. Actively maintains a working knowledge of information technology best practices, solution methodologies, and emerging technology trends as evidently through his continuous education in the field of IT. Completed both Masters in Business Administration and Doctor of Philosophy in Business Management Major in Strategic Management from Philippine Christian University, Manila, Philippines.

COPYRIGHTS