Human Factors in Cybersecurity, Vol. 168, 2025, 93–99
https://doi.org/10.54941/ahfe1006146

Next Generation Business Continuity Management Solution

Markus Sihvonen, Riku Lehkonen, and Arttu Takala

University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

The number of cyber incidents in industrial enterprises doubled from 2019 to 2020 and they have continued increasing in similar rate. At 2023, the global average cost of a single data breach was 4,45 million USD. Currently cyber threat detection solutions are monitoring critical systems and responds to odd incidents. Obviously, they are in reactive mode and are not dealing with core problem itself, just patching holes. In order to decrease number of attacks on critical infrastructures, threat detection systems must evolve to prevent such incidents. The research question of the paper is to define requirements for next generation BCM (Business Continuity Management) system. Future BCM systems must evolve beyond traditional disaster recovery to having a proactive, predictive, and threat data sharing capabilities. They must utilize advanced technologies, ensure regulatory compliance, and provide organizations with the tools to anticipate and prevent threats. Automated and comprehensive threat data collection solution is basic foundation for any threat prevention and analysis system. Internet of Things (IoT) technologies are to be utilized for massive amount of real-time data collection. Artificial intelligence (AI) is excellent tool for both massive amount of threat data analysis and collection. Blockchain technology should be used for secure and transparent distribution of threat data. This is critical since newly discovered weaknesses must be blocked quickly to prevent greater damage. Digital Twin solutions are excellent for simulating, further refining and optimizing organizations BCM strategies. Quantum computing can be seen as a significant risk for BCM solutions since modern cryptography relies on difficulty of solving certain mathematical problems, which are hard for classical computers but could be solved quickly by a quantum computer. Fortunately, quantum computing can also improve threat prevention solutions.

Keywords: Cyber-security, Business continuity management, Threat analysis, Threat prevention

INTRODUCTION

In today's dynamic business environment, organizations face a myriad of risks, including natural disasters, cyberattacks, pandemics, and supply chain disruptions. These events can threaten continuity of critical operations, making it imperative for businesses to establish robust BCM systems. BCM systems aims to minimize downtime, safeguard critical operations, and ensure swift recovery from unforeseen disruptions (Herbane, 2010). The objective of this paper is to define requirements for next generation BCM systems that must be capable of actively preventing cyber threats. Qualitative research method is used to analyse Finnish technology industry requirements to protect their critical systems that enable continuity of business operations in rapidly changing geopolitical environment.

The benefits of utilization of BCM systems sum up to substantial savings annually, and can be even paramount enabler for an organisation to continue its critical business operations. These systems offers' operational resilience, ensures minimal disruption to critical business functions during crises and it is aligned with industry standards and legal requirements. They enhance reputation and trustworthiness of an organization and demonstrates commitment to stakeholder security and operational reliability. They reduce risk of financial losses by mitigating risks and ensuring faster recovery in crises situations. In case of preventing cyber threats in nuclear energy systems, reducing risk exposure to the barest minimum in crucial (Zohuri, 2022).

The global cost of cybercrime alone is estimated to reach $10.5 trillion annually by the end 2025 according to Cybersecurity Ventures. Organizations face direct financial losses from due to successful cyber-attacks and Indirect costs include legal fees, regulatory fines, reputational damage, and loss of customer trust. Cyberattacks disrupt businesses' operations and therefore cause productivity losses. Attacks on critical infrastructure such as energy infrastructure, healthcare systems, and finance system can nationwide panic and loss of life. There are some known cases e.g. in Finland, that due to a severe cyber-attack SME (Small and Medium-sized Enterprises) has been forced shut down. Major problem is high economic incentives for cybercriminals with low risk of ever to face criminal charges. Therefore, cybercrime is highly profitable low risks business adventure, that encourage more hackers and criminal groups to operate.

Cybercriminals are fast to adopt very latest technologies to plan and execute cyber-attacks. They exploit software vulnerabilities before they are patched. AI is used to automate cyberattacks and may also be used by attackers to alter used malware quickly, thus altering their fingerprints to evade detection. Skilled cybercriminals sell ransomware tools to less-skilled attackers. They sell stolen data, hacking tools and services on marketplaces in dark web. Cryptocurrencies are used for completing business transactions. Today, there exists profitable business ecosystem that makes large profit on providing tools and services to execute cybercrimes (Akyazi, 2021).

THE MAIN COMPONENTS OF BCM SYSTEMS

The primary mission of any BCM (Business Continuity Management) system should be to guarantee critical business operations in unusual circumstances. It should provide information about threats and dangers (Abdukhalil, 2024). If it fails to deliver the safe and secure operational environment, then the system must provide solution to minimize damage and to restart critical operations as soon as possible. Therefore, any well implemented BCM system must include BIA (Business Impact Analysis), risk assessment of critical business functions, strategies to mitigate identified risks for critical operations, threats prevention plans, crisis management plans and training employees on their roles during disruptions to critical processes.

The BIA is the key component of any well-organized BCM system. It is the tool for any organisation for prioritizing their resources and recovery efforts during crises. Organization's risk management for critical systems are in important role in building its cyber resiliency (Assibi, 2023). A BIA's key objectives are to identify critical processes of an organisation, evaluate consequences of interruptions of the defined critical processes, including financial losses, reputational damage, legal implications, and possible operational setbacks. In worst case scenario when critical operations are halted, properly conducted BIA will provide recovery ranking of processes based on their urgency for the critical operations. It is a useful tool that identify dependencies of all functions of critical operations and helps to minimize financial losses, legal consequences and minimize damages for reputation. A comprehensive BIA also assess potential risks such as cyber threats, political risks and natural disasters. It will analyse potential impacts of identified threats and define critical operations and dependencies that need immediate recovery when operations are halted by any realised threat. It will also consider alternative solutions for failed processes and services. It is important to have thorough internal and external communication plan for any type of crisis situation in place. Finally, personnel must be familiar with disaster recovery plans and trained for dealing with situations where critical operations are halted.

Threat prevention capabilities are ever more important features of any BCM system. Any well implemented threat prevention solution includes threat identification, assessment, and mitigation planning features. In order to guarantee sufficient quality of the solution, it should be a compliance with relevant standards such as ISO 22301 for best practises for threat management. Currently, threat prevention is often planned to react on realised threats that were previously identified in BIA planning phase. Therefore, a proper threat prevention plan can handle natural disasters, cyber-attacks, technology failures, supply chain risks and insider risks once suspicious activities are detected. Instead detecting and identifying new threats prior to their realization and preventing their occurrence at first place is not practised usually by BCM systems.

ACTIVE THREAT PREVENTION

Traditionally, threat and risk prevention in BCM systems is preparing for known possible risks and when one of the known risks is realized, there is existing detailed plan to minimize damages. New approach is active threat prevention that focuses on finding potential new threats and preventing their possibilities to mature into harmful incidents. There are two required main components for true active threat prevention systems; a new threat data collection system, and a threat data analysis system. Properly designed and built active threat prevention system can discover any type of new threats for critical operations. Some of threats can not be prevented such as natural disasters, but a BCM system can be refined to mitigate consequences if the threats are discovered before actual disastrous events begin.

Information for identifying potential new threats can be collected from virtual and physical worlds. IoT (Internet of Things) networks are capable to collect vast amount of data from real world events, pre-proses it and store it for further analysis. Social media is a good source for collecting data on potential cyber threats such as new phishing campaigns and techniques that could be used for executing them. Social engineering can be targeted with help of AI for finding fake social profiles, impersonations, spoofed domains and possible correlation between them. Particular attention for AI solutions should be given for Dark Web monitoring such as breaching hacker forums and monitor underground market places when searching for potential new threat data. A secure network itself provides valuable data for threat analysis such traffic logs, end point logs, firewall alerts and application logs. This type of data is particular useful for AI for identifying insider threats and detecting anomalies specific to the particular organization. Decoy systems, honeypots, are particularly designed to lure attackers and collect data on their methods. These are helpful tools not just for collecting new threat information but also capturing new malware, discovering new attack vectors and identifying new cyber terrorist teams. Discovered threat information sharing is very effective way to protect whole society and industrial ecosystem from forthcoming potential disastrous events. Collaboration between organisations in threat information sharing enables quicker identification and mitigation of emerging threats. It also provides insights into broader global trends that might not be apparent to a single organisation executing threat information collection and analysis only based on its own specific requirements.

Once threat information is detected and collected from multiple sources, AI is the primary tool needed for analysing it in two main reasons; vast quantity of data and urgency in identifying new potential threats (Hussain, 2024). There are multiple key techniques that can be used for analysing collected potential threat information. Regardless of the used technique, detection of anomalies and clustering of threat patterns for malware classification based on their patterns and predictive analysis of attack likelihood must be accomplished (Walls, 2023). Also, identification on deviations from normal activities or behaviour in web or in a secure network should be discovered. Target is to discover unusual patterns, detects recurring TTPs (Tactics, Techniques and Procedures) and correlate them with known threat actors. This is particularly useful for identifying phishing domains created with similar naming patterns. Hypothesis-driven investigation can be used to proactively discover hidden threats with in the target environment. Forensic Analysis provides new threat data by investigating past incidents to uncover root causes and attacking methods. Instead of waiting for automated new cyber threat discovery systems to generate alerts, the threat prevention systems should actively execute analysis of unusual patterns, activities and signs of forthcoming cyber threats. It should collect potential threat information from multiple sources such as dark web, hacker forums and social media platforms. The most important is to have as much information available as possible since with lager data bank AI can better detect patterns that indicate potential new threats.

A digital twin is a virtual replica of a system, network, or physical asset that can provide help for cyber threat prediction and prevention. It ensures continuous verification of target system by mirroring real-time system behaviour. A digital twin is particularly useful for identifying vulnerabilities of a target system and therefore it is excellent tool optimizing cyber defence strategies. This is done by simulating cyber-attacks in virtual environment and various threat scenarios based on discovered new threat information and knowledge of previously executed cyber-attacks. Also, continuous execution of the virtual replica with real network's data traffic can be used for early detection of reconnaissance phase of activated cyber-attack. After discovering new cyber threat, a digital twin of the protected target system can be used to identify the best countermeasures for specific threats without disrupting operational system. In post cyber-attack analysis, a digital twin provides crucial support for forensic analysis and in determining root cause of the attack.

Blockchain technology, with its decentralized, immutable, and transparent nature, significantly enhances security by safeguarding the integrity and privacy of transactions in critical systems. Every transaction is recorded on a tamper-proof distributed ledger, making it nearly impossible for unauthorized users to alter or delete data. This transparency ensures that all transactions remain auditable, fostering trust and accountability within the organization's critical ecosystem. When integrated with AI, Blockchain not only strengthens data security but also establishes a reliable foundation for AI-driven threat detection, making it more resilient to manipulation (Abbas, 2024).

BUSINESS CONTINUITY MANAGEMENT SYSTEM'S CHALLENGES

Effective threat management within a BCM systems faces several challenges. Correctly identifying emerging new cyber threat is challenging due to rapid technological advancements employed by attackers. Economic instability and geopolitical risks create unpredictable disruptions for business operations that extremely difficult to be forecasted and prepared. It is evident that climate change increases a frequency and severity of natural disasters globally. Traditional risk assessment methods may not fully account for cascading effects.

Businesses increasing reliance on digital infrastructure makes them more vulnerable to cyber threats. Common cyber threats such as phishing, insider threats, and supply chain attacks are difficult to prevent. BCM systems must align with international standards such as ISO 22301, NIST and GDPR. Frequent changes in regulations require continuous updates to threat management plans since non-compliance can lead to legal penalties (ISO 22301, 2019). Employees may unintentionally cause security breaches or business disruptions. Insider threats, whether malicious or accidental, are difficult prevent on traditional tools. Many businesses depend on external vendors, which can go as deep as 5 tiers or more increase organizations' exposure to their vulnerabilities. Therefore, lack of visibility into suppliers' BCM systems can create weak points in threat management. This is also true if it is not integrated into IT disaster recovery, incident management, and cybersecurity management framework in the organisation. Finally, simulated exercises should be organized periodically to guarantee BCM systems required operational level, pinpoint potential new development topics to the system, and maintain personnel's proficiency for the real incident case (Lindström, 2009).

CONCLUSION

Business Continuity Management Systems are integral to safeguarding organizations against disruptions and ensuring long-term viability. Systematically identifying risks, planning responses, and fostering a culture of resilience, BCM systems enables businesses to navigate crises effectively. As the risk landscape evolves, continuous investment in and refinement of BCM systems will remain crucial for organizational success.

The requirements for truly secure BCM systems are comprehensive. It must meet challenges of rapid technology development, geopolitical uncertainties and forward moving climate change. The BCM systems must have proactive threat prevention capabilities. Therefore, it must actively seek new yet to be discovered cyber threats, threats caused by new emerging technologies, analyse potential changes in geopolitical environment and estimate risks to business operations caused by changes to the environment. This goal is achievable by collecting and analysing multimodal information with latest AI solutions and LLMs. When new threat is discovered, whether it is virtual world or physical world risk, it's potential damage to the business operations should be estimates, prevented and at least minimized. Digital twin replica of the critical business operation can be used to test effects of new discovered threat to determine it's potential to cause interruption to the business operations and to discover means to prevent the threat. The successful BCM systems must also consider human risks. Personnel requires periodically training in order to promote situational (Pöyhönen, 2024) and threat awareness within the organisation. Security culture of an organisation should also be communicated external vendors and potential threats they impose to the organisation should be analysed and included to the risk management plan. Finally, every BCM systems must a comply local regulations and standards.

REFERENCES

Abbas, Ghulam & David, Jameson. (2024). Artificial Intelligence and Blockchain: A Combined Approach for Predicting and Preventing Cyber Attacks in Financial Institutions. 10.13140/RG.2.2.18601.40808.

Abdukhalil, Ganiyev & Dostonbek, Tojimatov. (2024). Cyber Intelligence Practice in Preventing Cyber Threats and its Priorities. Journal of Contemporary Business Law & Technology: Cyber Law, Blockchain, and Legal Innovations. 1. 31–36. 10.61796/ejcblt.v1i6.653.

Akyazi, U., van Eeten, M. J. G., & Hernandez Ganan, C. (2021). Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum. Paper presented at Workshop on the Economics of Information Security.

Assibi, Awini. (2023). Literature Review on Building Cyber Resilience Capabilities to Counter Future Cyber Threats: The Role of Enterprise Risk Management (ERM) and Business Continuity (BC) Awini Thomas Assibi College of Business, Westcliff University, Irvine, CA, USA. Open Access Library Journal. Vol. 10, No. 4, April 2023. 10.4236/oalib.1109882.

Herbane, Brahim. (2010). The Evolution of Business Continuity Management: A Historical Review of Practices and Drivers. Business History. 52. 978–1002. 10.1080/00076791.2010.511185.

Hussain, Tahir & Daniel, Thomas. (2024). Predictive Cybersecurity for Financial Institutions: How AI and Blockchain Combat Threats and Vulnerabilities. 10.13140/RG.2.2.29506.59848.

ISO 22301:2019. International Organization for Standardization. (2019). Security and resilience — Business continuity management systems — Requirements.

Lindström J., Hägerfors A. (2009). A model for explaining strategic IT-and information security to senior management. International Journal of Public Information Systems. 1.

Pöyhönen, Jouni & Lehto, Martti. (2024). Architecture Framework for Cyber Security Management. European Conference on Cyber Warfare and Security. 23. 388–397. 10.34190/eccws.23.1.2340.

Walls A., McMullen L., Heiser J., Gopal D. Risk Management Produces Bad Cybersecurity, Maverick Research, 2023.

Zohuri, Bahman & Agarwal, Akansha & Kumar, Dinesh & Moghaddam, Masoud. (2022). Cost-Effectively Detecting, Preventing and Mitigating Cyber Threats to Nuclear Energy Systems. 3. 1–3.