Business Continuity and Disaster Recovery Strategies (BCRS) as Resilience Tools after Cyberattacks in Entrepreneurship Ecosystems: How ready is Peaceful East Asia?

Lukman Raimi
Assistant Professor of Entrepreneurship, Universiti Brunei Darussalam,
Brunei Darussalam

Synopsis

- To share valuable insights into the emerging phenomenon of cyberattacks and their future impact on entrepreneurship ecosystems in ASEAN.
- To sensitise ASEAN policymakers, entrepreneurs, and corporate organisations to business continuity and disaster recovery strategies (BCRS) as cybersecurity resilience tools.
- To provide key policy prescriptions for cybersecurity resilience and readiness in ASEAN.

Introduction

ASEAN was the focus of the workshop. ASEAN is the Association of Southeast Asian Nations. It is a regional body with ten member countries: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. ASEAN countries have a total population of over 662 million and an aggregated GDP of $3.2 trillion (over 34% of the world's GDP). ASEAN has large reservoirs of resources, land areas, consumer bases, business owners, farmers, employees, and entrepreneurs. ASEAN is predicted to emerge as the world's fourth-largest economy by 2030 (Council on Foreign Relations, 2022).

Catalysts for ASEAN's Growing Economy

The following catalysts that precipitate the growth of ASEAN need to be protected and deepened to ensure regional security, sustainable economic integration and inclusive economic growth (Syahwier, 2018; Kamil, Pratama, and Arief, 2019).

- Large market
- Investment in knowledge skills and abilities (KSA)Free trade areas
- Intra-ASEAN trade and investments
- Foreign direct investment
- Growth of micro, small and medium-sized enterprises (MSMEs) /entrepreneurship – tourism,
- Access to disruptive technology and adoption, and
- Education, training, and digital talent development.

Benefits of Disruptive Technologies for ASEAN

In emerging ASEAN digital economies, the utilisation of disruptive technologies would improve and enhance business activities and operations in business landscapes. The extant

literature (Abdallah, Phan and Matsui, 2016; Exposito and Sanchis-Llopis, 2018) affirmed that disruptive technologies provide the following benefits:

- Technical and economic performance of enterprises
- Employee productivity,
- Service delivery efficiency,
- Customer experience and satisfaction,
- Business and operations risk mitigation,
- Capacity for detection of human errors,
- Precision in the use of human, financial and material resources.

Potential Threats to ASEAN's Growing Economy

Cyberattacks, cyberterrorism, and cybercrime are real threats in a digital society. If unchecked, these threats would negatively affect entrepreneurialism, reduce control over information technology (IT) infrastructure, and create toxic business landscapes. How ready is East Asia, particularly ASEAN, peaceful?

- In the US, Ukraine, and other countries, cyberattacks have led to business disruptions, data theft, financial losses, bankruptcy, and threats to entrepreneurialism.
- Emerging threats and risks to economic activities, entrepreneurs, and corporate organisations necessitate cybersecurity resilience and preventive measures.

Defining Cyberattacks, Types, and Cases

A cyberattack is an attempt to disable computer systems, steal valuable business data through identity theft, breach of access, password sniffing, system infiltration, instant messaging abuse, website defacement, or use a breached computer system to launch attacks on business organisations (Unisys, 2022). In addition, cyberattacks have been defined as criminally motivated attackers to steal, expose, alter, disable, or destroy the information of individuals, organisations, and nations through unauthorised access to computer systems and IT infrastructural facilities to secure financial gain and enjoy unfair advantage over competitors, revenge by disgruntled current or former employees, and attention-seeking by hacktivists (IBM, 2022).

Furthermore, as cybersecurity experts, IBM (2022) and Unisys (2022) identified the following as the prevalent types of cyberattacks on businesses.

a) Malware attack: An attack that breaches a network when users click on links or email attachments that trigger attacks and instal malicious software, such as spyware, ransomware, viruses, and worms.
b) Phishing attack: This occurs by sending fraudulent communications via email to steal, compromise, and access sensitive data, such as credit card information and login details, on computer systems and IT infrastructure.
c) Man-in-the-middle attack: An attack that occurs when cyber attackers plant themselves in the middle of two parties involved in transactional relationships to interrupt, filter, and steal data in traffic.
d) Denial-of-service attack: Cyber attackers use multiple devices to fill computer systems and networks with heavy traffic that exhausts resources and bandwidth to deny their victims access to service and the capability to fulfil legitimate business requests.

e) Structured Query Language (SQL) injection: A cyberattack that occurs when a malicious code is inserted into a server with SQL, which forces the server to disclose confidential information and private data that have been kept secret.
f) Zero-day exploit: A cyberattack launched quickly at an organisation that announces a network vulnerability at a point in time before a connectivity solution is restored.
g) Domain Name System (DNS) tunnelling: A cyberattack that deliberately exploits the DNS protocol by disguising real DNS with evil intention to ex-filtrate data to the attacker's infrastructure to compromise the system of the victim.

Cases of Cyberattacks

This paper explains three important cyberattack cases to serve as eye-openers for entrepreneurs, corporate organisations, and policymakers in the ASEAN region. The emerging ASEAN should be alert if powerful nations and Fortune 500 companies are attacked.

1. Cyberattacks in Ukraine's capital city, Kiev, caused a six-hour blackout. The attack on the national power grid brought business operations to a sudden halt and inflicted serious hardship on hundreds of thousands of customers in Kiev (Sullivan and Kamensky, 2017).
2. From Dubai, fraudsters launched a business email compromise (BEC). BEC schemes involve hacking computer systems, gaining unauthorised access to a business's email account, and blocking or redirecting electronic communications. The aim was to exploit the international financial system (US Department of Justice, 2020).
3. In the US, cyberattacks have compromised the supply chain of SolarWinds, an Austin-based IT management company. The attack injected malware into Orion's updates that breached the data of most Fortune 500 organisations, including the US military and several US-based federal agencies responsible for nuclear weapons and management of critical infrastructure services (Imperva, 2021).

Implications for Business Ecosystems and Entrepreneurialism

Businesses and countries that experience cyberattacks and cybercrime suffer business disruptions, loss of customers, financial losses, reputational damage, bankruptcy, and threats to national security. This is a threat to intra-national business relations and interregional trade relations because of the theft of large-scale data breaches and the high incidence of e-fraud. The possible financial implications of cyberattacks include the following.

1. The International Data Corporation (IDC) reported that, on average, an infrastructure failure due to cyberattacks costs USD 100,000 an hour, while a critical application failure from cyberspace attacks can cost USD 500,000 to USD 1 million per hour (IBM Services, 2020).
2. The United States Federal Bureau of Investigation (FBI) reported that there are more than 4,000 daily ransomware attacks on different organisations (Chang and Ho, 2006), and more than 330,000 dangerous malware applications are created daily by cybercriminals (Hasan et al., 2021).

Readiness for Cybersecurity Adoption

Cybersecurity is also the deployment of people, processes, and technology to protect an organisation's IT-related assets, network installations, databases, and computer systems

from planned digital attacks with the intent of accessing, destroying, or changing sensitive information, and ultimately halting business operations (Cashell et al., 2004; Hasan et al., 2021). How? What are the potential strategies?

Business Continuity and Disaster Recovery Strategies (BCRS)

Scholars and professionals recommend the following strategies to forestall, prevent, and mitigate cyberattacks in entrepreneurship ecosystems:

1. **Readiness assessment strategy:** A planned and thorough diagnostic assessment of the capability and risk readiness to recover IT operations as quickly as possible after disruptive events.
2. **Risk management strategy (RMS):** The risk control measures implemented after risk assessment confirm a lower exposure to potential risks. RMS lessens the effects of threats and business disruptions and improves organisational resilience.
3. **Business impact analysis (BIA) strategy:** This strategy examines the impact of disasters and critical events on business and other operational activities when they actually occur. Proactive entrepreneurs conduct a BIA as a mitigation measure to identify business operations that have been affected.
4. **Emotional intelligence strategy (EIS):** EIS is a crisis leadership competency that helps top leadership motivate and encourage all other members to recover from a crisis by leveraging four (4) domains of EI: self-awareness, self-management, social awareness, and relationship management.
5. **Recovery point objective (RPO) protocol:** RPO is concerned with determining, prior to a disaster, how much operational data an organisation can afford to lose in the interim before the event hurts financially or disrupts business continuity.
6. **Recovery time objective (RTO) protocol:** RTO is concerned with estimating the impact that downtime will have on business operations in relation to a specified timeframe or length of time it would take for IT systems to be restored after a disaster for business continuity.
7. **Virtualized disaster recovery plan (VDRP).** This virtualisation strategy provides organisations with vantage opportunities to implement the DRP. When IT infrastructure facilities are halted by disasters, the VDRP spins new virtual machines within minutes, averting disruption and speeding up the recovery process.
8. **Network disaster recovery plan (NDRP)**: The NDRP strategy is a resilient plan developed to ensure business continuity and avert disruption to IT networks during network disasters.
9. **Cloud disaster recovery plan (CDRP): The CDRP** is an efficient and cost-effective cloud-based disaster recovery strategy that ranges from routine file backup in the cloud to complete data replication to secure physical and virtual servers.
10. **Data centre disaster recovery plan (DCDRP)**: The DCDRP creates a dedicated data centre charged with the responsibility of preempting disaster by conducting operational risk assessment under different possible scenarios on components of the organisations, such as building location, power systems and protection, security, and office space, to determine the vulnerability and resilience of the data centre to respond to disasters.
11. **Data backup plan:** The data backup plan is a proactive step for regularly maintaining and storing backup copies of all processed information and updated organisational

data to ensure easy retrieval and availability at all times as files, folders, SaaS applications, hard drives, and other business databases.

12. **Cybersecurity Insurance:** In reality, cybersecurity investments are costly compared to the benefits derived from incremental security. It is a sustainable means of transferring part of the cybersecurity risks associated with potential cyberattacks and future breaches to insurance companies at the cost of a premium.

Conclusion and Policy Prescriptions

To forestall cyberattacks in fast-emerging toxic entrepreneurship ecosystems, entrepreneurs and corporate organisations in ASEAN require comprehensive policy documents outlining their business continuity and disaster recovery strategies (BCRS). Entrepreneurs and corporate organisations in ASEAN urgently need to promote cybersecurity awareness and culture among managers and employees because it is impossible to predict the nature of cyberattacks and the timing and extent of disruptions and harm that could arise. ASEAN policymakers must invest heavily in cybersecurity because national infrastructural systems that are largely driven by interconnected computer systems and digital backbones, when attacked, can pose serious national security problems. Finally, strong regional, national, and international cybersecurity laws were expedient.

References

Abdallah, A. B., Phan, A. C., and Matsui, Y. (2016). Investigating the effects of managerial and technological innovations on operational performance and customer satisfaction of manufacturing companies. *International Journal of Business Innovation and Research*, *10*(2-3), 153-183.

Cashell, B., Jackson, W. D., Jickling, M., and Webel, B. (2004). The economic impact of cyber-attacks. *Congressional research service documents, CRS RL32331 (Washington DC)*, *2*, 1-45. https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf

Council on Foreign Relations (2022) What Is ASEAN? Online resources. https://www.cfr.org/backgrounder/what-asean

Exposito, A., and Sanchis-Llopis, J. A. (2018). Innovation and business performance for Spanish SMEs: New evidence from a multidimensional approach. *International Small Business Journal*, *36*(8), 911-931.

Hasan, S., Ali, M., Kurnia, S., and Thurasamy, R. (2021). Evaluating the cyber security readiness of organisations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.

IBM (2022) What is a cyberattack? https://www.ibm.com/topics/cyber-attack

IBM Services (2020) Adapt and respond to risks with a business continuity plan (BCP). https://www.ibm.com/au-en/services/business-continuity/plan

Imperva, (2021). 2021 Cyberthreat Defense Report. https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report/

Kamil, M., Pratama, M. I., and Arief, M. N. (2019, June). Openness, Labor, and Tourism; Case Study of ASEAN Countries. In *3rd International Seminar on Tourism (ISOT 2018)* (pp. 226-229). Atlantis Press.

Sullivan, J. E., and Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. *The Electricity Journal*, *30*(3), 30-35.

Syahwier, C. A. (2018). ASEAN Economic Integration and Inclusive Economic Growth. In *Talenta Conference Series: Local Wisdom, Social, and Arts (LWSA)* (Vol. 1, No. 2, pp. 383-391).

Unisys (2022) Cyber Attacks - What you need to know. Glossary of terms by Unisys https://www.unisys.com/glossary/cyber-attack/

US Department of Justice (2020). Nigerian National Brought to U.S. to Face Charges of Conspiring to Launder Hundreds of Millions of Dollars from Cybercrime Schemes**.** Press Release of the U.S. Attorney's Office**,** Central District of California**.** https://www.justice.gov/usao-cdca/pr/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds-millions-dollars