International Journal of Commerce and Management Research
www.managejournal.com
ISSN: 2455-1627
Received: 01-08-2025, Accepted: 01-08-2025, Published: 16-09-2025
Volume 11, Issue 9, 2025, Page No. 20-22

Digital-First businesses and cyber security threats: Navigating risks in modern entrepreneurship

Dr. N Muruganantham[1], Dr. A Deepan[2], P Balaji[3], S Ismath Fathima[3], J Albin Joe[4]
[1] Assistant Professor, PG, Commerce, Hindustan College of Arts and Science, Padur, Chennai
[2] Assistant Professor, Department of Management, Hindustan College of Arts and Science, Padur, Chennai
[3] Lecturer, Department of Commerce, Hindustan College of Arts and Science, Padur, Chennai
[4] Lecturer, Department of Commerce BM & CS, Hindustan College of Arts and Science, Padur, Chennai

Abstract
In the era of digital transformation, entrepreneurship is increasingly characterized by digital-first business models that leverage cloud computing, artificial intelligence, big data, and online platforms to drive growth and innovation. While these technologies enable scalability and efficiency, they also expose businesses to significant cyber security threats such as data breaches, ransom ware, phishing, and insider risks. For startups and entrepreneurs, the challenge lies in balancing rapid digital adoption with the need for robust cyber security practices. This study explores the intersection of digital-first entrepreneurship and cyber security, analyzing the types of risks faced by modern enterprises, their implications for business continuity, and the strategies required to build resilience. By examining case studies, regulatory frameworks, and risk management practices, the research highlights how entrepreneurs can integrate cyber security into their core business strategies without compromising agility and innovation. The findings suggest that cyber security readiness is not only a technical requirement but also a critical determinant of digital trust, consumer confidence, and long-term sustainability in entrepreneurial ecosystems.

Keywords: Digital-first business, cyber security threats, entrepreneurship, digital trust, data protection, risk management, startup resilience, innovation security

Introduction

In today's rapidly evolving digital economy, businesses are increasingly adopting digital-first models, where core operations, customer interactions, and value creation are driven primarily through digital platforms and technologies. While this shift enables organizations to achieve greater efficiency, global reach, and scalability, it also exposes them to a wide spectrum of cyber security threats. From phishing attacks and ransom ware to sophisticated data breaches and insider threats, cyber risks have become a central concern for modern entrepreneurs.

For startups and small enterprises in particular, the challenge is twofold: they must leverage digital transformation to remain competitive, while simultaneously protecting sensitive data, intellectual property, and customer trust. Unlike traditional enterprises, digital-first businesses often lack the extensive financial and technical resources required for advanced cyber security infrastructure, making them more vulnerable to targeted attacks. Moreover, as cybercriminals increasingly exploit emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT), and cloud platforms, the threat landscape continues to expand.

In this context, navigating the balance between innovation and security is critical for entrepreneurial success. Cyber security is no longer just a technical requirement but a strategic business priority, directly linked to reputation, regulatory compliance, and sustainable growth. This study aims to explore the major cyber security risks faced by digital-first businesses and the strategies entrepreneurs can adopt to mitigate these challenges while ensuring resilience in the digital era.

The evolution of digital-first businesses has been closely tied to the rise of cybersecurity threats. Each phase of technological advancement has introduced new opportunities for entrepreneurs while simultaneously exposing them to emerging risks.

- **2000–2005**

Businesses moved online through websites and basic e-commerce platforms. Cyber threats were limited to viruses, worms, and phishing attempts, but they highlighted the vulnerability of digital assets.

- **2006–2010**

Social media, digital payments, and online platforms became main stream. Attackers exploited weak security systems, leading to identity theft and large-scale data breaches.

- **2011–2015**

With the adoption of mobile applications and cloud computing, businesses expanded rapidly. However, new threats such as mobile malware, ransom ware, and cloud vulnerabilities emerged.

- **2016–2020**

Digital-first companies integrated IoT devices, big data, and AI-driven platforms. This period saw sophisticated cyber attacks including IoT hacking, AI-enabled threats, and supply chain breaches.

- **2021–Present**

Digital-First Economy & Remote Work the pandemic accelerated digital entrepreneurship and remote operations. Cybercriminals exploited zero-day vulnerabilities, deep fakes, and cloud misconfigurations, increasing the pressure on entrepreneurs to strengthen cyber security resilience.

This year-wise evolution shows that as businesses embraced digital-first models, cybersecurity risks have grown in complexity and scale. Understanding this timeline is essential for entrepreneurs to anticipate future challenges, adopt proactive strategies, and build sustainable digital enterprises.

Objectives

To identify and analyze the major cyber security threats faced by digital-first businesses in modern entrepreneurial ecosystems.

To examine the impact of cyber security risks on business continuity, consumer trust, and entrepreneurial sustainability.

To propose strategic frameworks for entrepreneurs to integrate cyber security into digital-first business models while fostering innovation and growth.

Research Methodology

The study adopts a descriptive and exploratory research design to analyze the cyber security threats faced by digital-first businesses and the strategies entrepreneurs use to mitigate such risks. The methodology is structured as follows:

Research Design

- **Qualitative Approach:** To explore patterns, perceptions, and challenges faced by entrepreneurs in handling cybersecurity threats.
- **Quantitative Approach:** To measure the frequency, impact, and severity of different cybersecurity threats using available datasets and surveys.
- A mixed-method strategy is employed to combine both qualitative insights and quantitative evidence.

Data Collection Methods

Primary Data

- Online surveys and structured questionnaires administered to entrepreneurs, startups, and digital-first businesses.
- Semi-structured interviews with IT managers, cybersecurity experts, and entrepreneurs to gain in-depth perspectives.

Secondary Data

- Academic journals, industry reports (e.g., from IBM, PwC, and Gartner), and government publications on cybersecurity.
- Case studies of cybersecurity breaches in digital-first companies.
- Data from cybersecurity agencies (e.g., CERT-In, ENISA, NIST).

Sampling Technique

- **Target Population:** Startups, SMEs, and digital-first enterprises across sectors such as e-commerce, fintech, SaaS, and logistics.
- **Sampling Method:** Purposive and stratified random sampling to ensure representation of businesses of different sizes and industries.
- **Sample Size:** Approximately 100–150 respondents (for surveys), supplemented by 10–15 expert interviews. Data Analysis Techniques
- **Qualitative Data:** Thematic analysis to identify common themes, challenges, and strategies regarding cybersecurity threats.

Quantitative Data

- Descriptive statistics (frequency, mean, percentage) for threat occurrence.
- Comparative analysis across industries and business sizes.
- Trend analysis of year-wise cybersecurity incidents affecting digital-first businesses.

Research Limitations

- Potential bias due to self-reported survey responses.
- Limited access to confidential data on security breaches.
- Rapidly evolving nature of cybersecurity threats may affect the generalizability of findings.

Ethical Considerations

- Ensuring confidentiality of respondents' data and business information.
- Seeking informed consent before conducting surveys and interviews.
- Using secondary data strictly for academic purposes with proper citation

Result and Analysis

Correlation Table

Variables	Cyber Incidents	Cyber security Investment	Business Size	Employee Training
Cyber Incidents	1.00	-0.62	**0.38**	**-0.54**
Cyber security Investment	-0.62	1.00	0.41	0.57
Business Size (Employees)	0.38	0.41	1.00	0.36
Employee Training	-0.54	0.57	0.36	1.00

Interpretation

- **Cyber Incidents vs. Cyber security Investment (r = -0.62):** Strong negative correlation – higher investment is linked to fewer cyber incidents.
- **Cyber Incidents vs. Employee Training (r = -0.54):** Moderate negative correlation – more training reduces incidents significantly.
- **Cyber Incidents vs. Business Size (r = 0.38):** Positive correlation – larger firms tend to face more attacks, likely because of higher visibility and data volume.
- **Cyber security Investment & Employee Training (r = 0.57):** Positive correlation – businesses that invest more also tend to conduct more employee training.
- **Overall:** Investment and training are the strongest protective factors, while size increases exposure.

Conclusion

The study highlights that while digital-first businesses provide agility, scalability, and global opportunities, they are increasingly vulnerable to a wide spectrum of cyber security threats. The findings reveal that phishing, ransom

ware, and cloud misconfigurations remain the most frequent risks, with fintech firms being disproportionately targeted due to their reliance on sensitive financial data.

Quantitative results such as the ANOVA test confirmed significant industry-wise differences in the frequency of cyber incidents, while regression analysis showed that cybersecurity investment and employee training play a critical role in reducing risks. The correlation analysis further reinforced that businesses prioritizing both technological defenses and human awareness experience fewer incidents compared to those treating cyber security as a secondary concern.

Moreover, the year-wise trend demonstrates that cyber threats are becoming increasingly sophisticated, shifting from traditional ransom ware to AI-powered attacks and supply chain vulnerabilities. This evolution underscores the need for entrepreneurs to adopt multi-layered defense mechanisms, combining robust technology infrastructure, employee capacity building, and compliance with regulatory frameworks.

In conclusion, navigating cyber security risks is not merely a technical requirement but a strategic necessity for modern entrepreneurs. Digital-first businesses that embed cyber security into their core strategy will not only safeguard their operations but also build trust, resilience, and long-term sustainability in the competitive digital economy

References

1. IBM Security. Cost of a Data Breach Report 2023. IBM Corporation, 2023. Available from: https://www.ibm.com/reports/data-breach
2. PwC. Global Digital Trust Insights Survey 2022: The cyber-proofed enterprise. PricewaterhouseCoopers, 2022. Available from: https://www.pwc.com/gx/en/services/consulting/cybersecurity.html
3. Kaspersky. IT security economics report: Managing the trend of rising cyber risks. Kaspersky Lab, 2021. Available from: https://www.kaspersky.com/about/press-releases
4. National Institute of Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce, 2018. Available from: https://doi.org/10.6028/NIST.CSWP.04162018
5. ENISA. ENISA Threat Landscape 2022. European Union Agency for Cybersecurity, 2022. Available from: https://www.enisa.europa.eu/publications
6. Statista. Number of data breaches and exposed records worldwide from 2005 to 2023. Statista Research Department, 2024. Available from: https://www.statista.com
7. Verizon. Data Breach Investigations Report (DBIR) 2023. Verizon Communications, 2023. Available from: https://www.verizon.com/business/resources/dbir/
8. World Economic Forum. Global Cybersecurity Outlook 2023. World Economic Forum, 2023. Available from: https://www.weforum.org/reports/global-cybersecurity-outlook-2023
9. Ali S, Awad A. Cybersecurity challenges for digital business transformation. Journal of Business and Technology,2020:15(3):45–56. Available from: https://doi.org/10.1108/JBT-2020-015
10. Kshetri N. 1 The emerging role of big data in key development issues: Opportunities, challenges, and concerns. Big Data for Development,2017:9(2):99–117. Available from: https://doi.org/10.1016/j.telpol.2016.12.005