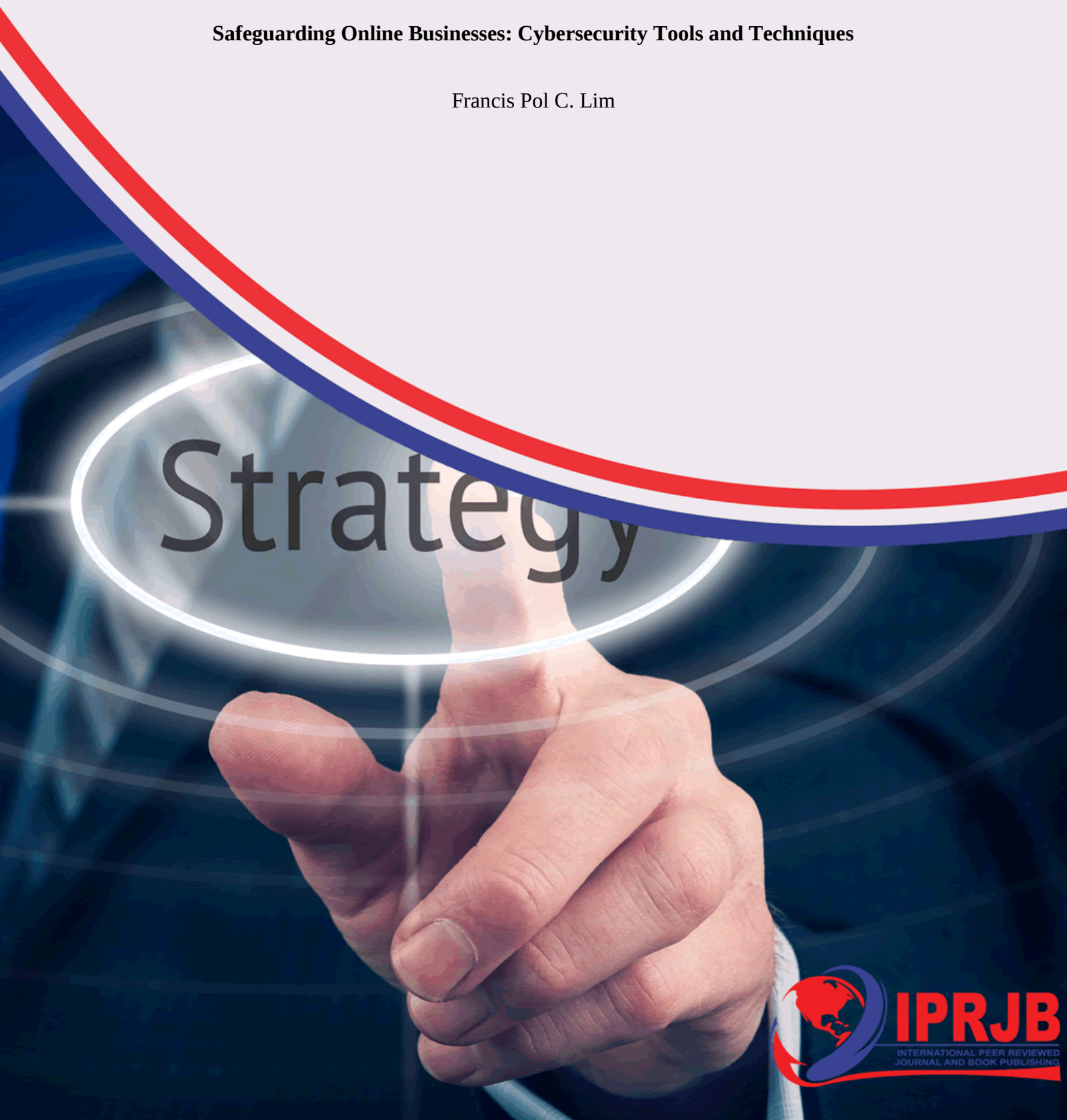
European Journal of
Business and Strategic Management
(EJBSM)

Safeguarding Online Businesses: Cybersecurity Tools and Techniques

Francis Pol C. Lim



IPRJB
INTERNATIONAL PEER REVIEWED
JOURNAL AND BOOK PUBLISHING

European Journal of Business and Strategic Management
ISSN 2518-265X (Online)
Vol.10, Issue 6, No.3. pp 40 - 53, 2025

www.iprjb.org

Safeguarding Online Businesses: Cybersecurity Tools and Techniques

[1*]Francis Pol C. Lim
Charisma University, Grace Bay, Providenciales, Turks and Caicos Island, American Management University, Orem Utah, USA

Article History

Received 16th August 2025

Received in Revised Form 20th September 2025

Accepted 27th October 2025

How to cite in APA format:

Lim, F. (2025). Safeguarding Online Businesses: Cybersecurity Tools and Techniques. *European Journal of Business and Strategic Management*, *10*(6), 40–53. https://doi.org/10.47604/ejbsm.3549

Abstract

Purpose: The accelerated expansion of business online has brought unprecedented commercial opportunities but also subjected businesses to emerging cybersecurity risks.

Methodology: This report is a conceptual review on fundamental tools, methods, and frameworks required to protect digital business, with emphasis on both technical and organizational aspects. Key strategies like firewalls, encryption, intrusion detection systems, and multi-factor authentication are discussed together with best practices in risk assessment and staff training. The forum also touches upon the establishment of a cybersecurity culture in organizations, with the focus on the human element of prevention.

Findings: Moreover, the research points to the importance of legal and regulatory compliance, including certifications and measures of protection of data used in the Philippines, other Asian nations, and the international arena. Cost-effective technologies combined with regulatory compliance can enhance resilience, safeguard customer trust, and ensure competitiveness.

Unique Contribution to Theory, Practice and Policy: The research implies that ensuring robust cybersecurity protection for online businesses is a fundamental prerequisite for organizational sustainability, consumer trust, and competitive growth in today's digital economy.

Keywords: *Online Business, Digital Economy, Cybersecurity*

European Journal of Business and Strategic Management
ISSN 2518-265X (Online)
Vol.10, Issue 6, No.3. pp 40 - 53, 2025
www.iprjb.org

INTRODUCTION

The digital evolution of business has fueled the expansion of online companies across various sectors, ranging from retail to financial institutions. This is caused by rising internet penetration, innovations in digital payment platforms, and the globalisation of supply chains. Online companies have become an essential pillar of the worldwide economy, facilitating entrepreneurs to extend their reach, lower the cost of doing business, and offer convenience to customers. But this dependence on online platforms has enormous cybersecurity issues (Kumar et al., 2022).

Cybersecurity attacks not only cause immediate monetary loss but also damage reputations that can prove more expensive in the long run. Evidence indicates that small- and medium-sized businesses (SMEs) are most susceptible to cyberattacks, with almost 43% of cybersecurity incidents hitting this sector (Verizon, 2022). In contrast to big corporations who have enough resources to invest in cybersecurity infrastructure, SMEs face budget constraints, a lack of technical expertise, and dependencies on third-party service providers, rendering them potential targets for cybercriminals (Alhawari et al., 2021).

Furthermore, the growing sophistication of cyber threats is increasing risks for online businesses. Cyber threats like phishing, ransomware, and DDoS attacks are becoming better armed with artificial intelligence and automation, rendering them harder to detect and neutralize (Akacha et al., 2023). With growing digital presence through e-commerce websites, cloud services, and mobile applications, businesses expose themselves to exponentially higher vulnerabilities.

With this environment, cybersecurity for e-business is not a matter of technology alone but a matter of strategy. Protecting online assets, customer data, and service continuity need to involve the use of effective tools, employee training, and compliance with regulatory environments. With an integrated cybersecurity approach, business owners can reduce threats, increase resilience, and create long-term trust with customers (Alier et al., 2021).

To address the challenges, this study aims to evaluate the effectiveness of cybersecurity tools and techniques used by online businesses to mitigate emerging digital threats. This research is justified by the growing need to strengthen cyber resilience among businesses to ensure data protection, customer trust, and sustainable digital growth in an increasingly interconnected economy.

Uncommon Cyber Threats in Internet Business

The evolution from face-to-face commerce to the internet and digital space has transformed businesses and consumers' interactions. Although the transformation opens untold opportunities for innovation and growth, it also presents a broad variety of cybersecurity issues. Online businesses themselves have a specially vulnerable risk profile as they are dependent on interrelated technologies like cloud platforms, mobile applications, and electronic payment systems (Fernández-Caramés & Fraga-Lamas, 2019). The digital touchpoints are both facilitators of business growth and possibly entry points for malicious entities.

The threat landscape that environs online businesses is marked by its fluidity and pace of change. In contrast to traditional security threats, cyber threats are automated, scalable, and borderless, and they can be used to attack vulnerabilities worldwide. The cybercrime-as-a-service model also further reduced entry barriers, and even those with limited technical knowledge can now initiate disruptive attacks (Zimba & Phiri, 2020). Therefore, the threat

environment for entrepreneurs and web platforms is not just confined to megacorporations but also largely spreads to small and medium-sized businesses (SMEs) that do not have strong defenses.

Additionally, cyber threats are becoming more entangled with psychological and social aspects. Psychological and social vulnerabilities are targeted by social engineering measures, including phishing and business email compromise, that abuse human trust instead of technical vulnerabilities. This melting pot of technological and human vulnerabilities highlights the complex nature of contemporary cyber threats (Hadnagy, 2018).

Against this background, recognition of and insight into the most prevalent types of cyber threats is essential for online business owners. Knowledge of these threats constitutes the basis for the deployment of effective defenses, for allocation of resources where they are needed, and for providing resilience against constant digital evolution. The next sections discuss five of the most widespread threats—phishing, ransomware, distributed denial-of-service (DDoS) attacks, insider threats, and data breaches—before discussing their implications for online businesses.

Phishing Attacks

Phishing is one of the most highly effective and popular techniques of breaching business systems. Attackers generally employ fraudulent emails, websites, or instant messages in order to lure employees or customers into sharing sensitive credentials. The growth of "spear phishing" using closely tailored messages directed at specific users has grown the success rates of such attacks (Jagatic et al., 2007). For online enterprises, phishing is especially risky because it can most likely go straight into account takeovers, unauthorized transactions, and identity theft. Improving employee awareness and using sophisticated email filtering systems are essential to addressing these risks.

Ransomware

Ransomware attacks have evolved into highly sophisticated campaigns that now target not only individual systems but also complete organizational networks. Ransomware once activated, encrypts business information and requires payment, frequently in cryptocurrency, to restore. The move towards "double extortion" ransomware, under which attackers threaten to publish stolen information alongside encrypting it, has caused this threat to become even more insidious (Kharraz et al., 2015). In the case of online businesses, a ransomware attack can bring operations to a standstill, hinder supply chain operations, and besmirch reputation, making backup and recovery processes paramount.

Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks bombard online sites with excessive traffic, crippling servers and rendering websites or applications unresponsive. Downtime of just a few hours for e-commerce sites can mean massive financial loss and dissatisfied customers. The increasing popularity of "DDoS-as-a-Service," with cyber attackers leasing botnets to carry out attacks, has reduced the technical hurdles for attackers (Mirkovic & Reiher, 2004). To counter such attacks, companies increasingly use cloud-based DDoS mitigation services and content delivery networks (CDNs).

Insider Threats

Insider threats happen when employees, partners, or contractors abuse their access to the organizational resources. Such threats can be intentional, as when stealing data for financial gain, or accidental, as when inattentive handling of login credentials. Insider threats are

especially hard to find since they use legitimate authorization rights and usually do not get detected until serious harm is caused (Cappelli et al., 2012). Developing a robust cybersecurity culture, using role-based access control, and scanning for unusual activity are good countermeasures.

Data Breaches

Data breaches refer to unauthorized access to sensitive customer and business data, such as financial data, personal data, and intellectual property. The consequences of data breaches go beyond monetary fines, impacting customer confidence and business reputation. Research indicates that customers are becoming increasingly hesitant to transact with companies that have experienced breaches, particularly in payment and personal information industries (Romanosky, 2016). Encryption, periodic vulnerability scanning, and adherence to data protection laws are essential for keeping online businesses at bay from breach risks.

Online Business Protection Cybersecurity Tools

For online businesses, the use of proper cybersecurity tools is critical to business operations security, customer data protection, and business continuity. Since cyber threats evolve constantly in sophistication, manual monitoring alone or conventional security measures are no longer adequate. Rather, online businesses need to use a layered defense approach that integrates several security tools, each covering a different security aspect. This method, which is commonly known as "defense in depth," ensures that in case one layer of defense is compromised, there are others that remain to avert or reduce damage (Tipton & Krause, 2019).

The choice of cybersecurity solutions should be influenced by the size of the business, business model, and industry needs. While large businesses have the resources to implement sophisticated enterprise-level solutions, small and medium businesses (SMEs) tend to require affordable, scaleable solutions that meet usability needs. The following subsections describe the most common cybersecurity tools for businesses operating online and their functions, as well as strategic value.

Firewalls

Firewalls are the first line of defense as they inspect and manage incoming and outgoing network traffic. They impose access policies, which allow only legitimate traffic to enter or exit the business network. Contemporary firewalls, also known as "next-generation firewalls," include features such as intrusion prevention, application awareness, and deep packet inspection (Alotaibi et al., 2016). Firewalls are important for online businesses as they prevent unauthorized access and expose the organization to minimum outside threats.

Antivirus and Anti-Malware Software

Antivirus and anti-malware software shields business infrastructure from malicious programs meant to destabilize operations or harvest data. The software scans devices non-stop, identifies malicious code, and quarantines or deletes harmful files. Over the past decade, signature-based detection techniques have been complemented by heuristic and behavioral analysis, allowing quicker identification of new threats (Idika & Mathur, 2007). For startups and SMEs, installing trusted antivirus software on all devices is one of the most affordable security investments.

Virtual Private Networks (VPNs)

VPNs became a must with the prevalence of remote work and global teams. VPNs encrypt internet traffic and establish secure channels for data transmission, keeping sensitive

information confidential even when traversed via public networks. For online businesses processing customer transactions or company information, VPNs protect communication channels from eavesdropping and unauthorized capture (Zhang et al., 2018).

Multi-Factor Authentication (MFA)

Passwords are not enough to secure business systems anymore, as they are usually stolen or broken using brute-force attacks. MFA provides an extra layer of security by demanding multiple types of authentication, like a password along with a one-time code or biometric data. This greatly minimizes the potential for unauthorized access, even when credentials are stolen (Das et al., 2018). For financial transaction sites online, MFA is now an industry norm to guarantee business and user account protection.

Intrusion Detection and Prevention Systems (IDPS)

IDPS solutions track network and system activity for indications of malicious activity. Intrusion Detection Systems (IDS) detect suspicious activity and issue alarms, whereas Intrusion Prevention Systems (IPS) actively prevent detected threats. Through ongoing examination of traffic patterns, IDPS solutions issue early warnings and automated response to potential intrusions, minimizing the effect of attacks (Scarfone & Mell, 2007). Online companies are advantaged through the use of IDPS by getting visibility into attempted intrusions and enhancing their proactive defense position.

Data Backup and Recovery Solutions

Security threats like ransomware underscore the need for data backup and recovery software. These solutions provide assurance that companies are able to recover from a disruption in a timely manner by having secure copies of important data. Cloud backup services, especially, provide scalability and geographic redundancy, minimizing the likelihood of data loss due to local incidents (Nayak et al., 2020). For Internet businesses, frequent backups and recovery planning are critical to sustaining customer confidence and business continuity in the event of unforeseen situations**.**

Techniques and Best Practices

Although cybersecurity tools represent the technical foundation of computer protection, their efficiency is enhanced by being augmented with clearly established techniques and organizational best practices. For Internet businesses, unification of human, managerial, and technical controls guarantees a comprehensive approach towards cybersecurity. Because the majority of cyber attacks are based on a combination of technical vulnerabilities and human fault, embracing proactive practices and developing a security-aware culture are critical to minimizing threats and guaranteeing operational robustness (Von Solms & Van Niekerk, 2013).

The following subsections define essential techniques and practices that online enterprises need to make a priority to enhance their cybersecurity stance.

Regular Software Updates and Patch Management

Perhaps the most widespread business system vulnerability is caused by software that is outdated and applications that have not been patched. Cybercriminals typically leverage well-known security vulnerabilities to obtain unauthorized access. Patch management is successful if it systematically identifies, tests, and installs updates for software, operating systems, and

applications. Automating the update and keeping an inventory of all digital assets allows companies to reduce exposure to vulnerabilities (Souppaya & Scarfone, 2013).

Employee Awareness and Training

Employees are the first line of defense and the weakest link in cybersecurity. Awareness training on phishing, password hygiene, and safe browsing can significantly lower risk. Research indicates that organizations with regular cybersecurity training have fewer successful phishing attacks and reduced data breach costs (Parsons et al., 2017). Online enterprises with distributed teams can utilize low-cost solutions through e-learning platforms and simulated phishing campaigns to enhance employee readiness.

Robust Password Policies

Password-related intrusions continue to be one of the most common reasons for cyber occurrences. The implementation of robust password policies, including the use of complicated mixes of characters, regular changes, and the banning of reuse across accounts, immensely strengthens security. The use of password managers also helps employees to create and update safe credentials without using weak or repeatable passwords (Florêncio & Herley, 2007).

Encryption of Sensitive Data

Encryption guarantees that confidential information—like financial transactions, customer data, and intellectual property—is still unreadable to unauthorized users. Online ventures need to apply encryption both in transit (e.g., with SSL/TLS protocols for safe web traffic) and at rest (e.g., encrypted databases). Improvements in end-to-end encryption add extra layers of security, particularly for ventures that provide communication platforms or process personal information (Kshetri & Voas, 2017).

Adoption of Zero-Trust Framework

The perimeter-based traditional view of cybersecurity is inadequate anymore, particularly as companies become more entrenched in hybrid and cloud environments. Zero-trust assumes that no device or user is always trusted and needs to be constantly verified before access is granted. Adopting zero-trust measures such as micro-segmentation, identity-based access, and real-time monitoring reduces the lateral movement threat by attackers in networks (Kindervag, 2010).

Incident Response Planning

Even with preventive approaches, cyber events are inevitable. A good incident response plan provides step-by-step actions for detection, isolation, and reduction of cyberattacks. Key components are the establishment of roles and responsibilities, maintaining open lines of communication, and post-incident analysis to better defend against future attacks. Companies with validated incident response plans have much lower breach costs and quicker recovery times (Lindström et al., 2020).

Developing a Cybersecurity Culture

Although technical protections are indispensable, most cybersecurity attacks are caused by human mistake, complacency, or ignorance. For web-based businesses, having a robust cybersecurity culture is as imperative as investing in cutting-edge tools. A cybersecurity culture is the collective values, beliefs, and practices existing within an organization that influence employees' behavior and attitude toward security (Da Veiga & Eloff, 2010). This development ensures that cybersecurity is integrated into the organizational culture and not an afterthought.

European Journal of Business and Strategic Management
ISSN 2518-265X (Online)
Vol.10, Issue 6, No.3. pp 40 - 53, 2025
www.iprjb.org

Below are the most important strategies to develop a cybersecurity-conscious workplace within online business environments:

Leadership Commitment and Tone at the Top

Effective cybersecurity culture starts with leadership. Executives and business managers need to lead by commitment through investment, policy definition, and practice of secure behaviors. Studies indicate that in organizations where leaders publicly back cybersecurity efforts, they have greater employee compliance and fewer incidents of insider-led threats (Knapp et al., 2006). For small and medium-sized online enterprises, buy-in by leadership is even more significant, as employees tend to reflect priorities defined by management.

Staff Involvement and Responsibility

Staff need to view cybersecurity as an integral part of their work responsibilities, rather than an IT task. Inducement of staff reporting suspicious behavior, practicing secure procedures when dealing with data, and actively engaging in security programs establishes a sense of shared responsibility. Reward programs—e.g., rewards for sound cybersecurity practice—can encourage good behaviors (Alshaikh, 2020).

Ongoing Security Awareness Programs

Cybersecurity consciousness cannot be attained from single-shot training. Repeated programs, such as repeated phishing simulations, scenario-based workshops, and gamification learning, retain employees' interest and awareness. Customized content—such as role-based training for finance teams, customer care staff, or systems administrators—also ensures that employees realize the threat related to their job functions (Parsons et al., 2017).

Integration of Cybersecurity into Daily Operations

A secure culture is healthy when it incorporates cybersecurity into daily processes. These include incorporating security scans into workflows, insisting on multi-factor authentication for access to systems, and frequent audits. Incorporating "security by design" principles guarantees that cybersecurity is thought about at each step of business processes, from website design to customer data processing (Schlienger & Teufel, 2003).

Insider Threats and Human Error

Human factors are the weakest link in most organizations. Companies need to identify risks from not only malicious insiders but also benevolent employees who inadvertently breach security. Methods such as role-based access control, separation of duties, and privileged account monitoring can reduce insider-related risks (Greitzer et al., 2014).

Measuring and Reinforcing Cybersecurity Culture

To maintain long-term gains, companies must quantify cybersecurity culture using worker surveys, incident reporting rates, and compliance measurements. Feedback loops enable organizations to update training and policies on a continuous basis. Creating a culture where failures are opportunities to learn, not excuses to punish, facilitates openness and limits underreporting of incidents (Da Veiga, 2016).

Regulatory Compliance and Legal Obligations

For digital businesses, cybersecurity is not only a question of defending assets but also of complying with regulatory and legal stipulations. Failure to comply with data privacy and cybersecurity regulations has the potential to attract immense financial penalties, damage to

brand reputation, and loss of consumer confidence. With businesses venturing into digital platforms, they face an intricate environment of law governing cybersecurity and data privacy that differs by jurisdiction (Tikkinen-Piri et al., 2018). Incorporating compliance into cybersecurity models benefits companies by minimizing exposure to risk while also solidifying customer trust in their products.

The subsequent subsections discuss the major areas of compliance and legal issues applicable to online businesses.

Global Data Protection Regulations

The General Data Protection Regulation (GDPR) within the European Union has been perhaps the most powerful regulation over the last few years. It imposes rigorous requirements on the manner in which companies gather, store, and handle personal information, with fines going as much as 4% of worldwide annual turnover for non-compliance. Other frameworks similar to it are present globally, including the California Consumer Privacy Act (CCPA) in the United States and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada (Greenleaf, 2018). Online enterprises that operate globally need to implement an adaptive compliance strategy to consider varying legal environments.

Cybersecurity Standards and Frameworks

To support legal requirements, organizations can apply industry-standard frameworks to inform their cybersecurity practices. Frameworks like ISO/IEC 27001 and the NIST Cybersecurity Framework offer well-defined methods for risk management, control establishment, and enhancement of resilience. These frameworks not only assist with compliance but also indicate due diligence, which can reduce liability in the case of a breach (NIST, 2018).

Consumer Protection and E-Commerce Regulations

E-commerce websites manage sensitive financial and personal information, so compliance with consumer protection legislation is a must. Rules frequently require secure payment processing, open data usage policies, and visible customer redress mechanisms. For instance, the Payment Card Industry Data Security Standard (PCI DSS) provides security requirements for companies that process credit card transactions (Mellado et al., 2010). Compliance with such standards fosters consumer confidence and fraud protection.

Cross-Border Data Transfer Problems

Most online companies run across various regions, and cross-border data transfers become a concern. Laws like GDPR prohibit the outflow of personal data to jurisdictions not approved unless proper safeguards exist. Business facilitates like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) assist companies in ensuring legal compliance while running business globally (Kuner et al., 2015). Familiarity with such mechanisms is important for companies utilizing cloud services or global outsourcing.

Data Protection Regulatory Certifications across Various Countries

In addition to adherence to law, most countries encourage or mandate that companies get certifications affirming their compliance with data protection regulations. Certifications assure regulators and clients of third-party assurance that companies have put in place appropriate measures.

- **European Union (EU): GDPR Certification** – Under Article 42 of the GDPR, organizations may obtain data protection certification from accredited bodies to demonstrate compliance. While voluntary, such certifications provide evidence of accountability and responsible data handling (Voigt & Von dem Bussche, 2017).
- **United States: SOC 2 and FedRAMP** – In the U.S., while there is no single federal privacy law, certifications such as SOC 2 (System and Organization Controls 2) validate an organization's data protection controls. For cloud service providers working with federal agencies, FedRAMP certification is required to ensure security and compliance with government standards (Sedgewick, 2014).
- **Canada: PIPEDA Compliance and ISO/IEC 27001** – Canadian businesses often pursue ISO/IEC 27001 certification to align with the Personal Information Protection and Electronic Documents Act (PIPEDA). Certification demonstrates structured risk management and secure handling of personal data (Cavoukian, 2012).
- **Singapore: Data Protection Trustmark (DPTM)** – Singapore's Infocomm Media Development Authority introduced the DPTM certification to recognize organizations with robust data protection policies aligned with the Personal Data Protection Act (PDPA). This certification signals reliability and transparency in handling customer data (Tan & Theodorou, 2020).
- **Japan: PrivacyMark System** – In Japan, the PrivacyMark is awarded to organizations that comply with the Japanese Industrial Standards (JIS Q 15001) for personal data protection. It has become a widely recognized certification that boosts consumer trust in businesses (Nishimura, 2008).
- **Philippines: National Privacy Commission (NPC) Seal of Registration and Compliance** – In the Philippines, businesses handling personal information are required to register their data processing systems with the NPC under the Data Privacy Act of 2012 (Republic Act No. 10173). The NPC issues a **Seal of Registration** to organizations that comply with registration requirements, and it has introduced mechanisms for **Privacy Management Program certifications** that validate adherence to data protection standards. These efforts strengthen accountability and trust among digital consumers (NPC, 2016).
- **Malaysia: PDPA and Data Protection Certification Framework** – Malaysia's Personal Data Protection Act (PDPA) 2010 regulates data processing by commercial organizations. The Department of Personal Data Protection introduced voluntary **data protection certifications** for service providers, demonstrating adherence to PDPA requirements and promoting good practices in handling sensitive information (Abdullah et al., 2019).
- **Thailand: Personal Data Protection Act (PDPA) Compliance Programs** – Thailand's PDPA (2019) requires businesses to adopt compliance programs aligned with global standards. Although certification programs are still developing, the law emphasizes accountability through **Data Protection Officers (DPOs)** and transparent practices. Organizations often pursue ISO/IEC 27701 (Privacy Information Management) certifications to align with local and international privacy expectations (Chotipong, 2020).

- **South Korea: ISMS-P Certification** – South Korea enforces one of the strictest data protection regimes in Asia through the Personal Information Protection Act (PIPA). The **Information Security Management System–Personal Information (ISMS-P) certification** combines data security and privacy standards into a unified framework. Businesses achieving ISMS-P demonstrate compliance with both security and privacy requirements, making it a recognized trust mark (Park & Shin, 2019).

Legal and Liability Implications of Data Breaches

If a breach occurs, companies can be subject to lawsuits, regulatory penalties, and contract disputes. Courts and regulators increasingly hold organizations liable not just for the breach but also for whether they employed best practices in cybersecurity (Romanosky, 2016). Inadequate measures can qualify as negligence and increase damages in a lawsuit (Romanosky, 2016). Compliance, therefore, lowers the risk of breaches and the severity of legal sanctions.

Blending Compliance with Business Strategy

Compliance cannot be considered a checkbox activity but as part of a sustained business strategy. Blending compliance into governance, risk management, and day-to-day activities establishes consistency and sustainability. Compliance-based cybersecurity practices also establish competitive advantage, as consumers increasingly look towards businesses that exhibit transparency and accountability in managing data (Cavoukian, 2012).

Conclusion

Protecting web businesses from cybersecurity issues is no longer a choice but a basic requirement for survival and expansion in the current digital economy. The intense growth of e-commerce, online services, and electronic transactions has raised the threat of data breaches, cyber deceit, and regulatory non-conformity, and hence, cybersecurity has become a strategic imperative. This article emphasized the essential functions of cybersecurity measures like firewalls, encryption, intrusion detection systems, and multi-factor authentication, in addition to the need for ongoing risk assessments and staff training. It also looked into the more general aspects of cybersecurity, such as developing a good security culture and compliance with changing data protection laws and certifications throughout various nations. For small and medium-sized businesses specifically, juggling affordable cybersecurity measures with compliance obligations is crucial to competitiveness and long-term vitality. Ultimately, e-businesses that integrate security into organizational processes not only safeguard confidential information but also foster trust among customers, partners, and regulators. With an interconnected digital world, cybersecurity must not only be understood as a protection system but also as a sustainability, innovation, and customer loyalty driver. In doing so, companies set themselves up to succeed securely in the constantly evolving online world.

REFERENCES

Abdullah, N. H., Mansor, Z., & Hamid, N. A. (2019). Personal data protection in Malaysia: Law and practice. *Pertanika Journal of Social Sciences & Humanities, 27*(1), 67–82. https://doi.org/10.47836/pjssh.27.1.05

Akacha, S. A., Alharthi, A., Alghamdi, A., & Alshamrani, A. (2023). Enhancing security and sustainability of e-learning: Threats, trends, and mitigation strategies. *Sustainability, 15*(19), 14132. https://doi.org/10.3390/su151914132

Alhawari, S., AlShihi, H., AlShihi, A., & Ali, S. (2021). Cybersecurity challenges in small and medium-sized enterprises: A systematic literature review. *International Journal of Business Information Systems, 37*(2), 135–158. https://doi.org/10.1504/IJBIS.2021.118237

Alier, M., Casany, M. J., Conde, M. Á., & Piguillem, J. (2021). Privacy and e-learning: A pending task. *Sustainability, 13*(16), 9206. https://doi.org/10.3390/su13169206

Alotaibi, F., Al-Bassam, N., & Ameen, A. (2016). Next-generation firewalls: Technologies, applications, and challenges. *International Journal of Computer Applications, 146*(7), 18–24. https://doi.org/10.5120/ijca2016910660

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes.* Addison-Wesley. https://doi.org/10.5555/2381026

Cavoukian, A. (2012). Privacy by design: Origins, meaning, and prospects. In *Privacy protection measures and technologies in business organizations: Aspects and standards* (pp. 170–208). IGI Global. https://doi.org/10.4018/978-1-4666-0987-9.ch009

Chotipong, S. (2020). Thailand's Personal Data Protection Act: Compliance and implications for businesses. *Asian Journal of Comparative Law, 15*(2), 303–324. https://doi.org/10.1017/asjcl.2020.22

Da Veiga, A. (2016). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information & Computer Security, 24*(2), 118–134. https://doi.org/10.1108/ICS-07-2014-0042

Da Veiga, A., & Eloff, J. H. P. (2010). A framework for information security culture assessment. *Computers & Security, 29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2018). The tangled web of password reuse. *Network and Distributed Systems Security Symposium (NDSS).* https://doi.org/10.14722/ndss.2014.23124

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2019). A review on the use of blockchain for the Internet of Things. *IEEE Access, 6*, 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web (WWW 2007)* (pp. 657–666). https://doi.org/10.1145/1242572.1242661

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report, 149,* 10–13. https://doi.org/10.2139/ssrn.2993035

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., & Ferryman, T. A. (2014). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. *2014 IEEE Security and Privacy Workshops,* 251–264. https://doi.org/10.1109/SPW.2014.41

Hadnagy, C. (2018). *Social engineering: The science of human hacking.* Wiley. https://doi.org/10.1002/9781119433750

Idika, N., & Mathur, A. P. (2007). A survey of malware detection techniques. *Purdue University, CERIAS Technical Report.* https://doi.org/10.5703/1288284314650

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks. In *Detection of Intrusions and Malware, and Vulnerability Assessment* (Vol. 9148, pp. 3–24). https://doi.org/10.1007/978-3-319-20550-2_1

Kindervag, J. (2010). Build security into your network's DNA: The zero trust network architecture. *Forrester Research, Inc.* https://doi.org/10.6028/NIST.SP.800-207

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24–36. https://doi.org/10.1108/09685220610648355

Kshetri, N., & Voas, J. (2017). The economics of "cryptocurrencies" and blockchain. *IEEE Computer, 50*(9), 18–21. https://doi.org/10.1109/MC.2017.3571047

Kumar, R., Shankar, R., & Lim, W. M. (2022). Cybersecurity and resilience in digital business: A review and research agenda. *Journal of Business Research, 139,* 1440–1455. https://doi.org/10.1016/j.jbusres.2021.10.058

Kuner, C., Bygrave, L. A., & Docksey, C. (2015). *The EU General Data Protection Regulation: A commentary.* Oxford University Press. https://doi.org/10.1093/oso/9780198826491.001.0001

Lindström, J., Johnson, P., & Johansson, E. (2020). A systematic review of information security incident handling. *Computers & Security, 92,* 101734. https://doi.org/10.1016/j.cose.2020.101734

Mellado, D., Fernández-Medina, E., & Piattini, M. (2010). A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces, 32*(6), 305–313. https://doi.org/10.1016/j.csi.2010.03.004

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39–53. https://doi.org/10.1145/997150.997156

National Privacy Commission (NPC). (2016). *Implementing Rules and Regulations of the Data Privacy Act of 2012.* Republic of the Philippines. https://doi.org/10.2139/ssrn.3512614

Nayak, R., Ojha, A., & Sharma, R. (2020). Cloud-based backup and recovery solutions for business continuity: A review. *International Journal of Cloud Computing and Services Science, 9*(1), 1–11. https://doi.org/10.11591/closer.v9i1.2020

Nishimura, A. (2008). Privacy and data protection in Japan: Law, policy, and institutions. *International Data Privacy Law, 1*(2), 104–112. https://doi.org/10.1093/idpl/ipq009

NIST. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Park, Y. J., & Shin, D. H. (2019). Privacy and security certification in South Korea: The ISMS-P framework. *Telecommunications Policy, 43*(10), 101815. https://doi.org/10.1016/j.telpol.2019.101815

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). *NIST Special Publication 800-94.* https://doi.org/10.6028/NIST.SP.800-94

Schlienger, T., & Teufel, S. (2003). Information security culture—from analysis to change. *South African Computer Journal, 31*, 46–52. https://doi.org/10.18489/sacj.v0i31.180

Sedgewick, A. (2014). Federal Information Security Management Act (FISMA) implementation project. *NIST Special Publication 800-53.* https://doi.org/10.6028/NIST.SP.800-53r4

Souppaya, M., & Scarfone, K. (2013). Guide to enterprise patch management technologies. *NIST Special Publication 800-40 Revision 3.* https://doi.org/10.6028/NIST.SP.800-40r3

Tan, J., & Theodorou, K. (2020). Singapore's Data Protection Trustmark: A step toward global accountability? *Computer Law & Security Review, 36*, 105398. https://doi.org/10.1016/j.clsr.2019.105398

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Tipton, H. F., & Krause, M. (2019). *Information security management handbook* (7th ed.). CRC Press. https://doi.org/10.1201/9780429192265

Verizon. (2022). *2022 Data breach investigations report.* Verizon Enterprise. https://doi.org/10.5281/zenodo.6604634

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide.* Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38,* 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Zhang, Y., Deng, R. H., Liu, J. K., & Zheng, D. (2018). Efficient and privacy-preserving online medical primary diagnosis with outsourced support vector machine training. *Computers & Security, 79,* 1–12. https://doi.org/10.1016/j.cose.2018.07.013

Zimba, A., & Phiri, J. (2020). A taxonomy of cyber-attack vectors in the cloud computing ecosystem. *Journal of Cloud Computing: Advances, Systems and Applications, 9*(1), 1–23. https://doi.org/10.1186/s13677-020-00173-9