Allie Griffin
2148000

Introduction

Online pharmacies already face more information security issues than the average business. These modern-day remote healthcare providers not only handle and store customers' personal data but also handle sensitive information about medical records and prescriptions. It has also recently been discovered that illegal bots are being used to gain access to online pharmacy customers' accounts with the intent to resell their prescriptions.[1] Despite these numerous information security challenges, a study by Kuzma revealed that the majority of audited online pharmacy websites had critical or medium-level vulnerabilities.[2]

In addition to the vulnerabilities inherent to online pharmacies, the ambitious business merger and expansion plans outlined by WebMeds and Superb-Storez will open both businesses to a variety of new information security risks. First, any business merger or acquisition is a complex procedure, and security risks are abundant. Depending on the specific circumstances, data can become compromised during migration, human error can result in data breaches, old equipment can become misplaced, resulting in a security risk, and new vulnerabilities can be introduced during the development of new software or during changes made to existing software.[3]

The fact that the merger is taking place between international organizations complicates matters even further. Both businesses will have to ensure compliance with information security laws in the UK as well as the US. This process will need to be repeated during the three-year expansion plan throughout Canada and the EU. These laws become even more restrictive and important to follow when a healthcare business, such as WebMeds, is involved.[4]

Finally, the businesses are also planning two major data migrations over the next three years. The first is a migration of the main data center from the UK to the US. The second is a migration to a cloud data processing in Asia. Both of these moves open the business to potential data breaches and data corruption, depending on how the migrations are managed. There are also different factors to consider for hardware migrations versus cloud migrations.[5,6]

Information Security Management Measures

Merger

One of the most important parts of maintaining information security throughout a business merger is to catch vulnerabilities early so they do not compound after systems, data, and networks have already been combined. Each organization should complete a thorough audit of its own information security policies, standards, and processes. Any relevant security breaches should be made known and an evaluation of mitigation efforts should be made.

If any hardware or IoT devices are being moved, a thorough inventory should be made beforehand so the organization is aware of any lost and potentially compromised devices as soon as they go missing. Companies might consider disabling these devices' connection to networks containing sensitive data before they are physically moved, as well.

With a merger comes a brand new workforce with sometimes conflicting training and habits. A companies-wide information security training plan should be put in place for all employees and contractors of both businesses. This can help mitigate human-error vulnerabilities that might be introduced. This is especially important for software developers and others with a direct hand in managing sensitive data. It could be helpful for the companies to appoint a security program manager to oversee international operations and maintain good relations with the workforce and clients.[7]

Expansion Throughout the US, UK, Canada, and EU

In addition to planning a large-scale merger, WebMeds and Superb-Storez will be expanding both businesses throughout the US and UK, at first, and Canada and the EU in the next three years. Expanding businesses internationally comes with a unique set of information security challenges.

The first is to maintain consistency throughout the expansion project. A solid set of organization-wide information policies should be put in place and followed throughout the entire process. All existing employees and new hires should be trained thoroughly and security-focused executives should be put into place to oversee each branch of the expansion.

Special attention should be given to software developers creating or expanding additional applications throughout the internationalization process. A prescriptive secure software development lifecycle plan should be followed throughout. Some examples of policies that should be implemented include providing security education and awareness to all employees involved in software development and incorporating security into the planning, requirement analysis, architecture and design, implementation, testing, release, deployment, and maintenance of all software.[8] This includes taking into account the technical specifications required by each country and area of expansion.[7]

Finally, a unique challenge of overseas expansion is the introduction of countless new laws and regulations that need to be followed with respect to information security. The initial expansion to the United States, for example, will require compliance with both federal and individual state security laws, as well as compliance with the Health Insurance Portability and Accountability Act, which is applicable to all companies with access to patients' medical records.[4] Other laws and regulations specific to Canada and the EU states will also become relevant in the three-year expansion plan.

New Headquarters and Data Center Initially in the US

Because WebMeds intends to move its headquarters and data center to the US initially, the company will have to consider how to complete the data migration without compromising its customers' information. The types of information security issues that may arise depend on how the company chooses to change location.

WebMeds will have three options when changing the location of its data center: physically move its current servers from the UK to the US, move the current applications from one hardware to another, or convert the physical machine to a virtual machine.[5] After the hardware has been changed, the company will need to synchronize the data to the new servers. Potential risks include losing data, data corruption, hardware loss, hardware damage, vulnerability to data breaches, and extended downtime for the company's online services. Ensuring that the applications and data are securely backed up before they are moved and employing proper encryption techniques are essential to mitigating the security risks involved.

Another consideration for WebMeds is the UK GDPR requirements for transfers of personal data outside the UK. The UK government requires companies to protect its citizens' personal data throughout all data transfers. The company should take care to follow these rules throughout the data migration process.[9]

Data Migration to Cloud Providers in Asia

After the initial data transfer to the US, the organizations will need to make a new information security risk mitigation plan for the move to cloud providers in Asia. Depending on their current goals, the organizations can move their applications as they are, change, rebuild, or refactor the applications for the cloud, or build entirely new cloud-based applications.[6] No matter what the method is, the software developers will need to ensure a compliance- and security-based development process to maintain the integrity of the applications and the migrated data.

Some prevalent security risks that might arise during cloud migration include the exposure of sensitive data to attack, the exposure of unsecured development environments to malevolent actors, expansion that outgrows current security measures, and data loss.[6] Using encryption, backing up data, and weaving information security practices into the software development lifecycle can mitigate these vulnerabilities. Choosing the correct cloud provider is also essential because the organizations will have to rely on the provider for compliance and security standards.

Information Security Policies

Secure Software Development Policy

Purpose

This policy is intended to set forth a standard for a Prescriptive Secure Software Lifecycle Process that will be used to create secure and compliant software.[10,11]

Scope

This policy applies to all WebMed and Superb-Storez employees and contractors.

Education and Awareness

- Make the entire development team aware of potential attackers' goals and techniques.
- Provide consistent education around secure development practices, including security tools and secure programming languages.
- Provide product managers, program managers, engineers, and developers with ongoing cybersecurity training.

Project Inception

- Define metrics and compliance reporting to hold the team accountable for minimum acceptable levels of security.
- Define cryptography standards to ensure proper use before implementation.
- Use the latest versions of organization-approved tools with the proper security checks and settings enabled.

Analysis and Requirements

- Define and continually update security requirements in line with functional requirements, compliance requirements, standards, and the current security environment using the System Quality Requirements Engineering (SQUARE) process.[12]
- Perform threat modeling and enumerate threats by considering each system component in relation to STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) threats.[8]

Architectural and Detailed Design

- Establish architectural and design requirements that are informed by the security requirements and enumerated threats discovered in the Analysis phase.

Implementation and Testing

- All developers must follow the OWASP Secure Coding Practices Guide.[13]
- Perform static and dynamic analysis security testing throughout project implementation and after integration.
- Perform penetration testing on the finished application to discover unknown security vulnerabilities.
- Use cryptography standards to encrypt and protect sensitive data.
- Manage the risk of using third-party components by maintaining an inventory of currently used third-party components and consistently testing these components for vulnerability.

Release, Deployment, and Support

- Establish a standard incident response that includes contacts in case of emergency, a protocol for vulnerability mitigation, a plan for customer communication, and a plan for quickly deploying solutions.

Data Backup and Disaster Recovery Policy

Purpose

The purpose of this policy is to set a standard for backing up and recovering data in the event of an emergency.[14,15]

Scope

This policy applies to all WebMed and Superb-Storez employees and contractors.

Backup Procedures

- Make a daily list of all changed objects in working libraries and directories.
- A complete save of the entire system is done daily.
- All critical business data will be backed up to an off-site location on a daily basis.
- All personal computers used for company tasks should be backed up once per day.
- All backup data will be encrypted following the organizations' encryption policy and local regulations.

Data Storage

- If data is backed up to the cloud, the cloud provider must have security, encryption, and restore capabilities that are in line with the organization and compliant with relevant regulations.
- If data is backed up to removable hardware, the hardware must be kept in a secure area and access must be given only to those who are authorized.

Versions and Data Retentions

- A minimum of five previous versions of critical business data will be retained for at least 30 days in the event of a major change in the data.
- Compliance with data retention regulations will be maintained based on each business location's jurisdiction.

Disaster Recovery Procedures

- A disaster action checklist containing initial actions to take following a disaster will be continuously maintained.
- Recovery startup procedures will be defined for use after an event such as a natural disaster, equipment failure, or fire.

Testing

- Perform semiannual testing of the organization's ability to restore data from backups.
- An up-to-date checklist for testing the data recovery process will consistently be maintained.

Conclusion

The example information security policies outlined in the previous section are just two of many policies necessary to help WebMeds and Superb-Storez maintain information security standards throughout their merger, expansion, and data migration plans. They provide a good start to meeting the ISO 207001 requirements for organizational information security policies, for example.[16]

Both of the policies fit into the ISO 207001 section on operational security. Many more policies would need to be written to meet security requirements covering security organization, human resource security, asset management, access control, cryptography, physical and environmental security, communications security, system acquisition, development, and maintenance, supplier relationships, incident management, business continuity, and compliance.[16]

Separate policies would also need to be written in regard to an increasingly remote workforce. The introduction of remote workers across the world produces compounded security vulnerabilities, and proper employee training and device maintenance should be put in place to mitigate those risks. The development of secure internal software and tools could also be beneficial in protecting remote workers.[17]

A final recommendation for WebMeds and Superb-Storez would be to appoint a Chief Security Officer or similar executive to oversee security operations for both businesses throughout the upcoming changes. The executive would see to incorporating security throughout the day-to-day operations of the business as well as maintaining business continuity in times of

growth. This top-down approach to security would ensure that responsibility is taken for security risk mitigation, compliance, and legal requirements for both businesses.[18]

References

1. Hagen, J. (2022, September 5). *The discovery of a new and compounding cybersecurity threat to pharmacies*. https://pharmaphorum.com/views-and-analysis/the-discovery-of-a-new-and-compounding-cybersecurity-threat-to-pharmacies/
2. Kuzma, J. (n.d.). Web Vulnerability Study of Online Pharmacy Sites. *University of Worcester Research and Publications*. https://core.ac.uk/download/pdf/49595.pdf
3. The Role of Cybersecurity in Mergers and Acquisitions Diligence. (2019). In *Forescout*. https://www.forescout.com/resources/cybersecurity-in-merger-and-acquisition-report/
4. Harroch, R. (2018, November 11). *Data Privacy And Cybersecurity Issues In Mergers And Acquisitions*. Forbes. https://www.forbes.com/sites/allbusiness/2018/11/11/data-privacy-cybersecurity-mergers-and-acquisitions/?sh=77687c9a72ba
5. Townsend, K. (2014, October 23). *3 risk factors and strategies when managing data center migrations*. TechRepublic. https://www.techrepublic.com/article/3-risk-factors-and-strategies-when-managing-data-center-migrations/
6. *Security risks of cloud migration*. (2022b, May 24). Infosec Resources. https://resources.infosecinstitute.com/topic/security-risks-of-cloud-migration/
7. Tom Echols, VP of National and Global Accounts at STANLEY Security, Tyler Jordan, Founder and CEO of Jordan Digital Marketing, Doers, W. E. F. C. &. P. D. A., & Doers, W. E. F. C. &. D. P. B. A. (2020, November 10). *5 Security Factors to Consider When Expanding to Global Markets*. Crunchbase. https://about.crunchbase.com/blog/5-security-factors-when-expanding-to-global-markets/
8. Laurie Williams. (2019). Secure Software Lifecycle Knowledge Area Issue 1.0. In Andrew Martin (Ed.), *CyBOK*. National Cyber Security Centre. https://www.cybok.org/media/downloads/Secure_Software_Lifecycle_issue_1.0.pdf
9. *International transfers*. (n.d.). ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/
10. *Software Development Life Cycle (SDLC) Policy | Division of Technology Services*. (2022, October 13). https://dts.utah.gov/policies/software-development-life-cycle-sdlc-policy
11. Irwin, L. (2022, February 25). *How to create an ISO 27001 secure development policy – with template*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/how-to-create-an-iso-27001-secure-development-policy-with-template
12. *SQUARE Process | CISA*. (n.d.). https://www.cisa.gov/uscert/bsi/articles/best-practices/requirements-engineering/square-process

13. *OWASP Secure Coding Practices-Quick Reference Guide | OWASP Foundation*. (n.d.). https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content
14. *Cyber Security Policy and Procedures*. (n.d.). Intact Public Entities. https://www.intactpublicentities.ca/centre-of-excellence/cyber-security-policy-and-procedures
15. *Backup and recovery*. (n.d.). https://www.ibm.com/docs/en/i/7.3?topic=management-backup-recovery
16. Irwin, L. (2022b, October 26). *ISO 27001 Annex A controls explained*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained
17. Personnel Security Guidance on Remote Working. (2012). In *Centre for the Protection of National Infrastructure*. https://www.cpni.gov.uk/resources/personnel-security-remote-working-good-practice-guide
18. *Chief Security Officer (CSO): Definition, Requirements, Duties*. (2022, November 7). Investopedia. https://www.investopedia.com/terms/c/cso.asp