Global Journal of
Information Technology:
Emerging Technologies

Volume 13, Issue 1, (2023) 01-06

www.gjit.eu

Information Security for Small Business Course Proposal and Design

Wenjuan Xu[a]* School of Integrated Traditional Chinese and Western Medicine, Binzhou Medical University, Yantai, Shandong 264003, P.R. China. wxu@frostburg.edu
Lei Ye [b]* School of Integrated Traditional Chinese and Western Medicine, Binzhou Medical University, Yantai, Shandong 264003, P.R. China.lye@frostburg.edu

Suggested Citation:
Xu, W. & Ye, L. (2023). Information Security for Small Business Course Proposal and Design. *Global Journal of Information Technology: Emerging Technologies*. *13*(1), 01-06. https://doi.org/10.18844/gjit.v13i1.8495

Received from; October 12, 2022, revised from; January 24, 2023 and accepted from February 11.
Selection and peer review under responsibility of Assoc. Prof. Dr. Ezgi Pelin YILDIZ, Kafkas University, Turkey.

Abstract

These days small businesses deploy different information systems to be more competitive and efficient, at the same time, which leads to different cyber attacks. To reduce the possible infrastructure damage and financial loss, business owners need to be aware of and recognize these various attacks, and know how to reduce or prevent them. In this paper, to help with the local small business owners, we propose an information security course especially designed for educating the business owners in cyber security for small business-related fields. This paper examines the course design details including the course structure, main contents, different exercises and main challenges.

Keywords: Entrepreneurship, Small Business, Business Owner, Cyber Security, Cyber Attack, Information Technology

*** ADDRESS FOR CORRESPONDENCE:** Wenjuan Xu[a]* School of Integrated Traditional Chinese and Western Medicine, Binzhou Medical University, Yantai, Shandong 264003, P.R. China. *E-mail address*: wxu@frostburg.edu

1. Introduction

E-entrepreneurship is creating a new business with information technology involved. Kollmann's work [1] mentions that information technology can make the business more successful and thus very important. However, with the different threats and cyber attacks happening, it is essential to ensure the information technology is secured and protected. For example, the attacker can try to extort money, act fraud, destroy data and systems, and so on. To overcome these attacks, companies built different security infrastructures to protect their data and systems.

On the other hand, with the development of information technology, currently, small businesses can use a lot of information technology used by large corporations before. As a result, the small business is also facing the attack that the large corporation has. As stated in the small business trend [2], 61 percent of companies experienced a cyber-attack incident in 2019, going up from 45 percent in 2018. As related, the small business is reported to have been as vulnerable as large enterprises. According to a 2019 Verizon report [3], 43 percent of the data breaches target small businesses. However, a normal small business cannot afford the time, security infrastructure, and money compared to the large companies for protecting the data from cyber-attacks. On the other hand, small businesses need more effort to earn customer trust and especially if the cyber-attack influences consumer data and can potentially impair the business reputation. Hence, it is critical to offer support to small business owners in the cyber security field.

The author's local area Allegany County in the state of Maryland has a population exceeding 280,000 people, with the entrepreneurial spirit alive, and well respected. Two main cities, Cumberland, and Frostburg, all have incentives for those interested in making their dream of business ownership or self-employment a reality. There are organizations and grants available for business owners. For example, the Department of Defense's Small Business Innovation Research (SBIR) [4] provides different grants to stimulate technology innovations. Maryland Small Business Development Center (SBDC) [5] offers consulting and other resources to help the small business owners establish commerce. Also, Tri-County Council for Western Maryland [6] is a regional economic development organization representing Allegany and two other counties. They offer help with business development efforts and direct business to state and federal for getting resources to set up a new business or expanding the business.

Other than the different organizations for business support, Frostburg State University [7] located in Frostburg is a high education institution offering a lot of support to the local enterprises including seminars and business conferences. Frostburg State University has successfully partnered with Allegany County to develop the infrastructure for the Allegany Business Center technology park [8], which includes 56 acres dedicated to the development of a technology business park. Several businesses currently operate out of the facility. In addition, at Frostburg State University, the college of business provides a wide range of degrees and courses in business, marketing , and finance-related fields. On the other hand, the Department of Computer Science has a strong information security undergraduate program.

With all these different small business development resources in the local area and the necessity of cyber security awareness for the small business owners, we are going to design and offer a general E-entrepreneurship cyber security course for the current and future small business owners to be more prepared and successful. The course will cover critical elements in information security and how to implement this security in the business field. Successfully finishing this course will get a certificate in small business cyber security.

The paper is organized as follows. In Section 2, we will introduce the related business security standards. In Section 3, we will introduce the course design with details. Finally, we will discuss and summarize our work in Section 4.

2. Related Work and Security Standard

In general, there are two main security standards used by e-businesses for assuring information security including ISO 27001 [9] and PCI DSS[10].

2.1 ISO 27001 for Small Business---- is the international standard about best practices for the information security management system. It covers the different security aspects for small businesses to achieve better security and in sequence gain competitiveness.

· Information security policies: The organization’s top management defines the mandatory documents for the leadership and commitment to the information security management system.

· Organization of information security: Establish a management framework for initiating and controlling the organization's security implementation and functioning.

· Human resource security: Ensure the employees and contractors understand the responsibilities.

· Asset management: Asset inventory management for auditors and stakeholders.

· Access control: Limits access to information and prevents unauthorized access through a series of controls.

· Cryptography: A set of security practices to ensure proper and effective use of cryptography to protect information.

· Physical and environmental security: Prevent unauthorized physical access and damage to the organization's information and facilities.

· Operational security: To ensure correct and secure operations of information processing.

· Communications security: this mainly includes network security and information transfer

· System acquisition, development, and maintenance:

· Supplier relationships: Assure the security of the valuable assets that are accessible or affected by the suppliers.

· Information security incident management is to manage, record, and analyze the security threats or incidents.

· Information security aspects of business continuity management: Information security continuity should be covered in the business continuity management system.

2.2 Payment Card Industry Data Security Standard (PCI DSS) is the standard that the business owner needs to follow when processing credit card transactions. PCI DSS enables trust between the consumers and the business involved when handling the payment with a credit card. Depending on the number of card transactions, PCI compliance has four levels. Normally the small business belongs to level 4, which has fewer than 20,000 card transactions per year. PCI DSS provides different specifications for the framework, tools, measurements, and other related supporting resources for helping the business securely handle the transaction, which gives the business owner support.

3. Enterprise and Cyber Security Course Design

This course will be designed as a case study leading course. We will deliver the contents with rich examples and real-life cases. In the following, we explain the course design from various aspects.

3.1 General Course Design

§ **The Emphases and Expectations:** In this class, we will have these course objectives.

o Define what cyber security is and its importance in small businesses.

o Introduce security policy and identify several types of information that need to be secured in the business.

o Identify the diverse types of cyber threats such as malware, data theft, website tampering, email phishing, etc.

o Explain the risk management in the business.

o List best practices for guarding against cyber threats.

Following these course objectives with the case studies from industry, students will not only learn important knowledge in information security, but they will also learn how to protect their small businesses with the corresponding project accompanying.

· **Audience:** The audience of the course will be university students or local small business owners, or people worried about cyber safety.

· **Delivery Format:** This course will be delivered online to suit the various needs of the different people.

3.2 Structure

The total course length is 15 weeks. Following the course objectives, we will cover topics including what cyber security is, why it is so important, what is security policy, and what are common cyber threats and crimes in business? And how do I determine my level of risk and how to protect my business?

Corresponding to these different topics, we will have lectures, case studies, invited talks, and students' presentations. The students who take this course successfully will have a certificate.

3.3 Context and Resources

Instead of using textbooks for this course, we provide current reading materials corresponding to the topics. We will use some of the reading materials from cyber security organizations including the National Institute of Standards and Technology (NIST) [11], and the Department of Homeland

Security (DHS) [12]. Especially NIST has different documents such as security policy [11], cyber security framework [12], etc. Some of the materials will come from ISO 27001 and PC-Dss. In addition, different states have information security guides for small businesses [13]. We will also supplement some materials from the book [14] and online paper [15][16][17] to adapt to the newest cyber security and business trend.

3.4 Exercises

To make sure the students understand the course objectives, students need to finish the work as follows.

- For each topic, we will have multiple-choice questions-based homework for the students to understand the materials.
- Students need to be active in the course discussion with the corresponding topics.
- Students will practice different security techniques for protecting a business.
- Students have a semester project working on corresponding to the topic and will present the work at the end of the semester. The project will work on the following aspects to fit their business requirements.

o Perform information security needing analysis for their business needs.

o Identify the important resources in the business

o Conduct the risk assessment of the business and assess the cost of cyber attack

o Create a plan about how to protect your information.

o Details about implementing the plan include information security policy, training, hardware, and software.

4. Discussion and Conclusion

In this paper, we have already introduced the local small business and the cyber security challenge, and the necessity of education support for small business owners. We explain our course design with the related objectives, contents, and related work. Soon, we will apply for certain grants related to this work for promoting the course support, submit applications for the course development, and advertise the course to the local community.

References

Kollmann, Tobias. “The Information Triple Jump as the Measure of Success in Electronic Commerce.” Electron. Mark. 8 (1998): 44-49.

Small Business Trend: https://smallbiztrends.com/2019/09/rise-in-cyber-attacks-small-business.html

2019 Verizon report: https://www.verizon.com/business/resources/reports/dbir/2019/results-and-analysis/

Department of Defense's Small Business Innovation Research (SBIR): https://business.defense.gov/Programs/

Maryland Small Business Development Center (SBDC) https://www.marylandsbdc.org/

Tri-County Council for Western Maryland: https://www.tccwmd.org/

Frostburg State University: www.frostburg.edu

Allegany Business Center technology park https://alleganyworks.org/industry-sectors/advanced-manufacturing/

ISO 27000 for small business: https://www.iso.org/isoiec-27001-information-security.html

PIC-DSS: https://www.pcisecuritystandards.org/

Maine government information security guide for small businesses: https://www1.maine.gov/ag/docs/Small-Business-Cyber-Security-Guide.pdf

D Kosutic: Book: Secure and Simple: A Small-Business Guide to Implementing ISO 27001 On your ownPaper1: information security for small business: http://infosecwriters.com/text_resources/pdf/Information_Security_for_Small_Businesses.pdf
Example class transcript: https://www.sba.gov/sites/default/files/cybersecurity_transcript.pdf
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf