Wendy C. Valenzuela Figueroa

IT-415-J3283 Advanced Info Systems Design 22EW3

Alexandre Lazzo

7-2 Final Project Prompt I Submission: Project Proposal

02/20/2022

Problem Statement

Employee onboarding at F-SECURE headquarters does not involve or provide cybersecurity training on phishing attacks. In the last year, threatening actors (anyone with access to protected, unsecured assets) or internal security issues compromised corporate confidentiality, including, but not limited to the following instances/events:

- ✓ Employees intentional, maliciousness or inadvertent destruction of corporate information.
- ✓ Disruption of services.
- ✓ The practice of carelessness when utilizing firm electronic systems and other assets.
- ✓ Lack of understanding of security procedures or the utilization of information systems.

Furthermore, the company's careless cybersecurity awareness training offers little defense against the following:

- ✓ The importance of passwords, access credentials, and the importance of secure network connections.
- ✓ The Employees were unaware of a shaky network connection, passwords, and precautions.
- ✓ Between 1990 and 2020, 200 users were easily duped into disclosing passwords, credit card numbers, data, or other personally identifiable information.
- ✓ When using Bring Your Own Device (BYOD) devices, attackers had entry points to connect to workplace networks and corporate access data.

Enforcing cybersecurity knowledge across all levels and departments in enterprises has become a must. It starts with the right training program for each employee to protect corporate data. Securing the company's corporate data requires enforcing a cybersecurity awareness training program. Everyone now should be concerned about cybersecurity. (E-Science Direct, n.d.)

Significance

Employees are educated about the cyber security landscape through Security Awareness Training. Security Awareness Training uses a variety of learning methodologies to improve awareness of cyber security dangers, lower the risks associated with cyber-attacks, and cement a security compliance culture in the firm. (E-Science Direct, n.d.)

Failure to secure information can result in the loss of a job, financial ramifications for the company, harm to people whose private data are revealed, and possibly legal and criminal fines. (E-Science Direct, n.d.) The following will be enforced as part of security awareness training:

- ✓ Create a shift in employee thinking and behavior change to improve organizational resilience against cyber threats.
- ✓ Encourage participation and dedication to cyber security activities.
- ✓ Boost audit findings and show regulatory compliance.
- ✓ Minimize security risks by reducing human mistakes. (Karl, 2021)

The company must combat malevolent intent by educating on frequent dangers. Furthermore, a thorough cybersecurity awareness training program reduces the danger of security threats and frees up time for the IT department by preventing cybersecurity breaches. (Karl, 2021)

Because training is frequently forgotten, a security awareness program should be ongoing. People are increasingly under pressure to boost productivity, so they view security as time-consuming and inconvenient, and they hunt for methods to get around it. Even if they are not under duress, most individuals forget to follow procedures and norms unless reminded regularly. (Karl, 2021) Any security and risk management strategy should include "security awareness" training for the broader employee population. (Karl, 2021)

Educating its employees is the most robust approach to protect a corporation against malware attacks, phishing frauds, and unsafe URLs. Many data breaches, according to research, are simply the result of workers' inability to spot a malware attack, unknowingly aiding hackers in their schemes. (Karl, 2021)

Objectives

Before being permitted access to the system, all individuals and contractors engaged in the administration, usage, or operation of the company's computer system must get periodic training in computer security awareness and recognized computer security practices. The user should also be taught to seek help if they have difficulty utilizing the system and report security issues. (Karl, 2021)

The following are the project's goals:

- ✓ Security Awareness Training Policy sign-off.
- ✓ Phishing awareness training
- ✓ Phishing training detention.
- ✓ Workstations best practices.
- ✓ Complex/strong passwords use, maintenance and disposition:
    - ➢ Requirements for using unique passwords:
        - Include a variety of character kinds, including upper- and lowercase letters, numerals, and symbols.
        - Are at least eight characters in length (longer is even better).
        - Include no portion of a username or email address.
        - Do not contain dictionary words.

- The password aging process requires users to update their passwords regularly (every 30 days).
- Keep a record of password history to prevent re-use.

- ✓ Social engineering evaluation.
- ✓ Insiders Thread identification and correction.
- ✓ Proper confidential data disposition.
- ✓ Physical security of the facility assets.

Deliverables

Security awareness refers to an organization's members' understanding and attitude toward the security of the organization's physical and, more critically, information assets. This project aims to mandate formal security awareness training for all employees/contractors/internal or external customers when they start working at F-SECURE and regularly after that (usually annually). (Karl, 2021)

Topics addressed in security awareness training are:

- ✓ Trade secrets, privacy issues, and government classified information are examples of sensitive material and physical assets they may come into touch with.
- ✓ Employee and contractor non-disclosure agreements process.
- ✓ The company's minimum requirements for correct physical handling of sensitive material.
- ✓ The proper methods for safeguarding sensitive data on computer systems.
- ✓ Password user requirements and the usage of two-factor authentication.
- ✓ Identification and management of malware, phishing, social engineering, and other computer security threats.

- ✓ Workplace security awareness training, including building access, security credentials, incident reporting, and prohibited items.

Additionally, a Web-Based training program will be selected and implemented for training delivery and compliance. The Security Awareness Training policy is, but not limited to, the training content for the Web-Based Training program.

Methodology

For this project, two Agile techniques, Kanban and Scrum, were examined, compared, and contrasted. The Kanban approach was used for this project's execution. Kanban is a flow-based system that allows the team to reprioritize incoming work regularly, adapting to recent changes much more swiftly without impacting the project schedule, cost, productivity, stakeholder motivation, or quality. (Pluralsight, 2019)

Kanban's significant benefit is its simplicity, as it is exceedingly simple to grasp and use. Its adaptability makes it simple to incorporate into current processes seeking the simplest method to transition to an agile workflow. Kanban teams do not have to be cross-functional to be effective. Kanban teams are frequently made up of smaller, specialized teams, such as an engineering team, a testing team, and an operations team, each in charge of a different part of the Kanban board. (Pluralsight, 2019)

Scrum is one of the most extensively utilized agile methodologies today. Scrum is a "framework" since it provides a simple project management structure to combine daily development operations. Scrum does not prescribe any specific development approaches instead of enabling the most appropriate practices for the team. (Pluralsight, 2019)

Scrum Teams, unlike Kanban, bundle their work into set timeframes called "sprints." Sprints usually last two weeks, although they can run anywhere from one to four weeks. Scrum inhibits altering the team's direction after a sprint has begun, which is one disadvantage. The teams must wait for at least the duration of a sprint, which is typically two weeks, before shifting their focus and goals. (Pluralsight, 2019)

A two-week delay before a modification may not be an issue for this training project's teams working with a solid release plan. Two weeks is unthinkable for the Information Technology and Human Resources teams, whose objectives change daily, so the Kanban technique is the best match for this project. (Pluralsight, 2019)

Risks

For this project, a qualitative risk analysis was employed. Qualitative risk analysis is more subjective than quantitative risk analysis because of the nature of identified risks; hence it is not being used for risk categorization on this project. The qualitative analysis was chosen because it focuses on identifying risks to evaluate the likelihood of a particular risk event occurring within the project life cycle and its impact on the overall schedule. (Project-Management.com, 2021)

The risks listed below have been prioritized based on their likelihood and potential impact on this project:

Risk 1: Change Control clearance is not received within the given period.

Risk 2: The Project Charter will not be approved within the given period.

Risk 3: Creating and publishing a Gantt chart within the allowed period.

There is a chance that getting project sponsors and stakeholders to sign off on deliverables will take longer than expected. This decision delay will impact the progress schedule.

To keep the project on track and deliverables on time, the project deliverables approval procedure must be completed in the allocated period. Delays in the approval or distribution of any deliverable may irritate customers, raise costs, increase risk, or alter resource allocation. For example, the Change Control approves the Project Charter's beginning, which includes stakeholders, project goal, and reason for requesting money and support; hence, delays in its approval cause delays in the project's start, scope, plan, budget, and resource allocation. (Project-Management.com, 2021)

The origination of the Project Charter is a dependence influenced by not accepting a Change Control; therefore, its delay in acceptance implies the project cannot start, the budget is not allocated or approved, resources are not reasonable, and there is no high-level scope supporting the project launch. As a result, the possibility of not having a project at all is genuine. (Project-Management.com, 2021)

If this risk is not handled, it will have ramifications for the project in terms of the triple constraint as follow:

- Cost: The offered project will not begin if the Project Charter is not approved within the specified period. A budget or financial allocation does not support the project's cost and resources.

- The primary document that sets the project in motion is The Project Charter. Delays in its approval have a detrimental influence on the project's timeline, planning, and effort to produce it on time and budget.
- Scope: Delays in Project Charter approval harm the project because it includes a high-level scope description required to develop the Scope Management Plan, Work Breakdown Structure, Requirement Documentation, Project Management Plan, and other necessary documentation that contribute to the project's success and on-time completion.
- Delays in Project Charter approval may have an impact on product quality because if the document is not approved within the allotted time, scheduled work will have to shift, putting pressure on stakeholders to complete deliverables in a shorter period, jeopardizing product quality and leading to customer complaints and unnecessary product rejects. (Project-Management.com, 2021)

Risk Mitigation:

A concise but persuasive rationale of a change is necessary to approve project deliverables effectively. The keys to a successful project deliverable approval and on-time delivery are justification and the correct approvers. (Team Asana, .2021)

The mitigation method will benefit the project by reducing implementation delays by choosing only trained individuals affected by the change for project deliverable assessment and approval. The RACI Chart, also known as a Responsible, Accountable, Consulted, and Informed Chart, is an important document that should be utilized to accomplish project deliverables. A RACI chart will help identify which stakeholders are accountable for delivery

approval and adherence to the project schedule's planned document release. (Project-Management.com, 2021)

The Change Control document is the optimum course of action to release the project and its deliverable. Having a reason for launching a Project Charter will offer the scope, project objectives, and other relevant project justification and business needs, allowing it to be approved more quickly. Furthermore, a well-defined RACI chart identifies just the stakeholders or department owners affected by the modification, and the project timeline identifies the period given for approval. With these technologies in place, the possibility of delivery approval delays is reduced. (Team Asana, .2021)

References

A. (2021, June 4). What Is a Change Control Process? (with Example Change Log) •. Asana. Retrieved January 23, 2022, from https://asana.com/resources/change-control-process

E-Science Direct. (n.d.). Security Awareness Training - an overview | ScienceDirect Topics. Retrieved January 23, 2022, from https://www.sciencedirect.com/topics/computer-science/security-awareness-training

F-SECURE. (n.d.). Why is Phishing still a problem? | F-Secure. Retrieved January 23, 2022, from https://www.f-secure.com/us-en/consulting/our-thinking/why-is-phishing-still-a-problem

Karl, T. (2021, October 7). The Importance of Cybersecurity Awareness for All Employees. United Training. Retrieved January 23, 2022, from https://unitedtraining.com/resources/blog/the-importance-of-cybersecurity-awareness-for-all-employees#:%7E:text=Educating%20employees%20on%20common%20threats,time%20by%20avoiding%20cybersecurity%20breaches

Pluralsight. (2019, July 10). Scrum vs Kanban. Retrieved January 23, 2022, from https://www.pluralsight.com/blog/software-development/agile-development-tips?b2b=true

Project-Management.com. (2021, December 21). Types of Risk in Project Management. Retrieved January 23, 2022, from https://project-management.com/types-of-risk-in-project-management/

Safran Software Solutions AS. (n.d.). An Introduction to Qualitative Risk Analysis | Safran. Retrieved January 23, 2022, from https://www.safran.com/content/introduction-

qualitative-risk-analysis?hsCtaTracking=a701b623-b1a2-4fa3-ac01-da5e106aad50%7C4d2c84e1-d9a2-4a46-9d69-082115214512