People and Risk

Robert Forto

School of Business, Liberty University

BMAL 714

Dr. Daniel Rogers

April 18, 2021

Authors Note

By submitting this assignment, I attest this submission represents my own work and not that of another student, scholar, or internet source. I understand I am responsible for knowing and correctly utilizing referencing and bibliographical guidelines.

Abstract

People are the key to an organization's success, and they can be its most important asset, they can also be a liability. People and risk have a long history of complexity when it comes to organizations and their behavior. This paper will examine information technology and how it has allowed organizations to cut costs, conduct more in-depth market research and build rapport with customers and clients, thus building stronger relationships. While this technology offers great rewards and opportunities, it also presents news risks and concerns for those in a position to take advantage of it. Dog Works Training Company, a small, family-run firm, is in the process of onboarding staff for the first time, and this paper will examine what risks are presented, their impacts, and mitigating factors that are recommended to be implemented.

The recommendations for the organization come from a review of the scholarly and biblical literature, and a risk management matrix was tabulated along with several activity and security controls. This plan will allow consideration of governance, strategic planning, and discussion while also allowing specific gaps to be identified in the chosen industry. While it is impossible to eliminate all risk in an organization, having comprehensive policy and procedure protocols in place will allow the company to mitigate any threats and, in turn, protect its assets moving forward.

Keywords: risk management, people and risk, risk mitigation, insider threat, information system, information security, intellectual property

Introduction

Information technology is crucial in the business world today. Everything that a business is involved in revolves around technology and access to the information that it provides. The use of technology has allowed organizations to cut costs, conduct more in-depth market research and build rapport with customers and clients, thus building stronger relationships. While this technology offers great rewards and opportunities, it also presents new risks and concerns for those in a position to take advantage of it. Organizations must develop security protocols to mitigate these risks and have the ability to monitor them and thwart the probability of potential threats and attacks. By creating such a risk management plan, the business can assess the likelihood of any attacks and the success of those attacks on the information that the organization holds. This plan can also evaluate the probability of the cost of any successful attack. Once a security breach is known, the organization's leadership must choose the correct countermeasures to offset the likelihood of an attack. The administration must consider if these attacks come from outside the organization or within from their employees by conducting thorough research.

The Organization

For this paper, a family-owned business, Dog Works Training Company, has taken steps for the first time to hire sub-contractors. Over the past twenty years, the company has been a closely held business with just the family working with their clients and keeping their proprietary training programs in-house. The business owners have invested a lot of time and money in developing a training program that is much different than what other companies in the industry are offering. The business owners consider this program’s protocols, including the client onboarding process, developing an individualized training plan, and its personality profile, one of the organization’s most valuable assets and a form of intellectual property.

Through this writing exercise, the business will better understand the relationship between people, risk, and security. If an insider or external threat is imminent, and how to best reduce the probability of an attack on the organization’s intellectual property. These threats could come by way of fraud, security practices, data, and security systems, or from theft of confidentiality, commercially valuable information, the theft of intellectual property, or the sabotage of computer systems (Wright, 2017).

As noted, Dog Works Training Company has operated as a small, family-run firm for many years. Their aversion to risk is predicated partly by the potential loss of assets and privacy due to system breaches and the theft of their intellectual property. Organizations also risk damage to their established reputation, and that can lead to vast repercussions for the company, and it may take years for that to recover, if at all (Pettersen Gould, 2021). In Dog Works Training Company’s case, their information technology system is proprietary, and any breach of that from bad actors will constitute a threat. A security breach, even so much as a leaked dog training program plan to a competitor in the industry, could be astronomical. It is in the organization’s best interest to protect and safeguard the company's information.

A company must consider many things when building a risk management plan requiring information technology. Intellectual property, proprietary information, and policies and procedures for employees and contractors are just a few. When considering all of these, the focus must be on people. As Park (2018) suggests, people are the ones who will commit acts against any of these areas of probable attacks. Even though Dog Works Training Company is small, the efforts to hold their intellectual property close is just the same as a much larger firm. Wright (2017) talks about espionage being on a large scale, but it can occur in a family-run firm with just a few employees. Employees or subcontractors have the opportunity to commit such acts and are more likely to have the ability to cover their tracks than would someone outside the firm. Proprietary information is a key component of Dog Works Training Company.

Elifoglu et al. (2018) posit as trusted employees or business partners, insiders are trusted to do what is in the best interest of an organization. Insider threats are caused by employees, contractors, or leadership that capitalize on the weakness in systems for financial or other types of gain. Management is ultimately responsible for the protection of the company's assets and intellectual property. Contrary to common belief, most insider incidents are not based on sophisticated hacker tools, and most threat incidents are the consequence of human actions, such as mistakes, negligence, greed, or reckless behavior (Elifoglu et al., 2018). According to Elifoglu et al. (2018), a risk management process and effective system of controls must be developed by organizational leadership. When it comes to informational security, consideration must be given to known risks regarding the organization's assets. All information must be identified, and a control system put in place to protect them. The conception, implementation, and operation of an integrated risk management system (RMS) must ensure ongoing monitoring of risk and integrate the risk response measures in a coherent risk strategy (Vasile and Croitoru, 2012; as cited in Rebelo et al., 2017).

Pettersen Gould (2021) postulates that as recently as 1990, professional concerns of risk analysts had an increased focus on people problems. Until then, research inside organizations focused largely on individual risk perception and ways to communicate about risks (Short, 1992; as cited in Pettersen Gould, 2021). It is sometimes difficult to predict why someone did something and what motivates them to do so. There is far too much indifference toward people regarding information security. In an increasingly more common digital age, it seems that there are new ways to implement attacks, so for a small firm to stay on top of information security is a challenge at best. Dog Works Training Company is no exception to attacks on their information system. They may not have a complex digital footprint, but what they do have is just as apt to a breach as a larger firm. One could argue even more so because they do not have the budget or the manpower to develop deliberate and sophisticated security protocols to manage any insider or external attack aside from commercially available tools that are easy targets.

Therefore, mitigating risks must remain at the forefront of organizational planning, and there will remain a constant need to educate employees and contractors of a company. Kou & Stewart (2018) discuss the need for a new approach. They suggest a group accountability model to educate staff and to get employees on board to follow the rules, and alert leadership to any suspicious activity. In this process, a group of collective individuals can be brought together to perform organizational tasks and whose workflow is characterized by interdependency and accountability (Kozlowski & Bell, 2003; as cited in Kou & Stewart, 2018). Using this process will allow this accountability by providing implicit and explicit expectations that a group's collective actions will be justified too, and evaluated by, an extremal audience with the ability to mete out consequences (Kou & Stewart, 2018). From a risk management standpoint, this expectation that all will be held accountable as a unit can be described as a state where group members collectively feel accountable for team behaviors (Kou & Stewart, 2018). Alas, employees and contractors can be the first line of defense in an information security protocol rather than the weakest link.

Risk Management Plan

The following is a risk management matrix that was developed for the project of outlining risk and mitigation factors regarding those involved in Dog Works Training Company. This matrix will look at three risks associated with the company adding subcontractors to their staff for the first time and how doing so adds to risks associated with people and risks to the organization.

Potential Risk	**Potential Impact**	**Mitigations**
Inadequate training and awareness	Lack of training means employees, contractors, and suppliers do not know the process of securing information, thus creating a weakness. At Dog Works Training Company, this weakness could come by sharing proprietary information, misuse of training materials, or failure/misuse of their onboarding process.	Develop a training program for everyone involved in the organization that results in group accountability at all company levels. Perpetually re-train employees and contractors. Dismiss those who ultimately fail to comply.
Inadequate security policy	Inadequate policies and procedures can lead to security breaches. Policies and procedures need to be the foundation of all operational facets of the company.	Security policies appropriately encompass all facets of creating a secure environment.
Inadequate privacy policy	Inadequate privacy policies can lead to the exposure of sensitive or proprietary information leading to operational and security risks. Irreparable reputation damage can result as well.	Privacy policy that adequately encompasses all facets of safeguarding access to private, sensitive, and proprietary information.

Dog Works Training Company should impose several activity and security controls to mitigate risks. There is a need for a perpetual risk assessment and mitigation plan to include potential threats or vulnerabilities. This will allow the organization to understand the full scope of their security controls instead of just the threats to the business. Secondly, the company should control, track and monitor all access to its assets. This includes proprietary information and other intellectual property as well as financial records and client information. The company should prevent unauthorized access to assets and have policies and procedures to enforce these protocols. Third, the organization should develop handling policies and accountabilities and repercussions, with the firm having the ability to act rapidly to cover any lost assets and continue business as usual after any breach of the company's information system. Lastly, the company should have a training plan to ensure that employees, contractors, and suppliers are to be held accountable for their actions. This training program should be implemented for everyone in the firm.

Conclusions and Recommendations

The bible is replete with many examples of great risk managers. Nehemiah 1 shows how Nehemiah's brother informed, "the walls of Jerusalem, has been torn down, and that gates have been destroyed by fire." In Nehemiah 2:1-10 (NIV), his response has his brother seeking the king's support of a mission to rebuild the walls. Ecclesiastes 4:12 (NIV) advocates strength in numbers and can apply to teams and organizations. Proverbs 21:15 (NIV) emphasizes that once an organization recognizes the threats, they must be diligent in planning for them. Otherwise, they may find themselves in a compromising position. Proverbs 22:3 shows clearly that the foolish fail to recognize risk, and the wise take adequate precautions to deal with the risk as they unfold proactively.

Wright (2017) postulates that an essential tool in managing risk and security is an explicit declaration of what is and want is not acceptable during business (p. 49). This code should detail the principles that an organization must follow to protect the organization’s standing with customers, clients, suppliers, and the community. This code should also include everyone involved in the organization, from the top managers to the subcontractors and suppliers. The organization's leadership must make it clear that employees, or in Dog Works Training Company’s case, subcontractors, are expected to operate at the highest ethical standards and uphold the company’s integrity when representing the firm in any capacity.

Dog Works Training Company must acknowledge that risks do exist. Doing so—especially to the point of discussing them internally requires managers to rely on their policies and procedures to work through issues that could lead to crisis, humiliation, or even loss. The organization must encourage transparency. Managers who are confident that their organizational policies and controls are acceptable can benefit from openness regarding risk and are more likely to share information that signal risk events and allow the business to resolve emerging issues long before they become a crisis. This means, in the Dog Works Training Company scenario, the firm needs to examine employment practices among subcontractors and make sure that they run congruent to its policies and procedures and share those practices with new contractors as they are brought into the company. This transparency will benefit both the company and the contractors and allow the firm to reallocate project tasks among contractors, thus reducing the company’s employment-practices risk and safeguarding project returns.

Dog Works Training Company must respect that risk exists. Most managers understand the need for controls to alert them to trends and behaviors they should monitor and better mobilize a response to an evolving risk situation. Even with proper monitoring, there can be difficulty controlling the risk that a company is susceptible to. Companies often celebrate a beat-the-system mindset, rewarding people who create new business, launch new projects, even if it means working around control functions to gain new clients. This workaround should be discouraged. Respect for the rules can be a powerful source of competitive advantage in the industry.

A company must understand that sustaining the right attitudes and behaviors over time requires continuing effort. This involves everyone in the firm. Managers are responsible for maintaining a risk culture that extends beyond those at the firm's top and includes everyone involved, including subcontractors and suppliers. It is recommended that an authentic leadership style, empowerment of and active engagement with those involved in an organization while focusing on continuous improvement can significantly mitigate risk (Love et al., 2016). Lastly, this risk management process does not need to be overly complicated. Having a policy in place will allow the organization to grasp what is acceptable and what is not by all people involved in the operation.

References

Elifoglu, I., Abel, I., & Tasseven, O. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. *Review of Business*, *38*(2), 61–73. https://search-proquest-com.ezproxy.liberty.edu/docview/2085003999?pq-origsite=summon

Kou, C., & Stewart, V. (2018). Group accountability: A review and extension of existing research. *Small Group Research, 49*(1), 34-61. https://10.1177/1046496417712438

Love, P. E. D., Ackermann, F., Carey, B., Morrison, J., Ward, M., & Park, A. (2016). Praxis of rework mitigation in construction. Journal of management in engineering, 32(5), 05016010.

New International Version Bible. (2011). The NIV Bible. https://www.thenivbible.com (Original work published 1978)

Park, W., You, Y., & Lee, K. (2018). Detecting Potential Insider Threat: Analyzing Insiders' Sentiment Exposed in Social Media. *Security and Communication Networks*, *2018*, 1–8. https://doi.org/10.1155/2018/7243296

Pettersen Gould, K. (2021). Organizational risk: "Muddling through" 40 years of research. *Risk Analysis, 41*(3), 456-465. https://10.1111/risa.13460

Rebelo, M. F., Silva, R., & Santos, G. (2017). The integration of standardized management systems: managing business risk. International Journal of Quality & Reliability Management.

Wright, L. (2017) People, Risk, & Security. Pan MacMillian Ltd.