Section 2: Week 5: Appraise Risk Analysis, Frameworks, and Models

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

May 3rd, 2020

North Central University

# Appraise Risk Analysis, Frameworks, and Models

Hi-Tech Manufacturing (HTM) operates electronic car assemblies plants across North America, Europe, and Asia. Their proprietary technologies provide a strategic advantage that international competitors desire to acquire. Since HTM has been unwilling to license these solutions, the business continuously fights forced acquisition across many battlefields. These arenas include targeted attacks against employees, social media smear campaigns, malicious assaults against the digital infrastructure, and espionage attacks against the physical plants. Additionally, internal sources create risks to the institution through a spectrum of malicious and negligent behaviors, such as an employee could interact with malware, and this spreads across the network. Team members might also lack security awareness and training, causing them to misapply safe equipment and processes. Regardless of the origin of the risk, organizations need to ensure their integrity, confidentiality, and availability, or it faces a disruption delivering their mission and objectives. Addressing these challenges requires a risk management framework that iteratively identifies, assesses, and then constrains the blast radius of decisions. Technicians will eventually fat-finger a database command, which controls prevents the cascade and revert the system to the previous state? These scenarios are a matter of ‘when-not-if,’ and choosing to acknowledge these issues upfront allows HTM to choose the battlefield. The approach to handling these concerns needs to a basis within academic and industry best practices. For instance, the Nation Institute of Standards and Technology (NIST) provides standards, such as ISO27000 and the Cybersecurity Framework. NIST’s guidance allows the institution to adopt different risk profiles so that the implementation is neither too hot nor too cold. After weighing the cost-benefits of acceptable risks, a formal review of those decisions needs to occur on a given cadence, ensuring those decisions are still valid.

# What influences risks to the Hi-Tech

When an organization begins with technological solutions, they are likely to devise incomplete protection strategies (Stevens, 2018). Instead, Hi-Tech needs to methodically begin with identifying and classifying what internal and external factors create the risk, then determine an appropriate response (Baskerville et al., 218). Due to resource constraints, it is not possible to address all issues under every scenario. The classification results can act as a mechanism for prioritizing the concerns and recognizing any non-starters upfront.

## Identify critical external and internal influences

External influences come from systems and actors that are outside of Hi-Tech’s control. For instance, the Internet is like “the American Wild West – a place of little regulation and considerable opportunity and danger (Quigley, Burns, & Stallard, 2015, p. 116).” Across this frontier are websites that distribute malware and attempt to steal credentials. Corporate digital resources must also operate within this hostile world and repel penetration scans and denial of service attacks. Malicious actors do not stop at the firewall and using physical espionage tactics in order to gain entry into the factories and office buildings (FBI, 2015). The business also needs to be aware of external factors that come from foreign markets, as other nations make trade-offs between government, societal, and international actor’s rights (Kovacs, 2018). Those environments can require additional protections for their citizens or take a laisse-fair approach to intellectual property. These foreign policy decisions can dictate what offerings are advisable to those markets. Specific authoritarian governments, such as Russia and China, have taken the position that stealing private sector secrets is a prerequisite to ensuring their sovereignty (Krebs, 2019). Partial mitigation solutions exist for many aspects, though a ten-foot wall does not stop a twelve-foot ladder.

Internal influences come from employes and venders as they perform various aspects of their role. It can be challenging to monitor the compliance of these persons because they routinely access sensitive systems. For instance, the branch manager and assistant manager have access to the office safe. If one of them decides to steal from the company, the other hopefully notices and reports the issue. However, when both trusted employees collude, then the issue could continue for years undetected. The recent film, Bad Education (2020), recalls such an incident in New York’s Rosyln school district, resulting in the theft of 11.5 million dollars. Erroneous behavior also plays a crucial role in creating internal risk factors, such as employees not wearing safety equipment or tricked into interacting with a malicious resource (e.g., spam). There are also negligent mishandling of process that could extend beyond private litigation to include a decrease in employee confidence and stain the public reputation of the business. Consider the ensuing ripple to Hi-Tech, if an assembly worker lost an arm or control of their Personally Identifiable Information (PII), such as Social Security Numbers (SSN). These preventable accidents linger in the minds of staff and create hesitation to trust the organization. In more extreme situations, these mistrusting deeds can incentive the employee to seek retribution either from lowering quality and performance to outright theft. After all, if the business will not take care of me, then why I should take care of them?

# How to approach these risks

There are numerous actors and assets at stake across these different risk sources. The business needs to consider both the criticality and how replaceable those resources are in the grand scheme. At the top of this list are the health and safety of employees, secrecy of intellectual property, and the ability to continue operations. Next, Hi-Tech needs to decide how they will approach risk from the perspective of self-protect, self-insurance, risk transfer, or avoidance (Baskerville et al., 218). Table 1 contains the definitions and examples of these when these different decisions are most relevant.

Table : Approaches to Risk

|  |  |  |
| --- | --- | --- |
| Approach | Description | Example |
| Self-Protection | * Using processes, training, or technologies to control risk * Low Impact / High Probability scenarios | * Firewalls * Anti-virus software * Compliance training |
| Self-Insurance | * Establishing reserves encase of an emergency * Low Impact / Low Probability scenarios | * Cash reserves * Maintaining excess raw materials |
| Risk Transference | * Compensating a third-party to accept the risk * High Impact / Low Probability scenarios | * Insurance * third-party consultants |
| Avoidance | * Refusing to engage in the high-risk scenario * High Impact / High Probability scenarios | * Not supporting the scenario * Redesigning manufacturing processes (e.g., build domestic assemble remote) |

## Incorporating Standards and Frameworks

## Appropriate laws

## Theories

# Use an established framework

## Describe practical issues and values