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?

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.

# How to approach these risks

Next, Hi-Tech needs to decide how they will approach risk either through 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) |

## Standards and Frameworks

There is an abundance of standards and frameworks available to determine if decisions are being made consistently across the industry. Four common incarnations are the Risk Management Framework (RMF), ISO2700x, NIST Cybersecurity Framework, and COBIT v5. Each of these solutions follows a similar cycle of plan-act-assess across different aspects of the stack (e.g., authentication, authorization, and auditing). However there are differences between the degree of enforcement versus guidance. The origin of the standard also has a significant influence on the framework designers’ perspective, such as COBIT deriving from industry commonalities.

## Balancing Guidance vs. Mandate

While each of these solutions follows similar cycles of plan-act-assess, they differ in terms of prescriptive guidance versus generalizations. For instance, ISO2700x has stringent requirements that necessitate a cultural shift for many businesses, and this is difficult to scale to an enterprise environment (Gillies, 2011). In contrast, the NIST Cybersecurity Framework describes various common scenarios then offers a good, better, best approach for the implementors (Grohmann, 2018). While there is a time and place for everything, introducing schedule risk to inflight commitments through abrupt policy change will always encounter political push back (Dai Zovi, 2019). For many businesses like HTM, having the flexibility to adopt a framework and then iteratively mature their processes over time reduces that risk is an easier sell to senior leadership. Arguably, this is not the utopian course during the interim. However, movement in the right direction is better than no action.

## Considering Framework Influencers

Frameworks like (COBIT)—Control Objective for Information and Information Related Technologies—does not officially use academic theory, but does contain many concepts from Principal-Agent Theory (PAT) and Stakeholder Theory (SHT) to describe the everyday successes from practitioners (Devos & Van de Ginste, 2015). This outcome makes sense, given that practitioners are typically working within corporate settings where PAT and SHT are typical. Also, security engineers culturally tend to gravitate toward hands-on solutions rather than formal academic theory, further explaining the design rationale (Shires, 2018). Comparably, RMF comes from the department of defense, which requires rigorous controls access that enforces access to information. The standard is often also paired with the Operational Test Program Set (OTPS) to provide a checklist of assertions and expectations of acquired products (Combass & Shilling, 2016). While there are strengths to both solutions, it is unlikely that either addresses all scenarios equally. Similar to NIST versus ISO, there needs to be considerations around the organizational culture and the degree of expected formality.

## Appropriate laws

In specific situations, the business needs to choose certain standards and maturity levels to meet expectations of regulation, customers, and partners. Before Hi-Tech can access the European market, they need to demonstrate their products and services meet the needs of the General Data Protection Regulation (GDPR). This law provides legislatures with the teeth they require to come after any organization that does not respect user privacy, or recognizes that user data belongs to that person (Kovacs, 2018). Outside of the digital space, the manufacturing organization also needs to meet the standards of the Occupational Safety and Health Administration (OSHA), that ensure employee safety. Legal expectations also apply to the final product in terms of being socially responsible (e.g., environmental) and reliable (e.g., acceptable service level). When Volkswagen failed to meet these social contracts, there was a backlash of class action lawsuits and fines that total excess of thirteen billion dollars (Ferris & Rosenfeld, 2019). Hi-Tech needs to avoid these penalties by working with legal counsel, operating in a socially responsible manner, and purchasing insurance.

Many frameworks and standards provide puzzle pieces and expect the organization to make them fit. This approach can require the specific implementation to get out the scissors and mutilate either their existing processes or the standard itself. However, the objective of a framework is to meet the needs of the organization, not the other way. This perspective most closely aligns with the NIST Cybersecurity Framework and its good, better, best mentality through risk profiles.

# Use an established framework

Hi-Tech needs to use the chosen framework to protect the corporate resources and end-user privacy, in a manner that aligns with regulatory and social norms. These scenarios include data governance, vendor management, cost management, organizational culture, and artificial intelligence (Lanz, 2018). For each of these cross-cutting concerns, a feedback loop must apply reasonable protections and mechanisms to detect, respond, and recover when those mitigations fail (Grohmann, 2018). When constraining risk within the guidance of the framework, it is not sufficient to set-it-and-forget. Instead, periodic assessments need to revisit the security decisions and confirm they still meet the maturity standards of Hi-Tech (Combass & Shilling, 2016). For instance, using the 56-bit Data Encryption Standard (DES) to protect the confidentiality of documents was an industry-wide standard. However, as Moore’s law took hold and the available computing power caused a supersedence with Message Digest v5 (MD5), then Secure Hashing Algorithm (SHA). Similar changes occur across the value-chain as the attack surface continues to evolve. While the term cybersecurity tends to draw the mind toward computer systems, it is critical to remember that computers are only a tool to execute a business process. Replacing the technology with pen and paper would not make Hi-Tech’s intellectual proprietary any less valuable, nor does it discourage attempts at forced acquisition (Stevens, 2018). Hi-Tech needs to apply the framework equally across people and process to constrain the risk of negligence and malicious intent. Analogous to encryption standards, employees change and evolve too. Perhaps the feedback loop needs to assess employee privileges on a regular cadence, such as part of an annual review. If that team member is going through a divorce, financially bankrupt, or similar life-event, then maybe the potential blast radius of their decisions necessitates further containment.