Section 1: Week 2: Importance of Risk Mitigation Strategies

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 14, 2020

North Central University

# Importance of Risk Mitigation Strategies

## Process for categorizing risks for privacy and security

CyberSecurity refers to a collection of mechanisms and processes that constrain risk to business systems by ensuring they meet performance and consistency expectations, even under erroneous conditions (Mickens, 2018). These erroneous conditions arise due to both malicious and negligent scenarios, degrading the confidentiality, integrity, and availability of our service offerings.

When categorizing these risks, a taxonomy needs to consider the incentives and origin of the risk (Li & Liao, 2018). Incentives of malicious and negligent behavior are drastically different and require unique approaches. Kosub (2015) proposes the terms cyber-risk (negligence) and cyber-crime (maliciousness) to distinguish between these scenarios. For instance, technical support staff wants to follow the cultural norms set by their employer and minimize any friction in completing their assignments. Meanwhile, malicious actors seek to exploit espionage, sabotage, and subversion attacks (Matsubara, 2014). While policies and training can reduce the impact of erroneous technicians, those same vectors do not apply to external criminals.

The next level of the taxonomy includes specific situations involving various people, process, and products. Privacy and cyber risks to a process can come from insufficient authorization and auditing controls. For instance, failure to maintain accurate inventory records can cause inaccurate accounting of the corporate position. Another example might come from a weak authorization policy that allows low-level employees to reboot mission-critical systems. In contrast, cyber-crime might attack processes through repudiation attacks, such as requesting a refund before completing the purchase.

Bit-rot is technical jargon for describing a product that is not consistently maintained. Over time a lack of attention to patch management and policy updates results in fragile systems that are less secure and increase the risk to data privacy. For instance, malware predominately targets vulnerabilities that are over one year old (Emery, 2017). Another common challenge comes from abandoning partial state on these devices, allowing unintentional access for malware and other intruders.

## Importance and value of corporate data and the cost of ownership

Corporate data is the fuel that powers decision processes, creates value differentiation, and customizes the experience for individual users (Knabke & Olbrich, 2018). Facebook has a market cap of roughly $650 billion market cap predominately because of their personalized data feeds, not because it invented a better user forum. As business processes mature, they can unlock hidden potential by transforming data into business intelligence, resulting in competitive advantages through more informed actions (Obeidat, North, Richardson, Rattanka, & North, 2015). However, as with any fuel, there is a risk of fire.

This metaphorical fire comes from the challenges associated with confidentiality, integrity, and availability of information. For instance, confidentiality breaches can come from malicious theft – such as an attacker compromising a user’s account or malware exfiltrating sensitive documents. A loss of confidentiality can also arise from negligent handling of information, such as storing personally identifiable information (PII) on unencrypted thumb drives. If that device becomes lost on an Uber, then all control is lost. When these security incidents occur, there can be regulatory repercussions and political fallout from users. For example, California and Delaware have stringent privacy laws that provide teeth for litigators to seek damages. Internationally, the General Data Protection Regulation (GDPR) enables the European Union to levy fines for abusing the public trust (Kovacs, 2017).

Not all sensitive information is confidential, and other scenarios exist where ensuring integrity is more critical. For instance, a mortgage contract contains public information but needs to be verifiable. Challenges exist around maintaining the integrity of information, such as ensuring malicious actors do not tamper with documents. Mitigations also need to exist for managing data corruption scenarios from network glitches or application faults.

Information that is unavailable promptly has little to no value (Hawking, 2012). These distruptions can come from situations like hardware failures, software outages, and erroneous deletions. The business needs to have business continuity and IT contingency strategies to restore access for information consumers (Kosub, 2015). If the organization fails to maintain high availability of data accessibility, then users of the service will seek out new solutions often from competitors. Internal customers that must continue using the data service will seek out political pressures and similar strategies to force change.

## Process of risk assessment or analysis

Formally, a vulnerability exists at the intersect of three conditions; system susceptibility, threat accessibility, and threat capability (Baskerville, Rowe, & Wolff, 2018). Therefore risk assessment needs to identify these junctions and devise a strategy to remove one or more predicate. Cybersecurity professionals can choose between various frameworks for assessing risk and analyzing business processes. For instance, the National Institute of Standards and Technology (NIST) provides the Cybersecurity Framework; meanwhile, the International Standard Organization (ISO) has 27000 and 27001. Other organizations have established their specific implementation, such as COBIT and the Risk Management Framework.

While there are distinctions between these different systems, they all follow a similar feedback loop of plan-do-check-act (Radhakrishnan, 2015). Each iteration through the loop enumerates the critical resources and available methods for interacting with those systems. Controls must exist on each of those interactions to perform authentication, authorization, and auditing of the caller. After discovering insufficient controls, the administrators need to create a strategy for hedging or removing that risk. For instance, a management service lacks proper controls and is prohibitively expensive to upgrade nor replace. In this situation, using network access controls (NACLs) could remove the threat accessibility, and therefore the vulnerability. The protections require testing to confirm they sufficiently prevent unauthorized access. Perhaps the vulnerable management service is accessible from three subnets, and only two are blocked. When these mitigations turn out to be partial solutions, it requires another iteration of planning and additional effort.

## Risk management strategies and countermeasures

When choosing a risk management strategy, the organization needs to consider the threat impact and likelihood (Baskerville, Rowe, & Wolff, 2018). If the impact is critical, then the business will need to either transfer that risk or avoid the scenario entirely. For instance, foreign markets lack intellectual privacy protections, and this can discourage the release of cutting edge technology to those audiences (Krebs, 2019). In other scenarios, avoiding a hostile market or business activity is not possible, making hedging with insurance a more appropriate response. For example, it might be prohibitively expensive to have redundant manufacturing plants, while unlikely, if the building burnt down, then the organization would go out of business. These situations of catastrophic failure are ideal for insurance and other risk transference solutions. If the situation is less impactful, then the company might choose either self-insurance or self-protection. A self-insurance strategy might be cash reserves or options contracts to acquire resources during extreme demand or short supply. For most other scenarios, the business needs to rely on controls that detect and react to failures promptly (Kosub, 2015). These might include technologies such as anti-virus and Intrusion Detection/Prevention Systems (IDS/IPS).

Another strategy is to form tighter integrations between the system components as a mechanism to reduce the attack surface (Baskerville, Rowe, & Wolff, 2018). For instance, if the network topology requires a user to maintain five accounts with different password complexities, the security of those passwords will decrease to offset the lost convenience (Busby, Green, & Hutchison, 2017). Instead, exposing Single Sign-On (SSO) capabilities improve the user experience and encourages the desired behavior. Another technical gain comes from the removal of redundant components, each with the potential to contain incorrect application code or configuration settings. Removing redundancies also aids in more consistency through centralized policy management and enforcement.

## Definition of each information security role

|  |  |
| --- | --- |
| Role | Description |
| Chief Risk Management Officer | Reduces the blast radius of process failures across the corporate strategy |
| Chief Information Security Officer | Accountable for the corporate strategy that protects business technology assets |
| Director of Information Security | Defines the policies that enact the corporate security strategy |
| Director of Privacy and Compliance | Ensures following of regulatory requirements around the handling of data |
| Security Engineer | Validates the implementation details of the security policy decisions |
| Everyone Else | Interacts with those policies and is critical for their successful execution |

## Relationship between roles and role of cybersecurity professional

Multiple security personas work in tandem to deliver a consistent and coherent risk management strategy that encompasses all business people, processes, and products. If that strategy lacks sponsorship from the executive-level or does not resonate with the troops, then it is unlikely to succeed (Weston, Conklin, & Drobnis, 2018). Instead, having a cultural alignment ensures that the standard operating procedure makes safe decisions that minimize risk and privacy concerns.

The Chief Risk Management Officer (CRMO) and Chief Information Security Officer (CISO) set the stage by determining what acceptable risks to business continuity. While smaller organizations combine these roles, the CRMO focuses on general risk versus the CISO is more concerned with the subdomain of information confidentiality, integrity, and availability (Grobler, 2018). Their broad policies and expectations form the corporate vision and guidelines that the Director of Information Security (DIS) must meet. For instance, the CISO might require customer data protections are Health Insurance Portability and Accountability (HIPAA) compliant. The DIS would break that down into a series of process changes and define a roadmap for achieving this goal. Incrementally delivering on the roadmap comes from teams of security engineers, that decompose problem statements into specific work items and validate policy decisions.

Last, but not least is everyone else, as it is security-critical that policies enable the business versus create artificial blockades (Weston, Conklin, & Drobnis, 2018). If the troops lack insights into the intent of a policy, they will follow the specific ask, not similar permutations of the rule. For example, the timely installation of operating system patches reduces the risk of malware spreading through the organization. While no one asked for similar updates to Java, Flash, and Adobe reader are equally vulnerable. Only through associating the request to policy to the roadmap to the vision are these auxilarly risks addressed.

## Conclusion

Addressing risk management requires a feedback loop that centers around plan-do-check-act cycles. At the beginning of that process are exercises that identify business-critical resources and enumerate threats against those systems. These threats can come in the form of cyber-risk or cyber-crime against the organization’s people, processes, and products. Corporate data is an incredibly valuable artifact, as it enables business intelligence and platform differentiation. However, there are several risks to owning information specifically around maintaining its confidentiality, integrity, and availability. When those security properties degrade, then the company runs the risk of alienating its customer base, violating privacy regulations, and fails to make timely decisions.

Various frameworks exist for formally making risk assessments and evaluating the quality of mitigating controls. Those controls must enforce authentication, authorization, and auditing capabilities where possible. However, general security controls are not appropriate or possible in every scenario, and this requires alternative strategies such as risk transference or avoidance. Depending on the situation, the business might need multiple risk countermeasures, such as reducing the features available to foreign markets and ensuring proper authorization checks.

A successful risk management solution needs sponsorship and agreement from the top-to-bottom of the organization. C-Level members like the CRMO and CISO establish the corporate norms and vision for the future. That vision must align the desires of other executives, enabling the business to deliver on its core mission safely. Directors-level establish a roadmap and oversee security engineers that build and validate those requirements. Finally, everyone else in the organization needs to understand how they fit into the risk management strategy, and how the policies map to roadmaps and grander visions.