Section 1: Week 3: Avoid or Control Persistent Threats

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 21, 2020

North Central University

# Avoid or Control Persistent Threats

Malicious actors, targeted attacks, and advanced persistent threats (APT) each seek to disrupt the confidentiality, integrity, and availability of information systems. These different groups seek out their victims with varying levels of specificity and sophistication (see Table 1). After gaining access through phishing emails, an APT has established a foothold within the NCU Financial (NCU-F) network. The organization needs a strategy to remove the uninvited guests and recover control of the network. When a significant security breach occurs, and the business experiences a state of crisis, this can be a highly efficient period to enact change and strength the overall security posture (Weston, Conklin, & Drobnis, 2018). This reinforcement process needs to consider changes to people, processes, and products through the lens of Risk Management Frameworks (RMF), regulatory and ethical standards, and new Intrusion Detection and Prevention Systems (IDS/IPS).

Table 1: Classifications of Attackers

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Target Selection | Description | Sophistication |
| Generic Malicious Actor (Fischerkeller & Harknett, 2017) | Random Selection | Use automation to attack thousands of systems, exploiting attacker defender economics | Relies on the Law of Large Numbers |
| Targeted Attackers (Alshamrani A, 2019) | Specific / Short Term | Identity specific industries and business artifacts for exploitation | Relies on social engineering and other known vulnerabilities |
| Advanced Persistent Threats (Alshamrani A, 2019) | Specific / Long Term | Seeks prolonged control over a target for months to decades | Well-financed organizations with ‘state-of-the-art’ weapons |

## Risk Management Framework (RMF)

When an attacker compromises an organization, there can be a sense that discarding the RMF is the best course of action. However, most frameworks fundamentally follow the same feedback loop of ‘plan-do-act-check’ (Radhakrishnan, 2015). Instead, the business needs to assess their needs in terms of regulatory requirements, process maturity, and cultural norms (see Table 2). If the process does not align with the expectations of internal partners, then it will face political pressure and avoidance (Dunn, 2014). After considering these aspects, the NCU-F security team recommends remaining on ISO 27000, as it addresses the regulatory expectations of financial institutions. Nevertheless, the system compromise highlights that improper controls exist, and changes to the framework’s implementation are necessary.

Table 2: Risk Management Frameworks

|  |  |  |
| --- | --- | --- |
| Name | Description | Ideal Environment |
| National Institute of Standards and Technology (NIST) Cybersecurity Framework (Grohmann, 2018) | Flexible methodology to approach controls and evolve them over time | Large enterprise and businesses with varying levels of process maturity |
| International Organizational Standards (ISO) 27000 (Gillies, 2011) | Rigid set of requirements for ensuring appropriate controls | Small enterprises and heavily regulated industries |
| Control Objectives for Information and Information related Technology (COBIT) (Devos & Van de Ginste, 2015) | Collection of industry best practices and guidelines | Organizations that need a middle ground between NIST and ISO frameworks |

## Relevant Laws and Standards

During the APT’s tenure within the private network, it could have been privy to confidential information about the institution and its customers. This situation creates both regulatory and ethical expectations of publically disclosing the security incident. States like California, Delaware, and Utah have strict privacy legislation that can hold NCU-F responsible for negligence. In September 2017, Equifax announced a data breach impacting 147 million people, costing over 575 million dollars in settlements plus public relations (Puig, 2019). If the incident exposes European customer data, then the General Data Protection Regulation (GDPR) can impose additional fines (Kovacs, 2017). Even without these legal requirements, NCU-F has an ethical obligation to be forthcoming. The truth always comes out, and failing to act degrades the companies ability to drive the public narrative.

## Adoption Process

The adoption of any process requires sponsorship from executive leadership and proper communication to the troops (Weston, Conklin, & Drobnis, 2018). When either the top or bottom of the organization lack agreement in the solution, it will not become a priority, and team members will sidestep it. Instead, having a cultural alignment ensures that the standard operating procedure makes safe decisions that minimize risk and privacy concerns. For instance, this intrusion began with a phishing attack. Security awareness training could reduce the likelihood of that scenario but not eliminate it (Hunt, 2019). Through a similar mechanism, RSA became compromised via malicious emails automatically triggered a zero-day exploit in Adobe Flash (Leyden, 2011). After slipping past the firewall, many enterprise environments lack defense-in-depth controls allowing lateral movement across the network (Stevens, 2018). Removes these auxiliary threats require a fundamental shift in approach that centers around zero-trust and an assume breach mindset. Promoting such change adoption is only possible under a shared vision of success and collective agreement that change is necessary.

## Changes to Operations and Services

## Best Practices for Security and Risk Management

## Software Solution Recommendations