Section 1: Week 3: Global Security Risk

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 19, 2020

North Central University

# Global Security Risks

Organizations need to honor the laws and norms of any locale that they operate within, or risk violating social or legal contracts resulting in lost business or punitive fines. As domestic organizations expand into multi-national corporations, maintaining compliance with these contracts becomes challenging as each foreign nation has different rules expectations. These variations alter the level of transparency and legal protections. For example, a ride-hailing app that wants to expand into the Chinese market needs to trade intellectual property protections for a broad audience of customers. The leadership team might be willing to accept that risk but only deploy last year’s feature set, not the most cutting-edge innovations. During a later expansion into Europe, the same app might use specific features that do not meet the privacy requirements for that region. These nuances are subtle and require an understanding of the rationale for their existence, and what changes are required across the people, processes, and products to mitigate risks introduced by foreign policies. Implementing these risk reduction strategies requires budgeting resources and devising an acceptable strategy for the senior leadership team.

# Section I: Understanding Global Risk

International organizations encounter specific risks towards their continuity, and this requires executing across decentralized compliance and regulatory environments. These distinctions cause the Internet to function more like a collection of islands than a homogenous communication platform. Businesses also need to consider any legal protection limitations around both personal and corporate privacy before sharing innovations or expecting assistance after a crime.

## Geography and Sovereignty

The premise of the Internet is an open communication system that connects people from around the world, enabling commerce and ideas to flow freely. However, nation-states also want to protect their sovereignty and enforce laws around these interactions (Inkster, 2015). These competing requirements cause national security policies to make trade-offs between government control, societal freedoms, and rights of international actors (Kovacs.2, 2018). Since the values of democratic and authoritarian nations vary substantially, it is unrealistic to assume a unified set of policies can exist that appeal to all countries. Instead, nearly all nations legislate laws that target the Internet infrastructure that resides within their state (Matsubara, 2014). These decisions create geography that influences the protective capabilities and behavioral norms. For instance, the European Union (EU) believes that building a digital economy begins with user privacy (Kovacs.1, 2018). While the EU’s Global Data Protection Regulations (GDPR) mandates severe penalties for negligence, like data breaches, authoritarian countries such as Russia are more laisse-fair. These value differences appear in other aspects like the transparency to share evidence or assist with criminal investigations.

## Cyberespionage

Businesses that operate solely within the United States have access to a legal system that enables seeking damages for malicious third-party behavior. For instance, when Uber stole intellectual property from Google, it was sued for $250M in damages (Bensinger, 2019). When the same theft occurs across international borders, jurisdiction becomes less clear and is more challenging to enforce. Participants in these hostile markets need to be aware that espionage comes from various sources, such as individual hackers and nation-states (Krebs, 2019). International law does not prohibit these nation-states spying, Article 51 of the United Nations charter even allows it under the disguise of self-defense (Banks, 2017). Some states argue that different rules should exist for monitoring public and private institutions. However, this perspective employs a very Western view. For socialist countries, the distinction is fuzzier than a purely capitalist society as the boundary between the industries lacks a consistent definition.

## Cyber sabotage

Using technologies like ransomware, malicious software that encrypts digital devices, nefarious actors can force an organization to purchase decryption keys before restoring service (Busdicker & Upendra, 2017). Attackers also send high volumes of network traffic into corporate websites as a mechanism causing Denial of Service (DoS) scenarios. When these cyber sabotage events occur, it disrupts business continuity and impacts the credibility of the victim. American companies have traditionally relied on deterrence, such as the Computer Fraud and Abuse Act (Fischerkeller & Harknett, 217). Technological solutions like deploying applications across multiple Public Cloud Service Provider (CSP) data centers can minimize the influence of DoS attacks. However, these same legal protections do not uniformly exist across the globe, and regulations around data placement can limit the accessibility of flexible fail-over solutions.

## Subversion

The international community does not agree on the strict definition of what constitutes a cyber-attack (Fischerkeller & Harknett, 217). These differences influence auditing and compliance requirements between countries and prevent direct comparisons across policies or statistics (Matsubara, 2014). The political values of nations contribute to the disparity, such as Europe prioritizing end-user safety versus authoritarian governments preferring to save face. When requirements around transparency do not fully exist, then even legitimate partners are unlikely to tell the whole truth. Being the only business that is forthcoming creates a competitive disadvantage, as customers only see “A” claims to be more secure than “B.” Without a carrot or stick, how can a domestic company ensure security incidents are timely and accurately communicated? Imagine the challenges with less reputable entities, if these are the risks with legitimate partners.

# Section II: Mitigating Global Risk

Mitigating risks from international interactions requires a comprehensive plan that spans people, processes, and products. These plans can begin life as grassroots initiatives but require ownership from executive leadership to gain the necessary funding and prioritization (Erickson & Neilson, 2018). Challenges from cybersecurity need the same attention as any other aspect of business continuity, such as supply chain shock or cash flow management. Ignoring these security vulnerabilities creates a timebomb that will eventually cause disruptions and impact the company’s ability to deliver success.

## People

The most crucial resource of an organization are the employees, and any plan for success needs to begin here. Valientes (2017) estimates that nearly half of security incidents result from employee negligence, like interacting with phishing attacks and fat-fingering database commands. Businesses that focus on security awareness training can reduce these statistics and create more reliable systems. This awareness needs to touch on cultural expectations, such as European customer data, cannot leave Europe. Initially, these expectations appear arbitrary, but communications the geographical nature of the Internet presents general consistencies and best practice patterns. It also leads to an understanding of how various levels of legal enforceability influence release schedules of new features and innovation into foreign markets. This training applies to all levels of the business, such as how technicians assist international customers, and how executives bundle products for international distribution.

## Process

Protecting against global risks requires augmenting business processes and asset lifecycle management. Hennig (2018) recommends starting with a threat modeling to identify what resources need protection and under which contexts. During this exercise, each step needs to consider any integrity, confidentiality, and availability risks that might exist. For instance, a prerequisite of deploying web services into authoritarian nations datacenters might involve exchanging sensitive communications with a foreign company. Those conversations are likely to be intercepted and also viewed nation-states, either across the wire an official subpoena. These challenges require design decisions that focus on disposable resources (e.g., one-time access tokens) and end-to-end encryption. Many real-world processes span cross-corporation and require communication across asset production, installation, operationalization, and retirement (Busdicker & Upendra, 2017). Identifying and repairing vulnerabilities across this lifecycle needs to be an iterative process that seeks feedback and incorporates it. An effective strategy for promoting these feedback loops begins an organizational culture, that feels comfortable reaching out to the incident response teams, without fear of retribution (Dai Zovi, 2019). Leadership teams need to prioritize building these intra-team trust relationships through combinations of social outreach and bug bounty programs.

## Products

The products released into a market need to consider the security assertions of both the foreign market and the domestic organization. For instance, authoritarian nations will steal innovations and share those trade secrets with foreign competitors. The inverse can also be true, where products lack the security assertions of the foreign market and are not permissible. Recently Kaspersky Anti-Virus was banned from several American institutions because of concerns that Russia could maliciously control the software (Krebs, 2019). This trait is not unique to authoritarian nations, as specific New Zealand products have been ban from France for not meeting privacy norms (Hunt, 2019). When a product does not meet the expectations of either the producer or the consumer, then a decision around acceptable risk needs to take place. Those decisions might result in bundling fewer features into a smaller version or blocking the deal entirely.

# Section III: Budgeting Resources

When evaluating how much mitigating global risk costs, it is analogous to asking how much a sack of groceries costs and is dependent on what needs to occur. Some aspects are relatively cheap, such as mandatory awareness training for the staff and periodically testing their competencies (Busdicker & Upendra, 2017). Other aspects can be extremely complex, like restructuring products to adhere to security and privacy concerns. Similarly, revising value chain pipelines to meet auditing and regulatory requirements after the fact can be very cumbersome. Microsoft Azure addressed these concerns by starting with an analysis of the different markets it wished to do business. After collecting the external requirements, the business categorized these expectations and then chose to implement the most strict asks. For instance, if some countries require infrastructure to reside within that nation’s border, then do that everywhere. When this level of planning does not take place, then there are fewer cheap solutions. That leaves the business with (a) accepting more risk or (b) delivering a less innovative and competitive product.

Along with creating a plan for improving local people, processes, and products, there need to be considerations around auditing the accuracy of foreign partners. Completing this objective might involve hiring third-party auditors or using sensors to measure efficiencies. If the local business has sufficient resources, perhaps even hiring a dedicated team member to work from the foreign office provides the necessary oversight. After minimizing the global risk and identifying the relevant resources, an iterative plan needs to be defined and approved. For example, training the local staff might entail contracting a security consulting firm to create a lesson plan. Other aspects become a matter of cost-benefit analysis and proposing an acceptable timeline. Perhaps having a remote manager in the foreign office is more critical during the second phase of the deliverable.

# Conclusion

When an organization seeks to do business in a foreign market, they need to understand the security guarantees and assertions of that new environment might differ from their native locale. Some foreign markets have more robust assertions that require upgrading our products to include encryption and related privacy features. In contrast, others have weak guarantees, such as rampant cyber espionage, sabotage, and subversion, and are less desirable to share trade secrets. An assessment of these risks needs to find a cost-benefit balance for accessing that market without compromising the integrity, confidentiality, and availability of the organization. That balance might come from reducing the available feature set, or declining the deal entirely. While it can be challenging to navigate these foreign policies, businesses that come with skepticism and security awareness are more likely to be successful. That awareness needs to be cognizant of the different geographics of trust that exist across markets, and not treat the Internet as one homogeneous locale.

# References

Banks, W. (2017). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory Law Journal; 2017, Vol. 66, Issue 3*, 513-525.

Bensinger, G. (2019, August 27). *Former Google self-driving engineer, who prompted a lawsuit against Uber, gets hit with criminal charges*. Retrieved from Washington Post: https://www.washingtonpost.com/technology/2019/08/27/former-google-self-driving-engineer-who-prompted-lawsuit-against-uber-gets-hit-with-criminal-charges/

Busdicker, M., & Upendra, P. (2017). The Role of Healthcare Technology Management in Facilitating Medical Device Cybersecurity. *Biomedical Instrumentation & Technology Sep; Vol. 51 (s6)*, 19-25.

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Blackhat USA 2019.*

Erickson, A., & Neilson, T. (2018). CyberSecurity -- the No. 1 Threat Facing Manufacturers. *Industrial Management. Jul/Aug, Vol. 60, Issue 4, p24-27*, 24-27.

Fischerkeller, M., & Harknett, R. (2017). Deterrence is Not a Credible Strategy for Cyberspace. *Orbis Volume 61, Issue 3*, 381-393.

Hennig, N. (2018). Privacy and Security Online: Best Practices for Cybersecurity. *Library Technology Reports. April, Vol. 54, Issue 3*, 1-37.

Hunt, T. (2019, May 20). *Keynote: Hack to the Future*. Retrieved from YouTube: https://www.youtube.com/watch?v=qCOefMiakps

Inkster, N. (2015). Cyber espionage. China’s Cyber Power. *Adelphi Series Vol. 55*, 51-82.

Kovacs.1. (2018). Cyber Security Policy and Strategy in the European Union and NATO. *Revista Academiei Fortelor Terestre. Vol. 23, Issue 1*, 16-24.

Kovacs.2. (2018). National Cybersecurity as the Cornerstone of National Security. *Revista Academiei Fortelor Terestre. Vol. 23, Issue 2*, 113-120.

Krebs, C. (2019, April 23). ICCE 2019 - Keynote by Christopher Krebs, Director, Cybersecurity, and Infrastructure Security Agency. Retrieved from YouTube: https://www.youtube.com/watch?v=aVfcgNhHSDM

Matsubara, M. (2014). Countering Cyber-Espionage and Sabotage. *RUSI Journal: Royal United Services Institute for Defence Studies, 159(1)*, 86-93.

Valiente, C. (2017). Addressing Malware WITH Cybersecurity Awareness. *ISSA Journal. Oct, Vol. 15, Issue 10*, 16-22.