Section 1: Week 3: Global Security Risk

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 19, 2020

North Central University

# Global Security Risks

Businesses 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 expectations and rules. These variations both add and remove visibility and 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. Then changes 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 the legal protections 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 behavior norms. For instance, the European Union 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 (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” is 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, such as supply chain shock or cash flow management. Ignoring these vulnerabilities creates a timebomb that will eventually cause disruptions and impact the companies ability to deliver success.

## People

The most crucial resource of an organization are the employees, and any plan for success needs to begin with here. Valiente (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 that various levels of legal enforcement influence release schedules of new features and innovation. 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 needs 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 or 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 environments through combinations of social outreach and bug bounty programs.

## Products

* 1. (Banks, 2017) be more like isis and encrypt
  2. (Choi, 2017)Choi QuantumNetworking

# Section III: Budgeting Resources

## What does it take/cost

* 1. (Fischerkeller & Harknett, 217)Fischerkeller – Deterrence
  2. (Busdicker & Upendra, 2017)Busdicker – awareness training
  3. (Emilio, 2018)Emilio – ChinaWarefare meet on battlefronts

# Conclusion