Section 1: Week 3: Global Security Risk

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 19, 2020

North Central University

# Global Security Risks

The latest sensation in the gig economy is Ride-Me, a mobile app that connects freelance drivers with riders. After receiving a one billion dollar valuation, the platform seeks to expand into international markets, competing against global powerhouses like Uber and Lyft. Moving a business onto the global stage introduces new risks that need to be understood and constrained. For instance, foreign nations seek to protect their national sovereignty and impose complex legal restrictions on data storage and user privacy. These requirements can increase the attack surface to espionage and intellectual property theft. Inconsistency of compliance and regulation creates challenges as definitions of transparency vary between locale. Organizations must be cognizant of the costs associated with mitigating these issues through people, process, and product solutions.

# Section I: Understanding Risk

## Risks from the International Community

**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 of policy or approach (Matsubara, 2014).

## Process for Establishing Risk

1. Geography
   1. (Moss, 2019)Moss Blackhat
   2. (Inkster, 2015)Inkster ChinaCyberPower
2. National Sovereignty
   1. (Fischerkeller & Harknett, 217)Fischerkeller – Deterrence
   2. (Kovacs.1, 2018)Kovac – PolicyStrategyEuropean
   3. (Kovacs.2, 2018)Kovacs Cornerstone
3. Legal Challenges
   1. (Emilio, 2018)Emilio – ChinaWarefare
   2. (Kovacs.1, 2018)Kovac – PolicyStrategyEuropean
   3. (Matsubara, 2014)Matsubara – CounteringCyber
   4. (Emery, 2017) – zero-day regulation

## Threats

1. Transparency, Compliance/Regulation
   1. (Erickson & Neilson, 2018)Erickson CyberSecManufacturing
2. State-sponsored actors
   1. (Kovacs.2, 2018)Culture (public v private) – Kovac Cornerstone
   2. (Inkster, 2015)Inkster - ChinaCyberPower
3. Zero-day attacks
   1. (Emery, 2017)Emery zero-day
4. Erickson – Manufacturing Ransomware

# Section II: Mitigating Risk

## People

* 1. Erickson – ownership, top-down mandates

## Process

* 1. Busdicker; Upendra Medical Devices

## 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