EN.650.683 (Cybersecurity Risk Management)

Final Research Paper

Jay Chow

13th May 2019

The U.S and Singapore are among the world's leaders in cybersecurity risk management and incident response as they share a collaborative and robust approach to addressing cybersecurity risks in the modern age. In my paper, I will first compare and contrast the organizational structures of the intelligence and defense agencies in Singapore and the U.S as they ultimately contribute to the different cybersecurity risk management approaches in each country, in terms of planning, implementation and execution. More specifically, the U.S and Singapore have dissimilar degrees of centralization and different amounts of resources available to make vital cybersecurity risk management decisions at the national level.

To define some key terms that will be used throughout my paper, risk is defined as the likelihood of an incident and its consequences for an asset. It could also be viewed as the effect of uncertainty on objectives. Cybersecurity risks, therefore, refer to exposure to threats in the realm of computers or computer networks. According to Kohnke[1], risk assessment is the assessment of the overall likelihood and impact of a threat. It is the process of risk identification, risk analysis, and risk evaluation. Risk assessment is one of the fundamental components of risk management, facilitating decision making at the organization level, mission and business process level, and information system level. Risk management is an ongoing process of identifying, assessing, and responding to risks. It can also be viewed as a set of formal organizational processes that are designed to respond appropriately to any identified adverse event. As such, it is crucial to understand both risk assessment and risk management in the context of both the U.S and Singapore at a national level.

Modern cybersecurity risks require a wide and deep range of technical expertise to fully control, manage and mitigate them. There is a saying that "there are two types of company or federal aXWgency – those who have been hacked or those who don't know that they have been hacked". As dangerous and pessimistic as it sounds, this is where highly specialized technical knowledge, skills and experience from engineers, researchers and technical leaders are needed. However, having the knowledge of the business, legal regulatory environment is also equally essential. These technical complexities must be simplified for businesses and governments to understand, take action and learn from past mistakes since many business and government leaders do not have backgrounds and training in cybersecurity.

[1]Kohnke et al., the complete guide to cybersecurity risks and controls

Since Singapore is a small but advanced country, it relies primarily on a few centralized but pivotal agencies while the U.S is a huge and resourceful country that relies on numerous agencies and frameworks such as NIST for cybersecurity risk management. Both Singapore and the U.S are immigrant nations at the core. However, the U.S has a massive population of around 330 million with a huge talent base while Singapore has a small population of around 5.6 million with a significantly smaller pool of human resources. As a result, in terms of quantity of headcount, Singapore has fewer number of government-led cybersecurity institutions and a smaller and a less robust cybersecurity risk management support system and infrastructure as compared to the U.S. It is also critical to understand that the U.S houses the largest and most powerful multinational technology companies such as Google, Apple, Facebook and Microsoft that have to abide to US laws and work alongside the U.S government if needed. In Singapore, U.S-based companies may or may not choose to work with the Singapore government, depending on the context and situation.

In the government space, I will first briefly describe the roles of the National Security Agency of the United States(NSA) and the Cyber Security Agency of Singapore(CSA), and subsequently discuss the similarities and differences in the roles of the NSA and CSA in affecting the cybersecurity risk management of the U.S and Singapore respectively. The primary goals of the NSA[2] is to save lives, defend vital network, advance U.S goals and alliances, protect privacy rights and carry out missions as NSA is both a member of the Defense Department and an Intelligence Community agency. It is the world leader in cryptology, which is the art and science of making and breaking codes. The NSA consists of many technical staff that discovers adversaries' secrets, protecting U.S secrets and outmaneuvering the adversaries in cyberspace, protecting the privacy rights of the American people. The NSA is America's cryptologic organization that coordinates, directs and performs highly specialized activities to protect U.S government information systems and produce foreign signals intelligence information by converting cryptic foreign intelligence communication into comprehensive text(codebreaking) and protecting U.S government information systems by using cryptography(codemaking). It has listening posts in the US and around the world to monitor and keep records on billions of international calls and emails that originated in the U.S.

[2] National Security Agency. (n.d.). Retrieved from https://www.nsa.gov/

On the other hand, the CSA[3] is the national agency overseeing cybersecurity strategy, operation, education, outreach, and ecosystem development and working with the industry to ensure compliance. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information. CSA focuses on engagement and outreach by nurturing ties with local and global industry and thought leaders, heightening cybersecurity awareness through public outreach programs and promoting security-by-design. It is responsible for developing a robust cyber security ecosystem to respond to and mitigate cyberattacks. CSA helps to protect Singapore's critical sectors by strengthening cybersecurity in our critical sectors, such as energy, water, and banking. CSA ensures the effective coordination and deployment in Singapore's response to cyber threats and engages with various industries and stakeholders to heighten cybersecurity awareness and develop Singapore's cybersecurity by setting the government wide policies.

Compared to the NSA for the U.S, I would argue that the CSA plays a larger role in terms of cybersecurity risk management for Singapore. According to "Singapore's cybersecurity strategy" by Ter Kah Leng from NUS Business School which is part of the National University of Singapore[4], the CSA was set up in April 2015 to oversee and coordinate Singapore's cybersecurity strategy. Under the Cybersecurity Act, the Commissioner of Cybersecurity, appointed by the relevant minister, will have extensive supervisory, regulatory and enforcement powers. Singapore's enactment of the Cybersecurity Act 2018 is an attempt to foster a secure and resilient national infocomm environment against cyberattacks. The Commisioner is to identify and designate as critical information infrastructure any computer or computer system which is necessary for the continuous delivery of essential services. The commissioner is to coordinate national efforts and monitor cybersecurity threats to Singapore's national security, defence, economy, foreign relations, public health, public order and safety or essential services, whether such cybersecurity threats occur in or outside Singapore. In other words, the commissioner has the power and authority to investigate any cybersecurity threat. However, this is clearly not the case for the U.S as the U.S uses a separate approach for cybersecurity risk management in which the White House releases cybersecurity strategies through the DoD. For example according to the U.S. Department of Defense official website, the White House released the first national cyber strategy in 15 years to protect America's networks, to protect the people, homeland and way of life, to promote American prosperity, to preserve peace through strength and to advance American influence.

[3]Cyber Security Agency of Singapore. (n.d.). Retrieved from https://www.csa.gov.sg/

[4]Kah Leng Ter, "*Singapore's cybersecurity strategy"*, NUS Business School, National University of Singapore, Singapore.

It is important to note that NSA has real operations in both defense and offense while the CSA is more of a regulatory agency which does not contain as much technical firepower behind the machines as compared to the NSA. To be more specific, the CSA is more regulatory and policy-oriented while the NSA is more narrow-focused with greater technical expertise in the specific areas of codebreaking and codemaking against adversaries. In October 2016, the prime minister of Singapore Lee Hsien Loong launched Singapore's Cybersecurity Strategy with the aim to create a resilient and trusted cyber environment for Singapore. The four pillars that underpin this strategy include building a resilient infrastructure, creating a safer cyberspace, developing a vibrant cybersecurity ecosystem and strengthening international partnerships. Expectedly, as part of Singapore's cybersecurity risk management strategy, internet access of workstations of civil servants will be cut off as there was too much data to secure. According to David Koh, chief executive of CSA, he recognizes that "there is no way to secure this as the attack surface is like a building with a zillion windows, doors and fire escapes".

However, there is a distinct similarity between NSA and CSA in the sense that they are both part of a bigger key governmental entity. NSA is a specific agency of the U.S Department of Defense(DoD)[5] while CSA is headed by Singapore's Ministry of Defence(MINDEF)[6]. The U.S Department of Defense with a budget of $716 Billion, 2.86 million employees and 4800 Defense sites, provides the military forces needed to deter war and ensure the U.S's nation security. Singapore's Ministry of Defence is a ministry of the government of Singapore entrusted with overseeing the national defence needs of Singapore.

More specifically, MINDEF's defence policy is to ensure Singapore enjoys peace and stability, and that Singapore's sovereignty and territorial integrity are protected. Defending Singapore in the 21st century, MINDEF focuses on strengthening total defence, dialogue, confidence-building and co-operation in the region and beyond. It has a policy of *Total* which consists of Military Defence, Civil Defence, Economic Defence, Social Defence and Psychological Defence involving the people, public and private sectors of the country. In other words, cybersecurity risk management is a minor but vital portion of the heavy responsibilities of MINDEF.

[5]U.S Dept Of Defense. (n.d.). Retrieved from https://www.defense.gov/

[6]Singapore MINDEF. (n.d). Retrieved from https://www.mindef.gov.sg/web/portal/mindef/home

Similarly, the DoD is an executive branch department of the federal government that co-ordinates and supervises all agencies and functions of the government concerned with national security and the United States Armed Forces. The DoD is headed by the Secretary of Defense, a cabinet-level head who reports directly to the President of the United States. In this sense, the organizational structure of the U.S is more comprehensive as compared to Singapore, due to a longer cybersecurity risk management history and the severity of cyber threats that the U.S has faced over the past few decades. Beneath the DoD lies the United States Department of the Air Force, the United States Department of the Navy, the United States Department of the Army, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency and the National Reconnaissance Office. It is also necessary to note other defense agencies such as the Defense Advanced Research Projects Agency, the Defense Logistics Agency, the Missile Defense Agency, the Defense Health Agency, Defense Threat Reduction Agency, the Defense Security Service and the Pentagon Force Protection Agency which are all also under the command of the Secretary of Defense. As such, on a national level, the U.S has a more robust organizational structure and decentralized ecosystem for cybersecurity risk management compared to Singapore which has a more centralized ecosystem with a shorter history of cybersecurity risk management.

Another similarity between the U.S and Singapore is that both countries heavily on third party contractors to outsource certain tasks. For example, Booz Allen Hamilton is a third-party contractor of the NSA that focuses on management and information technology consulting. In Singapore, the Defence Science & Technology Agency(DSTA)[7] is a also a third-party, central procurement agency for MINDEF and the Singapore Armed Forces. Using third-party contractors has both its pros and cons, which will be discussed later on.

Booz Allen is a consulting firm that is a defense and intelligence contractor for both the U.S government and private enterprises. According to the New York Times, tens of thousands of contractors are believed to work for American intelligence agencies, doing everything from helping secure the military against cyberattacks and plan intelligence operations, to training spies. In the U.S, a great deal of intelligence work is outsourced. Founded in 1914, Booz has been gaining business from the government. Its clients include every branch of the military and a long list of intelligence organizations, from the NSA to the National Geospatial-Intelligence Agency, which is essentially a high-tech mapping operation. Outside of the U.S, Booz Allen has helped the United Arab Emirates build its own high-tech spy agency.

[7] Defence Science and Technology Agency. (n.d.). Retrieved from https://www.dsta.gov.sg/

A major advantage of using contractors is to cut costs and reaping benefits such as accessing skilled expertise, reducing overhead, flexible staffing and focusing on core activities. In other words, the NSA, DoD, CSA or MINDEF could focus on other priorities while gaining skilled expertise in the private sector to remain competitive with private enterprises. As such, it is of extreme importance for contractors to appropriately draw the line between enterprise and government entities as there may exist a conflict of interest in serving both parties. Contractors allow the government to swiftly bring in people with technical expertise, and allow government agencies to get around staffing and budgetary constraints set by Congress. An example was when the Obama administration set a limit on the number of troops that could be deployed in Afghanistan. Despite of this, many third-party contractors were brought in by the DoD to get around the staffing limits.

However, employing contractors may bring security risks and leaks. A case that happened earlier this year was when a 54-year-old former National Security Agency contractor pleaded guilty to taking classified documents home in a deal likely to put him in prison for nine years. Harold Martin, who worked in the N.S.A.'s Tailored Access Operations hacking unit, committed a breach of classified information when FBI agents found stacks of documents and electronic storage devices stashed in his car, his home and a garden shed. Unlike Snowden, others argue that Martin did not leaked any of the information he was suspected of stealing, which was supposed to be highly classified computer code.

In Singapore, DSTA is a centralized statutory board and third-party contractor for MINDEF that harnesses and exploits science and technology to provide technological and engineering support to meet the defence and national security needs of Singapore. DSTA does project management and system integration for MINDEF. According to its official website, DSTA adopts a systems engineering approach by undertaking design, development, acquisition and systems integration responsibilities, as well as operations and support management. These span the entire spectrum of capability planning, development, and sustainment of weapon systems throughout their life cycle to ensure that the SAF continue to be a formidable fighting force.

In the context of cybersecurity risk management, there is a crucial difference in organizational structures between the U.S and Singapore. As mentioned earlier on, the DoD consists of a massive umbrella of agencies, with each agency possibly engaging different contractors for outsourcing work. This emphasizes my point that with around 330 million people, U.S is a mature cybersecurity ecosystem with a wide range diversity of human talent, resources, agencies and contractors to capitalize on. In contrast, with only around 5.7 million people, Singapore has a smaller talent pool with limited resources

and manpower. Therefore, Singapore has to rely on more efficient and centralized authorities for cybersecurity management. The Singapore Army, Singapore Navy and Singapore Airforce, all under MINDEF, rely primarily on CSA as a regulatory agency and DSTA as a contractor for outsourcing all cybersecurity-related work. However, the U.S Army, U.S Navy and U.S Airforce, all under the DoD, have a greater diversity of agencies, contractors, resources and talent pools for cybersecurity risk management. This is not surprising as Singapore is a younger country that suffered lesser cyberattacks on a national scale compared to the U.S that has been a bigger target from various nation-state adversaries.

Although the organizational structures of defense and intelligence agencies of Singapore and the U.S are different as explained above, similar controls are used in cybersecurity risk management for both countries. However, it is important to understand that it is impossible completely eliminate all cybersecurity risks. A control is any process, policy, device, practice or action which maintains and modifies risks. Controls are key to cybersecurity risk assessment, which is fundamental piece of cybersecurity risk management. Risks are accessed based on the controls which will ultimately lead to decisions being made for the risks identified. For example, the U.S and Singapore use NIST-specific controls to aid in the cybersecurity risk management process, namely access control policies, security awareness training and contingency planning.

Access control policies minimize the risk of unauthorized access to physical and logical systems. They are a means to restrict access to objects(files, data) based on the identity of subjects(users and processes). Discretionary access control indicates that a subject with a certain access permission is capable of passing that permission to another subject while mandatory access control means that the access control policy is uniformly enforced across all subjects and objects within the boundary of an information system.

Security awareness training is another example that when done correctly, can reduce the success of phishing campaigns and errors due to ignorance. Most cyberattacks start from social engineering techniques and spear phishing that target human factors within an organization. As such, trainings are more preventive to improve security awareness and educate the workforce for common security malpractices such as poor login credentials and clicking on malicious weblinks.

Contingency Planning, for example, decreases the risk of downtime and increase the availability of information technology systems. A full, complete, system backup that is updated and stored across multiple data centers across different geographies is highly important for institutions such as banks, critical infrastructures, technology and telecommunication companies that serve an immense number of

people on a daily basis. Without proper contingency planning, an organization is like a chicken in a farm, waiting to be slaughtered.

If controls are not being implemented and executed properly on a national level, national disasters are bound to occur eventually. Consider the serious data breach of Singapore's health system around July last year, which affected more than 1.5 million healthcare patients, including Singapore's existing prime minister Lee Hsien Loong[8]. It was a deliberate, targeted and well-planned cyberattack by an advanced, persistent threat group, not named to the public till today. After the data breach was discovered, there was an immediate response by the CSA. Teamwork was severely critical during entire process of incident response and disaster handling. Singapore's Integrated Health Information Systems acted immediately and implemented cybersecurity precautions when the first sign of unusual activities was discovered. Additionally, it quickly informed the Health Ministry and CSA to deal with the attack. Using a cybersecurity management framework that was consistent between the affected entities, teamwork was reflected among individuals in the same organization and key representatives across organization. Although Singapore did not prevent the serious data breach, the organizations involved carefully followed a pre-constructed cybersecurity risk management methodology to deal with this unfortunate issue promptly. As a result, further damage as a nation with huge assets and critical infrastructure was minimized. Singapore highlighted that teamwork is critical in any cybersecurity incident response.

Similarly, the U.S faces massive threats from nation-state adversaries but handles cybersecurity risk management effectively and collaboratively. The U.S faced a similar incident in June 2015 when the United States Office of Personnel Management(OPM) suffered a data breach of government data records from 4 million people[9]. This included people who had undergone background checks and were current or former government employees. Information targeted in the breach included personal identifiable information such as social securitiy numbers, names, dates and places of birth, and addresses. For this specific incident, the OPM should have dealt with this incident in a more collaborative, team-based and efficient manner like Singapore's Integrated Health Information Systems.

[8] Retrieved from https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most
[9] Retrieved from https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

It insufficient to comprehensively understand the U.S's cybersecurity risk management approach without analyzing the National Institute of Standards and Technology(NIST) framework and the United States Department of Defense. In terms of cybersecurity risk management for the U.S, I would argue that NIST framework is a better analog for my research topic. Likewise, it is shallow to study Singapore's cybersecurity risk management approach by only considering the MINDEF and CSA. One needs to also consider Internal Organization for Standardization(ISO).

NIST is a unit of the U.S. Commerce Department[10]. Formerly known as the National Bureau of Standards, NIST is responsible in promoting and maintaining measurement standards, being one of the oldest physical science laboratories in the United States with a world-class measurement and testing laboratory It has programs to assist industry and science to use these standards. However, more importantly in terms of cybersecurity, NIST implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S to adopt cybersecurity capabilities.

According to the official website, NIST's cybersecurity program supports its overall mission to promote U.S innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development that enhance economic security and improve the quality of life. It is key to note that NIST is a cybersecurity framework developed by the U.S, mainly for the U.S. As such, other countries may use other frameworks such as ISO for cybersecurity risk management. NIST provides cybersecurity standards and best practices that address interoperability, usability as privacy continues to be critical for the nation. NIST's cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.

[10] Retrieved from https://www.nist.gov/

ISO[11], on the other hand, is an independent, non-government international organization with a membership of 164 national standards bodies. ISO's key role is to develop and publish International Standards. It brings together experts to share knowledge and develop consensus-based, market relevant international standards that support innovation and provide solutions to global challenges. Other countries other than the United States such as Singapore may use this ISO international standards to get world-class specifications for products, services and systems to ensure quality, safety and efficiency to facilitate international trade. ISO has published 22598 international standards and related documents, covering industries such as technology, food safety, agriculture and healthcare. ISO's role is similar to a conductor in a band while the orchestra is made up of independent technical experts. The primary reason that I discussed ISO and NIST is that both Singapore and the U.S could better utilize and consider these frameworks for better cybersecurity risk management and controls.

The U.S is blessed with housing the most powerful technological companies in the world such as Google, Microsoft, Apple and Facebook. More importantly, there are many mature and dominant cybersecurity companies that specialize in firewalls technology such as Palo Alto and Fortinet, endpoint security such as CrowdStrike and FireEye and network based security such as Cisco. Therefore, should the U.S government require aid from the private sector for cybersecurity risk management, the U.S government could take advantage of these companies for cybersecurity risk assessment and subsequently implementing controls, which are part of cybersecurity risk management. Singapore, on the other hand, only has a few cybersecurity commercial firms such as MicroSec and Horangi Cyber Security which have smaller market capitalization and revenues. As such, the Singapore government will have lesser resources to utilize should it decide to rely on the commercial side. However, it is to my knowledge from working at Cisco that the Singapore government shares a close-knitted partnership with Cisco Talos, a threat intelligence sharing group that makes the internet safe for Cisco's customers, products and services.

[11] Retrieved from https://www.iso.org/home.html

Although the U.S uses the NIST framework or other frameworks such as ISO or CIS, Singapore has its own cybersecurity strategy. According to "Singapore's cybersecurity strategy" by Ter Kah Leng, Singapore's commitment to cybersecurity is reinforced in the latest five-year National Cybersecurity Masterplan 2018 which will provide strategic directions in securing the infocomm environment not only in the government and critical information infrastructure but also in the business and people sectors. Infocommunications is the expansion of telecommincations with information processing and content handling functions including all types of electronic communications on a common digital technology base, mainly through Internet technology.

According to the paper, Singapore is taking a balanced approach between security requirements and the ease of conducting business and daily activities. The vision of Masterplan 2018 is of Singapore is to be a trusted and robust infocomm hub by 2018. It focuses on three key areas. First, enhancing the security and resilience of critical information infrastructure. Second, increasing efforts to raise infocomm security awareness and adopting security measures among businesses and users. Third, growing Singapore's pool of infocomm security experts. The allocation of at least 8% of the government's infocomm technology budget to developing cybsecurity talent and the cybersecurity ecosystem underscores Singapore's commitment to engender a secure and resilient infocomm environment and a vibrant cybersecurity ecosystem. As such, Singapore has lesser resources and greater centralization in terms of cybersecurity risk management.

The U.S and Singapore are highly-developed societies that house critical infrastructures, intelligence property and digital assets that face cyber-related attacks on a daily basis. However, due to their mature cyber-defense infrastructures and collaborative approach in cybersecurity risk management, both countries are also effective in setting appropriate policies and efficient in implementing controls and appropriate incident response when necessary actions have to be taken from the top-down. However, both countries differ in the organizational structures, policy usage and implementation of cybersecurity risk management according to each country's government and culture.

4258 words

References:

1) ISO/IEC 27005:2018
2) ISO/IEC 31000:2018
3) ISO 31000:18
4) NIST 800-30
5) NIST 800-53
6) NIST CSF
7) Kohnke et al., *The Complete Guide to Cybersecurity Risks and Controls* (2016)
8) Refsdal et al., *Cyber-Risk Management* (2015)
9) National Security Agency. (n.d.). Retrieved from https://www.nsa.gov/
10) Cyber Security Agency of Singapore. (n.d.). Retrieved from https://www.csa.gov.sg/
11) Angelia Levy, "*An Overview of the Major U.S. Intelligence Agencies: What is difference between the DIA, NSA, CIA and FBI?"* Retrieved from https://angelialevy.com/2011/05/11/an-overview-of-the-major-u-s-intelligence-agencies-what-is-the-difference-between-the-dia-nsa-cia-and-fbi/
12) Kah Leng Ter, "*Singapore's cybersecurity strategy"*, NUS Business School, National University of Singapore, Singapore.
13) U.S Dept Of Defense. (n.d.). Retrieved from https://www.defense.gov/
14) Singapore MINDEF. (n.d). Retrieved from https://www.mindef.gov.sg/web/portal/mindef/home
15) Defence Science and Technology Agency. (n.d.). Retrieved from https://www.dsta.gov.sg/
16) https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most
17) https://en.wikipedia.org/wiki/United_States_Department_of_Defense
18) https://en.wikipedia.org/wiki/Ministry_of_Defence_(Singapore)
19) https://searchsoftwarequality.techtarget.com/definition/NIST
20) https://en.wikipedia.org/wiki/Infocommunications
21) https://www.nist.gov/
22) https://www.iso.org/home.html
23) https://www.nytimes.com/2016/10/07/us/booz-allen-hamilton-nsa.html
24) https://www.nytimes.com/2019/03/28/us/politics/hal-martin-nsa-guilty-plea.html
25) https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach
26) https://dod.defense.gov/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/