CYBER THREATS TO THE INTELLIGENCE COMMUNITY

Gianfranco Hernandez, Laren Spear, Melissa Pires, David Chaidez

NSC 325 - STEM for National Security

The University of Texas at Austin

Dr. Bianca Adair

May 7, 2021

Key Judgements

Our research question focuses on how the intelligence community (IC) might be vulnerable to cyber attacks from foreign adversaries or private citizens and what policy recommendations are needed to mitigate these risks. Our team focused on addressing vulnerabilities in the IC cyber defense strategy that might lead to data theft by criminals or foreign nations. We researched and examined our adversaries' use of cyber operations, primarily focusing on their intentions and capabilities. Furthermore, we discussed the need for research and development funding with the interest of continued cybersecurity in the IC in the face of new attacks.

This problem relates to U.S. national security because our competitors are becoming more adept at utilizing cyberspace capabilities to threaten our interests and improve their own strategic and economic goals. To protect our sensitive data, personally identifiable information, protected health information, personal information, intellectual property, governmental, and industry information from theft and destruction we must address and prevent the intelligence community's vulnerability to cyber-attack.

Key Judgement #1:The federal government will continue to work with private companies despite potential risks. We recommend a policy that the federal government should exercise more oversight and monitoring over private enterprises conducting cybersecurity work for the government

Key Judgement #2: Both insiders and outsiders present an information security threat. We recommend a policy to run more frequent audits of computer systems to detect anomalies, in both the public and private sectors.

Key Judgement #3: Oversight is a valuable part of our cybersecurity policy. Congressional oversight may be needed for the handling of known security exploits kept secret for intelligence purposes.

Introduction

The Intelligence Community has suffered multiple devastating cyberattacks, from both insiders and outsiders, that have damaged American intelligence collecting abilities as well as exposed the inner workings of our national security infrastructure. Systemic cybersecurity failures expose critical weaknesses to our adversaries, who may not even need to set foot in the country to steal classified information. Minimizing the occurrence and impact of future cyberattacks is in our nation's best interest.

Background

Our national security, economic prosperity and daily life relies on a steady and secure cyberspace. The intelligence community is vulnerable to a wide range of cyber threats. Highly skilled cyber actors and nation-states exploit these vulnerabilities to steal information and are improving capabilities to destroy, disrupt, or threaten the delivery of crucial services.

The Consumer Privacy Protection Act of 2017 focuses on protecting the personal information of customers, to prevent identity theft, to inform citizens and organizations about security breaches and prevent the mishandling of user's sensitive information. This law is related to our research because it is applicable to every organization that uses, gathers and transmits personally identifiable information of more than 10000 US citizens . Furthermore, the Cybersecurity Enhancement Act of 2014 was signed into law on December 18, 2014. It allows a voluntary public-private partnership to improve cybersecurity. This law relates to our research since it strengthens cybersecurity research and development, and workforce improvement and education.

Analysis/Substantiation

The federal government will continue to work with private companies despite potential risks.

The number of private companies conducting business with the government presents potential challenges when it comes to standards and regulations. While uniform standards are required for both government facilities and contractors, in practice, it can be hard to assess the security of all contractors. Respecting the independence of private companies but continuing to monitor them for compliance with federal cybersecurity regulations could limit the damage of future cyberattacks.

This policy recommendation is born out of the SolarWinds data breach. In early 2020, a foreign intelligence operation[1] directed at SolarWinds put IC network systems in danger. This breach took place through trojanized updates to SolarWinds' Orion IT monitoring and management software, went undetected for months, and is still ongoing. Post compromise activity following this supply chain compromise has included lateral movement and data theft. The campaign was the work of a foreign actors with resources to operational security. Furthermore, the attacker's post-compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.

Both insiders and outsiders present an information security threat.

Comprehensive security protocols should be enforced within both federal agencies and private companies that do work with federal agencies.We came into this judgement because of the June 2015 data breach, wherein OPM[2] discovered that the background investigation records of current, former, and prospective federal employees and contractors had been stolen. Specifically, the social security numbers of 21.5 million individuals were stolen from the background investigation databases, 19.7 million of whom were individuals that had applied for a background check along with 1.8 million non-applicants. Additionally, usernames and passwords that background investigation applicants used to fill out their background investigation forms were also compromised. Earlier in 2015, OPM discovered that the personnel data of 4.2 million current and former federal government employees had also been stolen. Potentially valuable personal information such as full name, birth date, home address and social security numbers were affected.

While outsider attacks can be devastating by themselves, insider threats must also be taken into account. No greater place is this principle evident than in the Edward Snowden data breach. According to a declassified document from the House Permanent Committee[3] on Intelligence (HPSCI), on March 25, 2009, Perot Systems sponsored Snowden for employment. From May 2009 to February 2012, Snowden worked in a variety of roles supporting IC contracts for Dell, which had purchased Perot Systems in 2009. He worked as an IT systems administrator at NSA. In December 2010, he started work in an uncleared "systems engineer/pre-sales technical role" for Dell. Through his employment, Snowden was able to collect and disclose documents that pertain to defense and intelligence programs of great interest to America's adversaries. The impact that his actions had on the intelligence community because of his data breaches and leaks were not fully disclosed, but such a significant breach cannot come without lasting effects. A combination insider/outsider attack combining the hacking power of a foreign

---

[1] FireEye. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor."
[2] "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation." United States House Committee on Oversight and Government Reform.
[3] House Intelligence (Permanent Select) Committee."H. Rept. 114-891"

nation with the collection capability of Snowden could be a nightmare scenario for intelligence.

Oversight is a valuable part of our cybersecurity policy.

Any one government agency exercising complete control over their part in cybersecurity has the potential to become biased in its own favor when choosing its handling. In 2017, a piece of malware known as WannaCry devastated businesses and individuals around the world. Born from a vulnerability in the SMB protocol in Windows XP through 7, which shares files between computers, affected machines would display a message requiring payment to regain access to the user's files[4]. This vulnerability was discovered by the NSA, but intentionally kept secret for unknown reasons. However, when this exploit was eventually leaked by the Shadow Brokers hacking group[5], it meant the number of unpatched computers had only continued to grow.

Had the NSA disclosed this vulnerability to Microsoft when it was discovered, a significantly smaller amount of computers would have been vulnerable to this attack. Whatever its motivations, the cost-benefit analysis of stockpiling the EternalBlue exploit deserves a second look. Perhaps if a congressional committee also had a say in whether this exploit would be disclosed to Microsoft, there would have been a more comprehensive analysis of the potential damage should the vulnerability be independently discovered. If a WannaCry incident were to happen again, the blame would not rest solely on the NSA.

[4] Wicker, Stephen B. 2021. "The Ethics of Zero-Day Exploits."
[5] Wirth, Axel. "The Times They Are A-Changin: Part Two."

Bibliography

1. FireEye. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor." FireEye. December 13, 2020. Accessed April 04, 2021. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

2. Hanauer, Larry. "OPM Hack Poses Overlooked Counterintelligence Risk for Economic Espionage." RAND Corporation. February 01, 2016. Accessed April 04, 2021. https://www.rand.org/blog/2016/02/opm-hack-poses-overlooked-counterintelligence-risk.html.

3. "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation." United States House Committee on Oversight and Government Reform. September 08, 2016. Accessed April 04, 2021. https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/.

4. Wicker, Stephen B. 2021. "The Ethics of Zero-Day Exploits." *Communications of the ACM* 64 (1): 97–103. https://doi.org/10.1145/3393670.

5. Wirth, Axel. "The Times They Are A-Changin: Part Two." *Biomedical Instrumentation & Technology* 52, no. 3 (2018): 236-40. doi:10.2345/0899-8205-52.3.236.

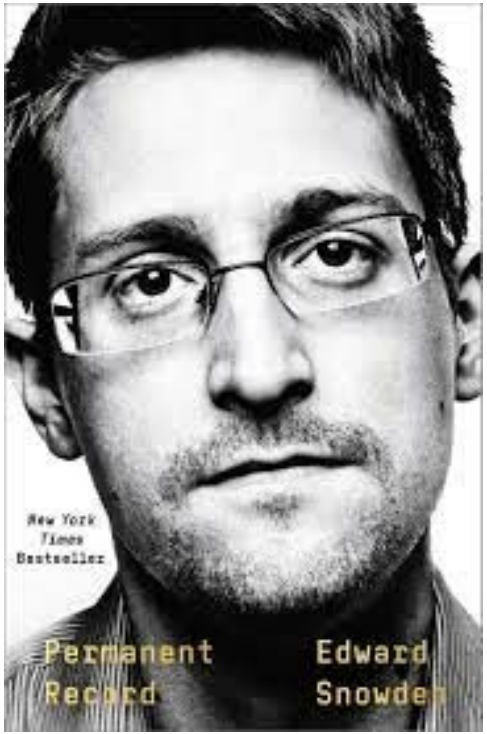
"Cybersecurity Resource Center Cybersecurity Incidents." U.S. Office of Personnel Management. Accessed April 04, 2021. https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

Geers, Kenneth. "The challenge of cyber attack deterrence." Computer Law & Security Review 26.3 (2010): 298-303.

"The Right Response to SolarWinds." Council on Foreign Relations. Accessed April 04, 2021. https://www.cfr.org/blog/right-response-solarwinds.

Cyber Threats to the Intelligence Community

Gianfranco Hernandez, Laren Spear, Melissa Pires, David Chaidez


New York Times Bestseller
Permanent Record
Edward Snowden


WANTED BY THE FBI
GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS
Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft
Yuriy Sergeyevich Andrienko
Sergey Vladimirovich Detistov
Pavel Valeryevich Frolov
Anatoliy Sergeyevich Kovalev
Artem Valeryevich Ochichenko
Petr Nikolayevich Pliskin
REMARKS
On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officers for their alleged roles in


Solarwinds

Research Question

- How is the intelligence community vulnerable to cyber-attacks from foreign states or private citizens and what policy recommendations are needed to mitigate these vulnerabilities?

Key Judgements

- The federal government will continue to work with private companies despite potential risks
- Both insiders and outsiders present an information security threat
- Oversight is a valuable part of our cybersecurity policy

Research Areas

- Data Breaches
  - Office of Personnel Management (OPM)
  - Solarwinds
- Edward Snowden (NSA Contractor)
  - Damage to intelligence collection capabilities
- EternalBlue Exploit

OPM Data Breach - *China*

- Background check records of current, former, and prospective federal employees and contractors were stolen
  - 19.7 million individuals that applied for a background check
  - 1.8 million non-applicants, primarily spouses of applicants
- Concerns of this information in the hands of foreign adversaries

SolarWinds - *Russia*

- Foreign intelligence operation directed at a US-based private company
  - Trojanized updates to SolarWinds' Orion IT monitoring and management software.
  - Begun as early as Spring 2020 and is currently ongoing

SolarWinds - *Russia*

Source:
https://techcrunch.com/2020/12/21/after-the-fireeye-and-solarwinds-breaches-whats-your-failsafe/

Edward Snowden

- The Breach
  - Mass downloads of classified documents
  - Defense and intelligence documents of great interest to America's adversaries
  - Disclosed to the media and later published
- Impact
  - Significant cost to rebuild intelligence capabilities

Source: Declassified document from the House Permanent Committee on Intelligence (HPSCI)

EternalBlue

- The NSA discovered an exploit in Windows XP through 7 and did not disclose it to Microsoft
- When the exploit was uncovered, hackers used it against American citizens (Wannacry)
- Files of unsecured computers encrypted, required users to pay to get their files back
- Billions of dollars in damage
- Every exploit provides offensive value, but also carries risk

Policy Recommendations

- The federal government should exercise more oversight and monitoring over private enterprises conducting cyber security work for the government
  - Are the standards really uniform?
- Run more frequent audits of computer systems to detect anomalies, in both the public and private sectors
  - Information should be safe from both insiders and outsiders
- Congressional oversight may be needed for the handling of known security exploits kept secret for intelligence purposes
  - The NSA is biased towards offensive use

Thank You!

This research would not have been possible without the guidance and support of our professor, Dr. Bianca Adair (CIA) and mentor, Launtz Rodgers (NGA).

References:

1. Hanauer, Larry. "OPM Hack Poses Overlooked Counterintelligence Risk for Economic Espionage." *RAND Corporation*. 01 Feb. 2016. Web. 04 Apr. 2021. https://www.rand.org/blog/2016/02/opm-hack-poses-overlooked-counterintelligence-risk.html

2.Geers, Kenneth. "The challenge of cyber attack deterrence." *Computer Law & Security Review* 26.3 (2010): 298-303.

3. "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation." *United States House Committee on Oversight and Government Reform*. 08 Sept. 2016. Web. https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/

4. "Cybersecurity Resource Center Cybersecurity Incidents." *U.S. Office of Personnel Management*. Web. 04 Apr. 2021. https://www.opm.gov/cybersecurity/cybersecurity-incidents/

5. FireEye. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor." *FireEye*. 13 Dec. 2020. Web. 04 Apr. 2021. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

6."The Right Response to SolarWinds." *Council on Foreign Relations*. Council on Foreign Relations. Web. 04 Apr. 2021. https://www.cfr.org/blog/right-response-solarwinds