10/22/2023

(IS 401/501-01 MERGED) (FA23) CYBERSECURITY PRINCIPLES

Case Study: Edward Snowden

Pod 6

Amogh Patel



# Table of Contents:

[**I. Introduction**](#_eozv3vflhd3a)

[**A. Brief overview of Edward Snowden and his actions**](#_r727uiy6pyr)

[**II. Background**](#_qoce5nr1mhmo)

[**A. Edward Snowden's role and behavior as an NSA contractor**](#_ja3yugf66tx3)

[**B. The significance of the leaked documents**](#_ty434m6a6u5c)

[**III. Snowden's Actions**](#_dntxjvl2t1d7)

[**IV. Cybersecurity Policies that led to the leaks**](#_fq5xeqngfcha)

[**V. Snowden’s Motivations**](#_2rwroqu026m6)

[**VI. Presentation of the Central Question: Hero or Traitor?**](#_w3wki5pl1mq3)

[**VII. Conclusion**](#_inhwahtl1l71)

[**VIII. References**](#_ot8c1z25e7zq)

# I. Introduction

Edward Snowden is a former National Security Agency (NSA) contractor who gained international attention in 2013 when he leaked a massive trove of classified documents to the media, revealing extensive government surveillance programs. Snowden's actions ignited a debate over whether he should be considered a hero for exposing what he saw as government overreach or a traitor for compromising national security.

## A. Brief Overview of Edward Snowden and His Actions:

Edward Snowden was born on June 21, 1983, in Elizabeth City, North Carolina. He came from a military family, and his parents divorced when he was young. Snowden struggled academically, eventually dropping out of high school and attending community college. He enlisted in the Army Reserve but left after five months due to health issues. He then worked various jobs, including as a security guard.

In 2006, Snowden joined the Central Intelligence Agency (CIA) as a contractor and later as an employee. His job was as a Telecommunications Information Systems Officer (TISO), a relatively low-level position. During his time at the CIA, he raised concerns about various issues, such as the process of overseas assignments for TISOs, pay discrepancies, and difficulties in transferring to other roles within the agency.

Snowden's decision to leak classified documents began in 2013 while he was working as an NSA contractor in Hawaii. He accessed and copied a vast amount of classified information, including details of NSA surveillance programs, and then fled to Hong Kong, later seeking asylum in Russia. In Hong Kong, he shared these documents with journalists, which led to a series of explosive news reports about government surveillance programs. Snowden cited his belief in protecting individual privacy and civil liberties as the main motivations for his actions.

# II. Background

## A. Edward Snowden's role and behavior as an NSA contractor

Edward Snowden served as an NSA contractor in various roles from May 2009 to June 2013. His roles and activities during his time as an NSA contractor were:

**1. Systems Administrator at Perot Systems (May 2009 to February 2012):** Snowden was an NSA contractor with Perot Systems, where he worked as a systems administrator. During this period, he supported intelligence community (IC) contracts, including those related to the National Security Agency (NSA). His duties included IT systems administration.

**2. Transition to Dell (February 2012):** Dell acquired Perot Systems in 2009, and Snowden continued his work as an IT systems administrator, supporting NSA's Agency Extended Information Systems Services (AXISS) contracts. During this time, he worked at NSA sites, and his role involved technical support for the IC.

**3. Background Reinvestigation (Fall 2010):** Snowden was due for a periodic background reinvestigation in the fall of 2010. This review found no derogatory information, although it was later described as "incomplete" and "did not present a complete picture of Mr. Snowden."

**4. Return to the United States (September 2010):** Snowden returned to the United States from overseas and sought a position with the CIA. However, his access to CIA information was denied due to an issue in the security database, Scattered Castles. He was eventually placed in a role that did not require a security clearance.

**5. Leave of Absence (August 31, 2011, to January 11, 2012):** Snowden took a leave of absence from his contractor job during this period.

**6. General Systems Administrator at NSA Hawaii (Early 2012 to June 2013):** After returning from his leave of absence, Snowden moved to Hawaii and took a position as a general systems administrator supporting Dell's AXISS work at NSA's Hawaii Cryptologic Center. He worked as a field systems administrator, primarily in technical support for NSA Hawaii.

**7. Security Clearance Issues:** Snowden encountered security clearance issues earlier in his career, with delays in obtaining the necessary access to information. His background reinvestigation was found to be incomplete and did not thoroughly investigate his CIA employment.

**8. Internal Conflicts:** Snowden had some internal conflicts and disagreements with co-workers and managers during his time at NSA Hawaii, including an incident involving a patch that caused server problems.

**9. "Breaking Point":** Snowden would later claim that his "breaking point" for his unauthorized downloads and disclosures of classified material was James Clapper's congressional testimony in March 2013, although he had already initiated unauthorized data transfers in July 2012.

Snowden's role as an NSA contractor primarily involved IT systems administration, technical support, and maintenance of information systems within the intelligence community, particularly at NSA facilities. His actions and decisions during this period ultimately led to the disclosure of classified information and his subsequent legal issues.

## B. Significance and impact of the leaked documents

The significance of the leaked documents in the context of Edward Snowden's actions is that they contained classified information about various U.S. intelligence and defense programs. Snowden's unauthorized disclosures of these documents had several important implications:

**1. National Security Impact:** The leaked documents included sensitive information related to military, defense, and intelligence programs. The exposure of these classified details posed a significant threat to national security by potentially aiding U.S. adversaries. It could have compromised the safety of American troops overseas and undermined U.S. efforts to protect against terrorists and nation-states.

**2. International Implications:** Snowden's actions had global repercussions. His disclosures not only made the information available to the general public but also to foreign governments and intelligence services, including Russia, China, Iran, and North Korea. This raised concerns about the potential exploitation of the leaked data by these countries for their own interests.

**3. Damage Assessment:** The full extent of the damage caused by Snowden's leaks remains unclear, but it prompted extensive assessments by the U.S. intelligence community and the Department of Defense. These assessments aimed to determine the scope of the harm and resulted in substantial financial costs as the government tried to mitigate the damage.

**4. National Security vs. Privacy:** Snowden's actions ignited a debate about the balance between national security and individual privacy. Some viewed him as a whistleblower exposing government surveillance programs that they considered invasive, while others saw his disclosures as harmful to national security.

**5. Security and Oversight:** The incident raised questions about the security of classified information and the oversight mechanisms in place to prevent such leaks. The government faced calls to enhance its security measures and improve the protection of sensitive data.

**6. Snowden's Motivations:** Snowden claimed to be acting as a whistleblower to inform the public about what he saw as government overreach in surveillance programs. However, the review of his actions suggested that his motivations may not have been solely driven by concerns about privacy rights, but also personal and other factors.

The significance of the leaked documents lies in their potential to affect U.S. national security, international relations, and the ongoing debate about the balance between government surveillance and individual privacy.

# 

# 

# III. Snowden's Actions

**1. Unauthorized Data Gathering:** Snowden used his position as a systems administrator at the NSA to collect classified information from NSA networks without proper authorization.

**2. Methods of Data Collection:** Snowden employed non-interactive downloading tools, commonly known as "scraping" tools, called "wget" and DownThemAll! to download files from NSA networks. He often used lists of website addresses and simple programming scripts to collect data.

**3. Accessing Personal Network Drives:** Snowden exceeded his authorized access by searching across other NSA employees' personal network drives and copying information from their drives. He also obtained security credentials from colleagues to access information beyond his authorized privileges.

**4. Infringement of Privacy:** Snowden infringed the privacy of at least several NSA personnel by searching their network drives without their knowledge.

**5. Additional Actions in Hawaii:** Snowden obtained a "thin-on-thick" computer setup, allowing him to exfiltrate data from the NSA network more easily. He took a two-week leave without pay, allegedly for medical reasons, and later fled to Hong Kong without informing his girlfriend or mother.

**6. Leaking Classified Information:** In Hong Kong, Snowden began releasing classified information to journalists, starting with Glenn Greenwald and Laura Poitras. He disclosed various surveillance programs, including PRISM and "upstream" collection, through articles published in The Guardian.

**7. Escape to Russia:** After the initial leaks, Snowden hid in Hong Kong and later traveled to Moscow, Russia, with the assistance of Wikileaks activist Sarah Harrison. He failed to board a flight to Havana and was eventually granted asylum in Russia in August 2013.

**8. Lack of Communication with Oversight Personnel:** Snowden did not raise concerns about the legality or morality of U.S. intelligence activities with NSA oversight personnel, intelligence community officials, or the appropriate oversight committees. He also did not use the available procedures for whistleblowers under the Intelligence Community Whistleblower Protection Act (ICWPA).

# 

# IV. Cybersecurity Policies that led to the leaks.

Based on the information provided in the book ‘Cybersecurity for Beginners’ by Raef Meeuwisse, there is no single policy that led to the leaks, several cybersecurity policies and practices allowed Edward Snowden to carry out his actions. These policies and practices include:

**1. Insufficient monitoring and evaluation of administrator activities:** The lack of robust monitoring and oversight of administrator activities allowed Snowden to go undetected as he accessed sensitive information and engaged in unauthorized activities.

**2. Toxic accumulation of domain knowledge:** Snowden was able to exploit his knowledge of the organization's security systems and vulnerabilities. This suggests that there were no policies in place to restrict or compartmentalize sensitive information to prevent any one individual from having comprehensive knowledge of security gaps.

**3. Toxic accumulation of privileges:** Snowden was able to retain privileges from his previous roles, allowing him access to various systems and data across the organization. The absence of a strict policy for revoking unnecessary privileges after job changes facilitated his actions.

**4. Lack of "Least Privilege" principle:** The organization did not adhere to the principle of providing individuals with the minimum level of access necessary to perform their job functions. This resulted in individuals like administrators having more access than required, increasing security vulnerabilities.

**5. Incorrect or inadequate classification of assets and information:** Sensitive documents, including security plans, were not adequately classified or protected. Snowden had access to these documents, providing him with insights into the organization's vulnerabilities.

**6. Inadequate system and process auditing:** There was a lack of regular and accurate auditing of security controls and processes to ensure they were in place and effective. The absence of such audits allowed security gaps to persist.

**7. Lack of two-person control for certain privileged functions:** Some critical functions did not require two individuals to operate, which could have acted as a deterrent against unauthorized actions by a single person.

**8. Complacent physical security:** The organization relied on trust and did not implement strict physical security measures to prevent the removal of devices like USB storage devices.

**9. Inadequate pre-screening processes:** While the organization acknowledged the need to improve pre-screening processes, this alone may not have been sufficient to detect security issues, given Snowden's track record and experience.

**10. Reliance on third-party contractors:** Snowden worked for a contractor, and the organization might not have had the same level of control and oversight as it would with direct employees. This allowed Snowden to access and exfiltrate sensitive data.

A combination of inadequate security policies, poor implementation of security best practices, and lax oversight allowed Edward Snowden to access and release sensitive information. It highlights the importance of robust security policies and practices, along with continuous monitoring and auditing, to prevent such breaches in the future.

# V. Snowden’s Motivations

Edward Snowden's motivations, as described in the ‘Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden’ by the House Permanent Select Committee on Intelligence, appear to be related to his concerns about various issues he observed while working as a contractor and later as a CIA employee. Some of these concerns included morale and retention issues among his colleagues, the process of assigning individuals to overseas locations, pay disparities, and difficulties in transferring to other positions within the organization.

Snowden seems to have been motivated by a desire to address what he perceived as problems or injustices within the intelligence community. He contacted his superiors and higher-ranking officials, including the Deputy Director for Support, to voice his concerns and recommendations. It appears that he wanted to make a positive impact and believed that raising these issues with higher-level officials was necessary to bring about change. Snowden's motivation, as presented in the text, was to "speak truth to power" and protect himself from potential reprisals for doing so.

# VI. Presentation of the Central Question: Hero or Traitor?

The question of whether Edward Snowden is a hero or a traitor is a matter of significant debate and depends largely on one's perspective. Different people view his actions through different lenses:

**Hero:**

**1. Transparency Advocate:** Snowden is seen as a whistleblower who exposed the extent of government surveillance and the potential infringement on civil liberties. His actions led to a much-needed public debate on the balance between national security and individual privacy.

**2. Sacrifices for Principle:** Supporters argue that Snowden risked his freedom and safety to reveal what he believed were unconstitutional and unethical government actions.

**3. Impact:** Some believe that his disclosures prompted necessary reforms and increased transparency in government surveillance programs.

**Traitor:**

**1. Violation of National Security:** Critics argue that Snowden's actions compromised national security by revealing classified information, potentially aiding adversaries, and weakening the government's intelligence capabilities.

**2. Legal Consequences:** Snowden's decision to flee the United States and seek asylum in Russia is seen by some as an evasion of justice, as he did not face the legal consequences of his actions.

**3. Unauthorized Disclosures:** Snowden did not follow established channels for whistleblowers, such as reporting concerns to superiors or appropriate oversight authorities, which is a key distinction for those who consider him a traitor.

Ultimately, whether Edward Snowden is considered a hero or a traitor is a deeply polarizing and subjective matter, with strong arguments on both sides. Public opinion varies based on one's views on privacy, government surveillance, and the role of whistleblowers in society.

# VII. Conclusion

The Edward Snowden case is a highly divisive and complex issue, provoking intense debate over whether he should be regarded as a hero or a traitor. His unauthorized disclosure of classified government information ignited a profound discussion about the trade-off between national security and personal privacy. Supporters view Snowden as a hero and advocate for transparency, applauding his bold exposure of what he perceived as unconstitutional government surveillance programs. They argue that his actions fostered essential public awareness, leading to reforms and greater government transparency.

Conversely, critics label Snowden as a traitor, asserting that his revelations endangered national security, potentially benefiting U.S. adversaries. They highlight his deviation from established whistleblower channels and his evasion of legal consequences by seeking asylum in Russia. Ultimately, whether Edward Snowden is viewed as a hero or a traitor hinges on individual perspectives, values, and priorities, underscoring the broader debate about government surveillance, personal privacy, and the role of whistleblowers in society. His case serves as a reminder of the intricate balance between safeguarding national security and protecting civil liberties, a debate that continues to shape public discourse and policy decisions.

# VIII. References

1. House Permanent Select Committee on Intelligence. (2016). Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden.

2. Cassidy, J. (2013, June 10). The New Yorker. Why Edward Snowden Is a Hero.

3. Meeuwisse, R. (2017). Cybersecurity for Beginners 2nd Edition: Case Study - Edward Snowden 2013.

4. ChatGPT - For outline and grammar check.