National Security Threats with Homogenous Software Adoption

Sheryl Cummings  
Course Number: CIST8950   
University Nebraska  
Omaha, NE  
Email Address: [cummings@unomaha.edu](mailto:cummings@unomaha.edu)

University Nebraska  
Omaha, NE  
Email Address: unomaha.edu

Ryan Thompson  
Course Number: CIST8950   
University Nebraska  
Omaha, NE  
Email Address:

University Nebraska  
Omaha, NE  
Email Address: unomaha.edu

Connor Flood  
Course Number: CIST8950   
University Nebraska  
Omaha, NE  
 Email Address:

University Nebraska  
Omaha, NE  
Email Address: unomaha.edu

Brian Gilbert  
Course Number: CIST8950   
University Nebraska  
Omaha, NE  
Email Address:

Table of Contents

[**ABSTRACT:** 4](#_Toc196048439)

[**1. INTRODUCTION:** 4](#_Toc196048440)

[**CROWDSTRIKE:** 5](#_Toc196048441)

[**JBS:** 5](#_Toc196048442)

[**2. LITERATURE REVIEW:** 6](#_Toc196048443)

[*PROBLEM STATEMENT* 6](#_Toc196048444)

[**WHY IS THIS AN URGENT OR SEVERE PROBLEM?** 7](#_Toc196048445)

[RESEARCH QUESTION(S): 7](#_Toc196048446)

[CONTRIBUTIONS MADE: 7](#_Toc196048447)

[*INVESTIGATIVE APPROACH* 7](#_Toc196048448)

[IMPLICATIONS FOR PRACTICE: 8](#_Toc196048449)

[IMPLICATIONS FOR RESEARCH: 8](#_Toc196048450)

[CHALLENGES: 8](#_Toc196048451)

[OTHER CHALLENGES 8](#_Toc196048452)

[*CONCLUSIONS* 9](#_Toc196048453)

[*REFERENCES* 10](#_Toc196048454)

**ABSTRACT:**

*In prior years, the mergers of firms in the defense industrial base system (DIB) had no impact on national security . Fast forward today where there is increased concerns over mergers and acquisitions. The landscape of threats to national security is concerning because companies have increased their footprint in mergers and acquisitions. This consolidation has created a national security risk when previously the only concern was in consolidation.*

*A survey was conducted to gather data analysis to help understand how software is selected in making informative decisions in the selection process. The survey was given to business leaders who make who are the decision makers based upon business needs. The survey covered software selection such as ease of use, functionality, ease of use, seamless integration, security best practices and standards for software assurance such as end-to-end encryption and risk management. The survey also targeted both the private sector and public sector to include the impact of market share among both sectors. The results showed business organization used xxxx. Based upon the survey x the government (private sector) felt the market share when selecting software, market share was not important.*

**KEYWORDS:** secure software development; secure software development framework (SSDF), secure software development best practices, software acquisition, software development lifecycle, software security, common vulnerabilities exploitation, industries best practices and standards, software assurance.

**1. INTRODUCTION:**

In prior years, the mergers of firms in the defense industrial base system (DIB) had no impact on national security[[1]](#footnote-2). Fast forward today where there is increased concerns over mergers and acquisitions. The landscape of threats to national security is concerning because companies have increased their footprint in mergers and acquisitions. This consolidation has created a national security risk when previously the only concern was in consolidation. Moreover, increased antitrust oversight has led to an increase in government challenges to mergers.[[2]](#footnote-3) This research paper introduces two case studies related to the project's development. The first case study discussion deals with CrowdStrike.

**CROWDSTRIKE:**

CrowdStrike is a well-known organization whose mission is to provide end-to-end point security while providing threat protection against cyber-attacks. This paper will also address policy recommendations to address cybersecurity risks associated with industry consolidation. For example, disruptions to food suppliers could lead to widespread food insecurity.

On July 19, 2024, a systems administrator at CrowdStrike caused the largest IT outage in American history. The system administrator performed a windows update which was neither validated, verified or followed the change management approval process. There was a security flaw discover in the Falcon sensor version 7.11 and above which caused the system to crash. This major outage caused 5.4 billion dollars’ worth of damage to many organizations globally to include Airline Industries, financial institutions, Amazon, healthcare industries and retail industries just to name a few financial institutions. [[3]](#footnote-4)

**JBS:**

JBS is major company known both globally and internationally as the world’s largest meat producer. JBS maybe the world’s largest meat producer but failed to protect their infrastructure against a cyber-attack.

JBS was affected by a phishing campaign from a Russian based group by the name of REvil. Revil held several American companies’ hostage by demanding ransomware in releasing the company’s data. Ransomware attacks account for 20% of all cyber-attacks while phishing attacks in the U.S. account for 47% of cyber-attacks.[[4]](#footnote-5)

When food suppliers encounter a cyber-attack, those industries would be affected and lead to a widespread food insecurity. For example, if Big Poultry Corporation produces 75% of domestic poultry products, a cyber-attack targeting them would create starvation conditions for large populations.

2. LITERATURE REVIEW:

Modern infrastructure enables adversaries to disrupt organizations such as cyber-attacks. This problem is exacerbated when a single company dominates specific industries or services, such as banking, healthcare, or food production.

Government oversight continues to be a challenge in addressing mergers and acquisitions in the defense industrial base sector. Not addressing this challenge could lead to conflicts between the goals of antitrust law fostering competition and nations security in protecting the security of the American people. [[5]](#footnote-6)

***PROBLEM STATEMENT***:

What is the primary problem that the study investigated?

Answer: The landscape of threats to national security is concerning because companies have increased footprint in mergers and acquisitions. The courts have to decide or analyze national security concerns in defense mergers because of the lack of competition in many defense markets, barriers to entry in those markets and limitations of non-antitrust tools for improving competition.

What has been done in the literature review?

**Answer:** The Department of Defense created five recommended actions to address national security concerns for company mergers or acquisitions:[[6]](#footnote-7)

* Strengthening merger oversight
* Addressing intellectual property limitations
* Increasing new entrants
* Increasing opportunities for small businesses
* Implementing sector-specific supply chain resiliency plans

**WHY IS THIS AN URGENT OR SEVERE PROBLEM?**

Answer: Mr. Michael McLaughlin, who conducted the research argued when companies merge, there is an increased risk competitively which increase national contracting world,[[7]](#footnote-8)

Researchers argued that it took longer to develop reuse of software components than developing a system. The lack of standards, reusable components and the granularity and generality of components made expectations difficult to achieve. Also the ownership to develop mitigated software independently would reduce communication and coordination efforts. [[8]](#footnote-9)

**RESEARCH QUESTION(S):**

What question related to the problem have not been answered by prior research?

Answer: How geographically software development teams do not communicate effectively across different industries and government sectors nor have the understanding on how to reuse software components in a rapidly changing environment.

**CONTRIBUTIONS MADE:**

The LeCroy software team developed a toolbox which can be integrated in a developmental environment and also be accessible to all members of ta geographical dispersed team.

***INVESTIGATIVE APPROACH***:

The LeCroy software team implemented customer-specific components, modification of existing components with the customers system. Members of the team worked across three geographical locations. Vendors of third-party components were located in various countries (more than 25 vendors total)[[9]](#footnote-10)

**IMPLICATIONS FOR PRACTICE:**

Supporting reusable components expanding across multiple platforms across geographical sites.

**IMPLICATIONS FOR RESEARCH:**

The potential benefits of implementing CBD methodologies in a globally distributed environment are many. Lessons from the aeronautics, automotive, electronics and computer hardware industries, in which Component Based architectures have been successfully employed for setting up globally distributed design and production in the reuse of software components[[10]](#footnote-11)[[11]](#footnote-12)

Policy Recommendations in national security for industry specific merges and acquisitions

**CHALLENGES:**

Researcher argued that it took longer to develop reuse of software components than developing a system. The lack of standards, reusable components and the granularity and generality of components made expectations difficult to achieve. Also the ownership to develop mitigated software independently would reduce communication and coordination efforts. Other challenges include each site having specialized experience in a different domain or market (e.g. site A specializes in the banking sector while site B specializes in the insurance sector. This could hinder the development of neighboring sectors and implementation of agility in the software design that offers future integration of existing solutions.[[12]](#footnote-13)

**OTHER CHALLENGES**:

Mergers and acquisitions does create challenges for innovation(s). These can hinder the DOD’s access to innovative products and services.

To only have one defense contractor as the sole provider to provide servers leaving other contract companies to not compete. The courts found the merged company would create monopoly having a competitive advantage

***CONCLUSIONS***:

A weakness in an organization’s security posture would set a dangerous precedence in opening the door to a cyber-attack and being a victim of ransomware attacks.

*REFERENCES***:**

“About Our Company.” *JBS USA | Sustainability Report*, https://sustainability2019.jbssa.com/chapters/who-we-are/about-our-company/. Accessed 13 Apr. 2025.

*America’s Data Held Hostage: Case Studies in Ransomware Attacks on American Companies*. United States Senate, Mar. 2022, p. 44, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf.

Computer Security Division, Information Technology Laboratory. “NIST Publishes SP 800-218A | CSRC.” *CSRC | NIST*, 23 July 2024, https://csrc.nist.gov/news/2024/nist-publishes-sp-800218a.

CrowdStrike. *External Technical Root Cause Analysis Channel File 291*. 25 July 2024, p. 12, https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

*Crowdstrike Falcon Platform Commands 3.02% Market Share in Endpoint Security*. https://enlyft.com/tech/products/crowdstrike-falcon-platform. Accessed 13 Apr. 2025.

“CrowdStrike Outage Explained: What Caused It and What’s next.” *WhatIs*, https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next. Accessed 2 Feb. 2025.

“---.” *WhatIs*, https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next. Accessed 2 Apr. 2025.

*Crowdstrike : Security Vulnerabilities, CVEs Published in 2022*. https://www.cvedetails.com/vulnerability-list/vendor\_id-28072/Crowdstrike.html?page=1&year=2022&order=1. Accessed 5 Feb. 2025.

*CVE - Search Results*. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=crowdstrike+vulnerabilities. Accessed 10 Apr. 2025.

*CVE-2022-2841 : A Vulnerability Was Found in CrowdStrike Falcon 6.31.14505.0/6.42.15610/6.44.158*. https://www.cvedetails.com/cve/CVE-2022-2841/. Accessed 5 Feb. 2025.

*CWE - 2024 CWE Top 25 Most Dangerous Software Weaknesses*. https://cwe.mitre.org/top25/archive/2024/2024\_cwe\_top25.html. Accessed 5 Feb. 2025.

*CWE - CWE-89: Improper Neutralization of Special Elements Used in an SQL Command ('SQL Injection’) (4.16)*. https://cwe.mitre.org/data/definitions/89.html. Accessed 5 Feb. 2025.

*DOD Needs Better Insight into Risks from Mergers and Acquisitions*. GAO-24-106129, United States Government Accountability Office, Oct. 2023, p. 49, https://www.gao.gov/assets/d24106129.pdf.

*Federalnewsnetwork.Com*. https://perma.cc/3PPF-H893. Accessed 12 Feb. 2025.

Jarzombek, Joe. “Software Assurance: Enabling Security and Resilience throughout SDLC.” *Assurance: Enabling Security and Resilience throughout SDLC*, https://csrc.nist.gov/CSRC/media//Projects/Forum/documents/2012/october-2012\_fcsm-jjarzombek.pdf.

Kotlarsky, Julia, et al. “Towards Agility in Design in Global Component-Based Development.” *Communications of the ACM*, vol. 51, no. 9, Sept. 2008, pp. 123–27. *DOI.org (Crossref)*, https://doi.org/10.1145/1378727.1389973.

Michael, McLaughlin. “National Security and Competition: How Courts Evaluate National Security When Assessing a Merger.” *Federal Trade Commission*, no. 6621, June 2024, https://jnslp.com/2024/06/27/national-security-and-competition-how-courts-evaluate-national-security-when-assessing-a-merger/#:~:text=3-,National%20Security%20and%20Competition:%20How%20Courts%20Evaluate,Security%20When%20Assessing%20a%20Merger&text=Michael%20McLaughlin%20examines%20the%20effect,ought%20to%20be%20framed%20cohesively.

Mohanty, Ashish. “The CrowdStrike Windows Outage: A Detailed Case Study.” *Workmates Core2Cloud*, 24 July 2024, https://cloudworkmates.com/2024/07/24/the-crowdstrike-windows-outage-a-detailed-case-study/.

National Security Agency, et al. “Securing the Software Supply Chain: Recommend Practices for Managing Open-Source Software and Software Bill of Materials.” *Enduring Security Framework*, NSA, ODNI and CISA, Dec. 2023, https://www.cisa.gov/sites/default/files/2023-12/ESF\_SECURING\_THE\_SOFTWARE\_SUPPLY\_CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20MANAGING%20OPEN%20SOURCE%20SOFTWARE%20AND%20SOFTWARE%20BILL%20OF%20MATERIALS.pdf.

“National Software Reference Library (NSRL).” *NIST*, Apr. 2016. *www.nist.gov*, https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl.

*NVD - CVE-2024-8465*. https://nvd.nist.gov/vuln/detail/CVE-2024-8465. Accessed 5 Feb. 2025.

Pascal, Zenker. *Modzero Security Advisory*. Modero Security Advisory, 22 Aug. 2022, modzero.com/advisories/MZ-22-02-CrowdStrike-FalconSensor.txt.

Paulin, Alois. “Measuring Impact on Confidence in Institutions by Their Use of Software Components.” *Proceedings of the Central and Eastern European eDem and eGov Days 2024*, Association for Computing Machinery, 2024, pp. 119–24. *ACM Digital Library*, https://doi.org/10.1145/3670243.3670249.

Riya Patel. “How to Mitigate the Threat of Industrial Base Consolidation.” *How to Mitigate the Threat of Industrial Base Consolidation*, Federal News Network, 11 May 2022, https://perma.cc/3PPF-H893.

*Secure by Design | CISA*. https://www.cisa.gov/securebydesign. Accessed 2 Feb. 2025.

“State and Local Government | CrowdStrike.” *CrowdStrike.Com*, https://www.crowdstrike.com/en-us/solutions/state-local-government/. Accessed 13 Apr. 2025.

*The Latest Ransomware Statistics (Updated January 2025) | AAG IT Support*. https://aag-it.com/the-latest-ransomware-statistics/. Accessed 2 Apr. 2025.

*The Model*. https://owaspsamm.org/model/. Accessed 2 Feb. 2025.

https://www.cve.org/CVERecord?id=CVE-2024-4040. Accessed 10 Apr. 2025.

https://www.cve.org/CVERecord?id=CVE-2022-2841. Accessed 10 Apr. 2025.

1. https://www.gao.gov/assets/d24106129.pdf [↑](#footnote-ref-2)
2. Leah Nylen and Michelle F. Davis, *Big Deals Being Chilled by Biden’s Aggressive Antitrust*

   *Agenda*, BLOOMBERG L. (May 10, 2023, 9:00 AM), https://perma.cc/P8S2-Q2BC. [↑](#footnote-ref-3)
3. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next [↑](#footnote-ref-4)
4. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf [↑](#footnote-ref-5)
5. https://www.gao.gov/assets/d24106129.pdf [↑](#footnote-ref-6)
6. https://www.gao.gov/products/gao-24-106129#:~:text=interviewed%20agency%20officials.-,Recommendations,its%20actions%20to%20address%20them. [↑](#footnote-ref-7)
7. https://jnslp.com/2024/06/27/national-security-and-competition-how-courts-evaluate-national-security-when-assessing-a-merger/ [↑](#footnote-ref-8)
8. https://dl.acm.org/doi/10.1145/3670243.3670249 [↑](#footnote-ref-9)
9. https://cacm.acm.org/research/towards-agility-in-design-in-global-component-based-development/#:~:text=The%20development%20team%20were%20distributed%20across%20three,various%20countries%20(more%20than%2025%20vendors%20in [↑](#footnote-ref-10)
10. https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF [↑](#footnote-ref-11)
11. https://cacm.acm.org/author/kuldeep-kumar/ [↑](#footnote-ref-12)
12. https://www.gao.gov/assets/imtec-93-16.pdf#:~:text=Even%20while%20proclaiming%20the%20potential%20of%20reuse%2C,reuse%20process%20are%20lacking%2C%20and%20standards%20to [↑](#footnote-ref-13)