NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

CAPSTONE APPLIED PROJECT REPORT

EFFECTIVE PATCH MANAGEMENT AND GOVERNMENT SYSTEMS

March 2023

By: **Cynthia M. Osborne**
Denayja S. Boone

Advisor: **Raymond D. Jones**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Capstone Applied Project Report

4. TITLE AND SUBTITLE EFFECTIVE PATCH MANAGEMENT AND GOVERNMENT SYSTEMS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Cynthia M. Osborne and Denayja S. Boone	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis establishes the importance of patch management and its role in the reduction of exploitable vulnerabilities and the increased security of government information systems (IS). As technology continues to evolve, cybersecurity has become a leading concern. The vast increase in computer usage and technological advancements have provided many benefits to organizations in both the private and public sectors. The need to protect ISs against cyber-attacks has grown at the same rate. Cybersecurity is not a new concept but its applicability continues to be a problematic concept or hindrance to incorporate into both legacy and new ISs across government and private entities. Government ISs tend to be more susceptible to cyber-attacks. Resiliency at the conception of an IS is imperative and maintaining that resiliency is key to sustaining the security posture of any IS. The primary goal of government ISs is to provide new capabilities and resources to the warfighter. New ISs rely heavily on the use of software and its ability to be upgraded or modified. Legacy systems often utilize outdated software. Both types of systems require maintenance throughout the lifecycle. Many government ISs operate out-of-date software versions or are not patched on a routine basis to ensure ISs are not exposed to vulnerabilities. Patch management is an important practice that can prevent the exposure to cyber-attacks the exploitation of known vulnerabilities and improve the cyber hygiene of ISs.

14. SUBJECT TERMS cyber-security, cyber, JCIDS, cyber resiliency, software, technology, information system, IS	**15. NUMBER OF PAGES** 59
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

EFFECTIVE PATCH MANAGEMENT AND GOVERNMENT SYSTEMS

Cynthia M. Osborne, Civilian, Department of the Navy
Denayja S. Boone, Civilian, Department of the Navy

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2023

Approved by: Raymond D. Jones
Advisor

Robert F. Mortlock
Academic Associate
Department of Defense Management

THIS PAGE INTENTIONALLY LEFT BLANK

EFFECTIVE PATCH MANAGEMENT AND GOVERNMENT SYSTEMS

ABSTRACT

This thesis establishes the importance of patch management and its role in the reduction of exploitable vulnerabilities and the increased security of government information systems (IS). As technology continues to evolve, cybersecurity has become a leading concern. The vast increase in computer usage and technological advancements have provided many benefits to organizations in both the private and public sectors. The need to protect ISs against cyber-attacks has grown at the same rate. Cybersecurity is not a new concept but its applicability continues to be a problematic concept or hindrance to incorporate into both legacy and new ISs across government and private entities. Government ISs tend to be more susceptible to cyber-attacks. Resiliency at the conception of an IS is imperative and maintaining that resiliency is key to sustaining the security posture of any IS. The primary goal of government ISs is to provide new capabilities and resources to the warfighter. New ISs rely heavily on the use of software and its ability to be upgraded or modified. Legacy systems often utilize outdated software. Both types of systems require maintenance throughout the lifecycle. Many government ISs operate out-of-date software versions or are not patched on a routine basis to ensure ISs are not exposed to vulnerabilities. Patch management is an important practice that can prevent the exposure to cyber-attacks the exploitation of known vulnerabilities and improve the cyber hygiene of ISs.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CVE	Common Vulnerabilities and Exposures
DOD	Department of Defense
DoIT	Department of Information Technology
IS	Information System
IT	Information Technology
NIST	National Institute of Standards and Technology
RMF	Risk Management Framework

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

A. PROJECT SUMMARY

Cybersecurity is a fast-paced global problem in both private industry and federal, state, and local government organizations. Keeping the nation's networks and information systems (IS) safe from infiltration is a top priority, especially for the Department of the Navy (DON). Patch management is an important piece of this security. However, patch management can be costly, time consuming, cumbersome, and overwhelming, which prevents the efforts from being regularly conducted. Is DON effectively implementing patch management best practices that will keep the nation's networks and information systems safe? How do these practices measure up against industry standards? Private industry has implemented strategies and processes that automate this process, saving time and ultimately money.

Information was gathered based on the results of studies conducted, articles written, and the authors' first-hand knowledge based on on-the-job observations in this area. The research includes evaluation of studies conducted by the United States Government Accountability Office, Security Scorecard's Government Cybersecurity Report, and the National Institute of Standards and Technology. These studies discuss the best practices for preventing vulnerabilities and find that patch management in most government information systems are lacking, creating vulnerabilities. Further evaluation should be conducted to determine how vulnerable these systems are and how can industry standards assist with closing those vulnerable windows.

B. BACKGROUND

While working in the field of information technology and cybersecurity at separate commands, both authors saw similar parallels in the security of DON's networks, including last minute mitigations to meet authorization criteria instead of timely mitigations to prevent vulnerabilities. This raised the questions of "Is the lack of patch management creating vulnerabilities in the DON's IS?" and "What are industry standards and best practices for patch management?"

Government information systems are targets of cybersecurity attacks. Understanding the significance of patch management and how its effective implementation can significantly reduce preventable compromises to government information systems is paramount. Emphasis is placed on the critical elements to the patch management process and understanding if the DON specifically follows this process to battle these attacks, compromises, and vulnerabilities. This study explores the exposure of government information systems to vulnerabilities that could potentially be remedied through effective patch management and its ability to reduce the exploitability of government information systems. Central to this study is the exploration of the types of exploitation government information systems are subject to and the common challenges observed from implementing an efficient patch management process. The purpose of this research method is to gain an understanding of the current security posture of government information systems lacking an effective patch management process and private industry best practices in comparison to that of the government.

Data collection includes studies from the United States Government Accountability Office, Security Scorecard's Government Cybersecurity Report, and the National Institute of Standards and Technology. This thesis uses a comparative analysis method of literature reviews. Comparative analysis led to the creation of a score card that demonstrates the validity of the claims, the reputation of the author and/or website, and the relevance to the issue. The comparative analysis led to the findings, conclusions, and recommendations discussed below.

C. FINDINGS AND CONCLUSIONS

This thesis explored the significance of effective patch management processes in preventing potential compromises to government information systems. Toward this objective, the research compared industry standards for information systems security to those adopted by DON in accordance with its Risk Management Framework (RMF). The method of data collection involved a comparative analysis of the literature on vulnerabilities, private industry/government best practices and patch management. The

research sought to determine if the lack of initial and continuous patch management has a direct connection to the vulnerability of government information systems.

Based on the analysis, it can be concluded that effective patch management significantly reduces and mitigates risk associated with vulnerabilities within various software applications and the number of known exploits within information systems.

Available information clearly shows that government agencies are particularly vulnerable to cyberattacks due to several factors. First, it was established that government agencies commonly use outdated operating systems and hardware. Second, it was also found that most IT executives have a hard time keeping track of the thousands of individual nodes on an organization's network environment, providing a vulnerable system. The most effective way to safeguard government information systems is through proactive and timely patching of known vulnerabilities.

This thesis also explored the best practices of patch management on reducing potential security compromises to government information systems. In addition to being a risk management exercise, patch management helps protect critical digital assets from total collapse or being ransomed by online attackers. Patch management is especially important because most cyberattacks happen between the time when a vulnerability is discovered and when a patch is made widely available. In summary, implementing a proactive patch management process, organizations can limit or eliminate data breaches.

D. RECOMMENDATIONS FOR FURTHER RESEARCH

The literature available on the security risks facing both private and government information systems shows that the risk of compromise is growing. The first line of defense for the DON should be to implement a proactive patch management process to minimize cyber-attacks following the discovery of vulnerabilities in information systems. Research indicates that attackers exploit known vulnerabilities that have been left unpatched for a significant period, making it the primary line of defense against cyberattacks. We recommend three things that government information systems must do to bring the greatest impact on their network environment:

1. Design a comprehensive security ratings software that evaluates the agency's aggregate security poise and assists teams in prioritizing and targeting vulnerabilities. A properly developed security performance management program can assist security teams to stay one step ahead of cyber criminals.

2. Take stock of essential digital assets, regardless of their location. Gaining a better understanding of critical digital assets can help security teams to identify vulnerable assets that are more likely to be compromised, creating a launchpad for threat actors to take control of critical network resources. The patch management process should be conducted on all digital assets.

3. Government information systems should also assess and monitor third-party applications and programs that can access critical digital assets. Attackers commonly enter, breach, or disable a network or website by first comprising third party applications before giving themselves escalated privileges within the larger organizational IT infrastructure.

This study has clearly demonstrated how government information systems are increasingly becoming victims of devastating online attacks. Future research on this topic could examine whether the government's willingness to pay hefty sums of money demanded by hackers before they can release vital information resources, they have held hostage is contributing to the recent spike in cyberattacks.

I. INTRODUCTION

A. BACKGROUND

For over a decade cybersecurity has become a leading initiative for the government. As technology continues to evolve the need to protect information systems against cyber-attacks grows at the same exponential rate. Cybersecurity is not a new concept; however, its implementation continues to be a problematic idea or hindrance for both legacy and new information systems. At the same time, building and maintaining resiliency for information systems is imperative. While software provides new technological advancements and capabilities, it also introduces the level of accessibility that attackers need to infiltrate and exploit vulnerable systems/networks.

Government information systems are primarily a target for cyber-attacks due to the nature of the systems and the information they contain. These attacks include but are not limited to phishing, malware, Man-in-the-middle, and Zero-day exploit. Automated attacks, such as those using malware or scripts, can take advantage of software vulnerabilities to gain unauthorized access to systems or steal sensitive information. As these tools become more advanced and easily accessible, they can be used by a wider range of attackers, including those with limited technical skills. This highlights the importance of regularly updating software and implementing strong security measures to protect against these types of attacks (GAO, 2003). A software program or operating system can contain weaknesses known as vulnerabilities, which can be exploited by hackers through specially crafted code targeting the vulnerability. The code is packaged into malware — short for malicious software (Symanovich, 2021).

Software companies release software patches regularly to fix bugs in their programs, address security problems, or add new functionality (Indiana University, 2018). Regular and consistent patch management is one of the primary ways of dealing with known software vulnerabilities. Patch management refers to the procedure of recognizing, obtaining, examining, and implementing software updates, which are commonly known as patches, on a computer network or system. (National Institute of Standards and

Technology [NIST], 2013). These patches are designed to fix security vulnerabilities, bugs, and other issues in the software. Patch management is an important aspect of maintaining the security and stability of computer systems and networks. It involves regularly checking for new patches, evaluating their relevance and potential impact, testing them in a non-production environment, and then deploying them to production systems. It also includes a process of keeping track of which patches have been applied to which systems and when, to ensure that all systems are up-to-date and secure.

This study examines the significance of patch management and how its effective implementation can significantly reduce preventable compromises to government information systems. Emphasis is placed on the "critical elements to the patch management process which include management support, standardized policies, dedicated resources, risk assessment, and testing" (GAO, 2003, p. 1). Also central to this study is the exploration of the types of exploitation government information systems are subject to and the common challenges observed from implementing an efficient patch management process.

B. PROBLEM STATEMENT

Government agencies are responsible for protecting sensitive information and maintaining the integrity of critical infrastructure. However, one of the major problems faced by these agencies is the lack of proper patch management. This creates vulnerabilities in the software used by these agencies, making them more susceptible to cyber-attacks.

Without proper patch management, government agencies may not be aware of new vulnerabilities or may not have the resources to properly address them. This can leave systems and networks open to exploitation by attackers, who can steal sensitive information or disrupt operations. Additionally, the lack of regular patching can also lead to compliance issues and penalties.

Proper patch management is essential for the security of government agencies. It allows them to address vulnerabilities, reducing the risk of cyber-attacks and ensuring the integrity of critical systems and information quickly and efficiently. The failure to implement adequate patch management can have serious consequences for the security and stability of government agencies and the nation.

In recent years, there has been a significant increase in the number of cyber-attacks targeting government information systems. These attacks can take many forms, from phishing scams and ransomware to advanced persistent threats and state-sponsored attacks. They can target various types of government organizations and can have devastating consequences on the operations and information security.

One of the main reasons for the increase in cyber-attacks on government information systems is the growing awareness of the value of the data held by these organizations. Government information systems often contain sensitive information such as classified and personal data and infrastructure control systems. Attackers are motivated by the potential financial gain from stealing this information or strategic advantage from disrupting the operations of government agencies. Additionally, the growing sophistication of hacking tools and techniques has made it easier for attackers to launch successful attacks on government information systems.

The increase in cyber-attacks on government information systems has also been driven by the increasing reliance on technology in government operations. The digitization of government services, the use of cloud computing, and the implementation of smart city infrastructure have all increased the attack surface of government information systems. As a result, government organizations must be more vigilant and proactive in protecting their information systems from cyber threats. This includes implementing robust security measures, regular security assessments, and incident response plans to mitigate the impact of cyber-attacks.

Despite the alarming rate of increase of cyber-attacks, many agencies fail to implement a patch management process that can eliminate known vulnerabilities. The importance of patching cadence lies in its ability to ensure that vulnerabilities are addressed in a timely manner, thus reducing the risk of cyber-attacks. A patching cadence that is too infrequent can leave systems exposed to known vulnerabilities for extended periods of time, while a cadence that is too frequent can disrupt the normal operations and cause inconvenience. Therefore, it is important to establish an appropriate patching cadence that balances the need for security with the need for operational stability. This can include regular patches on a weekly or monthly basis, as well as emergency patches as needed.

Additionally, having a standardized and automated patch management process can help to ensure that patches are applied in a consistent and timely manner, helping to reduce the risk of breaches. According to the Security Scorecard Government Report, patching cadence is an area that should receive considerable attention and care. However, companies across all industries frequently exhibit inadequate patching practices, missing out on the opportunity to protect their networks and essential information resources.

According to a recent survey, "80 percent of companies who suffered a data breach or a failed audit could have prevented it by having a better patch management system in place" (Ridzyowski, 2020). Patching is the one of the best approaches to address vulnerabilities in software products. Implementing patch management on Department of Defense (DOD) information systems that support government functions and warfighting present multiple challenges. It is important for organizations to develop a plan to patch systems effectively and efficiently to limit preventable compromise because software vulnerabilities are often exploited by attackers to gain unauthorized access to systems or steal sensitive information. By patching systems, organizations can address known vulnerabilities and reduce the risk of successful attacks.

Additionally, a well-planned and executed patch management process can also help organizations to comply with industry standards and regulations. Many regulatory bodies require organizations to demonstrate that they are taking appropriate steps to protect sensitive information and critical systems, and effective patch management is often a key component of this requirement. Organizations need to develop a patch management plan to effectively and efficiently identify and address vulnerabilities in their systems and networks, in order to reduce the risk of cyber-attacks, comply with industry standards and regulations and maintain the integrity of the systems and data.

This study investigated whether government information systems may be vulnerable and lack initial and continuous patch management. The study also explored the impact of a lack of effective and continuous patch management process by exploring the impact and frequency of avertible vulnerability attacks on government information systems. The problem is government information systems may be vulnerable and lack initial and continuous patch management.

C. RESEARCH QUESTIONS

The study explored the exposure of government information systems to vulnerabilities that could potentially be remedied through effective patch management and its ability to reduce the exploitability of government information systems. These are the questions asked:

1. Are government information systems vulnerable due to the lack of an effective patch management process?
2. Can private industry best practices enhance the current patch management process of government information systems?
3. What more can government entities do to protect information systems from vulnerabilities?

D. SCOPE

While evaluating information systems of private companies would take years to complete, understanding the best practices of private industry may help government entities with their patch management process. Though patch management spans across every type of information system, this research focused on private industry standards compared to the Department of the Navy's practices.

E. PURPOSE

Patch management is a critical aspect of maintaining the security of information systems. It involves regularly updating software and hardware to fix vulnerabilities and prevent attackers from exploiting them. The purpose of researching the significance of patch management on information systems is to understand the importance of staying up to date with security patches and to identify potential challenges in implementing effective patch management practices. This research can help organizations, particularly those in the government, better understand the risks associated with unpatched systems and how to mitigate them.

Effective patch management can reduce the risk of compromises to government information systems. Cybersecurity threats to government systems are an ongoing concern, with attackers constantly searching for vulnerabilities to exploit. Unpatched systems are often the target of these attacks, and the consequences of a successful attack can be severe. These can include data theft, disruption of services, and loss of public trust. By implementing effective patch management practices, governments can reduce the likelihood of successful attacks and minimize the damage caused by any that do occur.

Researching the significance of patch management on information systems is crucial for organizations, particularly those in the government, to understand the importance of maintaining the security of their systems. Effective implementation of patch management practices can reduce the risk of successful attacks and mitigate the damage caused by any that do occur. Governments should prioritize implementing effective patch management practices as part of their overall cybersecurity strategy to ensure the safety and security of their sensitive information.

II. RESEARCH METHODOLOGY

A. LITERATURE REVIEW

The topic of patch management and the direct relation to the security and vulnerabilities of Information Systems is vast and overwhelming. Narrowing the scope of this research was challenging. Research on the vulnerabilities for systems in private industry is abundant, and it was important to research private industry standards verse Department of Defense standards, specifically the Department of the Navy. Comparing industry standards on information security control efforts with the mandated Navy's Risk Management Framework (RMF) was a logical beginning, as RMF lays out the framework. RMF is a standardized approach to managing and mitigating risks to an organization's information systems. It is a process that guides organizations through the steps of identifying, assessing, and responding to risks to their information systems. The framework is used by many government organizations to comply with regulatory requirements and ensure the security of their systems. Compared to industry standards, the RMF is a comprehensive framework that takes a holistic approach to risk management. It was discovered through literature reviews that the lack of patch management in information systems played a very large part in the vulnerabilities of both private industries as well as government Information Systems.

The research process began with the question: "Does effective patch management factor into the vulnerability of Information Systems?" Beginning with literature reviews by reading articles on the specific topic of risk mitigation and vulnerabilities, research was available, and thus the best plan of action was to use a comparative analysis using literature reviews. Each reference studied was evaluated with a scale of questions (see Table 1). Each answer was then assigned a numerical value, and the total determined the credibility and relevance of each reference (see Table 2).

B. DATA CRITERIA

As the research questions suggest, there was an interest in determining if patch management was a critical component of keeping IS safe from vulnerabilities. To decide, we sought out information from government reports, military new articles, private industry, and reputable Information Technology/ Information Systems blogs to which subject matter experts in the field have contributed. This information discovered discusses the pros and cons of patch management, as well as best practices within industry standards and government organizations. Each reference was evaluated on its reputable merit and if it was a contributed site or government sponsored. The source of information was considered, as well as the emphasis on government IT/IS or private industry IT/IS. Results of this phase of the research process are provided in Table 1 and Table 2.

Table 1. Reference Score Card

Reference Title	Type of Reference	Similar Data	Contrasting Data	Article Relevance 1 (low) – 5 (high)	Additional Notes About the Reference
Information Security Effective Patch Management is Critical to Mitigating Software Vulnerabilities	Government Report	Critical steps to cybersecurity include standard patching polices. Patch management an effective cybersecurity mitigation. 3) Patches are not frequently or correctly applied (Dacey, 2013).	Ultimately, more rigorous SWING practices may result in the protection from attacks (Dacey, 2013)	5	*Report written and distributed by the General Accounting Office.*
Guide to Enterprise Patch Management Technologies	Peer Whitepaper	Patching is most ubiquitous means of addressing vulnerabilities (Soupaya, 2013).	No significant contrasting data	3	*Implements a honey-pot environment to "capture" vulnerabilities.*
Patch Management: Benefits and Best Practices	Internet IS Article	Software contains vulnerabilities. Required patch management fixes those vulnerabilities and minimizes the risk of cyber-attacks. (Rapid7, 2021).	Enforced regulations will continue to be the industry standard because businesses are significantly financially impacted by cyber risks. (Rapid7, 2021).	1	*Although the data is well-known and relative to how industry is conducting IS cybersecurity, this article is written and distributed by a cybersecurity vendor.*

Reference Title	Type of Reference	Similar Data	Contrasting Data	Article Relevance 1 (low) – 5 (high)	Additional Notes About the Reference
Managing Software Updates Still a Government Stumbling Block	Digital Magazine Article	Patch management provides a secure foundation. Manual patching makes updates more cumbersome, especially if disconnected systems are present. This truth is prevalent in government IS (Raths, 2019).	Outdated software makes maintenance challenging, if not impossible. Backups are minimal. Government agencies generally do not consider themselves high risk. (Raths, 2019).	1	*A website that focuses on technology in the government sector.*
60% of Breaches in 2019 Involved Unpatched Vulnerabilities	Information Security Blog	A high number of breaches were reported even though software patches were available (Truta, 2015).	Automation will potentially reduce the number of breaches (Truta, 2015). This is not new data, but other literature is not as blatant about automation as this article.	2	*Security Blogger Network that does not publish contributed articles.*
Top cybersecurity facts, figures, and statistics	Digital Magazine Article	The teleworking environment has left open vulnerabilities during the Covid-19 pandemic (Carlson, 2021).	No significant contrasting data (Carlson, 2021).	3	*This article focuses on industry statistics related to cybersecurity and do not publish contributed articles.*

Reference Title	Type of Reference	Similar Data	Contrasting Data	Article Relevance 1 (low) – 5 (high)	Additional Notes About the Reference
Information Assurance Vulnerability Compliance Tracking and Reporting for U.S. Navy Ships	U.S. Navy IT Digital Magazine Article	Regular software maintenance provides a secure posture and reduces the risk of attacks (Vigil, 2009).	The Department of Navy implemented its own patch management application to protect ship networks. (Vigil, 2009).	3	This is a Navy supported magazine; the article is outdated, and more advanced tools have since been implemented.
The Navy's Networks Are Vulnerable to Cyber Attacks—It's Time for Action	Digital Magazine Article	It is crucial to implement technologies that enable ongoing surveillance of all networks and devices and the identification and segregation of non-compliant devices. (Goure, 2019).	The Navy is ill prepared to address growing threats. (Goure, 2019).	3	This is an interpretative based website, and though the author of this article is reputable, the website boasts an appropriate source of controversy.
NIST Special Publication 800-40 Rev 3 Guide to Enterprise Patch Management Technologies	NIST (Dept of Commerce) Online Database	Patches provide security updates to vulnerable systems and software (NIST, 2013).	Lack of consistent patching techniques will cause problems. Being able to override patches will create more vulnerabilities. (NIST, 2013).	5	*NIST is a government entity that provides a standardized cybersecurity framework for government entities and private industry to mitigate vulnerabilities.*

Reference Title	Type of Reference	Similar Data	Contrasting Data	Article Relevance 1 (low) – 5 (high)	Additional Notes About the Reference
5 Reasons Why General Software Updates and Patches Are Important	Internet IS Article	Software updates include software patches and prevent hackers from being successful (Symanovich, 2021).	No significant contrasting data	1	*Although the data is well-known and relative to how industry is conducting IS cybersecurity, this article is written and distributed by a cybersecurity vendor.*
The Importance of Software Updates and Patches	Internet IS Article	The suggested solution is to keep a regular patching cadence. Organizations do not do this well. Understaffed and unqualified IT staff makes enterprise patching difficult. (Ridzyowski, 2020).	Most organizations who are victims of breaches, could have avoided the breach by a regular patching cadence (Ridzyowski, 2020).	1	*Although the data is well-known and relative to how industry is conducting IS cybersecurity, this article is written and distributed by a cybersecurity vendor.*

Table 2. Reference Credibility

Reference Title	**Is this a government supported reference? (+1 for Yes)**	**Does the site allow contributed articles? (+1 for No; -1 for Unknown)**	**Is this a reference solely based on data from a Government Agency? (+2 for Yes)**	**Is this a reference based on data drawn from private industry? (+1 for Yes)**	**Is this a known prestigious organization? (+1 for Yes)**	**Total:**
Information Security Effective Patch Management is Critical to Mitigating Software Vulnerabilities	Yes (1)	No (1)	Yes (2)	No	Yes (1)	5

Reference Title	Is this a government supported reference? (+1 for Yes)	Does the site allow contributed articles? (+1 for No; -1 for Unknown)	Is this a reference solely based on data from a Government Agency? (+2 for Yes)	Is this a reference based on data drawn from private industry? (+1 for Yes)	Is this a known prestigious organization? (+1 for Yes)	Total:
Guide to Enterprise Patch Management Technologies	No	No (1)	No	Yes (1)	Yes (1)	3
Patch Management: Benefits and Best Practices	No	Unknown (-1)	No	Yes (1)	Yes (1)	1
Managing Software Updates Still a Government Stumbling Block	Yes (1)	Unknown (-1)	No	Yes (1)	No	1
60% of Breaches in 2019 Involved Unpatched Vulnerabilities	No	No (1)	No	Yes (1)	No	2
Top cybersecurity facts, figures, and statistics	No	No (1)	No	Yes (1)	Yes (1)	3
Information Assurance Vulnerability Compliance Tracking and Reporting for U.S. Navy Ships	Yes (1)	No (1)	No	No	Yes (1)	3
The Navy's Networks Are Vulnerable to Cyber Attacks—It's Time for Action	Yes (1)	No (1)	No	No	Yes (1)	3

Reference Title	Is this a government supported reference? (+1 for Yes)	Does the site allow contributed articles? (+1 for No; -1 for Unknown)	Is this a reference solely based on data from a Government Agency? (+2 for Yes)	Is this a reference based on data drawn from private industry? (+1 for Yes)	Is this a known prestigious organization? (+1 for Yes)	Total:
NIST Special Publication 800-40 Rev 3 Guide to Enterprise Patch Management Technologies	Yes (1)	No (1)	Yes (2)	No	Yes (1)	5
2018 Government Cybersecurity Report	Yes (1)	No (1)	No	No	Yes (1)	3
5 Reasons Why General Software Updates and Patches Are Important	No	Unknown (-1)	No	Yes (1)	Yes (1)	1
The Importance of Software Updates and Patches	No	Unknown (-1)	No	Yes (1)	Yes (1)	1

C. COMPARATIVE ANALYSIS

This thesis used a comparative analysis method of literature reviews. The main purpose of this research method is to gain an understanding of the current security posture of government information system with the lack of an effective patch management process and private industry best practices in comparison to that of the government. Each reference studied was evaluated with a scale of questions (see Table 1). Each answer was assigned a numerical value, and the total determined the credibility and relevance of each reference. Comparative analysis provided insights and understanding that helped understand the differences between government processes and industry standards. Trends and patterns were identified through this process.

It was discovered through literature reviews that the lack of patch management in information systems played a very large part in the vulnerabilities of both private industries as well as government Information Systems. Moreover, due to limited funding and resource shortages in government sectors, private industry has better patch management process and implementation to resolve known vulnerabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESEARCH REVIEW

A. VULNERABILITIES IN GOVERNMENT INFORMATION SYSTEMS

As technology continues to evolve, government agencies become more reliant on information systems to perform day-to-day activities. Information systems make many processes more efficient, however, there are shortcomings with using technology. Hackers and cybercriminals are constantly finding new ways to exploit vulnerabilities in technology, making it difficult for entities and individuals to protect their sensitive information. Cybersecurity has been a leading effort for government agencies for the last decade as cyber-attacks have increased at an exponential rate over the years. As cyber-attacks have matured, and technology has advanced, automation has decreased the length of time it takes to infect and spread an attack. Dacey discusses the CERT/CC and notes that what "once took weeks or months…now may take just hours or minutes" (2003, p. 4). According to a 2018 Government Cybersecurity Report by Security Scorecard, although government agencies appear to be improving their cybersecurity posture, the performance of the Endpoint Security, Network Security, and Patching Cadence are still poorly performed. (Security Scorecard, 2018).

David Raths (2019) describes an audit in March 2019 of the Maryland Department of Information Technology (DoIT) by the state Office of Legislative Audits in his article, "Managing Software Updates Still a Government Stumbling Block." During the 2019 audit, issues seen frequently throughout government organizations were uncovered. The Maryland DoIT found workstations running on outdated software applications, which demonstrates the potential for vulnerabilities. Software patching provides updates that mitigate these vulnerabilities as the software companies discover the vulnerabilities and are typically provided regularly by the company/developer. Raths continues to describe how the Maryland DoIT audit found that the workstations had not been updated with the latest releases for three application software products that are known to have ongoing security-related vulnerabilities increasing the risk of security breaches.

Government agencies often may not think that updated computer systems and software are important because they may not fully understand the potential risks associated with outdated technology. This lack of understanding could be due to lack of technical expertise within the agency or lack of emphasis on cybersecurity within the organization. Without a clear understanding of the potential risks, agencies may not see the value in investing in technology upgrades and may prioritize other expenses. There are several reasons why government agencies may not spend money on IS. One reason is budget constraints, as government agencies often have limited funds, they may prioritize other expenses such as personnel, infrastructure, research and development, and program services over investing in IS. Another reason is that government agencies may not fully understand the potential benefits of investing in IS, such as cost savings, increased efficiency, and improved security. Additionally, the procurement process for government IS can be slow and bureaucratic, making it difficult for agencies to acquire the technology they need quickly and easily. Furthermore, government agencies may also have concerns about the risks of investing in IS, such as vendor lock-in, lack of scalability and potential for technical issues. Furthermore, there may be a lack of understanding of the potential benefits of IS, and the decision-makers may not fully understand the value of investing in IS.

Like David Raths' research, Dacey's 2003 GAO report also identified that government agencies are using outdated computer software, such as unsupported Windows operating systems. The 2003 GAO report also uncovered that agencies are not applying freely available software patches and not creating effective backups (2003). Backups are critical for ensuring the continuity of an organization's operations. Backups provide a copy of an organization's data and systems, which can be used to restore operations in the event of a disaster, such as a natural disaster, cyber-attack, or hardware failure. Backups also protect organizations against data loss, which can occur due to human error, software bugs, or other unforeseen events. This is important because data loss can result in significant financial and reputational damage. Additionally, backups are also used for compliance and regulatory reasons, as many industries have regulations that require organizations to retain and protect certain types of data. Furthermore, backups also help organizations to more

quickly recover from a disaster, by having a copy of the data and systems available that can be restored in a short amount of time, minimizing the downtime and disruption to operations.

The COVID-19 Pandemic has highlighted Cyber vulnerabilities facing government agencies. The effects of the pandemic have extended beyond economic and health crises to include cyber vulnerabilities. Data shows that cyber threats have spiked by as much as 40% during the global health crisis as bad actors seek to exploit the anxiety and the global uncertainty in the wake of the coronavirus pandemic (Joyce & Thomas, 2020). The public sector is particularly impacted by this increased rate of cyberattacks. This comes against a backdrop of government agencies who find the concept of remote work alien. The government has been caught up in trying to protect thousands of remote workstations which are potentially insecure to online attacks. Therefore, many government agencies have found themselves unprepared for handling the security demands of a remote workforce in addition to protecting critical IT infrastructure from cyber risks. The new security environment is a reality that is facing local, state, and federal agencies. This could potentially be an ongoing issue for government agencies as the work environments continue to evolve into hybrids of on-site and remote work.

In an article written by Brian Thomas for the BITSIGHT website, Thomas references a Bloomberg report on a cyber-attack incident that happened to the U.S. Department of Health and Human Services (HHS) in March 2020. This attack, which was aimed at undermining the government's COVID-19 response, had HHS servers overwhelmed with millions of hits per second. This attack was designed to take the servers down. Believed to be the work of foreign actors, the attack on HHS information systems was "linked to a wave of misinformation by social media, email, and text which falsely claimed that the U.S. president was on the verge of declaring a two-week mandatory lockdown for the nation" (2020, paragraph 3). Because citizens use the government to provide essential services and information, they then become victims of attacks, which leads to confusion and misinformation. Thus, the goal of these cyber criminals is achieved.

Part of the problem arises from the fact that government agencies have mistakenly believed that they are not prime targets for cybercrimes. The result has been inattentive or

absent patch management processes coupled with limited resources to deal with online security risks. In David Raths' article, he references an interview with Peter Romness, the head of cyber security solutions in the U.S. Public Sector CTO Office at Cisco Systems. Romness discusses how common it is to hear people say that basic housekeeping and patch management would be sufficient to prevent most security breaches (2019). However, IT security teams acknowledge the difficulty associated with implementing a patch management process, especially due to budget constraints. The difficulty of employing qualified IS professionals does not help with the maintenance of the security posture. Romness also notes how IT executives find it challenging to manage the thousands of computers that require frequent patching and updating and often do not even know every system in their IT infrastructure (2019). This makes critical security fixes to slip through the cracks. To compound the problem, most government agencies only develop patches or discover vulnerabilities. This means that undetected or newer threats will not be addressed by the latest patches.

B. THE IMPACT OF PATCH MANAGEMENT ON POTENTIAL VULNERABILITY REDUCTION.

The impact of a cyberattack on government information systems can be catastrophic. While researching this topic, one finding has been that there is a common theme throughout the various data written about government-based IS. In most cases, the single biggest reason for these successful hacking attempts boils down to a fatal information security flaw: government agencies are still using obsolete computer software, such as earlier versions of the Windows operating system that are no longer receiving security updates from Microsoft. Research also reveals that most government agencies are not proactively deploying freely distributed software patches. It is also common to find government agencies without effective backup plans.

Amongst IT/IS professionals, it is well known that most data breaches are facilitated by a known vulnerability for which a patch was widely available. Timely patching is essential. When new bug fixes in a software program are released, attackers compare existing software with the patch to pinpoint vulnerabilities being fixed. The whole process can be accomplished in a matter of minutes, rather than days, enabling hackers to

create malware targeting these security holes for systems that have not deployed the new patches.

Although estimates vary, there is a consensus among cybersecurity professionals that approximately 80% of cyberattacks exploit vulnerabilities for which fixes have been developed, and most exploit vulnerabilities that could have been fixed more than a year earlier. Studies also show that most attacks use common vulnerabilities, so fixing these common exploits should be a priority after assessing their potential security impact on IS. Therefore, patching helps minimize risks. Therefore, patching is a risk management process that can be used to mitigate intrusion to a manageable level.

Patch management is one of the most effective ways of reducing the number of vulnerabilities within any information system. Patches are implemented to correct software bugs after the release of the initial software. Software patch releases are commonly known amongst IT/IS professionals, and ensuring the patches are implemented on any connected network will protect assets from hacks, viruses, malware—forms of exploitation. The National Institute of Standards and Technology (NIST) Special Publication 800-40 Rev 3 recommends automating the organization's patch mangement as much as possible in order to focus on other security functions. This publication describes the various approaches to addressing patch management, which is outside the scope of this research. However, this publication is a trustworthy resource that emphasizes the importance of patch management to all IS's security posture (2013).

Patches are also frequently released to address known security vulnerabilities within operating systems. Information system owners are notified of patches to implement that will enhance the security posture of their operating systems. In Dacey's GAO report, it is stated: "According to CERT/CC, about 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches; however, such patches are often not quickly or correctly applied" (2003, pp. 5). Additionally, cyber-enemies are becoming more knowledgeable and are discovering vulnerabilities faster than the software vendors can mitigate. Implementing and maintaining frequent and effective patch management practices is the best way to protect against these cyber vulnerabilities.

Government agencies are more susceptible to known vulnerabilities due to the lack of effective patching. Due to funding issues and lack of resources, government agencies are known to procrastinate patching. Legacy systems also create vulnerabilities. These legacy systems often have unsupported, end-of-life software, leaving these agencies vulnerable. Experienced IS professionals in the DON often experience the need to justify the course of action (COA) plans due to legacy systems. Standardized patch management policies, procedures, and tools exist, but often the IS/IT community is spread thin and unable to act in a timely manner. Dacey (2003) identifies some best practices in the GAO report that can help with risk mitigation, which include exercises such as dedicated resources and tasking, current technology inventory tools, regular system scanning and distributing patches, and testing.

An effective patch management process can impact various areas of business continuity. These areas include but are not limited to enhanced security (reduction of a security risk), up-to-date software, budget reduction for fixing exploited vulnerabilities, maintain cyber-security compliance, enhance vulnerability and software improvements. The Rapid7 website has provided eight key steps to the patch management process:

1. Develop an up-to-date inventory of all your production systems.
2. Devise a plan for standardizing systems and operating systems to the same version type.
3. Make a list of all security controls that are in place within your organization.
4. Compare reported vulnerabilities against your inventory.
5. Classify the risk.
6. Test.
7. Apply the patches.
8. Track your progress. (Rapid7, 2021, paragraph 7)

These eight steps laid out by the Rapid7 (2021) website are meant to be a strategic approach to a patch management course of action. There are important aspects of this

approach that will reduce the labor hours, the cost associated with that labor, as well as keeping the network secure and updated. Rapid7 indicates that updating asset management will provide the mitigation team the ability to understand what is on the network and where the assets are located. Asset management can also help with software version control and IP address management (Rapid7, 2021). Rapid7 states that standardization of all assets makes patching and remediation faster and more efficient (2021). "Keeping track of firewalls, antivirus, and vulnerabilities will provide information regarding the status of assets, what is being protected, and which assets are associated with those protection methods" (Rapid7, 2021, paragraph 21). Rapid7 recommends understanding which vulnerabilities exist for each asset because that will help to understand the overall risk to the organization (2021). If you understand the priority of the assets, according to Rapid7 (2021), this will determine which assets are critical to the organization and will need to be remediated quickly. The more critical the asset, the higher the risk, the faster that asset will need to be remediated. Rapid7 (2021) recommends before moving patches into the production environment, testing a sample of assets in a lab environment to prevent issues is key. The article goes on to suggest that once the assets have been prioritized, applying the patches is key to remediating the vulnerabilities (Rapid7, 2021). Lastly, Rapid7 (2021) advises that rolling patches out in batches is recommended to avoid unexpected results. Finally, the article states that once patches have been applied, assess, and reassess to ensure patching was successful (Rapid7, 2021).

Consistency is also very important to effective patch management. Finding an effective patching cadence can take time for an organization to figure out. If an organization gets behind on this cadence, not only does the risk increase, but the amount of time it takes to mitigate the risk also increases, leaving the organization especially vulnerable. One thing that Dacey specifically calls attention to in the 2003 GAO report is the support of Senior Executives. "Management recognition of information security risk and interest in taking steps to manage and understand risks…is important to successfully implementing any information security–related process and ensuring that appropriate resources are applied" (2003, pp. 11). This statement is especially important to emphasize

because often Senior Executives do not understand the importance of patch management and the effort required to sustain this effort.

When it comes to effective vulnerability management, there are several core principles that need to be adhered to. The main objectives of vulnerability management include reducing the total number of security loopholes in an organization's IS, decreasing the time taken to fix vulnerabilities, and generating actionable insights for concerned parties. The first principle of effective patch management is the identification of potential security loopholes that could be exploited by nefarious actors. To discover where vulnerabilities may reside in an IS, it is imperative to undertake a thorough inventory management of the organization's assets in terms of the devices owned by the organization and the operating systems and software used. The second principle of effective patch management involves assessment of potential security loopholes of the organization's mapped information environment. This step involves using a platform that allows the organization to monitor its critical IT assets. After analysis of known and zero-day vulnerabilities, the next step in effective patch management process involves the prioritization of vulnerabilities identified. The process involves evaluating the risk level of hundreds of vulnerabilities and their exploitability. Ideally, the IT team should address vulnerabilities which have the highest likelihood of being exploited by attackers first before moving to less critical vulnerabilities. The last core principle of effective patch management involves remediating high impact vulnerabilities. The goal of remediation is to minimize the risk associated with a security loophole or software bug. Patching is the most common form of remediation. Patches are especially effective because they're tailored to specific vulnerabilities. Rather than spend a lot of time patching vulnerabilities, IT professionals should opt for automatic vulnerability remediation. Automation makes it easier to deal with the increasing complexity of vulnerability management due to the exponential growth of technology and helps reduce the number of personnel needed to accomplish vulnerability management tasks.

IV. DISCUSSION AND ANALYSIS

As mentioned in the methodology section of this thesis, the main purpose of this research was to examine the significance of effective patch management in cyber security of government information systems, specifically, the Department of the Navy. A secondary objective was to investigate whether the patch management process for government information systems could be enhanced by adapting private industry standards.

Many government information systems have outdated operating systems and hardware components that are susceptible to cyber-attacks. Joyce and Thompson cite that the Argonne National Library has conducted studies showing "that a large portion of cybercrime could be prevented by more proactive patch management" (2015, para 1). A vast majority of companies could have prevented data breaches or failed audits if they had implemented more rigorous and efficient patch management systems. The time in which vulnerabilities are identified and remediated is imperative to securing systems and preventing cyber-attacks. The potential exploitation of known vulnerabilities is widespread due to the lack of continuous upgrades and use of obsolete software and hardware. According to the 2003 GAO report, Dacey suggests that with the advancement of automation, hacking tools are becoming more sophisticated, more readily available, and easier to use as well (2003). Joyce and Thompson propose that cybercrime peaks during the time that a vulnerability is discovered, and the patch mitigation is released (2015).

Situational awareness and proactive measures aide in the reduction of at-risk information systems. The core of network security is proper awareness of the threat of commonly found vulnerabilities and available patches to remediate those risks. However, managing large amounts of software suites can be overwhelming, leaving a great margin of error. Security patches can help stop malware infections, simple human mistakes, and network compromises. Patch management includes fixing known vulnerabilities in operating systems, applications, the BIOS, third-party software, and device drivers. Figure 1 shows vulnerabilities in information systems by class. As previously stated, patch management accounts for nearly two-thirds of all cybercrimes. According to Dacey's 2003

GAO report, the CERT/CC claims that 95 percent of all network intrusions could be avoided with efficient patching (2003).

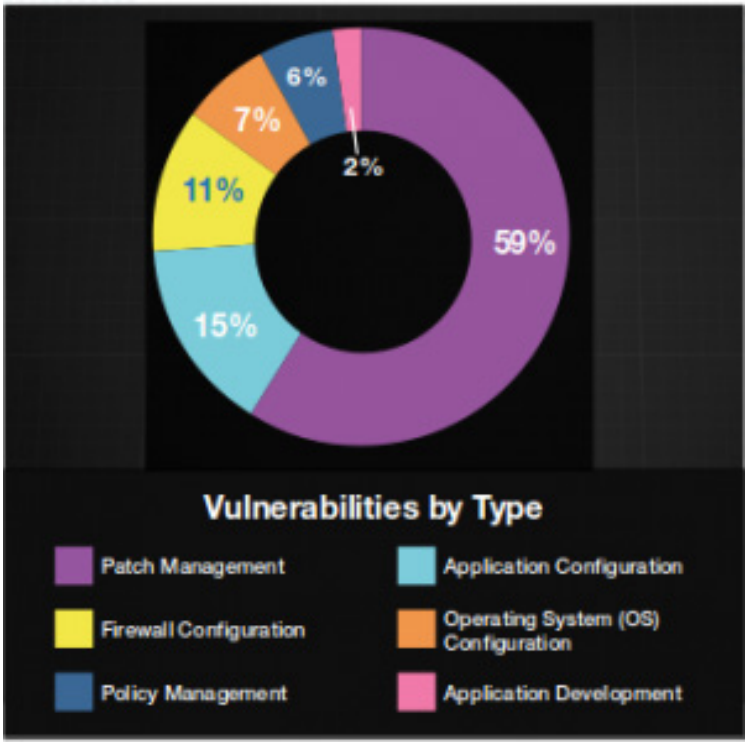

Figure 1. Vulnerabilities by Type. Source: Argonne National Laboratory (2015)

Governments do not consider themselves prime targets for cyber-attacks. In his article, Raths quotes Maria Thompson, chief risk officer at the North Carolina Department of IT as she states, "There are always gaps in your environment you can't see…and you can't protect what you can't see." (2019, para 26). Government information systems are particularly vulnerable to cyberattacks and other online security issues due to the connected nature of various government agencies and departments. One notable difference about the DON, as Goure references a recent Cybersecurity Readiness Review, and states that "the Navy is willing to take an unflinching view of its vulnerabilities, poor practices and technological inadequacies" (2019, para 10). The interconnected nature of government information systems means that hackers have an easier time escalating privileges from various points of the government information system.

Patch management is a critical aspect of maintaining the security of information systems. It involves regularly updating software and hardware to fix vulnerabilities and prevent attackers from exploiting them. The purpose of researching the significance of patch management on information systems is to understand the importance of staying up to date with security patches and to identify potential challenges in implementing effective patch management practices. This research can help organizations, particularly those in the government sector, to better understand the risks associated with unpatched systems and how to mitigate them.

Effective patch management can reduce the risk of compromises to government information systems. Cybersecurity threats to government systems are an ongoing concern, with attackers constantly searching for vulnerabilities to exploit. Unpatched systems are often the target of these attacks, and the consequences of a successful attack can be severe. These can include data theft, disruption of services, and loss of public trust. By implementing effective patch management practices, governments can reduce the likelihood of successful attacks and minimize the damage caused by any that do occur.

The significance of patch management on information systems is crucial for organizations, particularly those in the government, to understand the importance of maintaining the security of their systems. Effective implementation of patch management practices can reduce the risk of successful attacks and mitigate the damage caused by any that do occur. Governments should prioritize implementing effective patch management practices as part of their overall cybersecurity strategy to ensure the safety and security of their sensitive information.

While patch management is a critical component of risk management for organizations, there are several challenges that organizations encounter when implementing a patch management process. “Unpatched software vulnerabilities – one of the most common attack vectors for cybercriminals – remains a huge problem for organizations everywhere” (Truta, 2019). Both government and private industries face similar restraints when implementing patch management. Problems faced by organizations when implementing patch management include lack of experienced personnel to carry out the patch, uncertainty about the potential impact of the patch on information systems

integrity and functionality, inability to manage complex IT systems, issues with scalability, and network bandwidth limitations (IBM, 2014). Fillip Truta also emphasizes the importance of automation in patch management (2019). Automation is considered one of patching's best practices, as it will ensure that systems are kept up to date while minimizing the labor time it takes to patch systems (rapid7.com). According to the NIST Guide to Enterprise Patch Management Technologies, "patches are usually the most effective way to mitigate software flaw vulnerabilities and are often the only fully effective solution" (2013). Automation also helps to reduce the risk of human error, as manual patching processes can be prone to mistakes. Additionally, automation can save a significant amount of time and resources, allowing IS teams to focus on more strategic tasks. Overall, automation in patch management is essential for maintaining the security and stability of any organization's IS infrastructure.

Souppava states in the NIST *Guide to Enterprise Management Technologies* also recommends eliminating multiple ways of applying patches as a best practice. Having multiple ways of applying patches can cause conflicts. Multiple methods might each try to patch the same software, which is particularly problematic when the organization doesn't want certain patches applied because of issues with those patches, testing delays, etc. Multiple methods can also cause patches to be delayed or missed because each tool or administrator may assume another one is already taking care of a particular patch. "Organizations should identify all the ways in which patches could be applied and act to resolve any conflicts among patch application methods" (Souppaya, 2013, p. 4).

This report continues to discuss the problems associated with users being allowed to override the patch management processes. Best practices should include limited user access and continuous monitoring. Continuous monitoring is critical to maintaining the integrity and security of these systems, protecting sensitive data, and complying with industry standards.

To reiterate Dacey's recommendation in the GAO Report of 2003, the best practices for patch management include an emphasis for Senior Executive support; standard patch management policies, procedures, and automated tools; dedicated resources with clearly defined roles and responsibilities; updated asset and technology inventory; the ability to

identify the system's relevant vulnerabilities and patches; risk assessment and mitigation; and ultimately, testing; the distribution of patches; and finally monitoring through network and host vulnerability scanning (2003, pp. 11–13). These best practices, if implemented, provide the best framework for patch management.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This thesis explored the significance of effective patch management processes in preventing potential compromises to government information systems. Towards this objective, the research compared industry standards for information systems security to those adopted by the department of the Navy in accordance with its Risk Management Framework. The method of data collection involved a comparative analysis of the literature on vulnerabilities, private industry/government best practice and patch management. The research sought to determine if the lack of initial and continuous patch management has a direct connection to the vulnerability of government information systems.

Based on the analysis conveyed, it can be concluded effective patch management significantly reduces and mitigates risk associated with vulnerabilities within various software applications. The number of known exploits within information systems.

The research addressed the question of whether government information systems are vulnerable to cyberattacks. Available information clearly shows that government agencies are particularly vulnerable to cyberattacks due to several factors. First, it was established that government agencies commonly use outdated operating systems and hardware. For example, many government agencies still run unsupported Windows operating system versions such as Windows XP, Vista, and Windows 7. Microsoft no longer provides periodic security patches for these legacy operating systems, and any organization still running them is at an elevated risk of experiencing online attacks from malicious actors. It was also found that most IT executives have a hard time keeping track of the thousands of individual nodes on an organization's network environment. This means that some Vulnerable IP addresses and devices are left unlatched, acting as important gateway devices for hackers to launch devastating cyber-attacks on the whole information system environment. Another factor that makes government information systems to be especially vulnerable to security breaches is the misguided belief that government information systems are not the prime targets for cybercrimes. As attacks on the Human Health Department and Maryland's DoIT demonstrate, government information systems are increasingly being targeted by hackers and ransomware. The most

effective way to safeguard government information systems is through proactive and timely patching of known vulnerabilities.

This thesis also explored the best practices of patch management on reducing potential security compromises to government information systems. In addition to being a risk management exercise, patch management helps protect critical digital assets from total collapse or being ransomed by online attackers. Patch management is especially important because most cyberattacks happen between the time when a vulnerability is discovered and when a patch is made widely available. By implementing a proactive patch management process, organizations can limit or eliminate data breaches.

In summary, risk to both federal and private sector information systems continue to increase at an alarming rate. Research shows that government IS continues to be a target for hackers and cyber-enemies. The theme that remains throughout the IS/IT community is that patch management is the most effective way to mitigate those software vulnerabilities. Government organizations should invest in the appropriate automation tools and resources to complete this way of risk mitigation. By adopting effective patch management best practices discussed by various authors, including Dacey, patch management has several benefits, which include a reduction in the exploitation of vulnerabilities, patch management will maintain the security posture of assets and information systems, and will ultimately reduce the overall cost of reactive cybersecurity (2003).

VI. RECOMMENDATIONS

The literature available on the security risks facing both private and government information systems shows that the risk of compromise is growing. The first line of defense for the department of the Navy should be to implement a proactive patch management process to minimize cyber-attacks following the discovery of vulnerabilities in information systems. Because it is not possible to address all software bugs and security loopholes identified in an information system, IT professionals need to look for an effective way to prioritize Vulnerabilities according to their potential to cause serious harm or compromise vital information resources within an organization's IS. A proactive patch management process is the first line of defense against cyberattacks because research shows that attackers exploit known vulnerabilities that have been left unpatched for a long time.

First, government agencies need to scale up their cyber vigilance. All that a hacker needs to compromise an entire information system is poorly developed or configured software or a weak network security protocol. That is why government agencies consider Patch Management a critical component of their overall network security program to stop nefarious actors who want to hijack critical systems, take them down, breach data, or spread malicious falsehoods. Government agencies often must protect their online resources using limited resources, which is why it is imperative that they emphasize the areas that will significantly improve their overall security posture. Here, we recommend three things that government information systems must do to bring the greatest impact on their network environment:

Design a comprehensive security ratings software that evaluates the agency's aggregate security poise and assists teams in prioritizing and targeting vulnerabilities. A properly developed security performance management program can assist security teams to stay one step ahead of cyber criminals.

Take stock of essential digital assets, regardless of their location. Insights should be obtained concerning the data centers across geographic locations and cloud-based assets. Gaining a better understanding of critical digital assets can help security teams to

identify vulnerable assets that are more likely to be compromised, creating a launch pad for threat actors to take control of critical network resources. The patch management process should be conducted on all digital assets since patching a few of these assets leaves room for hackers to carry out their evil schemes.

Government information systems should also assess and monitor third-party applications and programs that can access critical digital assets. Any patch management process should also factor in third, fourth, and zenith party software and hardware to ensure they are not contributing to security risks associated with government information systems. Attackers commonly enter, breach, or disable a network or website by first comprising third party applications before giving themselves escalated privileges within the larger organizational IT infrastructure.

VII. FUTURE RESEARCH RECOMMENDATIONS

The current study has clearly demonstrated how government information systems are increasingly becoming victims of devastating online attacks. Hackers have realized the weaknesses and the hefty payouts that are associated with holding critical government information systems hostage and are continuously improving their game to take advantage of these opportunities.

Future research on this topic could examine whether the government's willingness to pay hefty sums of money demanded by hackers before they can release vital information resources, they have held hostage is contributing to the recent spike in cyberattacks directed.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Araujo, F., Hamlin, K., Biederman, S., Katzenbiesser, S. *From Patches to Honey-Patches: Lightweight Attacker Misdirection, Deception, and Disinformation*. The University of Texas at Dallas. https://personal.utdallas.edu/~hamlen/araujo14ccs.pdf

Carlson, B. (2021, October 7). *Top cybersecurity statistics, trends, and facts.* CSO United States. https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html

CHIPS. Secretary of the Navy releases cybersecurity readiness review. (2019, March). https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=12268

Dacey, R. F. (2013). *Information security effective patch management is critical to mitigating software vulnerabilities.* (GAO-03-1138). Government Accountability Office.

Department of Navy Information Technology Magazine. Information assurance vulnerability compliance tracking and reporting for U.S. Navy ships. (2009, June). https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=2683

Indiana University. (2018, January 18). *Knowledge Base: What are patches, hotfixes, and service packs?* https://kb.iu.edu/d/algb#:~:text=Software%20companies%20issue%20patches%20to,service%20packs%20for%20easier%20installation.&text=Sometimes%2C%20a%20hotfix%20refers%20to,applied%20without%20restarting%20the%20system

Joyce, A, & Thompson, M. (2015, November 23). *Lack of patch management leads to increase in cybercrime*. The Cyber Team: Cyber Research at Argonne National Library. https://coar.risc.anl.gov/lack-of-patch-management-leads-to-increase-in-cybercrime/

National Interest. *The Navy's networks are vulnerable to cyber attacks—it's time for action.* (2019, November 18). https://nationalinterest.org/blog/buzz/navys-networks-are-vulnerable-cyber-attacks%E2%80%94its-time-action-97091#:~:text=The%20Navy's%20Networks%20Are%20Vulnerable%20To%20Cyber%20Attacks%E2%80%94It's%20Time%20For%20Action,-Hackers%2C%20particularly%20thos

Perlroth, D. E. (2021, January 5). More hacking attacks found as officials warn of 'grave risk' to U.S. Government. *New York Times.* https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html

Rapid7. (2021, April 01). *Patch management: benefits and best practices.* https://www.rapid7.com/fundamentals/patch-management/

Raths, D. (2019, November). *Managing software updates still a government stumbling block.* Government Technology. https://www.govtech.com/security/Managing-Software-Updates-Still-a-Government-Stumbling-Block.html

Ridzyowski, T. (2020, January 21). *The importance of software updates and patches.* Turn-Key Technologies. https://www.turn-keytechnologies.com/blog/article/the-importance-of-software-updates-and-patches/

Security Scorecard. (2018). 2018 *Government cybersecurity report.* https://resources.securityscorecard.com/all/2018-government-cybe?xs=226461#page=1

Souppaya, M. (2013) *Guide to enterprise patch management technologies* (NIST Special Publication 800 40 Rev 3). National Institute of Standards and Technology (NIST). https://www.govinfo.gov/app/details/GOVPUB-C13-8b30a10a9d9de2366cd26e96d540b5ea

Symanovich, S. (2021, January 23). *How to: 5 reasons why general software updates and patches are important*. Norton How To. https://us.norton.com/blog/how-to/the-importance-of-general-software-updates-and-patches#

Temin, T. (2020, July 16). *Stepping up cyber protections for networks on Navy ships.* Federal News Network. https://federalnewsnetwork.com/navy/2020/07/stepping-up-cyber -protections-for-networks-on-navy-ships/

Thomas, B. (2020, March 27). *Coronavirus pandemic highlights government cyber vulnerabilities*. BITSIGHT. https://www.bitsight.com/blog/coronavirus-pandemic-highlights-government-cyber-vulnerabilities

Truta, F. (2019, October 31). *60% of breaches in 2019 involved unpatched vulnerabilities.* Security Boulevard. https://securityboulevard.com/2019/10/60-of-breaches-in-2019-involved-unpatched-vulnerabilities/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California