Configuration Management: a Critical Component to Vulnerability Management

Christopher Furton

Syracuse University

Abstract

Managing software vulnerabilities is increasingly important for operating an information technology environment with an acceptable level of security. Configuration Management, an often overlooked Information Technology process, directly impacts an organization's ability to manage vulnerabilities. This paper explores a Department of Defense organization that currently struggles with vulnerability management. An analysis of current vulnerability and configuration management programs reveals a gap between two. Further examination of the assets, vulnerabilities, and threats as well as a risk assessment results in recommendation of a new configuration management program. This new program leverages configuration management databases to track the assets of the organization ultimately increasing the effectiveness of the vulnerability management program.

Configuration Management: a Critical Component to Vulnerability Management

Vulnerability Management (VM) is essential to minimize risk and provide an available information resource to an organization. A critical part of managing vulnerabilities lies within the Information Technology department's ability to manage configurations throughout the environment. Configuration Management (CM) is considered a best practice for management of information systems. This paper will explore the relationships between VM and CM, analyze a Department of Defense organization's processes relating to VM and CM, and develop recommendations to effectively implement a CM program.

Business Process Overview

The Department of Defense organization being assessed, referred to throughout this paper as the *Organization*, is involved in Research and Development (R&D) and system acquisition of war-fighting equipment in support of the United States Marine Corps. The Organization operates a business information technology (IT) system to support the development of war fighting equipment throughout the acquisition system lifecycle. Within the Information Technology department, the staff performs functions related to managing an IT infrastructure, securing the infrastructure, and facilitating information management functions. Within the scope of the IT Department, a comprehensive vulnerability management program is already in place and a configuration management program is being developed.

Current Vulnerability Management Program

In accordance with Department of Defense directives, the Organization is required to "achieve information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare" (Department of Defense, 2007). Part of that defense-in-depth approach includes establishing a vulnerability management program that consists of monitoring systems, evaluating DoD impact, and tracking the mitigation of those vulnerabilities using DoD-directed Information Assurance Vulnerability Alerts (IAVAs).

The current vulnerability management program meets the requirements identified in the DoD Directive on Information Assurance. The Organization's VM program consists of mechanisms to discover vulnerabilities currently on the network, patch those vulnerabilities, and report to higher level organizations on compliance to the IAVA. This process is repeated for every IAVA announcement.

Detection of existing vulnerabilities is performed utilizing real-time scanning software which, through the use of signature files, evaluates a networked asset and creates a report of those assets that are not compliant. The scanning software is manually run by the Vulnerability Management Team (VMT) personnel upon receipt of an IAVA and again once remediation is finished. The intent is to create a check and balance with a 'before patching' and an 'after patching' scan. Although this method is successful, two major problems are encountered with the real-time scanning process:

1. Real-time scanning only identifies vulnerabilities on assets that are currently connected to the network infrastructure and powered on

2. Real-time scanning needs to be conducted during normal business hours to maximize the number of assets on the network. This has significant impact to network optimization and causes congestion.

Because real-time scanning can only identify vulnerabilities for systems actively connected, the possibility of missing vulnerabilities is high. With today's mobile computing environment, the Organization often has 20% of the assets, specifically laptops, off the network on travel or working from off-site locations. This introduces significant error when identifying how many assets are vulnerable and creates a challenge for patching systems.

Besides the challenge of accurately identifying vulnerable systems, using real-time scanning software creates spikes in network utilization. Because real-time scanning involves remotely checking computers based on signatures, the scanning produces significant traffic. Because the Organization utilizes a scanning server located on one side of the country and scans assets located at sites throughout the US, significant bandwidth is used scanning across channels with limited-bandwidth availability. The impact to business process is noticeable during peak hours if scanning takes place.

Once the real-time scanning identifies vulnerable assets, the mitigation procedures apply needed patches. At the Organization, patching of systems is performed using several commercial applications. With the exception of Microsoft patches, system administrators are required to manually create patching batch jobs within a software patching application for every instance of the vulnerability. For example, if an Adobe Reader version is released, a technician must create a software deployment package and initiate the push to each computer that is affected by the vulnerability. For Microsoft patches, the technician must approve a patch only once and the patch is automatically loaded to all affected Microsoft assets. This method of patching assets is very time consuming for administrators but affective.

Current Configuration Management Program

The configuration management program at the Organization consists of a request processing system to track and approve changes to the infrastructure. The system is designed to track historical change requests and approvals with limited search functionality for historical records. The workflow for change approvals initiates with the technician whom is requesting the change and is routed to the IT supervisor for final approval. Once approved, the system automatically generates a help desk ticket for the task and the technician is authorized to perform the work. Upon completion, the technician closes the help desk ticket. This configuration management system – which would more accurately be named a change management system – introduces several problems.

The first significant problem identified with the current configuration management system involves the workflow needed to approve changes. By allowing technicians to submit change requests directly to the IT supervisor, the Information Security (InfoSec) personnel are left out of the decision making process. If changes will affect Certification and Accreditation (C&A), the InfoSec personnel will need to make modifications to accreditation packages. By not involving them in the approval process, the accreditation package is not current and possible risks are introduced to the environment.

Another problem is that the current system is not comprehensive enough. Since the system only manages change requests and approvals with limited search functionality, using this system provides little value to the IT staff. A more robust system would increase the value and will be discussed later in this paper. The current system is not effective.

Existing disconnect between VM and CM

As discussed in the previous two sections, the Organization has a vulnerability management program and a configuration management program in place. Each program has its good and bad aspects; however, the two do not adequately work together. In order to form a global end-to-end security paradigm, the locally configured policies of all assets need to work in tandem. “Although a significant effort has been made…to develop defense techniques against security attacks, efficient management of security configuration has been overlooked” (Al-Shaer, Kalmanek, & Wu, 2008). The VM and CM programs and the systems at the Organization are networked systems that currently operate independently from each other.

For example, a technician who requests to install a software application gets approval in the configuration management system. That new software application gets installed in a production environment but the vulnerability management system is not aware of a new application that needs to be patched. The inverse is also problematic. If the vulnerability management program identifies an unpatched application installed on an asset, the VM system does not allow the VMT to identify other assets with the same application throughout the enclave. The VMT is only able to identify other affected assets by performing a real-time scan which does not identify assets that are turned off or disconnected. This makes it almost impossible for the VMT to properly mitigate 100% of the vulnerabilities.

Assets, Vulnerabilities, and Threats

The Organization has hundreds if not thousands of assets that need to be protected from many different forms of threat agents.   In order to transition the current processes mentioned in Part I of this paper to a more ideal solution, identifying the Organization’s assets is essential. Knowing which assets are important is key to successful implementation of a Configuration Management Database (CMDB). In order to accomplish this, the Organization must first identify Configuration Items (CI). A CI, according to the Information Technology Infrastructure Library (ITIL), is all hardware and software assets as well as documentation, processes, and people that compose, support, and consume IT services (Marquis, ITIL and the Evolving CMDB, 2007). Understanding the assets – or CIs – in use throughout the Organization, and assembling a CMDB, will allow security personnel to better assess the vulnerabilities. Understanding the vulnerabilities can help predict possible threats.

Configuration Items and the Configuration Management Database

Before getting a handle on Vulnerability Management, an “organization should first establish an in-depth study of the inventory of every computer system within the network” (Andrew, 2006). The Configuration Management Database (CMDB) for the Organization will be the repository for the outcome of that study. It is a complex data structure or set of data structures. The Organization needs a “database of databases” or an “n-dimensional “cube” of current and historical relationships between CIs” (Marquis, ITIL and the Evolving CMDB, 2007). Commercial off the shelf products are available to provide ITIL CMDB data structures without the need to internally develop the complex data structures. Utilizing manual methods to populate these data structures is futile. Automated methods discovering the current configuration is essential (Hurst, 2008).

Instead of focusing on the CMDB, the focus instead should be on identifying the configuration items. The Organization's configuration items need to be broken into several categories which may grow as the Organization adapts the ITIL CMDB framework. However, the following categories will provide a significant starting point: hardware, software, licenses & policies, knowledge base articles, users, and locations.

The hardware category of CIs consists of all equipment that is utilized throughout the Organization's information infrastructure. Each instance of a Desktop, laptop, server, router, switch, and monitor will all be a CI. Additionally, hardware that is not often considered directly related to the information infrastructure can also be included such as access control system components, teleconference equipment, and redundant/backup power systems. Hardware CIs for the organization will total approximately 3000 items.

The software category of CIs consists of all software utilized throughout the Organization. Commercial products, government off-the-shelf products, firmware products, and internally developed applications will be part of the software CI database. The digital media itself will be included in the CMDB which becomes the Organization's software portfolio. Software CIs for the Organization will total approximately 500 items.

Similar to the software CI category, a separate category for licensing and policy (L&P) will be needed. This category references the software items but includes additional information including product keys, expiration dates, service contracts, maintenance agreements, service level agreements, and policy documents. L&P CIs for the Organization will total approximately 1000 items.

The next CI category is for Knowledge Base (KB) articles. Using the CMDB to track KB articles as CIs allows the Organization to ensure that a system is in place to handle Knowledge Management. These CIs are assets to the Organization since knowledge and wisdom take time and experience to develop. Capturing this wisdom as a CI can help any help desk technician, regardless of experience, handle complex recurring problems and ensures solutions are secure and implemented properly. Currently, the Organization does not actively create KBs for known problems but the number of CIs can be substantial over time.

Another CI category that is important for the CMDB is the users. Utilizing current directory services, the users should be tracked as configuration items as they often have linkages to other CIs. For example, a user can be assigned hardware and be granted software licenses for use on hardware. Having the user be a CI can help with tracking equipment and ensuring adequate licensing. The average number of user CIs for the Organization is 800.

The final CI category is physical location. This category, similar to the User category, is essential to track cross-category relationships. CIs from other categories will have linkages to the Location category to include physical location of hardware and users. Understanding physical locations can assist with accountability as well as business continuity in the event of disaster. Following the Organization's current location tracking, the Location category will utilize building and room number totaling approximately 1000 different physical locations.

Software Category Vulnerabilities

The configuration items listed identify a partial set of the Organization's assets that need to be protected. Each category above can have controls put into place to help protect that asset. For example, Knowledge Base assets can be protected by utilizing backup systems for restoration in case of natural disaster or hardware failure. Additionally, the User assets can be protected by instituting annual information security training. However, this paper will focus primarily on managing the vulnerabilities of the software configuration items leveraging the Configuration Management System.

Current software applications often have significant vulnerabilities that are patched by the software developer. Because the Organization is part of the Department of Defense, the Organization will be notified of actions required by the Defense Information Systems Agency (DISA) in the form of a vulnerability notice. The notice will have severity categories assigned and the Organization will need to abide by these. According to DISA, the CAT I severity code requires *immediate* compliance within 25 days. CAT II, CAT III, and CAT IV have longer deadlines for mitigation of 60, 180, and 1000 days respectively (Defense Information Systems Agency, 2007).

The Organization has identified three software developers that are considered high risk and that require special attention from the Vulnerability Management Team. These companies are Microsoft, Adobe, and Oracle. Additional focus will be given to the products produced by these companies to ensure that the vulnerabilities are handled quickly. Because of this, the Organization has decided to assign CAT I priority to all vulnerabilities from these three companies.

The configuration items in the software category have potential to be exploited by many different attack vectors. Protecting from these attack vectors is a challenge and requires quick turn-around time for patch management. Some attack vectors, such as zero-day vulnerability exploits, are not prevented by patch management and require other defense mechanisms outside the scope of this paper. The critical tool for the VMT to use is the Configuration Management Database. Using the CMDB to identify which hardware CIs have a vulnerable software CI can expedite locating software vulnerabilities as opposed to just performing real-time scanning. Furthermore, utilizing the Location CI to determine the physical location of the hardware CI can allow the technician to quickly remove the asset from the network if needed.

Potential Threat Agents

The Organization, due to its role in developing weapon systems, has a high potential for targeting by threat agents. The possible threat agents range from fully funded nation states to unorganized scripted attacks by novice hackers. The man-made threats are of biggest concern as the Organization’s electronic information could benefit other countries. Natural threats, although significant, do not have the ability to compromise software vulnerabilities and will not be discussed.

Regardless of the origin of the threat agent (nation state vs. script kiddy), many of the software vulnerabilities require user interaction to execute the attack. This interaction may be in the form of opening a malicious email with embedded scripting, clicking on a malicious link in an email or on a webpage, or opening an attachment that allows execution of malicious code. Because the threat agent utilizes a CI (The User) that is difficult for the information security personnel to control, the Organization believes significant effort must be placed on education. A comprehensive user awareness training policy (part of the L&P CI category) needs to be developed to educate the users on how to identify potential threat actor exploit attempts and avoid becoming a victim. In this case, the user is unintentionally allowing an outside threat actor to execute an attack on the organization.

Another threat actor that is of concern for the Organization is the insider threat. Because users require access to information to perform job duties to support the mission, there is potential for intentional insider abuse. Users who have authorized access have the potential to leverage software vulnerabilities to increase their current level of access. “Privilege Escalation attacks try to give ordinary users root or administrator privileges” (Sequeira, 2003). Despite the Organization’s implementation of least privilege for access to information, proper protections need to be in place to minimize the risk of internal exploitation of software vulnerabilities. Keeping software up to date – leveraging the CMDB – can greatly reduce the likelihood of an insider exploiting software vulnerabilities.

Risks and Organizational Impact

Risk management, as defined by Kovachich (2003), is “the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources.” The Organization heavily relies on the IT business system to accomplish its mission. The system also contains historical information dating back to 1943. Because of this, managing the risk associated with the network system and ensuring the confidentiality, integrity, and availability is essential.

Without a confidential system, the Organization would not be able to control access to information that is often restricted and not publically available. The current infrastructure operates off access controls which only grant users specific access depending on the job that they perform. This confidentiality ensures that the Organization's products and information is controlled and reduces the chance of insiders stealing information. These confidentiality controls also reduces the risk of an outside intruder gaining full access to all the Organizations information. Without these risk mitigation controls, the Organization could not control who access which information.

In addition to confidentiality, integrity is important to the Organization's risk management goals. Because the organization often tests weapon systems to ensure compliance with system specifications, the integrity of information is important. For example, a weapon system is supposed to be capable of firing 100 rounds consecutively without overheating of the gun system. A breach in integrity which introduced misinformation changing the number 100 to the number 200 could have deadly repercussions. During the next test iteration, the test executer may fire the weapon more than it is intended (100 rounds) and cause overheating and the possibility of serious injury or death. Managing the risks associated with ensure integrity of information is also important and failure to do so could cause the Organization to be shutdown.

Finally, system availability is critical. Since the business system is the heart of all day to day activities, having the system unavailable can impact cost, schedule, and performance of other acquisition projects. Risks associated with loss of system availability must be mitigated properly as small system outages during daily operations not only become annoying to users but also has the ability to cause acquisition programs to fall behind very tight development timelines.

Risks Evaluation and Mitigation

In order to better understand the risks to the system's confidentiality, integrity, and availability as it relates to software vulnerabilities and configuration management, a qualitative analysis needs to be performed periodically. An initial analysis has been performed analyzing the following risks:

- Data theft by external threat agent due to outdated or unpatched software configuration item
- System denial of service by external threat agent due to outdated or unpatched software configuration item
- Misinformation introduced by internal threat agent by privilege escalation utilizing software vulnerabilities
- Inconsistent baselines due to employee shortcuts
- Inaccurate data in the CMDB caused my employee error

The risk assessment was conducted utilizing the Marine Corps Institute's process for Operational Risk Management. Within this process, the risk is assigned a probability of occurring code from A to D with A being the most likely to occur. A severity code is also assigned from I to IV with I being the most severe results. Depending on the severity and probability, and overall Risk Assessment Code (RAC) is assigned. The RAC with number 1 is critical, number 2 is serious, number 3 is moderate, number 4 is minor, and number 5 is negligible (Marine Corps Institute, 2002).

The first risk assessed was the theft of data by an external threat agent. From a configuration management view, the theft of the data was the result of unpatched software configuration items. The risk was determined as having a probability of *Probable (B)* and an impact of *minor*. Because of these, the risk assessment matrix in *table 1* shows the final risk assessment at *Moderate*.

To mitigate this risk, the Organization needs to reduce the amount of unpatched or outdated software. Doing so can potentially eliminate this risk. Data theft will still be a concern as other methods can be used to steal data, but this particular risk can be avoided through proper configuration management.

The second risk assessed was denial of system availability caused by outdated or unpatched software configuration items. From a configuration management view, the denial of service would have to be caused by unpatched software configuration items. The risk was determined as having a probability of *Unlikely (A)* and an impact of *detrimental*. Because of these, the risk assessment matrix in *table 2* shows the final risk assessment at *Moderate*.

Mitigation of this risk is challenging as the Moderate final assessment is solely based on the impact of a denial of service attack to the business processes. Since denials of service attacks rarely use unpatched software, mitigating this risk is unnecessary and the Organization can assume it.

The third risk assessed was introduction of misinformation by an internal threat agent. From a configuration management view, the failure in integrity would have to be caused by unpatched software configuration items. The risk was determined as having a probability of *May (C)* and an impact of *detrimental*. Because of these, the risk assessment matrix in *table 3* shows the final risk assessment at *Serious*.

To mitigate this risk, the Organization needs to reduce the amount of unpatched or outdated software. Doing so can potentially eliminate this risk. Although the insider threat is substantial, utilizing strict configuration management along with other least privilege access controls can reduce the likelihood. Due to the impact caused by misinformation, this risk had a final overall rating of *Serious*.

The fourth risk assessed was inconsistent baselines caused by employee shortcuts. This risk is directly related to the internal processes involved with keeping the CMDB up to accurate. The risk was determined as having a probability of Likely *(A)* and an impact of *severe*. The impact is significantly high because the repercussions caused by occurrence of this risk can increase the likelihood of other risks coming true. The risk assessment matrix in *table 4* shows the final risk assessment at *Critical*.

To mitigate this risk, the Organization needs to ensure Information Technology employees are properly trained. Policy and detailed procedures need to be available to those involved in system administration to ensure that configuration items are kept accurate.

Additionally, quality assurance checks conducted by supervisory personnel can help identify problematic CMDB entries.

The fifth risk assessed was inaccurate data in the CMDB caused by employee error. This risk is directly related to the internal processes involved with keeping the CMDB up to accurate. The invalid data in CMDB for this risk was not created intentionally. The risk was determined as having a probability of *Probable (B)* and an impact of *severe.* The impact is significantly high because the repercussions caused by occurrence of this risk can increase the likelihood of other risks coming true. The risk assessment matrix in *table 5* shows the final risk assessment at *Serious.*

To mitigate this risk, the Organization needs to ensure Information Technology employees are properly trained. Policy and detailed procedures need to be available to those involved in system administration to ensure that configuration items are kept accurate. Additionally, quality assurance checks conducted by supervisory personnel can help identify problematic CMDB entries.

Recommendations

In order to bridge the gap that currently exists between the configuration management system and the vulnerability management system, a quasi-ITIL solution of configuration management databases needs to be implemented. Because of the in-depth changes that would need to occur to the Organization’s processes, a full ITIL implementation is NOT suggested (Marquis, ITIL: What It Is And What It Isn't, 2006). With the creation of the CMDBs, the organization also needs to address policy shortfalls, hiring guidelines, and training. Lastly, the

Organization IT department and information security personnel need to develop a quality assurance and control program.

Configuration Management Database

In order to properly maintain configuration control, it is recommended that the Organization’s Information Technology department revamp the current configuration management program. Specifically, creation of a series of relational databases for the following software categories: hardware, software, licenses & policies, knowledge base articles, users, and locations. Each relational database needs a many-to-many relationship with each other so that configuration items within each database can have interactions between them (see figure 1).

One major concern for the CMDB is that it must be the authoritative source for all the data contained within it. For example, the current systems used for inventory and assignment of equipment to users should be replaced by the CMDB. Additionally, the software portfolio spreadsheet in use should be replaced by the software category in the CMDB. This allows for a single source for information. This will consequently provide the vulnerability management team a single place to look to find which assets (hardware CIs) have vulnerabilities (software CIs) and where the asset is located (location CIs). It is recommended that the Organization keep the current Configuration Management System but rename it to be the Change Management System.

Training

Because of the risk assessment, a requirement for increased training is recommended. Specifically, the Information Technology department will need to understand the new CMDB and will need training on how to perform operations on the databases. Since the likelihood of accidental or potential for intentional input of errors into the configuration management system, a semi-annual, hands-on training requirement is recommended. This training should include instructor led scenarios ofr training employees how to handle specific configuration changes.

Additional training is recommended for the Vulnerability Management Team as usage of the proposed CMDB is significantly different from their current real-time scanning methodology. The VMT will need to start at the bottom of the learning curve and modify many of the procedures for identifying vulnerabilities. This training is recommended as a one-time course with refresher training as needed.

Hiring Guidelines

Currently, the Information Technology department consists of a mix of government civilian and contracted personnel. Because of current human resource policies within the Department of Defense, the discipline and lawful termination of government civilian employees is difficult. It is recommended that the Organization increase the number of contracted personnel as those individuals often have more incentive to exercise attention to detail. Detailed Performance Work Statements (PWS) is recommended to ensure contractor performance is measured against the expected performance levels. Utilizing incentives for exceeding performance levels is also recommended (Executive Office of the President, 2003) .

Quality Assurance and Control

As identified in the Risk Assessment section of this paper, implementing a quality assurance program is needed to minimize risk associated with errors in the CMDB. Having a

Quality Assurance (QA) program and a Quality Control (QC) program is recommended to ensure accuracy of configuration items in the databases. QA program activities are planned checks by third parties not directly involved in the process while the QC program activities implement quality into the day to day processes (Intergovernmental Panel on Climate Change, p. 8.4).

The QC program will contain the planned quality measures built into the processes used by the IT technicians. It is recommended that all procedures used by the technicians that are related to the contents of the CMDB be reviewed and QC measures implemented. For example, the process of deploying software to a laptop should include a QC check for updating the hardware CI's relationship to the new software CI being deployed. Additionally, all processes should include a QC check to verify that the User CI and the Location CI are accurate.

In conjunction with the QC program, a QA program will contain measures to verify quality. The QA program should be conducted by the supervisory personnel in the IT department and personnel from other departments that rely on the CMDB. This QA checks consist of utilizing software tools to verify software CI are accurately assigned to hardware CIs. Additionally, the Location CI and User CI can be verified during routing equipment inventories as QA checks.

Policy

In order to make the recommended changes, some policies will need to be modified and some created. The current policies that need to be modified are the configuration management policy and the vulnerability management policy. The policy that will need to be created is the quality assurance and control policy. Additionally, procedures will need to be reviewed at the department levels to ensure compliance with the new policy.

The configuration management policy should contain two main sections: change control and configuration control. The change control section needs little modification as it is currently effective at providing a means to request and get approvals. An addition to the work flow to include the configuration manager on all changes upon completion of the technician work should be added. This will allow the configuration manager, who is the IT supervisor, the ability to perform a quality assurance check. The configuration control section of the policy will need to be written to include the CMDB with discussion of what constitutes a CI.

The vulnerability management policy should also be revised. The high level view for mitigating vulnerabilities should be included. For example, the current policy discusses using the real-time scanner to identify vulnerabilities, patching the software, and then using the real-time scanner to verify remediation. This should be reworded to discuss using the CMDB to locate software CIs that are vulnerable, patching the software, and then use the real-time scanner to verify remediation. A feedback loop between the VMT and the IT department should also be included in instances where errors are located in the CMDB.

The last policy that will need to be created is the quality assurance and control policy. This policy will provide explanation of the role of quality assurance and quality control and assign responsibilities as appropriate. For example, the IT supervisors will be assigned the responsibility of conducting quality assurance checks on the CMDB to verify accuracy of information. The emphasis placed on quality is important for mitigating risks associated with using the CMDB to identify vulnerabilities. The VMT will also conduct routine scans as a quality assurance check to verify software configuration items are correct.

Conclusion

Vulnerability Management and Configuration Management go hand in hand. The Organization currently has difficulty keeping software patched which results in software vulnerabilities. This failure introduces significant risk to the organization as the resulting vulnerabilities may be exploited by numerous methods and threat agents. Creating a Configuration Management System (CMS) that consists of the existing Change Management process and the new Configuration Management Databases (CMDBs) will help the Organization understand where vulnerabilities exist and enhance the technician’s effectiveness at mitigating those vulnerabilities.

References

Al-Shaer, E., Kalmanek, C. R., & Wu, F. (2008, October). Automated Security Configuration Management. *Springer*, 231-233.

Andrew, C. (2006, August). Orchestrate vulnerability management. *Communication News*, 26-27.

Defense Information Systems Agency. (2007, February 14). *DISA IAVM Process Handbook*. Retrieved August 1, 2011, from www.tricare.mil/tmis_new/ia/disa-iava-process-handbook.doc

Department of Defense. (2007, April 23). *Information Assurance (IA)*. Retrieved July 17, 2011, from http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

Executive Office of the President. (2003). *Performance-Based Service Acquisition; Contracting for the Future.* Washington DC: Interagency Task Force on Performance-Based Service Acquisition.

Hurst, T. E. (2008, July). Digital Technology Spawns Need for Configuration Management. *Power*, 83.

Intergovernmental Panel on Climate Change. (n.d.). *Quality Assurance and Quality Control.*

Kovachich, G. L. (2003). *The Information Systems Security Officer's Guidebook.* USA: Elsevier.

Marine Corps Institute. (2002). *Operational Risk Management.* Washington, DC: Headquarters Marine Corps.

Marquis, H. (2006, December). ITIL: What It Is And What It Isn't. *Business Communications Review*, 49-52.

Marquis, H. (2007, February). ITIL and the Evolving CMDB. *Business Communications Review*, 54-57.

Sequeira, D. (2003, March). Intrusion Prevention Systems: Security's Silver Bullet. *Business Communications Review*, 36-41.

CMDB databases

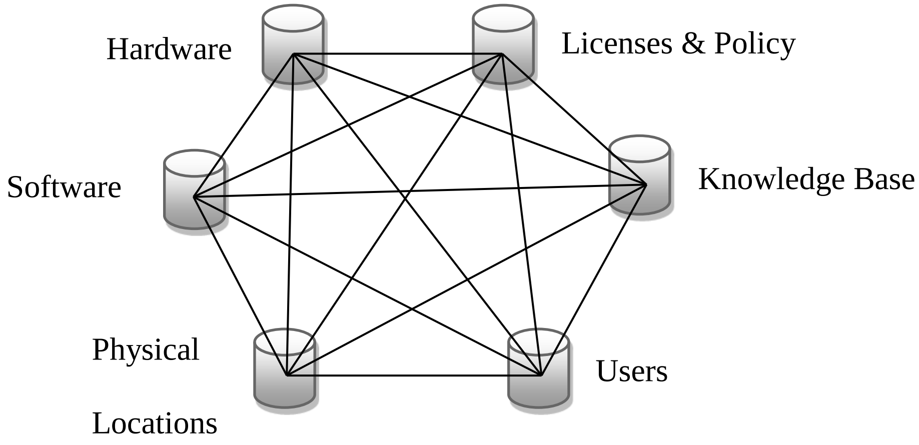

Figure 1: This figure shows the relationship between databases in the CMDB as a many-to-many relationship.

Table 1: Data theft by external threat agent due to outdated or unpatched software configuration item

Risk Assessment Matrix					
SEVERITY		PROBABILITY			
	CATEGORY	A	B	C	D
	I	1	1	2	3
	II	1	2	3	4
	III	2	[✓ 3]	4	5
	IV	3	4	5	5

Final Risk Assessment Code: 3

Corresponding Risk Assessment Code: Moderate

Table 2: System denial of service by external threat agent due to outdated or unpatched software configuration item

Risk Assessment Matrix					
S		PROBABILITY			
E	CATEGORY	A	B	C	D
V	I	1	1	2	[✓ 3]
E	II	1	2	3	4
R	III	2	3	4	5
I T Y	IV	3	4	5	5

Final Risk Assessment Code: 3

Corresponding Risk Assessment Code: Moderate

Table 3: Misinformation introduced by internal threat agent by privilege escalation utilizing software vulnerabilities

Risk Assessment Matrix					
S		PROBABILITY			
E	CATEGORY	A	B	C	D
V	I	1	1		3
E	II	1	2	3	4
R	III	2	3	4	5
I T Y	IV	3	4	5	5

Final Risk Assessment Code: 2

Corresponding Risk Assessment Code: Serious

Table 4: Inconsistent baselines due to employee shortcuts

Risk Assessment Matrix					
SEVERITY		PROBABILITY			
	CATEGORY	A	B	C	D
	I	1	1	2	3
	II	[✓ 1]	2	3	4
	III	2	3	4	5
	IV	3	4	5	5

Final Risk Assessment Code: 1

Corresponding Risk Assessment Code: Critical

Table 5: Inaccurate data in the CMDB caused my employee error

Risk Assessment Matrix					
SEVERITY		PROBABILITY			
	CATEGORY	A	B	C	D
	I	1	1	2	3
	II	1	[✓ 2]	3	4
	III	2	3	4	5
	IV	3	4	5	5

Final Risk Assessment Code: 2

Corresponding Risk Assessment Code: Serious

About the author

Author: Christopher Furton

Website: Http://christopher.furton.net

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

Visit the auhor's blog:
IT Management Perspectives - https://christopherfurton.wordpress.com/

Social Sphere:

LinkedIn Twitter Google+ Quora Wordpress Flavors.me

Slide Share Tumblr YouTube Pinterest About.me Vimeo