Cost Management for Security Applications

Arshi Naim[1], Zubairul Hasan[2]
Department of Information Systems, College of Computer Science, King Khalid University, Abha, KSA
University of Lucknow, India
Corresponding author's:

Abstract
This is an extended paper, focusing on the cost management for the organizations dealing with the crucial issues of security systems. Information Technology (IT) is an important and irreplaceable need of society and all working sector's success depends on IT to a greater extent; therefore maintaining security features is one of the most important aspects of IT. When security in the IT sector is discussed, Patch Management (P.Mgnt) has to be taken under account. P. Mgnt includes many concerns and areas to be described for IT security such as methods and problems in updating patch, methods of reducing security risks with P.Mgnt, methods of achieving economies of scale by controlling the operational costs and taking decisions in investing as and when necessary. This paper presents a general definition of Patch management, its benefits and management of working cost through theoretical models, also the paper gives methods of feeding techniques for microstrip patch antenna MPA, showing the contracting and non contracting methods.

Keywords:
Patch Management; IT; Microstrip Patch Antenna; Feeding Techniques; Operational Costs, Economies of Scale

1. Introduction

Major security problems are due to errors in software; these issues are commonly known as vulnerabilities which can create or enhance the security concerns [1]. In the current scenario IT industry faces major security challenges causing serious sabotages especially for confidential data in this situation investing for enhancing the security is not the choice but the need. Statistical data show that IT has a major objective to remove vulnerabilities because out of one thousand software codes, percentages of errors and mistakes are very high almost 20% of it. Below given figure is presenting the relevance of P. Mgnt as per IT in the system management [2] [4].

Figure1: Relevance of P.Mgnt in Systems Management [1]

Manuscript received July 5, 2024
Manuscript revised July 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.7.8

Benefits of P.Mgnt has many dimensions and it performs several jobs, some of them are maintaining current knowledge of available patches, deciding the patches that are suitable for particular systems, ensuring that patches are installed in a right way, testing systems after installation, and documenting all associated procedures [4] [21].

Table 1: Examples of Products for P.Mgnt [9]

Examples of Products Working to Automate Patch Management Tasks
RingMaster Software's APM
ManageEngine's Desktop Central
Central and SolarWinds Patch Manager.

Like the health and security are important for all areas, the same implies for systems also, health refers to the well being of the systems and working without any errors and security means systems without vulnerabilities; the P.Mgnt is important in aiding to maintain the health and security of the systems that are being patched. Besides the patches are also used to bring software up to date to be compatible with the latest hardware, but this process requires good investment and therefore the costs are likely to increase to a good level. Organizations incur the cost in the optimal frequency of patch updates to make the balance of operational costs and damage costs related with security vulnerabilities [5].

2. LITERATURE REVIEW

In the year 1950s, pioneer *Microstrip Antenna* (Ms.A) [23] was introduced but it took two decades to gain popularity and awareness for its use and benefits. Only after the development of printed circuit boards (PCB) in the 1970s, Ms.A got its recognition. Ms.A has many advantages such as light weight, low profile, low cost, planar configuration, easy of conformal, superior portability, suitable for array with the ease of

fabrication and integration with microwave monolithic integrate circuits (MMICs) and after PCB these benefits were known and used at a greater extent.

The applications of Ms.A are not limited to single areas but from official levels to personal levels, some of the examples are given in the figure below [7].

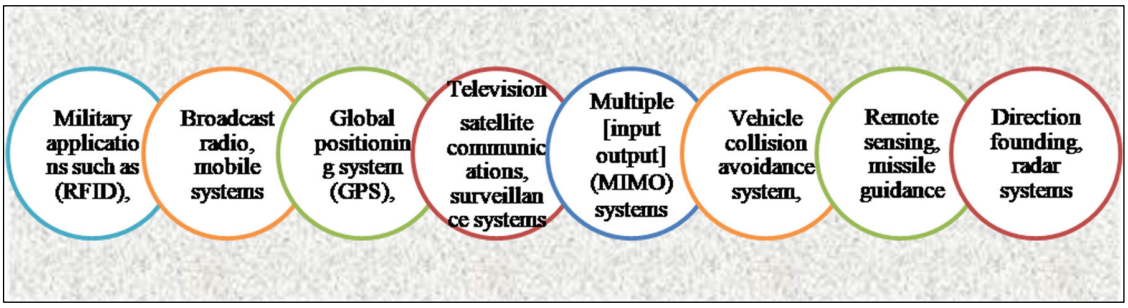
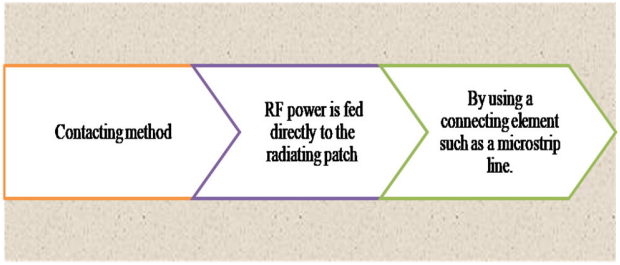


Figure 2: Applications of Ms.A [23]

Figure 2 shows the applications of Ms.A, but the applications are not restricted to these examples only, there are many more examples which are not covered in this paper. Antenna is a transducer which transmits or receives electromagnetic waves. Ms.A has several advantages over conventional microwave antenna (Mw.A) and therefore it is used in a variety of practical applications. Ms.A has two sides in its design; one side has dielectric substrate and ground plane (GP) on another side.

To describe *Microstrip patch antenna* (MPA), it has non planar and planar geometry on one side of a dielectric substrate and a GP on other side [23]. MPA is used widely because of its planar configuration and ease of integration with microstrip technology. It is a printed resonant antenna for narrow-band microwave wireless links requiring semi-hemispherical coverage. The rectangular and circular patches are the basic and most commonly used MPA [23].

2.1 Feeding Techniques: There are many methods of feeding techniques for MPA, here we show the contracting and non contracting methods and below given Figures present the methods of feeding techniques for MPA.



In this method, the use of connecting elements like microstrip line is used for RF power which later is fed straight to the radiating patches.

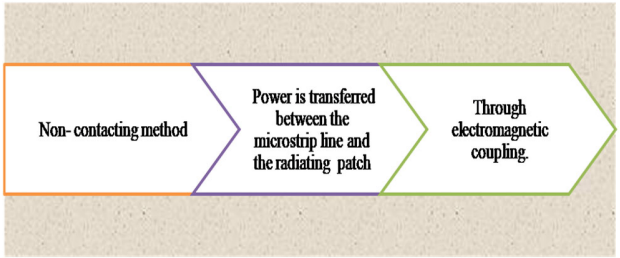


Figure 4 Non Contracting Method [6] [7]

Electromagnetic coupling allows the transfer of power between the microstrip line and the radiating patch in a non contracting method. Table 2 show most popular feeding techniques; although as mentioned earlier there are many other techniques also which are not given in this paper.

Table 2: Four Popular Feeding Techniques [17]

Popular Feeding Techniques
Microstrip line (Ms.L)
Coaxial probe (C P) (both contacting schemes)
Aperture Coupling (AC)
Proximity Coupling (PC) (both non-contacting schemes).

3. DISCUSSION

3.1 ***(Ms. L)*** is a kind of feed arrangement that has the gain that the feed can be fixed on the same substrate to supply a planar structure and the conducting strip is smaller in width in contrast to patch. In Ms. L the conducting strip is connected in a straight line to the edge of the Ms. P.

(CP) is difficult to model and has the issue that it provides narrow bandwidth, in CP, the inner conductor of the coaxial connector widens throughout the dielectric and is soldered to the radiating patch (RP), while the outer conductor is coupled to the (GP). The major advantage of this is that the feed can be positioned at any of the required locations inside the patch in order to match with its input impedance.

3.2 In *(AC)* technique, the RP and the microstrip feed line are parted by the (GP). The patch and the feed line are coupled through a slot (CS) in the ground plane. This technique has multiple layers that cause an increase in thickness of the antenna. This aspect is considered to be the big flaw and disadvantage in this technique. Below given figure shows the process of this feeding technique.

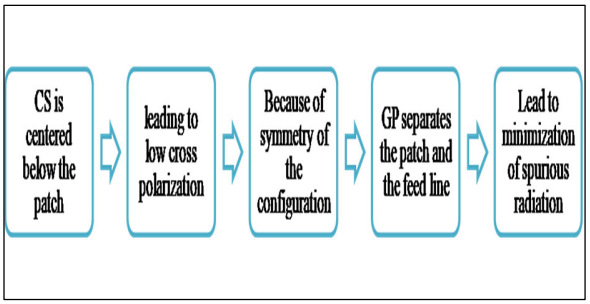


Figure 5: AC feeding technique [3] [6]

3.3 ***(PC)*** has another term which is electromagnetic coupling scheme that has two dielectric substrates which are applied between two substrates through a feed line. The (RP) is placed on top of the upper substrate which provides the benefits to this feed technique not only this it also offers high bandwidth. Below given table shows the major benefit and disadvantage of this feeding technique.

PC	
Advantages	Disadvantage
It is able to overcome and remove fake and suspicious feed radiation.	It has two dielectric layers which requires good mapping , therefore it gives rise to complexity in fabrication.

Table 3: PC Advantage and Disadvantage

3.4 Applications *of Microsript Patch Antenna*: The microstrip patch antennas (MPA) are well known for their performance and strong design [12] [23]. MPA has applications in various fields such as in the medical field, satellites, military systems, rockets, aircrafts missiles and many more. In the current situation these applications are growing for several commercial features also especially for the cost optimization options for different substrate materials and production. MPA has a number of applications and some of these applications are given in figure 6 and described in Table 4.

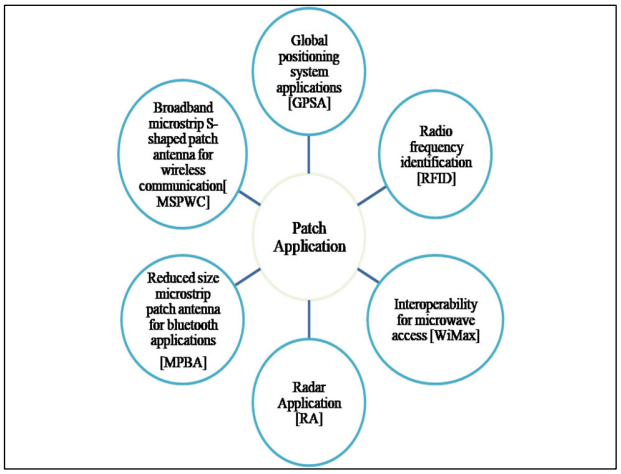


Figure 6: Applications of MPA [8]

Table 4: Description of Applications of MPA [8]

Application	Description
GPSA	Microstrip patch antennas having high permittivity sintered substrate material for global positioning system (GPS). These antennas are circularly polarized and very compact.
RFID	RFID is used in different areas like mobile communication, logistics, manufacturing, transportation and health care. RFID system generally uses frequencies between 30 Hz and 5.8 GHz depending on its applications. Basically RFID system is a tag or transponder and a transceiver or reader.
WiMax	The IEEE 802.16 standard is known as WiMax. It can reach upto 30 mile radius theoretically and data rate 70 Mbps. Microstrip patch antenna generates three resonant modes at 2.7, 3.3 and 5.3 GHz and can, therefore, be used in WiMax compliant communication equipment.
RA	Radar can be used for detecting moving targets such as people and vehicles. The microstrip antennas are an ideal choice. The fabrication technology based on photolithography enables the bulk production of microstrip antenna with repeatable performance at a lower cost in a lesser time frame as compared to the conventional antennas.
MPBA	The microstrip antenna operates in the 2400 to 2484 MHz ISM Band.
MSPWC	This is a single-patch broadband microstrip S-shaped patch antenna. Microstrip S-shaped patch antenna is fed by a coaxial feeding. The antenna is designed by inserting two slots into rotated square patch then it look like English letter 'S'. Because of the slots and thick substrate, bandwidth of antenna is increased.

3.5 Working of P.Mgnt: The working and application of P.Mgnt depends on the condition if patch is used to a standalone system or on a system for corporate networks. Figure given below explains both the cases; standalone system and corporate network [10].

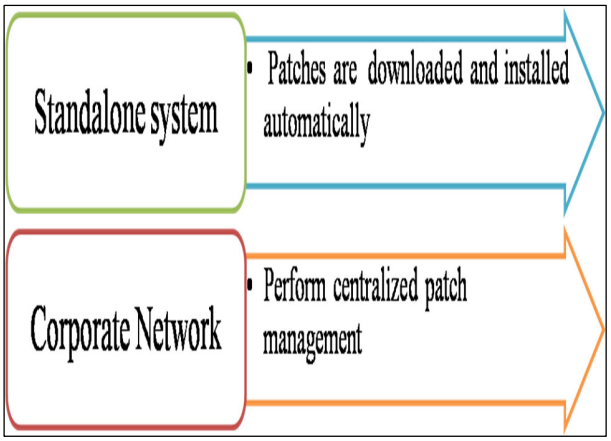


Figure 7: Application of Patch Mgnt for two cases [16] [17]

The case of Stand-alone system is automatic condition where the operating system and the applications on that system perform an automatic check on regular basis and find the availability of patches, in case of new patches are found, the system downloads them automatically. In case of corporate situation P.Mgnt work in a different way because firms have to keep the stability and consistency for all machines therefore automatic download is not feasible even if updated patches are available. In most of the situation organizations execute the centralized approach than of allowing machines to download the patches by themselves. Below given figure shows the P.Mgnt for corporate network [13].

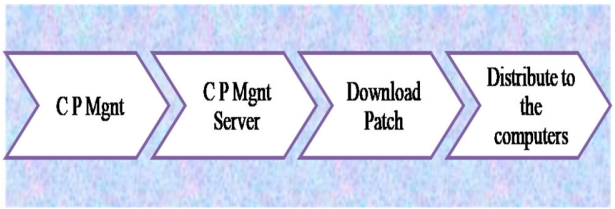


Figure 8: Working of P. Mgnt for corporate network [13]

A centralized patch management (CPM) server has many jobs like it gives the organization some level of control for P.Mgnt process, for instance if a particular patch is determined to be problematic, then the organization can configure its P.Mgnt policy to prevent that particular patch from being deployed apart from automating the P. Mgnt.

CPM provides many advantages for the firm like retaining the internet bandwidth, which is described as the advantage for the organization because it omits the need for all systems to download the similar patch rather it helps in downloading once and distributing for all the other systems in the firm. This is an ideal condition but does not mean that all organizations would follow the same strategy for P.Mgnt, some firms prefer to a higher professional for the security management and others refer to apply different network management services.

Most of the software companies in fixed intervals provide patches for their benefits for many benefits. There are basically three main purposes for the firms to release new patches for their products, given below figure present these three purposes and Table 5 gives the brief description of each purpose.

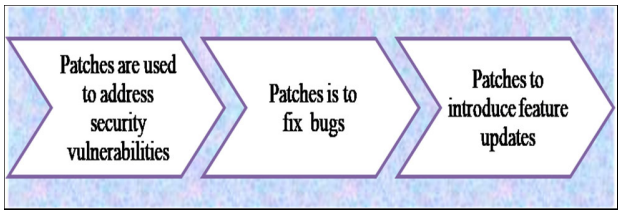


Figure 8: Three primary purposes of P.Mgnt [5] [13]

Patches may not have benefits all the time, there are many common problems such as[4] [17] Buggy Patch, New problems that are not known before can be initiated by patches, New Problems are introduced by the implementation of patch which otherwise were not present in the previous systems, Patches are deployed without being tested for bugs or any other compatible issues for the software system, Patches are not received timely and Patches are not updated or released for the new products.

Table 5: Description of purposes of P.Mgnt [14] [15]

Description
Hackers are always in the look out of week securities or vulnerable situations and the applications of Patches are to address security vulnerabilities, therefore if any such situation is identified or present in form of security risk then it is the responsibility of the vendors to work and control risk by issuing the patch to remove risks in the products.
Sometimes during the validation stage certain bugs are discovered so if the firm does not release patch to fix the problem it may lead to more serious issues of security. These preventive measure givens two benefits; first to increase software working with reliability and stops future security risk.
Quality management is always an important aim of all the software firms and for improving the existing feature or introducing the new firms would require to offer patches for better working, better security and even for updating the systems.

***3.6 Patch management life cycle*:** It is the work of firms to take testing under consideration before the release as well as deploying it at all the levels of organization. The IT department has to play the major role in P.Mgnt for conducting the test within the sandbox (SB) environment, this may result in controlling the problem of security and the production system will not get affected due to any loophole in P.Mgnt [13]. The IT department has to take many optional methods to maintain the security with any issues, the following figure shows those options.

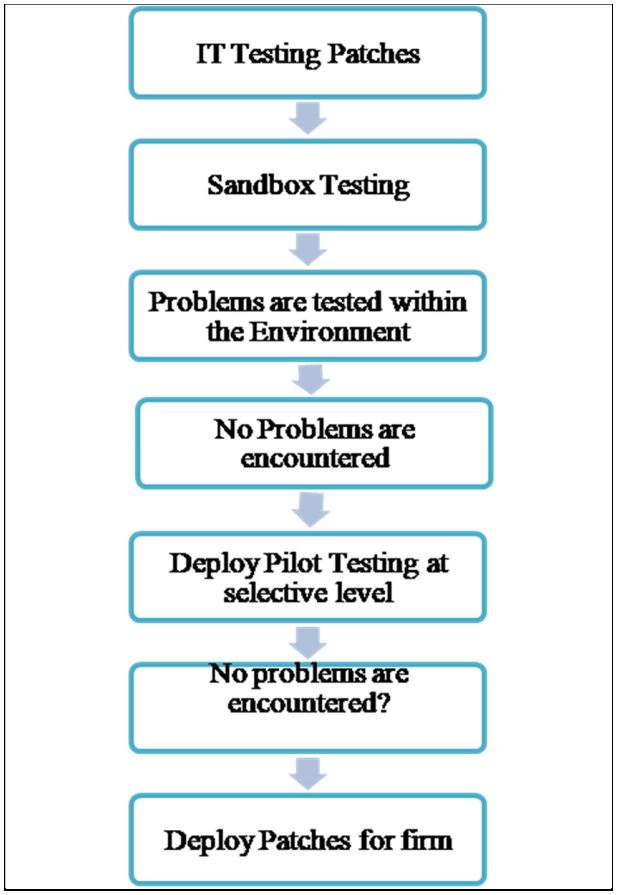


Figure 9: IT P.Mgnt for the Firms [13]

Results may vary from the testing to the real deployment of patches, however it is not a common scenario but sometimes patches are identified for causing the issues to the production systems in this situation firms take a decision to remove the patch to maintain the security systems. P.Mgnt is not an easy function; IT department has to take complex decisions on releasing, updating and deploying the patches also issues are witnessed on receiving the patches for the firm as and when needed. There are simple to complicated decisions IT has to take for the application of Patches for the Production systems. The IT recommends some suggestions for the P.Mgnt following table describes the recommendations for P.Mgnt for the firm.

Table 6: P.Mgnt Recommendations [12] [13]

Recommendation for P.Mgnt
Develop one Patch and Vulnerability Group (PVG) in small firms
Large firms to monitor and responsible for the execution of Patches
Large firm assign some team members for creating and deploying of these Patches and study PVG
Separate IT team with complete autonomy should work for the P.Mgnt and study the vulnerabilities.
Only IT team members should be responsible for the implementation.

The PVG is charged with a number of responsibilities, not least of which is taking inventory of all the IT resources in your company's system. It's important to capture hardware, which may require firmware updates, and software, including applications and operating systems. This puts them in a good position and be responsible for monitoring for updates and patches for this equipment.

Prioritizing the order of implementation of the patches is also PVG responsibility. Hopefully, if the company has the resources for the PVG to create a database as a repository for this information so all the patches/ remediation can be logged somewhere accessible to those who need to know about them. Most of the firms apply the following process for the P. Mgnt which is given in figure below:

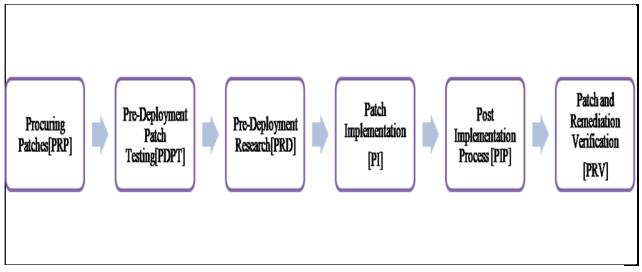


Figure10: Process of Procure and use of Patches [10]

a. PRP

Purchase/ obtain the real patches from any of the sources like downloading from the websites or other distributors. Although there are methods of automation for obtaining patches, it is relevant to check the authenticity of the patches; to do that PVG has to carefully be analyzed and then patches should be determined.

This process is not an easy process; PVG tests the virus and bug and makes sure for error free and no infection in patches. Firms can use a few easy methods to do so like updating the software, installing the licensed antivirus and updating it regularly. Hackers' mischief and attempt to make unauthorized access cannot be avoided but such applications can provide multi-layering in the security systems for patches.

b. PDPT

Before deploying the Patches, certain measures are recommended for the firms to apply because just implementing the new patch and replacing the old one does not necessarily enhance the security systems and it is not an easy process too therefore before using the patch for the real system, it is used for non production for testing. If testing doesn't encounter any problem deployment can be carried out smoothly. This pre testing is very important to avoid risks of crashing of systems or other major problems. This paper has mentioned two types of test environment for pre using of patches; such as SD testing for the environment and Pilot testing for the same specifications for the systems.

c. PDR

Sometimes firms have to meet the deadlines and do not have time or even infrastructure to conduct pre testing, in such situations previous studies and researches are very helpful for knowing the reasons and solutions for P.Mgnt. This existing research provides benefits and disadvantages of deploying the patches for the production systems, methods, and other necessary recommendations.

PDR elaborates the criteria and conditions to examine for describing and obtaining the patches, also provides reviews of threats, risks and other major issues apart from the results caused by the implementation of patches. Operational cost is also studied in PDR and gives details on how to maintain economies of scale for the future.

d. PI

If PI works in phases, chances of crash and other risks associated with patches are reduced, also it is not mandatory to consider the size of the firm, therefore if PVG is conducted and patches are first manually implemented followed by the automation it may result in better functioning of the system. Firms should apply patches for the entire system to defend all security threats and risks.

e. PIP

The IT department of a firm can use the approach of PVG for communication of information for solutions, and types of vulnerabilities for the existing systems. This method will lead to the IT team members to handle the critical issues without major administrative hurdles because the entire firm will be well distributed with the information about PVG. Besides dealing with the technical issues PVG also deals with administrative decisions on allocating cost for patches in the financial budget.

f. **PRV**

Implementation is not the last stage but to check whether the applied patches are working successfully for enhancing the security or not and also if its cost effect or not, therefore PVG offers all possible options for the good working of patches. PRV accounts on first results of testing on non production system before commercializing at the real production system for the firm, apart from these there are few more methods for the verification of patches like verifying the documents of service providers checking for the specifications, compatibility followed by checking the process of installation, correctness and effective testing on the systems.

3.6 COST MANAGEMENT FOR P.MGNT

Cost management for P.Mgnt focuses on methods of cost optimization, mostly cost increases for P.Mgnt due to two reasons, firstly when firm shows reluctance in investing in updating when the patches are released and important to be deployed and secondly when service providers wait for the identification of vulnerabilities [5] [11]. Both situations cause an increase in cost investment and firms have to take immediate application to maintain the security for the systems.

Achieving the economies of scale is important management issues for types of firms and when we

explain this for the IT sector, investment in P.Mgnt is more widely dealt, the firm incurs two types of cost in patch management [11].

a. Cost incurred as a remedy of damage
b. Cost incurred for the update

Firms have to invest more monetary inputs for the situation when security is not examined and existence of vulnerabilities are not patched causing major damage in the system. Another manor investment that a firm has to make on a regular basis is on updating, testing and installing the patches.

Cost management for the P.Mgnt is also a complex decision making process for the firms because occasionally remedial investment in updating or deploying new patches can cause other problems in product management. The last part of the paper deals with the cost management for P.Mgnt that includes various decisions for the firm. These decisions are given in figure 11.

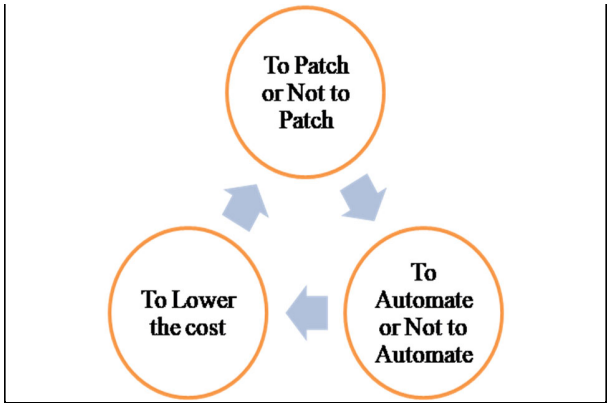


Figure 11: Cost Management decisions for P.Mgnt [11]

Here the firms need to take the decisions on cost effectively and tradeoff for security, therefore cost ratio analysis is done to evaluate if investment should be done for release of new packets, update the packets or install the packets or to compromise on security for product management. Here the decision is also based on the value and relevance of security in comparison to the investment necessary for the patches; also it depends on the affordability of the firms to invest more cost especially for small scale organizations.
Firms make comparative analyses for between automation and manual control to decide cost investment decisions [11]. The decision is based on the annual report for cost and benefit ratio between the two options to automate or manually deploy the patches [18] [19].

Most of the time avoiding const increment cannot be controlled and as mentioned earlier small firms are unable to increase the investment in the budget for IT sector in this situation firms have to compromise on other grounds, which are usually based on low cost solutions [11] [19]. These low cost solutions include, introduction of security at managerial levels, reducing cost for other infrastructure such as cost for material. However these solutions are not appropriate because software vulnerabilities can effectively be solved through deployment of patches, in this situation, the most suitable solution for the firm is to share the cost of software products. This method seems to be directed for cost optimization but the software experts question this type of solution for its implication. If the bugs or vulnerabilities are due to any faulty issues in the program and software firms are accountable for that, then further investment in P.Mgnt is not justified and cost should be borne by the software firms. Software experts suggest sharing of liabilities in this scenario and also to the methods of meeting cyber security challenges [17].

4. RESULTS

The results show that software vulnerabilities are best solved by the deployment of patches but firms have to make some complex decisions on when and how patches should be applied. There are many methods of feeding techniques for MPA, but this paper has shown two important methods; contracting and non contracting methods for the firms. Ms.A has its application in varied sectors and the working and application of P.Mgnt depends on the condition if patch is used on a standalone system or on a system for corporate networks. Conditions and working of Patches are defined for both the conditions. This paper also shows the working of Patch management life cycle and why firms have to take testing under consideration before the release as well as deploying patches at all levels of organization. The study offers recommendation for P.Mgnt for the IT firms and the process of procure and use of Patches, finally cost management for P.Mgnt is

described with the reasons for why cost investment is made for P.Mgnt and what are the major decisions firms have to take for cost optimization. Last but not the least the paper gives a brief recommendation by the software experts in the field of cost management for P.Mgnt.

5. CONCLUSION

This paper is a qualitative paper showing the general scenario of P.Mgnt that can facilitate the firms in overall management, understanding the benefits and disadvantages of P. Mgnt, and why Patches are important, the process of P.Mgnt and its cost management.

References

[1] Dey, D., Lahiri, A., & Zhang, G. (2015). Optimal policies for security patch management. INFORMS Journal on Computing, 27(3), 462-477.

[2] Martini, B., & Choo, K. K. R. (2014). Building the next generation of cyber security professionals. Martini B and Choo KK R.

[3] Wang, B., Li, X., de Aguiar, L. P., Menasche, D. S., & Shafiq, Z. (2017). Characterizing and modeling patching practices of industrial control systems. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 1(1), 1-23

[4] Force, J. T. (2017). Security and Privacy Controls for Information Systems and Organizations (No. NIST Special Publication (SP) 800-53 Rev. 5 (Draft)). National Institute of Standards and Technology.

[5] Chatterjee, S., & Thekdi, S. (2020). An iterative learning and inference approach to managing dynamic cyber vulnerabilities of complex systems. Reliability engineering & system safety, 193, 106664.

[6] Alshawish, A., & de Meer, H. (2019, June). Risk-based decision-support for vulnerability remediation in electric power networks. In Proceedings of the Tenth ACM International Conference on Future Energy Systems (pp. 378-380).

[7] Souppaya, M., & Scarfone, K. (2013). Guide to enterprise patch management technologies. NIST Special Publication, 800, 40.

[8] Hassani, P. (2020). Implementing Patch Management Process.

[9] Gauci, A., Michelin, S., & Salles, M. (2017). Addressing the challenge of cyber security maintenance through patch management. CIRED-Open Access Proceedings Journal, 2017(1), 2599-2601.

[10] Sihvonen, H. M., & Jäntti, M. (2010, August). Improving release and patch management processes: An empirical case study on process challenges. In 2010 Fifth International Conference on Software Engineering Advances (pp. 232-237). IEEE.

[11] Segre, H., Carmel, Y., Segoli, M., Tchetchik, A., Renan, I., Perevolotsky, A., ... & Shwartz, A. (2019). Cost-effectiveness of uncultivated field-margins and semi-natural patches in Mediterranean areas: A multi-taxa, landscape scale approach. Biological Conservation, 240, 108262.

[12] Nunez, Y., Gustavson, F., Grossman, F., & Tappert, C. (2010, June). Designing a distributed patch management security system. In 2010 International Conference on Information Society (pp. 162-167). IEEE.

[13] Song, K. T., Kim, S. I., & Kim, S. H. (2021). A Design of Improvement Method of Central Patch Controlled Security Platform Using Blockchain. In Advances in Computer Science and Ubiquitous Computing (pp. 555-561). Springer, Singapore.

[14] Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2020). Software Security Patch Management--A Systematic Literature Review of Challenges, Approaches, Tools and Practices. arXiv preprint arXiv:2012.00544.

[15] Mohlenhoff, K. A., & Codding, B. F. (2017). When does it pay to invest in a patch? The evolution of intentional niche construction. Evolutionary Anthropology: Issues, News, and Reviews, 26(5), 218-227.

[16] Lee, J. H., & Kim, H. (2017). Security and privacy challenges in the internet of things [security and privacy matters]. IEEE Consumer Electronics Magazine, 6(3), 134-136.

[17] Gauci, A., Michelin, S., & Salles, M. (2017). Addressing the challenge of cyber security maintenance through patch management. CIRED-Open Access Proceedings Journal, 2017(1), 2599-2601.

[18] Kim, J., Sohn, M., & Won, Y. (2017). An Automatic Patch Management System with Improved Security. In Advanced Multimedia and Ubiquitous Engineering (pp. 74-80). Springer, Singapore.

[19] Monperrus, M. (2014, May). A critical review of" automatic patch generation learned from human-written patches": Essay on the problem statement and the evaluation of automatic

software repair. In Proceedings of the 36th International Conference on Software Engineering (pp. 234-242).

[20] DeLuzio, C. (2019). Procurement Guide for Better Election Cybersecurity. New York: New York University School of Law.

[21] Naim, A. (2020). Realization of diverse Electronic tools in learning and teaching for students with diverse skills. Global Journal of Enterprise Information System, 12(1), 72-78.

[22] Humble, J., & Farley, D. (2010). Continuous delivery: reliable software releases through build, test, and deployment automation. Pearson Education.

[23] Sotres, P., Santana, J. R., Sánchez, L., Lanza, J., & Muñoz, L. (2017). Practical lessons from the deployment and management of a smart city internet-of-things infrastructure: The smartsantander testbed case. IEEE Access, 5, 14309-14322.

[24] Kaur, N., & Malhotra, S. (2016, October). A review on significance of design parameters of microstrip patch antennas. In 2016 5th International Conference on Wireless Networks and Embedded Systems (WECON) (pp. 1-6). IEEE.

[25] Naim, A., Khan, M. F., Hussain, M. R., & Khan, N. (2019). "Virtual Doctor" Management Technique in the Diagnosis of ENT Diseases. JOE, 15(9), 88.