Security Program Elements of Adoption

Term Paper

2015 Summer Network Security Management ICTN6823

By Robert Underwood

July 20th 2015

Eastern Carolina University Dr. Lunsford

Abstract

With the risk of losing information to an unwanted entity the process of securing information is at high level priority to businesses. Although there are many models and frameworks that can be applied if the culture does not accept or adopt the methodologies then the effort is in vain and the investment is lost. Understanding the culture within a business and applying the appropriate adoption methodology is the best chance for implementation success.

Understanding the culture and how to integrate new processes through training techniques geared to individual employees which provides a platform for successful adoption.

Security Program Adoption

Security models and frameworks possess one thing in common, tasks. These tasks are usually assigned by role and responsibility and are composed of actions need to carry out the security policy. As in the NIST framework where risk is the driving element that defines a common language for understanding, managing, and expressing cybersecurity risk and is a tool for aligning policy, business, and technological approaches to managing risk (National Institue of Standards and TEchnology, 2014) which each define levels of tasks to be implemented in order to complete the work needed to implement the framework.

Organizational Culture

The day to day employee for any business has a custom groomed process for their day to day work and integrated with coworkers who have done the same in a way that creates a synergy between employees and their work, known as organizational culture. According to (Martin M. J., 2006) culture consists of an organization’s shared values, symbols, behaviors, and assumptions

which allows its members to frame events in a similar fashion and provides the stability an organization needs for success.

Emphasis on implementation

With the implementation of a security policy depending on adoption and that adoption depending on how the culture accepts the new process it seems that industry would put more emphasis on the process and would included the integration techniques needed to motivate the culture toward adoption. Within the NIST framework the user is given the reasons and benefits of using the methodology and NIST acknowledges that more is needed to making adoption successful by publishing a roadmap (NIST, 2014) called "NIST Roadmap for Improving Critical Infrastructure Cybersecurity."

The NIST roadmap only address the issue of adoption through organizational influence from the top down methodology by implementing a governance framework that aligns with the company's strategic goals and collaborative work as seen through information stakeholders. As the roadmap explains there is a level of maturity that accompanies adoption over time which in other terms is the more you work with something the more familiar you become with the process (NIST, 2014). This idea sounds familiar as we defined in earlier in reference to culture where the day to day work become the status quo. The important takeaway from the roadmap is the top down methodology which is a critical step to adoption. As identified by (*) executives that understand and champion these effort help the implementation of information security polices by (*)

Failure to Implement

According to (Weaver-Johnson, 2010) from the website Infosec Island most organizations understand the importance of assessments and planning but where many fail to

deliver is in the implementation phase. Numerous headlines and lessons learned show a failure to implement can lead to expensive fines, lawsuits, and loss. An organization can have the best security policy but if it is not implemented down to the individual who has the role and responsibility to take action on the security policy is ineffective.

Recorded company failures of implementation in 2014 include Snapchat; Heartbleed, Shellshock and Poodle; Apple iCloud; Home Depot; and Sony Pictures (Wagenseil, 2014). The types of implementations failures vary in each case but are surely a case of missing the mark where known issues could have been mitigated by security practitioners. (Wagenseil, 2014) writes for a website, Tom's Guide, who reported that Snapchat could have avoided a massive data breach where more than 4 million users phone numbers and usernames were stolen. The information was gather using techniques that Snapchat had been alerted to almost a year previously. The question here is how did the mitigation not get administered, who is liable for this? In another incident with CVS where employees violated company security policy and HIPAA policies by throwing old prescription bottles into dumpsters exposing many customers to information loss CVS was fined $2.25 Million (Weaver-Johnson, 2010).

Ineffective Communication

(Weaver-Johnson, 2010) reports that and organization that just blasts out security policies in emails and memos has no way to determine whether the actions have been taken to read or understand the information and that to implement policies, procedures, plans and processes means that organizations have to document and prove that individuals have read, understand and acknowledge their roles and responsibilities. Additionally legal due diligence requires proof of implementation in the manner prescribed by documentation. Organizations must ensure all appropriate individuals are receiving updated policies and guidelines, reading the policies,

understanding the policies, and acknowledging their individual roles and responsibilities (Weaver-Johnson, 2010).

As Weaver-Jonson points out the flaw in the implementation process occurs at the individual level so what are some of the issues individuals face when given a security policy to implement?

Fear of the Unknown

No one likes change and when an organization tries to change the effect on employees can result in resistance and even outright defiance. According to (Quast, 2012) a writer for Forbs there are five main reasons people resist change:

1. Fear of the Unknown. Without adequate training, notification, and warning employees will not understand what is taking place and be fearful.
2. Mistrust. Managers can been seen as looking out for their best interest and not the employee's.
3. Loss of Job Security. Employees can feel as if they have lost control or might be replaced with the process and lose their job.
4. Bad Timing. Overloading employees with changes without considering their current workload can make an employee feel like it is the wrong time to change.
5. Individual's Predisposition to Change. Some employees overall tolerance for change is very low.

Knowing these facts can be very beneficial to the planning phase by gathering data through interviews, polling, or questioners a project manager who is implementing security methodologies can be prepare with cultural requirements for the implementation to mitigate these issues. Specifically to mitigate some of these issues a project manager could hold a

requirements meeting asking employees about how the change will affect the employees work mitigating fear and mistrust. A project manager could ask about scheduling the change at a time when which would give the employee more control over the change therefore mitigating loss of job and bad timing. Understanding why a person has a predisposition to change can help a project manager and the employee with the condition to develop a strategy to help the change occur within the scope of acceptance the employee can deal with.

In the scenario described the type of communication depicted is person to person or management to employee where the managing the expectation is the can circumvent the antithesis to the desired work. The key to the conversation is communication skill and expressing the expectation in a way that a person can understand, according to (Irmshen, 1996) the paramount precept to interpersonal relations are to seek first to understand then to be understood.

Types of Culture

Types of organizational culture also influence the way work is executed and when planning a project should be considered. How types of organizational culture is made comes from learned behavior by new employees form the current employees it is taught to employees in a process of knowledge transfer. This knowledge comes in the form of formal and informal training but generally is transferred in the form of stories, myths, rituals and shared behavior. The types of cultures come from two major areas the first being sociability or friendliness among workers which is a highly sociable environment that has pleasant working environment which fosters creativity and workers generally go the extra mile to complete their assigned duties. The second type of organizational culture is known as solidarity where employees only care about their performance and duties. By classifying the type of organizational culture an employee is engaged in a project manager can plan to address their implantation approach tailored to the type

of organization culture. As an example in a sociable environment a brainstorming session where everyone involved in the same roles and responsibilities would be a welcome forum or in and organizational culture of solidarity the project manager could set goals for the group giving an atmosphere of competition where organizational culture solidarity thrives.

Addressing the issue of culture is only part of the equation in a successful adoption scenario but understanding the parts of organizational culture are an important start to the process of knowledge transfer as we establish a training program.

Teaching and Communication

To help adoption be successful we need to look beyond communicating what tasks and schedules are required to implement a security policy and ask each individual the right questions that provide the roadmap for their success in the process which can be accomplish by implementing a teaching and communication plan.

Implementing a teaching and communication plan that identifies individuals with their roles and responsibilities will help group people so that training curriculums can be created. Gathering data on skillsets, employee expectations, work environment impact, and process design feedback will help define what type of teaching technique will be needed. By establishing a teaching plan each employee becomes identified personally which creates an atmosphere of personal involvement and according to (Digital Learning, 2015) personalized teaching improves learning by right resources to the right people.

By using personalized teaching methodologies the employee's success can be tracked and measured against expected success to which the employee becomes a learner and the learner becomes valued. To educate a learner (Barbara Bray, 2013) says there are six steps to successful personalize learning.

Step 1. Understand Who Your Learners Are and How They Learn Best. Instructors can determine each learner's needs by understanding the Universal Design for Learning (UDL) principles which are the what, how, and why of learning. To address "the what of learning" is to provide multiple means of representation to accommodate perception, ethnic culture, and language that address the learners style of comprehension. To provide "the how of learning" is to provide multiple means of action and expression to accommodate the barriers that come between learners and way the express what they know or have learned. To address "the why of learning" is to provide multiple means of engagement where the learner can be engaged or motivated to learn (National Center of Universal Design for Learning, 2014).

Step 2. Design a Stage One Personalized learning Environment. A stage one learning environment is designed form the information in step 1 and determining how the learner learns best by establishing learning goals and a learning plans and by determine learner qualities through monitoring progress through lessons.

Step 3. Develop a Universal Designed Lesson. Based on voice and choice techniques to engage the learner develop methods, materials, and assessments that work for your targeted audience (National Center of Universal Design for Learning, 2014). By creating a flexible approach for a targeted audience an instructor will have the tools needed to deliver task and schedule expectation in a way that everyone can understand and provide the necessary feedback to develop a comprehensive implementation plan.

Task Validation

Most of a security policy is about monitoring and controlling the data location environment, access to data storage systems and its locations but what about the validation of the work that is performed and what is the mechanism that defines the quality of the implemented

security policy. The SANS organization provides a guideline that includes a project management best practices guild as defined by (SANS Institue, 2013) which defines verified deliverables as "Operations may expect the project delivery team to deliver an inherently secure system, while the project delivery team may expect security to be the responsibility of operations management after the system is handed off. Consideration should be given to when and how security concerns are most efficiently and effectively addressed in the total system lifecycle, not just during project delivery (Scheessele, 2007) (Rodgers, 2002). Ownership of security should rest with the project manager to the extent that the initial system setup is securable. "An organization can either incorporate security guidance into its general project management processes or react to security failures." says Robert Ellison of Carnegie Mellon University (Ellison, 2006). If security has been included in requirements gathering with input from the operations team, operational hand-off will be organized around verifying security deliverables as specified and transferring ownership rather than reacting to security problems identified by operations staff as the system is being put into production. Operational Acceptance Testing checklists (Moraetes, 2009) for non-functional components of a system (i.e., quality attributes such as performance, availability, and reliability) like Security Best Practices for IT Project Managers | 17 Michelle Pruitt, michelle.pruitt@gmail.com backup/recovery, maintenance and security can guide the hand-off and ensure that operations staff have the documentation and verified configurations they need to support the system".

Quality Assurance and Quality Control

According to the Guide of Project Management Body of Knowledge Version 5 (PMBOK5th) (Project Management Institute, 2013) quality assurance is audit the result of the quality control process so that improvements can be made to the quality control effort. Quality

control is defined as the validation of a measurement of a specific deliverable. Referencing the previous teaching and lesson plans which include verifying the knowledge transfer the methodology does not provide a method to monitor daily operational efficiency or correctness, this is where quality assurance comes into play. But first we need to define quality control, the and how we are measuring.

Quality Control

Creating a quality control plan is a measurement of the deliverable as defined by the customer (Project Management Institute, 2013) so with regard to information security policy what are we going to measure? Everything that is being required to perform can be measured even if it appears to be and intangible task. As an example there may be a security task that states that all the people in the world have to be counted every hour. There is too much information required in too little time to accommodate the requirement, although a ridiculous requirement the requirement supports the point that we need a viable solution other than physically counting every person. A solution may be to provide a statistical solution, as seen in population counts taken from a small samples of the populations that are used in predicting the total population within a statistical standard variation (NIST SEMATECH, na).

To implement a quality control plan Six Sigma Online (Aveta Business Institute, na) States “Creating a quality control plan can include the things you want to do to ensure that your products meet the requirements of the customer before you release them to the customer. The plan might include sending the product to a testing team for Alpha testing, back to the developers to rework, to the testers for Beta testing, and so on. Be sure the plan you define for the organization is very detailed and specific about how the process for ensuring quality will carry out in the business.

Once the quality control plan has been designed, it is important that you customize it to fit the ability of every department involved. Speak with management and team leaders in each department. Let them review the plan and see if they would like to add any additional changes or if they have ideas about an easier way to control the quality of your product. Involving everyone allows you to share the ownership but customize it to fit too.

Once it has been determined the quality control plan you have designed is sufficient then it is time to train everyone on how to begin working it. Employees need to have a clear understanding on the purpose of the plan and why they are being asked to do certain things. Motivate employees when you train them so they want to ensure quality for the customer too. Training requires everyone to learn how to use the methodology so it can be used on a regular basis.

After training, the next thing you need to do with a quality control plan is ensure everyone is using it. Some people have a hard time with change and they might go right back to the way they were used to doing things once you walk away. Remain on top of the situation and pay close attention. There are controls you can put in place to ensure the plan is being used. This might be what you need to do.

Once a quality control plan is in place and has been working for at least a month or a minimum of two weeks, everyone will be able to get together and offer their input on the plan. This will give people the opportunity to communicate issues or bottlenecks with the processes, improvements, and ideas.

Implementing a quality control plan must be done in steps to ensure it is successful. Everyone involved should play a part in the creation, testing, and use. Always verify people are

using the plan and continue on a regular basis to find ways that the plan can be improved (Aveta Business Institute, na)."

Quality Assurance

Once our quality control method has been developed we will have all the tools needed to validate whether we have met the conditions of the requirements. The next step to in quality assurance is to determine a schedule of audit and perform analysis on the reports provided by quality control to determine where improvement can be made (Project Management Institute, 2013).

Conclusion

In conclusion we have defined requirements to understanding how to develop the adoption plans to implement an information security policy. We examined how industry has failed with information security implantation and the reasons why they failed. We reviewed the key elements that provide the critical ideas needed to define the requirements such as ineffective communication, fears of the unknown, and organizational culture types. To meet the requirements we defined proven ideas from industry on teaching and communication which provide the method to resolve the issues defined in the requirements. Then lastly we define the methods to validate and verify if the tasks completed meet the requirements with task validation, quality control and quality assessment.

References

Aveta Business Institute. (na, na na). *Steps to Implement a Quatlity Control Plan*. Retrieved from Six Sigma Online: http://www.sixsigmaonline.org/six-sigma-training-certification-information/steps-to-implement-a-quality-control-plan/

Barbara Bray, K. M. (2013). A Step-by-Step Guide to Personalized Learning. *Learning & Leading with Technology*, 12-19.

Digital Learning. (2015). Persnalise Teachng Impr9oves Learning. *Digital Learning*, 7.

Irmshen, K. (1996). Communication in Education Interpersonal Relations. *Black and White Photographs*, 28.

Martin, J. (20006). That's the Way We Do Things Around Here: An Overview of Organizational Culture. *Electronic Journal of Academic And Secial Librarianship*, 1.

Martin, M. J. (2006, Spring). *That's the Way We Do things Around Here: An Overview of Oganizational Culture.* Retrieved from Electronic Journal of Academic and Special Librarianship: http://southernlibrarianship.icaap.org/content/v07n01/martin_m01.htm

National Center of Universal Design for Learning. (2014, September 18). *The Three Principles of UDL*. Retrieved from National Center of Universal Design for Learning: http://www.udlcenter.org/aboutudl/whatisudl/3principles

National Institue of Standards and TEchnology. (2014, February 12). *NIST Cybersecurity Framework.* Retrieved from National Institute of Standards and Technology: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

NIST. (2014, Feburary 12). *NIST Roadmap for Improving Critical Infrastructure Cybersecurity.* Retrieved from NIST: http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

NIST SEMATECH. (na, na na). *Quantitative Techniques.* Retrieved from Engineering Statistics Handbook: http://www.itl.nist.gov/div898/handbook/eda/section3/eda35.htm

Project Management Institute. (2013). *A Guide to Project Managment Body of Knowledge Fifth Addition.* Newtown Square: Project Management Institute.

Quast, L. (2012, November 26). *Overcome The 5 Main Reasons People Reist Change.* Retrieved from Forbs: http://www.forbes.com/sites/lisaquast/2012/11/26/overcome-the-5-main-reasons-people-resist-change/

SANS Institue. (2013, June 18). *Security Best Practices for IT Project Managers.* Retrieved from SANS Institure InfoSec Reading Room: http://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257

Wagenseil, P. (2014, December 19). *5 Worst Security Fails of 2014*. Retrieved from Tom's Guide: http://www.tomsguide.com/us/security-fails-2014,news-20049.html

Weaver-Johnson, K. (2010, April 30). *What is a "Failure to Implement"?* Retrieved from Infosc Island: http://infosecisland.com/blogview/3876-What-is-a-Failure-to-Implement.html