

Security Policy Management – Should you be Loved or Feared?

A fictional case by Mark McFadden

“Naomi, can you make this meeting we are just starting?” “Sure,” Naomi replied.

As she made her way down the hallway to the conference room she was curious as to the content and intent of this meeting. She and other mid-level managers had heard rumblings about the need to tighten up information security. While network operations had always done a good job, many of the senior level managers were not satisfied with the overall state of organizational security. As she walked into the room Naomi was surprised to see that the room was full. Not only was her manager there, but all of his management staff were present as well.

Naomi Flax is a manager of a software development team for Seesme Financial a medium-sized financial services company. Fifteen software developers report to her. She, along with the enterprise software testing manager and four other software development team managers, reports to the Phil Johnson, vice-president of the application programming services.

“As many of you have heard through the rumor mill, we need to increase IT security. In addition to the external threats to our IT assets, we need to realize that we are also at risk from threats inside our organization,” said Phil. Jane Doring, another software development team manager asked, “Have we had instances of employees committing fraud or data theft?” “No” said Phil. “Yet, we want to keep that record going. Just as important, we want to help our employees not to unintentionally cause a security breach. We think that with a combination of having a clear security policy, training our staff about the policy, and then enforcing the policy we can greatly reduce the risk and better mitigate the results if a security breach does happen.”

The New Security Policy

A month prior to this meeting Seesme Financial hired a security consulting firm to assist with the creation of a security policy. Phil proceeded to hand out a copy of the policy. Naomi was surprised that the document was as brief as it was. However, she realized that there was a lot more to the policy than noted at first glance.

Among other things, the policy described what was called the segregation of duties and dual control. This check and balance system was used to ensure that no individual would have or appear to have conflicting or unsupervised duties that might jeopardize the security of the data or information systems. It then stated that if segregation of duties and dual control were not possible, compensating controls, such as the review of audit logs by responsible management, must be put in place to alleviate the resulting risks.

In addition to this, “acceptable use” was covered which contains the general responsibilities of all personnel who use corporate information systems and equipment. This section discussed that the transmission of confidential information over any network not wholly owned, controlled, and contained by the corporation by any means, such as email, web, etc., must be encrypted with approved technology. Moreover, e-mail systems that were not controlled by the company, such as Yahoo! or Google, must not be used for corporate purposes. Finally, personnel must not install software without an approval from Desktop and System Support.

Given that Naomi and others in the room managed software development teams and were familiar with computer auditing systems, Phil pointed out the Logging and Monitoring section of the policy. “I know your teams have been good at coding our applications to log critical failures but now we must log and monitor a lot more activity.”

Naomi glanced over the section and noted that each system log must record such program events as all authentication attempts (success and failure), all established sessions (including login and logout), system startup or shutdown, security control violations, unauthorized attempts to access or alter resources, and the disabling or deletion of logging. "Next week the security firm, RUPReady, who helped us develop this security policy will be presenting a workshop for you on the need for the security policy as well as increasing awareness of how your staff may be violating that policy," Phil stated.

Later that day, from the comfort of her patio, Naomi continued to review the policy. She looked specifically for areas that applied to her team. She found especially interesting the portion stating that in certain circumstances the corporation could monitor employees' activities on personally owned equipment used on the corporation's premises while investigating violations of information security policy or other corporate policies. What caught her attention the most was that violations of information security policy could result in disciplinary action up to and including termination of employment. Violations involving illegal activity could be referred to law enforcement and/or reported to other authorities as required by law.

Security Presentation to the Management Team

The following week at the security presentation Naomi took a quick drink of what was left of her coffee as the security consultant, Jill, from RUPReady, got everyone's attention. Jill started the presentation off by asking, "Why do you think that we are conducting security training for management staff first?" After a few seconds of silence, Phil stated, "So we can be informed of the security dangers and pass that information

on to our staff.” “Yes, that is correct” replied Jill. “But what is just as vital is that your group needs to be able to demonstrate to Senior Management, the investors, and your share holders that due diligence as been applied within your daily operations concerning security. Secondly, security risks are becoming critical business issues as they can contribute to incidents such as identity theft, monetary loss, the inability to deliver services, and public loss of confidence in your organization. Finally, if a security violation happens, legal action can be taken against the company.” Jill certainly had everyone’s attention! She went on to share the content of the security policy and the rationale for the items in the policy.

Next Jill discussed the dangers of internal threats by employees. “In the past the greatest threats were from outside your organization. Now hackers are attempting to access your company's sensitive data in other ways. In short, internal weaknesses are the new areas of exposure. Understand, you still need to protect yourself from outside threats with firewalls and other technological defenses, but the newer attack vectors are internal. According to a recent study by Ponemon Institute and PGP more than 88 percent of all breaches in 2008 involved incidents resulting from insider negligence.”¹

USB devices and software brought in by employees and installed on desktop and laptop systems should be among your greatest concerns. Palo Alto Networks published the ‘Application Usage and Risk Report,’ a study of data collected from the monitoring of traffic at enterprises that use its state-of-the-art firewall. Within this study, Palo Alto reported that in 60 IT infrastructures with about 960,000 users most of these enterprises

¹ http://www.pgp.com/insight/newsroom/press_releases/2008_annual_study_cost_of_data_breach.html

have rogue programs traversing the network.² In short, while I know you trust your employees, they either intentionally or not, are your greatest threat.”

By the end of the presentation Phil's team was well aware of the dangers of not only external threats to their business assets but the internal dangers as well. “I would like to offer one more item for your consideration,” Jill stated. “It is Monday morning; you just got settled at your desk when you get a visit from one of the network administrators who informs you that the web-proxy system logs show that one of your employees has been spending an inordinate amount of time surfing retail shopping websites. While this is not a danger to corporate systems, it does mean that they are not following the security policy which allows for ‘occasional inconsequential personal use’ of company equipment. From an evidence-based aspect, what would be the process of confronting that employee and how would you motivate them to change their behavior to be more productive?” “Evidence-based management, I remember reading about that,” piped up one of the managers. “That is when you rely on factual, tested information instead of whatever the prevailing management mythology is for that day.”

Manager to Employee—Function Securely

The next step in the implementation of the security policy was the discussion by Phil's management staff on the planning of how the policy will be disseminated to their employees. “The majority of the initial training will be done corporate wide via web-based instruction. This training will be required to be completed when each employee completes their annual online benefit enrollment,” said Phil.

² <http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201224>

Naomi understood that this web-based content would include a discussion on the risks of using corporation communication channels for unauthorized use, the content of social engineering-based attacks and how users are lured into unintentional information sharing, and how to identify confidential information and understand one's role in keeping it secure. Moreover, staff would be informed that they would, with the assistance of their manager, develop an Employee Security Plan. This plan would take into account their job functions, responsibilities, and day-to-day activities and specify what must be done within these areas to be in compliance with the corporate security policy.

Phil continued on, "In addition to the corporate web-based training, to give the security policy adherence 'teeth,' annual performance reviews will include the employee's fulfillment of their Employee Security Plan. Also, network and firewall logs and computer system event logs analysis concerning each employee will be considered within their annual review."

As she sat at her desk following the meeting Naomi considered the content of the discussion. She understood and appreciated the need for leverage with the employees and making the security policy a direct and necessary part of their everyday jobs. What concerned her at the moment was how she would assist her staff in effectively implementing the security policy. The nature of internal threats requires intensive, ongoing attention to ever-changing potential hazards. In other words, how would she best motivate her staff to closely adhere to the points within their Employee Security Plan?

Employee Motivation

As Naomi was driving home, she still was mulling over the question of how to best motivate her staff to ensure a secure work environment. She remembered an interesting and insightful book from college, *Driven: How Human Nature Shapes Our Choices* by Paul R. Lawrence and Nitin Nohria. Naomi stopped at the local public library. Encouraged that they had a copy of the book on hand, she borrowed it and proceeded home.

Naomi reviewed the book after finishing her dinner. During her skim of the content she noted that the book detailed four basic drives by which all individuals are motivated.³

1. To acquire objects and experiences that improves our status relative to others.
2. To bond with others in mutually beneficial, long-term relationships.
3. To learn about and make sense of ourselves and the world around us.
4. To defend ourselves, our loved ones, our beliefs, and our resources.

She then asked herself, “How could I utilize each of the four drives in motivating her employees?” Naomi opened her laptop and considered the first drive. “How can I help my staff to acquire objects and experiences that improves their status relative to others?” First, Naomi thought, “What are the objects and experiences in the context of my team, which each team member would consider improving their status? Perhaps when someone exhibits diligent compliance to the security policy, making a verbal mention of that to the team? What about special recognition when a staff member alerts the other team members to an attempted e-mail scam?”

³ (P. 10)

Negative Motivation

Naomi then considered what happens if someone violates the security policy? “This could get ugly,” she said out loud. Her neighbor across the yard looked up and then went about her business when she realized that Naomi was talking to herself.

Naomi continued the verbal dialog. “The security policy is written for the protection of not only the organization as an entity but for the company’s employees as well. Also, by the end of their training the staff will be well informed about the policy and will have agreed to follow it. If they choose to disregard it, that is their choice and they will have to accept the ramifications of their decisions.” What was ironic, thought Naomi, was that she was certain that she had heard this often from her parents and teachers while growing up. In any event, the reality of the existence of potential harm to the organization as well as its employees provided a level of unpleasant, but real, motivation to both her and her staff.

Management: Loved, Feared, or Both?

Historically, most management literature emphasizes that good leaders are positive leaders. However, managers such as Naomi realize that this is not always the case. The more she thought about it the more she realized that motivating her staff was not always going to be positive given the need to enforce security policy infractions. Unfortunately, at certain times, leaders must react in ways which may be interpreted as negative.

Naomi recalled reading a book in college entitled *The Prince* by Nicolo Machiavelli. Within that book this question is asked, “Upon this a question arises: whether it is better to be loved than feared or feared than loved? It may be answered

that one should wish to be both, but, because it is difficult to unite them in one person, is much safer to be feared than loved, when, of the two, either must be dispensed with.”⁴

Follow-Up Management Meeting

The next day Phil’s management team discussed how they would incorporate the security policy into their day-to-day management given their diverse teams. Phil looked over at Naomi and said, “I understand that you just inherited two new employees.” Naomi nodded her head in agreement. Hal, their former manager spoke up, “Yes, I would consider them as examples of two opposites. Mike is motivated by a more personable style. You need to engage him in friendly banter and discuss things important to him such as family and hobbies. The other, Julie, is motivated by a more direct manner. While she is a good worker, she is not motivated by friendly banter but seems to thrive on an ‘in your face, here is the task, now get busy’ style of management.”

Phil, with the look of a kid who had just discovered a new toy asked, “Okay, remember the question that the security consultant asked? The web proxy logs show that both Mike and Julie have been spending too much time surfing the web and buying gifts on Amazon. Using an evidence-based approach, how would you confront each employee and also how would you motivate them to change their behavior and be more productive?”

Rob, the senior manager of the team said, “First, I would have a copy of the logs in hand to take with me as I discuss the issue with each employee. With Mike, I see the approach as taking a more conversational aspect from which I lead into the need for

⁴ <http://www.constitution.org/mac/prince.pdf>. p. 79

him to refrain from personal shopping on company time. With Julie, I would affirm her hard work and contribution to the group and then simply present her the logs and ask her to refrain from personal shopping on company time. With both I would end the conversation by encouraging them to continue their good work and thank them for their time and consideration.”

“What do you do if either Mike or Julie becomes defensive and accuses you of harassing them or attempting to ‘micro-manage’ them?” asked Phil. After what seemed like a long silence, Naomi spoke up and said, “I have been thinking about this and there are times when the positive approach will not be effective or appropriate—then what?” “Yea”, said Hal. “What about serious security policy infractions? It’s not ‘lovey, dovey’ then, right?” Jane chimed in, “Yes, good point Hal. What about the Employee Security Plan that we discussed the other day? Phil, you said something along the lines of ‘in order to make the enforcement of the security policy more effective, the annual performance reviews will include how well the employee adhered to their Employee Security Plan and that the analysis of different system logs and how well they adhered to the plan would be considered within their annual review.’ What happens if a staff member is seriously violating security policy? Can we really be positive then?”

Conclusion

Earlier Naomi considered the Machiavellian question, “whether it is better to be loved than feared or feared than loved?” Within this scenario the task of motivating employees to be vigilant against being the intentional or unintentional cause of internal threats is presented. Given that this requires intensive, ongoing attention to potential hazards, the motivation must be persistent and effective. What do you think is more

effective in the long term with staff concerning enforcing security policy— management by relationship or management by fear?