Apathy in IT

Bryan McKinney

Liberty University

Professor Jeffrey Humphries

CSCI 561 - Ethics, Legal Issues, and Policy!

November 17, 2018

Research Objectives

- Describe security apathy
- Discuss how apathy in the workplace can lead to issues in policies and procedures.
- Discuss the advantages and disadvantages of what happens when we in the IT field become to relaxed in our duties.
- Discuss the potential security concerns that can be associated when IT professionals are no longer taking a offensive and defensive approach to security.

What is Security Apathy? There is a hole between a solid security plan and the end users safety while performing day to day operations at work. That hole is security apathy. When users of any IT platform fail to maintain a constant vilegence of their own personal safety online and when interacting with IoT (internet of things) devices they are commiting security apathy. They are no longer taking the “bull by the horns” and protecting one of their greatest assets...their own identity. According to Jacqueline von Ogden she states “Apathetic employees might not actually hand over their login credentials to cybercriminals, but there are a lot less likely to pull from their information security awareness knowledge when it comes to daily behaviors. Apathy is not a simple issue...” (Ogden, 2017). Ogden seems to understand that while most individuals will not knowingly hand over private information they might if they fail to use any of their information security awareness knowledge they learned earlier.

Security apathy shows up in many ways in the professional world as well as our day to day lives. Policies and procedures are meant to be a safeguard against threats and to mitigate the risks associated with using technology on any size scale. When someone becomes apathetic towards the security policies that have been implemented then they are allowing vulnerabilities to be introduced into a network of integrated systems. Apathy in the workplace also causes confusion and lack of trust between those in upper management and those who report to them. When one decides to ignore a policy or procedure and substitute in their own methods then the employee/employer relationship begins to erode. We see this erosion time and time again when working in a professional environment. Upper management will issue a new standard operating procedure then they fail to uphold those new standards wich forever weakens the relationships between themselves and their subordinates.

There are many disadvantage when we as IT professionals become to relaxed in their duties and responsibilities. The security professionals and IT team have been entrusted to keep the infrastructure and systems safe, secure, and accessible to all end users. When IT professionals and security professionals

become apathetic towards their responsibilities the negative repercussions are immense. In the IT world stress is the leading cause of burnout and is attributed with high levels of employee turnover. According to one study they found that “According to ESG research, 51 percent of organizations report having a “problematic shortage” of cybersecurity skills in 2018. This is up from 45 percent in 2017” (Oltsik, 2018). There should be no surprise that there is a serious lack of IT talent today. Many people chose to no go into the IT field because of the high levels of stress.

When IT professionals are no longer taking an offensive approach to managing their networks and mitigating risks then there is a wide gamut of exploits and vulnerabilities that can be taking advantage of. IT and security professionals must be on vigilant with both sides of the spectrum. They need a good offensive plan to deter any attacks and they need to be defensive to be able to respond to any attack that will eneveability happen over their career. Flexibility is key when mitigating the overall stress levels of security professionals. Being able to efficiently handle issues as they arise as well as being able to think though scenarios before they happen keeps the security professional on point which can mitigate the risk of burnout.

Literature Search Results

Security apathy is real and is becoming a bigger issue every day. Scott Boss said “When individuals are not motivated to follow security policies and procedures designed to protect both individuals and organizations, security fails. Thus, organizations face the challenge of how to promote security policies and procedures for individual employees in the most effective way” (Boss, 2009). A lot of individuals become apathetic over time. We see time and time again IT burnout in the workplace and after many years of hard work people just quit. Why are they not willing to put in the hours of study and why is there a lack of motivation for security? John Olstick believes that lack of education is a primary issues. He states “According to research from ESG and the information systems security association (ISSA), 62 percent of cybersecurity professionals believe their organization is not providing an adequate level of training for them to keep up with business and IT risks.” (Olstick, 2018). If security professionals are not keeping their skills up to date and staying on top of the latest trends then that will cause a sense of ignorance which can in turn have a direct correlation to burnout and fatigue.

Apathy in the workplace can lead to many policy and procedure errors. “A tendency to deflect or shift personal responsibility when it comes to security. Almost half (48 percent) of the government employees surveyed think responsibility for securing organizational data and devices falls squarely on IT professionals, senior leadership and colleagues, with only 13 percent putting the

focus on themselves as individuals” (Security, 2016). Most individuals like stated above do not believe that security is their issue to even begin with. That tends to lead to the IT and security teams being overworked and under appreciated. The data suggests that there will be a rise of security concerns and violations when people don't believe it is their responsibility to take their own personal and online security in their own hands. In the human factor of information security: unintentional damage perspective Efthymia Metalidou says “Employees need to be motivated to adopt secure behaviours and practices, and management needs to be able to identify what motivates their staff. Motivation occurs when security issues are shared and users are involved in decision making in order to follow security procedures” (Metalidou, 2014). Metalidou in her studies understands that there needs to be a level of “owning it”. Individuals need to be included in the decisions making process that directly correlates to their day to day lives. She seems to agree that a person's personal responsibility is important to keep apathy at bay. In the book of Galatians we read Galatians 6:9 “And let us not grow weary of doing good, for in due season we will reap, if we do not give up.”(Galatians 6:9, NIV). When Paul was writing this letter to the church in Galatia in this specific example the context is speaking about bearing each others burdens. Earlier Paul says “But let each one test his own work, and then his reason to boast will be in himself alone and not in his neighbor. 5 For each will have to bear his own load.” (Galatians 6:4-5, niv). Even Paul knew at that point in history you have to own your own load...to a certain point. With the Christian worldview in mind we are to be mindful of our brothers and sisters in Christ. It would be unreasonable to think that everyone has to have their best interest in mind when confronted with their online privacy. Some people are better at handling those situations better than their brother or sister. While we need to be individually mindful of that we should also be on the watch for our fellow brothers and sisters in christ.

When we as IT professionals become to relaxed in our duites we open the doors to a whole range of security risks and vulnerabilities that need to be address and mitigated before they get out of hand. Most people believe that.. “More than half of respondents (53 percent) believe that no matter what proactive measures they take, a hacker will find their way in. On the other side of the spectrum, 30 percent think they are more likely to be struck by lightning than have their organizations’ data compromised” (Security, 2016). Thus invokes the idea...why should I take any security measures when my information will be stolen anyways? Another study found that, “...examining the behavior of employees showed that upon receiving email that was designed to look suspicious, 37% would not only open the email, but would actually click on the link provided; while 13% would open the attached file. Additionally, upon receiving an email that was designed to appear legitimate, 42% followed a web link and provided sensitive information, while 30%

run an attached executable file" (Metalidou, 2014). Those last presented numbers are a staggering reality that must be addressed. Almost half of those surveyed opened a web link that most likely tracked personal information about the user and their employer. While almost a third installed a unsolicited executable file that one can only imagine took control over. "Thus it is reasonable to assume that how competent individuals feel in accomplishing tasks with computers should also increase their perceptions that they can take measures to secure their computers and follow policies. Likewise, the apathy literature indicates that individuals may disregard policies and procedures because they are too busy or just do not consider information security to be important. Thus, the lack of motivation will likely reduce the precautions taken by individuals" (Boss, 2009). The human factor is the biggest issue to deal with when talking about security risks and vulnerabilities. We as a collective whole believe we are being vigilant against threats but in reality the numbers do not lie.

There are a slew of disadvantages of an overworked underappreciated IT/security professional. It is easy to see why so many people become disassociated with their work and overtime allow apathy to set in. "When looking at what government employees fear most, only 14 percent report being afraid of someone infiltrating their organization and stealing files, trailing far behind potential scenarios such as a government collapse or food poisoning, and ranking it just three percentage points higher than alien invasion" (Security, 2016). Those people stated above that they fear someone infiltrating their organization and stealing files at a 14% rate. When people do not take the proper time to respect and keep infocus the magnitude of what the results can be from a security breach or data leakage then all that stress is placed on the security team. As we look at some basic statistics we can see that "70 percent of cybersecurity professionals say the cybersecurity skills shortage has had some impact on their organization. Of course, they are living this impact. 63 percent of cybersecurity professionals say the cybersecurity skills shortage has increased the workload on existing staff. More work and stress at the same salary is a surefire recipe for dissatisfied employees and high attrition. 41 percent of cybersecurity professionals say the cybersecurity skills shortage has led to a situation where the infosec staff spends a disproportionate amount of time dealing with high-priority issues and incident response. This means that many cybersecurity pros face a high-stress workplace from the beginning to the end of their workdays. 68 percent of cybersecurity professionals believe that a cybersecurity career can be taxing on the balance between one's personal and professional life. In other words, infosec pros are taking the pressure of their jobs home with them. It's safe to assume that this can leads to issues like substance abuse and others. 38 percent of cybersecurity professionals say the cybersecurity skills shortage has led to high burnout rates

and staff attrition. This affects cybersecurity pros and the organizations they work for." (Olsick, 2018). All the numbers presented by Mr. Olsick come at a staggering rate. More than 1 third and up to 70% of security professionals have felt the stress of working in an environment where security is clearly not a top concern.

Conclusions

With all the data that has been shown I have drawn a deeper understanding of why apathy runs rampant in the professional work environment. Apathy happens when there is an overworking and under appreciation of employees. Apathy happens when employees tried their hardest to make good solid security policies and procedures and then their fellow coworkers ignore or completely disregard those efforts. Apathy happens when upper management sets presidents for a company but then they take the back seat to security and good IT practices which then sets the tone for the company as a whole. In the bible we see an example of this in Revelation. Revelation 3:15-16 says "'I know your works: you are neither cold nor hot. Would that you were either cold or hot! So, because you are lukewarm, and neither hot nor cold, I will spit you out of my mouth" (Revelation 3:15-16, NIV). The Lord here is speaking to the Laodicean church about their attitudes toward God. They were not hot nor cold with their affections towards him. Nearby there was warm water from hot springs that people bathed in. The warm water served a purse...to keep the people clean. As well, cold water is a pleasure to drink, but the Laodicean had lukewarm water coming from an aqueduct nearby. God knew that water served no purpose. IT was not refreshing nor did it clean the individuals. God saw the Laodicean church as apathetic towards him in their affections. The were not on fire for him nor were they cold and passive. They were neither, which in many commentaries on the text they saw themselves as a people group that did not depend on God. Today in the security field we can relate the intentions of those around us as lazy and not caring as lukewarm water...it serves no purpose. IT would be best for everyone to be on fire for the best security practices and really take to heart what is being asked but that is not the case. Many people chose to forge their own path even against what has clearly been shown to be a narrow way of thinking. Apathy has no place in the lives of security professionals and it only servers as a hindrance to those around us.

Bibliography

Boss, Scott & Kirsch, Laurie & Angermeier, Ingo & Shingler, Raymond & Boss, Wayne (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security Retrieved from http://130.18.86.27/faculty/warkentin/BIS9613papers/EJIS_SpecialIssue/Bossetal2009_EJIS_18_2_security_policy_compliance.pdf

Metalidou, Efthymia & Marinagi, Catherine & Trivellas, Panagiotis & Eberhagen, Niclas & Skourlas, Christos & Giannakopoulos, Georgios (2014) The Human Factor of Information Security: Unintentional Damage Perspective Retrieved from https://ac.els-cdn.com/S1877042814040440/1-s2.0-S1877042814040440-main.pdf?_tid=016f499e-1180-49ff-aa6e-7a9972c47c73&acdnat=1542475016_6178347fe0eb410d3b6179db9dd4ac85

Ogden, Jacqueline von (24, January 2017). Employee Apathy is STILL One of thTop Cyber Security Threats in 2017 Retrieved from https://www.cimcor.com/blog/employee-apathy-is-still-one-of-the-top-cyber-security-threats-in-2017

Oltsik, John (6, Febuary 2018) CyberSecutiy Job fatigue affects many security prfoessionals Retrieved from https://www.csoonline.com/article/3253627/leadership-management/cybersecurity-job-fatigue-affects-many-security-professionals.html

Security (7, March 2018) Employee Apathy and Overconfidence Threatens Security of Public Sector Organizations Retrieved from https://www.securitymagazine.com/articles/88793-employee-apathy-and-overconfidence-threatens-security-of-public-sector-organizations