SECURITY VS. COMPLIANCE

Rob Hornbuckle

ICTN 6870

THE INFALLIBLE TRAP AND WHAT'S AT STAKE?

Within the industry of IT security there has been a constant struggle between security and compliance. Central to this struggle are C-level executives who fall short of completely understanding the information security risks their organizations face, nor do they understand the risk tolerance they should accept, with regard to the data housed. Consider also that IT security is pervasive in every other business unit within a company: human resources, finance, information technology, and operations. Due to the nature of risk tolerance levels being wholly dependent on an understanding of information security, more often than not, the executives in question tend to turn to a checkbox-type solution or a compliance-based solution because it's so easy to manage. However, this type of thinking can lead to a false sense of security, specifically a false sense of information security. Compliance is not the same thing as security. Compliance is the armed guard at your gate. Security is the retired marine who is well versed in tactics, has knowledge of current vulnerabilities, and has a pretty good idea where the next attack is coming from.

To help reinforce the differences between the two, compare the Merriam-Webster definitions for both.

"Compliance : (1a) the act or process of complying to a desire, demand, proposal, or regimen or to coercion. (1b) conformity in fulfilling official requirements. (2) a disposition to yield to others

Security: (1) the quality or state of being secure. (4a) something that secures : protection. (4b1) measures taken to guard against espionage or sabotage, crime, attack, or escape. (4b2) an organization or department whose task is security."

As illustrated by the definitions above, it is easy to see that compliance and security are different. A good point to reinforce in regards to the definition of compliance is that compliance is a 'disposition to yield to others'. This equates meeting a requirement, technical or otherwise, set forth by someone else and verified on occasion. To illustrate the difference further, consider a company performing a compliance check for a data storage area where one requirement is for there to be a lock on the door that leads into the building where data is physically located. Indeed, this is a very straightforward requirement and could constitute a box to check to have it completed; equally as easy for an auditor to verify compliance. However, a fancy new lock on the door to the building doesn't mean infrastructure and information is secure, after all, consider who may have access to the key. One could distribute keys at random on the street to such a lock and still appear to be compliant. As with most requirements, compliance is often developed by someone from a different organization with the best of intentions, however it was not developed with a company's unique network, requirements, and needs being taken into consideration.

To develop a complete view of a specific company, consider the difference in compliance versus security when analyzing the four major branches of an organization: human resources, finance, information technology, and operations as it relates to industry. Also, consider the implications of relying on compliance to satisfy security needs. Do so, and escape the infallible trap (ignorance) and save the most important commodity in your business (your reputation).

FINANCE

Assume that the finance unit of a business is involved in activities that revolve around money, both incoming and outgoing. With regards to money incoming, the most common payment accepted by most business is in the form of a payment card, such as VISA or MasterCard. These payment cards are governed by PCI standards (payment card industry). A good analogy to use to depict the dichotomy of compliance versus security is the analogy of the biker and safety. Consider that there is a biker who just got a new bike to ride for the first time, the biker representing the executives of the company, the bike representing the company itself, and the regulations representing the PCI standards. The biker goes to his security professional and asks, what do I need to do to be safe and secure when I ride this bike? In response, the security professional tells him that he needs to start with a good pair of steel toed and shanked boots, then he needs to get a good pair of pants, reinforced with ribs to protect his legs when he rides. After this he would need to get a pair of chaps to go overtop to protect him from smaller scraps. Next, we get a thick and reinforced jacket to protect your arms and torso from an impact that may happen. Finally, we get a full-face mask helmet to protect your head and your good to go after 2-3 weeks of riding classes to increase your skill level and reduce your risk of accidents. At this point to rider asks, this getup is pretty bulky, making it harder for me to move. It also is very expensive for what I was thinking and I'll need to wait a long time to really get to riding. Are you sure this is what is required? At this point the security professional responds with: this is the best way to stay safe and secure while riding, however the regulations only require you to wear a helmet. The rider at this point looses all the recommendations besides the full-face helmet. The security professional then mentions that the helmet is also not required to be a full-face helmet. The rider then dons a skullcap helmet and rides down the road, completely in compliance with regards to the regulations but far from secure.

It would be natural to ask oneself why compliance standards, like PCI standards, exist to begin with. A compliance standard exists to create an equal footing for one company to tell if another company has at least a minimum level of security in order to feel comfortable doing business. In this regard, they fulfill their purpose, albeit minimally. To truly have a secure company, compliance is baseline on which to build. It points at the direction of good judgment, which is noble, but doesn't replace judgment itself. Compounding the problem is the assumption that achieving compliance is achieving a sufficient level of security. Compliance offers hope of security without any real founding behind that feeling. That false sense of security is a liability in and of itself that a malicious entity might be so inclined to exploit. For a security solution to truly fit, it must be tailored to that specific company. If compliance standards, like PCI

standards, worked sufficiently, events such as the most recent Target store breach wouldn't happen or at least wouldn't happen as frequently.

HUMAN RESOURCES

Human resources can prove to be one of the largest vulnerabilities a company faces. Generally speaking, compliance lightly broaches the realm of human resources. The majority of the time, the compliance industry will refer to standards for confidential information of which certain HR data falls. This is where things can begin to get shifty. In a compliance-based scenario, a company would need to demonstrate that it sufficiently protected confidential information. Consider the following scenario of a company instituting a policy where it is stated that employees are not allowed to store any personal information on their work machines. This allows a company to circumvent the certification requirement of their responsibility to protect an employee's personal information. In essence, this shifts liability to employee. This type of policy would typically be covered under an acceptable use policy. This is a dangerous game because once the employee is exited, the protection granted by the acceptable use policy is no longer in force as the employee is no longer in control of the data. This shifts the liability back onto the company, who could unknowingly be storing confidential data that has the potential to be exploited. Consider other potential pitfalls such as whether or not the acceptable use policy is even enforceable as it could be construed that it was signed under duress because it was a condition of employment. Could it be argued that the employee didn't know what they were signing? Is the agreement enforceable or would it be deemed egregious by court precedent? Security is meant to address these questions.

The plot thickens depending on the industry. In intellectual property dependent industries, hiring practices can be called into question. Is the employee a company is about to hire going to reveal trade secrets? If a company is particularly profitable, is HR employee data sufficiently protected to prevent spoofing an employee to help desk in order to access industry sensitive data? Suppose the company is ridiculously profitable and the employees are handsomely compensated as a result. Should HR increase protection on employee data to prevent identity theft of their employees? Success can definitely contribute to being the target of attacks. The security industry knows this, can compliance possibly keep pace?

INFORMATION TECHNOLOGY

Technology has become pervasive in the way employees work. There are few job functions left where a computer of some sort isn't utilized in some way. As such, compliance has a major impact on functionality within this business unit. From a compliance standpoint, an auditor would insure than information technology employees are following the same rules as every other department. Issue being, that information technology is unique. Compliance does not address the issue of any internal threat. Consider the case of Mr. Snowden. Most folks

aren't strangers to the fact the Mr. Snowden was a SharePoint administrator who copied confidential files that were beyond the scope of his job even though he had access to these files due to his job function. No compliance program would have protected against this threat. This is the job of a competent security professional.

OPERATIONS

When security is considered in addition to compliance, its helpful to determine security needs by reflecting on the type of industry at hand. Most industry can be categorized into product based, whether intellectual property dependent or market share dependent, service based, whether corporate service based or consumer service based, and a commodity or retail based industry, whether the large amount of the companies in this sector would be consumer based or the smaller amount of companies who cater to corporations. Intellectual property dependent organizations may need to rely more heavily on shoring up their human resource practices to protect against internal threats. Whereas consumer service based organizations may need to beef up their payment card industry standards beyond regulation.

From an operation standpoint, the best thing to be done is to view compliance and security as two different activities. Realize that these two activities can and do overlap. In fact, a very well run and well-developed security program should already meet most if not all the compliance checks needed. The goal of compliance is to earn a certification or meet the requirements imposed by an external entity that may or may not be effective security for the unique environment of the company. Note this also when dealing with other companies that just because the company is compliant to the same standard that doesn't automatically mean the company is as secure. It's appropriate to focus on the inherent weakness in compliance in so far as that once a company has a certification, they are audited on a subsection of the overall certification on a regular basis in order to maintain the certification. This is subject to exploitation. Imagine the scenario where the company knows exactly what the scope of the audit is and can prepare for it while the rest of their structure is in shambles. For these reasons remember compliance is something companies do because they must and generally put in as much effort as required to get by.

Related to operations as a whole is awareness training. Awareness training is known to have a positive effect on overall security of a company. It's unrealistic to expect employees to help mitigate risk without arming them with the information to be able to protect themselves and their company. In order to maximize effectiveness, it needs to be monitored, enforced, and refreshed on a regular basis. Compliance doesn't regulate employee education but this type of education is a low cost way to dramatically improve security.

Usage audits are another useful tool that compliance doesn't dictate but that can have a dramatic effect on security. A usage audit is an audit of an employee's use of what they have access to. This will look at the frequency of access to the resources you are granted access too.

This can detect the first signs of abuse of an access privilege. For example, consider a developer who outsourced his job to China. He would come into the office everyday and initiate a VPN connection to a location in China and briefly review the code that was sent back to him. He was discovered during a usage audit due to the amount of bandwidth he was consuming throughout the day.

With security, the information security department should consider the complete confidentiality, integrity, and availability of all their companies computing resources and data as their main concern. To this effect, a risk-based approach should be used. Risk, budget, and degree of acceptable risk for the company should be taken into consideration to insure an effective and efficient security program for the company's unique environment.

AUTOMATION, METRICS, AND ACCOUNTABILITY

With the difference between compliance and security defined, the IT security implications concerning the confusion of the two can be addressed. It is reasonable to conclude that reliance on compliance can hamper the goals of IT security. For instance, the information security industry is realizing significant gains through automating security, both for ease and effectiveness of use, but can hit roadblocks when seeking implementation due to automation not currently being a part of any compliance program. Executives must balance their perception through compliance and their reputation through security.

Automation is an increasingly useful tool that is often overlook or considered to be unnecessary within even the elite in IT security. In early 2014, Target had a major PCI security breech. As it would happen, there were automated systems in place that could have prevented the breech had they been turned on. The specific tool Target had fully implemented and operational was a program called FireEye. When questioned afterwards, the CISO of Target made the comment to the effect of not turning the feature on because of the belief that human eyes should be laid on everything before action is taken. He subsequently resigned. If FireEye would have been configured to automatically respond, it would have shut down the one terminal that had been infected instead of the infection spreading to other terminals. Compliance would never dictate that automation be used in the case of Target, however, given the circumstance of Target, it would have been the wisest course of action.

There is also the issue of grading the security performance simply on compliance scores thus undermining many attempts to be more secure. The hope is that, in the future, tools that can monitor, report, and respond to incidents while reporting metrics may overcome this obstacle. The fear is that management that may not know any better will use automation tools for compliance and not properly automate risk management.

There is also the issue of executives justifying sufficiency through compliance. For instance, an executive could shift blame for an issue by falling back on the fact that the company was compliant with regulation. Compliance is much easier to measure; it is also easier to defend.

If you have a ‘compliant’ IT department and something happens, compliance and the associated paperwork is as good a defense as any, even as high as when reporting to Congress. If a company has a security based mentality and something happens, it is not as easy to defend, even if the security based company has a much stronger security program in place but simply missed something. It’s a situation where compliance defends against the notion of the company being negligent. This dynamic has lead many CISOs to choose a compliance mentality even though it may not be in the long term best interest of the company. This has also lead to a ‘fear the auditor’ mentality and fosters several unsavory methods for ‘dealing’ with audits. This is a distraction from true security but a direction that the industry seems to be going unfortunately.

THE BIG PICTURE

Gartner, an organization known for predicting IT growth in the market place, has weighed in on the issue stating that the IT trend is to focus on a risk based approach to security and that this will resolve the compliance vs. security issues. John A. Wheeler, a research director from Gartner, made the statement that ‘by simply trying to keep up with individual compliance requirements, organizations become rule followers, rather then risk leaders. CIOs must stop being rule follower who allow compliance to dominate business decision making and become risk leaders who proactively address the most severe threats to their enterprises.’ This is accomplished according to Gartner’s plan by absorbing the compliance requirements into the risk management office and out of the realm of security. This frees up security to operate as it was originally intended, a security department. Ideally, the risk-management office takes up the legal/regulatory requirements needed for compliance and approaches them independently with a check-box mentality. This creates an environment where compliance doesn’t go away entirely but allows the discussion to be based around risk, risk acceptance, and whether or not compliance holds any value thereby freeing up security to customize real security solutions for their specific environments based on their network, infrastructure, and business needs.

Does compliance hold any real value? While compliance doesn’t hold any real value from a security perspective, it is useful for companies to have a basis to start trusting one another. It’s also provides a baseline for what an organization should be doing in the way of due diligence but, it shouldn’t be confused with best practice, which is having a dedicated team of security professionals protecting the reputation and security of the organization itself.

References

Calonicoto, Scott. "Security vs. compliance: An MSP Guide." MSP. N.p., 21 11 2013. Web. 13 Apr 2014. <http://mspbusinessmanagement.com/blog/security-vs-compliance-msp-guide>.

Casaretto, John. "Security Compliance does not equal Security." wikibon. N.p., 09 Jul 2011. Web. 13 Apr 2014. <http://wikibon.org/blog/author/jcasaretto/>.

Chapple, Mike. "Security vs. compliance: Moving beyond a 'checkbox securit'y mentality." Search Security. N.p., n.d. Web. 13 Apr 2014. <http://searchsecurity.techtarget.com/answer/Security-vs-compliance-Moving-beyond-a-checkbox-security-mentality>.

"Compliance." Merriam Webster. N.p.. Web. 13 Apr 2014. <http://www.merriam-webster.com/dictionary/compliance>.

"Gartner Says Risk-Based Approach will Solve the Compliance vs Security Issue." Infosecurity. N.p., 08 Aug 2013. Web. 13 Apr 2014. <http://www.infosecurity-magazine.com/view/33908/gartner-says-riskbased-approach-will-solve-the-compliance-vs-security-issue/>.

Jackson, William. "Is an emphasis on compliance hampering IT security?." FCW. N.p., 10 May 2013. Web. 13 Apr 2014. <http://fcw.com/articles/2013/05/10/cybereye-auditor-security.asp&xgt;.

* Ninghui, Li. "Beyond proof-of-compliance: security analysis in trust management." ACM Digital Library. ACM, n.d. Web. 13 Apr 2014. <http://dl.acm.org/citation.cfm?id=1066103>.

"Security vs. Compliance." common denial. N.p., 29 Jul 2013. Web. 13 Apr 2014. <http://commondenial.com/2013/07/29/security-vs-compliance/>.

"Security vs. Compliance." Secure Connect. N.p.. Web. 13 Apr 2014. <http://www.secureconnect.com/pci-compliance/security-vs-compliance.html>.

"Security." Merriam Webster. N.p.. Web. 13 Apr 2014. <http://www.merriam-webster.com/dictionary/security?show=0&t=1397239936>.

* Siponen, Mikko. " Factors Influencing Protection Motivation and IS Security Policy Compliance." Innovations in Information Technology. N.p., n.d. Web. 13 Apr 2014. <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4085422&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4085422>.

Valladares, Cindy. "EXPLAINING INFORMATION SECURITY, RISK AND COMPLIANCE TO YOUR MOM." The state of security. N.p., 17 Feb 2012. Web. 13 Apr 2014. <http://www.tripwire.com/state-of-security/security-data-protection/explaining-information-security-risk-and-compliance-to-your-mom/>.

* Wallace, Linda. "Information Security and Sarbanes-Oxley Compliance: An Exploratory Study." AAA. AAA, n.d. Web. 13 Apr 2014. <http://www.aaajournals.org/doi/abs/10.2308/jis.2011.25.1.185>.