Security vs Compliance

Your company has an upcoming compliance audit and your security staff is working overtime preparing; every control is put in place and each system is set to the exact specifications of the compliance audit. The day arrives and your company passes with flying colors, receiving a passing grade from the compliance body. There's a collective sigh of relief as the company's day to day business lives to see another day and the proverbial bullet is dodged.

While compliance is important for a company to maintain contracts, the ability to use certain services, and avoid losing your shirt in lawsuits, compliance is not the end all be all of securing a company. Sadly, many companies take this stance – "we are compliant therefore we are secure." Putting compliance above security or even on par with security can be just as damning to a business as not having compliance at all. Whether a company is compliant or not, data breaches can still incur fines from the governing compliance body.

Perhaps the most important step to understanding that security and compliance are not one and the same is to define how each is used.

> *Putting compliance above security or even on par with security can be just as damning to a business as not having compliance at all.*

The strength of your information security program is often determined by your organization's ability to protect against, and respond to, the ever-changing threat landscape; it is important to note that the best security programs are proactive to get ahead of these threats. Whereas compliance is based on a set of controlled standards set in place by a governing body, which is commonly reactive. The endgame is the same but the paths differ.

> *Security is never finished and should be at the very least, always maintained and improved upon.*

Security is never finished and should be at the very least, always maintained and improved upon. Compliance is driven by the needs of the business rather than the technical needs and is achieved when the governing body is satisfied and issues a passing grade.

Again, it is important to reiterate that just because the compliance audit identified gaps within the security landscape of a company, that does not mean the company can check the box and say, "We found this gap, we closed it, we are now secure."

Take for instance, the Payment Card Industry Data Security Standard (PCI DSS) 12.6 that says, "§12.6 – Make all employees aware of the importance of cardholder information security. Educate employees (for example, through posters, letters, memos, meetings, and promotions). Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures." (a)

This requirement means making sure employees are aware of how to protect customer cardholder information. This, as seen above, can simply be achieved through posters or a security "test" where typically users just click through and

answer the questions at the end. Simply put, all that is required to check the box on the PCI DSS compliance audit for this measure is a security awareness program.

To be secure, however, there is much more that should and needs to be done. While compliance would be simply setting up an awareness program, security would create phishing campaigns to educate users using tools such as Knowbe4, and implementing antiphishing services such as Proofpoint. While the security awareness program might offer employees a "passing glance," actively monitoring and training these employees creates a more secure environment for the company's assets.

> *"The strength of your information security program is often determined by your organization's ability to protect against, and respond to, the ever-changing threat landscape;"*

This is not to say that a company should choose security over compliance, in fact, the two should go hand in hand and compliment the other. Compliance should be used to help establish a baseline to build on the practices of the companies security policies, and compliance is often not needed to ensure the business can keep operating. For instance, taking credit and debit card payments, as with PCI compliance. While security is there to take those baselines and cover them from every foreseeable, and even unforeseeable aspect, such as ensuring that the correct security controls are in place.

If a company is forced to check a box of either a. being compliant, or b. being secure, the company needs to write in its own checkbox or c. being compliant and secure, the biggest question we get here is: "where is the money going to come from?" This is a question that security leaders are all too familiar with...

Resellers, such as SecureNation, can help play a major role in a company's security posture. Having a team to help carefully and critically examine these next-gen security appliances, software, and services, as well as negotiating the lowest price on your behalf, will leave more time and money in the budget to work on both compliance and security.