IT COMPLIANCE VS IT SECURITY: WHAT'S THE DIFFERENCE?

For some IT professionals, the line between security and compliance becomes easily blurred and may seem like a moving target. How do we create comprehensive security programs while meeting compliance obligations? Is checking the compliance box really enough? And how does all this enable the business to function and move forward? These are questions that can shape the direction of an organization and ultimately cause it to succeed or fail.

IT Security Explained

Information Security (IS) is the practice of exercising due diligence and due care to protect the confidentiality, integrity, and availability of critical business assets. An effective IS program takes a holistic view of an organization's security needs, and implements the proper physical, technical, and administrative controls to meet those objectives.

Security officers follow industry best practices to ward off attackers who would seek to harm the business, or to mitigate the amount of damage that is done when an attack is successful. In the past, administrators would take a purely technical approach and rely heavily on systems and tools to protect their network: Devices like firewalls and content filters, along with concepts like network segmentation and restricted access, were the security professional's bread and butter. While these safeguards are still necessary today, modern threat agents employ much more sophisticated strategies which easily overcome old-school technical controls. Threats like social engineering, remote code execution, and vendor-created backdoors require the security professional to be much

more diligent and proactive in their approach.

The concept of "IT Security" come down to employing certain measures to have the best possible protection for an organization's assets.

IT Compliance: Following Rules and Meeting Standards

While compliance is similar to security in that it drives a business to practice due diligence in the protection of its digital assets, the motive behind compliance is different: It is centered around the requirements of a third party, such as a government, security framework, or client's contractual terms.

Compliance is often viewed as the figurative stick which motivates the donkey, rather than the carrot. If an organization wants to do business in a country with strict privacy laws, or in a heavily-regulated market like healthcare or finance, or with a client that has high confidentiality standards, they must play by the rules and bring their security up to the required level. For example, regulations like HIPAA and SOX, or standards like PCI-DSS or ISO:27001, outline very specific security criteria that a business must meet to be deemed compliant. A high-profile client may require the business to implement very strict security controls, even beyond what might be considered reasonably necessary, in order to award their contract. These objectives are critical to success because a lack of compliance will result in a loss of customer trust, if not make it outright illegal to conduct business in the market.

In short, IT Compliance is the process of meeting a third party's requirements for digital security with the aim of enabling business operations in a particular market or with a particular customer.

What Are the Differences? And Why are Both Necessary?

To restate from above, security is the practice of implementing effective technical controls to protect digital assets, and compliance is the application of that practice to meet a third party's regulatory or contractual requirements. Here is a brief rundown of the key differences between these two concepts:

Security:

- Is practiced for its own sake, not to satisfy a third party's needs
- Is driven by the need to protect against constant threats to an organization's assets
- Is never truly finished and should be continuously maintained and improved

Compliance:

- Is practiced to satisfy external requirements and facilitate business operations
- Is driven by business needs rather than technical needs
- Is "done" when the third party is satisfied

At first glance, one can easily see that a strictly compliance-based approach to Information Security falls short of the mark. This attitude focuses on doing only the minimum required in order to satisfy requirements, and nothing more.

This fact reinforces the need for an effective Information Security program, which will enable a business to go beyond checking boxes and start employing truly robust practices to protect its most

critical assets. This is where concepts like defense-in-depth, layered security systems, and user awareness training come in, along with regular tests by external parties to ensure that these controls are actually working. If a business were focused solely on meeting compliance standards that don't require these critical functions, they would be leaving the door wide open to attackers who prey on low-hanging fruit.

While compliance can be negatively perceived as only doing the bare minimum, these efforts do still have a useful purpose, and can actually be an asset to the business instead of just hoops that must be jumped through. Becoming compliant with a respected industry standard like ISO:27001, for example, can bolster an organization's reputation and gain them new business with security-minded customers. It will also help to identify any gaps in the existing IS program which might not have otherwise been identified outside of a compliance audit. Additionally, compliance helps organizations to have a standardized security program, as opposed to one where controls may be chosen at the whim of the administrator.

The astute security professional will see, then, that security and compliance go hand in hand, and complement each other in areas where one may fall short. Compliance establishes a comprehensive baseline for an organization's security posture, and diligent security practices build on that baseline to ensure that the business is covered from every angle. With an equal focus on both of these concepts, a business will be empowered to not only meet the standards for its market, but also demonstrate that it goes above and beyond in its commitment to digital security.

Additional Resources

How Will Your Cloud Strategy Impact Your Cyber Strategy? from **BMC Software**