Unification: Sooner or Later

Jim Tiller

For the better part of my career I’ve traveled the world speaking to companies about security; their challenges, strengths, and weaknesses, the regulatory landscape, and technical infrastructures. Ultimately, while the languages may differ as much as the landscape, the security troubles and goals are extraordinarily similar, seemingly unaffected by the diversity in industry and law. But, given the complexity of security, the art of application is best described as interpretation. One’s experience and attitude can translate into security programs that have the power to move mountains, while others continue to struggle.

In the 1980s, information security was little more than locking the door to your office. In the 1990s the advent of the Internet and firewalls, closely followed by Intrusion Detection Systems (IDS), raised awareness of the need for security surrounding data. During this time security savvy folks would interact, share, and work as a group to drive the meaning of security through best practices. Soon, the evolution of standards took shape, drawing from the best practices and the community at large, forever setting in motion a trend we continue to this day. Regulations affecting infosec began to make their debut shortly thereafter, leveraging the general consensus found in the standards. Finally, there was the facility for governing bodies to make demands in information security by referencing the standards.

Based on the inherent relationships between best practices, standards and regulations, we can begin to draw determinations of the future based on the past. For example, the insurance industry in the U.S. in the early nineteenth century was overcome with fire ravaging production facilities during the industrial revolution. Open flame sources of light, poor construction practices, and the use of flammable materials in buildings facilitated the destruction of property. However, without a standardized and regulated approach to construction concerning fire management, there were few methods available to insurance companies for measuring risk to people and assets. The insurance industry began to create standards and promote them throughout the industry. As they were adopted and refined by builders and manufacturers, these standards were eventually adopted by the government as laws and regulations affecting construction. We see the results even today in design, construction, materials, and protective systems.

It took years for the different standards to become fully adopted and converge, establishing a common approach that would promote consistency and in turn help the industry to apply common metrics to risk and, frankly, save lives. As this occurred more regularly, building enough historical and empirical data, governing bodies were able to confidently implement regulatory controls.
Security is in the embryonic stage of reevaluating multiple approaches and seeking to simplify the regulatory landscape. Unfortunately, the reality is regulations have sprouted into an environment that has not enjoyed the time it takes for the industry to ratify a small group of meaningful approaches — but this is beginning to happen. We are moving out of “regulatory-shock” into a state of mind where we’re now seeing similarities in compliance efforts.

Granted, the goal of regulations was, in many cases, to promote security, increase privacy, and motivate sound security practices in a highly connected economy. However, as practitioners it is up to us to cross this chasm and translate the demands of the regulations into meaningful solutions leveraging a multitude of standards without crippling the business — financially or operationally. Therefore, we are in a significant growth period in the world of security. We are effectively compressing the time that would have normally existed for other characteristics of society to drive consistency and unification to compensate for the advancement of infosec weaknesses.

Of course, the endeavor to be compliant across multiple domains and regulations is challenging. Fraught with dynamics in industry, technology, investment strategies, and business life cycles, today’s CISO must overcome many hurdles to reach this seemingly unreachable Nirvana. However, while these challenges appear as hurdles today, they are in fact enablers of the long-term process — stepping stones to greater, more flexible security, driving business through opportunity versus the general perception of security as an expensive disabler of business. Soon the similarities in regulations, interpretation, and approaches will increase, driving consensus and simplifying today’s challenges and preparing for tomorrow’s. Finally, as we promote consistency in approach, while maintaining open dialogue in new philosophies, security will become a significant core attribute of business.

It is generally within this context I hope to offer value to our subscribers. As the new editor of Information Systems Security, the objective is to seek out and provide insights to directions in the security industry. Together, we will learn about new technologies, security management philosophies, and emerging best practices, while continually reinforcing the foundations of security within the framework to advocate growth and expansion of what it means to practice security in the twenty-first century.

In this issue, we begin to exercise the new direction of the journal, starting with regulations. Chris Brown discusses the virtues of consistent practices to ensure compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA). By the establishment of a thoughtful approach, meeting the requirements of HIPAA will be less chaotic and promote value to the business overall.

Continuing with the promotion of open dialogue in an effort to instill a broader collaboration, Edwin Covert and Fran Nielsen introduce a new approach to measuring risk. As we begin to peel back the tactics of today’s risk analysis frameworks, many begin to challenge the validity of the process and the results. However, there is value and discussing these in a different light will ensure liveliness in the art of risk analysis.

From a technical perspective, there are many solutions that are quickly being adopted by the traditional enterprise. Once for only personal use and independent in nature, instant messaging has proven to offer value to organizations all over the world, promoting greater communications and employee effectiveness. However, this has introduced some concern regarding security and exposure. Joon S. Park and Tito Sierra highlight these risks and potential solutions.

We hear a great deal about being proactive in the security industry. Simply stated, it’s not always easy to do. Convincing management to spend money, developing processes, validating technology, and maintaining vigilance are all basic challenges. Nevertheless, we know it’s a must
for organizations to survive. Tim Keanini speaks to proactive security and the inherent relationship it has with reactive controls to offer insights to an area of security some have difficulty in making a reality.

Personally, I’ve very excited about the future of security and the role this journal will play in that evolution. While we may have come a long way, we’re just getting started.