Monetization of Security Theory

By Josh Ladeau, CISSP

The Monetization of Security Theory states that we are entering an era when privacy and network security investments can begin to drive “tangible” returns. To date, Return on Investment (ROI) around initiatives/investments related to internal network security control would typically be represented by the value of diminished risk — for example, the dollar reduction in an organization’s Annual Loss Expectancy (ALE) projections. However, we are now on the precipice of being able to measure security-related investment returns based on their potential impact to *revenue*. Let us examine some of the underlying factors driving us toward monetizing security investments.

Sound privacy and network security posture is difficult to achieve. There are myriad impediments, including the misconception that information technology departments have primary responsibility for addressing the issue, a woeful shortage of competent security professionals, and perhaps most significant, poor conceptual understanding of key issues at senior levels of management. As is almost universally true, the more difficult something is to achieve, the more value there is in achieving it. In other words, security posture has the potential to be a long-term, material differentiator for

businesses that embrace the idea.

The interdependency of the technological ecosystem in which virtually all companies now operate — coupled with the concept that privacy and network security is a “weakest link proposition” — means that companies need to focus not only on their internal controls but also on the relative security posture of their business partners. Relatedly, it is widely accepted that while virtually any component of an operation can be outsourced, liability associated with privacy and network security cannot be. It follows that businesses will place more focus on the security posture of their vendor partners in an effort to holistically insulate themselves from security incidents/breaches and the resulting liability.

Beyond liability, the potential for first-party exposure also exists. Businesses are often reliant on external suppliers and distributors in conducting their operations. A disruption on either end of the supply chain can result in the loss of income, loss of market share, and diminished reputation in the eyes of prospective clients.

The above considerations will force companies to trend toward operating within a network of relatively secure vendor/supplier/distribution partners to whatever extent possible. And they will pay a premium — relative to working with less secure, but otherwise equivalent, vendors/etc. — for the privilege, as it is critical to the long-term viability of their

organization. Over time, companies that are able to demonstrate a heightened security posture relative to their competitors will be the beneficiary of these enhanced revenue opportunities. (This is already happening in many areas — we are commonly seeing clients scrutinize the security posture of cloud providers and select more secure providers at a higher cost, for instance.)

Achieving BLIS (**B**usiness **L**ed **I**nformation **S**ecurity)

For the vast majority of companies today, organizational responsibility for privacy and network security resides with the Information Technology group, whether there is a formal Chief Information Security Officer (CISO) position in place, reporting to the Chief Information Officer (CIO), or simply a dual hat worn by the CIO/CISO (generally not viewed as a best practice). In rare instances, an organization's CISO will report directly to the Board, CEO, CFO, Audit Committee or GC. This is an improvement over the more common practice of CISOs reporting to the CIO (or the dual hat approach) because it provides the checks and balances necessary for an effective security organization. For the same reason, auditing departments typically report outside of the business units; meaningful separation of duties provides greater assurance of compliance. That said, even in most instances of this preferred reporting structure, IT is still viewed as having primary responsibility for the security of data. I believe a more effective approach is to shift primary responsibility to the

business/production units.

This is because the needs of the business (vs. operational and support sides) generally drive organizational direction and behavior, as revenue generation is the lifeblood of any for-profit enterprise. Conversely, IT units do not generally drive organizational decisions, are viewed as a cost center, and have limited (if any) authority over the business units they support. Driving behavioral changes through the more influential business/production elements of a company increases the likelihood of shifting organizational culture as relates to privacy and network security.

While the concept sounds daunting, let us explore what this might look like in practice. Before we jump in, it is important to note that the goal is not to turn production units into security administration units; that is not practical since those production employees obviously need their primary focus to remain on generating revenue. Achieving BLIS does, however, require a paradigm shift in the way that revenue-generating units view their relationship to data, and the protection thereof.

Where to Begin?

The first and most critical aspect is to establish the concept of Data Ownership within the business units. Production employees need to understand that the data they collect or generate related to selling a product or rendering a service is *their* data, and they are therefore ultimately responsible for the

protection of that data in line with company policy, industry regulations, contractual requirements, and/or law. Everything else flows from that very basic tenet.

As postulated in the first section, organizational investments in security have the potential to be monetized by essentially becoming a built-in component of core products/services. In order to realize that potential, however, business units must have a conceptual understanding of the manner in which data is transmitted, processed, and stored by their organization, including the elements of security associated with each. This will require proactive training, and likely more significant interaction between the production units and IT as well as Legal, Compliance, and other key stakeholders in a comprehensive security organization.

The BLIS model for organizational management of privacy and network security exposures leverages the influential nature of the business relative to other units of the company. Once production employees begin to gain an understanding of the way data flows through their organization, as well as the controls in place relating to that data, they can begin to drive organizational change. The topic is far too broad to cover granular aspects of this process holistically, but for the purpose of illustration, we can focus on one control area that organizations generally contemplate in an effort to protect data: Access Control.

Access Control, broadly, addresses the level of access individuals have to data and what they can do with that data once accessed. IT units regularly manage access control through various tools (such as Active Directory), a custodial and appropriate function for the IT or IT security unit. However, the “rule sets” for access to data should be tightly controlled by the Data Owner, which again, in a best practices environment, would be a profit center/production unit lead(s).

Below is a hypothetical comparison of two similar organizations (25-attorney law firms), one employing the most common model for managing privacy and network security exposure, and another using the BLIS model.

Limiting the analysis to access control only, the first organization has the following in place: IT is responsible for all aspects of privacy and network security management organizationally. Active Directory is the primary tool they use to control access to network storage (drives). All attorneys and paralegals for the firm have access to all case/client-related files in the network, regardless of their specific area of practice. IT, at the specific request of Human Resources, has controls configured so that only HR can access things like employee records. But otherwise it makes sense from the IT perspective that all attorneys and paralegals have access to all case files, and nobody instructed them otherwise. Most of the attorneys (core production employees in a law firm) are not proactively aware of the existence of access control rule sets. They know

they can access all files but don't really think about it or use that ability and consider those concerns the realm of IT. The senior management/partners are comfortable that they are addressing access control in a proactive manner because employee files are restricted to HR employees.

Some of the potential issues with this approach are as follows: It's unlikely that all attorneys have a business need to view all case files in the organization (they would typically need access only to files for their area of practice). But the approach noted above allows a curious attorney or paralegal to view the files for any case, in any area of practice. Further, if any of those 25 attorneys and their respective paralegals has his or her credentials stolen, the thief now has access not just to the files of the victim but to *all* of the firm's files. If an attorney decides to take a job at a competing firm, he or she could access and take case or client data for the entire firm. Any of these potential outcomes could significantly impact an organization, dependent on the type and volume of data being stolen, inappropriately viewed, or used in manner inconsistent with legitimate business purpose. A regulator investigating a breach in one of these instances may focus on the fact that management didn't identify the need to limit access control beyond HR records – their approach considered only the confidentiality of employee records but completely ignored the same confidentiality concerns for clients.

The second organization employs the BLIS model: Since the

attorneys in this organization are directly charged with the protection of their client data, they are very concerned with who might have access to it. As a result, they had conversations with senior management and IT to determine the current access controls in place. These attorneys realize there was no business need for all attorneys to have access to all files and developed the following “rule sets” for IT to implement: Only attorneys and paralegals within a specific area of practice are allowed to view case files for that area of practice. Some attorneys in the more sensitive areas of practice, such as mergers and acquisitions, restrict access further so that only they are able to access these active client files (but not other attorneys within the M&A practice). Further, paralegals dedicated to a specific attorney have access only to that attorney’s files (even within the same area of practice). Finally, other support staff such as the office manager, have no access to active case files. Partners at the firm also institute a policy stating that any deviations from these access control parameters need sign-off from both the practice area leader and a partner (who can’t also be the practice area leader) so that attorneys can’t unilaterally change their level of access through an IT request.

For this second firm, some of the same types of issues noted for the other firm still exist, but they are mitigated to a significant degree. Curious paralegals are much more limited in what they can explore. Departing attorneys can’t access files or client lists

beyond their own area of practice. A credential thief would be limited to the victim's access level, which likely includes only the files of that single victim (vs. all the clients of 25 attorneys). In the event of a breach, a regulator may not even need to be notified because the small section of the network that was breached didn't include any Personally Identifiable Information (PII). Breaches of commercial client information don't require regulatory notice in this instance.

Again, this is a high-level hypothetical analysis focusing on a single control. It is simply intended to demonstrate the potential for impact when the business is proactively driving privacy and network security practices of an organization. It also demonstrates that these attorneys need not have a deep technical understanding of access control in order to significantly insulate their organization from loss/liability. They simply need to understand that access *can* be controlled by certain technologies, and that their granular understanding of the business, applied in conjunction with those technical controls, can materially improve organizational security posture.

Again, access control is just one control area that should be a focus for production units. Material improvement to organizational security posture requires attention across a wide array of control areas; these areas could include effective implementation and management of encryption, training and awareness programs, system monitoring for anomalous activity /behavior, tracking and remote destruction features for portable

devices, incident evaluation and response policies and processes, application and/or URL whitelisting, pre-contracting with the appropriate response vendors, among many others.

(Improving) The Bottom Line

The influential nature of business units is not the only advantage of the BLIS model. Production units are usually better-suited to quantify the value of their various data and can help determine the level of security investment appropriate for different subsets of that data. They are also, generally, some of the most externally active members of a workforce and can therefore be a key component in establishing a formidable perimeter defense.

Most importantly, from the perspective of monetizing security investments, business units are in the best position to leverage the value of those investments with their clients; effectively communicating security posture to a potential client could materially impact the value of, or even the ability to compete for, a new business opportunity.

Companies will continue to trend toward placing more focus on the security posture of their vendors, suppliers, and distributors. Organizations that recognize this trend and that can demonstrate stronger relative security will benefit through higher relative revenue and/or more opportunities to compete. Even though these types of organizations will also enjoy a lower likelihood of being targeted for attack, a lower likelihood

of being breached if targeted, and a lower expense if ultimately breached, the day is coming when those facts become secondary considerations for organizations contemplating investments around privacy and network security.