Information Security Trends – 2015 and Beyond

As regular and predictable as the rise and setting of the sun, the field of information security is always moving, changing and different each moment of the day. Threats, themselves, are organic and change depending on many factors, and their TTP, tactics, techniques and procedures alter themselves depending on their target and what defenses they need to get through. This makes things harder for your defenders, as the amount of resources required and expended to defend from one or many attackers ends up being a force multiplier to the attacker. So what is a company to do? This is the core attribute of risk analysis, and takes into account not only the technical components of information security, but also those involved with the business – insights only obtainable from working across business units within an organization.

Before you can assign resources to protect your assets (digital, physical or otherwise), you need to know what they are and assign a value to them. Since risk management is a concept derived from the financial industry, it's very easy for the business-minded side of equation to quickly run down their list of assets and place a valuation on them. Often since they are the primary users of these assets, they know how they work, in what environment they operate in, and in many cases, who shares in their access and use. Often referred to, when a technical asset is in play, as system owners or stewards, they are valuable sources of information to the risk management process. This will help the defenders think about what protections need to be put into place and how to structure a layered defense to protect those components – typically referred to as "defense in depth". What throws some of the easier protection methods and techniques off before you start is not who access these assets, but from where. The biggest change in the last decade has been the rise of mobility, and, much to an information security professional's chagrin, techniques to protect access, use, and manipulation of assets hasn't matured at a speed in which those business-sided individuals can feel comfortable about.

This, of course, speaks directly to information security spending, and 451 Research's Global Digital Infrastructure Alliance Report which was released this August. These numbers are usually the broad brushes that tend to overlook the actual state of information security within many global organizations, and can merely indicate certain trends but not much can be addressed as to why it occurred. The way the numbers portray it, security spending has "stabilized" to the point of less increases expected within 2015 and no declines, indicating business leaders feel that those operations are adequately funded for their planned operations. In short, most business are spending to maintain current investment levels in information security regardless of any increases in threats, changes in technology or special projects or activities. From the same report, 66.5% of information security spending at respondent organizations reflect 10% or less of the total IT budget. This is somewhat equivalent to spending a significant amount of money to build and maintain a house, put all your belongings in it and use what amounts to what is about equivalent to sales on that home, to spend on security alarms and cameras, fire doors and locks, exterior safety lighting, storm windows, stair railings, home and liability insurance, and fire suppression – the items that make living in that house, and the contents within – safe and secure. The second section asks if those respondents feel they are adequately funded, and when you take in the entire concept of funding to mean "adequate resourcing" that includes people and their skills as well as money, the view is grim, with 97.4% of the respondents just being able to or not meeting the needs – again, indicating that budgetary allocation for information security programs are essentially crumbs they feed off of. However, some of the funding issues may not be directly responsible by management and budget allocators, but could come from the complex nature of communicating the abstract nature and value of information security from technicians up to business decision-makers, and helping them answer the "why" when it comes to need. This is a rare skill to have and maintain within an information security organization, and should be nurtured if acquired through hiring or development.

However, 451s report attempts to put a positive spin on the dour numbers it uncovered in the survey, even resulting in, if viewed from the standpoint of practicing information security professionals, other than management-level staff, some pretty dire conclusions. This, again, returns to potential communication issues between practitioners and decision-makers, as to what are macro-level concerns versus those issues which, at the micro-level, aren't considered major enough to maintain line items in a program or budget to directly address. There's essentially a line differentiating actual operational security concerns and compliance concerns, and while both are integral for a holistic risk management program, they are often driven and managed by two different groups within an organization. This is also made difficult by qualifying what can be considered "success" due to compliance taking a "scorecard" approach and operational security marks success by the reduction or the "no-event" of something occurring, something very abstract to have to ask for support to do. To that end, 451's report on "Most Important Security Concerns" reflects that rift, and that, as noted above, something such as compliance which can be scored, take the focus of respondents. Rolled up, compliance-centric concerns are 48.1% while operational "attack/defense" concerns 50.8%, but that 50.8% is very broad, encompassing only three nebulous categories ("Hackers With Malicious Intent", "Cyber-warfare", "Prevent/Detect Insider Threats"), while compliance concerns are very refined and specific to address. With those broad operational concerns, it's very hard to pinpoint what is and needs to be invested in. Sure there are plenty of tools and just as many vendors to sell them, but it still leaves the question to ask: "will it solve the problem or prevent the issue from occurring?".

Pairing this with the data following those concerns is the identified challenges that the reporting organizations have reported, the top two, by a fair margin are paired well: "Fear of Data Loss/Theft" and "Timely Detection of Attacks" (26.3% and 23.0% respectively). I usually refer to this as "What lunch Is going to be eaten, and when will I know about it?" conundrum. This surmises that your organization has something that somebody wants and at some point, somebody is going to make and effort to get it, but you don't know how, who's going to do it, from where and what they are using. This does lead to a lot of guesswork from the point of the defender, and layering in detection and mitigation tools is the common strategy, but far from comprehensive. The rest of the identified challenges are internally focused, addressing, again, compliance and risk analysis as well as a "skills gap" of having the right resources available to perform the work necessary for the information security functions, roughly 47.2% of answers from respondents. Another item shakes out from these survey responses, which address the volume and complexity of collecting information on the environment, overwhelming threat information (2.6%) and solutions requiring “too many” sensors (0.9%). Given that most defenders are dealing with a blend of automated/scripted attacks and those that are targeted and hand-crafted, trying to have personnel consume, analyze and synthesize detection methods, let alone defense, these two items will jump out and illicit a head nod from those who deal with those challenges daily.

Conversely, when organizations responded to the survey to indicate the saturation of security technologies deployed in their environments, the top three, Intrusion Detection/Prevention Systems (IDS/IPS), Vulnerability Assessment and Enterprise Mobility/Mobile Device Management systems are generators of large amounts of data. So the tools available to detect or counter threats within an organization, by design, end up creating some of the top problems for organizations trying to get a handle on their information security operations. Of the top five (5) planned deployments reported by the survey, the top two Security Information and Event Management (SIEM) and Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) are there to catch, and if correctly configured (which not only should include triggers on events, but should contain business logic rules to help score and categorize the risk of those events). However none of these top projects is aimed that the most important, yet most vulnerable asset of most organizations, and that is its data. While data loss protection/prevention is a concern, very few organizations tend to know how to approach such a task as it requires a large scale culture change (tagging and classification) as well as a high technical overhead required for addressing current data stores and implementing DLP technologies on gateways and endpoints.

What remains curious about the tail end of this report, is the focus on IDS/IPS technologies as either the first or most useful forms of enterprise information security. The report highlights “inhibitors” first, but should actually try to ask what the goals are for an IDS/IPS deployment as depending on how the organization’s technology is structured and used, the deployments, if leveraged are vastly different. One of the biggest questions to ask for the selection and/or deployment begins with looking at the difference between IDS and IPS, the “detection” versus “prevention”, and how that impacts the amount of organizational and business operations knowledge required to have a successful solution. While 451s report highlights that the major inhibitors are staff/resource related (lack of expertise – 34.5% and inadequate staffing – 27%), when setting up an IDS/IPS deployment, an IDS/IPS are best served by gathering information about how the business’ technologies communicate with each other and for what reasons. That gather logic is what helps feed and tune the rules to avoid false positives in detection, but also, when placed into a prevention mode, can be more effective by ensuring critical communication and operations are not blocked by extremely broad enforcement policies. The skills gap usually occurs due to the lack of knowledge of how to tune the devices once the business knowledge is acquired and how to write effective custom rules to reflect those processes, but generally nothing that requires extensive expertise. Much like firewalls, IDS/IPS systems are “policy devices” and require good logic and processes to make detection and prevention, where possible, useful and value-added to an organization’s information security architecture.

Again, survey results veer towards monitoring of such solutions, but tend to not link the previous data, the “people” component, of staff and skills, which equated to 61.5% of reported inhibitors – and indicate the grasp of the effective deployment and use of such tools severely lacking. While it is fine to employ an external organization, through contracts or managed service, to operate your IDS/IPS solution, management and subsequent rules creation and tuning, unless they are also managing the enterprise gateways, will lack the required deeper understanding of those necessary business rules and processes to make the solution realistically useful. The opportunity to see these solutions address the Pareto principle for effectiveness (80/20 rule), it will more likely be lottery odds when actually protecting assets and data. Even more worrisome is the results highlighting that organizations either only have people monitoring their systems during business hours or are automated with no professional staff looking at or reviewing configurations or alerts, or only using the system after an event has occurred (45.3% of respondents). To note, attacks can occur at any time of the day or night since we’re all globally connected, and relying on general rules (in a fully automated solution) or only looking to the tools and data after an event (thus negating any “prevention” of IPS to actually be useful) leads groups into a false sense of security, especially indicating they don’t value those parts of the enterprise they bought these tools to protect. Looking at (or not at all) your data after the fact will only help you indicate the scope of the problem you have and will have to recover from, since whatever has been damaged or stolen is long gone (theft occurs at the speed on milliseconds in Internet time).

So, where does this leave the companies who participated in this survey as well as others? Well, for compliance, there are plenty of audit tools, policy orchestrators and configuration management systems that are in place in most places due to the need to manage the technology on a day-to-day basis that can be queried and polled to collect the data sufficient (and in some cases, more than sufficient) to respond to regulatory requests and requirements for PCI, HIPPA, SOX and a litany of other continuing and annual reporting and certification requirements. The key activity here for companies is finding out best ways to reuse and share data already in place, and result more in handling people and leveraging soft skills, than any real technical overhead to achieve those goals. On the other hand, for active detection and protection activities, things remain and will remain complex and changing as technologies in use by employees, companies and the public are constantly changing and placing demands on architectures and infrastructure.

As noted above, mobile technology has changed the information security “game” more rapidly than any other technology that had come before it. The perimeter for business operations no longer stops at a network gateway, so traditional “castling” of vital assets within an enterprise no longer applies and new forms of data protection and access control management must be employed, as well as any detection of theft or other malfeasance. To manage these mobile outposts of the enterprise, organizations have to think differently (and quickly) on how they manage their data (such as encryption, access control and transport security), access control and management (strong authentication, multi-factor, PKI), as well as the more traditional layered components such as host-based intrusion detection and prevention, anti-virus and anti-malware, digital rights management, application and system process auditing, port control and security, vulnerability assessment and management, and more traditional systems management techniques of policy auditing and configuration management. It's important to have them working efficiently and in consort with each other to ensure that their alerts and protective capabilities and reported to right team or individual for threat assessment and remediation, but also to have a holistic view of the state of enterprise information security and operations. Strangely, tools such as SEIM promise some or all of this capability, but as noted earlier, developing triggers set to and actions on business process and other policy rules is required to effectively enable the solution. Conversely, beyond mobile, the addition to off-premises hosting and cloud services complicate these technologies and traditional architecture, in some cases making them moot. Most cloud providers will not allow customer hardware and tools traditionally used to monitor and respond to threats on the network or systems to be installed in cloud instances, and what remains are virtualized tools that may or may not not work as effectively in these environments, given that much of the infrastructure is virtualized and "software defined". The flexibility and scalability of cloud challenges the capabilities of these tools, which are often designed to operate in a certain way, either based on processing volume, placement on a network, or the type of systems it is monitoring (such as those with virtual or multiple IPs). Due to this nascent operational security environment, traditional vendors are still adapting their offerings, as well as information security staff, to a new model that challenges traditional levels of control and response capabilities.

Overall, the information security trends aren't as bleak as highlighted above, as long as organizations are willing to learn and adapt and understand their needs and better vocalize the demands of features, capability and usability to the vendors who push "solutions". This should be less of and exchange between organizations ad vendors of a child being handed candy, and not knowing what to do with the sugar rush afterwards, but making smart and healthy choices that will help their operations and move the progress towards the goal of awareness and response capability to an effective and efficient level. It's important for information security leads within organizations to share information, techniques, trends and other related data about the effectiveness of their operations so any gaps can be addressed, not only in the vendor and operations space, but identify the skills necessary to be acquired or developed in staff whose responsibility it is to install, configure, operate and respond to these tools and solutions.