ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

CISO Solution Fatigue

Overcoming the Challenges of Cybersecurity Solution Overload

Authors

James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (Researcher – Institute for Critical Infrastructure Technology)

Contributor:

Rob Roy (Fellow – Institute for Critical Infrastructure Technology)

Underwritten by:

Hewlett Packard Enterprise

An organization's network is only as secure as its most vulnerable connection. Cybersecurity is a fundamental component of the overall security of every organization in possession of valuable information. Due to the plague of APTs, malware, ransomware and other malicious initiatives by invisible adversaries, few C-level executive positions are as critical as the CISO. As a result of the constant barrage of breaches over the past five years, 54% of organizations have created the role of Chief Information Security Officer (CISO) within their organizational structure. CISOs enjoy a median salary between $194,000 and $270,000 and an unemployment rate of less than 1%. CISOs have the difficult position of finding the harmony between not impeding business operations while implementing risk informed security strategies that protect the important information assets and accesses of their organization. The CISO must be able to adapt quickly to changes in both the threat landscape and the organization. Though cybersecurity implementation times are decreasing due to virtual infrastructure and simultaneous systems, some solutions can take days to months to implement. The process may be longer when the acquisition process is included. CISOs need the foresight to implement solutions before problems arise. The pressure on CISOs mainly derives from relentless cyber-adversaries, from an overabundance of information and vendor solutions, and from communication difficulties within the organization.

Solution Overload

In many cases CISOs operate under the unrealistic expectation that they should be able to prevent every breach with a finite budget. They are expected to have enough technical expertise to develop a strategy to protect the business and enough business acumen to convince the board to adopt that strategy because it aligns with the goals of the organization. As a result, modern CISOs tend to function more as Chief Information Risk Officers, managing the risk to data and technology within the organization. Lack of understanding of the role and unhappiness in the position contribute to an average turnover rate of 17 months. Another primary reason for rapid burnout is the solution overload, which results from the pressure to find comprehensive solutions and the overabundance of vendor solutions. Over the course of their role, some CISOs claim that annually they may hear hundreds of company pitches for security tools and solutions.

Cyber-attacks have recently increased in severity and cultural awareness. As a result, organizations heavily invested in innovative startups. According to a CB Insights report, between 2010 and 2015, investors funded approximately 1208 private cybersecurity startups with over $7.3 billion. Each company is attempting to aggressively push its competitors out of the market. Many startups over-promise and under-deliver on their proposal by offering

unreliable silver bullet solutions. To lower development costs and to beat their competitors in the race to market, startups solicit CISOs to test minimally viable products and provide feedback to fuel future development and refinement prior to mass market release of the tool. The process often nets the CISO a discount and occasionally results in a customized and refined solution to the cybersecurity problem. However, every time a CISO discovers that the adopted vendor solution is unreliable, they must either adopt or develop a replacement solution. The additional responsibility across a platform of products increases the compounded stress and pressure associated with the role.

Aside from a rapid increase in venture funds, the vendor market has bloated due to the availability and affordability of cloud architecture. Software as a service (SaaS) delivery models have a very low barrier to entry. This allowed for cybersecurity startups that promised to solve every problem imaginable or who created new problems to solve. Vendor solutions that failed to address security concerns or that introduced new problems for the organization led many CISOs to attempt to develop and market their own products. One example of this is HPEs DNS Malware Analytics product, which is the direct result of an R&D request from HPE's CISO to address a malware problem on the network. In effect, these CISOs joined the vendor ecosystem and contributed to the solution overload affecting other CISOs.

Solution Overload can be overcome by altering the business model to value long-term stability over short-term potential gains. Technical staff should listen to pitches and evaluate tools so that the CISO can focus on the development and alignment of the strategic vision of the security program to the business mission and to the policies, procedures, guidelines, and standards to which the organization must adhere. Solutions must meet the business needs instead of just the CISOs need to find a solution to alleviate pressure on the position. CISOs need to understand the environment of their organization and they need to include all stakeholders, including the security team, information technology team, members of the board, and personnel from the acquisition, finance, legal and other departments in the decision to adopt a vendor solution. This holistic discussion of the capabilities and capacity of the product will better ensure that the product meets the need of the organization and that it aligns with the organization's policy, governance, and personnel capacity.

Vendor attempts to offer silver bullet solutions undermine the community at large and poisons the vendor-customer relationship. The culture promoting these inadequate solutions distracts CISOs, technical personnel, and solution developers from the risks and threats in the threat landscape and it distracts them from designing the right solutions to address the market

needs. Reliable vendor solutions solve an actual market problem instead of a hypothetical or market derived problem.

Failure to understand the realistic capabilities of a proposal and failure to understand the needs of the organization can result in either overlapping and redundant unintegrated solutions or it can lead to gapping cyber vulnerabilities. CISOs, who make the ultimate purchase decision, need to focus on their business need, instead of the availability of tools. In many cases, the CISO has the responsibility to turn down even promising solutions because they do not meet the current needs of the organization. Solutions are meant to enable the safe conduct of business instead of hamper operations under a blanket of unnecessary software that restricts personnel productivity. Vendor solutions need to be transparent, they need to support growth, and they need to offer layered security. Most importantly, they need to perform as promised and address the needs of the organization.

CISOs can reduce solution overload by ignoring the hype surrounding a solution, and instead looking for the value offered. An easy rule of thumb is to look for solutions instead of products. Information sharing within the sector can help to determine what solutions live up to their product pitch and what solutions promise only false hope. Rather than investing in innovative solutions, the CISO can adopt or customize tools that have already had lasting success in the industry. An organization in desperate need of a solution should not be a viable guinea pig. It is the CISO's responsibility to separate fact from fiction and make responsible decisions. Seeking tools from "outside the box" is great when the organization is stable and has the extra resources; however, it is important to occasionally remember that some tools are in the box because they have proven themselves reliable or essential.

Addressing Organizational Needs

The CISO must be cognizant of emerging technologies, the roles they could play in the organization and the threats that they introduce into the operating environment. Many organizations still have not addressed the threats posed to them by user owned and operated mobile devices. For example, the advent of BYOD meant that organizations were more efficient, because employee devices were more mobile and more current; but it also meant that they were more vulnerable to internal and external threats to the network. It is difficult for native IT and security teams to detect and manage all of the potential mobile devices because personnel feel disenfranchised by their attempts. In some organizations, key leaders, such as the executive board are the main violators of BYOD policy. Adopting a vendor solution to BYOD introduces an objective and efficient option for the CISO because it is devoid of internal organizational bias and because it maintains accountability.

Similarly, the Internet of Things poses a threat to every organization. Monitoring or preventing the communication between mobile and native devices can consume a significant amount of the attention of the CISO and the security team. Vendor solutions that secure IoT devices and that securely monitor or regulate communication to those devices can improve the organization.

Ultimately, the organization needs to prevent the loss of data due to internal and external threats. Data loss prevention services are implemented to prevent the extraction of confidential information, to ensure the appropriate reporting in the event of an incident, and to appropriately monitor the infrastructure and associated people for attempts against the system. Small organizations who lack an information security team and massive organizations whose team is disproportionately unable to monitor all personnel, are best served by adopting a vendor DLP solution. The DLP solution should be in addition to data encryption solutions which are used to protect sensitive and mission critical data. The CISO must ensure that the solution adequately addresses all attack vectors.

To ensure the integrity of systems owned or operated by the organization, the CISO may promote application and system testing solutions. These services, such as penetration testing, help to identify vulnerabilities in the organizational infrastructure before adversaries breach the system. The services can also be used to detect and remove attackers' footholds on the network. Vendor services range in their sophistication, regularity, and cost. CISOs should select solutions that meet the needs of the organization, who have a reliable reputation, and who can be trusted to maintain confidentiality.

The CISO and the information security team cannot monitor every aspect of the organization and threat landscape. There is far too much information. Personnel become bogged down by data from log sources, information from endpoints, information from identity management systems, deep packet visibility, and internal and external threat intelligence. Educational security awareness solutions can be used to change poor employee behaviors. User behavioral analytics systems can be used to identify insider threats. Vendor solutions that help security and IT teams sift through the data to identify anomalies or trends in the data can immensely reduce the inefficiency imposed by big data. Solutions that deliver current or immediate information about threats, recent incidents, or shifts in the threat landscape can also help organizations improve their cybersecurity posture. The CISO may seek a solution that delivers information through regular updates or continuously through a virtual SOC.

Cloud computing enables an organization to reduce costs by virtualizing physical devices and eliminating redundant positions. Often CIOs and executive boards are in favor of these external solutions due to the perceived efficiency and savings. The CISO must ensure that cloud architecture and virtual tools are adopted according to the security needs of the organization, from reliable vendors. Vendors should be held accountable with comprehensive service level agreements. Appropriate security measures should be in place on the vendor side and their operations should be transparent to the organization. CISOs value dashboards and tools that allow them to monitor vendor operations and the safety of the organization's data in the cloud. However, these tools can lead to information overload if the monitoring criteria are not properly chosen. Dashboards must be regularly reconfigured as the organization's values change or as the organization grows.

CISOs also value cloud services that are scalable to the current and future needs of the organization. Cloud services cannot be secured with the same perimeter security solutions native to most organizations. When possible, the CISO should promote the adoption of cloud vendors who appropriately include security as part of their service. Otherwise, the CISO will need a cloud security solution that scales to the cloud service and comprehensively secures data. The advantage of employing a cloud security solution that is agnostic of the cloud service that it secures is that the organization can diversify and rely on multiple cloud vendors. In this case, the CISO needs to have visibility and enforcement authority in each service. The CISO should base their choice of a cloud security solution on the capabilities of the entire security platform and its interactions with other services instead of on the efficiency of a single security feature. Long-term decisions can be made by researching how quickly new features are sent to market and how much those features disrupt the market.

Cloud solutions should be compliant with the constraints of the organization and be securely available on-demand. When possible, cloud services and cloud security solutions should be automatically or easily configurable to the needs of the organization. Feasible solutions must be able to be integrated into existing infrastructure and they should depend on an accessible or open API.

Communicating Across the Organization

According to many CISOs, communication with decision makers within the organization is one of the most important and exhausting responsibilities of a CISO. William Lay, former CISO at the U.S. State Department, recently said "The biggest challenge [for me personally was] ... telling the story consistently to a large enough number of people that it starts to resonate… The hardest thing about getting a new idea in is getting the old idea out and that's particularly

true in cybersecurity." CISOs do not always control the security budget and they may not even be the final authority of security solutions if the organization relies on an architecture review committee. CISOs' power derives from their ability to justify cybersecurity solutions to business and technical audiences according to the relevant criteria. If a CISO does control the security budget, then he must be the premier champion of desired solutions. The decision must be justified according to regulatory compliance needs, cyber threats and risks, competitive pressures, and organizational limitations. Otherwise, the CISO may need to convince stakeholders with quantitative measures, and with a qualitative pitch. The pitch should be 2-3 simple, but not necessarily non-technical, benefits that the solution offers the organization according to its mission and interests. In some organizations, the CISO reports to the CIO instead of the CEO or a board. This indirect structure can result in gaps in understanding and communication within the organization.

The CISO must defend their solution based on technological gaps and internal organizational risk tolerances. The most influential tool that a CISO can leverage is a cyclical information security risk assessment, such as Octave Allegro, that identifies the critical assets of the organization and defines the risk to those assets according to the current threat landscape. Qualitative justifications can be used to persuade stakeholders that a solution is feasible, though quantitative metrics are more convincing and more easily understood by nontechnical audiences. Each stakeholder will have different driving motivations, concerns, and biases. The CISO must address each audience accordingly without alienating or dismissing their views. Stakeholders want informative high-level descriptions of the security strategy and implementation descriptions. Quantitative measures, such as risk metrics and ROI can also be used to elicit cooperation from the upper management.

Return on Investment

The return on investment (ROI) of security solutions can be equated to the fiscal component of the impact that the organization would assume if an adversary exploited the vulnerability that the solution addresses. For example, assume that a hospital was attempting to procure a solution to prevent personnel from clicking on phishing emails because other hospitals had recently fallen victim to ransomware attacks through that vector. The CISO could begin to calculate the ROI by averaging the paid ransom demands or downtime costs (if the system was restored from backup) of other hospitals. The mission of many healthcare organizations is driven by their reputation; as a result, the CISO could calculate the reputational harm caused by a ransomware attack according to the publicity, charity, and other costs assumed to repair the organization's reputation. If the attack has an impact on turnover or talent acquisition rates,

then those associated costs may also be considered. Any fines, breach notification costs, and other expenditures should also be included. Other factors may be considered, depending on the sector and the organization.

The risk assessment should also have predicted the likelihood of each cascading impact. The probability of the impact should be multiplied by each associated outcome. For example, if an attack has a 10% likelihood in resulting in $10 million in reputational harm, then the product would be $1 million. The CISO should then take the aggregate of the probable potential impacts and multiply it by the probability that the organization will suffer an attack that the solution could prevent, within the lifetime of the solution. This number is the assumed cost that the organization faces if it does not adopt a solution. Now, the CISO should find the sum of the cost of the solution, any associated costs (such as implementation), and the upkeep costs of the solution over the expected lifetime of the product. A probabilistic cost may be considered to account for the possibility that the solution fails.

The CISO can then present the solution to the board according to the standard ROI model. If the solution is not adopted, then the organization will likely face the former cost calculated. If the aggregate cost of the solution is equal to or lesser than the assumed impact, then the organization should adopt the solution because it has a positive or net zero ROI. Some organizations may even adopt negative ROI solutions if they are cautious, value public good more than the profit line, or if they expect aggressive changes in the threat landscape.

Conclusion:

CISOs are critical in the defense of organizations from cyber-crime. According to the Economist Intelligence Unit, proactive CISO-led strategies can cut the success rate of cyber-breaches by more than 50%, hacking successes by 60% and ransomware infections by 47%. A well informed CISO can improve the engagement of the C-Suite and improve the cyber posture of the organization. Every CISO must combat information overload and vendor solution overload to possess the information necessary to effectively communicate with the board and ensure optimal security for the organization. Paradoxically, vendor solutions must be drawn from the overabundant ocean of options, coherently rationalized to the board, and then implemented to prevent information overload. The real solution is a knowledgeable and discerning CISO who is capable of identifying and adopting the best solution for their organization.

Contact Information

Legislative & Executive Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

Cloud Passage:

https://blog.cloudpassage.com/2015/03/03/how-to-turn-the-ciso-from-dr-no-to-a-true-business-enabler/

CSO Online:

http://www.csoonline.com/article/3077243/it-careers/vendor-overload-adds-to-ciso-burnout.html

http://www.csoonline.com/article/2926173/security-awareness/cisos-turn-to-security-awareness-solutions-to-change-poor-employee-behaviors.html

Digital Guardian:

https://digitalguardian.com/blog/make-vs-buy-cisos-guide-evaluating-managed-security-services

Ecommerce Times

http://www.ecommercetimes.com/story/82074.html

Enterprise Cloud Resource

http://www.enterprisecloudresource.com/articles/416395-ciso-dashboards-securing-information-one-metric-a-time.htm

Fedscoop

http://fedscoop.com/state-dept-ciso-leaving-laments-security-fatigue

IT Pro Portal:

http://www.itproportal.com/2015/12/22/when-job-title-not-enough-why-do-cisos-only-stay-with-you-18-months/

IT World Canada:

http://www.itworldcanada.com/article/rsa-2016-how-analytics-and-threat-intelligence-meets-ciso-needs/381311

Mimecast:

https://www.mimecast.com/blog/2016/01/ciso-of-2016-balancing-prevention-and-remediation/

Security Intelligence:

https://securityintelligence.com/the-ciso-job-market-in-2016-time-to-jump-ship/

Securonix:

http://www.securonix.com/cisos-must-quickly-adapt-to-any-situation/

Tenable:

http://www.tenable.com/blog/cisos-face-tough-challenges-when-procuring-security-technologies

Tripwire:

http://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/the-ciso-as-a-sales-person-part-1-selling-to-the-security-architects/

Secure Digital Solutions:

http://trustsds.com/playbook-for-the-ciso/

Value Walk:

http://www.valuewalk.com/2016/06/c-suite-leadership/

Veracode

https://www.veracode.com/blog/2015/10/presenting-board-what-board-members-really-want-hear-cisos-sw