Getting the Basics of Cybersecurity Right

Security professionals understand and acknowledge that there are a myriad of challenges facing cybersecurity teams today. However, not all challenges are relevant to all organizations at any given time. It is important to understand what the real challenges are for the vast majority of cybersecurity teams and chief information security officers (CISOs) as opposed to the challenges that are faced by the minority of cutting-edge organizations. This article discusses some conclusions about the relevance of challenges based on the author’s experience in addition to efforts in the social media realm. These conclusions come from an ongoing exchange of experiences and opinions with peers from various sectors, industries, geographies and organizations of all sizes and maturity levels. As obvious as these conclusions may sound, many articles on cybersecurity seem to be unaware of them. Many articles seem to address high-profile organizations that are far from representative of most organizations. The conclusions discussed herein can be applied to the vast majority of organizations. The points that follow are closer to a written mind map rather than a formally structured framework.

Affording Security Technology

Leaving aside cutting-edge or high-risk-profile organizations, critical service providers and other, similar businesses, the following lessons appear to be true:

• **Organizations buy the technology they can afford**—That is the reality. Technical features are good to know and technological fit into the organization’s IT landscape may be a weighing factor, but, at the end of the day, the money available to spend on a firewall, security information and event management (SIEM) system, data loss prevention (DLP) system, or any other security control is, in the vast majority of cases, the single most influential criterion used to make the decision. This is primarily because there should be an inevitable proportionality between the value of the assets the organization intends to protect and the cost of the resources the organization devotes to actually protect them. More than the technology itself, it is likely that the organization’s chief restriction is the price it can pay for technology, and that is strictly related to the value of the assets it is protecting (figure 1).

• **The vast majority of organizations are not ahead of the market**—They either represent “the market” or are behind the market. So, while certainly there are debates on the limitations of the technology currently available in the market to prevent, protect, detect and respond to cyberattacks, and discussions as to where artificial intelligence will

---

**Ramón Serres**, CGEIT, CISM, CSX Fundamentals, CCSP, CISSP

Is an industrial engineer with a long career in IT and a passion for information security and risk management. After being a management and e-business consultant in his early years, he has held several management positions in consumer goods and pharmaceuticals. Over the last few years, Serres has successfully led a transformational project in his current company, bringing the information security function to the business and the C-level and pushing the organization to a higher maturity level.
find, not a big gap, but an ocean of gaps between what good practices recommend and what really happens. Most organizations use a security framework more as an inspiration, guideline or stimulating target, rather than a real objective, unless a stakeholder actually manages to clearly demonstrate the relevance of those frameworks and controls to the particular business and its particular senior management. It is crucial to think thoroughly about the controls to implement and the relevance they have to the business.

- Organizations know what needs to be done—Thanks to all the good advice that circulates—even from before the Wannacry attack, but particularly after high-profile breaches that are becoming more frequent—and the beautifully formatted presentations, infographics and other communication tools, organizations know what to do. Most readers have seen dozens of pictures with the key messages: Patch, invest in detection and prevention, gain resilience. What to do is known to most practitioners and organizations. What most do not know is how to do it because there is a major step between the goal (e.g., the systems must be patched) and its realization (e.g., actually patching the systems). The challenge has a lot to do with organization, definition of responsibilities, service level agreements (SLAs), managing people, etc.

In this general context, much of the cybersecurity content that goes around in specialized blogs and magazines could be considered as missing the point, as it would apparently seem that missing extra features in the current technology and getting even more advanced features are the most common problems organizations face when, in fact, they are not.

The majority of organizations can definitely do with the technology that is available. The real challenges remain in the basics around having those technologies in full operation.

- Senior management lives far away from the frameworks, methodologies, maturity models, standards and other tools of the cybersecurity trade—ISACA® frameworks and good practices, the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the International Organization for Standardization (ISO) with all its recommended controls, and other relevant standards/guidance are valuable assets indeed, but the bridge between these frameworks and senior management needs to be built. The most common reality is that in virtually all domains, it is not unusual to lead, those conversations actually apply to a very limited minority. In global terms, by remaining grounded, it becomes clear that the limitations current technologies may have are likely a problem for a very small minority. Most organizations are not in that elite class. It can be likened to commenting on the possible defects of a McLaren, while the truth is most will actually be driving a Volkswagen. Figure 2 shows this in further detail.

Figure 2—Is Individual Reality Representative of a Majority or of an Elite Class?
The Real Challenge

Basic cybersecurity recommendations that appear in many sources are fine and sufficient for most organizations, but the challenge remains in how to do it, how to get things done. Organizations struggle to get things done.

Having a third party scan the organization's network to find vulnerabilities; check controls to see which ones are missing; point at the network’s, systems' and applications’ weaknesses; and interview key stakeholders to complete the picture is relatively easy, particularly on the most technical part, as the available tools are effective.

Translating all those weaknesses and vulnerabilities into a program that makes sense to that particular business is a key challenge. The program will be a set of activities and projects, some of them performed as a sequence, some of them in parallel. Again, this is relatively easy, particularly if there is no particular commitment as to the feasibility of the deadlines.

Building a Simple Model

This leads to a very simplistic model where there is, on the one hand, the implementation and deployment of new solutions, whatever they are (based on technology, people, processes or organization) and, on the other hand, the business as usual, the operations.

The implementation and deployment of new solutions refers to new projects, which can tackle any domain of information security: a new regulatory framework, a new security architecture design, the implementation of a new perimeter firewall, a DLP system, a cloud access security broker (CASB), an identity and access management (IAM) process, a SIEM, etc. Something new. Something the organization did not have previously that now must be implemented and set in operation.

The reference to business as usual points to all security operations: alert monitoring, systems adjustments, policy compliance monitoring, incident response, security reporting, etc. All new systems, projects and solutions end up adding new tasks to the business-as-usual side.

Governance

All these projects and business-as-usual activities should be done under a certain direction—knowing why things are being done; knowing that what is being done is good for the organization's goals; and knowing that these activities are consistent with a well-defined direction that has not been laid down as a result of improvisation, but formally by the organization's senior management. This all can be described extensively in processes and concepts, but it all comes down to one single word: governance. As figure 3 shows, deviations should progress toward the end target.
A complete operating model may be sensibly built on ITIL. Nevertheless, for those organizations that cannot afford to go for such a complete model, the following guidance may be useful:

- **People**—Managing security is about managing people: leading a team; organizing people; and conveying clear messages as to the priorities, mission, general criteria and guidance that should steer all decisions in which the leader will not be directly participating. For those decisions that are delegated across teams and service providers, to be consistent, the mission and vision should be clearly stated and effectively communicated. Another thing relating to people is motivation. The leader must keep up the motivation and convey a challenging future that engages a team that will, in many cases, cover a 24/7 service and, in the event of a severe incident, will stay awake long hours doing forensics, hunting threats and monitoring the network at an inch-by-inch level.

- **Processes**—Even at different maturity levels, all organizations need to have clear processes. If the right context and culture are in place to create a perfectly defined organization, then processes, their inputs and outputs, their activities, and their measurement will need to be defined in a formal way. If the organization’s context, culture or size does not fit with a formal definition, then an effort should be made to implement a process-like organization that enables the organization to work as smoothly as possible.

- **Roles and responsibilities fall somewhere in between processes and people**—They define who does what and the more concrete, the better. This is especially important when various teams are involved such as security operations, infrastructure management, enterprise architecture and service management. This becomes not only important, but critical, when various service providers interact with each other. The organization should face the definition of responsibilities at the earliest possible stage. The sooner the potential conflicts are identified, the sooner a solution can be devised, which, in most cases, will be a compromise. Blurred, unclear or informal definitions of roles...
and responsibilities are bound to be a problem. And, if the organization has to manage a security incident, which, unfortunately, is likely, an unclear definition of responsibilities will explode.

**Internal regulatory framework**—That is, the organization’s information security policy and related documents, whatever they are: guidelines, standards, baselines, procedures. It is worth dedicating time to creating these documents to suit the organization rather than just downloading a policy from the Internet. The regulatory framework has to be tailored to the organization’s particular context, size, culture and, most important, risk map. There are often many stakeholders that have a say in elaborating an information security policy: IT, legal, human resources, information security, even finance. But once it is all written, some time should be devoted to gaining explicit approval and endorsement from senior management. This may take time, some explanation and some minor changes, but it will pay off because a proper regulatory framework will enable further security-project-related decisions that come as a consequence of what is stated in the policy.

**Conclusion**

Managing cybersecurity or, more specifically, managing cybersecurity risk, is much more than just technology and, in most cases, has nothing to do with having the money to afford state-of-the-art technology.

Managing cybersecurity risk is generally a matter of acquiring affordable technology and, above all, getting the basics right: managing people, processes and organization, and setting up governance and operational models that work. This is easily said but is a big challenge by itself, particularly in larger organizations where several teams and service providers are involved, each of them with a specific service level agreement. The more pieces in the puzzle, the more complex it becomes. And the reality will prove that defining roles and responsibilities, processes and organization will turn out to be more important than what particular technical feature has the last next-generation firewall acquired by the organization.

There is no magic solution, nor a single approach that fits all. Knowing the organization, the particular industry in which it operates, the risk and the resources will result in a better position to develop the right solution.