Volume 3 Issue 6

COVER STORY

# CISO

## THE TECHNICAL UNICORN

David Katz, Partner, Adams and Reese



27

CISO MAG | June 2019

Volume 3 Issue 6

COVER STORY

Alone sentry stands guard on the eastern end of towering granite stone wall with sweeping views of the approaching terrain. Bravely, he scans the expansive horizon like an eagle searching for its prey. The sentry maintains a single-minded focus and a determination to identify and eliminate any potential threat at a moment's notice. The sentry is filled with trepidation knowing an attack is imminent and that he is all that stands between security and total destruction and, in spite of the fear, performs with honor and does his duty.

The parallels to the plight of the modern-day CISO as the lone sentry guarding against the barbarian hordes charging the wall, while dramatic, are not far off the mark for comparison. A closer examination of the role of a CISO reveals far more than just the role of a lone sentry, expendable and vulnerable for the collective safety of others and the greater good. Far from expendable, the modern day CISO should be viewed and equipped like a five-star general responsible for leading a coalition of capable and technologically advanced war fighters against a determined enemy bent on the destruction of our economic and national security. Making the case for such treatment by the C-suite and corporate directors can be challenging and requires a high degree of technical proficiency, emotional and social intelligence, and raw political skills not seen since the days of the Medici in Florence, Italy.

The question presented and answered in this article is how the modern day CISO can position themselves to be successful in the face of such challenges and lead their organizations with confidence and, most importantly, with a full complement of material to assure victory in the face of significant cyber security threats.

## The Evolving Requirements of the CISO

The CISO's responsibilities within an organization can vary in scope depending on the management reporting structure within the organization. Typically, the CISO is an executive that is responsible for the organization's information and data security; however, in recent years some organizations have expanded the role of CISO to encompass more of a direct management and decision-making role in operations and direct reporting to the CEO or


directors in their capacity as a vice-president or CSO.

The CISO's evolving duties include an interwoven set of responsibilities that combine complex technical operations with underlying business operations. The resulting outcome is that in many instances the success of business operations from a security perspective are dependent on those technical operations overseen by the CISO. These unique responsibilities are not shared or governed by any other individual business owner within the organization. This evolution is one of the many elements that makes the role of the modern CISO very challenging and unique to all other executives. The dependency here puts tremendous pressure on the CISO to ensure that security does not impede the business operations, yet any failure of security which leads to an operational failure will likely be blamed on the CISO.

As an example, the CISO must make decisions concerning expenditures for security architecture that involve planning, purchasing software or hardware, and working with IT operations and networking infrastructure teams to ensure best practices are implemented from a security perspective. Again, in this case, the operations are dependent from a security perspective on the work of the CISO, but the decision making from a business perspective is removed from the CISO. To the extent a conflict develops between the security and business teams around network architecture planning, the CISO must adeptly navigate and make the case without impeding the business and ensure the ultimate decision makers for the business have the information necessary to adopt the best practices even if this may be an impact to operations.

The second example of this interwoven set of responsibilities and dependencies occurs in the security domain of access and identity management. This area of responsibility requires the CISO to ensure that only authorized individuals have access to restricted data and restricted systems. Here, the CISO's responsibilities are interwoven with the human resources department. In this case, the operation is dependent on the CISO to ensure only authorized individuals are granted access to restricted data and restricted systems. Ultimately, it is the business operators in the form of human resources representatives or individual managers that determine accessibility or control the means by which the CISO is made aware of personnel changes. This creates a potential

Volume 3 Issue 6

COVER STORY

conflict in that failure to restrict an unauthorized individual can result in a security incident for which the CISO may be held accountable, but the CISO may not ultimately have control over the designation of who is or is not an authorized individual.

In summary, these examples illustrate an existing tension for the modern day CISO in many organizations. In simple terms, the CISO is accountable for the security of systems and operations for which they may have no ultimate decision-making authority. The CISO must instead rely on their communication and persuasion skills in order to resolve conflict or be in a position to escalate up through management to resolve potential conflicts without alienating their internal business clients. Exacerbating this tension is the fact that corporations are organized to create wealth and value for their shareholders and to secure a profit. Where a conflict arises that forces a decision that could impact profitability over security, it becomes very difficult for management teams and directors, given their primary mandate to make any decision that could imperil profitability. Even if the risk of loss from a security failure could potentially impact profitability, management teams and directors won't be rewarded for playing it safe at the expense of earnings. To say this creates a difficult position for the CISO is at best an understatement. In light of these dependencies, potential conflicts, lack of decision-making authority, and primary mandate of the corporate form for profitability, the primary question remains: How can the CISOs position themselves to be successful, lead their organizations with confidence and obtain all of the necessary resources required to secure their organizations?

## The Unicorn Theory

In order to be successful, the modern day CISO must first possess all of the technical skills required to perform their responsibilities and these skills are not easily acquired or in abundance in the marketplace. Second, the CISO must have all of the communication, emotional and social intelligence, and political skills to consistently and adeptly negotiate the inherent conflicts that exist in the successful performance of their duties and responsibilities within the organization. Like the technical skill-set required, the communications skill-set is also not easily acquired or readily found in the marketplace. It is the combination of both these

sets of unique skills that can ultimately lead to the success described above in this article. The evolution of the CISO is a testament to the unique position and challenges inherent in this position. The growing influence and recognition of the CISO as a key position within the management team and the trend in organizations to create an independent line of reporting up to the board of directors is also a recognition of the growing complexity in the duties of the CISO. The CISO must think of themselves as a unicorn: a mythological creature so rare as to have thought not to exist. A CISO must view themselves as both a technical expert but also a polished corporate executive capable of navigating the challenges of the most complex business problems and communicating their solutions clearly while obtaining support from their ultimate business owners. A CISO that can identify and translate complex technical security risks to the business and provide tactical solutions with a business minded approach that management can understand in terms of profitability and cost can achieve the desired support and resources even if conflicts exist that appear insurmountable. Working to develop and master these dual skill-sets will ultimately result in all of the necessary resources being obtained in order to perform their duties successfully.

*The opinions expressed within this article are the personal opinions of the author. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.*



Volume 3 Issue 6

COVER STORY