Millennium Alliance event tackles the challenges of cybersecurity today with an eye on the future

Analysts - Aaron Sherrill

Publication date: Friday, January 24 2020

Introduction

Regardless of title – CISO, CSO, VP of information security – those ultimately responsible for an organization's information and data security are facing a growing mountain of challenges, demands and expectations. Almost one-third of enterprises identify security and risk issues as having the greatest impact on the organization's IT strategy, and over half report that security and data privacy are among the key drivers for digital transformation initiatives (451 Research's Voice of the Enterprise, Macroeconomic Outlook 2019).

At Millennium Alliance's Transformational CISO conference, one of many events held throughout the US each year, security leaders from across the country gathered for roundtable discussions and interactive sessions exploring strategies and tactics to tackle the evolving cybersecurity challenges facing their organizations.

The 451 Take

Security leaders from every sector have a seemingly unending thirst for information, but only a third are actively leveraging peers for insights and perspectives. For most, it is not for lack of desire, but rather lack of opportunity. Although many large security conferences offer networking opportunities, and virtual peer groups are available through a variety of avenues, security leaders are also seeking more opportunities to have face-to-face, in-depth discussions around pressing topics. Connecting with peers provides opportunities to discover blind spots, validate current strategies, understand how security programs compare to similar organizations, and learn from the failures and successes of others. The Millennium Alliance's Transformational CISO conference seeks to provide such an alternative, offering to connect with peers across a wide spectrum of industries in an unpretentious and open-minded environment.

Details

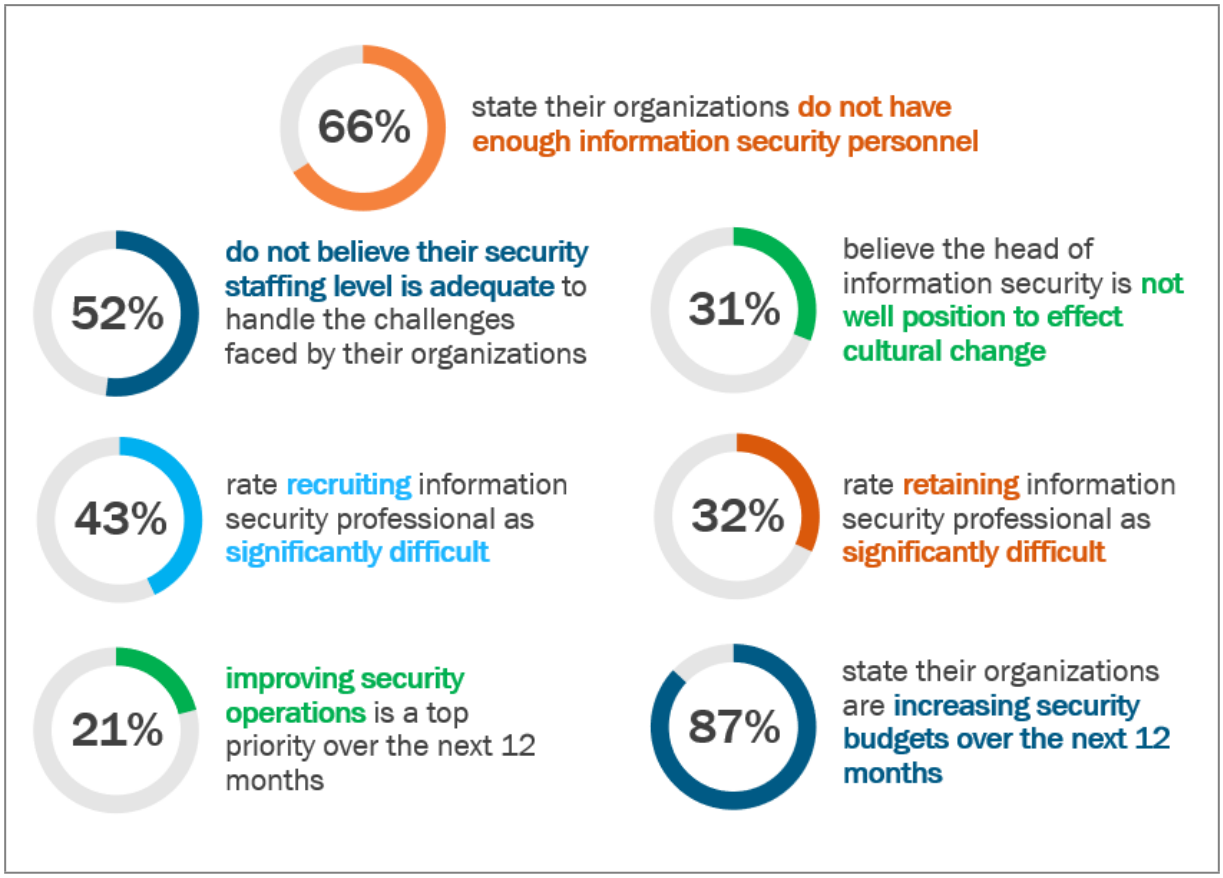
Headquartered in New York, the Millennium Alliance hosts a number of executive-level, invitation-only events throughout the US each year. Designed to be small, intimate gatherings, content is centered on the digital transformation of the enterprise. Events are either focused on particular industries, such as healthcare, retail, financial and insurance services, or specific areas of the enterprise, including cybersecurity, data, information technology, marketing or human resources. Constructed to help business leaders stay ahead of the curve in the ever-evolving landscape of technology and digital transformation, the events attract executives seeking to engage and connect with peers and thought leaders.

In stark contrast to the many large, and often vendor-driven, cybersecurity events held throughout the world each year, the Transformational CISO events are guided, and often led by, conference attendees, and are focused on relevant and timely issues facing cybersecurity leaders. Smaller, interactive roundtable sessions enable peer-to-peer discussions that promote the sharing of ideas, success stories and strategies. Engaging sessions are often infused with healthy and constructive debate and exploration.

The discussions and sessions at the recent Transformational CISO East event held in Nashville, Tennessee, underscored the yin and yang that cybersecurity leaders in every industry are battling on a daily basis. On the one hand, organizational leaders chronicled unique and challenging security issues surrounding an array of emerging technologies that are rapidly being adopted by the enterprise. These transformational and disruptive technology challenges ranged from securing drones that perform inventory functions, to artificial intelligence and machine learning used for fraud detection, to securing industrial control systems and operational technologies. Most concurred that the adoption of new and emerging technology by the enterprise is often outpacing the ability of security teams to adapt and secure these new paradigms.

On the other hand, however, many of these same organizations were often more vocal about the difficulties spanning a range of traditional problem areas for cybersecurity leaders – finding and retaining expertise, adhering to increasing regulations, impacting organizational culture, and improving security operations were among the top pain points for most organizations. These challenges align with 451 Research's findings from recent VoTE surveys (see Figure 1), and will likely be a burden for security leaders for the foreseeable future.

Figure 1: Information Security Snapshot



Source: 451 Research, Voice of the Enterprise, Information Security: Organizational Dynamics, 2019; and Information Security: Workloads and Key Projects, 2019

Even so, several security leaders reported gaining ground in some of these trouble areas. The most notable area of success was in addressing staffing and expertise shortages. Recognizing that the shortage of security expertise will continue, and the skills needed from existing staff are quickly advancing, security leaders are looking beyond just hiring or developing more expertise. Automation and orchestration were cited as having one of the largest potential impact in addressing shortages in staffing levels. While approaches and strategies varied, most believed they had yet to realize the full benefits that automation and orchestration can deliver.

The growing visibility of technology offerings emphasizing artificial intelligence and machine learning was a topic of interest in addressing expertise and staffing shortages. Most security leaders believe that artificial intelligence and machine learning hold great potential in alleviating workloads and improving security operations, especially when combined with automation and human expertise. However, as promising as these emerging technologies are, most said they have yet to see significant impact from AI or ML in their security operations.

Leveraging managed security service providers (MSSPs) has proven to be an impactful tactic for several security leaders, citing access to on-demand expertise, access to advanced security technology, cost savings, and improved threat intelligence as key benefits. However, many indicated they have been reluctant to engage with an MSSP due to past experiences, fear of loss of control, or compliance concerns. Even so, staffing and expertise shortages and other demands are pushing them to consider leveraging managed security services for specific use cases in the coming year.

Leaders that were successfully engaging with MSSPs reported that their path to success with managed security services was often laden with trials and tribulations. Finding the right provider was key. Security leaders cited lack of transparency and collaboration, low detection rates, lack of integrations, and poor customer service as common problems with MSSPs. This should be a wake-up call for MSSPs as enterprises become more open to leveraging managed services.

Unfortunately, security leaders continue to face a plethora of security challenges that can be difficult to decipher and solve. The approach and technology that security leaders use to address the challenges of today and tomorrow can vary widely, both in terms of the solutions used and the level of success. While progress has been made in many areas, security leaders continue to look for opportunities to gain ground in their fight to protect their organizations.