CIO Executive Summary: Cisco Cybersecurity Report Series
Security and IT strategy go hand-in-hand. When CIOs and CISOs collaborate efficiently, organizations surpass their goals and securely implement their most promising opportunities.

What if CIOs could see into the future and know exactly what to do to protect their systems, employees, customers and entire infrastructures from security breaches? Adversaries these days are more clever than ever – but luckily, so are modern defense mechanisms.

When CIOs initiate proper implementation of strategic security improvements, the ability to anticipate the unknown becomes possible and powerful, and organizations are able to reduce risk exposure and gain more visibility into the threat landscape. Our 2019 CISO Benchmark Study looked at security practices from more than 3,200 respondents and showed that defenders are facing the following challenges:

1. The biggest thing keeping CISOs up at night is the difficulty of anticipating unknowns across the entire gamut of cybersecurity, including users, clouds and apps.

2. User behavior (e.g. clicking on malicious email links) is now the top concern for CISOs.

3. Email is the number one distributor for both malware distribution and phishing.
Preparing for unknown threats starts within the organization

While security leaders are certainly making strides forward in their commitment to build defenses, detect cyber threats and contain breaches, many are still struggling to implement other actionable strategies, such as vendor consolidation. Moreover, CISOs are collectively worried about how to prepare for unknown threats. Many are growing increasingly concerned about the number of user-initiated malware attacks – the majority of which occur via email.

Attackers nowadays are not only capable of using software to create emails that look eerily legitimate – they’re continuing to play on user’s emotions to get them to act. Unfortunately, the process of fully securing an entire email platform is tricky. Our research found that 56% of CISOs feel that defending against user behaviors is very or extremely challenging, which explains why the amount of organizations currently using email security as part of their defenses has dropped to 41% from 56% in 2014.

The silver lining is that proper employee training and education, multi-factor authentication, phishing exercises and other practical strategies can prove very effective in minimizing the amount of email threats that even come knocking to begin with.

Adversaries are not only becoming more adept at evasion – they’re weaponizing systems such as encryption, cloud services and legitimate internet services.
As the Internet of Things (IoT) and cloud services continue to expand, adversaries are exploiting these undefended gaps in security.

Defenders must be aware of the different types of attacks and the vulnerabilities of their cloud and IoT systems. Our research suggests that CISOs are showing less reliance on key technological tools used to secure the organization – namely, machine learning, artificial intelligence, and automation. It is likely this decrease is caused by the same technology now being built into products, which are utilized at a practitioner level. Regardless, CISOs are doing a better job at leveraging cloud security systems and increasing investments in company-wide security defense solutions.

93% turned to the cloud for increased security efficiency for their teams and allow them to be more effective.

What are defenders’ main challenges?

An organization’s ability to address and rectify security vulnerabilities is dependent on people, products and policies. In order to successfully manage all of these factors, security must be the foundation of every framework and be fully embedded into every layer of the organization. The tendency of many organizations to implement a complex mix of products and vendors makes it harder for systems to successfully orchestrate alerts and create single points of accountability.

79% of respondents said it was somewhat or very challenging to orchestrate alerts from multiple vendors.

Source: Cisco 2019 CISO Benchmark Study
Key takeaways for defenders

In order for CISOs to move past these cunning and ever-evolving roadblocks, they must focus on creating foundational security strategies that strengthen every cog in an organization. These strategies necessitate a commitment to:

1. Collaborating across siloes in order to fully understand all underlying security needs

2. Relying on ML, AI and automation to exponentially improve security efforts across the organization

3. Implementing practical strategies for developing security budgets

4. Mandating regular company-wide educational and phishing exercises to significantly decrease cases of user-inflicted malware

5. Taking a three-pronged approach to improving defenses against phishing and other email attacks that includes employee participation, standardization of operating procedures and secure controls

For more information on how to jumpstart your digital transformation, download the CSO Benchmark Study and the Cisco Cybersecurity Report Series, visit cisco.com/go/securityreports