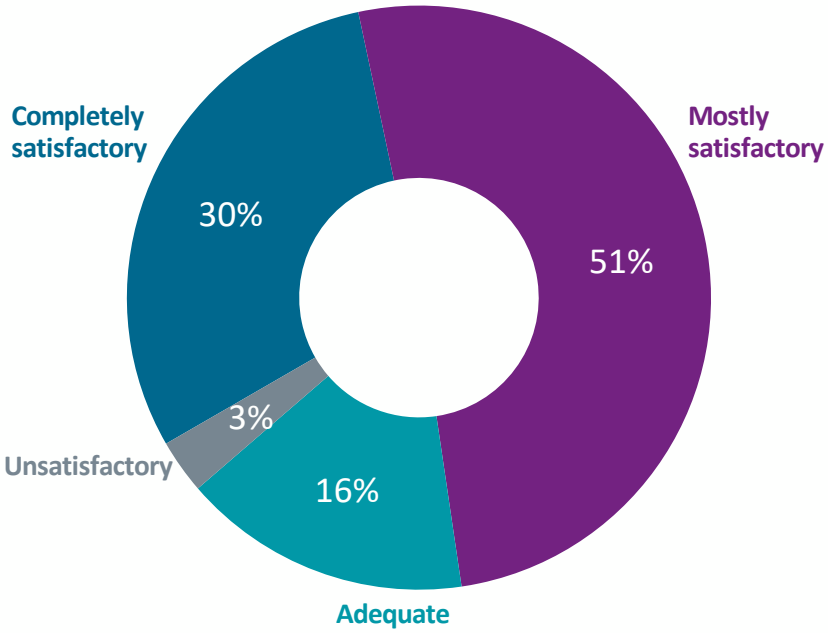
STATE OF CYBERSECURITY 2022: ASEAN

Over the past year, the business world has been adjusting to lessons learned from the COVID pandemic. On a workforce level, companies are struggling to decide the best ways to balance employee flexibility and corporate culture. On a technical level, the many benefits of a cloud-first architecture are being weighed against the challenges of managing complexity and cost in a multi-cloud environment. It will still be years before we understand what equilibrium looks like in the post-pandemic environment, but the early changes point to a significant restructuring.

Another prominent takeaway from the pandemic is that symptoms are often easier to diagnose and treat than root causes. This obviously has implications beyond corporate strategies, but a prime example of this concept in the business world is the field of cybersecurity. Companies are made all too aware of poor cybersecurity when they are breached, and a postmortem can identify processes or tools that would have prevented or mitigated the attack. But that may not address underlying problems that can lead to a different cyber incident down the road.

CompTIA's 2022 State of Cybersecurity report examines the disconnect between root cause and symptoms. Digital transformation driven by cloud and mobile adoption is forcing a new strategic approach to cybersecurity, but fully adopting this new approach poses significant challenges, both tactically and financially. Although cybersecurity remains one of the most pressing issues for modern business, the hurdles that come from legacy views of IT and low understanding of the threat landscape make it difficult to follow the prescribed treatment.

Satisfaction with Organizational Cybersecurity



INTEGRATING A ZERO TRUST APPROACH

In many ways, the field of cybersecurity is a reaction to the ways that enterprise IT evolves. After all, the need for cybersecurity only comes after technology has been implemented. This dynamic has intensified in recent years, as businesses aggressively pursue technology with the tendency to treat cybersecurity as a secondary consideration.

One way that cybersecurity mirrors the evolution of enterprise IT is that both have become more strategic. When it comes to overall IT, organizations are generally embracing the transition to a more strategic approach, even if there are some growing pains along the way. Cybersecurity, on the other hand, is proving a bigger challenge when it comes to adopting a strategic mindset.

One of the most significant parts of a strategic mindset is recognizing that cybersecurity is no longer focused primarily on external events. When examining the issues driving cybersecurity, most of the top issues cited are outward-facing. The focus on volume, variety or scale of attacks is a focus on things happening outside the business. Even concerns around privacy are concerns around external expectations. There is lower recognition that cybersecurity is attached to the changing nature of internal operations, such as a growing reliance on data or a need to maintain compliance with changing regulations.

Over the next year, there will be a concentrated move toward integrating cybersecurity with business operations. Accepting cybersecurity as a critical component of digital transformation will drive new questions and new measures of success throughout the organization. At the same time, adopting a holistic viewpoint will address many of the existing hurdles around changing the approach to cybersecurity.

The introduction of cloud computing and mobile devices drastically altered the viewpoint of a secure perimeter, which had been the dominant mindset for decades. As organizations grappled with the paradigm shift, part of the difficulty was in defining a comprehensive approach that informed a wide range of cybersecurity decisions. Zero trust emerged as the answer to that dilemma.

This year, zero trust is starting to move from broad policy into tactical processes. For several reasons, adoption of zero trust will not take place overnight. First and foremost, zero trust represents a drastically different way of thinking about cybersecurity. Rather than viewing cybersecurity as one of many components within the IT function and simply investing in hardware or software, companies must now view cybersecurity as an organizational imperative, extending beyond technology products into decisions around workflow and workforce.

Cybersecurity Practices in Place

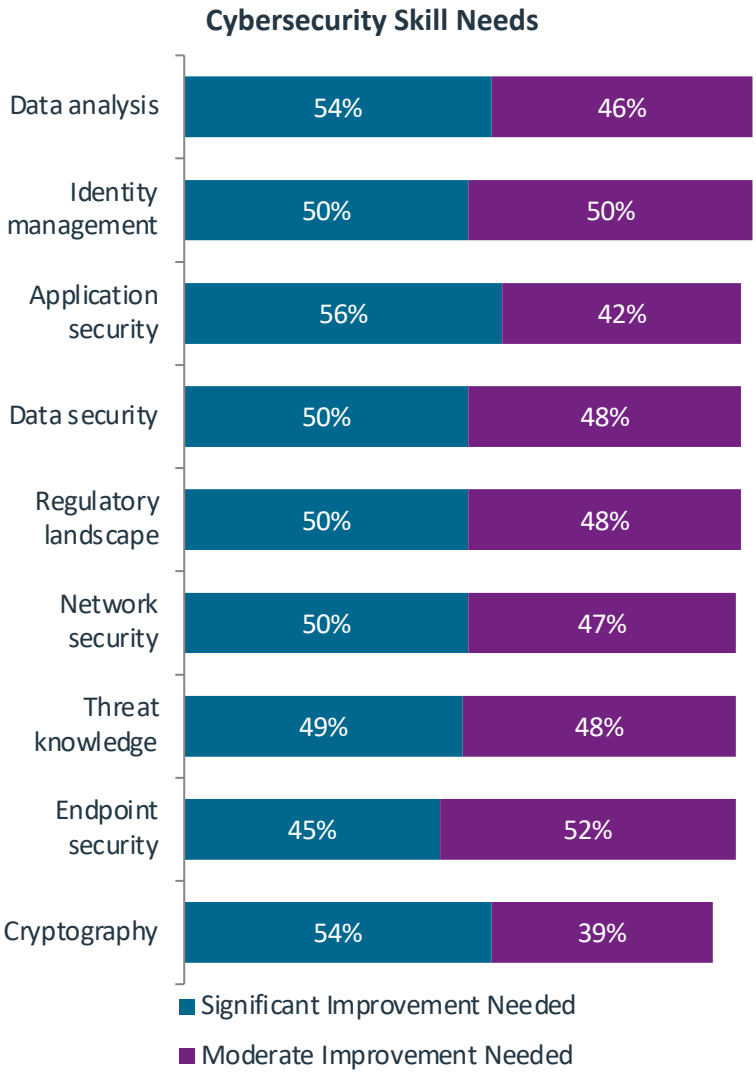
Zero trust is not a single product or action, and many discrete tools and practices can be part of a zero trust approach. Looking at components that typically fall under a zero trust umbrella, there are more organizations that recognize individual parts vs. the collective whole. Multifactor authentication, one of the best tools to validate trusted identity, is in place at 50% of organizations. Cloud workload governance, a process that ensures cloud resources are being used according to plan, is in place at 46% of organizations. Other elements, such as software-defined microsegmentation (47%) and least-privilege access (29%) are also outpacing broad awareness for a zero trust policy.

The main takeaway is that zero trust is a philosophy around cybersecurity that informs questions and decisions. The best way to adopt zero trust is not to define a set of criteria that indicate complete success, but to build a road map identifying the best steps to take based on the status of the organization. Those steps might include a full audit of data and workflow, implementation of specific products such as identity and access management (IAM) software, or creation of an ongoing workforce education program. Each step should address a specific question, and each step should have measurable outcomes.

TYING PEOPLE AND PRODUCT INTO STRATEGY

As businesses try to address the root cause of their security shortcomings, they discover that the problem has multiple layers. There is obviously the technical layer, which has been the focal point for years and continues to be a substantial part of a cybersecurity solution. There is also the workforce layer, and many companies have turned to cybersecurity awareness education to improve this aspect. However, other layers dealing with business operations and corporate measurements have likely received less attention in recent years.

As companies focus on cultivating the cybersecurity chain to include all layers of the organization, technical specialists will always be a critical component. After performing a thorough assessment of skill gaps, improving skills is the next challenge. Network security may seem like an area with deep expertise since the task has been performed for a long time, but the reality is that changes in the IT landscape demand constant improvement. Other areas such as threat knowledge, data analysis and identity management are more obvious candidates for skill growth since they represent more recent trends in cybersecurity.



The cybersecurity product list starts with pieces that have been around for a long time. Firewalls, antivirus and anti-malware were the primary components of the secure perimeter, and they still serve that function even as the secure perimeter has dropped in importance. These tools are ubiquitous, although many end users (and possibly even IT staff) may not think of them as part of the product set since they are so common.

Network monitoring is another tool with a long history and another tool that is evolving to fit the times. Tools such as SolarWinds Network Performance Monitor, Datadog Network Monitoring and Auvik offer extensive capabilities for observing and analyzing an entire network architecture. Recent features in network monitors include visibility into cloud components of the network and analytical tools to better understand data flow.

Highlighting the importance of cloud systems, SaaS monitoring and management tools are quickly gaining traction. Acceleration in cloud adoption was one of the largest shifts in IT operations during the pandemic, and companies are now responding to the second-order effects of that activity. Along with cybersecurity issues, cloud systems come with a unique set of concerns around utilization and cost, and new management software is needed to properly administer, orchestrate and secure cloud architecture.

On the other end of the spectrum, there are tools that still have low adoption rates but should be strongly considered as imminent additions. Although SaaS is the most popular form of cloud adoption, IaaS is also prevalent and may be more critical for proper monitoring and management. Comprehensive network monitoring tools are crucial for providing a view of the big picture, but packet sniffers and LAN analyzers are targeted products that can root out hard-to-find problems.

With so many tools in the arsenal and so many constraints on cybersecurity personnel, the obvious next step is automation. Automation cuts through the complexity of multi-product adoption, but it does not necessarily remove the need for cybersecurity specialists. New expertise is needed to properly implement automation and perform ongoing adjustments as needed.

Even if automation does not completely solve the resource issue, it makes the situation more manageable. Integrating cybersecurity with business operations makes cybersecurity even more critical than ever, and implementing a zero trust philosophy leads to a range of new processes. A dedicated organizational structure and the proper tool set are the first steps in tackling added complexity. By adopting a balanced approach to automation, organizations can fully address their underlying difficulties and move towards a healthy cybersecurity outlook.