NOBODY KNOWS CYBERSECURITY BETTER

SHI

cisco Partner

Security

Ready, Set, Secure – The Complete Approach to Cybersecurity

While technologies for protecting devices and data have been widely adopted, more progress is needed across identity, networks, and apps.

How Ready Is Your Organization?

Among the results on a study across 27 market participants, device security had the highest percentage of companies in the mature category at 31%. A similar trend was observed when it came to data security with 22% of organizations globally ranking mature.

Application workloads were the biggest drag on overall readiness. Only 12% of the organizations globally were ranked mature. As with identity management and the network, the challenge is deployment, with more than half of companies at either the Formative or Beginner stage.

Readiness varies across company sizes in an interesting way. The data shows that globally mid-sized firms of between 250 and 1,000 employees are best prepared, as well as those in emerging markets. This suggests that while larger organizations may have bigger budgets, they typically require more complex deployments, which can take longer to implement. It highlights that 'tech debt' continues to be a major driver of the readiness gap.

Those in sectors with the most to lose tend to have more companies in the Mature state of readiness, including healthcare (18%) and financial services (19%). However, it is retail, with 21% of organizations in the Mature category, that comes out on top.

A bright spot in the data is that 88% of organizations that have not yet deployed solutions plan to do so within the next two years– getting closer to "full coverage".

When the consequences of cyberattacks are so clear to see, readiness must be a priority for all organizations and deployment of solutions needs to be accelerated across all pillars. Let's look at some organizations doing this well.

A Secure and Seamless Patient Experience

Vulnerabilities and risks can emerge from anywhere, which is where Zero Trust comes in as a guiding principle on decisions, policies, and best practices.

As one of the best children's hospitals for orthopedic and pulmonary specialties, Dayton Children's Hospital (DCH) needed a robust IT infrastructure and cybersecurity to keep its two campuses and 20 remote sites protected.

DCH has about 25,000 IoT devices across its network, so it's critical to ensure each device is reliable, secure, and always visible. Whether it's a smart TV, security camera, MRI machine, or robot aid for the hospital's neurosurgeons – each remote device needs protecting.

After an initial gap analysis, DCH deployed Cisco Secure Network Analytics for faster, simpler, cloud-based network monitoring alongside Cisco Umbrella to extend the hospital's security footprint.

Holistic Transparency and Compliance

As financial services face significant scrutiny and stringent legislation, Lake Trust Credit Union needed to elevate its digital security to protect its hybrid workforce, customers, and digital assets.

Implementing Cisco security solutions gave Lake Trust unified visibility across users and devices for a single point of oversight and control, making sense of the spaghetti integrations that stemmed from multiple mergers and disjointed systems.

Cisco improved Lake Trust's threat hunting as the company can quickly isolate infected environments, take them offline, and rebuild a server from its backup system. Security event investigations that previously took eight-plus hours now take minutes.

Protecting an Expansive Network

Owner and operator of 62 shopping centers across Australia, Vicinity Centres was significantly impacted by the pandemic and its drive towards remote working. This shift was an important opportunity to reframe security measures across cloud edge and IT infrastructure.

Implementing Cisco Umbrella ensures Vicinity Centres can securely provide guest Wi-Fi for shoppers alongside the various digital elements that

connect directly to the internet – such as digital wayfinding, digital media screens, and even counters that measure foot traffic.

Today, the company has reduced internet outages and investigation times while securing remote workers, shoppers, and other users' web activities.

Reflecting on the Stats

A common point highlighted across each of these transformation stories is the importance of implementation– the ability to outline risk-management benefits and tie them to direct impacts and improvements for frontline staff.

While some of the statistics from the Cybersecurity Readiness Report may seem deflating, there are some key takeaways that we can learn from the companies, segments, and markets more prepared for cybersecurity resilience.

With Cisco's integrated security portfolio and recent innovations, it's clear that the company that connected the world is here to make sure it's protected across every pillar.