CIO Essential Guidance

The CISO security threat landscape

Table of Contents

Understanding the Challenges of the Threat Landscape

Rick McElroy,
Principal Cybersecurity Strategist,
VMware Security Business Unit

The cybersecurity professionals who contributed to the fourth edition of our Global Security Insights Report are in a very different position than when they answered the 2020 survey. After a year that saw the largest and fastest transformation in work patterns in history, security teams now preside over an ecosystem that is more distributed and heterogeneous than ever before.

Digital transformation programs advanced rapidly as the cyberattack surface expanded to include living rooms, kitchens, home networks, and personal devices. The remote workforce behaves very differently to the office workforce, accessing the network at unpredictable hours as they balance the demands of work and family. As a result, network traffic has changed beyond recognition. Defenders must adapt monitoring systems and trigger points, or risk leaving opportunity for threat actors to use atypical patterns to mask infiltration attempts.

Against this rapidly changing backdrop, some things remain the same: One industry that was not disrupted by COVID-19 is cybercrime.

The frequency of attacks is high, sophistication continues to evolve, and breaches are the inevitable result.

Three-quarters (76 percent) of the 3,542 respondents to our survey said the number of attacks they faced has increased in the past year. Of those, 78 percent said attacks had increased as a result of more employees working from home. 79 percent said attacks had become more sophisticated.

The result? The number of breaches has risen, with respondents who had a cyberattack reporting 2.35 breaches on average per year. These were not minor incidents. In eight out of 10 cases, the breach was a material incident requiring reporting to regulators or the involvement of an incident response (IR) team.

Clearly, security teams are under pressure, and there is little complacency: 56 percent of the CISOs surveyed fear that their organization will experience a material breach in the coming year.

The importance of brand and reputation

Brand and reputation remain the holy grail for businesses, both of which are easily lost. In fact, the reputational impact of security breaches outstrips financial impact.

75% of those who suffered a cyberattack say there was a negative impact on reputation.

82% of respondents had to report to regulators or engage an IR firm to overcome the reputational problems caused by material breaches within the past year.

CISOs need better visibility

Not only have cyberattack volumes grown, but the rapid pivot to remote working means businesses are not seeing the full picture. Erratic employee behavior, personal devices, and home network use reduce visibility, creating blind spots and dark corners where attacks go undetected.

78%

said attacks increased as a result of home working.

2.35

breaches on average have been reported per organization in the last year.

82%

said they had suffered a material breach.

Third-party apps and ransomware among leading breach causes

When asked what is causing breaches, three vectors almost tied at the top to build a picture of external threats and internal weaknesses. Third-party applications were the most common culprit, followed closely by ransomware and out-of-date security technology.

The rapid pivot to work from anywhere has exposed organizations that had lapsed in security hygiene and failed to implement multifactor authentication, while process weakness and OS vulnerabilities were also common breach causes.

In addition to these threats, the rapid escalation in ransomware has added unwelcome tension. Multistage campaigns involving penetration, persistence, data theft, and extortion are ramping up pressure as attackers capitalize on the disruption faced by remote workers. In most ransomware attacks, email continues to be used as the most common attack vector to gain initial access.

Third-party apps are the leading cause of breaches according to our surveyed CISOs. So, it's not surprising that security teams are focusing on sharpening their approach to consuming and developing them.

Almost two-thirds of respondents agree they need better visibility over data and apps to prevent attacks. A similar number agrees that better contextual security is needed to track data security through the application lifecycle. The impact of COVID-19 can't be overstated as three in five respondents agree they need to view security differently than they did in the past due to an expanded attack surface. Apps also topped the list as the most vulnerable point on the data journey.

Security concerns stifling business innovation

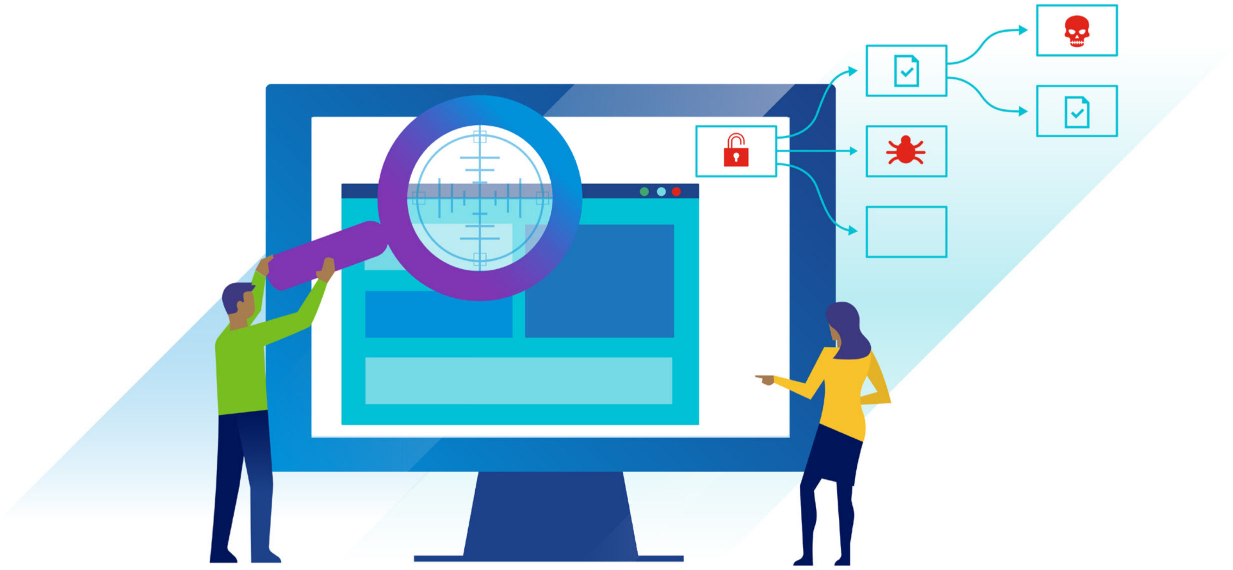
Another stumbling block: the perceived difficulty in securing AI-based apps. AI is the next frontier for business innovation as businesses seek an edge to drive more competitive customer services and digital experiences. According to our survey, however, more than half of respondents worldwide (56 percent) agree security concerns are holding them back from embracing AI-based apps.

Workloads as a source of perceived vulnerability

15 percent of respondents said workloads were the most vulnerable breach point in the data journey at their organization, noting this wasn't the case 12 months ago. A further four percent said they had been the most vulnerable point for more than 12 months.

Teams are recognizing that traditional antivirus fails to secure server workloads, and misconfigurations are a significant breach risk. This often arises due to a knowledge gap between security teams and infrastructure teams. Security teams don't know how production workloads are expected to behave, and infrastructure teams aren't experienced in recognizing attacker behavior. This year, we anticipate organizations will be looking to address these gaps and strengthen defenses for workloads in the cloud.

On the topic of cloud, our research finds an inexorable shift is underway. Almost all the CISOs we surveyed either already follow a cloud-first security strategy, or plan to do so very soon. This is a considerable shift and shows that organizations are accelerating their cloud security roadmap in response to the challenges of COVID-19. It may be a road they were already traveling, but they are putting their foot on the gas in recognition of the imperative for comprehensive cloud-first security for a cloud-first world.



5 Ways to Mitigate Your Risk

When it comes to mitigating breach risk, respondents said they were prioritizing simplification and consolidation of security solutions by building security into applications from the ground up. Updating technology and policy and committing budget to the issue were also important.

Almost half of respondents (43 percent) said they plan to build more security into their infrastructure and apps, and reduce the number of point solutions. This rose to 48 percent in the retail and food and beverage sectors.

1. Prioritize improving visibility

The true scale of attacks is often hard to discern because defenders can’t see into the corners where personal mobile devices and home networks have been grafted onto the corporate ecosystem. Add to this the challenges of monitoring third-party apps and vendors, and the number of blind spots escalates.

Put simply, defenders don’t know what they don’t know, and businesses are exposed as a result. This limited contextual insight into risk puts defenders at a disadvantage when protecting the extended attack surface. Organizations must prioritize improving visibility into all endpoints and workloads to secure the remote work environment. Robust situational intelligence that gives context to threats will help defenders prioritize and remediate risk with confidence.

2. Respond to the resurgence of ransomware

Cyberattacks have continued to increase in sophistication, and ransomware is no exception. Attackers are gaining undetected access to networks, exfiltrating data, and establishing back doors before launching ransom demands and/or directly monetizing stolen data. To avoid becoming victim to repeated attacks, organizations need to combine advanced ransomware protection with robust post-attack remediation that detects the continued presence of adversaries in their environment.

3. Address ineffective legacy security technology and process weakness

Out-of-date security and process weaknesses continue to pose significant risk to organizations, and the switch to remote working has exposed them further. As we emerge from the immediate response phase and begin to see the shape of the long-term future, organizations must identify the critical changes to processes and technology needed to support remote and hybrid workers to work securely and reduce risk.

The good news is that there is recognition of a fundamental shift in security for a highly connected, remote work-supporting, digital age.

61% agree they need to view security differently as the attack surface has expanded.

63% agree they need better contextual security in place to track data through the lifecycle.

63% agree they need better visibility over data and apps to preempt attacks.

4. Deliver security as a distributed service

There was a time when security teams were securing company-owned desktops for employees working on campus, connecting to corporate applications running on servers in a company-owned data center. The world is a more complicated place today with remote workers connecting to applications running on infrastructure that may or may not be managed, owned or controlled by the company.

With so many new surfaces and different types of environments to defend, security cannot be delivered as a litany of point products and network choke points. Instead, endpoint and network controls must be delivered as a distributed service. This means delivering security that follows the assets being protected, no matter what type of environment you have.

5. Build cloud-first security into applications

The biggest change uncovered by our research is the shift to a cloud-first security strategy. It is difficult to overstate the changes that have occurred in such a short space of time; very few CISOs before 2020 described their security strategy as cloud-first. Of course, many organizations shifted focus to the cloud to support a remote workforce due to COVID-19.

Moving to the cloud presents its own security concerns. Not all clouds are equal, and controls need to be vetted by consumer organizations because if adversaries want to attack at scale, the cloud is the place to do it. As this shift builds momentum, investment in public cloud security will be critical.

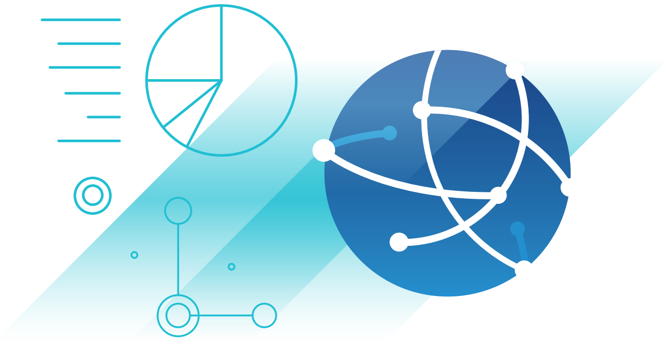
When you move to a public cloud, you're moving to a very tough neighborhood where security is contingent on your own actions and those of your neighbors. You may be able to secure your own resources, but you have no control over those sharing that environment with you. Organizations must prioritize securing cloud workloads at every point in the security lifecycle as the great cloud shift continues.

The CIO Takeaway

Our fourth Global Security Insights Report finds that senior cybersecurity professionals and the organizations they serve continue to face high-volume, sophisticated threats. These are exacerbated by the pivot to a highly distributed workforce and, though most organizations have managed to shift to remote working, CISOs acknowledge that a security-first approach would have made the transition easier.

The report reveals an industry that is now focused on building on gains from the last year and responding to the changing threat environment. As risk has intensified, innovation has stepped up to match it. CISOs are now keenly aware of lessons learned and taking steps to get the tools they need to help stay one step ahead of attackers.

About the 2021 Global Security Insights Report



VMware commissioned a survey, undertaken by an independent research organization, Opinion Matters, in December 2020. 3,542 CIOs, CTOs and CISOs were surveyed from companies in a range of industries, including financial, healthcare, government and local authority, retail, manufacturing and engineering, food and beverage, utilities, professional services, and media and entertainment.

This is the fourth Global Security Insights Report from VMware, building on the previous surveys that were undertaken in February 2019, October 2019 and June 2020. This forms part of a global research project across 14 countries, including Australia, Canada, Saudi Arabia, the Middle East, the United Kingdom, France, Germany, Spain, the Netherlands, the Nordics, Italy, Japan, Singapore, and the United States.

About VMware

VMware software powers the world’s complex digital infrastructure. The company’s cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit vmware.com/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com