THE CIO's GUIDE TO SECURITY IN THE NEW HYBRID WORKFORCE

eBook

Gold
Microsoft Partner

Microsoft

DATAPRISE

DATAPRISE

Introduction

For businesses, one of the biggest upheavals of the COVID-19 pandemic was a major shift from office-based workspace to remote working habits. As the pandemic recedes and offices once again become safe to open, it seems the old way of working is gone forever.

Today, 73% of workers want flexible remote options to continue, but at the same time, 67% of employees want more in-person work or collaboration in the post-pandemic world. To meet this mixture of demands, businesses will likely adopt a hybrid model, where workers divide their time between the office and other environments of their choosing.

In fact, change is already underway — 63% of leaders say their company is considering redesigning office spaces for hybrid work. Plus, research from Microsoft has found that 76% of companies now have a set remote work policy, compared with just 16% last year.

An increase in remote work will naturally lead to an increase in cyberattacks, too, thus forcing security teams to rethink many of the old approaches to cybersecurity.

In this ebook, we'll take a look at what's changed in cybersecurity, the challenges facing security teams, and how companies can successfully adapt to this new landscape.

Security in a Hybrid Workplace

What does a new hybrid workplace model mean for security? It introduces a range of brand new threats and challenges that organizations must address.

Cybercriminals are increasingly focused on remote workers, taking advantage of the lack of security on individual devices and home networks. Attack vectors like phishing, insider threats, and taking advantage of outdated software are all major issues in 2021.

"You'll see some stats about how ransomware attacks have gone down, but what's happened is they went from the shotgun gun effect to more sniper-type, more measured. They're going after groups where they think they're going to get paid the most. So they're wasting less of their time," explains Jeff Wheat, CISO at Blue Team Alpha, Dataprise's partner in incident response.

Attacks focus on major financial targets first and gravitate towards health care data, particularly embarrassing personal information that can be held for ransom.

One of the most concerning threats of all is a focus on advanced persistent threats (APTs), where a bad actor reverse engineers security patches on platforms like Windows to identify the original exploit, rewrite the code, and then sweep all the exchange servers on the planet to target all those who haven't patched it yet.

According to a report by Microsoft,

73% of CISOs

said they had encountered data leaks in the last 12 months and planned to spend more on insider risk technology due to the pandemic.

What's Changed in 2021

In the very recent past, remote workforces were relatively uncommon. Before the pandemic, 47% of workers never worked remotely and only 17% did it full time. By mid-2020, 44% of workers were fully remote.

As the pandemic recedes, these numbers will likely decrease, but only a little. Research by Gartner suggests that 82% of company leaders plan to continue to allow employees to work remotely at least some of the time.

Among its many benefits, offering employees the option to work remotely allows companies to save money by migrating to the cloud instead of maintaining expensive offices in major cities — a significant move from a security perspective.

According to a report by Microsoft, 73% of CISOs said they had encountered data leaks in the last 12 months and planned to spend more on insider risk technology due to the pandemic. With new data leaks come new challenges, and businesses will need to adapt and find innovative solutions.

DATAPRISE

How to Stay Ahead of the Bad Guys

Wheat talks about the importance of identifying your organization's "crown jewels," finding out what attackers will value the most, and putting endpoints in place. Techniques like forensic imaging can be used to secure these critical assets.

He also stresses the importance of prioritizing education and ensuring your team understands where the risks are coming from, what they need to do (and avoid doing) to maximize security, and what security solutions they are buying.

When choosing a cybersecurity company to work with, ask for examples and proof of efficacy. Read the insurance fine print and do your prior research.

Perhaps most importantly, plan for the inevitability of an attack. Don't wait until a crisis emerges to act — go through a tabletop exercise and drill for different scenarios.

Wheat suggests taking lessons from the U.S. military: study the terrain and hazards, then train for all potential challenges. He says, "If everyone knows what they're supposed to do — and that's why the U.S. military does well, because they train and train and train — when bad stuff happens, there's less emotion-fallback on your train."

Key decision-makers must remember that threats can come from anywhere. Layered defense is essential, and you need to look at endpoints first and work within your budget.

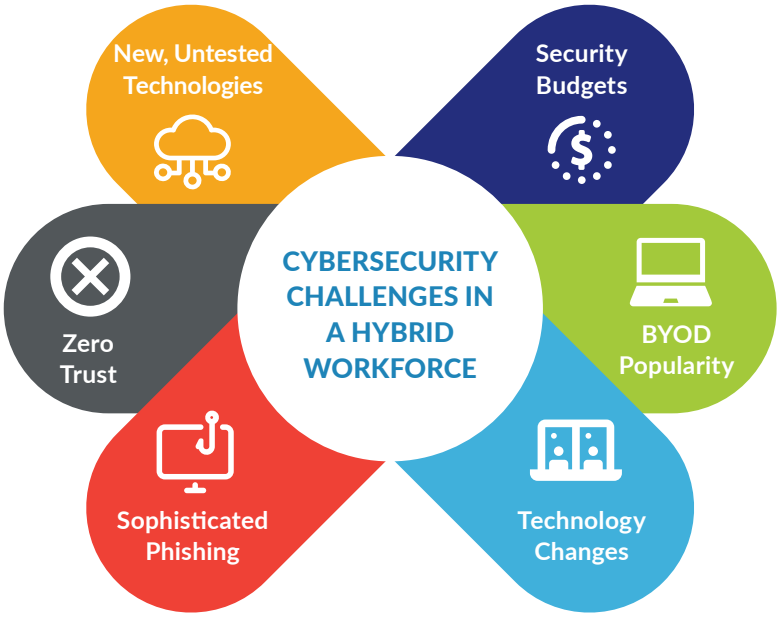
Cybersecurity Challenges in a Hybrid Workforce

As we enter a new digital landscape and a rapidly changing world, cybersecurity teams need to do everything they can to prepare for new attack vectors, a range of threats, and unprecedented challenges.

If your company plans to shift to either a fully remote or hybrid workplace model, you should first consider the following six most critical cybersecurity challenges:

Security Budgets

Recently, security budgets have been trending downward for many companies. However, in a new era with new risks, it's essential that businesses consider shifting to more-effective security models — for example, to zero trust security architectures that provide effective protection for distributed workers. Naturally, this costs money.



Fortunately, there are a number of money-saving solutions. In a remote world, it's no longer necessary to maintain large office spaces to house entire companies. Downsizing can free up real estate costs and real locate the funds to cybersecurity. Moving to SaaS platforms, thereby eliminating the need to store every thing on the premises, can also free up money for security.

Steve Jones, Senior Director of Cybersecurity at Dataprise, helps companies stay secure and competitive with managed services. He says the most important thing is to treat security as a core value. Stop treating it as an optional extra and an easy target for budget cuts. In today's world, it's essential to take cybersecurity seriously and allocate budget accordingly.

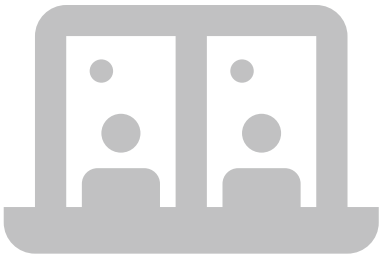
Dataprise's Security Operations Center encompasses a team of cybersecurity analysts and threat hunters using advanced security information and event management (SIEM) technology to rapidly identify and respond to anomalies. With this fully managed solution, midmarket organizations no longer need to weigh the pros and cons of building an in-house SOC – Dataprise seamlessly acts as an extension of an in-house team or assumes full responsibility.

BYOD Popularity

BYOD — bring your own device — policies have increased massively. In fact, the global market for BYOD and enterprise mobility is expected to spike by more than 21.1% through 2020. That said, BYOD isn't a completely accurate description anymore, since employees aren't "bringing" their devices anywhere, they're simply accessing them from home.

There are many challenges with applying patches to devices outside the office and keeping security software updated. Company-issued devices can be tracked, providing visibility for security teams, but many people are using their own personal laptops, tablets, and phones to access sensitive company data from their own home networks.

The only modern-day solution is endpoint software that controls access to networks and forces individual users to meet certain standards and authenticate each session every time.



Technology Changes

The hybrid work model depends on a range of new technologies and tools to function. While these tools are no doubt incredibly useful, they can also represent security risks if organizations fail to do their due diligence.

Many of the SaaS platforms that modern businesses rely on to run their operations effectively with a distributed workforce are exposed to security risks and vulnerabilities. When the pandemic began, for example, and millions around the world were forced to work and telecommute from home, Zoom usage exploded.

During Q1 2020, Zoom saw a growth of 354% , placing an enormous target on the company's back and encouraging hackers to try to gain access to confidential company meetings and steal valuable data.

Your best solution is to be extremely careful when choosing SaaS providers. Do your homework and look into their policies, mechanisms, encryption, and more. Who has the encryption keys? Can they be trusted? What kind of security controls does the platform use?

Failing to exercise appropriate caution here risks putting your company's resources in danger. It's not something to gloss over.

Sophisticated Phishing

One of the most significant security trends of 2020 was a record increase in phishing scams. Google detected 2.11 million phishing sites in 2020, a 25% increase from 2019.

On top of that, cybercriminals are using the pandemic as a tool in their phishing attempts. Sixty-four percent of businesses are anticipating an increase in COVID-19-related phishing emails in 2021, preying on the fears and preoccupations of their targets.

Among the many factors behind this surge is the increase in email communication that has followed the rise in remote work, giving phishers more opportunities to attack.

We've also observed more sophistication in phishing attacks. Jones tells a story about an email he received, supposedly from his own CEO, asking him to buy gift cards because he was in a meeting and unable to do so.

He says, "Not all users or employees are trained enough in spotting stuff like that. They see the CEO's name and some people are enticed to do whatever's being asked of them."

Google Detected

2.11 Million

phishing sites in 2020, a 25% increase from 2019.[8]

DATAPRISE

This kind of attack is much more credible and dangerous than traditional phishing scams, which were easy to identify and avoid. The good news is organizations have a wide range of solutions at their disposal to combat phishing scams, including mail gateways, effective DMARC settings, and company-wide education to make team members aware of security.

The latter must take place on a regular basis as phishing scams evolve and as we learn more. It's also important to incentivize completion of the learning to maximize participation and encourage openness and safety as a company value. In today's world, it only takes one naive or inexperienced employee to cause a data breach and a huge amount of damage to the organization.

Zero Trust

The main challenge when it comes to securing a distributed network is ensuring that users can safely access critical data from a network that the company has no control over.

The only way to do this effectively is by using a zero-trust approach; in other words, assuming that no user of the network is implicitly trustworthy until they prove and authenticate their identity. Authentication must be required every time anyone attempts to access company resources, whoever and wherever they are.

Microsoft also talks about the need for "device-based security" and the importance of protecting sensitive company data on endpoint devices.

As Jones explains, "We're seeing a shift to things like zero-trust, which is where we're not relying so much on physical boundaries, but we're relying on proving identity in order to access things."

Organizations, then, will have to build their own mechanisms for monitoring all users of the network and ensuring each one is authorized every time they access data. Without gaining full visibility over your users and assets, you'll always be at risk in a hybrid working model.

Jones says, "A lot of new technologies are sprouting up to solve some of these problems, which is great — it really shows the ingenuity out there and the creativity." However, he adds that "a lot of these technologies are a bit newer, so this is another risk that we're taking."

Core Zero Trust Scenarios from Microsoft

Scenario 1
Applications and services can validate multifactor authentication and device health.

Scenario 2
Employees can enroll devices into a modern management system that enforces device health to control access to company resources.

Scenario 3
Employees and business guests have a secure way to access corporate resources when using an unmanaged device.

Scenario 4
Access to resources is limited to the minimum required—least privilege access—to perform a specified function.

1 https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work
2 https://news.microsoft.com/europe/features/flexible-ways-of-working-are-here-to-stay-finds-new-european-research-with-leaders-focused-on-maintaining-culture-and-innovation/
3 https://www.statista.com/statistics/1122987/change-in-remote-work-trends-after-covid-in-usa/
4 https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time
5 https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/
6 https://www.prnewswire.com/news-releases/global-byod-and-enterprise-mobility-market-2021-2027-logistics-travel--transportation-sectors---high-potential-verticals-301246467.html
7 https://www.theverge.com/2020/6/2/21277006/zoom-q1-2021-earnings-coronavirus-pandemic-work-from-home
8 https://www.techradar.com/uk/news/2020-was-a-record-year-for-phishing-sites
9 https://www.fsmatters.com/Firms-fear-COVID-themed-phishing-attacks
10 https://pulse.microsoft.com/en/work-productivity-en/na/fa1-device-based-security-for-the-new-hybrid-workforce/

New, Untested Technologies

As technology rapidly advances, many of the new tools and solutions we use are untested and potentially vulnerable to attack. Companies are increasingly relying on cloud technologies like AWS and Azure, and it's too early to say what new boundaries we'll hit and what security issues we'll run into.

For Dataprise, the solution is focusing on quality and striving to be the best at everything they do. Jones talks about the importance of getting the foundations right, ensuring the building blocks of security are solidly in place before trying to add anything else. "That way," he says, "everything that we build on top of it will stand."

Too many companies skip this stage and jump ahead to incredibly advanced solutions like AI without investing time into building reliable foundations.

A Message to Security Teams

Cybersecurity is more important than ever before. With the radical changes that have taken place in the last year, companies simply cannot afford to keep doing the same things they were a year or two ago.

It's critical for security teams to push their leadership to prioritize security. Ensure they are fully aware of the risks and what is at stake, and do everything you can to secure the necessary support and funding to keep your company safe in 2021 and beyond.

It's our job to push executive leadership to really prioritize cybersecurity right now. In the future, we're only going to get more connected — it's our job to encourage that and to be the ambassadors for our organizations.

– Steve Jones

To find out more about how Dataprise can help your organization prioritize cybersecurity and ensure they have all the tools and resources they need to survive in a hybrid workforce, contact us.

DATAPRISE

DATAPRISE

About Dataprise

Founded in 1995, Dataprise is the leading strategic IT solution provider to midmarket IT leaders who believe technology should allow you to be the best at what you do. Dataprise's unbeatable IT solutions and services are tailored to the needs of strategic CIOs and provide best-in-class managed security, network, infrastructure, collaboration, and end-user solutions. Dataprise has offices across the United States to support our clients.

About Dataprise Managed Cybersecurity

Dataprise Managed Cybersecurity solutions provide the real-time detection, validation, reporting, and response capabilities needed to protect an organization's IT environment from end-to-end.

We expertly combine a world-class **managed detection and response** with a complete cybersecurity program to increase visibility, shut down bad actors quickly and dramatically mprove your total security posture.

Beyond next-gen cyber technology, you get **an elite security team** defending and protecting your organization 24x7 at a fraction of the cost of building the capability in-house. Our security professionals, analysts and hunters are always on and ready to detect, investigate and remediate any threat, any time.

Let's Talk Cybersecurity:

CLICK HERE >

1-888-519-8111 | dataprise.com