Secureworks®

WHITE PAPER

The Evolving Workplace and its Implications for Cybersecurity

Explore the Cybersecurity Risks of Working from Home and the Challenges of Rapid Organizational Change

With the onset of the COVID-19 global pandemic, the structure of workplaces has evolved rapidly, oftentimes without warning. Accelerated digital transformation to the cloud has meant both working from home (WFH) and bring your own device (BYOD) policies have become commonplace for many organizations. And with that, new cybersecurity challenges have arisen. For business leaders, understanding how to address these challenges and mitigate cyber risk is more essential than ever. For instance, ransomware remains an existential threat and the March 2022 FBI Internet Crime Complaint (IC3) report[1] for 2021 showed there was a 7% increase in complaints and cybercrime losses from all sources exceeding $6.9 billion!

86%

of all organizations victimized by a successful ransomware attack in the last 12 months failed to recover all their data after paying a ransom.[3]

58.6%

of the total American workforce are currently remote workers.[4]

The Evolution

The many "fully remote" employees hired during the pandemic and the "Great Resignation" mean the business world is witnessing a permanent workplace transformation. In addition to remote working, organizations are also adopting BYOD, which has seen an explosive upward trajectory. While at first the BYOD trend was fueled to attract younger employees and their preferences for highly mobile devices like laptops, smartphones, and tablets, the pandemic and WFH meant BYOD mechanics shifted too. Now almost every worker needs access to a laptop and other smart devices capable of supporting cloud-based collaboration and cloud-based application tools. The shift to BYOD was apparent in 2021, as a record breaking 341 million[2] PCs were shipped, the highest total since 2012. Most of these sales were for Notebook/Laptop PCs, and, more incredulously, this growth is despite severe supply chain constraints.

As the pandemic forced many organizations to adopt remote work or hybrid work models, this WFH exodus has impacted employees and companies alike. A 2022 State of Remote Work survey[5] has some startling findings on just how much WFH has become the norm. 97% of respondents globally said that they would recommend remote work to others, and also that they would like to work remotely at least some of the time for the remainder of their careers. The survey also asked people to describe their experience with remote work. The responses were: 61% very positive; 29% somewhat positive; 9% neutral; 1% somewhat negative; and 0% very negative.

These statistics create a clear picture that most workers see WFH as something they want as a normal part of employment. Companies, too, have benefited from this remote work shift. WFH has, in many reports, seen increases in productivity, and the total cost per employee has gone down. Also, the flexibility to employ the best talent regardless of geography has meant companies with attractive WFH policies have benefited greatly in recruiting the best staff.

There are of course sectors where WFH is not as desirable or productive, but a workforce report[4] found that, by 2028, 73% of all departments are expected to have remote workers. Conversely, in a time like now in the USA, where there are more than 11 million job openings, not having any WFH or BYOD flexibility can be disastrous from a recruitment perspective.

Risk Management Considerations

Companies need to manage this new remote workforce and must confront the new risks involved and implications for their cybersecurity programs. Securing a WFH and BYOD workforce does initially create hurdles, but many companies have risen to the challenge and realized that, as with other aspects of their digital transformation, cybersecurity needs to transform itself and evolve, too.

With people's personal devices being used from unique home networks, the attack surface for potential threats is greatly expanded. A threat actor merely needs to compromise one device on a home Wi-Fi connection, such as a tablet or laptop, to access a device with sensitive company data.

Managing hundreds or even thousands of remote workers only further expands the attack surface. Not only are employee devices at risk of exposure, but cloud-native platforms implemented to virtually connect employees must now be a consideration. Plus, the rapid deployment to remote work transformed what used to be an in-person meeting or conversation around the water cooler to a digital file. And that adds another layer of complexity to the already huge amounts of data a company must protect and secure.

While security defenses have improved as WFH and BYOD attack surfaces increased, many companies are still challenged with scaling their security preparations and operational responses to match. While many organizations increased their security budgets, the impact of more technology left many of their cybersecurity teams under resourced and overwhelmed by the persistency of attacks, effects heightened by the ongoing cybersecurity recruitment shortage.

At the start of 2022, there were around 435,000 cybersecurity job openings in the USA, which is up from 314,000 in 2019.[6] A Forrester survey for 2021[7] shows 51% of cybersecurity professionals experiencing extreme stress and burnout, and 65% are considering leaving their job because of stress. So, this situation of skills shortage and burnout is going to need a fresh approach—and soon.

Adapting to the New Environment

As organizations adjust to ongoing workplace changes, there are several practical steps business leaders should take to ensure they are prepared.

1. Evaluate your security posture to know where you stand

Do you know what information or data is accessible via your internal network, cloud, endpoints, or a remote VPN? Knowing where your valuable data assets reside and having the security controls in place to protect those assets is a fundamental first step. A simple Security Audit conducted by an independent vendor will greatly help you focus on the priority areas of your data defenses.

2. Assess and address your perimeter

Perimeters used to mean a dotted line around an office building; these borders have now expanded around the entire planet and likely include many systems hosted by third parties in the cloud. While some of these security considerations will be provided by an audit, you should also consider regular vulnerability scanning and penetration tests to highlight both perimeter and internal security issues.

3. Consider changing work patterns and user behavior in this environment

A remote and global workforce means activity on your network will no longer take place from only office locations or during the same set of hours. Understanding these types of changes to user activity will help security teams with the right tools identify any potential anomalies. Many companies are implementing the concept of zero-trust to help with this.

4. Ensure you are implementing the basics of network defense

Once you have assessed your perimeter, having the right telemetry data—such as firewall and endpoint detection and response—in the right security operations environment is critical to establishing a baseline level of security to prevent the most basic intrusions.

5. Implement companywide employee education

Every employee has a responsibility to a company's security. It's important to spread awareness that it's not just on IT to secure company data. It's on everyone to know when not to click or react to a business email compromise scam. All it takes is one click on a link for a malicious threat actor to execute a successful hack. One report on successful data breaches showed that 85% occurred because of phishing, pretexting, and human error.[8]

6. Employ multifactor authentication (MFA)

MFA—a security measure that verifies a user's identity by requiring multiple credentials—is a critical and non-negotiable part of a layered defense strategy. In fact, looking at access permissions and tightening down how access is gained (especially to valuable assets and key network and cloud systems) is always a priority to minimize an attacker's lateral movement.

The New Cybersecurity Normal

The workplace today is vastly different than it was just a few years ago, and it appears those changes that may have seemed fleeting are going to be the new "business as usual" in many companies' futures. How can your organization prepare for this reality?

For starters, it’s prudent to take a closer look at your security investments. What may have worked just a few years ago is not sufficient for today and tomorrow's security operations. Staying up to date with futureproofed solutions is critical to keeping your company’s assets protected. For example, organizations should consider using software and artificial intelligence to help correlate, contextualize, and prioritize the vast amounts of data being processed by a security team. As we’ve seen, a lack of prioritization leads to burnout. “Always on” endpoint security is another imperative to address the changing, 24/7 workforce of today.

From a cultural perspective, it’s time for organizations to embrace, rather than resist, the necessary evolutionary changes needed to secure their organizations. At a minimum, most companies must be ready to support and enable a majority of their workforce to work remotely, while implementing the right measures to ensure security.

This means that security operations must have a holistic approach to unifying and integrating the various operational layers of endpoint, network, and cloud security, preferably under one single XDR management platform to gain efficient and effective prevention, detection, and response (mitigation) security controls.

Finally, IT and security functions should welcome the opportunity to prove to the larger organization how security can enable business growth and safeguard data in times of rapid change. The accelerated evolution caused by the pandemic has demonstrated that every business strategy should incorporate cybersecurity measures into their business continuity plans. And, in order to prepare for the unexpected, security teams should have the tools and resources to be nimble and ready to adapt to what’s next.

For better or worse, the new multi-faceted workplace is here to stay. Organizations must keep up with the evolution of work to attract the right workers and evolve their security or get overwhelmed. Doing both badly only benefits your competitors or cybercriminals.

Sources:

[1] FBI: 2021 IC3 Annual Report

[2] Canalys: Market Pulse, PC Analysis, January 2022

[3] ESG: The Long Road Ahead to Ransomware Preparedness – March 2022

[4] Upwork: Future Workforce Report 2021: How Remote Work is Changing Businesses Forever

[5] Buffer: 2022 State of Remote Work

[6] eSecurity Planet: Cybersecurity Employment in 2022: Solving the Skills Gap

[7] Forrester: Predictions 2022: Cybersecurity, Risk, And Privacy

[8] Verizon: 2021 Data Breach Investigations Report

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States

1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Europe & Middle East

France

8 avenue du Stade de France 93218
Saint Denis Cedex

Germany

Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom

One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates

Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086

Japan

Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Availability varies by region.