THINSCALE Work at Home: BPO's "Road to Damascus" Cybersecurity Moment

Stephen Loynd
Founder & Principal
TrendzOwl

Introduction

With the sudden and dramatic shift to the work-from-home model (WFH) in early 2020, IT security teams have raised a host of important questions. How secure is corporate data saved locally on unvetted, uncontrolled machines? Are corporate machines inherently secure in WFH deployments? Is there an increased likelihood of data leakage and other cyber-breaches in the WFH environment? For TrendzOwl, the recent history of cybersecurity tells a complex story, raises a host of additional questions, but ultimately also reveals new possibilities for the WFH model going forward.

The Cybersecurity Journey: A growing Threat Long Before Covid

Prior to the Covid pandemic, cybersecurity was already top-of-mind for enterprises. A report from Audit Analytics, "Trends in Cybersecurity Breach Disclosures" examined the years 2011-2019 and found that cyber-attacks were a growing threat. The most common methods hackers used to obtain company data was malware (34%), phishing (25%), unauthorized access (20%), and misconfiguration (12%). Meantime, 43% of firms that experienced a data breach declined to disclose the type of attack. Reviewing 639 cybersecurity breaches at public companies since 2011, that same Audit Analytics report found that the average cost of a cyber-breach to a publicly traded company was an eye-catching $116 million.

The report found that the two elements of cyber-breaches having the most significant financial impact are remediation costs and stock market values.

And according to cloud computing firm iomart, a typical data breach for a large company results in data loss of between 10 million and 99 million records and hits a company's value by an average of 7.27%. For small businesses, a single breach can be catastrophic.

Six months before Covid hit, Cybersecurity Ventures was already predicting that global cybersecurity spending would exceed $1 trillion from 2017 to 2021 alone.

> a typical data breach for a large company results in data loss of between 10 million and 99 million records

The Shift Home: Cybersecurity Gains New Prominence

With the onset of the global pandemic in early 2020, the great work-from-home experiment began in earnest. More business — from banking to ecommerce — was being conducted online than ever before. And in the rush to continue with business as usual, many organizations took shortcuts with security. Cyber criminals immediately took note.

The news of global cyber-breaches came in waves. Sometime in March or April, 2020, Israeli fintech company Sapiens experienced a major cyber-attack after its employees had pivoted to remote work. Eventually, Sapiens would pay a $250,000 ransom in bitcoin after hackers threatened to shut down the company's network.

In the United States, the Federal Bureau of Investigation (FBI) was warning of a sudden jump in cyber-risks. The Bureau described how both domestic and international hackers were taking advantage of America's increasing online activity. In May, 2020, the FBI claimed there already had been a 300% increase in cybercrimes reported.

Cloud computing firm iomart agreed. According to its own study, large-scale breaches grew in intensity and frequency throughout 2020, with the number of breaches increasing 273% in the first quarter compared to the year before.

According to VMware, by the summer of 2020 there was a disturbing uptick in even more sinister attacks. There was a 90% increase in criminals encrypting files and demanding a ransom to restore access. Attacks in which data or networks were destroyed was up 102%. And island hopping, in which criminals take over company digital transformation efforts by using their networks to attack customers and partners, increased by 33%.

Meanwhile, government agencies and local governments were being hit as well. The city of Florence, Alabama, paid nearly $300,000 after a bitcoin cyberattack on its computer network system in June.

In California, the city of Torrance was hit by a ransomware attack that disabled its website, email, and financial system. The criminal group responsible demanded 100 bitcoin, worth around $700,000.

In other words, with the arrival of Covid and the shift to the WFH model, it had become clear that the corporate security perimeter had been broken. In the words of Emily Mossburg, a global cyber leader at Deloitte:

This was compounded by ad hoc security controls early on, as companies scrambled to get employees up and running. Now, as the crisis drags on, companies are realizing employees may need to work from home for the foreseeable future. There's a transition from 'a solution that was built together with duct tape and string and chewing gum' to more 'robust operationalized solutions.'

In May, 2020, the FBI claimed there already had been a 300% increase in cybercrimes reported.

The Epiphany: Corporate Devices were No Panacea

By June, 2020, Morphisec (a unified threat prevention platform), released a 2020 WFH Employee Cybersecurity Thread Index that examined how more than 800 employees in the United States were coping with the changes associated with a new way of working.

Andrew Homer, a Morphisec vice president of security strategy and business development, noted that, ***"We've seen anywhere between a doubling or a tripling of the amount of attacks that we blocked since Covid. When I say about a tripling, that's over 170,000 attacks a week across the five million endpoints."***

Homer went on to describe a situation in which organizations weren't able to guarantee employees were working on secure devices or trusted Wi-Fi connections (articles to consider on this unique threat include, "The security dangers of home networks," from Computer Weekly, and, "Identifying Unique Risks of WFH and Remote Office Networks," from bitsight.com).
While Morphisec's findings suggested that up to 56% of employees were using personal computers to work from home, it was clear that homeshored employees working on corporate devices were proving to be a vexing issue as well.

Morphisec found that corporate devices are often exposed to other individuals in the household.

"We've seen a tenfold increase in the amount of adware, [which] is games, or unwanted software on these devices," added Homer. "That's indicative of kids using their parents' machines. That's really concerning because adwares have become the delivery mechanism of putting malicious, highly nefarious malware onto these machines. Now that we're outside the corporate network, the endpoint itself has become ground zero."

Homer insists that large companies now realize they must have automated self-protection baked into employee endpoints: "When you have a dirty environment… people can't make heads or tails out of what is a good event versus what's a bad event because they're blending the personal and work activity on the same machine. They now need an architecture [focused] on prevention, not on detection, that stops the attacks."

Indeed, encrypted data cannot even be considered secure, as leakage of any data is considered one of the main risk in WFH environments.

Cyber security publication site, Security Boulevard, found that 86% of IT practitioners report someone within their organization has had a laptop lost or stolen, 56% reported it led to a data breach.

Malwarebytes themselves have stated that the majority of people use their work devices for personal use, including allowing other members of the household to send and receive emails, and download third party software – drastically increasing the risk of introducing malware into a corporate environment.

Clearly, both unsecured personal devices or corporate devices accessing resources through unsecure connections to corporate resources (local, virtual, and remote applications and desktops) risk data leakage while offering almost no IT control and no real way to force through updates. Ironically however, data storage on corporate laptops makes such corporate devices prime targets for theft, in many cases increasing the risk of data leakage.

It's also important to add the sheer number of anecdotal reports of users simply utilizing their own OS while working from home despite delivered corporate machines. And even VPNs are a risk, as a lot of tech can find a way around them. VPN services protect the data to and from the VPN provider, but not to the destination. Remote locations often remain insecure. And VPNs are not always activated.

Unfortunately, malicious behavior by agents must also be considered as a possibility. A WFH agent might take pictures of customer details with their mobile phone, for example. Consider too that malware can be introduced to an environment via USB, and most organizations will therefore restrict the use of USB storage in their on-premise environments. However, corporate devices sent to home environments are not always restricted in the same manner, introducing additional risk for organizations.

Corporate Control, Security, & Management: ThinScale

The case of an easy, effective solution for the huge percentage of home-based agents in the business process outsourcing (BPO) space is worth examining. Fast-growing technology company ThinScale, founded in 2013 and based in the Media Cube on the IADT campus in Dublin, Ireland, offers solution-driven products that aim to help enterprises optimize their virtualized environments and increase productivity while improving security. Its focus is on transforming the way endpoints are secured, delivered and managed.

ThinScale's ThinKiosk is a software-defined thin client specifically designed to help enable organizations to provide high levels of endpoint security on corporate machines for WFH programs. ThinKiosk applies the relevant policies and settings, blocking, but not overriding the device's OS; with ThinKiosk machines the agent has no opportunity to leave the secure UI installed on the device.

- Thousands of agents can be up and running quickly, easily, and securely without the need for additional hardware. In other words, agents are able to access corporate environments, applications, and data while meeting all security and compliance standards.
- The agent's device can only be used for work Only the agent is using the secured device (no family or third parties have access)
- Each agent is in effect using a trusted WiFi connection
- Each agent is in effect no longer using a personal computer
- The risk of data leakage from lost or stolen machines is eliminated
- The risk of deactivated VPNs is a non-factor

Clearly then, despite the belief that corporate machines are inherently secure, there are flaws in corporate machine deployments that must and can be fixed in at-home environments. ThinKiosk's Virtual Desktop Agent intercepts virtual machine access from all sources, and can deny connection from any endpoints not running ThinKiosk. In essence, agents are prevented from using any machine other than the one provided to them.

> ThinScale's ThinKiosk is a software-defined thin client specifically designed to help enable organizations to provide high levels of endpoint security on corporate machines for WFH

Journey's End: A Surprising Conclusion

One thing the journey through a decade of cybersecurity history shows is that corporate machines are not inherently secure, especially at home. Devices deployed with VPNs, portals, and basic lockdown policy can be relatively easy to get around for the resourceful hacker. Indeed, home Wi-Fi networks pose risks to company data; updates to home router software are often neglected, and many home networks have weak firewalls or lack them altogether.

Or consider how many employees fail to closely follow the guidance they're given. It only takes one mistake to cause costly damage. Healthcare, an industry at high risk for cyber-attacks, is a prime example. The American Medical Association (AMA) and the American Hospital Association (AHA) have developed a cybersecurity resource called, "Working from home during the COVID-19 pandemic," to help guide those that are more susceptible to phishing attacks (Verizon's 2020 Data Breach Investigation Report found that phishing is one of the top threats, with 22% of data breaches involving phishing).

That healthcare resource was designed to teach physicians working from home to strengthen their personal or business computers, networks, and even their medical devices to fight against the rise of Covid19-related cyber threats. Yet employees can easily dismiss or bungle such corporate security measures; in either case there's a high likelihood of malicious actions such as "man-in-the-middle" (MiTM) attacks, which IBM claims account for 35% of cyber-attacks on home-based employees. Think too about all the home-based employees who simply ignore procedures altogether.

But there's a larger lesson here too. The fact is, most employees already use a personal device for work, and the trend seems unstoppable. In May, 2021, Techjury provided the stunning statistics. According to Microsoft, a full 67% of employees use their own devices for work, regardless of the official BYOD policy. Even if forbidden, many people are using their personal devices in some form for their work.

In the wake of Covid19, we've made some surprising discoveries during the cybersecurity journey. Relying on traditional methods of WFH provision poses massive security risks. But by properly securing corporate machines, an array of vexing security issues can be largely avoided.

> **a full 67% of employees use their own devices for work, regardless of the official BYOD policy. Even if forbidden, many people are using their personal devices in some form for their work.**