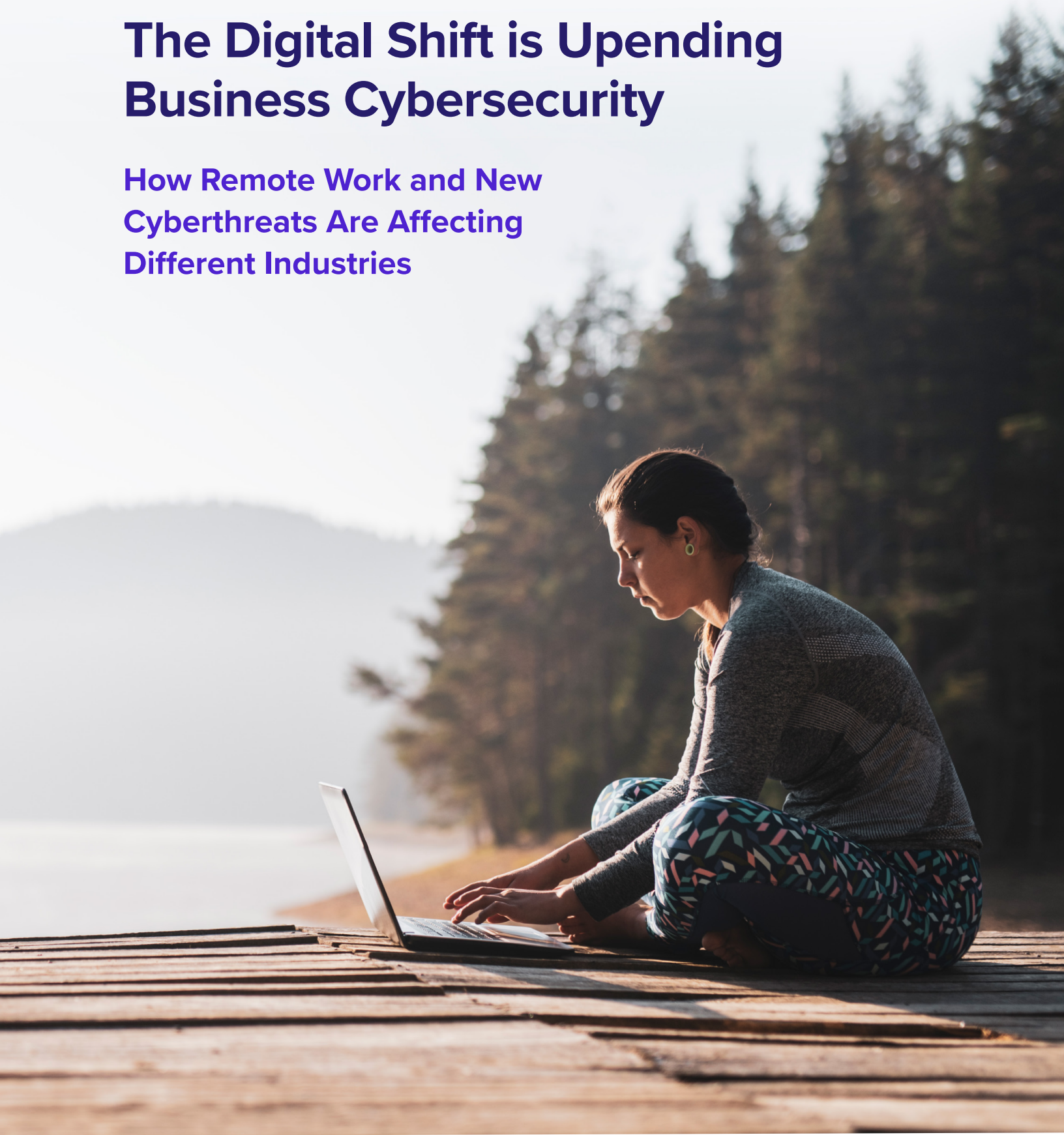
avast business

The Digital Shift is Upending Business Cybersecurity

How Remote Work and New Cyberthreats Are Affecting Different Industries



Embracing Remote Work

As the global pandemic hit, businesses across nearly every industry were forced to suddenly shift entire workforces to working from home. For many, the work-from-home (WFH) model is likely to become permanent.

One reason for embracing remote work even after restrictions are lifted is that for those businesses that could make the shift, many are reporting significant benefits. In a survey of small and mid-sized business owners, more than half (57%) of those who increased remote working as a result of social distancing requirements say they will likely maintain increased remote working options for employees in the long term.[1]

What these and other business owners might not realize, however, is that the sudden and potentially permanent shift to remote work also presents new risks for the business in the form of cyberthreats. For example, 63% of respondents in a cybersecurity survey reported either a significant or slight increase in attempted cyberattacks related to the pandemic.[2] At the same time, in a survey of cybersecurity professionals, only 41% said their companies are utilizing best practices to secure the remote workforce.[3]

Let's take a closer look at the risks as well as understand the impact of remote work and increased cyberattacks across five different industries.

Is Remote Work the New Normal?[4]

57% of business owners said they are likely to continue increased remote working options for employees in the long term. They cite benefits including:

Extending the Business to Unsecured Home Work Environments

Companies that suddenly moved to a WFH model for employees face a double challenge:

1. A greater risk of breach due to the shift away from a secure workplace to work from an unsecured home. Hackers are exploiting any weaknesses they can find in a remote work model
2. An escalated risk of cyberattack because of a large spike in attacks during the pandemic

Even before the pandemic and the shift to remote work, smaller and mid-sized businesses were preferred targets for cybercriminals. Nefarious actors know that, unlike large corporations, smaller companies are often more vulnerable to attack because their resources are more limited. They may not have the time, budget, expertise, or IT staff to adequately protect their businesses from cyberattack.

Beyond resource constraints at the company level, employees who suddenly find themselves working from home may not be educated about secure WFH practices. This can put your company at greater risk of data breaches and cyberattacks such as ransomware because people working from home may be:

- Sharing devices with non-authorized people
- Accessing sensitive information through unsafe home networks
- Opening attachments or clicking on links in phishing emails that put sensitive data and login credentials at risk

COVID Isn't the Only Thing Spreading[5]

Cyberattacks Are on the Increase

37%

increase in hacking and phishing activity between February and March 2020

300%

increase in cybercrimes reported to the FBI as of May 2020

EDUCATION

Teaching and Learning Remotely[6]

Pre-pandemic, the education industry was a prime target of cybercriminals, with K-12 schools experiencing three times the number of cyber incidents in 2019 compared to 2018.[7] As the pandemic forced schools to move to remote learning, both universities and K-12 schools have experienced disruption of distance learning caused by hackers. At the same time, more sophisticated attacks have led to the theft of taxpayer dollars, stolen identities, and denial of access to school technology.[8]

there are
4 MILLION
U.S. teachers

56.6 MILLION
U.S. elementary and secondary students

EDUCATION
ranked last in cybersecurity preparedness compared to 16 other industries

348 CYBERATTACKS
on K-12 school systems in 2019; 3x as many cyber incidents as 2018

RANSOMWARE
attacks on education providers more than doubled from 6% in 2019 to 15% in the first half of 2020

INSTITUTIONS
were warned that malicious cyber actors are targeting K-12, leading to ransomware theft of data, and disruption of distance learning

NONPROFIT

Reimagining Everything as Virtual[9]

As travel, work, and socializing restrictions hit at the beginning of the pandemic, nonprofits had to rapidly shift into virtual delivery of nearly everything they do: from virtual fundraising and events to remote program delivery, WFH models, and virtual internships and volunteering. While the shift to virtual has brought unexpected benefits in terms of greater participation and improved collaboration, it also means that these organizations must rely much more heavily on technology than ever before — exposing them to greater risk of cyberattack.

69%
of nonprofits can accommodate working from home for all staff

69%
say they are contemplating remote work even after the coronavirus crisis passes

NONPROFITS
can be at higher risk for cyberattacks because they have fewer resources invested in cybersecurity than for-profit companies

NON GOVERNMENTAL ORGANIZATIONS
(NGOs) report increased volume of cyberattacks since the pandemic

THE WORLD HEALTH ORGANIZATION
(WHO) reported double the normal amount of cyberattacks in the first quarter of 2020

BLACKBAUD
financial and fundraising platform for nonprofits was hacked in 2020; the company paid a ransom to have the hijacked data destroyed by the cybercriminals

HEALTHCARE

Virtually Caring for Patients[10]

While hospitals struggled to handle spikes in COVID-19 patients, other providers had to pivot from in-person to telehealth appointments to safely provide access to care for non-emergent patients. The rise of telehealth, remote work, virtual waiting rooms, and online check-in and payment mean that both patients and health systems have had to rapidly adopt new technology. Knowing that lives are at stake if hospitals and health systems can't access their data, medical devices, and systems, cybercriminals continue to target the healthcare industry for financial gain.

154% INCREASE
in telehealth visits during the last week of March 2020, compared with the same period in 2019

#1 TARGET
for cybercrime is healthcare

50% INCREASE
in healthcare-related cybersecurity breaches reported in the first half of 2020 to the U.S. Department of Health and Human Services

A RANSOMWARE ATTACK
in September 2020 caused an outage at all 250 U.S. facilities of the hospital chain Universal Health Services

RYUK RANSOMWARE
hit six hospitals in the U.S. over a 24-hour period in October 2020

FINANCIAL SERVICES

Working Remotely in a Highly Regulated Sector[11]

Before the pandemic, work flexibility was far from the norm in financial services companies. Part of the reason for this was the need to monitor compliance with regulatory requirements by employees interacting with customers. Then COVID-19 forced banks, insurance, mortgage, credit card, and other companies to shift to a WFH model to continue operating. While they may have overcome many of the regulatory hurdles for WFH, allowing them to continue offering work flexibility to employees, have they overcome increased cybersecurity risk?

29%
of financial services companies pre-pandemic had at least 60% of their employees working from home at least once a week

61%
of financial services companies plan to make remote work permanent for roles that allow it

238%
surge in cyberattacks against banks during the pandemic

70%
of financial services firms experienced a successful cyberattack in 2020

57%
of financial services companies believe cyberattacks are increasing in severity as a result of WFH

41%
believe remote workers put the business at risk of a major data breach

MANUFACTURING

Running Factories From Afar[12]

The manufacturing industry has been hard hit by the pandemic. First, many manufacturing jobs are onsite and unable to be carried out remotely. Second, the pandemic reduced demand for some goods, which impacts company revenue. Social distancing and employee safety measures put an additional level of pressure on those manufacturers able to continue production. At the same time, shifting office employees and knowledge workers to remote work opens the door for increased cybersecurity, potentially exposing the business to cyberattacks that could shut down an entire operation.

UP TO 60%
of employees of manufacturers are office staff

"VIRTUAL SHIFTS"
using remote personnel can use diagnostic, management, and collaboration tools to guide and support a reduced "physical shift" of onsite personnel

11% INCREASE
in the first half of 2020 in attacks on manufacturing companies and intrusions on their networks, compared with all of 2019

HONDA MOTOR COMPANY
experienced a ransomware attack that crippled operations in multiple countries in June 2020

CANON
suffered a ransomware attack and theft of corporate data, including employee information in July 2020

AMERICOLD
was hit with a cyberattack in November 2020 that disrupted its phone systems, email, inventory management, and order fulfillment

Protect Your Business With Modern Solutions

If you've shifted some or all of your employees to WFH, either temporarily or permanently, the remote work model can make your business more vulnerable to cyberattack. Likewise, if you've adopted or plan to adopt new technology to deliver virtual services, enable remote employee communication and collaboration, support customer needs as you pivot to conduct business virtually, or handle other essential capabilities, be aware these tools can also expand your attack surface and increase your cybersecurity risk.

To protect your business during the pandemic and beyond, you need a cybersecurity solution that is faster, smarter, and more reliable than ever before. This means replacing outdated security models with modern security solutions that are both robust and simple to use, so you can protect your business while focusing on adapting and growing in the new normal.

All-in-one cloud security solutions offer maximum protection, even for those businesses with limited IT resources.

You Don't Need to Go it Alone

Working with a managed security service provider can help your business reduce risk without having to invest in a an IT team. By partnering with an MSSP or MSP, you get:

- Deep cybersecurity expertise and experience
- Proactive cybersecurity monitoring and protection
- Faster identification of and response to cyberattacks
- Access to enterprise-grade cloud security solutions for maximum protection

Next Steps

Regardless of whether your current business model is temporary or the changes you've made during the pandemic will prove to be longer lasting, the reality is that cybersecurity risks won't go away in either situation. Now more than ever, a successful cyberattack could devastate your business just as you're recovering from the impacts of the pandemic.

Make sure you've done all that you can to protect your business against attack by cybercriminals. Work with experts, such as MSSPs or MSPs, that understand the needs of businesses like yours and the increased risks of remote work. They can help you identify and fill your company's security gaps as well as provide ongoing monitoring to ensure continuous protection against cyberattacks and rapid response to threats.

LEARN MORE

About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.

[1]*"New Study Finds More Than Half of U.S. SMB Owners Believe Working Remotely Is Here to Stay Post-Pandemic," Darcy Mekis, Intermedia Cloud Communications, May 2020*
[2] *"The Impact of the COVID-19 Pandemic on Cybersecurity," Jon Oltsik, ESG, July 2020*
[3] *"(ISC)² Survey Finds Cybersecurity Professionals Being Repurposed During COVID-19 Pandemic," (ISC)2, April 2020*
[4]*New Study Finds More Than Half of U.S. SMB Owners Believe Working Remotely Is Here to Stay Post-Pandemic," Darcy Mekis, Intermedia Cloud Communications, May 2020*
[5]*CloudFlare, FBI Internet Crime Complaint Center (IC3)*
[6]*Sources: Kaiser Family Foundation, Educationdata.org, SecurityScorecard, K-12 Cybersecurity Resource Center, Barracuda Networks, Cybersecurity & Infrastructure Security Agency*
[7]*"Cyberattacks on Schools Tripled in 2019, Report Finds," Alyson Klein, EducationWeek, March 2020*
[8]*"Back to School Ransomware Attacks," SecurityMagazine, September 2020*
[9]*Sources: Nonprofit HR, The NonProfitTimes, Devex, Security Boulevard*
[10]*Sources: Becker's Hospital Review, Centers for Disease Control and Prevention, Medical Economics, AP News*
[11] *Sources: Pwc, VMware Carbon Black, Keeper Security*
[12]*Sources: CrowdStrike, BBC News, SecurityWeek, BleepingComputer*