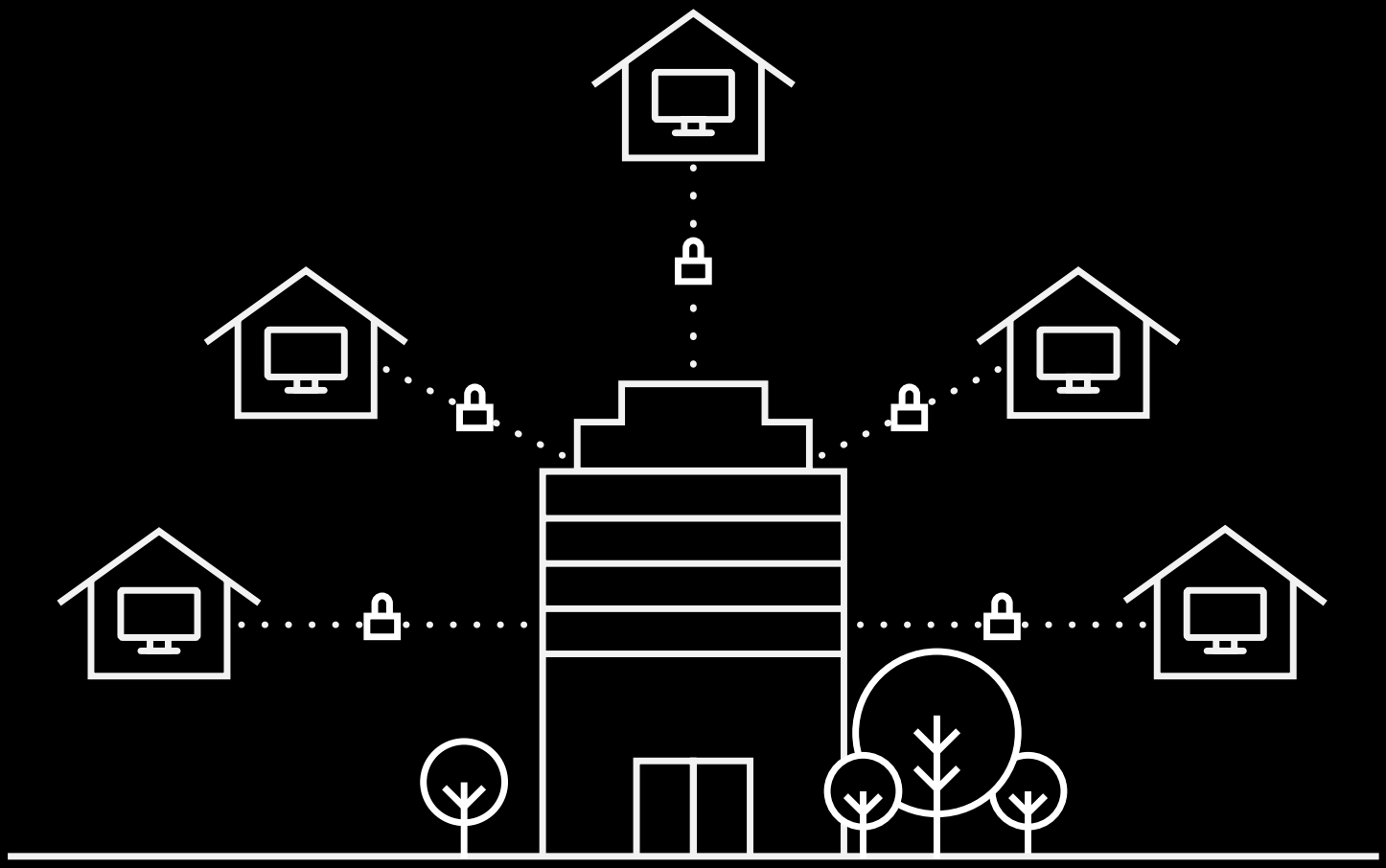
White paper

Securing a remote workforce

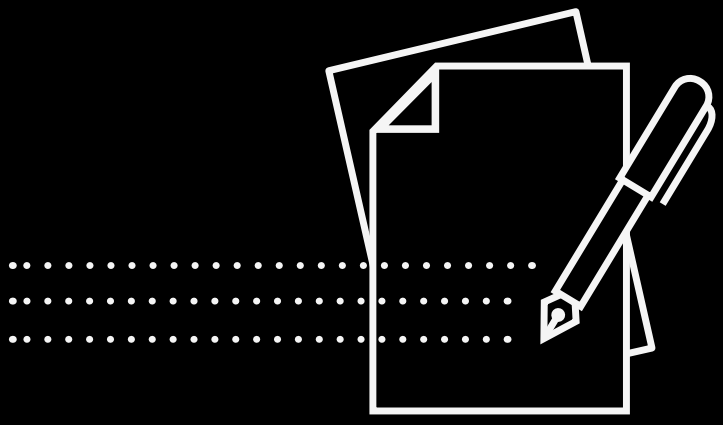
Future-proofing your organization against cyber threats



verizon

Table of contents

Executive summary



COVID-19 radically accelerated the shift to remote working. But it also raised new questions around how your business should go about securing a remote workforce. Proponents have long argued that more flexibility in working patterns supports greater productivity, happier workers and less churn for employers to manage. But as we have seen over the past few months, it has also exposed organizations to an increased risk of cyber-threats as attackers start to probe remote working infrastructure and distracted employees.

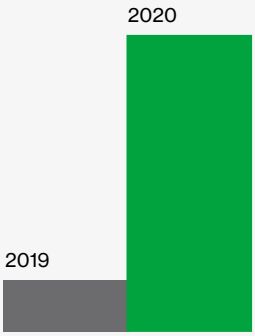
Business decision makers wrestling with these challenges will find much to help them in the following paper. It reveals how:

- Phishing, malware and other threats are increasingly being targeted towards devices, networks and remote workers
- These threats could lead to serious financial and reputational damage if corporate security is breached
- The challenge requires a response that is both technology and human-centric
- Your organization can tackle these threats by developing new policies and processes, enhancing staff training and awareness and updating device and network security.

By April 2020, 62% of Americans were working remotely,[1] compared to just 11% in 2019.[2]

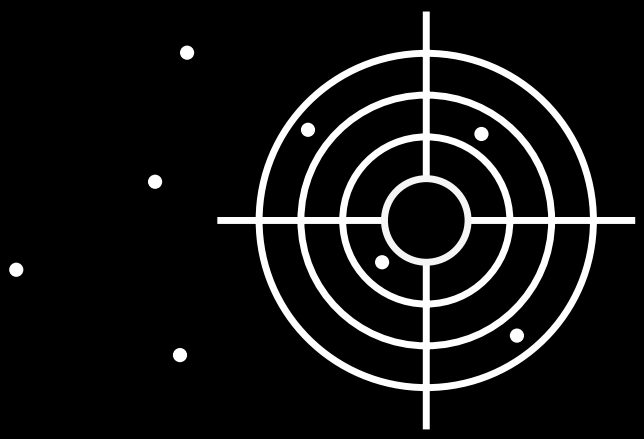
51%

Increase in remote working.



Remote work is now business as usual – only time will tell how long the shift to a distributed workforce outlasts the restrictions of the pandemic. The key for businesses will be to develop strategies that preserve productivity and growth while mitigating emerging cyber risks. With signs that remote work will remain popular long after COVID-19 has receded,[3] the race is on to future-proof your organization against online threats.

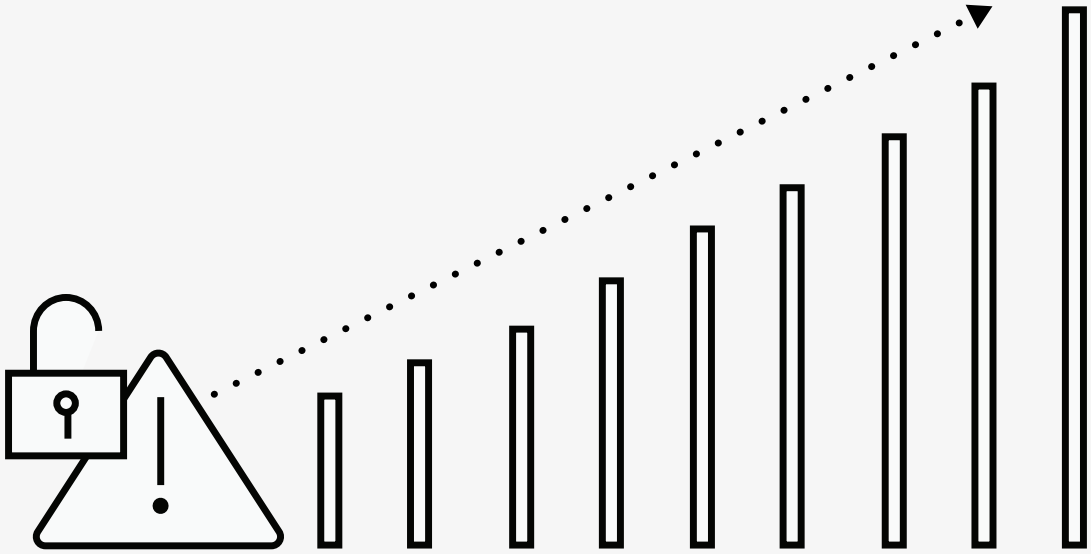
In the crosshairs



For many organizations, the first few weeks of pandemic response flew by. Senior executives and IT teams scrambled to maintain operations and customer engagement amid government lockdowns as they transitioned their workforce from the office to the homestead. Organizations that did so successfully must now turn their focus to remote work security.

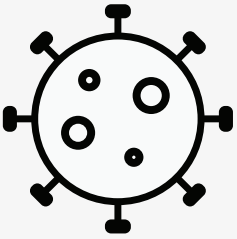
Threat levels are higher than ever. The digital infrastructure has expanded. Remote work endpoints have mushroomed.

Attackers are turning their focus to exploitable security gaps. Businesses have been caught off-guard: 85% of chief experience officers and vice presidents reported feeling ready to shift to a remote workforce, according to a Tanium report, but 98% admitted to being caught flat-footed by the security challenges they faced in the first two months of the pandemic, and 90% reported an increase in cyber attacks.[4]

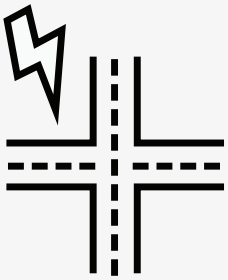


The key threats

A joint advisory published by the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) highlighted two main threats to organizations and their remote workers:[5]



COVID-19-themed phishing and malware attacks



Attacks against newly – and often rapidly – deployed remote access infrastructures

Google claimed in April to be blocking 18 million daily malware and phishing emails related to COVID-19.[6] And exposed remote desktop protocols spiked, increasing on some days as much as 127%.[7]

Attacks using these techniques could result in large-scale theft of customer information and intellectual property or serious service outages. More than 27 billion records were exposed in the first half of 2020,[8] and 121 million ransomware attacks were recorded during that same period.[9] And that does not include social engineering attacks – a review of Mimecast's global customer threat intelligence data found that impersonation fraud increased by 30%[10] in the first 100 days of the COVID-19 pandemic, and the US Federal Bureau of Investigations warned in April 2020 of an expected rise in business email compromise attacks.[11]

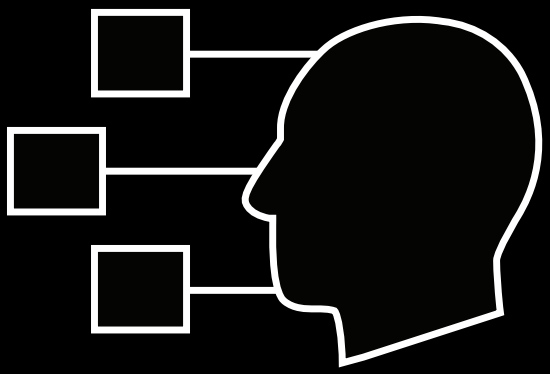
It's best to build resilience into your business ahead of time to prevent such attacks. Once security is breached, it can be difficult – and expensive – to put things right. According to Verizon's 2020 Mobile Security Index Report, 55% of companies that experienced a mobile compromise suffered lasting repercussions.

The financial and reputational effects of a serious incident could include:

- Lost productivity
- Service outages
- Legal costs
- Regulatory fines
- Remediation, investigation and cleanup costs
- Reduced consumer trust
- Lost customers

Securing a remote workforce involves a tried-and-tested combination of people, processes and technology. It requires enhanced employee training, redesigned policies and a renewed focus on securing mobile devices and network infrastructure.

The human factor



Millions of cyber threats used COVID-19 as a lure in the opening months of 2020, but, in total, there were no more threats than usual, according to the NCSC and the CISA. Rather, cyber attack campaigns were tweaked to take advantage of interest in the pandemic and to target remote workers, who arguably pose a greater cyber risk than their office-bound peers. Employees who work at home might be more distracted and more prone to click on phishing links, and their devices might not be as heavily protected. Home computers, devices and networks could also be used in riskier ways or shared with family members who engage in risky online behavior. A Trend Micro survey found that 56% of remote workers use personal apps on their corporate devices, 66% have uploaded corporate data to these devices and 39% regularly access corporate data from a personal device.[12]

A secure remote workforce management strategy depends on developing effective policies and processes – and it starts at the employee level.

Training and awareness

Securing a remote workforce means changing how employees behave online. According to Verizon's 2020 Data Breach Investigations Report, 22% of breaches were due to human error, and another 22% were traced to social engineering attacks. A business cannot afford these unforced errors.

With the right training, employees can be transformed into an effective line of defense. One large bank drove a 95% improvement in employee click rates by running more frequent phishing awareness campaigns, enacting monthly anti-phishing tests adapted to COVID-19-themed lures and enacting more restrictive security policies.[13]

Use online tools that simulate social engineering attacks and can be adapted over time as threats evolve. And put in place a mechanism to analyze results and deliver feedback to individual users. Tools and training are best deployed repeatedly and in short bursts. Every employee, from the board room down through the mail room, must be involved. And if an employee consistently underperforms, give them extra lessons.

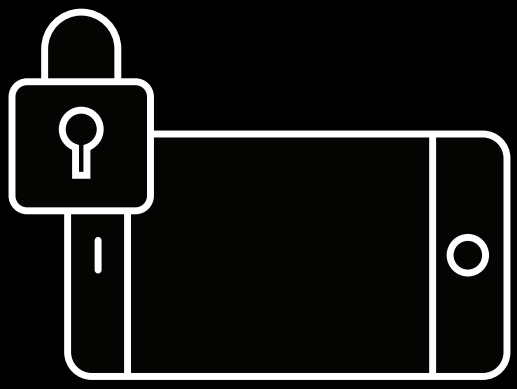
Acceptable use policies

Wider acceptable use policies (AUPs) will also help bolster remote work security. What those policies include will depend on your appetite for risk, but consider setting rules regarding:

- Which websites, apps and networks will be allowed to access corporate data and systems
- Which devices can access corporate data
- Appropriate language on internal and external channels
- Sending corporate data outside the organization

Convey these policies as succinctly as possible, and make the repercussions for violating them abundantly clear.

Mobile device security

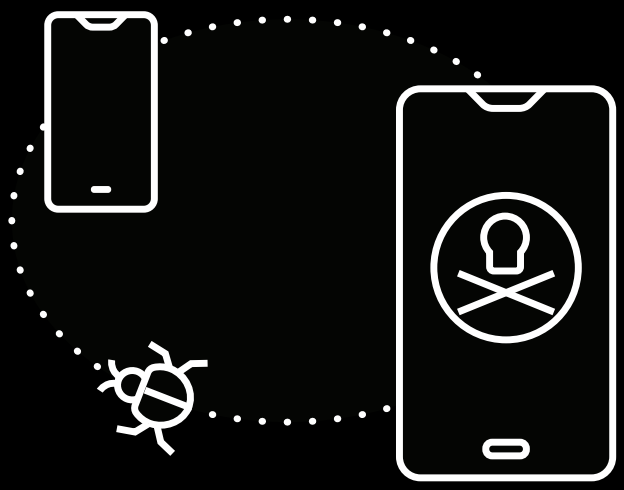


Securing a remote workforce effectively also means mitigating the cyber risks associated with mobile devices. These threats are increasing: 39% of organizations suffered a security compromise through a mobile channel in 2020, up from 27% in 2017, according to the Mobile Security Index Report. Companies of every size and in every vertical have been hit, and two-thirds of them are hit hard by downtime, reputation damage and regulatory penalties.

Many of the threats in the fixed world – phishing, ransomware, business email compromise attacks, cryptojacking (the unauthorized use of a computer to mine cryptocurrency) – appear in the mobile world. In the mobile world, though, phishing targets are more likely to be exposed to malicious missives sent over social media, text messages, gaming platforms or apps.

Remote workers are also exposed to:

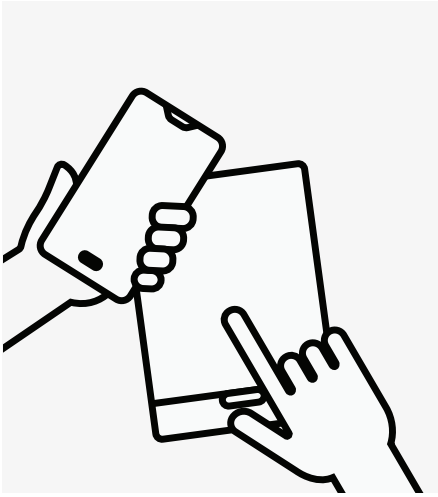
- Man-in-the-middle attacks conducted via public Wi-Fi
- Malware hidden in mobile apps that look legitimate
- Device theft or loss
- SIM card swapping
- Compromised USB charging points (also called juice jacking)



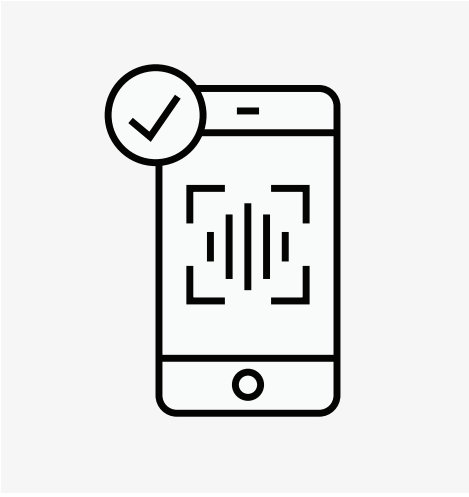
"39% of organizations suffered a security compromise through a mobile channel in 2020"

Mobile device security

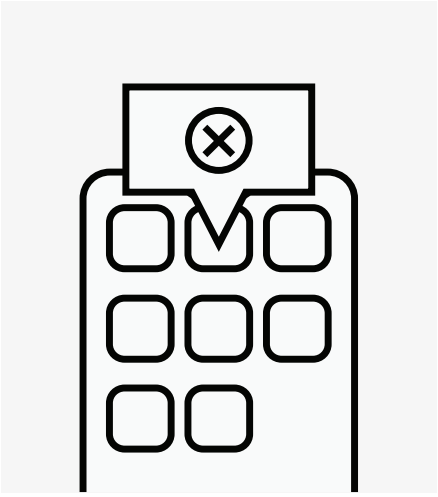
A few tactics can help mitigate the threats to remote workers' mobile devices:



Bring-your-own-device policies: Establish in your AUPs whether employee-owned devices can access corporate networks and data. If they can, ensure that devices are covered by corporate security policies and protected accordingly.



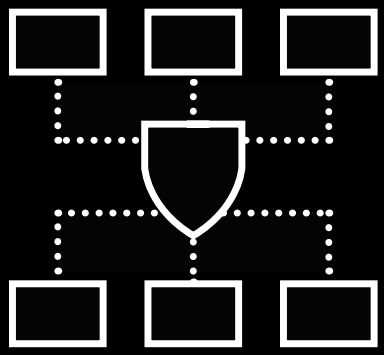
Mobile threat detection: Whether a device is corporate- or employee-owned, it should be loaded with mobile threat detection tools that offer anti-malware protection. Mobile threat detection apps should be set to automatically update, with regular scans for malware.



Application control: Twenty-one percent of compromised organizations said that a rogue or unapproved application was the source of the incident, according to the 2020 Mobile Security Index Report. App control solutions will ensure that only whitelisted software can download to the device, minimizing the threat.

Mobile device management can extend corporate security policies to every employee's mobile device. Widely available solutions let IT managers control and restrict app downloads, scan for malware, enforce advanced authentication and remotely wipe lost or stolen devices.

Securing the network infrastructure



Now that you've addressed the risks posed by employees and mobile devices, consider the networks connecting remote employees to the corporate network and its cloud resources. These communication channels link mobile devices and computers to the applications that power productivity, so they need to be fast, secure and easy to manage.

Businesses have many options here:

Virtual private networks (VPNs)

Offer a secure, encrypted tunnel between the remote worker's laptop or mobile device and the internal corporate network and its cloud resources. Attackers can't eavesdrop on communications or steal sensitive data and log-ins. VPNs are particularly useful for mobile devices, as VPNs mitigate the risk of man-in-the-middle attacks that use public Wi-Fi. Look for offerings that are easy to configure, prioritize mission-critical apps, block unauthorized traffic, provide flexible connectivity options and feature dynamic mobile network routing for improved scalability.

A **software-defined wide-area network (SD WAN)**

Could offer your business a useful alternative to multiprotocol label switching networks. The key here is that the network is software-defined, meaning it can be managed centrally and will not require technician call-outs to fix issues. Traffic can be dynamically routed to optimize bandwidth and ensure that mission-critical apps are prioritized. Most importantly, security can be baked in, including firewalls, encryption and threat prevention features. An SD WAN offers simplicity, efficiency, availability and security at low cost; you could also choose a managed SD WAN and let a third-party provider do the heavy lifting, freeing up your in-house IT team to work on higher-value tasks.

Verizon's Secure Gateway

Lets your business securely connect remote workers to your main offices and retail locations. An encrypted, secure web gateway safeguards access; you control who and what can access your data, and you can scale bandwidth as needed.

Verizon's DNS Safeguard

Is a cloud-based security platform designed to prevent connections to known malicious sites and protect your remote workers from known and emerging malware, ransomware and phishing threats. Blocking access in this way also supports AUPs and keeps corporate data and systems clean.

Recommendations

The remote workforce is likely here to stay. Three in five US workers who have been doing their jobs from home during the coronavirus pandemic would prefer to continue to work remotely as much as possible once public health restrictions are lifted, Gallup reports.[14] The Harvard Business School estimates that at least 16% of remote workers will stay remote long after the COVID-19 pandemic has subsided.[15]

Security is frequently sidelined in favor of more pressing business concerns. According to the 2020 Mobile Security Index Report, mobile security is most often sacrificed for expedience (62%), convenience (52%) and profitability (46%). However, security is a prerequisite for long-term business growth. Without the right remote working security strategy, digital investments and business-critical operations could be derailed at a time when few organizations can afford it.

"Without the right remote working security strategy, digital investments and business-critical operations could be derailed at a time when few organizations can afford it."

If the new normal is to be defined by the distributed workforce, then the best way to get your business in the pole position is to take steps now to secure your networks, your employees and their devices:

1. Revisit and re-architect employee education and awareness programs.
2. Redesign AUPs to take account of the new reality of mass remote working.
3. Eliminate blind spots by ensuring that connected devices are covered by corporate security policies.
4. Support new remote working policies through mobile device management to mitigate threats to devices.
5. Decide on the best network infrastructure to enable seamless and secure access to the corporate network and its cloud resources.

Learn how

Verizon's high-performance network technology can secure cloud access for your distributed workforce.

verizon

1. "U.S. Workers Discovering Affinity for Remote Work," Megan Brenan, Gallup (April 3, 2020).
2. "Availability of flexible work schedule and student loan repayment benefits in the United States," June 2019, US Bureau of Labor Statistics (accessed September 30, 2020).
3. "The New Future of Work in a Post-Pandemic World," Emily He, Forbes (June 1, 2020).
4. "When the World Stayed Home," tanium.com (Accessed September 30, 2020).
5. "Advisory: COVID-19 exploited by malicious cyber actors," NCSC/CISA (April 8, 2020).
6. "Protecting businesses against cyber threats during COVID-19 and beyond," Neil Kumaran and Sam Lugani, Google Cloud (April 16, 2020).
7. "127% increase in exposed RDPs due to surge in remote work," Asaf Aprozper, Reposify (March 30, 2020).
8. "New Research: Data Breach Reports Down in 2020, Yet Over 27 Billion Records Exposed," RiskBased Security (August 17, 2020).
9. "121 million ransomware attacks recorded in the first half of 2020," Bobby Hellard, IT Pro (July 24, 2020).
10. "The State of Email Security 2020," Mimecast (accessed September 30, 2020).
11. "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic," fbi.gov (Published April 2, 2020; accessed October 2, 2020).
12. "Employee Security Training Is Vital to Remote Success," Trend Micro (July 1, 2020).
13. "A dual cybersecurity mindset for the next normal," Venky Anant, Soumya Banerjee, Jim Boehm and Kathleen Li, McKinsey (accessed September 30, 2020).
14. "How Much Will Remote Work Continue After the Pandemic?" Kristen Senz, hbswk.hbs.edu.
15. Op. cit., Gallup (April 3, 2020).