Remote Work and COVID-19 Cybersecurity Impact Report

May 2020
To understand the impact COVID-19 and working from home has had on cybersecurity, Tripwire partnered with Dimensional Research to examine what security teams have faced and how they are managing the changing threat landscape.

This report covers findings from a survey conducted April 14 through April 21, 2020, outlining security professionals’ top areas of concern in the wake of COVID-19 and how they are responding.

A total of 345 qualified individuals from around the globe completed the survey. All had responsibility for IT security at a company with more than 100 employees.

### Participant Demographics

- **Region**
  - AMER: 75%
  - EMEA: 18%
  - APAC: 8%

- **Company Size**
  - 100–1,000 employees: 32%
  - More than 5,000 employees: 31%
  - 1,000–5,000 employees: 31%

- **Job Level**
  - Executive: 21%
  - Team manager: 47%
  - Individual contributor: 33%
63% have experienced COVID-19 related attacks

How has your company been impacted by COVID-19 related ransomware, phishing, and social engineering attacks?

- 61% We have been breached
- 37% There have been unsuccessful attempts
- 2% We haven’t had any attacks

68% experienced difficulty in dealing with COVID-19

How prepared was your security organization to deal with the impact of COVID-19?

- 56% We weren’t impacted by COVID-19
- 29% Somewhat prepared – we had a plan, but it was work to implement
- 12% Very prepared – it was simple to adjust
- 2% Not prepared – we scrambled to make it work
83% report a significant increase in employees working from home as a result of COVID-19

Which of the following statements most closely represents your company’s approach to employees working from home as a result of COVID-19?

- We made a rapid shift to enable a significant number of employees to work from home that had not prior to COVID-19
- We had many employees that worked from home before, but we increased that significantly because of COVID-19
- We had many employees that worked from home before, and that increased a bit because of COVID-19
- Most of our employees didn’t work from home before COVID-19 and they still don’t

94% are more concerned about security now than before COVID-19

What areas of your company’s security are you more concerned about now than you were before COVID-19? Choose all that apply.

- Employee home network security: 45%
- Increased ransomware, phishing, and social engineering attacks: 41%
- Keeping remote systems configured securely: 36%
- Keeping remote systems compliant: 36%
- Securing and analyzing the traffic coming through VPNs: 35%
- Authentication of remote devices: 35%
- Health of security team members: 34%
- Security short-cuts made to enable remote access to legacy applications: 27%
- Keeping remote systems compliant: 23%
- Backup of data on remote devices: 19%
- Increased threat from disgruntled, laid-off workers: 15%
- My security concerns are the same as before: 6%

Other
Most common: Physical security – Physical security of work from home setups; Theft of assets from empty offices; Physical security of offsite workplaces
Also: Health of remote workers; VPN; Lack of security in collaboration apps
89% say working from home makes it harder to do a great job at security

How has working from home impacted the ability of your company’s security staff to do a great job? Choose all that apply.

- Can’t effectively secure employees’ home office environments
- More challenging to manage what devices are connecting to the corporate network
- Harder to get visibility of remote assets and systems
- Harder to collaborate and communicate with each other as a security team
- Difficult to access all needed tools
- Don’t catch employee bad behaviors by casual observation
- Difficult to secure new infrastructure that was rapidly deployed to support working from home
- Challenging to effectively distribute and manage the workload of individual team members
- Other (please specify)
- It hasn’t impacted our security staff

83% are more concerned about the security of collaboration tools

How has your level of concern about the security of collaboration tools like Zoom, Webex, Teams, Slack, etc. changed as a result of COVID-19?

- Significantly increased 41%
- Increased somewhat 38%
- No change 32%
- Decreased 30%
- Other (please specify) 1%

Other: Secure VPN oversaturation; Users are accustomed to call the help desk for problems they could solve on their own
Almost half of security professionals believe employees are more susceptible to attacks when working from home

Which of the following statements best represents your opinion?

- Our employees are more susceptible to phishing, social engineering, and other security attacks when they work from home
- There is no difference in susceptibility to security attacks if employees are at home

65% report their security is worse because of COVID-19 (at least temporarily)

Overall, how do you think security of your company’s systems and data has changed as a result of COVID-19? Choose the one answer that most closely applies.

- We are significantly less secure than before
- We are slightly less secure than before
- We were temporarily less secure, but now it is the same
- There has been no change
- We are more secure now than we were before
Which of the following compliance activities are more difficult as a result of COVID-19? Choose all that apply.

- Assessing remote endpoints for compliance
- Determining how to apply compliance standards to remote endpoints
- Assessing new supporting infrastructure for compliance
- Determining the applicable scope for compliance standards
- Demonstrating compliance to auditors
- Discovering and cataloging Personally Identifiable Information
- Other (please specify)
- Compliance is not more difficult as a result of COVID-19

Into which of these types of data does your security team have the least visibility on remote systems? Choose up to three of the following.

- System update status of user endpoints
- Vulnerability assessment
- Backup status of user endpoints
- Remote access infrastructure
- Policy compliance
- Network management infrastructure
- Configuration hardening status
- We have excellent visibility into all of these

Overall, how has security visibility been impacted by increasing numbers of employees working remotely? Choose the one answer that most closely applies.

- Much more difficult
- Somewhat more difficult
- No change
- Somewhat better
- Much better

81% say compliance is more difficult because of COVID-19

64% report that security visibility is more difficult because of more employees working remotely

Other (please specify)

Data loss management; Physical security; Harder to access the systems that must be updated; Inventory is difficult or impossible; Bandwidth to access equipment is shared by hundreds of remote workers
84% are already taking steps to respond to COVID-19

What immediate steps is your security organization taking to respond to COVID-19? Choose all that apply.

- Expanding the use of current security tools: 53%
- Pausing new projects to focus on response: 53%
- Investing in new security tools: 28%
- Increasing security budget for this year: 26%
- Other (please specify): 3%
- We are not doing anything special: 13%
- I can’t say—our plans keep changing: 2%

Other: Secure VPN oversaturation; Users are accustomed to call the help desk for problems they could solve on their own.

92% are already thinking about the future in a COVID-19 world

What steps is your security organization taking now to better prepare for the future? Choose all that apply.

- Identifying new tools to address the post-COVID-19 environment: 57%
- Identifying capabilities in existing tools that are underutilized: 53%
- Investing in staff training for new skills required: 42%
- Considering managed services to reduce staff burden: 31%
- Planning for a reduced security budget in 2021: 14%
- Other (please specify): 1%
- We are not taking any special steps: 8%

Other: Hardening current systems and implementing new redundant ones; “Deconflict profitability and security”; “Don’t have time to think about that at this moment in time.”
53% are increasing security investments (at least temporarily)

How are security investments at your company changing as a result of COVID-19?

- Increasing temporarily: 36%
- Increasing long term: 18%
- Decreasing: 4%
- No change: 4%
- Too soon to say: 18%

Broad agreement about many of the impacts of COVID-19 on security

Please indicate your level of agreement with each of the following statements.

- When everyone is a remote worker, security coverage needs to be much wider: 54% Strongly agree, 33% Agree somewhat, 10% Disagree somewhat, 4% Strongly disagree, 1% Strongly disagree
- The real security repercussions of COVID-19 are yet to be realized: 9% Strongly agree, 31% Agree somewhat, 40% Disagree somewhat, 10% Strongly disagree
- COVID-19 is going to force security to do even more with less in the coming year: 30% Strongly agree, 18% Agree somewhat, 54% Disagree somewhat, 5% Strongly disagree
- COVID-19 has been a stress test of every security control and policy we have: 3% Strongly agree, 28% Agree somewhat, 61% Disagree somewhat, 3% Strongly disagree
- COVID-19 has forced us to make security tradeoffs in order to move quickly to support remote workers: 22% Strongly agree, 43% Agree somewhat, 20% Disagree somewhat, 14% Strongly disagree
- The rapid expansion of infrastructure to support remote workers has left us exposed from a security perspective: 10% Strongly agree, 40% Agree somewhat, 30% Disagree somewhat, 20% Strongly disagree

COVID-19 has been a stress test of every security control and policy we have
Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world’s leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations’ digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. Learn more at tripwire.com

The State of Security: News, trends and insights at tripwire.com/blog
Connect with us on LinkedIn, Twitter and Facebook

©2020 Tripwire, Inc. Tripwire, Log Center/LogCenter, IP360, Tripwire Axon and others are trademarks or registered trademarks of Tripwire, Inc. All other product and company names are property of their respective owners. All rights reserved.