ELECTRIC 2021

CYBERSECURITY REPORT

Evaluating the Pandemic's Impact on Remote Work & Cybersecurity

A Whitepaper by the Electric Research and Insights Division
**Executive Summary**

The Electric Research and Insights division surveyed cybersecurity industry professionals to discover the impact the COVID-19 pandemic is having on cybersecurity and remote work practices at their respective organizations. The research took place in December 2020 to assess how these professionals are dealing with cybersecurity challenges 9+ months into the pandemic. Respondents self-identified as either working as a cybersecurity professional or being responsible for cybersecurity at their organization, e.g., an IT professional.

Remote work has presented additional challenges that cybersecurity professionals need to keep in mind, including inexperienced employees, unsecured home networks, and unsecured devices. At a high level, the results of our survey indicate the majority of respondents are more concerned with cybersecurity as a result of these additional challenges and have subsequently implemented new security measures and protocols to mitigate risk. However, the findings also indicate that a higher level of adoption of more advanced security measures like a zero trust policy or endpoint detection and response solution might be necessary to actually improve respondent organizations’ security posture.

While near-universal work from home was initially thought to be a temporary situation at the outset of the pandemic, it is likely that we will be living with this model of work for a long time. This means that companies need to develop long-term, sustainable protocols to manage remote business operations while avoiding data breaches and cyber attacks. Data breaches are always a concern for companies whether or not they have a distributed workforces.

According to IBM’s “Cost of a Data Breach” report, the global average cost of a data breach is $3.86 million. While that may be manageable for large corporations, that could put small and medium-sized businesses—common victims of cyber attacks—out of business. Of those surveyed in the IBM report, 70% said that remote work would “increase the cost of a data breach” and 76% said that remote work would “increase the time to identify and contain a breach.”

The Electric Research and Insights division additionally found in the following survey that 96% of respondents have subsequently made at least some changes to their security strategy as a result of more people working from home during the pandemic. We wanted to conduct this study to help organizations benchmark how they are dealing with the challenges of maintaining a secure remote workforce amidst the ongoing pandemic compared to others. This whitepaper will present our findings from a group of cybersecurity decision makers.
Findings At a Glance:

- 96% of respondents have made at least some changes to their security strategy as a result of more people working from home during the pandemic.

  Of those changes, the most common were:
  - 55% Sharing a guide on cybersecurity and working from home
  - 44% Installing the latest patches
  - 39% Implementing multi-factor authentication (MFA)

- 76% of respondents are more concerned with social engineering attacks as a result of the pandemic.

- 71% of respondents indicated an employee at their organization succumbed to a social engineering attack attempt since the outset of the pandemic.

- 93% of respondents are at least taking some additional precautions to mitigate against supply chain attacks, IP Theft, Advanced Persistent Threats, cyberespionage, or IoT as an attack vector as a result of the pandemic.

Respondents rated the following as the three most concerning behaviors related to employees working remotely:

1. Another person having access to an employee’s company device
2. Using untrusted networks
3. Using personal messaging services for both business and personal reasons
Examining Cybersecurity Concerns at Respondent Organizations

76%

indicated that they are more concerned with social engineering attacks at their organization as a result of the COVID-19 pandemic.

On the following pages, we take a look at overall cybersecurity concerns as they relate to adapting to the pandemic. We also specifically ask about concern related to social engineering attacks (phishing, spear phishing, malware, vishing, etc.) and which employee behaviors respondents consider most concerning when working remotely.

The results indicate a majority of respondents (57%) are moderately to extremely concerned about their organizations’ ability to adapt to the COVID-19 pandemic. This concern is justified, as 71% of respondents indicated an employee at their organization succumbed to a social social engineering attack attempt since the outset of the pandemic.

1. Please rate the level of overall cybersecurity concern related to your organization as it currently stands as a result of adapting to the COVID-19 pandemic:

2. Are you more concerned with Social Engineering attacks (Phishing, Spear Phishing, Malware, Vishing, etc.) at your organization as a result of the COVID-19 pandemic?
71% indicated an employee at their organization succumbed to a social engineering attack attempt since the outset of the pandemic.

3. Have any employees at your organization succumbed to a social engineering attack attempt since the outset of the COVID-19 pandemic?

(Phishing, Spear Phishing, Malware, Vishing, etc.)

4. Which of the risky employee behaviors below is most concerning when employees are working remotely?

- Another person having access to an employee company device: 33%
- Using untrusted networks: 29%
- Using personal messaging services for both business & personal reasons: 17%
- Unintended company information disclosure: 10%
- Randomly switching from business to personal devices: 6%
- None of these are concerning to my organization: 5%
Examining How Respondent Organizations are Mitigating Cybersecurity Risk

96% indicated that they are making some changes to their security strategy as a result of people working from home because of the pandemic.

In the graphs below, we take a look at how respondents are implementing changes to mitigate cybersecurity risks at their respective organizations. We also ask about budget relating to the investment in cybersecurity.

Our results indicate that a majority of respondents (96%) are making at least some changes to their security strategy as a result of more people working from home as a result of the pandemic. Likely in response to the increased concern noted in the earlier part of this survey, a majority of respondents (56%) indicate they plan on increasing investment in cybersecurity for 2021.

5. Have you taken any additional precautions to mitigate against: supply chain attacks, IP Theft, Advanced Persistent Threats, cyberespionage, or IoT as an attack vector as a result of the COVID-19 pandemic?

6. Have you made any changes to your security strategy as a result of more people working from home as a result of the pandemic?
7. **If you have made changes, what are they? Choose all that apply.**

- Shared a guide on cybersecurity and working from home: 55%
- Installed the latest patches before people started working from home: 44%
- Implemented multi-factor authentication: 39%
- Started providing additional IT support from home: 30%
- Provided VPN for employees: 28%
- Implemented pre-approved applications for collaboration and calls: 26%
- Enforced using only company devices for work purposes: 23%
- Implemented application control and content filtering: 23%
- Implemented a zero trust policy: 19%
- Provided modems to employees: 13%
- Altered alert levels in endpoint detection and response solution: 10%

56% indicated they will increase spending in 2021 as it relates to cybersecurity.

---

8. **Looking forward to 2021, how does your organization plan on spending as it relates to cybersecurity?**

- Increase investment: 56%
- Keep investment the same: 40%
- Decrease investment: 4%
Conclusion

Survey respondents are more concerned about maintaining cybersecurity at their respective organizations because of the pandemic. However, in question seven, in which we ask what changes they have made since the outset of the pandemic. The most common change implemented among respondents was providing employees with a cybersecurity guide, which, while important, is not a sufficient security measure or a form of actual defense unless properly enacted by employees.

Even security measures like providing VPNs (28%) and implementing MFA (39%) ranked lower than the guide, despite them widely being considered critical to ensuring a secure remote workforce.

Although 96% of respondents reported they have made at least some changes to their security strategy as indicated in question 6, there is still a substantial margin by which the measures need to be improved. The survey results illustrate a clear knowledge gap in what respondents think will protect their organizations vs. actually taking definitive steps to bolster cybersecurity protections.

With that being said, we’ve put together the following recommendations on How to Maintain Cybersecurity in a Remote Workforce.
How to Maintain Cybersecurity in a Remote Workforce

1. **Follow Established Frameworks**
   Cybersecurity best practices can be adapted to most kinds of work environments, and developing a plan does not require you to start from scratch. Many IT security experts recommend following the guidelines established by the National Institute of Standards and Technology (NIST) in its **Cybersecurity Framework**. It consists of five “core” functions that organizations should perform continuously:

   - **Identify** - Understanding the current state of your assets and data and who has access to them.
   - **Protect** - Creating the safeguards necessary to limit the access and release of sensitive data.
   - **Detect** - Implementing tools and actions that can detect breaches or suspicious events.
   - **Respond** - Developing protocols that allow you to quickly take action in the result of a data breach.
   - **Recover** - Developing protocols that allow the organization to resume normal activity in the case of an incident.

2. **Consider Zero Trust Architecture**
   Zero Trust is a security methodology that is centered on the assumption that no person or device inside or outside of a network can automatically be trusted. Users and devices must be authenticated and authorized to access multiple, smaller perimeters to access data. The concept of trust is usually divided into five main **pillars**:

   DEVICE | USER | SESSION | APPLICATION | DATA

   Once trust has been initially established, then the system will grant or deny access. In addition, it is important to regularly re-verify all of the pillars. Zero Trust architecture is maintained through a combination of protocols including multi-factor authentication, privileged access, and real-time monitoring.

   In a time when many employees are accessing company data from everywhere but the office, it is particularly important to have security measures in place to address this change.
3. **Educate Employees About Cybersecurity**

Conversations about cybersecurity threats need to happen more than just during an employee’s initial onboarding. This is education that must continue throughout the entirety of a person’s time with the organization. Consider scheduling regular educational sessions with remote employees explaining how security is particularly important now when they do not have the protections of the office environment.

Education should not only be centered around tasks that employees can take to secure home networks or devices. It’s also important to discuss how cybersecurity is the responsibility of everyone in a company, not just IT or management. Some employees—especially those who do not work with sensitive information a part of their jobs—may not be aware that they could be vulnerable to hackers or malicious actors.

In addition, regularly sending emails and newsletters about remote work and security will help keep this issue at top of mind.

4. **Develop a Remote Cybersecurity Policy**

If you have not done so already, now is the time to develop a remote work cybersecurity policy that is specific to the current situation. Here are some recommendations for what it should address:

- Company-issued device usage for non work-related activities
- Limitations on what can be accessed from personal devices
- Securing home wireless networks
- How to notify IT of a possible attack or phishing scheme
- A response plan that allows employees to quickly get back to work
Methodology

Respondents self-identified as either working as a cybersecurity professional or being internally responsible for cybersecurity at their organization, e.g. an IT professional. The survey is based on the responses from 167 individuals.

All of respondents are from the United States. All geographic regions were represented in the study.

The respondents work at organizations with employee headcount between 10 - 500 employees. The Electric Research and Insights division commissioned the study in December 2020.

About Electric

We’re the new standard of IT.

Electric is revolutionizing IT support. Through a first of its kind technology, paired with an elite squadron of IT technicians, Electric delivers lightning-fast IT support. Whether you’re remote or onsite, Electric provides real-time issue resolution, security at the device, app and network levels, employee onboarding/offboarding and IT management (device, inventory, network, server, application, cloud, procurement, provisioning and strategic projects).

Contact Electric

Electric.ai
Twitter.com/Electric_AI
hello@electric.ai