COVID-19’s Impact on Organizational Cybersecurity Posture

By Douglas Shuman https://www.linkedin.com/in/douglas-shuman-06221b122/

In the second of a two-part series, this article focuses on a survey of how organizational cybersecurity transformed due to remote work during the pandemic.

Abstract

Organizational cybersecurity landscapes changed as a result of employees working from home during the COVID-19 pandemic. This research focuses on a survey of how organizational cybersecurity transformed due to remote work during the pandemic. The survey found further reliance on VPN and VDI, an increase of MFA usage for remote access, and some slight negative trends which eased the employee experience or the impact to technology. Organizations need to ensure they are continually evaluating how they secure their environment to allow for remote work and ensure best practices are in place.

Introduction

When the significance of COVID-19 became clear in early 2020, many organizations’ cybersecurity landscapes changed as a result of sending employees home to work remotely. Organizations had little time to prepare for a crisis response and suddenly sent employees to work remotely. Because the cybersecurity landscape of remote work influenced by the coronavirus is still being learned, I performed a survey to address areas not well documented. This survey addresses gaps identified in Part 1 (literature review) of this two-part series. Current literature does not provide much insight on what remote access solutions were used, how remote authentication was configured, what devices people used for remote work, if internal resources were externalized, and employee sentiment for organizational cybersecurity and remote work. Due to the abrupt changes, organizations need to reflect on and continually evaluate their cybersecurity posture to prevent potential incidents. At the time of writing, organizations have mostly moved on from the changes required to enable high-volume remote work to supporting remote work over the long term.

Regardless, decisions with cyber implications made during the beginning of 2020 are likely still putting organizations at risk. The research question serving as the foundation for this survey and the literature review in Part 1 was: as a result of COVID-19, how have organizations’ cybersecurity postures changed due to the influx of people working from home? Specifically, how have cybersecurity postures weakened or improved?

Research Method

The research method I chose was quantitative with online surveys through the Qualtrics platform. This is the most appropriate method because I collected data from a variety of employees who work for different organizations. Prior to collecting results, my hope was that survey results would illustrate patterns in the ways organizations enabled work from home during the pandemic regarding cybersecurity. This would show if organizations successfully applied cybersecurity best practices or if they made decisions that harmed security posture. Surveys were distributed to Pennsylvania State University students in the College of IST Master of Professional Studies Degree and Certificate programs. My expectation was that these students work for a variety of employers of different industries and sizes, producing a diverse survey set.

Survey Findings

A total of 61 responses were collected prior to removal of unusable responses, producing 53 complete responses. In terms of response rate, the survey was sent to approximately 200 students, meaning about 25%–30% of students responded to my survey. This section includes the results and highlights the notable findings with some relevant tables and figures.

Demographics Questions

Responses were primarily U.S. based, but some were international based on IP geolocation estimates. The top industries
that participants indicated they worked for include: 28.30% for Information, 16.98% for Education, and 16.98% for Public Administration (government). See Table 1 for the full breakdown.

<table>
<thead>
<tr>
<th>#</th>
<th>Answer</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Accommodation and food service</td>
<td>1.89%</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Arts, entertainment, and recreation</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Education</td>
<td>16.98%</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Financial and insurance</td>
<td>5.66%</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Healthcare</td>
<td>7.55%</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>Information</td>
<td>28.30%</td>
<td>15</td>
</tr>
<tr>
<td>8</td>
<td>Manufacturing</td>
<td>3.77%</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>Energy and utilities</td>
<td>1.89%</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>Public administration (government)</td>
<td>16.98%</td>
<td>9</td>
</tr>
<tr>
<td>12</td>
<td>Real estate, rental, and leasing</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>Retail</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>Transportation and warehousing</td>
<td>5.66%</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>Other</td>
<td>7.55%</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>Not employed</td>
<td>3.77%</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>100%</td>
<td>53</td>
</tr>
</tbody>
</table>

Table 1 - Table of respondent industry representation

The majority (77.36%) of respondents work for large organizations, with only 10 working for small or medium organizations. 86.79% of participants worked from home during the pandemic. Those who did not work from home could have for a variety of reasons, such as they were unemployed, they could continue working from their normal workplace, or they were essential workers who needed to physically be in their workplace. Respondents who did not work from home did not receive the following questions.

**Exposure Questions**

The survey responses in this section focus on questions about how organizations enabled work from home before and after the pandemic. Responses for eight questions are in this section.

**Remote access solutions pre-pandemic**

The next three responses address how employees remotely accessed their organization before the pandemic, if at all. Sixty-four point sixty-two percent of selected remote access solutions in use were virtual private network (VPN), 6.15% were zero-trust network access (ZTNA), 24.62% were virtual desktop infrastructure (VDI), and 4.62% did not know what they used. No participants indicated they did not have a remote access solution before the pandemic, meaning this data set cannot provide insight into organizations that needed to implement a remote access solution where one was not previously available.

**Remote access authentication frequency pre-pandemic**

The majority (80.43%) of respondents authenticated every day for remote access. However, 6.52% indicated they were only prompted to authenticate for remote access the first time they connected, which is concerning, and 13.04% authenticated less than once every workday.

**Remote access MFA frequency pre-pandemic**

Most organizations implemented multifactor authentication (MFA) for remote access, which is best practice. Of those, 63.04% used MFA every time they connected, and 17.39% used MFA less than once a workday. Unfortunately, 17.39% did not have MFA implemented for remote access.

**Remote access solutions during pandemic**

The following three responses indicate how employees remotely accessed their organizations after the pandemic began. During the pandemic, there was a slight increase in VPN usage (by two respondents) and VDI usage (by four respondents). There was no increase in ZTNA usage since the same respondents who used ZTNA after the pandemic began also used it pre-pandemic. This is somewhat discouraging because organizations increased their dependency on legacy VPN and did not adopt the modern ZTNA.

**Remote access authentication frequency during pandemic**

Regarding how often respondents authenticated during the pandemic, there were minimal differences. One additional participant indicated they authenticated once a day, and two more indicated they only authenticated the first time they connected. Ease of use for the employee experience could be the cause of the slight increase in users only prompted for authentication initially, but this is speculation for a change that minor.

**Remote access MFA frequency during pandemic**

MFA did have an increase in usage, where four more people used MFA every day. Additionally, there was a reduction of four people who did not use MFA for remote access at all. This is an encouraging trend, which points to employers taking MFA seriously with increased remote access to their networks.

**Work devices during the pandemic**

The next set of responses are for work-from-home devices used during the pandemic.

Of the respondents, 78.26% used a managed device from their employer, 15.22% used an unmanaged personal device, and 6.52% used a managed personal device. Only one respondent was provided an employer (aka “corporate”) owned and managed device after the pandemic began. This suggests for most employees, if an employee did not have an employer-owned device when the pandemic started, they typically used a personal device. While it is best that most employees used employer-owned devices, it is concerning how many employees used unmanaged personal devices. The amount of unmanaged personal devices in use was likely due to employers lacking the setup to manage personal devices or the shortage of devices on the market.
COVID-19’s Impact on Organizational Cybersecurity Posture | Douglas Shuman

### Table 2 - Table of devices used for remote work during the pandemic

#### Externalizing internal resources

These responses are about employers making websites available on the public Internet which were previously internal. This is not necessarily a cybersecurity issue since it can be done securely, but this is the key: organizations need to ensure appropriate security controls are in place if they put internal resources out on the Internet. Of the participants, 19.57% indicated their organization made websites which do not work with sensitive data external, and 4.35% said their organization made websites that work with sensitive data external. Overall, this is nearly a quarter of respondents whose employers externalized websites. This provides two benefits: employees can access those resources without needing to go through remote access, and there is less strain on the organization’s network to allow access to those resources from the Internet.

### Table 3 - Table of if employers externalized any previously internal resources/websites

#### Outcome Questions

The remaining responses of the survey focus on employee sentiment regarding their organization given their work from home experience. How employees felt was likely influenced by how they responded to the prior exposure questions. Responses for three questions are in this section.

#### Organization security sentiment

Overall, most participants felt positive about their organization in terms of cybersecurity with respect to their work from home experience. In figure 1, we see most respondents (71.74%) felt their organization was as secure as it was before work from home was enforced, 19.57% perceived their organization as more secure, while 8.70% felt it was less secure. Interestingly, of those who felt their organization became less secure during the pandemic, over half of those respondents used an unmanaged personal device for work.
Learning to offer secure telework

Finally, most respondents felt their organization learned how to securely provide work from home (71.74%). However, 15.22% felt their employer did not learn, and 13.04% were unsure. There was not a significant trend in responses for those who selected the latter two options. Four of those respondents used unmanaged personal devices, and two respondents did not use MFA for remote access.

Figure 3 - Histogram of employee sentiment on if organizations learned how to securely provide work from home

Discussion

Before I sent out this survey, I had a few hypotheses written down. These were the following:

Hypothesis 1

My first hypothesis was that most respondents would have worked from home during the pandemic. I expected this because of the survey pool of Penn State IST graduate students, who I assume to mostly be in the tech industry with office jobs. My survey results confirmed this hypothesis, with 86.79% of participants working from home during the pandemic. Interestingly, four out of the five respondents who worked during the pandemic, but not at home, had government jobs.

Hypothesis 2

My second hypothesis was that most organizations relied on VPNs for remote work during the pandemic. This hypothesis was also confirmed. In fact, other than one respondent who did not know what their organization used and one respondent who did not use remote access, every participant had a VPN solution in place during the pandemic. Interestingly, four out of the five respondents who worked during the pandemic, but not at home, had government jobs.

Hypothesis 3

My third hypothesis was that most respondents would have managed devices when they began working remotely during the pandemic. I expected this for the reasons in the first hypothesis regarding assumptions of the survey pool. This hypothesis was also supported, with 76.09% of respondents working with managed devices they had before the pandemic.

Hypothesis 4

My last hypothesis was that most people would feel their organizations responsibly provided remote work despite insecure decisions made. This was not supported, although it was the second most selected option. Instead, most participants felt their employer ensured security without compromises. It is important for employers to show that they take cybersecurity seriously. If employers do not take cybersecurity seriously, neither will the employees.

Research Limitations

There are some considerations for these survey results. First is that I did not have as large a sample size as I would have liked, meaning that the results could differ if the sample size were larger. I also speculate that the industry with the most selections, “Information,” was chosen because most participants work in the IT department, where they should have selected the industry with which their organization is accurately aligned. This also brings up the limitation of my sample size being students obtaining IT degrees (who likely work in IT), so the response results may be different if people in other job roles completed the survey. Although, I expect employees in non-technical roles may have some difficulty responding to the question set, possibly selecting “unsure” and “unknown” more often.

Also, I did not specifically ask what employers people work for, because I did not want employees disclosing potential vulnerabilities for their named employers. This means if more than one representative from the same employer completes the survey, then the total counts are inflated by that employer. Due to this, larger organizations could have more influence on total counts in the survey because they have more employees.

Topics for Future Research

There were several ideas which stood out to me that could use additional research across parts 1 and 2 of this series. Some thoughts include:

- Prevalence of organizations instating security policies for work from home, and what these policies contain (limiting work locations, devices listening, etc.).
- Prevalence of organizations experiencing COVID-19 themed cyber attacks to understand what attacks were seen and how successful they were. This could include counts of COVID-19-related incidents such as:
  - Phishing
  - Pharming
  - Malware installs
  - Attacks targeting remote work infrastructure (e.g., VPN, remote access protocols)
- Metrics of cyber attacks targeting resources related to COVID-19 (e.g., vaccine/medical research, government financial aid)
- Since all my respondents had remote access solutions in place before the pandemic, additional research is needed...
to learn what solutions were implemented for organizations who did not previously support remote access.

Conclusion
This survey provided insight on how securely organizations implemented new work from home programs. There was an increase in VPN and VDI usage during the pandemic, but little to no increase in ZTNA usage. Most organizations followed the best practice of requiring employees to authenticate and use MFA once a day for remote access. MFA usage increased for remote access, which is an encouraging trend. Most devices used for work were employer owned and distributed before the pandemic. Employees who had insecure implementations for remote work often indicated their organization felt less secure, did not provide adequate security, and/or indicated their employer did not learn how to securely offer remote work. If you are interested in reviewing the full dataset for this survey, please contact me at my LinkedIn page.

Organizations should consider moving away from legacy VPN technology, which does not scale well for fluctuating amounts of remote work. Instead, we should invest more in zero trust network access solutions which solve this and offer additional security. Employees should authenticate and use MFA to begin each remote access session, because organizations need to verify the users who access their network. Employer owned devices are generally the most secure because the employer fully controls the security configuration. With the understanding that personal devices are sometimes necessary for work, employers should ensure they manage those devices. Finally, organizations must consider that any internal resources accessible from the Internet are inherently at greater risk from threats like hackers and previous employees. If more resources are Internet accessible, organizations must ensure appropriate security controls are in place, so they are protected from attacks.

Because of the sudden shift to allow employees to work from home, changes were made which posed cybersecurity risks. Organizations must continually evaluate and implement best practices for cybersecurity. This is especially important because of the many drastic changes made as a result of the COVID-19 pandemic.

About the Author
Author Douglas Shuman has about 5 years of experience working in cybersecurity, primarily as a cyber risk analyst. He recently completed his Master’s Degree in Cybersecurity Analytics and Operations from Penn State University and is certified in Open Factor Analysis of Information Risk (FAIR). His focuses are cyber risk assessments and cybersecurity consultation. He can be reached at his LinkedIn page.