COVID-19 and At-Home Workers, Cybersecurity Considerations

March 25, 2020

The British writer and politician Benjamin Disraeli once observed that the fear of danger should be a spur to preventing it, noting too that he who fears not gives advantage to the danger.

This sentiment seems especially relevant regarding cybersecurity in light of the now-mandatory work-from-home environment we find ourselves facing thanks to COVID-19. As small and midsized companies that had previously rejected the idea of remote workers find themselves scrambling to implement exactly that, it is important to appreciate the particular risks that a distributed workforce presents and to review some simple measures to address them. Not to do so would – in Disraeli's words – give advantage to the danger presented by cybercriminals, and compound the injury we are all now experiencing.

Forced At-Home Workers

As data privacy regulations have ramped up, there has been a lot of ink spilled by a lot of lawyers about the cybersecurity implications of a remote workforce. However, that was then and this is now. Thousands of companies, due to shelter-in-place orders and mandatory quarantines, have been forced to deploy a distributed workforce rapidly, and with little, if any, time to plan or evaluate the legal implications.

Cyber-Risks of At-Home Workers

From where we sit, the most useful approach to this situation is to first outline the operational steps clients can take immediately to minimize the chances of a cybersecurity incident. Next comes an overview of the potential contractual liabilities a distributed workforce presents, including the potential impact on insurance coverage. Accordingly, any discussion of the legal risks of a newly distributed workforce has to start with managing human behavior.

Why? Because the most common cybersecurity breach is so-called "social engineering." Social engineering is manipulating, gaslighting, or otherwise tricking people into lowering their guard and inadvertently opening up a network to bad actors. This can happen in a lot of different ways. Interestingly, several of the most popular methods for this are probably much harder to pull off when workers are at home instead of in the office. For instance, in a remote workplace, the risk is lower of physical intrusion by those pretending to be employees and getting through security, or tricking workers into inserting purposefully corrupted physical media (like thumb drives) into office machines. For both of these methods, home offices are probably actually safer.

There is increased risk, however, of "phishing" and "spear-phishing," popular hacking techniques that are part social engineering, part technological. In each instance, a target receives an email intended to deceive the recipient into taking some (reportedly urgent) action they should not, and that action compromises their

computer or network. Phishing emails tend to be general and eye-catching (You've been selected! Click here to Redeem!), while spear-phishing emails are more targeted and appear to be from a known sender (Purportedly from CEO: Hi, Bob. I am at home under quarantine and accounting needs you to approve the attached forms). In either event, clicking on the link or attachments can deploy malicious software that allows the scammer to infiltrate the local computer and any larger network to which the computer is connected. While workers in their offices may tend to be careful about such things, their defenses relax a bit while at home dealing with kids, dogs, laundry, or whatever. There's been a spike recently in COVID-19 phishing emails, assuredly proving that this tactic works. Distributed workers are easier targets for this sort of thing.

The final hacking category is pure technology, and this is where a distributed workforce can be especially vulnerable. Out-of-office workers tend to rely on personal or third-party equipment and Internet access. This equipment may not be updated as frequently as business equipment. It also tends to use softer passwords that are not updated as often, may not include enterprise-grade antivirus software for detecting and preventing malicious code or activity, and is not monitored as closely as office-based networks. All of this makes it easier for hackers to enter, explore, and manipulate or steal data flowing into or out of the remote worker's devices.

All in all, a distributed workforce is simply riskier than a centralized one from a cybersecurity standpoint.

Lowering the Risk

What, then, can a business do to protect itself in the scramble to distribute its workforce? The steps are simple (if not always easy):

- Use company equipment for accessing and processing data, whenever possible
- Encrypt data at rest (i.e., on hard drives and servers)
- Encrypt data in transit (i.e., secure email)
- Use virtual private networks to access servers
- Use multi-point authentication to access data
- Train and retrain your team members in security protocols
- Choose your vendors carefully, and monitor them closely
- Keep your network updated and patched

Review Contract Requirements

In addition to these actions to lower the risk presented by a distributed workforce, it is also important to review any information security requirements in your contracts with key customers or business partners. If your contracts specify security standards for data processing activities, it is important to ensure that your distributed workforce still meets those requirements. Failing to do so may put you at risk for breach of contract and may subject you to significant money damages. If the information technology and security configuration of your

remote workforce seems problematic in light of your contract requirements, seek modifications or waivers from your counterparties, even if temporary.

Review Regulatory Requirements and Guidance

Similarly, and particularly important for industries like financial services and healthcare, regulatory compliance is critical. In response to the pandemic, many regulatory bodies across the country have issued guidance loosening their requirements. It remains essential, though, for regulated firms to confirm that the operational and technological changes made in moving to a distributed workforce do not jeopardize their compliance status, and applicable licenses remain in effect.

Regulatory compliance is often dependent on a complex, interrelated matrix of state and federal requirements. It is important to consult with counsel to ensure you know the applicable regulations, which are often challenging to interpret when applied in a work-from-home environment. For example, if you are processing loan applications remotely, is your home now a branch office? If you are working at the dining room table and your husband is around, does that constitute a cybersecurity breach? The answer differs from jurisdiction-to-jurisdiction, regulator-to-regulator and is highly fact-specific. When in doubt, enlist regulatory counsel for guidance.

Review Insurance Coverage and Exceptions

The manner in which you deploy a remote workforce can also affect your insurance status, depending on the specific language of your policies. If you have a cyber-liability policy, and your employees are working remotely, are you covered in the event of a data breach through the data processing activity of an at-home worker? Policies differ widely and should be reviewed carefully in light of your particular operations.

Conclusion

Returning briefly to Mr. Disraeli, the COVID-19 situation is unique because there is a large-scale government mandate effectively requiring companies to distribute workflows. For companies that have resisted remote-work arrangements previously, let the situation spur action to mitigate the increased risk these arrangements present. To do otherwise could quickly compound an already trying time.

If you have questions, reach out to one of the authors of this alert or another member of the firm's Cybersecurity and Data Privacy team, or visit our **COVID-19 Resource Center**.