VORYS

Publications

Cyberattacks on the Rise During the COVID-19 Pandemic

Related Professionals

Petra G. Bergman

Brent D. Craft

Marcel C. Duhamel

J.B. Lind

Jacob D. Mahle

Eric W. Richardson

Emily E. St. Cyr

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 4.20.2020

Cyberattacks are on the rise and novel cybersecurity risks are emerging due to the unprecedented changes in the way companies and their employees are currently forced to do business. In the last month, cyberattacks have exploited the unique challenges that businesses face due to increased teleworking. Some examples include:

Hacking

Companies are reporting increased instances of hacking. For example, two websites operated on behalf of the San Francisco International Airport (SFO) recently announced that they were the targets of a cyberattack in March 2020. The attackers inserted malicious computer code on these websites to steal users' login credentials.

Video-teleconferencing hijacking (Zoombombing)

In late March, the Federal Bureau of Investigation (FBI) warned of teleconference hijacking after two schools in Massachusetts were "zoombombed" by individuals who accessed the virtual classrooms, shouted profanities, and displayed hate symbols.

These attacks continue to occur. For example, a video-teleconference meeting of the Milwaukee Election Commission had to be shut down due to zoombombing after pornographic images and racial slurs began appearing on the computer screens of meeting participants.

Zoom is also facing an increase in class action lawsuits alleging violations of the California Consumer Privacy Act (CCPA), as we reported in this alert.

Data breaches

Due to the extreme increase in the number of individuals who are working remotely, companies are highly susceptible to data breaches. For example, SCUF Gaming, a manufacturer of high-end gaming controllers, announced recently that it had suffered a data breach. In its announcement, SCUF explained that that the "issue was specific to one system, being operated off-site ***due to work-from-home precautions resulting from the current COVID-19 pandemic."***

Fraud

Fraudulent scams are also more frequently emerging in the current climate. In early April, the FBI warned that business email compromise (BEC) scams, which target businesses that perform funds transfers, are on the rise, including scams targeted to exploit COVID-19. The warning noted an increase in BEC frauds targeting municipalities purchasing personal protective equipment or other supplies needed in the fight against COVID-19.

Businesses are having to quickly adapt to operate with a remote workforce and, without proper precautions, remote working can increase a company's exposure to the types of threats and cyberattacks described above. Cybercriminals will rely on these adjustments, which have been made on short notice, to exploit the vulnerabilities businesses are trying to address while remaining operational. The following precautions are a few of the steps businesses can take to protect themselves, their employees, and their data from cyberattacks.

- **Review and communicate data security policies and practices:** Review and update data security policies to ensure they are compatible with a remote work set-up. Communicate data security policies to your employees, and send frequent reminders to employees regarding data security best practices while working from home.

- **Limit the access to protected and confidential information:** Consider restricting employee access to confidential and protected information on a role-specific basis to ensure employees have access to only the information needed to complete their specific duties.

- **Use VPN access when able:** To the extent possible, encourage employees to work using a Virtual Private Network (VPN) or other secure form of remote access, which will provide an additional layer of protection to your company's information.

- **Be mindful of COVID-19 centric scams and phishing emails:** Remind employees to be diligent in their review of emails prior to opening links or attachments, and to report phishing attempts as soon as possible once discovered.

- **Remind employees to keep information confidential:** Be mindful of the potential presence of third-parties when using cell phones, teleconferencing or video conferencing to conduct confidential conversations.

- **Secure videoconferencing meetings:** Utilize the security features offered by your company's selected videoconferencing software, including access by invitation, locking meetings once initiated, disabling screen sharing when practical, and using a virtual waiting room before the host joins. The most robust security features are included in enterprise-grade videoconferencing systems. Using "free" conferencing platforms often comes at a significant price to your company's security.

Vorys offers training to law departments, sales teams, customer service teams, and your workforce generally on the above topics. To read more about this training, click here. If you have questions about the impact of COVID-19 on your data security policies and practices, please contact a member of the Vorys cybersecurity team: Petra G. Bergman, Brent D. Craft, Marcel C. Duhamel, J.B. Lind, Jacob D. Mahle, Eric W. Richardson and Emily E. St. Cyr.

--

Vorys COVID-19 Task Force

Vorys is continuing to monitor the COVID-19 outbreak and related guidance to insurers. In addition, Vorys attorneys and professionals are counseling our clients on a myriad of others issues related to the outbreak. We have established a comprehensive COVID-19 Task Force, which includes attorneys with deep experience in the niche disciplines that we have been and expect to continue receiving questions regarding coronavirus. Learn more and see the latest updates from the task force at vorys.com/coronavirus.