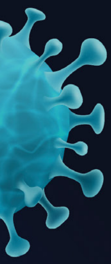


INFORMATION SECURITY and PRIVACY BEST PRACTICES in the Age of Pandemic

BY ELIZABETH B. VANDESTEEG, PARTNER & KATHRYN C. NADRO, ASSOCIATE, SUGAR FELSENTHAL GRAIS & HELSINGER LLP

The COVID-19 pandemic has changed, perhaps permanently, how and where employees get their work done. A majority of the U.S. workforce is currently working remotely, and in the last several weeks corporate giants such as Google, Twitter, and Facebook have announced that some employees will be permitted to continue working remotely indefinitely. Other companies have stated they are not reopening their offices for at least one to three months, according to a recent survey conducted by Littler Mendelson PC.[1]

In light of this new reality, how should businesses ensure proper information security practices by their remote workforces? And for those businesses that are contemplating a broader return to the office, how should they approach the new privacy and information security issues arising from the pandemic?

Shoring Up Weaknesses

Due to the pandemic, many companies were forced to implement widespread remote work environments with little or no notice in March 2020. For many companies, these hastily implemented arrangements resulted in less-than-ideal data security and privacy practices. Countless employees had no choice but to use communications technology without appropriate safeguards in place, to create workarounds with applications to get work done, and to work from personal devices without security protections, like virtual private networks (VPNs), in place.

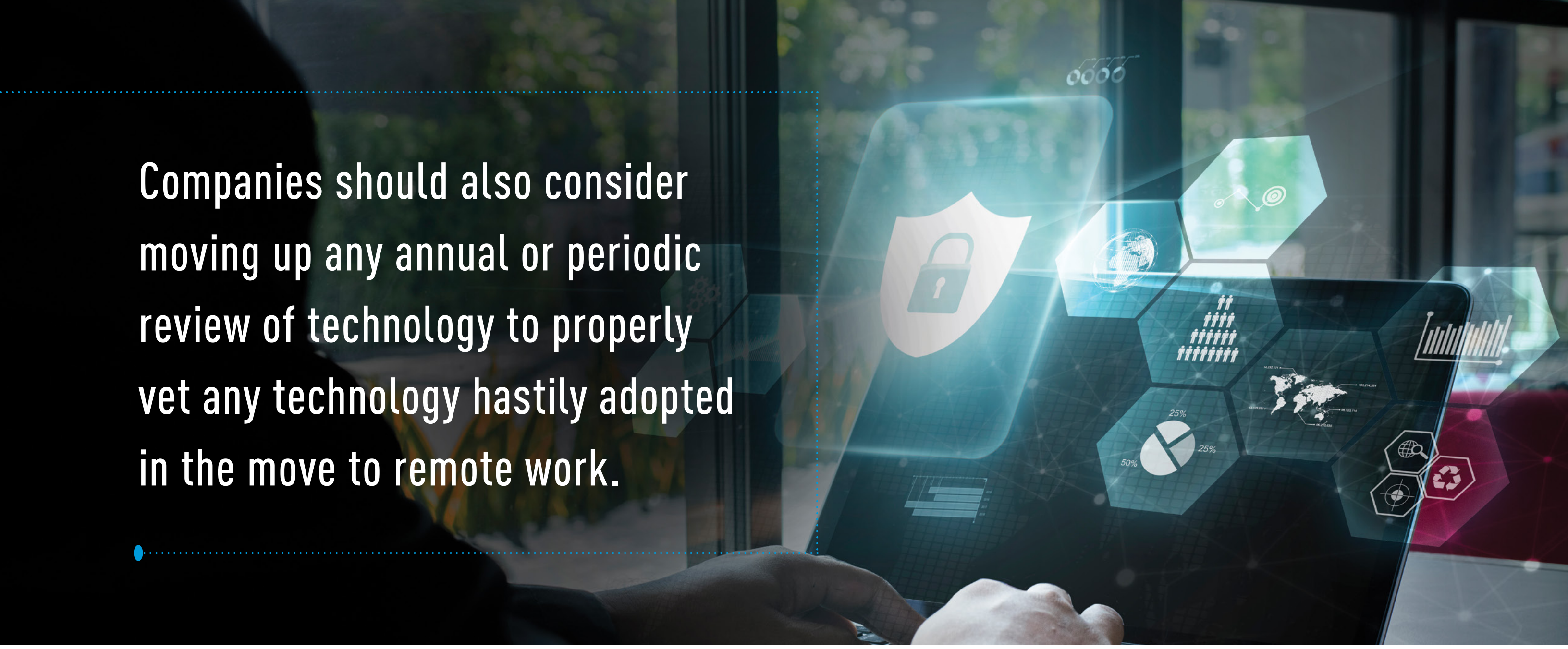
Many companies did not have an information security policy setting forth rules and processes for remote work in place before the pandemic. And for those companies that did have such policies before the pandemic, violations of those policies likely occurred during the sudden shift to a completely or mostly mobile workforce.

As the pandemic continues and many businesses face the prospect of many more months of remote work (or of a broader permanent shift in overall in-office requirements), information security policies should be implemented or updated as soon as possible.

While the large number of employees working from home underscores the need for robust information security policies, the recommended content of those policies has not changed. The essential elements should be reviewed by companies to construct or patch holes in their information security programs during remote work.

Provide Adequate Company-Controlled Equipment and Support. Early on in the pandemic, companies

continued on page 8



Companies should also consider moving up any annual or periodic review of technology to properly vet any technology hastily adopted in the move to remote work.

continued from page 7

may have permitted employees to work on personal devices out of necessity. This practice, however, invites a host of potential information security problems caused by unsecured personal machines and personal Wi-Fi networks. If employees were not equipped with sufficient enterprise technology before beginning remote work, companies should address that issue now. Issuing company-owned laptops and other technology with built-in approved and acceptable security measures to remote workforces, or requiring appropriate VPN connections from personal devices, are critical fixes to potential gaps in cybersecurity.

If a company's IT procedures were not set up to prevent unauthorized access to the network before initiating widespread remote work, such fixes should be put in place now. Employees should be prevented from connecting to the company's network or conducting company business without such protections in place.

Companies should also continue (or, in some cases, begin) using recommended security best practices with respect to both company-owned and personal devices. This could include the use of multifactor authentication (MFA), strong password requirements for all enterprise applications, and policies against locally saving company materials to personal devices. Instead, companies should use cloud-based or other remote storage solutions for saving enterprise data and implement MFA for all enterprise accounts. Company-owned laptops and other equipment can be formatted to require MFA and strong passwords, and robust internal policies can help prevent unauthorized downloading or saving of documents to personal devices. Where personal devices are being used, businesses should consider implementing mobile device management and ensuring that such devices can be wiped remotely if lost or stolen. In addition, IT should be regularly monitoring logins and login attempts and staying on top of patching.

Properly Secure Communications Technology. Communications technology applications such as Zoom, WebEx, and Slack have become critical tools for remote workforces. During the immediacy of the pandemic, however, many of these applications were either hastily vetted by companies or not vetted at all. Some companies, for example, may have allowed employees to temporarily take advantage of free Zoom memberships to fill the gap in communications, rather than seeking out an enterprise solution. Employees, too, might have used programs outside the business's control either for simplicity or out of necessity.

To safeguard employee (and client) communications to the greatest extent possible, businesses should sign up and pay for enterprise solutions for videoconferencing and other communication needs and require employees to use only those authorized applications. Enterprise-level IT security settings can also be implemented, such as requiring a business account and password for Zoom or WebEx meetings and blocking access from unapproved domains or toll-free international numbers to avoid "Zoombombing," the unwanted intrusion into a video conference call by an individual. These solutions can in many cases be pushed down from the IT level to all employees automatically.

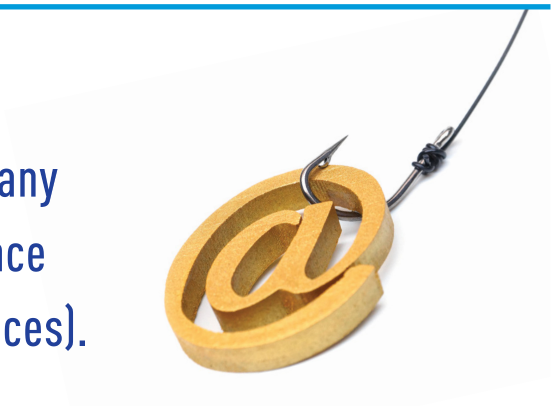
Companies should also consider moving up any annual or periodic review of technology to properly vet any technology hastily adopted in the move to remote work.

Implement Proper Training. Now more than ever, training the workforce to detect and avoid cybersecurity threats is a critical piece of any information security program. Employees should remain vigilant against phishing attempts or other incursions into the company's systems, particularly since remote work with multiple potentially unsecured home networks increases the threat of hacking.

Unfortunately, bad actors are reportedly stepping up cyberattacks during the pandemic and are sending additional phishing emails with purported information from government sources, like the Centers for Disease Control and Prevention or the White House. And a recent report from specialty insurer Beazley Group says that it observed a 25% rise in ransomware attacks reported to its breach response team in the first quarter of 2020.[2] Employees must continue using sound practices to verify the source of suspicious emails, particularly when wire transfers and other requests

continued on page 10

Incident response plans should be reviewed with remote work in mind and evaluated for any weaknesses due to a lack of physical presence in the office (and in any critical vendors' offices).



continued from page 8

for information are involved, and to avoid clicking on links or opening attachments from unknown or unverified senders.

Employees should also be trained on the continued need to protect information relating to clients, customers, and other employees while working remotely. For businesses that handle personally identifiable information (PII) or personal health information (PHI), such information should be securely transmitted and stored, in encrypted format when possible, and not simply emailed or locally saved on a personal device.

Employees should also be trained to be mindful of physical risks from remote work, including the need to minimize printing confidential material on home printers, to avoid conducting confidential calls in the presence of family members or other third parties, and to otherwise secure devices containing confidential information.

Update Incident Response Plan. Every business should also draft and regularly update the incident response plan they would use to respond to a security breach. In the event of a data breach during remote work, employees should know who to contact and which resources are still available. Incident response plans should be reviewed with remote work in mind and evaluated for any weaknesses due to a lack of physical presence in the office (and in any critical vendors' offices).

Privacy Considerations in Returning to the Office

While many businesses may keep the majority of their workforces remote for at least the next several months, many are also beginning the transition back to the office. The new health and safety measures these businesses must implement to protect their workforces often come with additional data security and privacy obligations.

Temperature Checks and Symptom Questionnaires. As part of the return to in-office work, many businesses are introducing temperature checks and symptom questionnaires for employees and those visiting the office. While these measures are necessary for health and safety, they also collect sensitive and protected data from both employees and third parties and implicate data security and privacy laws.

Temperature checks and symptom surveys of employees constitute gathering protected health information on employees and are governed by the Americans with Disabilities Act (ADA) or relevant state law, the Rehabilitation Act, and data breach notification statutes. The Equal Employment Opportunity Commission (EEOC) now explicitly permits such temperature checks as a business necessity during the pandemic, although this action would ordinarily constitute a prohibited medical evaluation of employees unless job-related.[3] The results of any temperature screening should be kept confidential, like other employee medical information. This information should also be considered PHI subject to data breach notification laws and should be safeguarded appropriately.

Similarly, employers may survey their employees about any potential COVID-19 symptoms, such as fever or cough, but should keep the results of those surveys confidential in compliance with the ADA. An exception may be made to share positive employee COVID-19 results with appropriate public health agencies, but that data should be aggregated and anonymized before sharing to protect employee privacy.

Contact Tracing. Businesses returning to the office may have to take certain protective measures if an employee tests positive for COVID-19. For example, in the event an employee contracts COVID-19, businesses may want to engage in contact tracing among employees and visitors to the office space to determine whether others in the immediate vicinity may have been exposed. Contact tracing involves collecting data from a person infected with COVID-19 on all other persons he or she has been in contact with for 10-15 (depending on state standards) minutes at a time over the prior two weeks. This data may include names, phone numbers, addresses, email addresses, and location data.

To the extent a business wants to engage in contact tracing, those inquiries constitute data collection and may be protected by privacy statutes or subject to data breach notification statutes. If a business chooses to use a contact tracing app, that app should be carefully vetted to ensure compliance with privacy and security obligations.

In collecting this data, whether directly or through a contact tracing app, businesses should ask for the least amount of information possible to accomplish their aims, and they must also understand the potential uses of the information prior to its collection. How the information will be stored, used, and shared are critical questions for a business to contemplate before collection to comply with privacy and data security laws most efficiently. Will the data be stored in encrypted form? Will the app collect location and