Data Security and Protection in the New Work-From-Home Regime

On February 20, 2020, a small fraction of the American work force was working remotely at any given time. Then COVID-19 hit the United States and, almost overnight, certain sectors of the workforce became 99% remote. As the dust continues to settle on the technical feasibility of this unprecedented shift in working conditions, businesses should consider their ability to comply with pre-existing company policies as well as data security and protection obligations. These trying times may require every company to rethink its approach, and the coming months will demand deliberate and thoughtful policy decisions to improve and correct the ad hoc solutions of the past few weeks.

Organizations Are Ensuring Efficacy of Remote-Work Transition with Compliance and Security in Mind

The first issue many companies will seek to address is whether the new remote work environment fits within existing policies: did policies scale with the expanded surface area of user endpoints? As the number of user endpoints increases, it may become more difficult to detect unauthorized access attempts. Automated tools that organizations relied on to detect such intrusions may have been appropriate for pre-COVID-19 usage, but may not scale to the new environment. Similarly, manual control of access policies may be untenable with the new influx of offsite users. Companies are now faced with transitioning any manual processes to automated solutions – but new solutions entail new risks, including roadblocks to usability and vulnerability to hackers.

As office buildings are shut down, as they are now in New York and elsewhere, organizations must also pay attention to their physical security plan as well. Any physical security plan that depends on the regular presence of a person at the office – like a security guard – is now likely compromised or invalid.

Organizations must undertake these policy changes methodically. Because physical and electronic security plans, data control plans, and internal controls are often overlapping and interdependent, an organization should consider the immediate consequences and second-order effects of any change. Policy changes should also take into account their impact on data privacy considerations, consumer-facing privacy policies, and self-certifications such as the EU-US Privacy Shield. In particular, an organization will need to ensure that its mobile work plan does not modify its data inventory and mapping in ways that would run afoul of data privacy regulations by, for example, shifting access or storage to a foreign country in the absence of an adequacy determination under Article 45 of the GDPR or other means of complying with Article 44 of the GDPR.

Organizations Must Stay Ahead of Vendor Issues

While addressing its own internal policies, organizations must also pay special attention to their vendors' transitions as well. At this time, it may be incredibly difficult to verify that critical third party vendors have also appropriately scaled their policies with the shift to remote work. Many vendors of remote services have seen their bandwidth stretched to the limit, but it is important to maintain good lines of communication with vendors to be sure that their security and reliability representations and warranties are not in breach. This is particularly important with respect to data privacy regimes, such as the GDPR, where an organization may incur significant liability as the result of a vendor's action. Working with vendors today to identify and rectify breaches will be important to maintain business continuity in a difficult time and minimize potential liability in the future. Nevertheless, it is equally important to preserve any contractual rights to damages or indemnity resulting from a vendor's breach.

Organizations Are Paying Special Attention to Internal Controls

Perhaps the most important step to take is to reassess internal controls on critical assets. With key personnel and support staff working remotely, traditional methods of preventing social engineering attacks have virtually disappeared. Accountants can no longer walk down the hall to the CFO's office to verify that an unusual wire transfer request is legitimate, for example. Similarly, many procedures for handling key trade secrets and other intellectual property may be incompatible with a work-from-home environment. Internal controls may need to assume key person unavailability and build in new checks to verify authority for any controlled activity. Particularly with respect to sensitive intellectual property, technology may provide a tempting solution as blockchain and other tracking technologies can aid in managing material checkouts and encourage individual responsibility for data security. However, tracking measures that would allow a company to identify a bad actor may be a small consolation compared to the loss of key materials.

Many organizations are now preparing written shelter-in-place funds transfer procedures for use in the coming weeks and months when professionals cannot access physical office space and may not have access to key personnel. These measures appear to be prudent approaches to improve security of vital cash assets in the absence of the normal infrastructure for such transfers.

Employee Education Remains Important

Though it may seem trivial, or even an afterthought under current circumstances, employee education remains the key element in bolstering the weakest points of any security scheme. When an organization fails to communicate with its workers, hackers will jump at the opportunity to fill the information void. Attackers are already

weaponizing the fear surrounding COVID-19 by targeting phishing emails that are disguised as official communications from governmental and non-governmental authorities regarding the pandemic. Given the urgency of this public health crisis, click-through rates on these phishing emails have been astounding.

These threats can be mitigated by improving organizational transparency so employees are confident in their organization's plans. Many organizations are also directing employees to trusted sources of information in an effort to "drown out" the potentially malicious voices from outside. In this environment, it is not enough to draw a line between personal equipment and company equipment. When employees work from home, even on their personal devices, any breach is a threat to corporate security. Given that organizations may not have the same level of control over electronic security measures in remote work environments, helping employees remain vigilant and take responsibility for electronic security is more important now than ever.

For more information about Curtis, please visit www.curtis.com.

Attorney advertising. The material contained in this Client Alert is only a general review of the subjects covered and does not constitute legal advice. No legal or business decision should be based on its contents.

Please feel free to contact any of the persons listed below if you have any questions on this important development:

Jonathan Walsh
Partner
jwalsh@curtis.com
New York: +1 212 696 8817

Daniel Banaszynski
Associate
dbanaszynski@curtis.com
New York: +1 212 696 6153

Edward Combs
Associate
ecombs@curtis.com
New York: +1 212 696 6069