crowell moring

CLIENT ALERT

Privacy and Cybersecurity in the Time of COVID-19: What Comes Next?

Apr.20.2020

As businesses continue to grapple with and progress through the challenges presented by the COVID-19 crisis, it is not too early to focus beyond the horizon on what the privacy and cybersecurity landscape might look like when the crisis finally passes. Crowell & Moring's Privacy and Cybersecurity Group seeks to identify likely issues and new norms arising from this crisis in a series of client alerts. We begin by attempting to level-set and understand what the crisis has already wrought in this space and identify issues that will need to be addressed as we slowly inch towards a new reality.

1. Adjust your security stance for an emphasis on endpoints. Security practices for most companies and industries focus first on protecting the company's perimeter (*e.g.*, with firewalls) and closely monitoring systems within that perimeter for unauthorized access (*e.g.*, network traffic analysis, ingesting log data into SIEM tools, etc.), with endpoint protection a secondary focus because of the security offered by network-level protections, especially with respect to employees who rarely or never work outside of company facilities. Increased teleworking, however, has meant that employees – and their laptops, mobile devices and other endpoints – are now connected outside of those secured company systems and networks. Accordingly, companies need to reevaluate and adjust their current posture to account for endpoint security needs in light of the changed use cases for their employees now and going forward.

2. Manage your regulatory environment. Many regulators initially took relatively lenient enforcement stances regarding security and compliance issues related to telework during the early days of COVID-19 response when companies were scrambling to deal with the sudden need for telework. Companies should not assume that regulators will remain lenient; regulators will expect mature security programs to adapt to new circumstances and to revise controls and practices that were implemented during COVID-19 leniency and necessity in order to comply post-COVID-19. Companies will need to meet their compliance requirements for any new systems or tools that were adopted in response to COVID-19 circumstances, especially those in heavily regulated industries such as banking, healthcare and defense.

3. Adjust to the new threat environment. Threat actors have been quick to adapt and take advantage of changing habits in response to the COVID-19 pandemic. Tailored spear phishing campaigns that incorporate COVID-19 information are being aggressively conducted, but attackers are also pursuing other vectors. For example, social media scams are targeting employees operating outside of company networks as well as targeting those who may be searching for other employment (*e.g.*, by masking malicious URLs as links to job applications). Ransomware attacks seek to take advantage of changed operations (*e.g.*, less attention to network monitoring as skeleton IT staffs are stretched thin; dispersed staffs leading to slower detection and reaction to malware spread). There are many other examples, with more certain to arise. Companies need to remain diligent in their security practices, but also be prepared to adapt to a rapidly evolving threat environment. Companies should be prepared to implement their Incident Response Plans in a variety of adverse circumstances.

4. Plan around new infrastructure. In response to the sudden operational changes during the COVID-19 crisis, many companies rapidly adopted new infrastructure, such as remote access technology, SaaS tools, collaboration and messaging platforms, new

video teleconferencing providers, and greater numbers of laptops and mobile devices issued to employees. When operations inevitably begin transitioning back toward prior norms, companies will need to plan for this new infrastructure and for any changes in information governance and records management practices that the new infrastructure might require. Some of the new infrastructure will be incorporated into standard operations, while elsewhere the interim use of COVID-19- specific infrastructure and adaptations will need to be discontinued.

5. Plan for a return to the office. While timelines are still uncertain, at some point employees will return to the office, and companies need to start planning for that now. For example, if employees have been using personal devices or third party platforms, how will they be transitioned back to using company systems (and returning to standard operating norms)? How will the company ensure that all company information returns to systems that it controls (and does data need to be deleted from external systems, including mobile devices, printers, and cloud-based collaborative tools)? Can the company ensure that all systems and data that are re-integrated with company systems are free from malware or other malicious elements? Does the company have plans to document and track compliance around these needs? In addition, data collected during the crisis may impact who returns to the work environment and when. For example, data concerning an employee's health vulnerabilities or potential contact with other infected individuals may influence the employer's decisions regarding that employee's return to the physical work environment.

6. Plan for the future of COVID-19 data. Most companies have at least some sensitive data related to COVID-19 (*e.g.*, employee diagnoses), and some have gathered more advanced data through steps taken in response to the pandemic, through administrative processes and use of technology. For example, employers may be collecting data related to employee health (*e.g.*, temperature scans) or employee behavior (*e.g.*, location tracking, tracing employee interactions, and information about the health of family members) both on-site and outside of company facilities. While such activities have understandably occurred in rapid response to companies' evolving needs in the midst of a crisis, there should be a practical plan in place regarding these data and practices once the crisis passes. Issues for consideration include aligning collection with (and limiting to) specific needs, determining where this COVID-19-specific data is stored (level of security; geographic location), determining who should have current and future access, and data retention plans (alignment with needs; whether different from standard policies; and whether personal data being retained can be aggregated or anonymized to reduce privacy-related risks). Companies will additionally need to ensure that they are complying with applicable federal and state law in their collection, use and retention of this information. At some point, collection will become more limited or end completely, and companies will also need to have a plan in place to wind down their programs.

7. Begin planning for the "unknown new." Most companies plan for the enhancement, growth, and overall evolution of their IT, data protection and security environments on multi-year cycles – for both technical and people/process needs. That means that now is the time for companies to look beyond the current crisis and start incorporating the lessons learned from their COVID-19 experiences in terms of planning for newly identified needs, reviewing and updating existing plans, and making informed projections about what is coming over the horizon, including areas such as increased telework, increased focus on endpoint security, changes in the collection of personal information like employee health information, and the increased need for resiliency as business continuity and disaster recovery plans are expanded to include future scenarios with stressors similar to COVID-19.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Matthew B. Welling
Counsel – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com