crowell moring

CLIENT ALERT

Ensuring Cybersecurity When Organizations Consider Teleworking and Remote Access

Mar.11.2020

As more employees stay home in the wake of COVID-19, it is increasingly vital for organizations to focus on the cybersecurity and privacy concerns that may arise with increased teleworking and that can pose new threats to business operations.

Here are our Top 10 issues for companies to consider:

1. **Cybersecurity is a team sport, and organizations need to have a playbook for working together**. An important aspect of preparedness for COVID-19 is for companies to work across teams and take proactive steps to ensure that key stakeholders are aligned with the company's strategy for addressing cybersecurity risks and responding to incidents, are informed of their respective responsibilities related to preparedness and response, and are trained accordingly. This becomes even more important when employees are not co-located and need to coordinate while working remotely.
2. **Cybersecurity preparedness and incident response are not just for technical teams.** The evolving COVID-19 situation presents a good time for companies to bring together a team from key components of the organization to consider potential cybersecurity risks to the company (overall and specific to the evolving COVID-19 situation) and strategies to mitigate or otherwise respond to these risks. The team will often include representatives from legal, information technology, security, communications, Human Resources and senior leadership. Decisions made should be captured in the company's policies and procedures, such as its cybersecurity incident response plan. For companies that have already gone through this process, this is a good time to revisit those decisions and ensure that they align with current circumstances.
3. **Plan for changes in remote access and teleworking**. Remote access may put a strain on an organization's systems and connectivity options. Before implementing teleworking and remote work force options on a large scale, organizations should assess whether their current IT capabilities, including VPNs and remote desktop systems like Citrix, can handle the increased demand and, if not, what alternatives are available or additional resources needed. Organizations should also evaluate their bring your own device (BYOD) policies against the potential scale of usage and to ensure that policies line up with risks associated with broader usage.
4. **Plan for compliance with industry regulations on remote access**. Some industry sectors are subject to regulatory cybersecurity requirements for remote access. Government contractors, for example, may be subject to specific technical controls established by NIST SP 800-171, including for access control, awareness and training, configuration management, incident response, media protection, physical protection, and system & communications protection. This is a good time for government contractors to review their system security plans for compliance with these controls for teleworking.
5. **Prepare for changes in threat actor behavior**. Organizations allowing remote access should be on the lookout for threat actors deploying new threats to remote workers and for an overall increase in targeting. They may, for example, use spear phishing attacks that appear to ask company employees to validate their work from home credentials or that are intended to tempt people to open documents that result in the deployment of malicious links/files when launched.

During times of increased telework, employees may also be more exposed to social media-based threats and should be made aware of those risks as well.

6. **Assess capabilities to manage information security remotely**. Organizations will need to assess their abilities to manage information security remotely, including through their current security operations centers (SOCs). This review should include determining if the company has infrastructure in place to promptly stand up incident response teams, coordinate response activities, and communicate with key company stakeholders if the individuals involved are not co-located and primary (and secondary) systems are compromised or unavailable.
7. **Prepare for risks associated with shared devices and networks**. Shared resources, for example using home printers and connecting to shared wireless access points, pose high risks that will need to be addressed by organizations that allow teleworking. Education, training, and workshops should be considered to alert individuals to these risks and appropriate actions to address them.
8. **Changes in how technology is used can lead to other changes in employee behavior**. While addressing technical risks, companies also need to be aware that changes in employee behavior associated with increased telework may also trigger physical security concerns. For example, teleworking often results in an increased use of paper documents, and the possession and use of those documents outside of company facilities. Accordingly, policies and plans related to proper marking, handling, disposal and collection of documents containing sensitive information will need to be developed and shared. If already in place, this is a good opportunity to provide employees with a refresher on them.
9. **Ensure that personal information, protected health information, and other regulated data is appropriately used and properly protected.** Organizations will need to take steps to ensure that regulated data, including personal information (PI) and protected health information (PHI), are secured and managed in compliance with applicable laws and guidance across borders where applicable. This includes, for example, considering guidance issued by HHS to clarify permissible uses/disclosures of PHI and limitations placed on companies' collection, use and disclosure of sensitive health information in many jurisdictions. Organizations should also be aware that making inquiries related to employee health, including conducting medical examinations, creates potential issues under the Americans with Disabilities Act (ADA).
10. **Ensure that supply chains are also prepared**. Now is a good time for organizations to be in contact with their suppliers and vendors to assess what preparations are being made throughout their supply chain and whether those vendors will be able to continue providing goods and services without interruption. Additionally, this is a good time to review service agreements with technical vendors and have conversations about the potential impact of COVID-19 on services and resources, including their ability to accommodate the company's changing needs in light of increased telework.

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

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Evan D. Wolff

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

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

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