Cybersecurity Challenges During the COVID-19 Pandemic

On-Demand Briefing Call - Key Takeaways

Cybersecurity and COVID-19—What are we talking about?

There are four key aspects of cybersecurity that individuals and companies need to keep in mind, especially during this unique time when millions of individuals are exposed to unsecure devices at home.

1. **Keep your online data secure.** Whether you are an individual suddenly working from home full time, or a seasoned corporation, what measures have you put in place to keep your online data secure?
   - Do you understand the security protections offered by your employer and do you understand how to take advantage of those protections?
   - Have you explored how to keep your internet connection secure with your service provider?
   - Are your passwords strong and encrypted, i.e. a combination of letters, numbers, and symbols, versus a string of numbers like "12345"?
2. **Maintaining Internet connectivity.** Now that millions of individuals around the world are working from home, there may be a strain on your internet speed, depending on where you live. Many service providers have taken steps to ensure seamless connections in order to avoid disruptions with online banking and other essential services.
3. **Protect the integrity of your data.** For individuals and corporations, it is important to take steps to ensure your data has not been tampered with or corrupted. This is especially relevant when it comes to online banking and personal health records.
4. **Industries increasingly reliant on digital systems.** Power plants, water processing plants and many other industries that we rely on daily are increasingly digitized and under threat from cyber-attacks. Attacks on power or transportation systems can result in significant loss of life and economic damage.

Best Practices for Individuals, Companies, and Emerging Economies

Individuals

Be Aware. Be mindful of your devices and your security vulnerabilities.

- Download your software updates. They are designed to address security vulnerabilities.
- Be aware of phishing. Familiarize yourself with the ways hackers try to trick consumers into clicking on malware and other nefarious links.
- Strengthen and encrypt both your passwords and data.

Companies

Have a Plan. Consult with your legal advisors about implementing a governance and compliance framework.

- Are you taking a risk or threat-based approach? Which one is right for your enterprise?
- Carefully assess your most valuable assets and digitally wall them off (i.e. add extra layers of protection around critical data).
- Be assured that you have an effective and tailored incident response and preparedness plan that helps you detect threats, and provides a clear set of tactics to implement in response, and that are informed by governing law and regulations.

Emerging Economies

Take a global perspective. According to the McKinsey Global Institute, we are transitioning into a world where the global trade in services has grown more than 60% faster than traditional goods traded, and half of all global trade in services depends on access to cross-border data flows. The instinct to hold and hoard data defeats the purpose of a digitally interconnected world. Africa has the opportunity to accelerate the creation of high value and technology enabled jobs and opportunities like India has through its expansive customer service industry, which of course is powered by the digital revolution. Cutting any nation off from global data is as damaging as cutting that nation off from global trade.

How can Covington help?

Covington has assisted many clients over the years develop incident response and preparedness plans, including other related categories of work that help companies mitigate and respond to cyber threats. Three examples include:

1. **Governance and Compliance**
   - Design and help implement a company's cybersecurity program following detailed consultations with the Board, executive teams, and the IT departments that manage the programs.
2. **Risk Management and Assessments**
   - Analyze existing risk management programs in order to assess and ensure that they adequately address current threats and align with existing legal obligations imposed on data controllers before and after a data breach.
3. **Mergers and Acquisitions (M&A)**
   - About 50% of the work we've done around cyber intrusions is the result of M&A deals where the target company's systems introduce cyber threats to the parent company's operations when the two systems are integrated

Our deep capabilities, expertise and global reach on cybersecurity issues also includes: government engagement and information sharing; cyber disputes, insurance, and regulatory responses; law and policy; and general security and technology advice.

* * *

If you have any questions concerning the issues discussed, please contact the following members of our Data Privacy and Cybersecurity and Africa practices:

Trisha Anderson	+1 202 662 5048	tanderson@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Robert Kayihura	+27 11 944 6906	rkayihura@cov.com
Witney Schneidman	+1 202 662 5375	wschneidman@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com