

Cybersecurity in the Age of COVID: How to Protect Your Data

Technology, Privacy, and eCommerce





As the pandemic continues to surge, it has brought on a wave of other threats: cyberattacks and data losses. The Federal Bureau of Investigations (FBI) is now reportedly inundated with 4,000 cybersecurity complaints a day — a 400 percent increase compared to before the pandemic.

This spike in hacks and breaches is alarming for anyone with a digital footprint — and these days that means just about everybody. But it is especially so for general counsel who are part of the team responsible for protecting their companies' data — and who will be accountable when data is exposed.

Over the past few years, law departments have become more intertwined with IT teams as cyberthreats increase and companies in general — and legal departments in particular — realize the advantages of multidisciplinary approaches to problems.

According to the ACC Foundation 2020 State of Cybersecurity Report, 71 percent of organizations have enlisted their chief legal officer in a leadership role or as part of a team dedicated to mitigating these risks. That number will skyrocket in tandem with the COVID-related attacks.

We spoke with ACC Deputy General Counsel Veronica Pastor to learn the most common and insidious cyberattacks and how to safeguard your company from them.

ACC Docket: Why have cybersecurity risks increased during the pandemic?

Pastor: The emergency move to work from home arrangements is the key factor. Neither companies nor workers were ready for an overnight transition to a WFH environment, yet that is exactly what happened. Companies had set up their systems to accommodate a few workers working remotely some of the time, not the whole workforce operating from home at once. Then in one short week, they had to adapt to a very different scenario.

This presented companies with issues of capacity and mobility, among others, which were exacerbated by the fact that everybody was suddenly working from home — in-house IT departments, but also all the vendors of technical solutions, software and hardware, and the helpdesks. Throw in the effects of the sudden crisis on the supply chain and the general confusion we were all experiencing at the time and this creates an ideal environment for noxious actors and a nightmare scenario for the technically-challenged.

And of course, the workers weren't ready either. All of a sudden you had people handling sensitive data in an environment that was not set up for it, both from a technical and a psychological perspective. Workers may not have been completely familiar with mobility tools, or may not have had full access to them.

And of course, shifting the work environment from an office, with its order and predictability, to a home full of distractions in the middle of a crisis meant that people were less attuned to potential threats — they were just trying to get their work done. This situation greatly enhanced the attack surface, as the entry points that hackers and other malevolent actors can exploit to conduct attacks by creating security gaps.

But let's not forget that not all breaches stem from cyberattacks. Some will be the result of well-meaning employees who innocently put information at risk while just trying to get their work done. Education and support remain essential.

ACC Docket: What are some of the most common cyberthreats that companies are currently facing?

Pastor: Amazingly, the most prevalent threat continues to be the good old phishing attack using social engineering. One good example has happened at ACC many times. Someone was calling ACC employees asking them to confirm the email of our director of finance.

Fortunately, our colleagues saw through this. Other examples are brute force attacks, where a bot sends thousands or random combinations of letters and numbers to try to crack somebody's password. Often the "best" approach is to combine more than one form of attack.

And of course, ransomware continues to be a big problem — let's not forget that for a few hours, a 17-year-old hacked the Twitter accounts of Bill Gates, Elon Musk, and US President Barak Obama to post a cryptocurrency scam. And that a few days later, Garmin was the victim of an attack by Evil Corp, a highly organized hacker group out of Russia.

ACC Docket: How can in-house counsel protect their company's data?

Pastor: Legal departments should remain committed to and fully involved in cybersecurity efforts. One big area where they can make a difference is in the development of appropriate cybersecurity policies. They can also build cybersecurity into workflow and governance considerations. And of course, the legal department should be involved in incident response, as it has legal implications.

This is a compliance issue as well, as in some cases, regulators and affected individuals will have to be notified under applicable laws. In other instances, companies have to implement certain cybersecurity processes to comply with law or contractual requirements.

In the United States, for example, companies in the healthcare sector have to be mindful of the HIPAA Security Rule that protects the electronic health information of patients. And in Europe, the new EU Cybersecurity Act has introduced a voluntary certification framework for ICT products, services, and processes. All of this is in addition to recognized security frameworks, such as ISO 27001 and NIST-800, to cite just two.

In addition, any sort of criminal activity should always be reported to the authorities, and there are also various public and private forums where companies can share their experiences and potential solutions.

Finally, the legal department can play a role in education — and the key here is to be inclusive. At the end of the day, individuals are the weakest link, but also the best line of defense.

ACC Docket: What challenges do in-house counsel face in mitigating these risks as most companies are working remotely? How can they resolve them?

Pastor: Remote working has increased the attack surface, as described above. The main challenge is that we no longer have all the people, equipment, and systems under one roof and as easily available. There are technical solutions to minimize risk, such as using data loss prevention software, implementing technology for access control and identity management, and blocking access to nefarious sites.

But ultimately, it comes down to having a good relationship with the departments responsible for information management and with employees as a whole. That way, they can disseminate the message that security matters and that the legal department is an ally.

ACC Docket: Since many companies are still working remotely, how can in-house counsel effectively communicate the importance of cybersecurity to their staff?

Pastor: The best way is an education program that points out new threats without making anybody feel bad about having fallen victim to an attack (as long as this is not part of a personal pattern of carelessness). Free and frank discussion of the issues also helps. And having trainings on threats and policies on a regular basis.

Prevention works best when people understand what the goal is and feel that they are in it together, and so a good education program has to be cross-functional and involve input from all departments.

At ACC we developed the “ACC Cyber Eagle” program that invites employees from various departments to come together and discuss cybersecurity issues as a fun learning experience and then share their topics of interest with the wider group.

Each Cyber Eagle then has the opportunity to educate their colleagues on cybersecurity basics by writing email alerts or hosting “lunch and learns.” This behind-the-scenes experience helps these employees see how real and pervasive cyber threats are, and that each of us has a role to play in keeping our colleagues and the company safe.

ACC Docket: What’s the best way anyone — in-house counsel or not — can protect their data and avoid these cyberthreats?

Pastor: First and foremost: awareness. Be alert! Malevolent actors prey on distraction and lack of information. Be informed and be suspicious. The means of delivery of the threats will vary, but in the large majority of cases, there will be something slightly “off” about the communication attempt. It could be the email header, poor grammar or unusual syntax that does not seem in line with how the alleged sender normally communicates.

Of course, technology has a key role to play, as do the right corporate policies and implementation programs. At the end of the day, a policy has to be understood to be implemented well, so it is important to tailor policies to the realities of the business and adapt them to the way the company works. Then it is important to make sure everybody understands that policies and processes exist for a reason, and what that reason is.

The clearer your policy is, the higher the buy-in will be. And with higher buy-in comes better compliance and success. Where important data is at risk (e.g., for payments or other important actions) — always use a second means of confirming the instructions. Make it a policy that if you get an email, you should supplement it with a phone call before acting on the instruction, no matter who it purportedly comes from.

In general, use secure portals and encryption, both in transit and at rest. There are many vendors who offer good technical solutions, and some are quite specialized and industry-specific.

For more guidance on the coronavirus pandemic, visit ACC's COVID-19 Resource Center. To connect with other in-house peers in the cybersecurity industry, join ACC's IT, Privacy, and eCommerce Network.



Veronica Pastor is deputy general counsel at the Association of Corporate Counsel and focuses on privacy, cybersecurity, and international contracts.

Karmen Fox



Web Content Editor

ACC