CLIENT ALERT

VIDEO: Is Your Company Prepared for a Cyber-Incident?

May 8, 2015

Data security breaches are on the rise. Increasingly, companies see cybersecurity as a critical concern for their reputation and business. The stakes could not be higher. Fighting cybercrime, keeping data and proprietary information secure, and protecting networks has become a board responsibility and essential function. Success requires cooperation and management throughout the enterprise—lawyers, IT professionals, managers, security officials, communications professionals, and others need a strategy and plan.

In this three-part video alert series, **Evan Wolff**, Crowell & Moring partner and former Department of Homeland Security adviser, discusses the trends he's seeing in cybersecurity, how companies should prepare for cybersecurity breaches or incidents, and what companies should do when a cyber-incident or breach occurs.

Part 1: When Cybersecurity Becomes a Legal Consideration

Part 2: Trends in Cybersecurity

Part 3: Preparing for Cybersecurity Breaches and Cyber Incidents

---

Transcript

Why is cybersecurity a legal issue?

> I think cyber is increasingly becoming a legal issue for three reasons. First and foremost, because the government is beginning to regulate the space. We're seeing this in the defense sector through the Defense Federal Acquisition Regulations, where they've created a new rule called the Safeguarding Rule that are requiring companies to implement specific requirements: both technical controls on their system and also incident response requirements for reporting incidents.
>
> Outside of the defense sector, we're also seeing increased activities in the utilities sector and other sectors. The second reason is because of the investigations after incidents and the response to incidents. It's critically important that a lawyer be involved in incident response; not only in the engagement of technical forensic experts but also in running the investigation and in understanding disclosure.

The third reason is because we have so many third parties involved that often have complex relationships. A great example is the supply chain and the vendors of companies. Oftentimes, the contractual relationships require companies to be able to understand when an event occurs and to be able to do joint investigations. And, on the flip side, when a company enters into a contract with its customers, that they understand the legal risks and responsibilities.

What are the trends in cybersecurity?

First and foremost, we're seeing an increased focus on cyber threat information sharing. And, what I mean by that is sharing the information on how you are being attacked, the tools the adversaries are using, and some of the other information associated with those attacks. By companies sharing them, either with other companies in your sector, or sharing them with government, you can both increase your ability to protect your networks and make it much harder for those to attack them.

A secondary focus that I'm seeing is in the area of compliance. This means establishing clear governance with very clear roles and responsibilities.

They're also developing policies and procedures and making sure that the entirety of the company is involved; both from the senior level to the people that are responsible for protecting their networks, and ultimately they're also making sure they are doing some of the basics involved in training and some of the IT security issues.

The third trend I'm seeing is the change in technology itself. Increasingly, companies are focusing on what technology is appropriate to them and making sure that that technology is used and not something you are buying for decades at a time; but for sometimes six months or a year at a time. Because, ultimately, technology is going to be both the solution to many of the threats we are seeing, and in the interim, they give companies the market advantage to be able to look across the horizon and see what's coming down the road.

How should companies prepare for cybersecurity breaches or cyber-incidents?

There are three things companies should be doing right now, which is be proactive by first building a team. That team should involve not just lawyers and IT directors but also people from management and people from communications. You really need to build a coalition of the people that are going to be involved in an incident response.

Then, once the team is built, the second thing they need to do is build very clear policies and procedures. Three of them that I think are critical for most companies are: having a very clear privacy and security plan, having an incident response plan, and and having a vendor management policy.

Once you have those clear policies, the last thing a company should do is practice. You should be using these policies and practicing through scenarios and through tabletop exercises, or going through a scenario of what an incident or breach would look like on at least an annual basis. From that, you can learn and develop the appropriate toolkits and appropriate responses so you all understand—if there is an incident—how to be prepared and what you need to do to be prepared.

What should a company do when a cyber-incident or breach occurs?

First, and most importantly, gather the team. You need to make sure you have a group of both people within the IT department, the business department, the management, and of course legal and communications that are all working together to manage the incident.

Second, you need to focus on security. You need to make sure your system is safe and, for example, if you think your email system has been compromised, don't send emails to people until you are sure that the system has been secured and cleaned.

Third, you need to put together an investigation team that is very thorough. Sometimes this involves using third party forensic investigators. Make sure that they are hired through the legal department and that you have thought through those privilege issues at the forefront.

Last, really manage the interactions with third parties, whether it be disclosures to the government, working with law enforcement, or managing some of the relationships with the vendors. Those third party disclosures can be very critical and oftentimes very difficult.

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

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com