JANUARY 9, 2017

Legaltech news ONLINE

An ALM Publication

Cyber Becomes Mainstream: The Lessons Learned for 2017

These three lessons impact our daily lives as professionals, as well as citizens.

BY ANDREW SERWIN, MORRISON & FOERSTER

In a year of change, one issue has become so tied to our daily lives that its emergence has been somewhat masked—and that issue is cyber.

Just a few short years ago, cyber was seen as an edge issue that impacted technology companies. Now one need only look at the continuing discussion regarding the presidential election and the effect of the alleged interference by state-sponsored threat actors to see that cyber is embedded in our daily lives in a way that many did not imagine.

There are a few lessons to be learned from the events of 2016, and these lessons impact us as professionals, as well as citizens.

Credit: SWEviL/Shutterstock.com

1. It's Not Just Consumer Data and Tech Companies Anymore

Direct cyber threats can take many shapes, and as we have seen in 2016, the threats are not just limited to stealing consumer data. The threat can be directed towards business data for industrial espionage, insider trading, and other criminal activity, as well as towards damaging businesses by destroying data, holding data for ransom, or damaging physical hardware or other systems to impact the

business in often unforeseen ways. As the threats continue to change, companies need to consider what their exposure is, including beyond the theft of consumer data.

2. Cyber as a Threat Vector/Hacking for Hire

Cyber has also become a way for attacks to start, even where a "cyber event" is not the end result. In essence, just as a physical or kinetic attack doesn't always have theft as the end result, cyber has become an entry point for other criminal activity that isn't always directed towards information or information systems, and one need only consider the debate currently occurring about "hacking" an election to see this point clearly.

This issue is closely tied to the new trend of "Hacking for Hire," which really means that certain hackers have begun emphasizing a different business model—creating easy to use "weaponized malware" that even less sophisticated people can use. In essence, some hackers have moved from hacking to becoming cyber arms dealers, and these cyber arms are readily available. This means that companies must factor in that they may be under an increasing number of sophisticated attacks, and attacks that might seek to publically disclose information rather than steal it.

3. The Ultimate Asymmetric Threat

One of the real challenges is that companies in many cases face organized threat actors who look for a company's weakness and exploit it, which is why cyber is a classic asymmetric threat. The threat actors in many cases share information and exploits and are now increasingly selling them, as noted above. This gives companies an information deficit if they are not looking at whether they should be considering information-sharing in some form, whether that is sharing among private sector companies, or sharing with certain public sector entities.

Given the trends noted above, sharing information in the private sector, as well as with the public sector, is becoming an even more important consideration. Knowing what the threat trends are and how these threats materialize, is critical information for many companies, and the importance of information-sharing will likely only increase as the cyber threat continues to grow.

Andrew Serwin *is global co-chair of* ***Morrison & Foerster's*** *market-leading Privacy + Data Security group, Mr. Serwin is an internationally-recognized practitioner and thought leader in the fields of privacy, cybersecurity, information governance, and information sharing.*