CORPORATE COUNSEL
An ALM Website
corpcounsel.com | October 16, 2018

'Dawn of the Code War': Real-Life Lessons for GCs About Cybersecurity and Ongoing Threats

Former assistant attorney general for national security and current Morrison & Foerster partner John P. Carlin has written a new book about the growing cybersecurity threats against global companies, organizations and governments. He talks about why law firms and in-house counsel need to step up their defenses and those of their clients.

MP McQueen

In his new book, "Dawn of the Code War," former assistant attorney general and current Morrison & Foerster partner John P. Carlin writes about the growing cybersecurity threats against global companies and Democratic governments posed by nations including Russia, China, North Korea and Iran, terrorist organizations and crime rings. Carlin and co-author Garrett M. Graff, a national security journalist who works at the Aspen Institute's Cybersecurity & Technology Program, believe it is time that everyone— including corporate counsel, law firms, government officials—stop regarding cyberattacks and social-media disinformation campaign wars as science fiction, and realize it is now a fact of modern life and international relations, soon to worsen with the advent of the internet of things.

"It is putting companies in the front lines of a national security threat in an undeclared war," he said.

For instance, earlier this month the Justice Department in Western Pennsylvania indicted seven Russian military intelligence agents for alleged cyberintrusions on the computer network of nuclear power developer Westinghouse Corp., among other organizations globally. It was the second publicly disclosed cyber-plot against the company—a group of Chinese military officers were indicted by the DOJ in 2014, while Carlin was assistant attorney general for national security. Westinghouse contends that no information was stolen in recent alleged plot, and the Russian government denies perpetrating it. But the earlier Chinese intrusion at Westinghouse as well as U.S. Steel, Alcoa Inc., panel manufacturer SolarWorld and several other big companies and a labor union hit pay dirt in the form of trade secret theft, legislative and litigation strategies and privileged attorney-client relations, all of which allegedly pilfered from the computer networks of law firms and legal departments, according to the Justice Department.

John Carlin, with Morrison & Foerster.

Why are these attacks occurring? What are hackers doing with all this data? Carlin says that sometimes the answers are more sinister than is generally known: In 2015, for example, a hacker originally from Kosovo working in Malaysia on behalf of ISIL hacked into an American online retailer's server stealing personally

identifiable information of tens of thousands of customers. The hacker then culled through the stolen data to extract information on 1,351 military or government personnel based on their email addresses, and passed on the information to ISIL, which became the basis for a kill list that ISIL posted on Twitter. The FBI traced the hacker's IP address after another cyberattack on an online retailer in which he was paid $500 in bitcoin ransom to leave the merchant's server alone. The hacker, Ardit Ferizi, was apprehended in Malaysia, pleaded guilty and sentenced to 20 years in federal prison.

In a recent interview with Carlin, we asked him to highlight some of the takeaways from this new book and lessons general counsel and law firms can take from it about cybersecurity and the ongoing threats. His answers have been edited for clarity and brevity. The book "Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat" is published by the PublicAffairs imprint of Hachette Book Group, and is due out Oct. 16.

Q: Why did you write this book?

As I have gone around talking to businesses and audiences it became clear that a lot of what people thought were threats that were science fiction or in the future had already happened. Despite efforts to catch who did it and how it happened the message was not reaching the public and it was important that people realize that we are in a Code War right now and under attack each day otherwise we will never have the consensus to fix what we need to fix before something truly terrible happens. So much of what we are seeing has changed in terms of scale but they are not new.

Q: Who or what is behind some of these massive data breaches we hear about? Criminals, states or terrorist groups?

Across the board we are seeing increasing activity from nation-states, from organized criminal groups and terrorist groups. There is general consensus that the trend is likely to continue in the next five years. In terms of top actor out there, I think a lot of what we consider as our criminal problem is "dark market" business [for stolen IDs, credit card data, etc.] is really a Russian problem. They are harboring the world's most notorious criminals and instead of locking them up they are using them for intel purposes as long as they don't target Russia. If you look at some really sophisticated disruptions, they have been able to catch people around the world except for the ones in Russia where they are unable to take action. Of course North Korea, China and Iran present concerns.

Q: Why was Westinghouse targeted, allegedly by both Russia and China?

If you are a company of a certain size you are a target for almost all of the nation-states unfortunately, and that is not a surprise. That case is a good example of something that didn't get the attention that it deserves. A lot of fights we are having among ourselves, but that is a good reminder [that] those who don't share our values who are undermining everything from sports and the Olympics, to violations of agreements on chemical and biological warfare to cause indiscriminate damage through cyber-weapons. I hope we can put aside partisanship and agree that what was laid out in that case is not acceptable, and there needs to be a response to keep us safe.

Q: Law firms and counsel also were compromised in the earlier attack on Westinghouse, correct? How should in-house counsel and law firms prepare?

Unfortunately intelligence has figured out that lawyers are great targets, they compile information [as part of litigation] that will damage the company most, in hopefully well-written and succinct memorandums whether diligence or litigation strategy, so dating back to when I was in government, the bad guys have figured that out and targeted law firms and in-house lawyers and once they break into a network, they look to find them. So, it is important that firms invest in cybersecurity and clients [also] with other vendors and supply chains and expect a certain amount of security. That said, at the end of the day, there is no internet-connected thing that is safe. If you are in a spot that is a high target, you need to think about resilience and some things that you should not store digitally. It ranges from putting limitations on what you can access from work, and limitations on personal devices to awareness and training and education on cybersecurity but we are seeing an increase in the private sector and government in focusing on the whole person in vulnerabilities.

Q: Whether or not to disclose a cyber-intrusion or data breach is a big consideration for most

organizations when they've been attacked. What's your perspective on this?

[He says he can't speak about a specific event because of firm conflicts.] But generally, I don't think we have the right carrots and sticks for a logical system of disclosure that properly incentivizes companies. There is no uniform data breach law and there are 45 and counting state laws impacting businesses with customers and employees in different states. Our regulators have inconsistent approaches to when to report and there is a disconnect as to those who want to improve defensive practices with liability for failing to prevent intrusions and law enforcement intel agencies that can't work to identify threats without cooperation from victims. It is confusing for clients right now in that world. You really need expert legal advice to navigate those different risks. Without that, you can underestimate the risk of not telling someone in law enforcement about something that turns out to be mission critical, overly weigh the cost of a potential fine or litigation and underestimate the damage to your brand if you haven't informed law enforcement. … We do not have a uniform federal law on what to do on a breach and we need one. Presidents Bush, Obama and Trump disagreed on a lot but they agreed on that, and we still haven't gotten one passed.

Q: You wrote in the book about an instance that illustrated why it isn't always apparent until after investigation why a business was hacked and why it's important intrusions be reported to authorities.

Companies sometimes, without education on what is occurring, underestimate the risks as we talk about in the book in some detail, like the harrowing real case of what looked like the criminal breach of a small number of companies that wound up [with victim identities] on a terrorist kill list. If every company knew that, they would avoid just quick fixes but want to talk to law enforcement about it so their neighbors aren't killed. That would be the end of the business if it turned out that someone was killed because of their stolen information.

Q: What is the biggest failing of U.S. industry and government today with respect to cyber threats?

Three main things: As we move toward the internet of things we need either voluntary or involuntary rules to make sure that security is built-in by design, because when it comes to life-and-death consequences we can't make the same mistakes that result in lost Social Security numbers. It is another thing when it is heart monitors and cars on the road [getting hacked]. No. 2 would be education across the board to making it part of every child's curriculum and to focus on the skills gap that I hear throughout government and the private sector, to make sure they are given adequate cybersecurity skills but also to make sure that those who code know cybersecurity risks. You can become a computer scientist, but cybersecurity is an elective. It is not part of the standard curriculum even for experts. And No. 3 is working to ensure that private companies share with the company what they are seeing, and for the government to do a better job of sharing information that is classified and sharing information that cross the govt private sector line.

Q: Finally, having worked for Special Counsel Robert Mueller, what's your prediction for the alleged Russia U.S.-election manipulation probe?

Having worked for him the one thing I am sure of is that he will do the job that he has been given to the best of his abilities. He is going to follow the facts wherever they lead regardless of consequences and apply the law. He will do it as thoroughly and as great and professionally as anyone I can think of. Wherever it lands, I will have faith that it was done by the book.

MP McQueen *is editor-at-large, and can be reached at mpmcqueen@alm.com*