JULY 26, 2017

Legaltech® news

ONLINE

An ALM Publication

'A Wild Ride': Ruskin's New Cyber Co-Chairmen Talk Future Threats

The new additions to Ruskin's Cybersecurity and Data Privacy Practice Group, Richard Frankel and Steven Kuperschmid, discuss why modern attacks are so successful and why they will be getting worse.

BY RHYS DIPSHAN

Ransomware malware is crafted to exploit system vulnerabilities documented by the National Security Agency and deployed with alarming success. Personal information from millions of corporate clients is exposed due to simple, third-party errors. And all the while, questions remain about how deep recent cyberespionage acts may have penetrated the nation's institutions and economy.

For many businesses and consumers, this era of constant cyberthreats is a disturbing new normal. But for some, it's just another day at the office.

Of Counsel Richard M. Frankel and Partner Steven J. Kuperschmid of Ruskin Moscou Faltischek P.C.

As the two new co-chairmen at Ruskin Moscou Faltischek's Cybersecurity and Data Privacy Practice Group, Richard Frankel and Steven Kuperschmid are tasked with keeping a watchful eye on the current state of online threats and attacks.

For Frankel, who oversaw cybercriminal investigations for 16 years at the FBI, including serving as senior FBI representative to the Office of the Director of National Intelligence, such vigilance is second nature. And for Kuperschmid, who before joining Ruskin previously represented a host of corporate clients from health care and pharmaceutical brands to manufacturers and retailers, it's an inherent part of doing business in today's ever-digital world.

Legaltech News caught up with the co-chairmen to pick their brains on the most pressing cybersecurity issues. Here are highlights from the interview:

LTN: Ransomware attacks such as WannaCry and its variants exploit vulnerabilities in old

Windows operating systems. Why don't more companies regularly patch these systems?

Frankel: I have heard from people I know, CISOs in business, that say it can be very expensive and time-consuming to do these patches. It's not like doing a patch on your personal home computer. Usually these companies need to do multiple computing systems, whether it's laptops or desktops, and then they have to do their servers. And every time they need to do a patch or do an upgrade, it costs time and money. The question is, would you rather pay some money up front or pay more money down the line? And that's a risk that every company is going to take.

Kuperschmid: Cybersecurity needs to be looked at not just in the technological sense. Companies need to examine and update their administrative, physical, and technological safeguards to protect their data and defend against cybersecurity attacks. There are so many ways that hackers have to infiltrate into a company's network, and only a few of them are the traditional technological attack.

How do you think the cyberespionage threat will evolve in the near future?

Frankel: Cyberespionage has expanded exponentially over the last several years. We've gotten better [at understanding the threat], but I only see this getting more aggressive as things go on. Where we are going to be in several years, I can't imagine, other than to say, hold on this going to be a wild ride. Because I do think it's going to get worse and worse.

It's kind of like the nuclear arms race. As other countries were able to get nuclear weapons, it changed the layout of how [the U.S.] would defend itself and how [the U.S.] would deal with countries that had nuclear weapons. Cyber is so much easier for countries to get involved in, because you don't need that whole support that you do for nuclear weapons, you don't have the expenses. All you need is people who use computers and the ability to get on the internet. So this is going to become much more widespread.

What's your take on the proposed cyber cooperation plan between the U.S. and Russia?

Frankel: In my personal opinion, cooperation between governments is good, but you have to go into these cooperation agreements with your eyes wide open.

We have cooperated with Russia and China and with other countries on criminal matters for years. The FBI has legal attachés in China and Russia for when we work on law enforcement matters together. That's not to say that we shouldn't be aware that they are spying on the U.S. and that they are trying to get information out of the U.S. And if we enter into any of these agreements, we need to do so knowing that they're going to continue [such espionage].

In light of Verizon's Yahoo acquisition, why do you think M&A attorneys and businesses haven't been more focused on uncovering cybersecurity issues in the past?

Kuperschmid: Cybersecurity has and will continue to be an area of focus in M&A transactions. However, M&A is no different than business operations. Companies that are in highly regulated industries or highly susceptible to a cybersecurity attack have a better understanding of where cybersecurity fits into an M&A transaction. But those companies that are not in these industries don't yet have the understanding of the axiom that a cybersecurity attack is not if, but when. However, the field is beginning to change, and we are starting to see more companies take a focus on cybersecurity in M&A transactions.

Contact Rhys Dipshan at rdipshan@alm.com.

Steven J. Kuperschmid
skuperschmid@rmfpc.com
516-663-6686

Richard M. Frankel
rfrankel@rmfpc.com
516-663-6534