LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

THURSDAY, JANUARY 3, 2019

PERSPECTIVE

Top 10 cybersecurity predictions for the new year

By Robert E. Braun
and Michael A. Gold

'Tis the season for prognostication — from September through March, pundits and would-be pundits make their predictions, ranging from World Series winners to Nobel Prize laureates to Best Picture. In that spirit, we present our "bold predictions" — including some perhaps surprising thoughts — on cybersecurity for 2019.

1. Predictions of Doom: We would be remiss if we did not lead off with the most predictable of predictions: over the next year we will be inundated with regular and increasing predictions of doom, highlighting the evils of data collection and the evils of regulation of data collection; the ascendancy of artificial intelligence and other technology driving new and nefarious malware and breaches; and the increasing inability to fend off attacks.

2. Cryptomining: Cutting against predictions of doom, cryptomining on desktops, at least on the consumer side, will just about die. This isn't because we're getting better at combatting it. Rather, it's an economic issue: cybercriminals just aren't getting value out of targeting individual consumers with cryptominers. Instead, attacks distributing cryptominers will focus on platforms that can generate more revenue (servers, IoT) and will fade from other platforms (browser-based mining).

3. Privacy Legislation: Since the Yahoo attack, and following on the large scale attacks in latter 2018, our elected representatives in Washington, D.C. will follow industry leaders and demand comprehensive privacy legislation. They will hold hearings, they will make speeches, they will even introduce (more) legislation. But they won't pass any and if by chance they do, it won't work.

4. Breaches: Data breaches, on the other hand, don't have to worry about compromises between government and industry and the attendant horse trading. And because the hacking community never sleeps, we can expect that in 2019 there will be a breach whose magnitude exceeds that of any other recorded breach. And after that one, there will be another.

5. State and Self-Regulation: While federal legislators are unlikely to enact meaningful laws, state legislatures have been able to do so, and we fully expect to see more states join California in adopting comprehensive (and in many cases, contradictory) privacy legislation. And as they view this increasingly painful landscape, technology companies will attempt to create a code of conduct or similar industry-sponsored regulation. Public sentiment, and impending legislation, about privacy will cause companies to reconsider how they handle data. In an effort to stand out, companies will build their brands around transparency of their data collection practices and acknowledge that data is valuable.

6. Governance: One of the largely overlooked but essential elements of information security will finally rise to its deserved prominence. Information governance will be a priority as companies move beyond simply having written policies to automating their execution and incorporating information security as a key corporate governance competence. When buyers issue RFPs, they will include a governance component, requiring a commitment to data security and the enforcement of a defensible governance program that manages data through its lifecycle.

7. Internet of Things: People (and companies) are going to get tired of hearing about how their cameras, doorbells, washers, and shoes are insecure. Companies that want to rise above the crowd will join in establishing security standards for consumer and small business-grade IoT devices, creating a UL-like listing. The standard would let consumers know that a device with such certification meets specific minimum security standards (although it might not actually define security!). Expect the standards to require strong administrative passwords (recognizing that consumers don't voluntarily update their passwords), hardening operating systems, not listening on any ports except one or two that require encryption and authentication, and other obvious and desirable, but as yet ignored, requirements.

8. Data Localization: The internet recognizes no borders, but don't tell that to Russia, China, India and several other nations. Expect more jurisdictions to join them, that require information on its citizens or other key information to be maintained on servers located in that jurisdiction. This will force companies to either make significant investments in those jurisdictions or avoid them altogether.

9. Skimmers Go Digital: You're probably aware that when you use an ATM or hand your credit card to a server, there's a possibility your credit card information will be stolen, an event otherwise known as skimming. Expect skimming to reach more and more online payments. Cybercriminals are going after websites that process payments and compromising the checkout page directly. Whatever you buy, when you enter your information on the checkout page, if the shopping cart software is faulty, information is sent in clear text, allowing attackers to intercept in real time. Security companies saw evidence of this with the British Airways and Ticketmaster hacks.

10. Cyberwarfare Gets Rules: We don't think about it much, but war has rules; most nations have agreed to prohibit torture, poison gasses, attacks on civilians. But even though cyberwarfare is real, there are no real rules governing cyberwarfare, and some nations believe they can do almost anything with near impunity. This, however, may be the year when we see a Geneva Convention for digital warfare. This won't necessarily create a much safer world — some nations will continue to push boundaries when it comes to cyber warfare, and cyber attackers will continue to have a safe haven in Russia and China and North Korea. But cyberwar rules would recognize the potential damage that cyberwarfare can cause.

We don't necessarily expect all of these predictions to become reality. But we do think that these will be some of the things at top of mind for cybersecurity professionals and consumers alike.

Robert E. Braun *(rbraun@ jmbm.com) and* **Michael A. Gold** *(mgold@ jmbm.com) are the cochairs of Jeffer Mangels Butler & Mitchell LLP's Cybersecurity and Privacy Group. The Group counsels companies in all industries regarding compliance with state, federal and international privacy laws and regulations, establishing corporate governance frameworks and controls to establish effective information security, and in connection with security incidents and data breaches.*