SUMMER 2023 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss mobile device messaging risks to organizations, as well as legal and data security implications.

Shifting Legal Liability for Phishing and Smishing to the C-Suite

In September 2020, research firm Gartner, Inc. released a bold prediction: "Liability for cyber-physical security incidents will pierce the corporate veil to personal liability for 75% of CEOs by 2024," (https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl). That prediction set off a tsunami of both analysis and marketing addressing the questions of can we, should we, and how do we hold CEOs and CISOs responsible for data security? At the time, one of the indicators that Gartner may have been looking at could have been Massachusetts Senator Elizabeth Warren's Corporate Executive Accountability Act ("CEAA") and thinking about the ramifications for CEOs if the bill ever becomes law (it was sent to the Judiciary Committee in April 2019, and has not moved since). Despite the stalling of Senator Warren's bill, has Gartner's prediction borne out? More specifically, is liability for preventing data breaches resulting from phishing (social engineering emails), and smishing (text-based social engineering) attacks shifting to the C-Suite?

From the Ultimate C-Suite Desk

Beyond Senator Warren's proposed legislation, the Biden administration is also seeking a higher level of responsibility for cybersecurity. In its March 2023 National Cybersecurity Strategy ("NCS") (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf), the White House promoted a strategy that begins with "two fundamental shifts," one of which could be interpreted as a warning to organizations to strengthen their cybersecurity: Rebalance the Responsibility to Defend Cyberspace. The NCS promotes the idea that the best approach for the future of cybersecurity is for those who are building systems and holding data to be the ones who are bearing the weight of protecting the data. To the extent that phishing and

smishing are covered under this rebalancing goal, the NCS goes on to say, "[a] single person's momentary lapse in judgment, use of an outdated password, or errant click on a suspicious link should not have national security consequences." In other words, the Biden administration believes that we cannot rely on our employees and customers to be the solution to cybercrime – organization leaders are going to have to commit to strengthening their cybersecurity posture.

State AGs Acting in Concert

State attorneys general agree, and a growing number of states are acting upon the FCC's and FTC's rules regulating telecommunications firms and suing firms that do not act to prevent potentially fraudulent calls and texts from being disseminated across their networks. In May of this year, at least 48 states attorneys general joined together to sue Avid Telecom for violating the Telemarketing Sales Act, the Telephone Consumer Protection Act, the Truth in Caller ID Act, as well as many state codes and regulations (*State of Arizona et al, v Michael D. Lansky, L.L.C., dba Avid Telecom, et al.*, Case 4:23-cv-00233-EJM, US Dist. Ct, Dist. of AZ, (2023)). This landmark case names not just the corporation, but two of the officers individually, as responsible for potentially billions of harassing and possibly fraudulent calls. Similar cases by individual states have been brought by Vermont, North Carolina, and others. Whether these cases will do much to stop phishing and smishing is yet to be seen, but in the case of Avid Telecom, if you let through 7.5 billion robocalls in just over 4 years, someone is going to call you on that.

A Smish by Any Other Name

The FTC and FCC agree that SMS messaging is the equivalent of a phone call for the purposes of regulation, and both are making efforts to combat phishing of all types. The FTC is encouraging cellular customers to forward smishing messages to their carriers through a universal SMS number (7726 or SPAM) and to file complaints with the FTC at ReportFraud.FTC.gov, which will then begin a process that involves both the carrier and the FTC. The FCC has created a Robocall Response Team to address the problem of harassing and fraudulent calls and messages through cease-and-desist orders, fines, and collaboration with carriers to solve the problem at its origin. The message being sent by the FTC and the FCC is to make certain that carriers know they can be held responsible for not doing their part in stopping smishing attacks.

With so much attention being paid to the responsibility that organizations are expected to take in keeping data safe and protecting consumers from scammers, it's becoming more probable that we'll see the legal liability shift to organizations, even individual officers. This has already happened to one Silicon Valley CISO, indicating that the odds are good it will happen again. As this occurs, smart organizations will take steps to shore up their cybersecurity before a problem arises and not wait for service of process.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

DFRWS USA 2023
Baltimore, MD: July 9-12, 2023

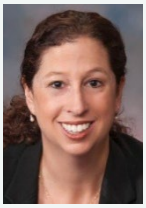
MASTER'S CONFERENCE JULY 2023
Seattle, WA: July 19, 2023

PFIC 2023 VIRTUAL
August 1-4, 2023

ABA2023 ANNUAL MEETING
Denver, CO: August 2-8, 2023

SANS DFIR SUMMIT
Austin, TX: August 3-4, 2023

Click here to see more upcoming events and links.



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: