SHARE:

Join Our Email List

View as Webpage

March 31, 2022

Welcome

Welcome to the sixth issue of *Decoded* for the year.

The Pennsylvania Chamber of Business and Industry is hosting the 2022 Information Technology Security Conference on May 5 in Hershey, Pennsylvania. Attendees of this in-person event will learn the steps they should take to protect their companies; how to secure evidence for internal and court purposes; when to let corporate leadership take the reins on the case, and more.

You can learn more and register by clicking here.

We hope you enjoy this issue and, as always, thank you for reading.

Nicholas P. Mooney II, Co-Editor of *Decoded* and Chair of Spilman's Technology Practice Group

and

Alexander L. Turner, Co-Editor of *Decoded*

Massachusetts-Based Background Check Company Creative Services Faces Multiple Lawsuits Over Data Breach

"'CSI determined that certain files dating from November 2018 to November 2021 may have been copied from their systems as part of a cyberattack,' BU wrote in its notification."

Why this is important: Companies that are handling confidential information need to ensure that they have rigorous protocols to guarantee the protection of that confidential information. Handling and processing confidential information without rigorous protocols to protect that information opens a company up to potential massive liability, as evidenced by the four class action suits against Creative Services Inc. ("CSI"). As explained in the article, it appears that the basis for the four lawsuits is that CSI did not take adequate steps (and was thus negligent) in protecting its customers' information. These

protocols should be reviewed on a regular basis to ensure that they are complying with any applicable local, state, or federal privacy requirements, and also account for the changing threat landscape.

Additionally, companies also should ensure they are teaching their employees to follow cyber hygiene by implementing regular training on how to spot suspicious emails or potential threats (amongst other things) and a thorough, regularly updated, employee cyber use policy for employees to follow. An employee's inadvertent carelessness in opening a suspicious email could result in a cyberattack and potential data breach, putting the company at risk. While the type of cyberattack that led to the breach at CSI was not specified, having a thorough training program and comprehensive employee cyber use policy will prevent cyberattacks against companies in the future. It also demonstrates that the company is not negligent in its protection of customers' confidential information. --- Alyssa M. Zottola

---

US Courts Mixed on Letting Data Breach Suits Go Forward

"But after about eight months of lower court decisions, the picture seems to be one of complexity rather than certainty."

Why this is important: The Supreme Court's decision last year in *TransUnion v. Ramirez* changed the legal landscape surrounding data breach litigation. In all litigation, in order for a plaintiff to bring any legal action, he or she must have standing. To have standing, the plaintiff must show that he or she has a tangible injury-in-fact. With many data breach and ransomware cases, it is difficult to show a concrete injury-in-fact because the injury is often an intangible harm, like the fear that your identity may be stolen in the future as a result of the cyberattack. Prior to the Supreme Court's ruling in *TransUnion*, various federal Circuit Courts had held that future injuries could qualify as an injury-in-fact that would support standing if the injury was "certainly impending" or if there was "substantial risk that the harm will occur." That changed with the Supreme Court's decision in *TransUnion* where it held that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm." Therefore, pursuant to *TransUnion*, the fear or risk of a future injury from identity theft following a cyberattack that exposes personal identifying information ("PII") is insufficient to convey standing to bring a suit against the breached entity.

While one would have a sufficient basis to believe that the Supreme Court's decision in *TransUnion* would provide clarity and lessen the risk of litigation in the event of a data breach, the opposite appears to be the case eight months after the decision. In some federal courts, a narrow reading of the holding in *TransUnion* has resulted in not much of a change, and standing is still being conveyed to plaintiffs in cyberattack cases on the basis that the injury-in-fact is "certainly impending" or if there was "substantial risk that the harm will occur." In a federal district court in Florida, the court stated that the holding in *TransUnion* did not apply in an identity theft case because the plaintiffs in the Florida case were seeking compensatory damages, whereas the plaintiffs in *TransUnion* were seeking statutory damages. Federal courts also continue to apply the *McMorris* factors from the Second Circuit's decision in *McMorris v. Carlos Lopez & Associates*. In *McMorris*, the Second Circuit set out a test for determining whether the risk of a future harm was sufficient to create standing in data breach cases. Even though it would appear that the holding in *TransUnion* would preclude the utilization of the *McMorris* factors when determining standing in data breach cases, federal courts in the Second Circuit continue to utilize the *McMorris* factors. Plaintiffs also are being creative in their attempts to circumvent the holding in *TransUnion* by framing their claims the same as or similar to a traditional cause of action, e.g. claims of improper data collection, or intrusion upon seclusion. However, these workarounds may still fail in ransomware cases because ransomware attacks rarely result in the disclosure or improper use of PII, so there is usually little to no future risk to the individuals whose PII was held ransom. So, what is the result of the Supreme Court's decision in *TransUnion*? Unfortunately, a continued lack of clarity. --- Alexander L. Turner

---

The FTC's New Enforcement Weapon Spells Death for Algorithms

"It may have found a new standard for penalizing tech companies that violate privacy and use deceptive data practices: algorithmic destruction."

Why this is important: This article describes the steps that the Federal Trade Commission is taking against companies gathering private information and using algorithms to target individuals for sales and products. The FTC appears to be increasing these efforts to protect consumers against the unauthorized use of personal data in ways not anticipated by those consumers. This is good. (Do not confuse this FTC

push, however, with anything related to proposed amendment of Section 230 of the Communications Decency Act. That act treats internet providers such as Facebook, Twitter, YouTube, Instagram, etc. not as publishers or speakers, but merely as aggregators with no liability for content. The FTC efforts are not related to the algorithm criticisms alleged in discussions of Section 230.) --- Hugh B. Wellons

---

Web Vendor CafePress Fined $500,000 for Giving Cybersecurity a Low Value

"Unfortunately, as the US Federal Trade Commission explained in a case report bluntly entitled CafePress, In the Matter of, the company wasn't up to scratch when it came to looking after the personal data of its customers and signed-up sellers."

Why this is important: CafePress is an online retailer that allows you to customize designs or logos on merchandise such as shirts, hats or coffee mugs. According to the U.S. Federal Trade Commission ("FTC"), CafePress' customer information was the subject of a security breach where the hacker accessed email addresses, passwords with weak encryption, unencrypted names, physical addresses, unencrypted social security numbers and other vital information. The failure of CafePress to properly respond to the breach through timely notification to affected consumers and their failure to fully investigate the breach for a number of months were noted in the FTC press release.

As part of a proposed settlement, Residual Pumpkin Entity, LLC, (CafePress' former owner) and PlanetArt, LLC (purchased CafePress in 2020), will be required to implement security programs to address the inadequacies that made the information vulnerable. This includes using security questions with multi-factor authentication methods, minimizing the amount of data that is collected and retained, and encrypting social security numbers. In addition to other terms, the companies will be required to have a third-party assessment of their security programs that will be provided to the FTC in a redacted format.

This matter demonstrates that organizations must conduct a thorough review of the effectiveness of their information security programs. Having minimal measures in place is insufficient and will not allow an organization to avoid responsibility for their failure to properly secure client data. An organization may consider retaining a neutral third party to review their policies and procedures so that any deficiencies can be addressed before a breach occurs. --- Annmarie Kaiser Robey

---

Controversial Alzheimer's Drug Approval Ignites FDA Reform Debate

"But critics say that more needs to be done to prove these drugs actually work in the real world, which could have big implications for the pharmaceutical industry."

Why this is important: Interesting article. The FDA adopted an Accelerated Approval Process years ago to permit conditional approval of a drug much faster, if the drug is aimed at addressing an unmet need. Drugs conditionally approved are placed into a longer-term program to study safety and efficacy while the drug is made available to patients. This program has been controversial since it was adopted, although many patients, especially patients of terminal conditions, favor this. Recently, a new Alzheimer's drug was approved in this program, even though its advisory committee voted against it. Also, the drug was allowed nine years to prove its efficacy, which many deem too long. Many now are criticizing this program and how decisions are made about who qualifies for it. --- Hugh B. Wellons

---

Cyber Stress: This is Why Employees are More Worried About Their Virtual Security

"In 2019, 64% of employees said that data privacy scandals make them worried that their data might be at risk, according to a study conducted by information technology company Accenture."

Why this is important: This article discusses the security risks companies must consider when implementing remote work or hybrid work arrangements. The security of their employees' networks and homes become significant. Research has revealed that more than half of remote employees use a

personal device to access work data, meaning that employers also need to consider the security of their employees' personal devices. This research further showed that as much as 67 percent of cyberattacks target remote employees. Security risk concerns are not limited to the employer. Employees report that using personal devices or their home networks for work purposes leaves them concerned that their personal photos, banking and other private information, and private communications are more vulnerable to attacks. At bottom, remote and hybrid work arrangements are here to stay for some companies and industries. Employees and employers both have reason to invest in cybersecurity to protect these arrangements. --- Nicholas P. Mooney II

Redesigned CRISPR Gene Editing Tool is 4000 Times Less Error-Prone

"This may revolutionize genetic editing."

Why this is important: CRISPR-Cas9 has been revolutionary in editing genetic material. A problem is that sometimes the "fix" does not work exactly as the physician/operator wanted it to work. There are sometimes errors and unintended consequences in the process. Other researchers have developed ways to work around this problem, but at huge reduction in speed. University of Texas-Austin has studied this and determined that Cas9, the protein used to cut the gene has difficulty dealing with a specific part of the gene. It developed an improved protein, called "SuperFi-Cas9," which allows improved gene editing with little or no reduction in speed of process. --- Hugh B. Wellons

---

Cloud Security: How Your Public Cloud Environment May be Vulnerable to Data Breach

"Half of the security pros surveyed by Laminar said their cloud environments were hit by a data breach in 2020 or 2021."

Why this is important: Thinking about lowering costs by utilizing a cloud service to host your data? Before you make that change, you may want to think about how the short-term financial gains you may experience with the switch to cloud storage compares to the long-term costs associated with increased data security risks. Recently, a cloud security provider, Laminar, released a report on how relying on multiple cloud providers can add complexity and risk to your data security. Laminar surveyed 500 data security professionals last month. Of those 500 security professionals, 56 percent said that their organizations used two or more cloud service providers. Even though the surveyed individuals are the data security professionals for their organizations, 51 percent stated that they did not have full visibility into all of their organization's cloud data. Scarier still is that 50 percent of them responded that their organizations had data breaches in the past two years, and another 13 percent said they were unsure whether their organizations had been breached in the past two years. What is the cause of this lack of transparency and data vulnerability? A lot of it has to do with shadow IT, which is when employees install or use technology without the permission or assistance of IT and security staffers. Shadow IT can result in shadow data, which includes "databases in test environments, unmanaged backups, old or outdated databases and unlisted databases, all of which can be vulnerable to security risks." If you decide to switch to a cloud-based data storage system, or already have made the switch, you would be wise to adopt adequate cloud-based security tools to protect your data. This includes preventing employees from utilizing unauthorized cloud-based tools. By utilizing the proper tools and protocols, you increase the visibility of sensitive data and aid in the detection of possible data breaches. --- Alexander L. Turner

---

Brain-Computer Interface Helps Patient with Locked-In Syndrome Communicate

"The patient, a 37-year old man with ALS, was able to communicate despite not having any voluntary muscle control."

Why this is important: Some neurological disorders -- stroke and ALS/Lou Gehrig's Disease are the most common -- can create a condition called "locked-in syndrome." This horrible condition removes the ability of the person to communicate with the outside world, even though they are fully aware. This new

technology involved implanting electrodes into a patient's brain, teaching him how to align brainwaves with the electrodes, and use "auditory feedback" to begin communicating with health professionals and others. Eventually, he could spell words and perform other communications to answer questions and even comment on conversations. --- Hugh B. Wellons

---