SHARE:

Join Our Email List

View as Webpage

June 9, 2022

Welcome

Welcome to the 12th issue of *Decoded* for the year.

Before we discuss the top technology news stories for this issue and why we found them important, we wanted to announce that our Education Practice Group has launched their own e-newsletter -- *The Academic Advisor*. This education-focused publication takes the same process we have here -- finding timely and interesting news stories and explaining why they are important to the reader. They cover a wide variety of areas from important legal cases that impact the education field to technological issues that affect the educational world. As a matter of fact, the first article listed below comes from our first *The Academic Advisor* issue. If you have a specialized interest in the educational field, you can read the inaugural e-newsletter here and sign up to get on the mailing list.

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*

Universities Share Lessons Learned from Ransomware Attacks

"According to a recent Sophos poll of IT professionals, 44 percent of educational institutions suffered ransomware attacks in 2020, and 58 percent of those hit said the attackers successfully encrypted their data."

Why this is important: Despite patching, back-ups, and testing, educational institutions remain ripe targets for ransomware attacks. Adding flame to the fire, *Ed Tech* reports that recovery costs in the education sector are nearly 50 percent higher than other industries with an average $2.7M price tag.

Tools like PYSA, a form of malware that exfiltrates data and encrypts users' critical files, have been increasingly used by cyber criminals to target higher education, K-12 schools, and seminaries in order to elicit ransom payments, according to the FBI. On college campuses, siloed operations and lack of communication with IT can be a contributing factor.

At institutions like California State University and Michigan State University, strategies for fending off and responding to ransomware attacks were enhanced through first-hand experience with hacker infiltrations. In the wake of such attacks, preventive measures employed and recommended by these institutions have included: (1) user education, (2) ongoing communication between IT and campus members, (3) use of multi-factor authentication, (4) network segmentation into tiers, (5) enhanced vulnerability testing of internet-facing systems, (6) establishing relationships with threat intelligence agencies, and (7) use of endpoint/extended detection and response tools.

Additional mitigation strategies recommended by the FBI include, among other things: (1) backing up critical data with air gap and password protection offline, (2) avoiding lags between the release of operating system updates/patches, software, and firmware and its installation on campus networks/devices, (3) disabling hyperlinks in received emails, and (4) disabling unused remote access/RDP ports and monitoring remote access/RDP logs. NIST, the National Institute of Standards and Technology (part of the U.S. Department of Commerce), encourages organizations to create an incident recovery plan that includes defined roles for company leadership, strategies on decision-making, and critical contacts for responding to a ransomware attack.

With cyber criminals' focus on the education sector, schools should act now to defend against future attacks and to develop their response plans. --- Erin Jones Adams

---

Cryptocurrency Meltdown is Wake-Up Call for Many, Including Congress

"Two senators — one Democrat and one Republican — proposed legislation that seeks to build a regulatory framework around the cryptocurrency industry; other members of Congress are considering more limited legislation."

Why this is important: This article discusses last month's collapse of stablecoin TerraUSD and the general "meltdown" in the cryptocurrency market that reduced the total value of cryptocurrencies from a high of $2.8 trillion last November to below $1.3 trillion. This drop has brought about a new call for regulation, and at least two bills have been introduced in Congress. This is the beginning of the process, but it's likely some amount of regulation will result from this. In the practice of law, we say bad facts make bad law. We saw this when the 2008 mortgage meltdown and financial crisis led to the passage of laws that have been questioned, criticized, and wrestled with now for over a decade. Just as Know-Your-Customer requirements came to the crypto space, more regulation is coming. We need Congress to be deliberate in what it does and not react to the sticker shock of the market drop. --- Nicholas P. Mooney II

54% of CISOs Struggle to Convince Board to Prioritize Cybersecurity Investments

"Communicating cyber risk to C-suite executives is clearly improving—only 4 percent of executives said that they did not discuss cybersecurity in the boardroom."

Why this is important: Previously in Decoded, we discussed the importance of a company's Chief Information Security Officers ("CISO") communicating with board members about potential cybersecurity threats and vulnerabilities. Failure by a CISO to inform company leadership of potential cybersecurity threats and vulnerabilities can result in the CISO being held personally liable in the event of a data breach. Additionally, C-suite executives and board members who fail to heed their CISO's warnings about cybersecurity vulnerabilities can also be held personally liable in the event of a data breach. However, there is a worrisome trend in corporate cybersecurity where 54 percent of surveyed CISOs report that they are struggling to convince corporate leaders to focus on and invest in cybersecurity. As a result, the survey found that only half of the surveyed executives give cybersecurity a top priority when discussing the company's strategic plan. The frustration CISOs are experiencing in not being able to break through to corporate leadership about the importance of proactive cybersecurity is likely contributing to the burnout among CISOs that Nick Mooney discusses in this edition of Decoded. What is a CISO to do in the face of continued corporate leadership's ambivalence toward cybersecurity? They should communicate

with corporate leadership in a language they understand -- business risk. The issues associated with lax cybersecurity should be framed as a significant business risk where the upfront cost of cybersecurity may be significant, but the cost of responding to a cyberattack post-breach will cost the company even more. Reminding corporate leadership that their personal finances may be at risk if they fail to proactively address cybersecurity concerns will likely also stir them to action. Fostering a corporate culture that values and promotes cybersecurity can help strengthen an organization's security posture and alleviate some of the pressure placed on CISOs. --- Alexander L. Turner

---

North Carolina's Pandemic Tech Boom Ranks Top 5 Nationally

"The number of tech workers in North Carolina grew by nearly 5% during the pandemic."

Why this is important: North Carolina has attracted tech industry employers for some time. There are employment opportunities with larger companies such as Apple and Google as well as local tech startups.

The Research Triangle area (which contains Duke University, UNC-Chapel Hill and North Carolina State University) provides an excellent environment for companies seeking tech-savvy employees. After the onset of the pandemic, many people exited more costly areas such as New York City and the Bay Area to relocate to less costly areas such as North Carolina. Although housing prices and other costs have started to increase there as well, people are still moving to the region. As companies seek to fill positions with qualified individuals, they should be mindful of the trends related to such population shifts. --- Annmarie Kaiser Robey

---

Kaiser Data Breach Exposes Health Care Data of 69K Patients

"Kaiser says an attacker accessed an employee's email account containing patients' protected health information."

Why this is important: "Chair-to-Desk Interface Error" is a tongue-in-cheek way for tech support analysts to name human error as the cause of an issue. Kaiser Permanente has become yet another recent example of email information security breaches. Human error is by far the leading cause of data breach, accounting for almost 95 percent of incidents. In the case of Kaiser, the breach stemmed from unauthorized access to a single employee email account, which just happened to expose the PHI of approximately 69,000 patients. Data exposed included full names, medical record numbers, service dates and laboratory results. Fortunately, this appears to be a mere exposure incident, and there is no indication that data was stolen or misused to date. But, all this points to several key takeaways for employers handling PHI. Training, training, training. Human error is mitigated by regular training. Email security should also be a top priority, both on the training side and on the infrastructure side. Systems can and should be developed such that an individual email account does not unnecessarily host the data apart from the secured database. Even a small exposure of PHI can result in significant legal risk for an organization. --- Brian H. Richardson

---

How and Why Ransomware Responses Go Haywire

"A lack of fortitude and preparation on the communications front often puts enterprises at risk for greater harm."

Why this is important: What happens when your company has suffered a ransomware attack? According to this article, businesses often respond with a five-alarm-fire response that is not well-planned. That leads to problems. The article advocates steps that businesses can take before an attack to better position themselves for the moment when the inevitable occurs. Have a rapid response team with ransomware negotiators on standby. Be transparent and consider having press releases prepared and approved by the company's legal department beforehand. Don't rush to pay a ransom before understanding the full scale of the attack. And, most of all, of course, don't panic. The message here is plan for an attack before it occurs. --- Nicholas P. Mooney II

New York Judge Dismisses Class Action PACS Data Breach Lawsuit for Lack of Standing

"A class action lawsuit filed against NorthEast Radiology PC and Alliance HealthCare Services over a data breach that exposed the protected health information of more than 1.2 million individuals has been dismissed by a New York Federal Judge for lack of standing."

Why this is important: Even though medical-related data breaches are on the rise, courts continue to dismiss data breach cases for a lack of standing. In this case, the protected health information ("PHI") of almost 300,000 patients were exposed due to a misconfiguration of the health facility's Picture Archiving Communication System ("PACS"). The breach was discovered by security researchers when they noticed the misconfiguration of the PACS and they notified the facility and its vendor. Plaintiffs alleged that the facility and its vendor failed to implement adequate security protocols to protect patient's PHI, which allowed unauthorized access to patients' PHI. However, the plaintiffs failed to plead or show that the plaintiffs suffered an injury-in-fact. Stated otherwise, the plaintiffs did not plead and could not show that they suffered any harm as a result of the data breach. Without the showing of a specific harm as a result of the breach, there can be no finding of standing to allow them to bring the case. Specifically, the Court utilized a three-factor test for determining whether allegations of an injury from a data breach gave rise to a cognizable Article III injury-in-fact establishing standing. That test is: (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud. Finding that the facts of the matter did not satisfy this test, the court found that the plaintiffs had not suffered an injury-in-fact and, therefore, lacked standing to proceed with their case, thereby necessitating the dismissal of their action. --- Alexander L. Turner

---

Kmart and Bunnings are Tracking Customers with Facial Recognition

"For the most part, customers are having their biometric data captured without their knowledge or consent."

Why this is important: Do you consent to a retail store's privacy policy simply by walking into the store? That is a key question faced by Australian regulators looking at the way certain retailers have been operating in recent years. A new consumer report indicates that several retailers in Australia have been passively collecting biometric data on their customers using facial recognition software. The retailers point to their online privacy policy statements, but consumer advocates say the practice does not comply with the Australian Privacy Act, which regulates the use of biometric information to a higher standard than other personal information. In the United States, retailers have long used a telephone number to create a customer profile, selling the data for targeted ads, coupons, and other purposes. Customers actively participate in this and consent to the practice by entering their phone number or signing up for a store's program. Passive collection of biometric data is an entirely different approach, but could be used for much more. Profiles could be expanded from simply what a customer actually purchases to include such data points as what areas of the store they pass through, which particular ads catch their attention, whether product is selected and then returned to the shelf, and much more. Security risks would certainly extend to protecting the data. As increasingly more products and services turn to biometric signatures for increased security, those data points must be protected. In Australia, the question is being turned over to a Commissioner to decide whether the practice breaches consumer protection regulation. --- Brian H. Richardson

---

The Unrelenting Threat of Ransomware is Pushing Cybersecurity Workers to Quit

"Cybersecurity professionals face immense pressure to keep businesses secure, and this stress is leading many to consider leaving the industry altogether."

Why this is important: Virtually anyone in business knows that cybersecurity is growing more significant every day. The need to train employees, bolster processes, secure networks, repel attacks, and maintain confidentiality of customer data is a critical daily task. The frequency of cyberattacks,

whether they be on financial institutions, schools, hospitals, infrastructure, or connected medical devices, are playing out daily in the media. This article highlights one of the overlooked issues that comes with this increased focused on cybersecurity: the threat that cybersecurity professionals will quit. This article reports on the "increasing and unsustainable stress levels" those professional face and discusses a recent survey by cybersecurity company Deep Instinct on the fallout. It "found that 46% of senior and executive-level cybersecurity professionals have considered quitting the industry due to stress." More than 90 percent of those professionals admit to being stressed in their roles, with many of them admitting that the stress is having a negative impact on their ability to do their jobs. Larger workloads, longer hours, the need to always respond immediately, and the extra measures needed to secure a remote workforce all add to the stress these professionals are feeling. At bottom, Deep Instinct's survey results are alarming. Ransomware and other cybersecurity threats are a constant presence, and it's critical that businesses find a way to help their cybersecurity professionals manage the stress and burn out that the industry is reporting. --- Nicholas P. Mooney II

Bill Calls on FDA to Regularly Update Medical Device Security Guidelines

"Senators introduced a bill that would require the FDA to update medical device security guidelines every two years."

Why this is important: As we have discussed in previous issues of *Decoded*, most medical devices are leaving manufacturers with known cybersecurity flaws that leave them vulnerable to attack. In response, Congress is proposing a number of new data security bills in order to address these known cybersecurity vulnerabilities. In the last issue of *Decoded*, Brian Richardson and I discussed the PATCH Act, which addresses the medical device security at the premarket state. In addition to the PATCH Act, Senators Jacky Rosen (D-NV) and Todd Young (R-IN) have introduced the Strengthen Cybersecurity for Medical Devices Act, which would require the FDA to update its medical device security guidance every two years. Having the FDA update its cybersecurity guidance every two years is a significant step up from the eight years it has taken the FDA to update its latest guidance on medical device cybersecurity (2014-2022). In addition to the FDA having a regular schedule to update its cybersecurity guidance, the proposed bill also would require the GAO to issue a report "evaluating the challenges that providers, health systems, and manufacturers face in accessing federal support when addressing medical device security vulnerabilities." In addition to this report, the GAO will be tasked with providing guidance to other federal agencies on how they can assist with improving medical device cybersecurity. We will have to wait and see what the final form of both the PATCH Act and the Strengthen Cybersecurity for Medical Devices Act look like, and whether they will pass. While these bills are good steps in the right direction to improve the cybersecurity of medical devices around the country, the legislative process is slow, and even if passed, rules, regulations, and guidance will lag behind innovation. Therefore, medical device manufacturers and healthcare organizations must take it upon themselves to advance and promote cybersecurity in their industry instead of relying on Washington, D.C. to tell them what to do to protect the nation's medical devices from cyberattacks. --- Alexander L. Turner

---

Share Tweet Share

This is an attorney advertisement. Your receipt and/or use of this material does not constitute or create an attorney-client relationship between you and Spilman Thomas & Battle, PLLC or any attorney associated with the firm. This e-mail publication is distributed with the understanding that the author, publisher and distributor are not rendering legal or other professional advice on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use.

Responsible Attorney: Michael J. Basile, 800-967-8251