CLIENT: MyIDMatters

PROJECT: Issue 62, Q4 2024

DATE: 12/02/2024

Articles:

1. Just How Important Is Customer Privacy, Really?

It has been a few issues since we have discussed a widespread trend in customer behavior that has impacted how companies do business. In the age of AI, it is more important than ever for companies to take proactive and intentional steps to safeguard the privacy of our personal data. There is publicly observable data to support this shift, including Google Trends: the term "cybersecurity" has seen a nearly 250% surge in popularity over the last five years. Moreover, research shows there has been a significant increase in the number of people who have experienced a cybersecurity breach in the last decade. This is in addition to private company data that signals the extent of this shift, as well.

With the recent release of Cisco's "2024 Consumer Privacy Survey," the company's chief privacy officer agreed that "privacy has grown from a compliance matter to a customer requirement." This claim is bolstered by the survey's findings: 75% of respondents indicated that trust in data practices influences their buying choices. This is perhaps influenced by the fact that more than 50% of respondents are aware of public privacy laws, which represents a notable rise from past surveys. This increased awareness makes sense when one considers a correlated rise in data breaches, sales of customer data as well as a collective back-of-the-mind concern that companies may even steal data without customer awareness.

Regardless of whether customers understand the complexity of privacy laws (which can be chock-full of legalese), we all have a general opinion about what it means to ethically handle our own personal data. Other customer surveys, such as the PwC Voice of the Consumer Survey, suggest that consumers overwhelmingly (as high as 80%) require assurances from companies that their data will neither be shared improperly nor sold. This is roughly the same number of respondents who are concerned about the utilization of generative AI in complex industries, such as healthcare. The advent of generative AI represents a potential turning point for companies: if the privacy concerns surrounding AI are not carefully addressed, the backlash could be immense. Because if these end-of-year surveys prove one thing, it is that customer privacy is of critical importance—no, really.

2. The FCC's New Role (Legal)

The launch of the Federal Communications Commission's (FCC) privacy and data protection task force in June of 2023 has led to several major privacy actions and multiple partnerships between the agency and 10 different state attorneys general. The decision of the FCC to take an active role in enforcing cybersecurity and data protection has increased federal intervention in cybersecurity protections (in lieu of any overarching federal legislation). Moreover, the expansion of this partnership with state attorneys general means that there is currently more federal-state collaboration on cybersecurity protections than ay any other point in the United States' history.

This focus is a change in scope for the FCC. According to its leader, Loyaan Egal, the task force is a recognition "of the importance of ... the amount of data that we generate on a day-to-day basis." A couple of the task force's interventions have already led to public victories: this year alone, the FCC has fined major telecommunications carriers $196 million for consent violations, forced TracFone Wireless to pay $16 million for three separate data breaches, and cracked down on additional data breaches and unlawful storage across the telecom sector. These enforcement interventions have come in the wake of a December 2023 Report and Order that expanded the scope of data breach notification rules for telecom carriers. According to these new rules, companies are required to notify the FCC in the event of a breach within seven business days of a breach being determined.

Due to this change in scope, the FCC has decided to hire a new chief technology officer to provide technical and strategic advice to the Enforcement Bureau and task force. With previous experience as a senior director of technology at Verizon, Andy Hendrickson is expected to offer insight into how comms networks operate, thereby allowing the task force to better respond to the rapid development of new technologies that are able to be compromised. However, with its attention turned toward data breaches and treatment of customer data, Hendrickson's hiring might not be the last addition to the FCC task force. A new federal focus might mean new roles for everyone.

3. Changes to HIPPA Coming (Legal)

For nearly 30 years, the Health Insurance Portability and Accountability Act (HIPPA) has protected sensitive health information from being disseminated to third parties without the consent of the patient. The right to one's own medical information is critical, and it is especially important in a day and age in which personal information has been monetized by bad actors. This is why it is notable that The Department of Health and Human Services (HHS) has filed proposed modifications to HIPPA in order to strengthen cybersecurity protections. At a time when there is widespread legal ambiguity over what data is HIPPA protected, the HHS is taking steps to ensure patient rights.

Why are there legal questions as to how healthcare organizations can/should share patient data with one another? A federal case, *AHA v. Becerra*, complicated what pieces of information could be considered patient information because the ruling was not sufficiently clear with respect to what could and could not count—this has led to confusion and a reluctance for healthcare organizations to act for fear of lawsuits. Furthermore, these concerns come at a time when ransomware is being utilized more than ever to attack these same organizations: nearly 400 attacks have occurred in 2024, and the scope of these breaches is far more significant than in years prior. Not only are healthcare organizations worried about sharing data with one another, they are afraid of losing it to outside parties.

So although HIPPA changes and updates occur far more than the general public realizes, this update has been sorely needed. The framework for this change was conceptualized with the development of cybersecurity goals for the healthcare sector in mind. At the moment, compliance for these cybersecurity rules will be voluntary; however, the Health and Human Services Department's Office for Civil Rights (OCR) believes a new update will make some of these requirements mandatory. A senior advisor for the OCR has been quoted as saying there has been "tremendous increases in the use of ransomware and hacking to obtain unauthorized access." Thankfully, there is also tremendous attention on this issue from the OCR. We will continue to monitor this story for additional updates.

4. Android Malware Strikes

Although most cybersecurity attacks are levied against laptops and home networks, the rise of smartphones has forced bad actors to get more creative. One recent case of a smartphone malware campaign targets Android users specifically: by stealing contactless credit card payment data, hackers are then able to leverage this information for making purchases. This attack is predicated on both social engineering and SMS phishing that directs individuals to domains that impersonate websites and banking applications. The good news is that it does not appear that these actors have managed to leverage legitimate programs; the bad news is that these impersonations sure do look real.

So how does it work? The process is remarkably simple. The attackers send an SMS text that includes a link for an app download that appears legitimate to the recipient. After the victim downloads the app, the hackers then phish their banking credentials to access their accounts. However, because banks have protocols in place to avoid this kind of attack, the hackers then call the victim pretending to be a bank employee. After informing the victim about the security incident (that they themselves carried out), the victim is then asked to change their PIN code as well as to validate their banking card via a different malicious app. When the victim complies, the hackers have everything they need to drain the victim's accounts. Now at this time, there is no evidence to suggest that these apps were distributed through the Google Play Store. It is also important to note that another reason this attack is carried out in two steps is because the second malicious app is already banned from the Play Store.

Avoiding this attack is simple, but it does take diligence and discipline. Do not open links from unknown numbers unless you can absolutely verify that the number is from someone you know. Furthermore, if your bank calls you, make certain that they can prove they are a member of your bank: an unknown or non-public number here tends to suggest that the call is fraudulent. Ultimately, this story is an important warning about the rise of cyberattacks. Even when you are off your computer, you still need to be careful.

5. Global Cybersecurity Rule Changes (Legal)

In previous issues, we have discussed the relative paucity of cybersecurity laws in the United States. And although there has been some movement on the state level, these efforts tend to mirror other gold-standard privacy laws (such as Connecticut's cybersecurity law) as opposed to the enactment of a law specific to the state itself. However, despite the lack of legal engagement in the United States, 2024 saw tremendous changes with cybersecurity rules across the globe. Here are some of those changes:

The E.U.'s NIS2 – With a 21-month implementation period, this direction was designed to strengthen cybersecurity resilience with respect to healthcare networks and transportation services as well as to unify regulations across the European Union. Additionally, this directive is set to enhance cooperation amongst national authorities while also forcing organizations to report cyber breaches within 24 hours (which is six days sooner than most United States federal regulations demand).

The U.S. National Cybersecurity Strategy – Although this strategy is not technically a federal law, it does help bolster weak areas in the United States' cyber approach. There has been notable progress on objectives ranging from helping critical infrastructure owners prepare better for cyberattacks to ensuring that the U.S. is at the forefront of developing cybersecurity standards. Overall, this strategy is working to reduce the burden from individuals and communities back toward those organizations best prepared to manage these risks. It is a necessary step toward a comprehensive cybersecurity plan.

Singapore's Operational Technology Cybersecurity Masterplan – The goal of this legislation is to increase cybersecurity support surrounding operational technology (e.g., traffic lights, fuel station pumps, etc.). These are pieces of technology that are rarely considered when it comes to cyberattacks and yet are essential for a functioning nation. More than 60 organizations contributed to the plan, which shows the collective cybersecurity buy-in across Singapore.

The E.U.'s Cyber Resilience Act – Finally, this last piece of legislation covers the other side of technology—smaller products and software with digital components (e.g. baby monitors and smart watches). For these pieces of technologies to be properly protected, the cybersecurity protocols surrounding them must be maintained across their entire lifecycle. This means that consumers are protected throughout every step of the production and usage process.

6. The Importance of Federal Cybersecurity Infrastructure (Infrastructure)

We know, we know: infrastructure is not the sexiest topic when it comes to cybersecurity. However, powerful cybersecurity is not only impossible without strong infrastructure—infrastructure is also one of the most important assets for cybersecurity to protect! The unspoken bulwark against bad actors is our federal cybersecurity infrastructure; however, some experts believe that we do not have the proper assessments in place for community-wide cyber resilience. It is of critical importance that communities and agencies coordinate their cyber defenses and responses amongst one another, and this posture is currently lacking in the wake of a collective, demonstrated cyber resiliency.

What is the real-time assessment of cyber resilience? According to Jeff Le, who spent four years in the cabinet affairs function for the California governor, it is the ability to:

1. Identify the number of risks in the sector, thereby highlighting potential vulnerabilities.
2. Quantify the number of incidents that did occur against what could have happened.
3. Understand and learn from the percentage of risks monitored.

Le's argument is that we do not actually have a strong recognition of our national cyber resiliency because we have never performed a widespread assessment across our communities. Unfortunately, the need for this assessment has become even more important in the wake of cyberattacks that targeted and compromised the information of many federal workers. These attacks on federal workers are so crucial that a bipartisan bill was introduced in the Senate to ensure contractors also adhere to vulnerability disclosure policies in order to reduce known security vulnerabilities.

Le is not the only expert who questions the strength of our cyber resilience. The nation's former federal CISO has said that it is "a really good time to step back and just examine the current landscape of threat trends and technology... what's the current posture of civilian enterprise today and how do we help it move up together?" Additionally, a private-sector vice president at Booz Allen has argued we need a "holistic national cyber strategy—one that goes beyond compliance and urges companies to put resources to the rhetoric." With these experts aligned, it is clear we need to double down on cyber resiliency. Whether we can determine a way to do so will have to been seen.

Quarterly Newsletter:

What Is the Amazon Threat Intelligence Unit?

Many important cybersecurity interventions occur at the federal level, but maintaining a strong national cyber defense is an imperative issue that has also been taken up by the private sector. Since 2010, Amazon's threat intelligence unit has been working to both identify domestic and international cyberattacks as well as to eliminate these threats. Unlike companies like Google or Microsoft that publish threat intelligence reports (thereby raising their public perception), Amazon's threat intelligence unit has been working in relative anonymity for the last 14 years. This highlights a central issue at the heart of the federal government and private sector's relationship—Amazon is financially motivated to demonstrate the superiority of its products relative to its competitors. However, this might be to consumers' benefit.

For example, Microsoft has had a number of breaches from other nation-states, including from a Russia-backed threat group earlier this year. On the contrary, Amazon's infrastructure size allows for protection advantages that its competitors may not be able to match. One example would be its threat detection systems, such as a system of honeypots (called MadPot) that lure in 750 million potential threat interactions every day. Additionally, Amazon has a threat intelligence system called Mithra that is responsible for discovering nearly 200,000 malicious domains per day. This is one area in which Amazon's infrastructure offers an enormous benefit: MadPot and Mithra can interact with one another to share data as well as to pull in additional data from Amazon's cloud platform.

But Amazon has also had success against state-sponsored bad actors, as well. For one calendar year, the threat intelligence unit had been monitoring Anonymous Sudan; as a result, two Sudanese nationals were arrested in conjunction with this cyberthreat group's attacks against United States agencies and infrastructure. Moreover, the unit has also been a player in the Ukraine-Russia conflict, helping the former's cyber defense agency, CERT-UA, to defeat a mass-phishing campaign carried out by Russia. These two examples were publicly noted by Amazon; however, there are other actions by the unit that have not previously been disclosed, such as shuttering disinformation campaigns aimed at discrediting the United States Army by Iranian and Chinese actors. With its ability to identify hacking campaigns before they become public, Amazon is becoming a major asset to U.S. intelligence agencies.

Glossary:

Five Cybersecurity Attack Terms

Attack Vector

There are many points of vulnerability through which a cybercriminal can attack a system: these are called Attack Vectors. These vectors do not only extend to technological weak points, but they also target human psychology as well. With the joint rise of smartphones and work-from-home employees, these vectors have increased exponentially as individuals (often unwittingly) increase their exposure.

Brute Force Attack

Brute Force Attacks involve guessing a victim's password by attempting a series of combinations until the password is discovered. This attack is as old as cyberattacks themselves; however, hackers continue to employ it because it works. One way to combat this type of attack is to limit the number of password submissions within a specific time limit—that way, bad actors do not have unlimited attempts.

Drive-By Download Attack

A common method of large-scale malware attacks is called a Drive-by Download. Websites that are not properly encrypted or secured are infiltrated, and hackers place a malicious script into the website's coding. The reason these attacks are so pernicious is because they do not require any action of behalf of the victim other than visiting the site—this is an attack that occurs automatically.

Process Hollowing

Process Hollowing is an attack that involves altering the code in an executable file to turn that executive function against the user. The process is “hollowed” when its initial command is replaced with malicious code that can often escape detection (often through an initial phishing attack). This hollowing allows these attacks to, for example, avoid detection analysis software.

SIM Swapping

SIM Swapping involves bad actors intercepting the online banking SMS codes you receive to verify your account. To do this, cyber attackers create a copy of a victim’s SIM card and/or acquire the SIM card through fraudulent means. Banks attempt to combat this attack by reattaching the SIM card to the original account; however, you should be on alert whenever you receive a SIM notification.