CLIENT: MyIDMatters

PROJECT: Issue 60, Q2 2024

DATE: 6/21/2024

1. Artificial Intelligence & Academia (Privacy)

In previous articles, we have discussed the outsized effect artificial intelligence has on cybersecurity as well as on privacy laws. Moreover, we have considered how chatbots, such as ChatGPT and Microsoft Co-Pilot, are fundamentally altering the world of academia (along with the potential privacy concerns that accompany their use). These two chatbots, however, are not the only generative AI bots that students and workers are utilizing to complete assignments. Accordingly, parents and organizational managers alike face several security challenges and risks that must be properly addressed by both AI companies and users.

So what risks do generative AI users face? And what they can do to better guard against potential attacks? The first set of risks has little to do with cybersecurity: for example, generative AI chatbots can not only get questions wrong, but they can also make up facts they believe to be correct; they can be biased with respect to leading questions from users; they can also be persuaded to produce toxic or offensive content without employing self-censorship. However, despite these risks, many users still find generative AI useful and, ultimately, a net-plus for their schooling or work products.

This is where the second set of risks becomes critical. Because artificial intelligence requires immense amounts of data to effectively work (remember: generative AI is only as good as the information you feed it), this means that it can capture a substantial portion of your personal data, as well. Bad actors can gain access to this data, which means bypassing attacks on your personal device (otherwise required for conventional attacks). This is one of many reasons why you should avoid sharing personal or company information with generative AI. Additionally, as academic institutions and workplaces continue to embrace generative AI, this can lead to increased pressure to provide personal data—especially when these institutions do not understand how to implement proper cybersecurity safeguards.

To protect yourself against attacks on generative AI, it is essential to continually backup your information and use encryption whenever possible. Install antivirus and anti-malware software on any devices you might utilize when accessing generative AI. If you can, store your most sensitive data on a hard disk as opposed to your local disk. And whenever possible, check back with MyIDMatters to see whether any new breaches or parent company vulnerabilities have been reported.

2. Trends in U.S. Cybersecurity Law (Legal)

In a recent blog by the International Association of Privacy Professionals, two privacy experts wrote that "the obligation of data custodians to protect the confidentiality, integrity and availability of the personal information they hold is becoming increasingly complex." This important claim is worth further consideration—as we know, the United States does not have a comprehensive federal cybersecurity protection policy. Instead, there have been dramatic changes with respect to state laws, all the way to federal agency oversight. The potential changes to future cybersecurity regulations and policies are as undetermined as they have ever been.

Prior to 2023, privacy professionals were guided by each individual state law concerning cybersecurity protections. States like Connecticut, for example, provide far more state protections than Ohio. However, the Securities and Exchange Commission (SEC) recently adopted a rule that requires publicly traded companies to disclose cybersecurity incidents within four days of identifying a material breach. This has positioned the SEC as a new regulator of cybersecurity, along with other governmental agencies on the forefront of cyber such as the Department of Homeland Security and its sub-department, the Cybersecurity and Infrastructure Security Agency.

As we have noted, the previous year saw increased state activity on the cybersecurity front. Following their federal counterparts, state agencies such as the New York Department of Financial Services introduced new data protection regulations for the organizations it oversees. Additionally, there was an overall increase in the number of individuals and government representatives suing for data breaches, state/federal wiretapping laws and biometrics laws. As it currently stands, cybersecurity protections for AI applications are lagging behind the public adoption of these programs; for this reason, regulators will look to adjust data privacy and cybersecurity laws as this technology advances.

Unsurprisingly, each of these trends suggests further changes in the coming years. It is possible that this means a national cybersecurity framework; however, past failures suggest that the United States is still far from any kind of federal adoption. Instead, individuals should continue to monitor the biggest events in cyber and stay connected to their congressional and state offices. We will make sure to continue updating this space with any new information on changes to cybersecurity laws.

3. The Effectiveness of the SEC's Cyber 8-K Rules (Privacy)

We are a little over six months into the enactment of the U.S. Securities and Exchange Commission's Form 8-K cybersecurity reporting rules, which means that now is a good time to review the effectiveness of these regulations. In this issue, we have discussed how these rules represent a new trend in cybersecurity that encourages the SEC to be a regulator of breaches. The Form 8-K reporting rules compel organizations to report material cybersecurity incidents within four business days. The goal of this reporting is to increase the transparency around cybersecurity attacks and the exposure of user data. If properly enacted, this rule should allow the public to be better protected and aware of when their information has been compromised.

According to the SEC, there are two key components to the new rules: first, companies must disclose "any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope and timing." This means each company must also explain what constitutes this material impact. Second, these companies must describe their processes "for assessing, identifying and managing material risks from cybersecurity threats." This tells us that the SEC is not only concerned with the reporting of cybercrimes but that they also recognize that many companies do not have processes in place for responding to attacks once they occur.

Since the enactment of the SEC's rules, several public-facing companies (e.g., Microsoft, Hewlett Packard, UnitedHealth Group, Prudential Financial, etc.) have made cybersecurity incident disclosures. The problem is that these disclosures have not followed the SEC guidelines: in fact, instead of focusing on the material, quantitative losses from attacks, these companies have instead offered qualitative losses. This is permissible because of what we observed with the first component: there are vagaries in the SEC's definition of reporting, which has allowed these companies to save face with their investors.

Broadly, the companies that have filed in this calendar year center around two types of industries—technology and financial services. As experts have written, these qualitative losses are a bit strange: "companies have made materiality determinations in the past on the basis of non-financial qualitative factors… but these situations are more the exception than the rule." Ultimately, for this process to be truly beneficial for consumers, the SEC will need to get much more specific about reporting requirements; otherwise, companies will continue to report the bare minimum.

4. Bumblebee Attacks Are Back (Crimeware)

One of the ways in which MyIDMatters attempts to keep you up to date on cybersecurity threats is by tracking crimeware attacks as they develop. For example, after months of dormancy, it looks like the malware loader, Bumblebee, is back on the scene. First identified in March 2022, Bumblebee executes payloads against users who unsuspectingly download the file. It is believed to have been developed by the TrickBot cybercrime syndicate, but after it disappeared from sight, it was thought to have possibly gone into retirement. Now the malware loader is back and more dangerous than ever.

As mentioned, traditionally Bumblebee has been used to download and execute follow-on payloads such as ransomware. However, once Microsoft started blocking macros in Office files that were downloaded by default, bad actors began modifying their attacks. This means that the new Bumblebee campaign differs significantly from previous campaigns, going so far as to attack targets with themed lures that contain links to OneDrive URLs. Right now, Bumblebee is being distributed via phishing email campaigns, which means that individuals need to be more alert than before. According to experts, these attacks are only growing in size and scope.

For these campaigns, the Word document-used macros create a script in the Windows temporary directory. Then a PowerShell command downloads and executes the next stage from a remote server, which begats yet another PowerShell command. This is what leads to in turn downloads and runs the Bumblebee DLL. Essentially, this means that the attack is several steps removed from the initial download; this is why it is so important to avoid downloading *any* files you are not expecting.

This resurgence is notable because it demonstrates how, even when cybercriminals are assumed to have been shut down, these attacks can be repurposed and reconfigured in new ways. Experts have noted that although the winter was a slower time for cyberattacks, 2024 has seen an increase in new and creative attacks meant to bypass traditional defenses. Despite their malfeasance, these bad actors are remarkably adaptable and willing to adjust at a moment's notice. This means that it is up to individuals to be as cautious and vigilant as ever when it comes to their security.

5. A New Federal Cybersecurity Strategy (Legal)

Even though the United States does not currently follow a federal framework for cybersecurity protections, the executive branch is completely stagnant in its efforts to protect U.S. citizens. And although legal penalties are realistically a decade away, the Biden administration recently held intense discussions with software developers. The goal? To craft frameworks that incentivize the private sector to manufacture and release software that lacks exploitable flaws.

Currently, consumers do not privilege or align their software purchases to developers prioritizing consumer privacy in software development. This is problematic as, currently, there is *no economic incentive* for eliminating exploitable flaws in software. Instead, vendors have evaded legal liability for customer damages by including language in their licenses/terms of services that eliminates the possibility of renumeration. In fact, in the case of Progress Software—whose product vulnerabilities led to more than 600 organizations being breached, compromising the privacy of 40 million people—the company has not faced any liability for customer losses. Rather, it has signaled that it intends to collect on a $15 million cyber-insurance policy without offering consumers a dime.

These discussions are not the first instance of the Biden administration taking a proactive step on cybersecurity. Software liability is, in fact, a major component of the administration's National Cyber Strategy. Released in 2023, the strategy outlines nearly 70 objectives meant to tackle critical issues that might otherwise be addressed by a federal cybersecurity framework. The importance of these discussions is that they signal the need to shift the cybersecurity burden away from consumers and onto the manufacturers who best understand these products.

Furthermore, the recent software discussions are not the only time software and cyber professionals have convened on the White House. A few months earlier, the White House held "A Legal Symposium on Software Liability," which saw academics and think tank experts considering the advantages of various legal approaches to software. The goal was to operationalize and enforce a standard of care and safe harbor for software developers who engage in strong cybersecurity practices. Additionally, members of the symposium also discussed ways of limiting the aforementioned liability disclaimers to better protect consumers. These recent efforts should hearten individual consumers, if for no other reason than they indicate that the executive branch takes their personal privacy seriously

6. Attacks on Financial Institutions (Crimeware)

Last year, Americans lost $12.5 billion to internet crime, which represented a near-25% increase from the year prior. As cybercrime grows increasingly sophisticated, financial institutions loom as targets ripe for attacks—and even more so as bad actors become more adept with AI attacks. There are several concerns facing banks and other financial institutions, including the worry that deepfake technology could allow these bad actors to impersonate employees or customers. Cybersecurity experts believe criminals will capitalize on the popularity of direct payment systems, leading to the exploitation of mobile banking Trojans. These are major concerns for our financial security.

Take, for example, mobile banking apps. As more and more consumers utilize these apps for their transactions, the more they open themselves up to the possibility of potential breaches. Although financial institutions have a robust understanding of how to protect physical assets, they are relative newcomers to the digital security scene. This can also be observed by the prevalence of deepfake technology in bank attacks. A few months ago, a Hong Kong company was defrauded of $26 million after bad actors produced a deepfake video in which the company's CFO ordered money transfers.

We have recently witnessed how the cybersecurity approaches of financial institutions have left consumers open to attacks. For example, a recent attack by a ransomware group called LockBit compromised the personal information of more than 57,000 Bank of America customers. Perhaps more alarming is the fact that the bank will likely be unable to determine what information was accessed. This attack occurred in a similar timeframe as when the Federal Reserve sent three notices to Citi Bank to change how it measures risks to cybersecurity. These six-month and 12-month deadlines came after Citi also failed Office of the Comptroller of the Currency exams.

What does this mean for consumers? After all, it is impractical (if not impossible) to suggest totally divesting from banks due to their cybersecurity practices. However, one step that consumers can take is to choose to bank with financial institutions that take their cybersecurity protections seriously. Because although many banks are implementing preventative measures (e.g., security audits, advanced firewalls, multi-factor authentication, etc.), this does not mean that every bank is investing in cybersecurity to the same degree. Choosing to bank with those institutions that can protect your digital assets is the pragmatically safe decision.

Quarterly Newsletter:

The TikTok Ban Is Finally Here

Well, that did not take very long, did it? After months (and years) of speculation and warnings, the United States government has finally made a move on TikTok. The popular social media application, which is owned by the Chinese parent company ByteDance, has faced intense scrutiny by US legislators in the past for fear that U.S. citizen data could be sold to a foreign adversary. Indeed, TikTok has been seen by many experts as a key security challenge facing the United States.

The new bill is aimed at protecting the data of more than 170 million Americans by forcing ByteDance to either divest itself from TikTok within nine months or face a ban from the U.S. market. Now, ByteDance has filed a suit against the United States, claiming that the ban infringes upon their 1st Amendment right to free speech. According to the suit: "For the first time in history, Congress has enacted a law that subjects a single, named speech platform to a permanent, nationwide ban." Of course, United States representatives argue that the ban has nothing to do with free speech and instead has everything to do with the national security threat posed by China.

Importantly, the language of divestment means that the U.S. can credibly claim that it is not attempting to place a ban on TikTok, per se, but rather that it is acting on the behalf of the nation's security interests. There are further concerns that ByteDance could censor TikTok to push favorable propaganda from foreign governments—running the equivalent of a psyop through the application. And although TikTok has spent $2 billion on measures to protect U.S. user data, this has not quelled concerns.

One issue that is worth monitoring is how this ban could actually *increase* privacy concerns after the app is removed from stores. Although it would no longer be available for download, TikTok's 170 million American users would still be able to use the app, albeit without any updates or security patches. This means that the app would eventually become entirely unusable; however, it means that in the meantime, TikTok would be more open to attacks. Fundamentally, nothing about TikTok has changed since the ban was signed by President Biden: this app is still a security risk, and users should delete their accounts. Instead, this ban is a public acknowledgement that the United States cannot wait for users to make that decision on their own.

Glossary:

5 Funny-Sounding Cybersecurity Terms You Need to Know

Rootkit

Just like in gardening, when a rootkit takes hold, it is exceptionally difficult to remove. Rootkits are collections of programs that allow bad actors to access and control your network from a distance. This means that, while they do not damage users by themselves, they open the door for cybercriminals to introduce malware and viruses into your system.

Hacker – White Hat

It takes a thief to catch a thief. Often talented cybercriminals themselves, white-hat hackers are hired by IT services and companies to test systems for vulnerabilities. That way, security can be strengthened and enhanced prior to an attack. These friendly agents are occasionally called "ethical hackers" because their cyber activity is limited to legally permissible actions.

Spoofing

This goofy term references a not-so-amusing attack. When hackers engage in spoofing, it means they change their email's IP address so that it appears to come from someone you know. This could either be a contact in your address book or a larger organization from which you regularly receive communications. The goal here is to stay vigilant and not fall for the fake-out!

Hacker – Black Hat

These are the bad actors who wear the proverbial black hat, which means they are the criminals that your cyber defenses are actively working against. Working with larger cybercriminal organizations or by themselves, black-hat hackers release malware onto your system that is designed to destroy files, hold computers hostage or steal passwords and other personal information.

Penetration Test

These tests are one of many methods a white-hat hacker might use to test your system for vulnerabilities. One important note, however, is that these advanced security evaluations are also utilized by an organization’s security professionals. The goal of a penetration test differs by the organization, but good outcomes usually involve a more comprehensive understanding of the weakness of a defense system.