Adarian Henderson, Jalen Oakley, Quinten Williams
Professor Dennis Harvey

RMI 413

4/12/2023

Emerging Issues: Data Breaches and Security

Since its beginning in the early 1980's the Internet and devices connected to the Internet of things (IoT) have undergone immense changes. The internet has revolutionized not only communication but has also allowed enterprises to grow. Fast forward to 2023, and life without the internet seems almost unthinkable. The internet is something that people around the world use daily to help enhance their lives, whether it's for education, work, shopping, or communicating with friends and family. IoT devices have also helped automate many of life's tedious tasks. With all these great advancements the internet and IoT devices have brought, bad actors have found ways to manipulate the internet and cause catastrophic loss. One of the biggest concerns of the internet for both individuals and companies is data loss through data breaches. As the internet advances, society faces an emerging issue of data breaches and security.

The world is starting to shift rapidly toward a fully digitalized society. The global COVID-19 virus helped show that everyday functions, such as going to work or school can be continued via internet access at home. For many people, the leisure of working at home was great. Employees got to spend more time with family while not having to commute or encounter any more awkward interactions with co-workers. The peace of working at home for employees provided additional stress to the organization's Chief Information Security Officers (CISOs). Home networks often lack the essential security features, such as top-of-the-line firewalls found in offices and school environments. The lack of security features in combination with the additional access points to an enterprise's network essentially opened hundreds, if not thousands

of new doors to bad actors looking to steal, exploit information, and commit other crimes over the internet (cybercrimes).

According to the National Institute of Standards and Technology (NIST), a data breach is "An incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information may include credit card numbers, personal health information, customer data, company trade secrets, or matters of national security" (NIST). The general idea of a data breach is not new. Bad actors such as nation-states have always had spies trying to steal other nations secrets. Companies have also tried to get the "upper hand" on the competition by stealing intellectual property. In a highly digitized world, these types of heists have shifted to being committed over networks. Threats such as elite military hacking groups from nation-states such as Russia and Iran, hacktivist groups such as *Anonymous*, and poorly skilled "script kiddies" all threaten the vital networks that help store and protect customer data.

In December of 2022, a Russian hacking group was caught targeting Global Ordinance, a U.S. military weapons and hardware supplier. This group is called TAG-53 but is broadly known in the cybersecurity community as Blue Callisto. According to historical public records, TAG-53 breaches systems and gains access via phishing. It is said that the group conducted these phishing attacks through email and used 38 different domains with 9 of them even containing references from companies like UMO Poland, Sangrail LTD, DTGruelle, Blue Sky Network, the Commission for International Justice and Accountability (CIJA), and the Russian Ministry of Internal Affairs (Lakshmanan). They use these domains to appeal to masquerade as genuine and authentic parties as well as to appeal to a certain audience as these domains are associated with social engineering. The group is known for using the same strategy repeatedly and this strategy is

spear-phishing. They communicate with people through email and build a relationship and a sense of trust. After a few emails have been exchanged, and this has been accomplished they then attach a decoy PDF containing a fraudulent link to avoid detection and then that is when the payload is released.

Crimes committed over the internet or cybercrimes are not only nation-state groups attacking foreign military projects. Rampant cybercriminals from all around the world are also targeting individuals and their sensitive data. Most people are unaware of the vast amount of data they create or volunteer to give up. Popular apps and websites such as Facebook, Amazon, financial institutions, and healthcare websites collect vast amounts of personal data such as emails, phone numbers, locations, credit card numbers, banking information, and sometimes even social security numbers. Customers see it as just "another cost" to using these apps; but to hackers, sensitive personal information is extremely valuable. Being able to break into the data centers of large social media companies, financial intuitions, and healthcare providers is difficult. However, with the correct tools, skills, and patience hackers can cause data breaches that can cost people money and terror. In 2018, roughly 23% of American households experienced some sort of cybercrime incident, such as a security breach or data loss targeting personal information, credit card, and bank information, which was higher than the rate of reported street crime. (Reinhart). What is scary is that the number of cybercrimes is expected to increase as society becomes more dependent on the internet (Jardine).

One of the largest healthcare sector data breaches in recent years was a data breach that targeted Anthem Blue Cross Blue Shield. In 2015, Anthem announced that 79 million policyholders across the United States had personal information stolen in a data breach. Victims' data that was stolen consisted of social security numbers (SSNs), medical identification numbers,

addresses, dates of birth, email addresses, and employment information (HHS). Cyberattackers were able to penetrate Anthem's systems through an advanced persistent threat attack (APT), a stealthy and continuous form of attack, and through a series of spear phishing emails. Individuals' data was stolen for nearly a month before IT professionals discovered that there was a breach (HHS). Many officials believe that the Anthem attack was the largest data breach involving healthcare reported to date while also crediting much of the blame on Anthem. The Office of Civil Rights Director Roger Severino stated

> "Anthem failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information…We know that large healthcare entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion" (HHS)

Corporations need to be able to protect customers' data in both efficient and effective manners. If not, breaches will cost individuals added stress and corporations millions of dollars in loss. Data, especially personally identifiable information (PII) and personal health information (PHI) are extremely valuable on the darknet. In 2020, Anthem agreed to pay $16 million in a settlement for the damages caused by the attack and violation of the Health Insurance Portability and Accountability Act (HIPAA) (HHS). As individuals and large organizations rely heavily on electronic data storage, they must ensure the data is safe and secure because if not, there will be extreme loss and consequences.

With millions of people's sensitive information susceptible to cybercrime, this leaves a large burden of liability to companies that are responsible for keeping this information secure, and the current demand for cyber insurance is greater than ever. The global cyber insurance

market size was valued at USD 4.3 billion in 2018 and is expected to register a CAGR of 25.6% over the forecast period (GVR). With so much potential market value for this sector of insurance companies, there is a growing demand for risk advisors who are affluent in cyber security to be able to advise their clients on guidelines and procedures to follow to best avoid a claim. For instance, companies could apply stronger backups and encryption capabilities to strengthen security. The trouble that insurance companies are starting to notice is that smaller businesses that can't afford cyber coverage are being targeted more often, and with the average ransomware claim costing over $500,000. This type of claim can be devastating to the insured and their reputation as a company. Even with safe cyber practices in place, there can never be 100% certainty that a firm is safe from ransomware and other cyber attacks. While cybercrime is becoming more common, only a lesser majority of firms carry cyber insurance.

Data breaches have been an emerging issue and will continue to be so as time advances. While it is known to be an issue, it is also often depicted as an attack, which it often is but it is not rare for it to be due to a bug or vulnerability. Recently, OpenAI suffered an outage and data breach. OpenAI is better known for its AI chatbot, ChatGPT, and on March 20th of 2023, there was an outage and data breach due to an open-source library bug in OpenAIs database client Redis (Jewett). ChatGPT is a popular tool that can perform tasks such as writing papers, answering questions, as well as have a conversation with an individual through chat. It has become extremely popular amongst individuals that are involved in anything academic, in other words, people that may be in high school or college. With the emphasis on its popularity, one could assume that the amount of users is extremely high and when there are a lot of users this means a lot of data. The breach occurred during an outage and exposed payment-related and other personal information of the people subscribed to ChatGPT Plus, ChatGPTs paid version.

For nine hours, it was possible for some users to see other active users' personal information like first and last names, email addresses, or payment addresses, and the last four digits of card numbers as well as the expiration dates. Luckily, only about 1.2 percent of ChatGPT Plus users were affected (Nicastro). OpenAI acted promptly and swiftly on the bug and resolved the issue by patching the bug. Actions taken to patch the bug consisted of extensively testing the fix of the underlying bug, adding redundant checks to ensure that the data returned by its Redis cache matches the requesting user, and examining its logs to make sure that the messages that users see are the ones they are supposed to see, correlated several data sources, improving logging, as well as improving the robustness and scale of its Redis cluster (OpenAI). The importance of this comes with the fact that no matter how data breaches happen, whether it's due to a bug or an attack, it is something that we must do whatever to prevent although it isn't 100 percent guaranteed.

As the world rapidly expands into a more digital environment, the risk of cybercrime-related incidents, such as data breaches and ransomware will expand. In the coming years, it will be critical that organizations, businesses, financial institutions, and educational institutions maintain and follow proper security measures, while also potentially looking into cyber insurance policies to protect sensitive data. The Internet and IoT devices give bad actors around the world access to negatively affecting and destabilizing the United States and United States citizens. It is important for companies and individuals to protect their data at all costs, because as the internet and IoT grow, so will the number of bad actors attempting to steal sensitive data.