A Look Back at the Year in Data Security – and Predictions for 2022

Insights
12.28.21

As 2021 comes to a close, this article recounts some of the biggest trends in data privacy and cybersecurity from the past year and looks ahead at what we anticipate will come to workplaces in 2022. Employers across the nation need to review what happened this past year when it comes to ransomware attacks, consumer privacy legislation, biometric privacy, and the Biden administration's cybersecurity efforts – and need to prepare for the year to come.

Ransomware Attacks: 2021 Wrap-Up

What do national and state governments, meat processors, wind turbine producers, and schools have in common? They were all the targets of ransomware attacks in 2021. Ransomware attackers use a form of malware that encrypts a company's files, locking the company out and rendering the data unusable. Attacks may include the exfiltration of data that attackers then threaten to sell or leak if a ransom is not paid. These nefarious actors typically seek payment in cryptocurrencies, such as Bitcoin, making payments more difficult to track and enhancing anonymity. If the demand is not paid, the attackers often threaten to sell, leak, and/or refuse to return exfiltrated data or authentication information.

The Department of Homeland Security reports that ransomware attacks increased 300% from 2019 to 2020, and other studies have reported an even larger increase. 2021 was no exception, as major companies and governments faced ransomware attacks throughout the year. The increase in remote work due to the pandemic has led to an increased vulnerability to these sorts of attacks. As remote work arrangements seem likely to persist beyond the end of the pandemic, you need to make sure that your employees are trained to spot and avoid phishing attacks. You also need to review security protocols on a regular basis to prepare for evolving and increasingly sophisticated ransomware attacks in the future.

Ransomware Attacks: 2022 Predictions

Over the next five years, acting National Security Agency Director Paul Nakasone expects the frequency of ransomware attacks to remain at least constant, if not increase. He believes that at least one business or organization in the United States will face a ransomware attack "every single day" down the road.

In 2022, it is likely that this trend will continue, with ransomware groups likely to use even more sophisticated technology to hold employer's data hostage and attempt to extract large payments through threats of disclosure of sensitive data and information. You will need to remain diligent in preparing for attacks and have a plan in place to respond if one occurs.

Consumer Privacy Laws: 2021 Wrap-Up

This past year saw a proliferation of proposed privacy legislation at the state level, largely mirroring California's CCPA. Two more states, Virginia and Colorado, passed their own consumer privacy laws that will take effect in 2023. These bills provide consumers with certain rights regarding their data, such as a right to opt out of the processing of their personal data for uses such as targeted advertising or sales, a right to access their data, a right to correct it, a right to have it deleted, and others. These laws do not, however, currently provide for a private right of action (with an exception for data breaches under the CCPA).

Beyond Virginia and Colorado, at least 25 other states have had data privacy bills introduced in their legislatures in the last year. While not all of these bills were successful, it is telling that they are beginning to appear in legislative chambers across the country.

Consumer Privacy Laws: 2022 Predictions

In 2022, you should expect more states to enact their own consumer privacy laws, as well as a potential federal law on the subject. There has been an increased interest of late regarding such laws, and several high-profile members of Congress have called for bipartisan action to protect consumer data. Even before these calls for action, several data privacy laws were introduced in the Senate, with one being backed by Senators from both parties. There is debate over whether a federal bill would preempt states from providing further protection, which will be an issue to look out for when and if these bills progress through the legislative process. There is also no consensus on whether such a law should include a private right of action.

Further pressure is coming from the European Union, whose Justice Commissioner has stated that the United States passing federal privacy legislation would be an "important element" in moving forward on restoring a European-US data transfer agreement. This would once again allow for transatlantic data flows between the US and EU. Given these statements, you can expect a federal bill to gain traction in 2022.

Biometric Privacy Legislation: 2021 Wrap-Up

This past year also saw numerous states enact biometric privacy legislation. Illinois was the first state to enact its version of this legislation in the Biometric Information Privacy Act (BIPA) in 2008. The BIPA regulates the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information. Some examples of biometric information include fingerprints, iris scans, and voiceprints. Following in Illinois' footsteps, four other states enacted

legislation modeled on BIPA: Arkansas, California, Texas, and Washington. Additionally, 27 other states had some version of BIPA legislation pending as of this past summer.

Also, New York City's biometric data protection law took effect on July 9, 2021. This law requires businesses that collect biometric information – such as facial recognition and fingerprints – to conspicuously post notices and signs to customers at their doors explaining how their data will be collected. The law applies to a wide range of businesses including retailers, restaurants, bars, theaters, and gyms, for example. The law bans businesses from selling, sharing, or otherwise profiting from the biometric information that they collect.

Biometric Privacy Legislation: 2022 Predictions

With the BIPA influencing other states to enact similar legislation, there is the potential for federal legislation on biometric privacy issues. The National Biometric Information Privacy Act of 2020 (NBIPA) has been pending in the Senate ever since it was introduced more than 15 months ago. Like BIPA and other laws modeled after it, NBIPA is aimed at regulating the biometric data practices of private entities. It provides a private right of action for violations, and it expressly states that a violation of its provisions "constitutes an injury-in-fact and a harm to any affected individuals." This would effectively nullify the standing issues that have plagued litigants in BIPA class action lawsuits. As the NBIPA would be enacted at the federal level, it would most likely preempt any state laws that cover the biometric privacy field.

President Biden's Cybersecurity efforts: 2021 Wrap-Up

President Biden signed into law a historic $1 trillion infrastructure bill on November 15, the Infrastructure Investment and Jobs Act. Included in this package is nearly $2 billion for cybersecurity and related provisions. In an era where there are more bridges being created on the internet via mechanisms like the blockchain, it is encouraging to see a recognition that cybersecurity remains a main focus. Indeed, the White House said this plan is one "that will make our communities safer and our infrastructure more resilient to the impacts of climate change and cyber-attacks."

One key element of the cybersecurity funding is a Federal Emergency Management Agency cyber grant program that would distribute $1 billion over four years to state and local governments. These grants will be administered through the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Another $21 million will go to the Office of the National Cyber Director, which has not been able to hire critical positions due to funding shortages. The law also holds back $100 million over four years for when the Department of Homeland Security (DHS) declares a "significant incident" that would allow CISA to provide aid to the public and private sectors. The DHS will also receive nearly $158 million for research in cybersecurity and related areas and CISA will get $35 million for sector risk management work.

Within the Energy Department, the infrastructure bill establishes two $250 million programs which are aimed at: (1) rural and municipal utility security; and (2) grid security research and development. Where the legislation does not provide additional funding, it makes it an option to use existing grants on cybersecurity. For example, there are Department of Transportation grant programs for highway projects that would allow the states to deploy some of these funds to help cybersecurity efforts.

President Biden's Cybersecurity efforts: 2022 Predictions

The historic $1 trillion infrastructure bill goes a long way toward ensuring that the U.S. modernizes and fortifies its existing cybersecurity infrastructure. The investment of $2 billion in reserves intended for cybersecurity improvements is indicative of is the federal government's dedication to fortifying U.S. defenses against future cyberattacks. You can expect to see an increased focus from the Biden administration throughout 2022 on staying ahead of the constant threats posed by increasingly frequent and ever-more sophisticated cyber-attacks.

Conclusion

As the line between work and home continues to blur while the technologies used in the workforce become more sophisticated and expensive, it is crucial that employers stay on top of emerging trends in data privacy and cybersecurity.

Fisher Phillips will continue to monitor further developments in these areas, so be sure to subscribe to Fisher Phillips' Insight system to stay up-to-date. If you have any questions regarding how cybersecurity threats or data privacy laws could impact your organization, please consult your Fisher Phillips attorney, the authors of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group or our Cryptocurrency and Blockchain Taskforce.

Service Focus

Consumer Privacy Team

Privacy and Cyber