SHARE:

Join Our Email List

View as Webpage

December 16, 2021

Welcome

Welcome to our last *Decoded* issue of 2021. With this last publication, we wanted to do something a little different. We looked at the top issues that affected the industry and our clients over the past year. And, we look ahead to 2022 and the issues that we believe will have great impacts.

As such, each of us took a deep dive into several issues and hopefully provide some clarity and actionable steps to move forward. If you have any questions about these topics and feel counsel could be helpful, please contact us. We look forward to helping all of you throughout the rest of 2021 and into the new year.

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*

---

10 Things to Do Before and After Business E-mail Compromises Happen

By Nicholas P. Mooney II

One of the most common forms of data or security breaches is the compromise of a business e-mail account that allows a threat actor to obtain financial or other sensitive information. Security professionals report that business e-mail compromises account for more than half of all data security incidents, and the FBI calls it "one of the most financially damaging online crimes." Commentators predict that these types of breaches will continue to grow, based partly on the number of employees working from home, the general increase in cryptocurrency usage, and the implementation of artificial intelligence and deep fakes. With the likelihood that these breaches will increase in the coming years, companies should take action now.

Despite the fact that these breaches may be nearly inevitable, there are things you can do to protect yourself and your company and to make it easier to deal with, and recover from, one of these breaches.

Click **here** to read the entire article.

Ransomware: Where We are and What is to Come

By Alyssa M. Zottola

The technological era has wrought numerous changes in traditional crimes that have plagued society from time immemorial. Ransom attacks have long been recognized by criminals as a method of extracting money from a desperate victim. With the rise of ransomware attacks, criminals can hold healthcare institutions, businesses, or individuals hostage with a single virus. Ransomware attacks are becoming an ever-increasing threat to today's economy. The first half of 2021 saw an increase of 151 percent in global ransomware threats compared to the first half of 2020.

This increase in ransomware attacks is unlikely to dissipate in 2022. In fact, industry experts predict that 2022 also will see an increase in "triple extortion ransomware." In a triple extortion ransomware attack, a business is hit with the initial ransomware attack, totally incapacitating the business. The business's partner is now faced with the extortionary threat of either paying the business's ransom or losing the supplier to incapacity as the business seeks to regain control of its systems. These attacks have the potential to cripple industries.

Click **here** to read the entire article.

What was Fascinating in 2021 for Biotech

By Hugh B. Wellons

2021 was a fascinating year in biotech, especially for legal issues. Of course, 2021, as the second year of a global pandemic, must be viewed in context with 2020.

Hugh Wellons takes a look at the top issues he found interesting and where we go from here.

Click **here** for the full article.

Paying and Playing in the Digital Realm: Cryptocurrencies, Contactless Payments, and Virtual Worlds

By Nicholas P. Mooney II

Next year will see the continued growth of digital or virtual currencies, payment options, investments, and real estate.

Digital currencies have been around in some form for more than a couple decades. Many consider e-gold, which was introduced in the mid-1990s, to be the first form of electronic money. In the mid-2000s, M-PESA was launched, creating a way for unbanked people in Kenya to digitally transfer money throughout the country. It spread beyond Kenya and is still in use today.

Click **here** to read the entire article.

Reliance on Multiple Cloud Infrastructure Services will Become More Popular Next Year Due to Recent High-Profile Cloud Computing Failures

By Alyssa M. Zottola

Businesses are increasingly relying upon the cloud computing infrastructure for hosting their websites, storing their data, and deploying artificial intelligence. Using a cloud computing service saves businesses the costs associated with purchasing and maintaining their own IT infrastructure, allowing them instead to purchase the services and storage that they need. Amazon, like with many other aspects of the economy, dominates the cloud computing services industry, controlling 33 percent of the world's cloud infrastructure, while Microsoft controls only 20 percent of the market and Google controls a mere 10 percent of the market.

Click **here** to read the entire article.
