Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

February 21, 2019

CYBERSECURITY

Hack of Email Provider Destroys Servers and Two Decades of Data

We predicted last year that hackers would become more malicious in the future, not only stealing and selling data for nefarious purposes, but actually destroying data and even systems. That reality hit email provider VFEmail last week, and on February 12, founder Rick Romero tweeted "Yes, @VFEmail is effectively gone. It will likely not return. I never thought anyone would care about my labor of love so much that they would want to completely and thoroughly destroy it." The tweet went out after he watched the intruder reformat the hard drives of his email service, which has been in existence since 2001. The intrusion wiped out two decades of data. This is a tragic story. *Read more*

CISA's Failure May Come to Haunt the Technology Industry

The Cybersecurity Information Sharing Act of 2015 (CISA) was intended to incentivize private entities to share threat intelligence information with the federal government (specifically the Department of Homeland Security), allowing all parties to react more quickly and efficiently to cyber threats. The vision was that thousands of companies would sign on, creating a powerful network that could form a joint defense in real time against emerging cyber threats. The dream is not going well. At last count, there were six non-federal entities signed up with DHS. The reasons for this failure are both technical (DHS has allegedly done a terrible job of contextualizing threat data to make it actionable) and non-technical (privacy is increasingly a business consideration, and working with the government creates bad optics). *Read more*

DATA BREACH

Is Bad Cyber Insurance Coverage Actually Good for Consumers?

The cyber insurance market continues to evolve, and major questions remain unanswered. Should policies cover regulatory fines? Should first- and third-party claims be addressed in separate policies? The list goes on. *Read more*

ENFORCEMENT + LITIGATION

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Data Privacy
Drones
Enforcement + Litigation
New + Now
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Fortnite Players Sue for Alleged Exposure of Payment Information for Vbucks

Players of the popular video game Fortnite have filed a proposed class action suit against the video game's owner, Epic Games Inc. (Epic), alleging that Epic failed to protect players' accounts, allowing hackers access to their payment details in a 2018 data breach. According to the suit, the players gave Epic their payment information in order to purchase "Vbucks," which is the digital currency used while playing Fortnite. The suit alleges that Vbucks were stolen and that the hackers were also able to access players' Fortnite accounts. *Read more*

DATA PRIVACY

Data Mining Shaping the Global Political Climate

The 2016 U.S. Presidential election demonstrated the importance of digital campaigning. President Trump's campaign was vastly outspent by Hillary Clinton's campaign, and placed little emphasis on traditional ground-game tactics. Instead, Trump focused his campaign on digital strategies to target "persuadable voters" via social media. The outcome of the election demonstrated the efficacy of this strategy; not only did Clinton lose the election, but she became the first general election candidate in nearly 40 years to lose after outspending their opponent. *Read more*

Behavioral Biometrics: Constructing the Digital You

During WWII, Morse Code was an indispensable asset that allowed the Allied powers to transmit sensitive information over long distances with great accuracy. However, it contained an obvious, and potentially fatal, flaw — it provided no built in mechanism for identifying the sender of the messages. In order to combat this, U.S. intelligence officers implemented a methodology known as the "Fist of the Sender," an early system of "behavioral biometrics" that verified the sender's identity by analyzing subtle, non-replicable and idiosyncratic "typing" patterns of individual users. *Read more*

NEW + NOW

HIPAA Data Breach Reports Due to OCR by 2/28/19

The HIPAA (Health Insurance Portability and Accountability Act) breach notification regulations require covered entities to self-report the unauthorized access, use or disclosure of unprotected protected health information (PHI) to the Office for Civil Rights (OCR).

If the data breach involves more than 500 individuals, the notification must be made to the OCR immediately. If the breach involves fewer than 500 individuals, the covered entity must notify the OCR before 60 days after the end of the calendar year (or February 28). *Read more*

DRONES

NASA Selects Hosts for Final Drone Technical Testing

This week, NASA selected the Nevada Institute for Autonomous Systems in Las Vegas and the Lone Star UAS Center for Excellence and Innovation in Corpus Christi, Texas to host the final phase of its four-year series of unmanned aircraft systems (UAS) technical demonstrations. Both of these organizations will host demonstrations to confirm whether NASA's UAS Traffic Management (UTM) system functions safely and effectively in urban areas. *Read more*

PRIVACY TIP #178

Check and Set (and check and re-check) Your Privacy Settings

The tip this week is to continue to check and set your privacy settings—microphone, location services, camera, photos, Bluetooth sharing, contacts, health, motion, and fitness. *Read more*