Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Cybercriminals Recruiting Employees on the Dark Web to Assist with Fraud Schemes

Darkreading.com has issued a survey entitled *Monetizing the Insider: The Growing Symbiosis of Insiders and the Dark Web,* which states that malicious insiders are responsible for 27 percent of all cybercrime. This statistic confirms that cybercriminals are increasingly recruiting insiders by using the dark web as a recruiting tool. So not only do businesses have to worry about employees who make honest mistakes and cause security incidents, or disgruntled employees who steal company information, but they now have to worry about malicious insiders who are being recruited by criminals on the dark web. *Read more*

DATA BREACH

Marriott Announces Massive Data Breach—Illustrates the Importance of Cybersecurity in M & A Due Diligence

Last Friday, Marriott International announced a major data breach, perhaps one of the largest in history. This breach illustrates the often made point that breaches and intrusions happen and can go unnoticed for months or years. Marriott's breach involved an unauthorized party that copied and encrypted information in the Starwood reservations database back in 2014. When Marriott acquired Starwood in 2016, the breach went undetected as that merger went forward, only to be discovered in 2018. This situation should be a red flag for anyone involved in mergers and acquisitions signaling that cybersecurity should be a top priority in the due diligence process. *Read more*

Multiple Lawsuits filed Against Marriott After Data Breach – "One of the Largest Digital Infestations in History"

Calling the Marriott data breach "one of the largest digital infestations in history," a putative class action was filed in Oregon this week seeking up to $12.5 billion dollars in relief. It should come as no

December 6, 2018

FEATURED AUTHORS:

Linn Foster Freedman
Deborah A. George
Kathleen M. Porter
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Data Privacy
Drones
New + Now
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

surprise that soon after Marriott announced its massive data breach potentially affecting 500 million customers in the Starwood reservations database, several putative class actions were filed around the country and at least one in Canada. Lawsuits were also filed in Maryland and New York. *Read more*

DATA PRIVACY

Recruiting Scams on the Rise

With more companies hiring, online recruiting scams have re-emerged to prey on job seekers and employers. The Better Business Bureau tracked more than 3,000 recruiting scams in the first 10 months of 2018 with losses in the millions of dollars. The online recruiting scam works this way: the scammer fraudulently uses a company's name and logo, and perhaps the names of the company's employees handling recruiting or human resources, to solicit applications from job seekers for fake jobs. Many times the companies are long established, household names, which gives the scam an air of legitimacy. Sometimes the solicitation comes by email, but most often it is posted on a professional or recruiting website or social media platform. Like most phishing schemes, the scammer's email address is similar to, but not the same as, the legitimate company's email address. *Read more*

NEW + NOW

Use of Multifactor Authentication

This has been quite the year of O365 intrusions. The story seems to be almost identical in each security incident we investigate. It goes like this: An employee receives a pop-up message from Microsoft advising employee that s/he must change his or her password for security purposes. The employee then types his or her user name and password into the pop-up message and provides "Microsoft" with the new information.

In fact, an intruder has penetrated the employee's email box with a phishing email that has just compromised the employee's email box. Once the intruder is in the email box, he places forwarding rules on every email the employee receives to a gmail account, and then watches the email traffic. *Read more*

DRONES

New Drone System Tested Without Use of GPS

The National Aeronautics and Space Administration's (NASA) Langley Research Centers has taken on the challenge of using drones in GPS-deprived environments. Recently it gathered a group of students from the Massachusetts Institute of Technology (MIT) to help find a solution for that problem. Those students came back to NASA with a plan for a fleet of drones that can autonomously fly through a thickly vegetated forest, communicate with one another, and create a 3-D map of the environment without hitting a tree or using any GPS. How? The drones have onboard laser-range finders for positioning and planning their routes as they pilot themselves. The technique is called Simultaneous Localization and Mapping (SLAM), which creates algorithms to guide the drones and map efficiently while also avoiding re-mapping already covered area. The data is sent back via WiFi to a base station where all the drones' maps are stitched together into one comprehensive map. *Read more*

NYPD to Add Fleet of Crime-Fighting Drones

This week, the New York Police Department (NYPD) announced that it will be adding a fleet of crime-fighting drones to its ranks. The NYPD plans to roll out 14 drones as part of its technology "evolution." Police Commissioner James O'Neill said, "As the largest municipal police department in the United States, the NYPD must always be willing to leverage the benefits of new and always-improving technology." The hope is that these drones will enable the NYPD's trained police officers to be even more responsive, effective and efficient. A NYPD spokesperson said the drones will not be used for everyday police patrol, unlawful surveillance, or to enforce traffic laws. Additionally, these drones will not be used as weapons or equipped with any weapons. *Read more*

PRIVACY TIP #168

USPS Security Vulnerability Affects More Than 60 Million

This week's privacy tip, builds on privacy tip #164 and addresses some additional risks around the United State Postal Service's (USPS) "Informed Visibility" service. *Read more*