Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

U.S. Estimates that Cyber Hacks Cost Up to $109 Billion in 2016

The Council for Economic Advisors (CEA) issued a report this month, entitled "The Cost of Malicious Cyber Activity to the U.S. Economy," which concludes that "malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016." *Read more*

DOJ Forms Cyber-Digital Task Force

The Department of Justice (DOJ) has announced it is forming a Cyber-Digital Task Force which will combat global cyber threats.

The Task Force will concentrate on gathering the methods the DOJ uses to fight cyber threats and figuring out ways law enforcement can combat the problem, starting with what efforts are being used to combat election interference, the use of the internet to spread violent ideologies, theft of private information, and attacks on computers to attack U.S. citizens.

The Task Force is to provide a report to Attorney General Jeff Sessions by June 2018.

SEC Updates Guidance on Public Companies' Disclosure of Cyber-Attacks

The U.S. Securities and Exchange Commission (SEC) updated its guidance to public companies this week on how and when they are to disclose cybersecurity risks and breaches. The SEC suggests that public companies should disclose potential weaknesses that have not been targeted by hackers. *Read more*

HaoBao Malware Hitting Banks Scans for Bitcoin Activity

Lazarus, the well-known hacking group responsible for the WannaCry ransomware attack from last year, as well as the attacks on the Bangladesh Central Bank and Sony, is now targeting global financial firms and Bitcoin adopters with a phishing campaign dubbed

February 22, 2018

FEATURED AUTHORS:

Kathleen E. Dion
Conor O. Duffy
Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

"HaoBao."

The phishing campaign was discovered by McAfee Labs in mid-January. The way it works is that Lazarus distributes a Dropbox link in an email that looks like a job advertisement for executive level bank jobs. When the user opens the link, malware is implanted into the user's system. *Read more*

DATA BREACH

EDUCAUSE Challenges the U.S. DOE's Guidance on Data Breach Reporting

On January 30, 2018, EDUCAUSE, a higher education technology association, submitted a letter to the U.S. Department of Education describing concerns that it has with the Federal Student Aid's (FSA) ability to protect federal student financial aid data. EDUCAUSE's members include IT professionals from over 1,800 colleges and universities as well as other organizations. *Read more*

ENFORCEMENT + LITIGATION

Dumpster Diving Leads to $100,000 Fine for Defunct Business Associate Due to Improper Disposition of Medical Records

On February 13, 2018, the HHS Office for Civil Rights (OCR) announced a $100,000 settlement with a court-appointed receiver representing Filefax, Inc. (Filefax) arising from the 2015 discovery of medical records that contained protected health information (PHI) of over two thousand individuals in a dumpster. Filefax, a now-defunct medical records moving and storage company located in Illinois, acted as a business associate under HIPAA. *Read more*

TOPS Software Company Hit with TCPA Class Action

Last week, TOPS Software LLC (TOPS), a software company that specializes in condominium and homeowners association communication platforms, was served with a class action lawsuit in Illinois federal court which alleges that TOPS violated the Telephone Consumer Protection Act (TCPA) by using autodial technology to solicit consumers to attend the "CAMfire Conference." The CAMfire Conference is a community association of management professionals, thought leaders, and TOPS software users. Lead plaintiff, Scott Dolemba, claims in his two-count complaint that he and the other class members suffered damages when they received autodialed calls from TOPS and demands that the court issue an injunction to stop them from making unsolicited telemarketing calls in the future. *Read more*

DRONES

Charleston Helicopter Crash: Possibly First Aviation Accident Caused by a Drone

Federal investigators are investigating a helicopter crash occurred on Daniel Island (near Charleston, South Carolina) that may have been caused by a drone. The helicopter pilot reported to investigators that he crashed after trying to avoid a drone that came into his flight path. The helicopter was flying in this area for a flight lesson, and when the drone appeared in the helicopter's path, the flight instructor pilot had to make a hard turn about 50 feet above the tree line, nicking brush or a small tree. The helicopter then lost control and fell to its side. No one was hurt in this crash. *Read more*

Close Calls with Drones Increasing Dramatically

Aviation regulators, the Federal Aviation Administration (FAA) in the United States, and the Transportation Safety Board of Canada, have been investigating a flurry of close calls between consumer drones and manned aircrafts, which poses a significant risk to the flying public and the public down below. *Read more*

Texas Dept. of Public Safety Launches Drone Program

The Texas Department of Public Safety (DPS) has launched a new unmanned aircraft systems (UAS or drones) program for public safety purposes. The DPS plans to use its 17 drones for a variety of public safety purposes across the state, including officer safety, search and rescue, disaster support, aerial observation support, crash reconstruction, crime scene photography, and communication tower inspection. *Read more*

PRIVACY TIP #127

Emails Continue to Pose High Risk to Companies

According to a Proofpoint study that analyzed 160 billion emails delivered to 2,400 global companies at the end of 2017, 88.8 percent of organizations were targeted by at least one email phishing attack over the past year. This is an increase over its 2016 report conclusion of 75 percent.

In addition, more identities were spoofed in 2017, and almost 50 percent of organizations had more than five spoofed email identities. This is when fraudsters leverage spoofed emails to impersonate individuals within an organization to trick their victims. Proofpoint found that the spoofed emails concentrated on job titles related to finance and/or accounting.

Proofpoint found that social media-themed email phishing attacks were highly successful, and spoofed LinkedIn notifications were the most convincing. Fake LinkedIn emails actually fooled 53 percent of test subjects.

Surprisingly, a PDF is the most common file type used in cyber-attacks, according to a report by Barracuda Networks, which found that 41 million malicious PDFs were sent by email over a three month period.

The message is clear: emails continue to pose a high risk to companies, and employees must be knowledgeable about the fact that they are being attacked every day and are a high risk to their employer.