Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Intel Bug Affects Millions of Devices

Intel has confirmed it has a bug in its remote server management tool. The tool, known as Management Engine, permits administrators of IT systems to access devices remotely to apply updates or troubleshoot problems for users. The bug allows unverified code to be run on Intel chipsets, so the intruder can gain control of devices. The Management Engine bug affects most Intel chips, which are embedded in most servers, personal computers, and IoT devices. Meaning millions of devices may be vulnerable. *Read more*

Connecticut Cyber Task Force Announced

The U.S. Attorney's Office of the District of Connecticut has announced the creation of a Connecticut Cyber Task Force (CCTF) in partnership with the FBI, the DEA, the Secret Service, Homeland Security, the IRS, Connecticut State Police, and 11 local police departments throughout Connecticut as well as other federal authorities. The CCTF's initial focus will be twofold: (1) to "target criminal activity on the dark web, notably the illicit acquisition and distribution of fentanyl and other dangerous drugs that are the cause of tens of thousands of overdose deaths annually" and (2) "to identify and disrupt criminal organizations that use computer intrusions to defraud companies of their money and information." *Read more*

VIRTUAL CURRENCY

Hacker Steals $31 Million of Tether Cryptocurrency

Virtual currency exchanges are popping up at breakneck speed. Tether, which operates USDT, a cryptocurrency backed up with the U.S. dollar, announced that almost $31 million of its USDT was stolen from its core treasury wallet "through malicious action by an external attacker." *Read more*

November 30, 2017

FEATURED AUTHORS:

Pamela H. Del Negro
Nuala E. Droney
Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Privacy Tip
Virtual Currency

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

DATA BREACH

Health Care Data Breaches Continue but Fell in October

The news about data breaches always seems to be dire lately. Some good news: data breaches in the health care industry were lower in October than in September, based on reportable data breaches to the Office for Civil Rights (OCR). Note that only breaches involving more than 500 records have to be disclosed to the OCR at the time of the breach, so these are not the final numbers. *Read more*

Imgur Discloses Breach Affecting Email and Passwords of 1.7 Million Users

On November 24, 2017, image-sharing website Imgur disclosed the email addresses and passwords of 1.7 million users were stolen in a 2014 hack on the company. Imgur became aware of the breach on November 23, 2017, when a security researcher alerted the company about the potential issue. The breach was confirmed on November 24 and Imgur posted a notice of the breach on its blog later that same day. According to the blog post, the breach does not include personally identifiable information (PII) because Imgur has never asked for users' real names, addresses, telephone numbers, or other PII. Imgur is still investigating the breach but believes it may have been caused by a security algorithm in use at the time, which has since been replaced. Imgur has already begun resetting passwords of affected users and recommends that individuals use a different combination of email and passwords for every site and application. Imgur has approximately 150 million monthly users. *Read more*

Cottage Health Pays $2 Million to CA AG for Data Breach

Cottage Health, a three-hospital health care system located in California, has agreed to pay the California Attorney General's Office $2 million to settle allegations that it failed to implement data security safeguards to protect patients' health information that was accessible online and indexed by search engines.

In December 2013, it was discovered that one of Cottage Health's servers was connected to the Internet without encryption, password protection, firewalls, or access controls, which exposed health information of 50,000 patients between 2011 and 2013. Then on November 8, 2015, when state authorities were investigating the first incident, the hospital's server was misconfigured and the medical records of 4,596 were publicly available. *Read more*

North Carolina DHS Notifies 6,000 People of Data Breach of Drug Testing Information

The North Carolina Department of Health and Human Services has notified close to 6,000 individuals that a spreadsheet containing the names, Social Security numbers, and test results for routine drug testing for employment, internships, and volunteer opportunities was sent via an unencrypted email to a vendor in error.

Misdirected emails are a frequent occurrence and can have dire consequences. Limiting information in spreadsheets is a strategy to reduce the risk of a breach in the event that an email containing information is sent to the wrong recipient. It is unclear why full Social Security numbers were on this particular spreadsheet or why they were needed by the recipient, but it is a potent reminder that deleting or not including high-risk information before sending it to others is an important practice. *Read more*

DRONES

The Benefits and Hurdles of Using Drones for Conservation Surveillance

Drone technology has myriad conservation and environmental protection applications. Drones offer quick, easy, and cost-effective aerial imaging as well as sensor and monitoring capabilities. Unlike traditional surveying techniques, drones do not require substantial manpower and can overcome common access issues (e.g., impenetrable vegetation, boulders, crevasses). With these benefits, more and more drones are being used for forest health monitoring, forest inventory, wildlife surveys, antipoaching activities, reforestation, compliance monitoring, and air quality monitoring. *Read more*

PRIVACY TIP #116

Insider Error or Threat Continue to Cause Data Breaches

You continue to hear that your employees are your biggest risk when it comes to causing a data breach. Recent incidents that we have been involved in that were caused by employee error include:

- lost or stolen unencrypted laptops, phones, or removable media
- downloading sensitive information onto thumb drives or USB drives and losing them
- clicking on infected links or attachments and introducing malware or ransomware into the system
- misdirecting an unencrypted email containing personal

information

The sad thing about these incidents is that they were all completely preventable. Protecting your company from your employees is an odd concept but essential in the context of data security.

Some protections include:

- implement security measures so employees can't download information onto unencrypted laptops or thumb drives
- prohibit noncompany encrypted thumb drives from being connected to your system
- educate employees to detect and report phishing and spear phishing schemes; test them with internal phishing drives and retrain employees when they fail
- require the transmission of sensitive data with encryption;
- implement procedures for employees to use with the phone or face-to-face contact when receiving odd requests via emails for financial information, benefit information or wire transfers
- implement multifactor authentication and strong password procedures
- educate employees to slow down, take their time, and verify the intended recipient before sending an email
- educate, educate, educate and engage your employees on data security so they can become the company's stewards of data

These basic data security measures could have protected the companies who suffered the incidents above from mistakes made by their own employees.