How Ransomware Became a Billion-Dollar Nightmare for Businesses

News

The FBI says ransomware attacks cost their victims a total of $209 million in the first three months of 2016, up from $24 million in all of 2015. And the real number could be much higher if unreported attacks are considered, reports *The Atlantic*.

For Businesses, Vendor Contracts Can Have Huge Cybersecurity Implications

Insight

Companies can be at risk and liable when dealing with vendors who have direct access to sort, store or transmit their data, a Dallas lawyer told the *Dallas Business Journal*.

Increasing Use of Cyber

Insurance Requirements in Contracts

Insight

Insurance requirements are common in commercial contracts, and many contracts now include a sub-clause regarding cyber insurance, write Branwen Buckley and Corby J. Baumann of Thompson Hine.

Big Banks Form New Group to Combat Cyber Threats

News

The financial-services industry ranked third in number of cyberattacks last year, after health care and manufacturing, according to a U.S. cybersecurity report released by IBM Corp. in May.

Largest HIPAA Settlement Ever: What You Need to Know

Insight

The operator of 12 hospitals and more than 200 other treatment centers in Chicago and central Illinois has agreed to the largest settlement to date with the Office for Civil Rights

for multiple potential violations of the Health Insurance Portability and Accountability Act, reports Shumaker, Loop & Kendrick.

Cybersecurity for Banks: The Legal and Regulatory Framework

Event, July 26, 1-2:30 p.m. EDT

Practical Law will present a complimentary webinar Tuesday, July 26, 1-2:30 p.m. EDT, on evolving cybersecurity issues for banks.

Court Upholds Ex-Korn/Ferry Executive's Conviction in Hacking Case

News

A federal appeals court on Tuesday gave the U.S. Department of Justice broad leeway to police password theft under a 1984 anti-hacking law, upholding the conviction of a former Korn/Ferry International executive for stealing confidential client data, reports Reuters.

Computer Use Policies – Are Your Company's Illegal According to the NLRB?

Insight

The National Labor Relations Board has continued its assault on businesses and their ability to legitimately protect their computer systems and information against unauthorized non-business use by employees, writes Shawn E. Tuma, in Cybersecurity Business Law.

Morgan Stanley Pays $1 mln SEC Fine Over Stolen Customer Data

News

Reuters is reporting that Morgan Stanley has agreed to pay a $1 million fine to settle U.S. Securities and Exchange Commission civil charges that security lapses at the Wall Street bank enabled a former financial adviser to tap into its computers and take client data home, the regulator said.

Managing HIPAA Data Breaches

Event, June 15, 2 p.m. EDT

Compliancy Group will present a complimentary webinar designed to give individuals and entities operating in the health care sector the skills they need to be prepared to identify, respond and manage data breaches.

The Dangerous Misperception of Ransomware

On-Demand

A new complimentary on-demand video posted on BrightTALK discusses ransomware attacks and how to protect an organization using a holistic and unifying visibility into the network and endpoints.

Kate Morris Earns Distinguished Certified Information Privacy Professional Certification

News

Kathryne “Kate” M. Morris of Strasburger & Price earned the credential based on successfully passing the IAPP

comprehensive examination covering privacy and data protection laws and practices in the United States

---

A Leak Wounded This Company. Fighting the Feds Finished It Off

NEWS

LabMD's future changed one day in 2008 when the company's general manager received a phone call from a man who claimed to be in possession of a file containing patient information, including more than 9,000 Social Security numbers, reports Bloomberg.

What Can Be Learned From the Panama Papers About the Cloud?

Article

An article posted by ContractRoom discusses how the hack into the Panama Papers happened and what this means about how law firms store documents.

Legal Group Poised to Quiz Clinton Aides About Email Server

News

The State Department has agreed to a conservative legal group's request to question several current and former government officials about the creation of Hillary Clinton's private email system, reports the Associated Press.

Microsoft Sues Feds, Challenging Gag Orders on Customer-Data Seizures

News

Microsoft sued the U.S. government Thursday, arguing that a law that can prohibit technology companies from telling customers when law enforcement comes looking for their data is unconstitutional, reports *The Seattle Times*.

How Law Firms Should Strengthen Cybersecurity to Protect Themselves and Clients

Article

Law firms store a wealth of sensitive and confidential information electronically, making them prime targets for hackers. Not only does weak data security affect business development and client retention for firms, but can result in legal and ethical violations as well. How can firms meet clients' increasing data expectations?

FTC Commissioner Julie Brill Joins Hogan Lovells

News

Hogan Lovells announced that Julie Brill, a Commissioner at the U.S. Federal Trade Commission (FTC), will join the firm's Washington, D.C. office as a partner and co-director of the Privacy and Cybersecurity Practice on April 1.

Hillary Clinton Says She Won’t Be Indicted Over Emails. Is That Right?

News

A report by *Christian Science Monitor* staff writer Peter Grier addresses the question: Is Clinton right to be so dismissive of the possibility of being indicted?

Apple’s Angry Response to the Department of Justice: A ‘Cheap Shot’ That’s ‘Intended to Smear the Other Side’

News

The U.S. Department of Justice filed a legal response on Thursday to Apple’s refusal to help the FBI unlock an iPhone used by one of the San Bernardino shooters, and Apple quickly responded, with general counsel Bruce Sewell delivering a tense and angry response in a conference call with reporters, reports *Business Insider*.