Contracting in the Cloud: Who Pays for a Data Breach?

Insight

Data stored in the cloud faces many of the same threats as locally-stored data and, due to the growing amount of information in the cloud, it can be an attractive target for hackers, write Sidley Austin lawyers Scott Nonaka and Kevin Rubino for Bloomberg Law.

How to Identify and Mitigate Cybersecurity Threats for Business [Free Webinar]

Event, Oct. 26, 11 a.m. PST

SecureDocs will present a complimentary webinar designed for professionals who are interested in understanding, identifying, and mitigating potential data breach disasters before they occur.

Big Law Business Summit – West

Event, Oct. 27

Bloomberg Law invites leaders of big law – the top law firms

in the country and the legal departments they serve – to the Big Law Business Summit – West.

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*.

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.

Watchdog Group Denied Depositions in Third Clinton

Email Case

News

The ruling gives some relief to the State Department and Clinton, which have both been the subject of intense scrutiny over the private email setup that the former secretary of State used throughout her time in the Obama administration, reports *The Hill*.

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.

Two Accused in J.P. Morgan Hacking Case Plead Not Guilty

News

Two Israeli men pleaded not guilty on Thursday to charges that they broke into a dozen companies' computer networks, including J.P. Morgan Chase & Co., to facilitate a global network of criminal activity, reports *The Wall Street Journal*.

Drafting Data Privacy and Security Compliant SaaS in a Post-Safe-Harbor World

Event, June 15, 1 p.m. EDT

Data privacy and security are key issues for businesses who seek to upload their information onto the cloud. Customers

need assurance that the software as a service (SaaS) or other cloud service provider will maintain effective policies and practices to safeguard the confidentiality and security of their information.

Governance Challenges 2016: M&A Oversight

White Paper

The NACD report addresses the importance of early board engagement in strategy, the need for proactive dialogue with all key stakeholders, and the imperative to balance short-term and long-term goals throughout the M&A process.

Judge: Video of Clinton Aides' Depositions to Be Kept Secret

News

Videos of Hillary Clinton's former aides and others giving depositions in a lawsuit related to her private email set-up will be kept secret, at least for now, a federal judge ruled Thursday, according to a report by Politico.

Clinton E-Mail Use Violated Rules, State Department Audit Finds

News

Hillary Clinton’s use of a private e-mail system while she was secretary of state violated State Department rules, the agency’s Inspector General concluded.

Obama Signs Trade Secrets Bill, Allowing Companies to Sue

News

“Unfortunately, all too often, some of our competitors, instead of competing with us fairly, are trying to steal these trade secrets from American companies, and that means a loss of American jobs, a loss of American markets, a loss of American leadership,” President Obama said.

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.