September 4, 2018

Dear Readers,

Please find below the latest edition of the Cloud Computing Committee’s SciTech Cloud News. Do not hesitate to contact me with any questions, comments, or contributions (including suggested articles for the next publication) to make this most valuable for your practice.

Sincerely,
Jastin Mostowtt
Editor
Jastin.Mostowtt@botw.com

---

**Bennett B. Borden**
*Committee Co-Chair*
Chief Data Scientist and Chair, Information Governance Group
Drinker Biddle & Reath LLP
bennett.borden@dbr.com

**Joe Pennell**
*Committee Co-Chair*
Partner, Technology Transactions Group
Mayer Brown LLP
JPennell@mayerbrown.com

**Janet A. Stiven**
*Committee Co-Chair*
Vice President & General Counsel
The Moody Bible Institute of Chicago
Janet.stiven@moody.edu

**Arash Heidarian**
*Committee Vice Chair*
Senior Corporate Counsel
Amazon Web Services
heidaria@amazon.com

**Eric A. Hibbard**
*Committee Vice Chair*
CTO Security and Privacy
Hitachi Data Systems
Eric.Hibbard@hds.com

**Nkechi Kanu**
*Committee Vice Chair*
Associate
Crowell & Moring
nkanu@crowell.com

**Edward Paddock III**
*Committee Vice Chair*
Senior Counsel
Data & Technology Practice Group
McDonald's Corporation
edward.paddock@us.mcd.com

---

**Data Security**

**Why Your Business Should Implement Multifactor Authentication**
*Tech Republic, August 6, 2018*

In July 2018, Timehop, a small cloud-based company that retrieves old social media content for users, reported that its database of 21 million users had been breached. According to the company’s incident response team, the cause of the security breach could be traced to the fact that there was no multifactor authentication required to access its cloud computing environment. This article advocates for multifactor authentication to be enabled for cloud environments, in addition to other controls to mitigate the inherent risks of the cloud.

**EU Nations Lag in Implementing Law to Fight Cyberattacks**
*Bloomberg Law, July 20, 2018*
The European Commission sent warning letters to seventeen EU Countries instructing them to speed up their adoption of a new directive designed to increase cybersecurity. This directive requires EU countries to take steps to ensure protection of vital economic activities against cyberattacks. For example, countries must list operators of essential services in energy, utility, banking, transportation, and health care sectors and require them to take cybersecurity precautions. All EU countries must also list companies that would be required to report cyberattacks by November 9, 2018.

**Cloud Computing Remains Top Emerging Business Risk**
*Help Net Security, August 16, 2018*
For executives in risk, audit, finance, and compliance roles, cloud computing remains a top risk. Additional and closely related risks included information security risks and GDPR compliance. According to the survey, despite record spending on information security in the last two years, organizations have lost an estimated $400 billion to cyber theft and fraud worldwide. As cloud usage continues to expand, cloud security will remain a top concern.

**The State of Cybersecurity at Small Organizations**
*CSO, August 16, 2018*
A recent survey reveals that the majority of small organizations have had at least one cybersecurity related incident over the past year, including system compromise, malware, data breach, etc. Contributing factors to these incidents include human error, general lack of understanding and training about cyber risk, and implementation of new IT initiatives without proper controls. Small business executives are encouraged to stay up-to-date in cybersecurity knowledge and train employees to avoid such incidents.

**Enterprises Beware: Cybersecurity Challenges in The Cloud**
*Security Info Watch, August 10, 2018*
This article describes and addresses several top security concerns that companies face when utilizing cloud computing, particularly ensuring compliance with HIPAA, PCI DSS, and IFRS. Other cybersecurity concerns addressed include: vulnerabilities with collaboration apps, mobile devices delivering convenience with risks, IoT devices opening the door to hackers, and managing security with a multitude of data.

**Data Privacy**

**Trump Administration Working on Consumer Data Privacy Policy**
*Reuters, July 27, 2018*
Following the implementation of the European Union’s GDPR framework and California’s adoption of recent data privacy legislation, the Trump administration is developing federal consumer data privacy policies. The Commerce Department is meeting with key technology companies, such as Facebook, Comcast, and Alphabet, to gain insight and consensus for adopting a policy that eventually can be memorialized in legislation. The administration “aims to craft a consumer privacy protection policy that is the appropriate balance between privacy and prosperity…”
Cloud Computing
JD Supra (Bryan Cave Leighton Paisner), August 13, 2018
This article encourages companies and law firms using cloud-computing to take careful steps to safeguard their data. The article details fifteen questions that companies should evaluate in selecting cloud service providers in order to minimize data security risks.

Microsoft Calls for AI Face Recognition Software Regulation
Bloomberg Law, July 13, 2018
Microsoft is urging lawmakers to regulate the use of artificial intelligence in facial recognition software to prevent abuse. Microsoft is improving its facial recognition software by improving its capability to recognize individual faces; taking steps to make those systems less prone to bias; developing new public principles to govern the technology, and moving more deliberately to sell its software and expertise in the area. This call for regulation is in response to Microsoft and other cloud companies selling facial recognition software to government agencies and police departments, with push-back from civil liberties groups and company employees.

Market News & Developments

Exclusive: India Panel Wants Localization of Cloud Storage Data in Possible Blow to Big Tech Firms
Reuters, August 4, 2018
The Indian government’s cloud computing panel drafted a proposal that would require data generated in India to be stored within the country. Indian government authorities believe that storing information locally would allow for easier access when conducting investigations. However, this would negatively impact the American tech giants, such as Microsoft and Amazon. They, along with smaller cloud-companies, believe this proposal would increase costs for cloud companies and their customers due to the need for an increase of data centers in India.

Alibaba Takes More Cloud Products Global, Eyes APAC Growth
ZD Net, August 15, 2018
Alibaba launched a set of cloud products for the global market, noting Asia-Pacific as a priority region for growth. The Chinese firm is highlighting its youth, regional data center footprint, and global product releases as key differentiators from Amazon Web Services and Google.

Public Sector News

A Closer Look at DOD’s Cloudy JEDI Contract
FCW, August 10, 2018
This article summarizes the turbulent start to the Joint Enterprise Defense Infrastructure (JEDI) infrastructure as a service and platform as a service cloud computing contract, with an estimated transaction value of over $10 billion deal over ten years. The focus of concern is that there will be a single cloud provider.

Government’s Move to Improve FedRAMP Aims to Ease Cloud Adoption
GCN, August 13, 2018
The FedRAMP Reform Act of 2018 was proposed by representatives in July to improve the current FedRAMP legislation. The goal of the bill is to increase cloud service providers’ efficiency and reduce redundant processes. For example, the bill would protect program investments already made by CSPs, establish metrics for certifications, more clearly define roles and responsibilities for management and agencies, and provide funding for the FedRAMP program through the Acquisition Services Fund.

**Oracle Challenges Pentagon’s Multibillion-Dollar Cloud Computing Contract Before Bids Are Even Submitted**
*The Washington Post, August 7, 2018*
Oracle is challenging the Pentagon’s decision to choose just one company for the not-yet-awarded $10 billion JEDI cloud computing contract. This article details the various challenges to JEDI including the Pentagon’s failure to adhere to procurement regulations and pursuit of a strategy that will hurt the military’s technological prowess.

**Governance & Agreements**

**9 of the Biggest Cloud Computing Legal Myths, Debunked**
*The National Law Review (Practice Panther), August 15, 2018*
This article promotes cloud computing practices by addressing common concerns from law firms and other legal organizations that are hesitant to move to the cloud. Myths addressed include: (1) The cloud does not provide enough security for my law firm’s sensitive data; (2) The cloud is a passing trend; (3) Moving to the cloud costs too much; (4) With the cloud, migration comes with too many changes, including having to use different applications; (5) No one needs the cloud – our current infrastructure works well enough; (6) Moving to the cloud will be a piece of cake; (7) Cloud computing is an immature technology; (8) Cloud computing does not provide technical support; and (9) Cloud providers are the number one reason for data breaches.

**Tips for Legal Organizations to Embrace Digital Transformation**
*Bloomberg Law (Microsoft Corporation In-House), August 15, 2018*
This article encourages legal organizations to adopt cloud-based technology to better serve clients and stand out. Tips to accelerate digital transformation include: be bold and embrace change, get help and learn from others, define requirements, greater diversity and inclusion, leverage existing technology, test drive solutions, select only trusted technology partners, and set the tone at the top and use technology.

**European Banking Authority Issues Recommendations for Outsourcing to Cloud Service Providers**
*JDSupra (Morgan Lewis), August 1, 2018*
Effective as of July 1, 2018, European financial institutions must now comply with the European Banking Authority’s recommendations when outsourcing to cloud service providers. These recommendations are also useful when outsourcing to cloud providers outside of the European financial services industry in Europe. These recommendations cover: (1) Materiality Assessment, (2) Duty to inform supervisors, (3) Access and audit rights, (4) Security of Systems, (5) Location of data and processing, (6) Chain outsourcing, and (7) Contingency plans.