SHARE:

Join Our Email List

The KIT — Knowledge & Information Technology

No. 214 - 16 April 2018

Was this forwarded to you?

join our mailing list

In This Issue

Consulting Services

- IT Strategy
- Enterprise Architecture Roadmap
- Business Process Modeling & Analysis
- Enterprise Software Selection
- IT Innovation Briefings
- IT Due Diligence
- Executive IT Seminars
- Cloud Computing
- Security Maturity
- Software Process
- Knowledge Strategy
- Technical Communities
- Knowledge Capture
- Taxonomy development
- Enterprise Social Media

Data Governance -- Are the Starts Aligning?

With the implementation of the European Union's Global Data Protection Regulation (GDPR) on May 25 rapidly approaching, the need to address not only privacy but also data residency, ownership and sovereignty is becoming clearer. Coincidentally, the leaders of several ongoing efforts within the Object Management Group (OMG) have started discussing whether and how to join forces. Those efforts include:

- the Data Residency Working Group formed in 2015
- the Data Provenance and Pedigree Working Group formed in 2016
- the Information Exchange Facility (IEF)
- the Data Tagging and Labeling (DTL) proposal from the C4I Task Force

The next OMG meeting (Boston, June 18-23) will include a discussion on whether to unite these efforts within a single Special Interest Group or Task Force. Stay tuned!

Digital Business World Congress in Madrid

The U.S. Embassy in Madrid is organizing a U.S. Pavilion at the Digital Enterprise Show/Business World Congress in Madrid, May 22-24. U.S. exporters of cybersecurity, blockchain, cloud computing, AI, and Internet of Things technologies are encouraged to join the U.S. Pavilion where they will receive counseling and support by U.S. Embassy industry experts, invitations to exclusive networking events featuring high-level U.S. Government dignitaries, B2B matchmaking, and the chance to connect with business opportunities from across Europe. For more information, contact Jesus Garcia with the U.S. Embassy in Madrid.

The Long Arm of the Law... Gets a Little Longer

What's become known as the Microsoft Ireland case has been exhibit A in the data residency debate. As a reminder, Microsoft refused in 2013 to obey an order from U.S. authorities, based on the 1986 Stored Communications Act, to produce the e-mails, stored on an Exchange server in Ireland, from one of their clients suspected of drug trafficking. After wending its way through lower-level courts, the case was heard by the U.S. Supreme Court in February and was to be decided this June.

On March 30, the U.S. Department of Justice asked the Supreme Court to dismiss the case; and on April 5, Microsoft concurred. That should be good news for privacy, right? Wrong. The reason behind the DOJ's move is that their initial case is now moot, since the "Clarifying Lawful Overseas Use of Data" (CLOUD) Act, passed by Congress on March 22 as part of their massive spending bill, gives law enforcement a new and easier way to seize those e-mails. In its concurring filing, Microsoft called the Act "a nuanced legislative scheme," but that assessment is controversial. The CLOUD Act allows the U.S. Attorney General (the Minister of Justice, in most other countries' parlance) to enter into direct agreements with other countries to allow data seizure across borders, without the checks and balances of the independent court system.

Contact Us:

cébé
IT & Knowledge Management

www.cebe-itkm.com
info@cebe-itkm.com
+1 415 870 ITKM
Twitter: @cbaudoin

Archive:
Previous KIT Issues

Forward this issue to colleagues and friends: use the "forward email" link below at left, rather than "Forward" in your email software, to preserve your privacy, give the recipient more options (their own unsubscribe link, etc.) and to give us better click-through data. Thanks!

IoT Device Patching

The lag in upgrading and patching computers to remove known vulnerabilities has been a major enabler of security attacks for decades. With IoT devices in the picture, the problem is becoming even worse. In "IoT Security Disconnects: As Attacks Spike, Device Patching Still Lags," ThreatPost reports on a survey by Trustwave, in which 61% of respondents with connected device deployments said they experienced security issues, but only 49% percent have "formal patching policies and procedures in place that would help prevent attacks."

At the consumer IoT level, the problem is hard to address, since the device owners are not professionals and the device maker often doesn't know who operates the devices or where (a problem that the U.S. National Telecommunications and Information Administration is trying to address, as explained in previous KIT issues). In Industrial IoT, however, there is not really a good excuse. The enterprise's configuration management database (CMDB) needs to be extended to include IoT devices -- even if it is simpler to say than to implement. This is not a new idea -- see a presentation given at a meeting of the British Computer Society two years ago.

Seen Recently...

"[The] RSA Conference should rename itself as Fear-Based Selling Conference."

-- @cloud_opinion, "Parody + Tech commentary"

"Every tech conference though is either a Fear-Based Selling Conference or a FOMO [Fear Of Missing Out] Based Selling Conference."

-- Justin O., host of "On the Air" at Spiceworks, @justinongisrad

"You make it sound like it's a bad thing :-)"

-- Bernard Golden, VP Cloud Strategy at CapitalOne, @bernardgolden

"Come on, at least a few of them are a recruiting-each-other's-employees conference."

-- Jonah Horowitz, site reliability engineering manager at Apple, @jonahhorowitz