

SHARE:

[Join Our Email List](#)

The KIT – Knowledge & Information Technology

No. 230 - 17 December 2018

Was this forwarded to you?



In This Issue

[Comments on Secure Electronic Voting](#)

[Cloud Lessons Learned](#)

[BPMN 2.0 Book](#)

[Cybersecurity Priorities](#)

[Seen Recently](#)



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

Contact Us:

→ Happy Holidays!

We wish our 900 or so readers a happy holiday season. The next issue will appear on January 2, 2019.

→ Comment on "Baby Steps in Secure Electronic Voting"

In the last issue, we mentioned an electronic voting pilot project for voters in West Virginia who reside in another country, based on a mobile application from Voatz that relies on facial recognition and blockchain to secure the voting process. Bertrand Ducastel wrote back with a useful clarification:

"The key sentence in the Washington Post is:

'Votes are stored on a private blockchain -- essentially a database where records are secured using complex computational algorithms -- and unlocked by county clerks when the polls close.'

The part 'secured using complex computational algorithms' is incorrect. That would be correct for Bitcoin's blockchain, but not for Voatz's blockchain. In the case of Voatz, record certification is effected by Voatz, not by distribution, as is the case for Bitcoin. That creates the security issue at hand, as certification by distribution does not present a single point of failure (an attack must overwhelm the distribution to succeed), while for Voatz the attack can concentrate on Voatz processes."

→ Cloud Lessons Learned

The latest issue of the Cutter Business Technology Journal (December 10, 2018) was entitled "Riding the Next Wave of Cloud Computing." Claude Baudoin wrote one of the four articles included in this issue, "Cloud Lessons Learned." Here is the abstract:

"This article tries to take a very pragmatic viewpoint about cloud computing: what are the things we have learned? What do most reasonable analysts and users now agree on, as opposed to questions to which the jury is still out? What should you spend time worrying about, and what should you consider settled, for good or for bad? Finally, with various lessons learned, what should you educate your managers or clients about so they don't waste their time or yours?"

If you are a Cutter client, [get the article here](#). If not, either go to that same page and click on "become a guest," or [let us know](#) and we will get you a copy.

→ Learn BPMN 2.0

There have been several books on the Business Process Model and Notation (BPMN), one of the most successful standards from the Object Management Group besides UML and SysML. Dr. Joshua Fuehrer and Joseph Butchko's new book, "[Learning BPMN 2.0 -- A Practical Guide for Today's Adult Learners](#)" (\$30 on Amazon) distinguishes itself by the use of several teaching techniques:



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!

- it is absolutely filled with figures (239 of them!), most of which are fragments of process models or examples of notation elements.
- It is printed in full color, which helps with the book's clarity and appeal.
- On almost every page, one of 8 reader stereotypes ("Meditating Mike," "Forum Felicia," "Surfer Dave," etc.) launches into an aside, providing a tip or example based on his/her distinct perspective -- a trick that keeps the main flow of the lesson very compact but provides helpful commentary when the reader needs it.

→ Cybersecurity Priorities for 2019

A month-old article on the ITProPortal website, "[Top Ten Cybersecurity Predictions for 2019](#)" (there is apparently an unwritten rule that from Halloween until New Year's Eve, every other article in IT publications must be entitled "Top N predictions in X for <YYYY+1>", where N is an integer preferably between 6 and 12) breaks no new ground for reasonably informed people, but its author Ian Kilpatrick, from the Nuvias Group, provides a good checklist for all.

The third point on "cloud insecurity" sounds alarmist. We said it many times, here and in various papers: public clouds are not necessarily less secure than on-premises systems. One of the reasons is the "needle in a haystack" effect. If my data is on my own servers, you can find their IP addresses via the Domain Name System and you will know where to attack, while if it is in a public cloud, good luck finding my data! But the article points out a scary fact: "*Skyhigh Networks research indicated that 7% of S3 buckets are publicly accessible and 35% are unencrypted*" (an S3 bucket is a data storage resource rented from Amazon Web Services' Simple Storage Service, or S3).

The sixth point talks about "cyber hygiene" and mentions awareness techniques that are still not sufficiently widespread, such as simulated phishing and social engineering attacks.

→ Seen Recently...

"We can put a man on the moon but we can't get meeting technology to work."

-- MikeKavis, [@madgreek65](#)

"When you allow people to communicate, whether 1:1 or 1:many, there will be harm."

-- [Alex Stamos](#), responding to @zooko, who had said that "all the bad things about the Internet [...] come from the advertising revenue model." Stamos' pointed out that even ad-free services see abuse.