

SHARE:

[Join Our Email List](#)

The KIT – Knowledge & Information Technology No. 255 - 6 January 2020

Was this forwarded to you?



In This Issue

[Happy New Year](#)

[Steve McConnell on Software Leadership](#)

[Cybersecurity of IoT Devices](#)

[AI for Risk Management](#)

[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

→ **Happy New Year!**

It's certainly not "the end of history," in IT or in the world in general, as current events show. Who knows that the year has in store for us? We've played the prediction game before, but as the cliché goes, change is the only thing that doesn't change.

cébé and its partners wish our friends, colleagues, clients, past clients... and future clients (hint!) a successful and safe 2020. We're looking forward to bringing you more updates, twice a month, with focuses (foci?) on governance, architecture, cloud, IoT, security, and more.

We also remind you that you are more than welcome to contribute. You may send us a comment on a published piece, an entire article (250 words maximum, please), or even a series of contributions spaced out over the year.

Finally, we're open to giving you the rights to *publish co-branded foreign language editions*, perhaps at a different frequency or with just a subset of the articles. We can even host you on our Constant Contact account, so there would be no hard cost besides your labor. Let us know if you are interested and we'll discuss the details!

Note: to space the next issues more evenly, The KIT No. 256 will come out on January 20, No. 257 on February 3, and then we will be back on our normal schedule (1st and 16th of each month, or the first working day thereafter).

→ ***Tomorrow* Steve McConnell on Software Leadership**

Register [here](#) for the next free ACM TechTalk, "Seven Unbreakable Rules of Software Leadership" by Steve McConnell, CEO and Chief Software Engineer at Construx Software, on Tuesday, January 7, at 10:00 am Pacific / 1:00 pm Eastern / 1800 GMT. You need to register too if you want to receive a link to the webinar recording.

"After more than 10 years of working with top software executives across a full spectrum of software-intensive industries, [...] McConnell has found a method for predicting which technical executives will be successful in their organizations and which will end up looking for different positions."

→ **Internet of Things Security (again)**

In an article in the Lawfare blog, "[Closing a Critical Gap in Cybersecurity](#)," Christopher Krebs, director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), warns that *"too often we come across cybersecurity vulnerabilities sitting on the public internet and are unable to act because we cannot identify the owner of the vulnerable system."* He says that this while CISA can discover the IP addresses of vulnerable devices, it currently cannot legally obtain the names of their owners from the ISPs. The government is seeking to establish an "administrative subpoena" power to obtain the owners' identities.

Contact Us:



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!

To bolster his point, Mr. Krebs says that "CISA is currently aware of a system that controls water pumps, one controlling an oil and natural gas facility, and one controlling emergency management equipment that can be accessed without a password and modified by anyone with an internet connection."

After a few years of often ignored warnings about the security risks posed by misconfigured IoT devices, it should not be surprising that companies are going to get a knock on their door by someone saying "we're from the government and we're here to help you." With these security enforcement powers comes the risk of misuse. To his credit, Mr. Krebs directly acknowledges this concern and explains why, in his opinion, the risk is minimal.

→ AI for Risk Management (Fake News Alert)

We were surprised when a colleague pointed out a report in the Business Insurance journal about the forum of the Federation of European Risk Management Associations held in Berlin in November. Written by Gavin Souter and entitled "Artificial intelligence set to be the tool for risk managers," this piece quotes multiple participants and in particular attributes the following quote to Ms. Bénédicte Huot de Luze, CEO of AI Risk Services in Paris: "When you use AI, it is only to replace a practice with no added value, it is only something repetitive with a high volume and done without expertise."

We thought this statement sounded so ignorant that we questioned its authenticity. We contacted Ms. Huot de Luze, who adamantly denied having said anything like this, and agreed with us that AI can generate risk information from data in novel ways and add value. An example we used in our conversation with her is the exploitation of drilling reports in the oilfield industry -- specifically, using natural language processing (NLP) to decode the domain jargon of drilling decisions and incidents and develop correlations between the two (see for example [this research paper](#)).

We also contacted Mr. Souter about his quote over a month ago, but we have not received a reply. The quote still appears in the article at this time.

→ Seen Recently...

"Stop abbreviating 2020."

-- Article in USA Today, warning people that writing the date as "m/d/20" would allow fraudsters to change it to "m/d/2019" or "m/d/2021," causing legal or financial problems. Is it just me, or is there a Y2K déjà vu about this?