DOI:10.1145/3486590

Article development led by acmqueue
queue.acm.org

The time is (also) way overdue for IT professional liability.

BY POUL-HENNING KAMP

The Software Industry Is *Still* the Problem

AROUND THE TIME computers were old enough to drink, software engineering guru Gerald Weinberg said: "If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization."

This is not a plotline science fiction authors have ever neglected.

Actually, some titles are still worth a trip to the library: for example, Poul Anderson's *Sam Hall* from 1953, which shows how too much reliance on "infallible" computer surveillance can turn into an autoimmune collapse for a nation-state, or, for that matter, any large organization.

At the more obscure end of the spectrum, there is Swedish Nobel Laureate Hannes Alfvén, publishing in Swedish under the pseudonym Oluf Johannesson, with *Sagan om den stora Datamaskinen* [*Tale of the Big Computer*] from 1966.

As with almost all science fiction pieces, however, they miss the future by a wide margin. Not because they are bad at it, but because science fiction authors tend to focus on interesting and chaotic second-order effects with lots of crinkly bits around the fjords, because, let's be honest, they sell more books that way.

If any science fiction author, famous or obscure, had submitted a story where the plot was "modern IT is a bunch of crap that organized crime exploits for extortion," it would have gotten nowhere, because (A) that is just not credible, and (B) yawn!

And yet, here we are.

The good news is the ransomware attack on Colonial Pipeline in May 2021 probably marks the beginning of the end. Comforting as that might sound, it tells us very little about how that ending will turn out.

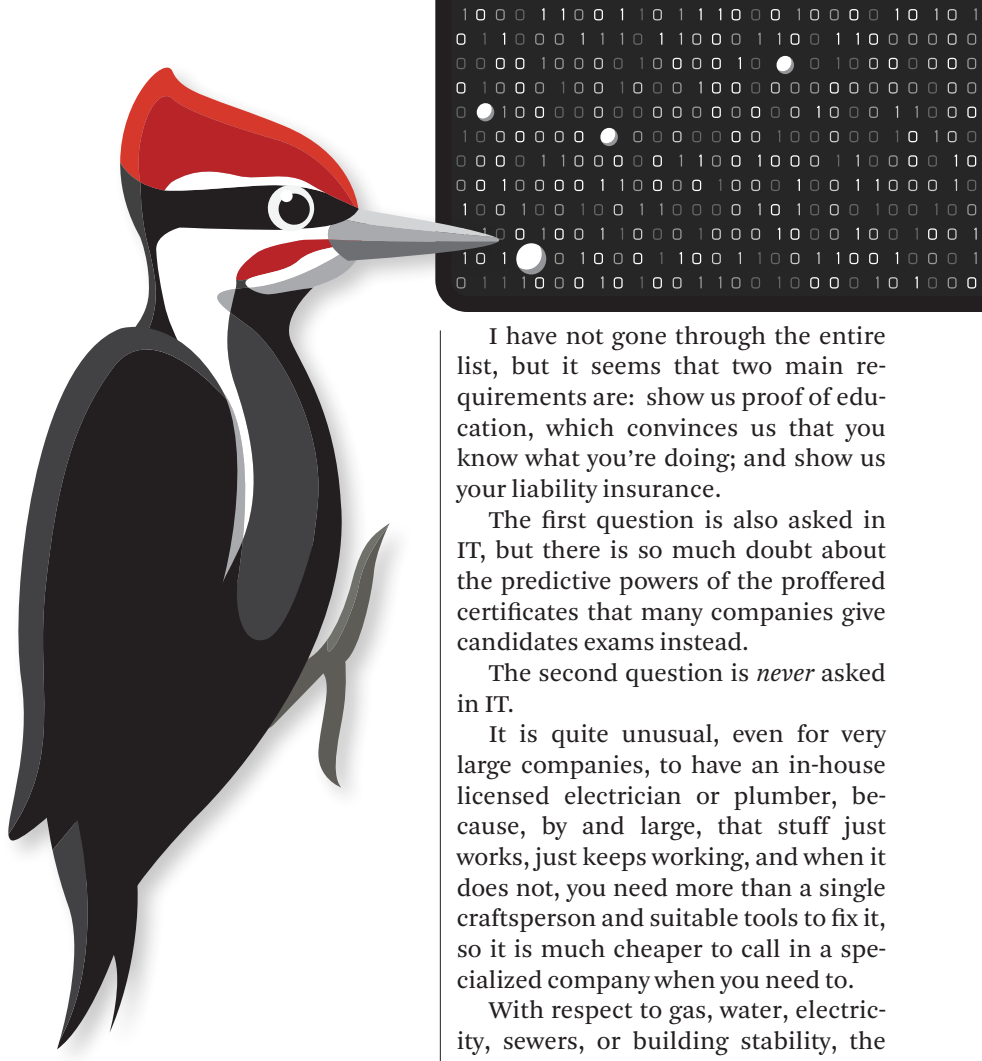
The first to react were the insurance companies. Some of them dropped the product, leaving their customers to their own devices; others were busy trying to come up with requirements and standards that would apply to their customers' claims for coverage.

I hope they put somebody competent on that assignment, because "following the industry best practice" is not going to cut it.

As I write this, 200-plus corporations, including many retail chains, have inoperative IT because extortionists found a hole in some niche, third-party software product most of us have never heard of.

Some 200 corporations are enough to argue they all "followed industry best practice," and that is precisely where Gerald Weinberg was coming from with his famous quote. The woodpecker is not leveling individual, particularly bad buildings, it is leveling civilization, because *all* the buildings are bad.

In a schoolbook instance of not seeing the forest, people who should know better are busy determining if it was a *Leuconotopicus albolarvatus*, a *Dendrocopos hyperythrus*, or some other member of *Picinae*.



Governments have finally noticed that a well-run nation-state is heavily dependent on an awful lot of computers working properly—computers that no one in the so-called "national security apparatus" previously gave much attention.

I mean, who cares how some oil company runs its billing system?

Politicians do not worry that thousands of toilets may suddenly start spewing water because goods like that have to "follow code" and adhere to product liability standards.

In contrast to this, lawyers for today's 200-plus affected corporations will find out that the full and complete extent of the third-party software vendors' liability is that they will send a new CD if the first one is unreadable.

We *badly* need real product liability for software. (See my article, "The Software Industry *IS* the Problem," in the November 2011 issue of *Communications*, p. 44.)

But what about the people who installed the toilets?

Most organizations seem to hire their first part-time IT person before they reach 20 employees. When that first IT person is replaced, the new IT person bores everybody with complaints about how "totally incompetent" the first person must have been, and, usually, is correct. When you hire somebody's teenage kid, you almost invariably get the competence you pay for.

It is also not uncommon for companies—at some point in their growth—to decide that they have to replace their entire IT installation because what they have "hampers their growth." It is only slightly less common for such projects to be a ruinous experience for all involved, because, as the eventual summary invariably goes, "Nobody seemed to know what they were doing."

Politicians do not worry about thousands of toilets spewing water because whoever installed the toilets in Colonial Pipeline's IT department had to go through examination, certification, and authorization before they were allowed to do that.

In Denmark, 129 jobs are regulated by law (https://bit.ly/33wLnPC). There are good and obvious reasons why it is illegal for any random Ken, Brian, or Dennis to install toilets or natural-gas furnaces, perform brain surgery, or certify a building is strong enough to be left outside during winter. It may be less obvious why the state cares who runs pet shops, inseminates cattle, or performs zoological taxidermy, but if you read the applicable laws, you will learn that animal welfare and protection of endangered species have many and obscure corner cases.

Notably absent, as in *totally* absent, on that list are any and all jobs related to IT; IT architecture, computers, computer networks, computer security, or protection of privacy in computer systems. People who have been legally barred and delicensed from every other possible trade—be it for incompetence, fraud, or both—are entirely free to enter the IT profession and become responsible for the IT architecture or cybersecurity of the IT system that controls nearly half the hydrocarbons to the Eastern Seaboard of the U.S.

I have not gone through the entire list, but it seems that two main requirements are: show us proof of education, which convinces us that you know what you're doing; and show us your liability insurance.

The first question is also asked in IT, but there is so much doubt about the predictive powers of the proffered certificates that many companies give candidates exams instead.

The second question is *never* asked in IT.

It is quite unusual, even for very large companies, to have an in-house licensed electrician or plumber, because, by and large, that stuff just works, just keeps working, and when it does not, you need more than a single craftsperson and suitable tools to fix it, so it is much cheaper to call in a specialized company when you need to.

With respect to gas, water, electricity, sewers, or building stability, the regulations do not care if a company is hundreds of years old or just started this morning, the rules are always the same: Stuff should just work, and only people who are licensed—because they know how to—are allowed to make it work, and they can be sued if they fail to do so.

The time is way overdue for IT engineers to be subject to professional liability, like almost every other engineering profession. Before you tell me that is impossible, please study how the very same thing happened with electricity, planes, cranes, trains, ships, automobiles, lifts, food processing, buildings, and, for that matter, driving a car.

As with software product liability, the astute reader is apt to exclaim, "This will be the end of IT as we know it!" Again, my considered response is, "Yes, please, that is precisely my point!" C

Poul-Henning Kamp spent more than a decade as one of the primary developers of the FreeBSD operating system before creating the Varnish HTTP Cache software, which approximately one-fifth of all Web traffic goes through. He is an independent contractor; one of his recent projects was a supercomputer cluster to stop the stars twinkling in the mirrors of European Southern Observatory's new Extremely Large Telescope (ELT).

Copyright held by owner/author.

IMAGE BY ANDRIJ BORYS ASSOCIATES. USING SHUTTERSTOCK