Darwin was right (even about IT)

by Przemysław Myszka

Photo: Rajant

We've been covering technological developments and how they have changed the transport and logistics domains for a number of issues now. However, the subject is far from exhausted. It even seems that we've sometimes barely scratched the surface, so many things are happening virtually on a daily basis. During the latest TOC Europe we sat down with Rajant's Chris Mason to talk about IT and how it ties to security, people, communications, standardisation, and ultimately Charles Darwin himself.

- ***Why do we need to worry about cyber-security in the first place?***

Data is most probably the biggest asset an organisation has. Organisations are therefore concerned with the integrity of their data and also with its competitive nature. At the same time, however, it is often underused, not disseminated widely enough, and potentially a point of vulnerability. In the modern industrial world, how one handles data makes all the difference between a successful and an ailing process. Take for instance automation, the next big thing for a lot of various industries. While it's true that automating things takes some people out of the equation, it also makes those who stay all the more important, because they supervise the automation process. These people then have to act based on correct information. Imagine now that you're dealing with heavy assets, like expensive autonomous machinery that takes care of tonnes of valuable cargo. If you're prevented from controlling that equipment to the point of not being able to stop it if required, due to a hacker attack or malfunction, you find yourself in a grave situation with possible loss of life and limb, not to mention other damages, including reputational. Integrity of data is, therefore, absolutely vital.

#Inside
#Communications#Cyber-security
#Chief Security Officer
#Automation#Connected Port of Things
#Blockchain
#Wi-Fi#LTE#Mesh

- ***What can we do to manage the risks? What should be the specific safety measures or obligations of different port employees, starting from dockers and clerks, and going all the way to managers and C-level execs?***

To my mind security in general, and its cyber part in particular, is composed the same way as IT is, namely as a combination of people, process, and technology. As such, most security breaches happen because people do not follow the rules. Frankly speaking, it's never the fault of the third component; technology has the capability to be secured against cyber-attacks. Yet, this is compromised either because people fail to behave in line with the right procedures, or the process is flawed itself. In short, you need to train people, govern them, and monitor in order to keep an organisation safe and secure. Technology helps with this – e.g., our particular speciality is securing from interventions on Rajant's wireless networks – but for the time being it won't do the whole work for humans. It's a vulnerability, the fact that you cannot take people 100% out of the equation. Understanding this is key, because rather than squaring the circle, an organisation can focus on equipping their staff with the right set of IT tools and competencies.

Putting it a bit bluntly, if the CEOs of major companies were more forthright in acknowledging their security, they'd agree that they had vulnerabilities and that they had suffered hacks, or any other security issues at some point in their operations, like a contractor plugging in an infected thumb drive, a staff member clicking on suspicious links or responding to e-mails from scam artists who promise the moon, etc. And I mean all of them. However, you won't see this happening, because this would negatively impact share prices and the company's reputation. If security isn't on the agenda during each and every board meeting, it should be.

In addition to the need for raising the awareness of CEOs on the subject, we're seeing a very strong trend of hiring Chief Security Officers. These CSOs – often coming from

the military, computer, radio, and system integrator sectors – sit at the board and have governance over both the managerial and operational aspects of a company's IT. That's a major shift in comparison to how things were arranged in the past, when there was no real interface between the different IT and exec silos, and how they communicated with each other. For instance, at Rajant we have acquired a whole team of cryptographers to make sure that we can offer absolute data security to our customers, including the United States Department of Defense and other defence agencies, but increasingly also commercial clients.

- ***What is Rajant's answer to the challenges of modern communications? Specifically, why traditional, fixed Wi-Fi and LTE networks aren't good enough anymore?***

Our CEO, Bob Schena, asks in this context one short, yet very apt question, "How important is your data?" If you're operating in an environment in which data is essentially your business, and the port environment is very data-oriented, you can manage it only if you have constant communication. Every asset that is controlled by IT must have a connection at all times as well as having no points of vulnerability. The latter are defined as single points without which the system could not function. A good example is LTE where every communication must go through a switch which identifies the subscribers and allocates traffic to them. Target the switch and communication is a goner. Another of LTE's single vulnerabilities is the fact that this technology runs on a single frequency. Traditional Wi-Fi does exactly the same; it has different frequencies, but for different purposes. Typically, the access points will be connected by one frequency and the client's devices on another frequency. Now, if you take out the access point, the client's devices connected to it won't work and operations will stop. If you want to have autonomous operations, this is a clear no-no.

In stark contrast, the Rajant kinetic mesh system gives you multiple physical routes for data and multiple frequencies. In other words, it provides a core data transmission platform – connectivity that's 100% fully mobile, has low latency, and offers a wide bandwidth – upon which companies can expand their businesses. Wi-Fi needs to disconnect in order to connect anew. So, if you break a session, you must start a new one. With a Rajant mesh network, this session would be maintained, as the network does not have the need for handoff if a failure occurs, another node simply picks up where the other left off with no down time, providing you with constant connectivity.

- ***Your company is using the term "Connected Port of Things". What stands behind it?***

Ports are not benign environments for radio signals. In many ways, harbours are similar to mining – you move heavy items from one place to another as seldom as possible and according to a predetermined plan by using machinery that itself needs to be monitored (as modern port handling equipment is loaded with all sorts of engine, tyre pressure, load, hydraulic, and even human alertness sensors). At the same time, though, there are barriers to communication and all kinds of interferences scattered all over the place. For years, port communication was a real problem, and that isn't just our opinion at Rajant, it is replayed by others, too. For a port to operate efficiently, uninterrupted connectivity is simply a must, hence the term Connected Port of Things.

You've now got organisations, e.g. OSIsoft, that are offering platforms that take in feeds from different sources and integrate them, as where in the past you had to juggle silo data. Now, imagine that you're a terminal operator and your yard fleet comprises STS cranes from one company, RTGs from another, and straddle carriers and reachstackers supplied by yet other companies, etc. You've got a few IT systems for these machines, supplying data either to you directly or which goes via cloud to the manufacturer who then gives you access to the information. What we're seeing now is a big drive toward standardisation, so that operators will be able to manage their heavy-duty assets through a common standard. This can only be a good thing, and you don't have to look far for proof. Just as containers have standardised the hardware part, parties like OSIsoft will do the same at the software level. An analogy would be if you'd imagine ports and terminals as computers or smartphones, run by common operating systems, such as Windows, Linux, or Android.

- ***How about tech-developments which until recently were considered as science fiction, but nowadays are making it to the headlines, like, for instance, blockchain? Is this only hype or can such technologies revolutionise the way economies are set up?***

Technologies like these require a first-mover. Our experiences with industries that involve significant investments, like mining, oil & gas, ports, manufacturing, or refining, is that it takes time for them to assess and then embrace technology. However, once a given tech solution is adopted by one of them, proving that it's actually doable and workable, and it delivers a competitive edge in the end, others then follow suit.

My understanding is that companies are grappling with these technologies, seeing how can they use them, as well as how to steer clear of repeating such mishaps as the dot-com bubble. For instance, if blockchain will be the technology that enables reinventing how we set up supply chains, how payments are carried out within them, how integrity is maintained throughout them, etc., surely it will become the stepping stone to new processes, businesses, or the economy in general. The bottom line is that Darwin was and still is right – it will be survival of the most adaptable to change. ■