Zero Outage
INDUSTRY STANDARD

INTERVIEW WITH PROF. DR. EBERHARD VON FABER, ZOIS SECURITY STREAM

Which would you say are the more unique challenges, compared to other industries, that IT faces - as far as executing standardisation is concerned?

Large-scale, complex IT is used in a dynamic environment and is characterised by the changing requirements of user organisations and severe cost pressure. Both trends require continuous adaptations of IT applications. Standardisation must keep up with these developments.

Some have accused the IT industry of lagging behind in establishing such universal standards – what would you say to those who take this POV (and if you agree what are the main reasons for such)?

IT applications are an important means to generate competitive advantages for user organisations, and the businesses of the latter are really different. This is a challenge for a “one size fits it all” approach. It is true that the IT industry also drives the changes. There are standards, e.g. IT security. They are, however, primarily specifying the “what” and not the “how”. Most standards concern a monolithic organisation and do not reflect the reality of supply-chains and the division of labour or distribution of IT tasks in a supplier network and between user organisations and providers. This is one area where the IT industry falls behind aviation. Our Zero Outage Industry Standards started filling this gap.

How challenging is it to create standards that take into account technology that is the result of less planned convergence like IoT, rather than those being the result of deliberate design & integration?

Today’s security standards do not really consider the flexible composition of deliberately designed IT services. However, this is everyday business e.g. in cloud services. Standard elements are selected from service catalogues and assembled or integrated to a composite, user-specific IT service. That’s why security standards have to be organised in a hierarchical and thoroughly modular way. Our Zero Outage Industry Standards introduced valuable methods and tools from the ESARIS security architecture to achieve the necessary flexibility. It is planned to expand the approaches to IoT, OT etc. since these IT environments are also not designed as monolithic, ring-fenced or siloed IT stacks.

In a talk you gave, you made a very compelling series of comparisons between the aviation & IT industries - both are technologically-driven, sharing complex operations with security/safety and performance as key priorities – is there more that the IT industry can learn or borrow from other sectors to improve their IT practices?

Definitely. The ATA reference and numbering system for airplanes is used as a reference for exchanging information in the supply chain including airlines and with certification bodies. The Zero Outage Industry Standard association provided the ESARIS Security Taxonomy and other means that serve a similar purpose. Modern airplanes are optimized to fulfil very specific requirements e.g. relating to number of seats, range, comfort, speed, payload, weight. Nevertheless, for cost reasons they must be produced in an industrialised way. Standardisation of "IT security" is totally underestimated though it is the key element to achieve quality and efficiency. The standards on our website treat standardisation of IT security. Last but not least, the first generations of airplanes often crashed as today's IT applications do. IT will in the near future serve applications like health and vehicle traffic. It's time to develop the standards that help improving the reliability and security of IT so that future applications do not end in disaster.

Do you think that, as with the GDPR –the introduction of strict fines would provide a good incentive for ensuring all parties adhere to agreed IT standardisation? (You noted in your talk that the aviation industry incur financial penalties for not meeting proposed flight performance) - or do the benefits of standardisation speak loud enough for themselves?

Regulation is definitely supporting and enforcing security. I would, however, not recommend to solely rely on governments, though they also played a major role in the aviation industry. In any case, the IT industry must develop the solutions itself. The IT industry wants to foster the "digitalisation" in many new areas. This requires having the power and consequence to develop new standards for better quality including high reliability and good security.

With IoT representing the largest connected network the world has known - security is a key area of concern for many. In the near future, what extent do you believe the onus for responsibility will be on users to determine the security & reliability of IoT devices/solutions, compared to the manufacturers & providers?

Users and providers are interacting via markets. Users have requirements which they consider in their purchasing decisions. Manufacturers and providers have the responsibility to care for reliability and security. But they are lowering quality to decrease costs to offer their services with competitive prices. It is important that there are rules and means balancing between users and providers. Moreover, both groups of market players need help to play their role. E.g., the buyers need to have transparency about security, and providers require means to deal with market pressure while providing a sufficient level of security. These are topics of the Zero Outage Industry Standard.

How much do you think the people factor is overlooked when businesses examine their IT infrastructure – is there more that can be done in your opinion to incorporate this (e.g. culture, skills etc.) into the idea of standardisation?

A cultural change is required in many organisations. Security managers must understand IT production not just IT. They must have a sense of costs and standardisation. They must also learn to use tools as ESARIS to manage the complexity of today's IT and IT security. Security architecture and taxonomies are important. Security managers must widen their horizon and understand the complexity e.g. in the IT supply chain. With the right approach we all can manage IT security in this environment.

There seems to be a lot of focus within businesses to innovate their IT with less on securing their current platforms in use – how do you get the message across for the need to address this imbalance?

I think that providing the means / tools / standards that considerably help people to secure IT services is the only thing that really works. ESARIS is an example that is proven and tested.

If you had to speculate, what do you think the main factors will be that will see the IT industry shore up standardisation of its IT infrastructure and practices?

The IT industry will utilise the appropriate standards, means and tools if they exist (provided that this does not destroy their business case e.g. because of costs). The main driver will be the new emerging markets like health which have difficult reliability and security requirements as I stated above. I hope that the IT industry learns to care for security before these businesses are actually digitalised and automated using IT.