ICS
CYBER SECURITY

IMPROVING CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS:

Rebuilding the OT/IT relationship

Thoughts from Andy Oliver,
Technical Management Solutions

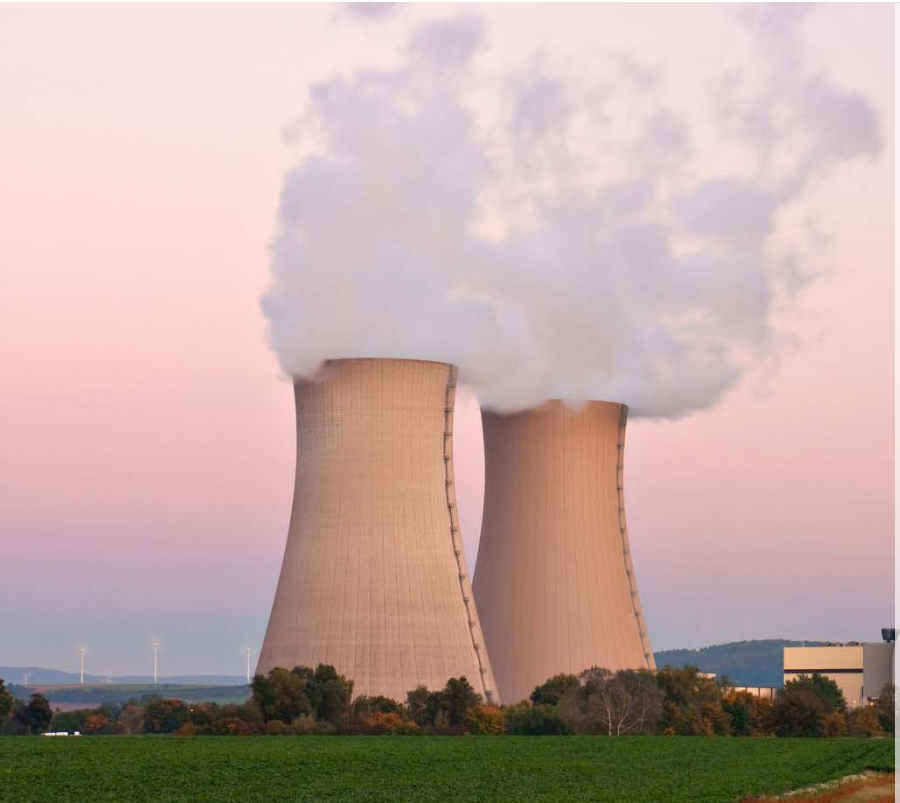
Introduction

While the majority of companies have implemented cyber security solutions for their industrial control systems, they are not yet addressing the gap between OT and IT and thus, the risk it creates. The issue now is to mitigate it by improving the communication between the two departments and assess who is responsible for cyber security and what should be done to improve it.

Ahead of the ICS Cyber Security 2018 conference, we had the opportunity to discuss with **Andy Oliver, currently working on assignment as Project Manager for OT Cyber Security at a major pharma company,** on the need for a OT/IT convergence and what strategy companies need to implement to ensure the digital safety of their organisation.

I'd like to start by you giving me a bit of a context on ICS and the relationship between OT and IT.

This is a big topic. In summary, I guess what's really happened over the years is that IT and OT progressed towards the same point, but on parallel paths.
IT, over the last 20 years, has been going down a path of rapid technology turnover. There has been a focus for big corporations on IT productivity and getting their business value out of the IT. That has meant a lot of sameness, a lot of scale, a lot of standardisation.
OT, on the other hand, has been really driven by the needs in the moment of the particular problem that they're trying to solve. For example, if you're building a new chemical asset or a bit of critical infrastructure, OT is asking 'What is the best fit?'. There may be some strategic direction in that, because companies may want to choose from the same supplier or same set of suppliers.
If you go back a long time, OT systems were very proprietary. They would run on proprietary hardware or software, all supplied by the vendor. They weren't connected to anything and were the digitalised version of the analogue system. Frankly, that was fine until OT started to drift into the more traditional IT space, and in particular connectivity to the internet and the associated security risks that come with that. The OT space doesn't have the same level of cyber security maturity as IT and learning lessons from it and building on it and making it OT-specific is the real trick, I think. That's where I believe the industry needs to go. Enlightened companies, those that have been addressing their cyber security protection in critical infrastructure or the oil and gas have come to a way of doing it.
They have developed international standards and they are using them as the bedrock and building on that to layer in their own security.



"Over the years, IT and OT progressed on convergence to a certain degree, but on parallel paths"

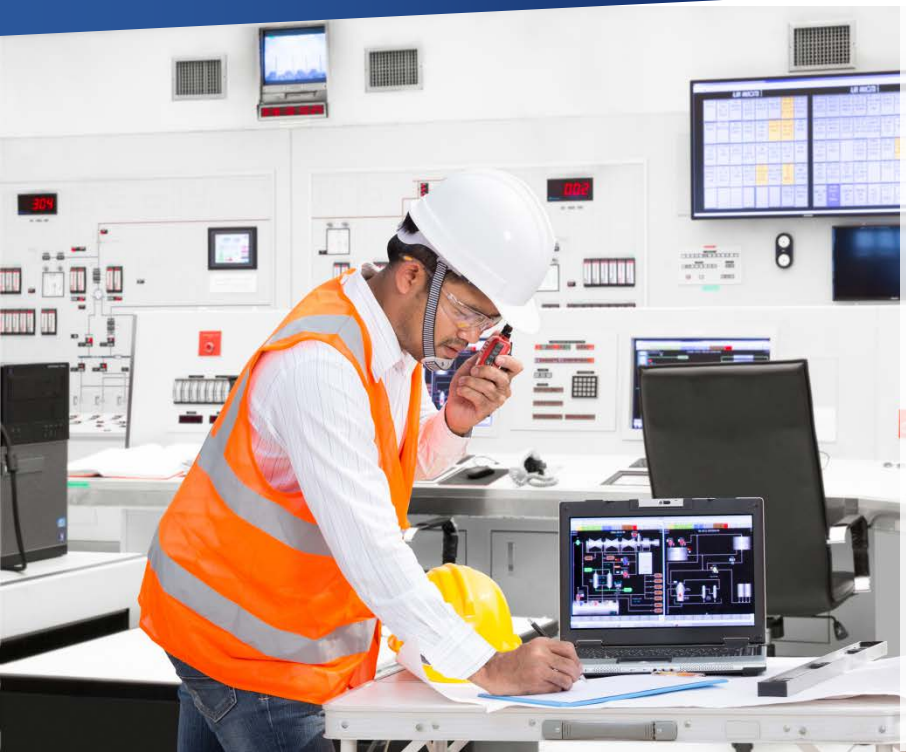
What do you believe is the next phase, in terms of cyber security, of a strong relationship between OT and IT?

That's a very good question. The real link, ultimately, is organisations understanding the risks that they have, the threats to their organisations, and most importantly the likelihood of a significant incident. That is what is going to connect these two because enlightened boards and other organisational teams should be aware of the risks, both in their IT AND OT space. They need to be in a position to manage that and understand what that risk is, how much risk they're accepting and how much they want to spend to mitigate that. Elevating this subject up to the ones who make the decisions is what is really going to bring IT and OT together. I don't think the connection between the two will be technological, it is ultimately all about business.

> *"Enlightened boards and other organisational teams should be aware of the risks, both in their IT AND OT space"*

Who should address cyber security in an organisation, between management, IT and OT?

In an ideal world, senior leaders would start asking questions about the extent to which the company relies on OT and what risk its OT estate and environment represent. This is the kind of discussion you want to get to, because that will start the dialogue, which will lead to an assessment, which will then lead to action. Just landing the problem of OT Security onto the already full inbox of the IT Chief Security Officer may not be sufficient as they might not have the background nor the visibility; it needs to be in collaboration with the Manufacturing or Supply Chain leadership as well.



> *IT is optimised around cost and to a certain degree, around security. OT is optimised around availability*

What would you say is the current main issue between IT and OT? If you had to pick the main one, what would it be?

I would say it's a question of focus. If you look at big corporations and the way they generally run their IT, you can see it being standardised and optimised around cost and to a certain degree, around security. If you look at the OT space, it's optimised around availability. A perfect example of that is if you get a problem with one of your company laptops, the organisation is quite happy to say, “well, we'll shut it down and we'll look at it when we get to it.” And that might take four or eight hours, but that's the service-level agreement that you have to accept. That would be unacceptable in the OT space because it's generally managed in real time and you cannot afford to shut down the associated business. It is such a different focus.

In a sense, you don’t want to change the situation, because you cannot change the principal focuses and objectives of the businesses that are using OT into IT or vice-versa. What can be done is to recognise that there are two different states in the organisation and even though they share skills and techniques, they need to be managed differently. Ultimately we need to recognise that these two departments have to coexist. The convergence really happens when an OT estate starts using the IT infrastructure, such as the corporate internet and intranet connectivity. That clearly is an overlap and the organisation needs to decide how to manage that, where the ownership lies and who manages the support and the response features in case of an incident. I have seen organisations successful in creating an OT computing or an OT/IT sub-organisations to manage that grey space

What are the three main advantages in working towards an IT/OT convergence?

Well, that presupposes that you're going to achieve IT/OT convergence. I tend of think of it more as coexistence than I do convergence, as coexistence implies both sides understand what is being done in the other area and they both understand the risk they share.

- Ultimately, the first big advantage I can think of is if organisations reduce their risk profile and shine a light on protecting their organisations from cyber security threats.
- The second point is that there is something to be gained if an organisation understands what OT it has and what it means to the business. When you look at those organisations that are quite immature as you engage stakeholders, this is a huge advantage for the education and awareness around the issue. Some leading questions might be: are you aware of all the OT elements you have in your organisations that run your business? Did you realise the degree of criticality they may have? What can we do to collectively help with this and what skills do we need?
- This leads me to my third point: it is all about upskilling your organisation and providing opportunities for people to cross that wall and do both OT and IT roles.

If we keep this coexistence in mind, who is liable for the cyber security of the organisation?

I've seen in some instances the Chief Information Security Officer or the Head of Manufacturing or Supply Chain getting on board and leading this type of work. It is really for an organisation to decide where the best focal point is to know what needs to get done and how to turn that into action.

Has the discussion on cyber security around the OT space already started?

There is a broad range of stages organisations are at. Some will be advanced in terms of their thinking, their application and their execution. They will have a well-established cyber security programme in the OT space, and they will have executed a number of projects to reduce risk and protect against threats; they will have a mechanism for future strategy and future projects and implementation. Others will be very early on the journey and wondering what the next step is. In any case, every organisation will reach a point when they have to consider who "owns" OT security; is it IT, OT or a combined organisation?

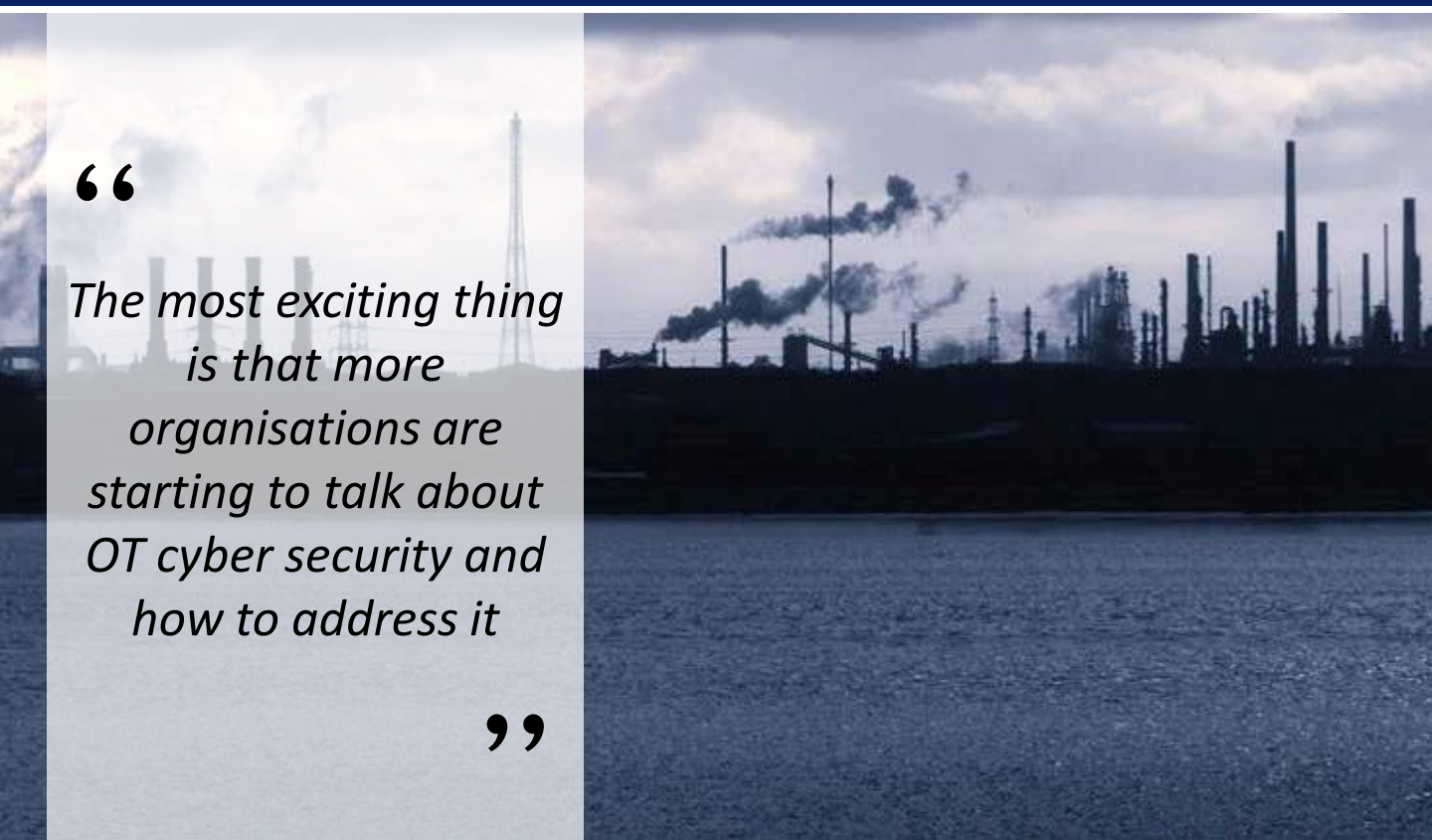
There are two kinds of triggers for this discussion to happen. The first one would be strategic, top down where the organisation wants to develop a cyber security for OT strategy and appointing someone responsible for developing programmes and executing projects. The other is more tactical and comes out of the execution of projects where the need for OT security governance becomes apparent.

Who is currently leading the industry in terms of ICS cyber security?

From what I've seen, the oil and gas sector, the nuclear industry and other elements of critical infrastructure are quite mature in their cyber security approach. I am not quite sure about defence and the military as I've not worked with them but I assume they are quite mature as well.

Have you seen any key exciting developments that you believe others should follow?

I'm a delivery person, and it's my role to help companies get from A to B, to either develop a strategy or execute the one they already have. Whilst it's tempting to get excited about the latest technology, and that's certainly a key component, I tend to think that the most exciting thing is in terms of how organisations are approaching the delivery of OT security programmes.
I suppose the most exciting thing is that more organisations are starting to talk about OT cyber security and how to address it.



How do you see the future of ICS cyber security in the next five years, in relation to the IT/OT relationship?

We will begin to see companies that will start to think less in terms of just straightforward technology but more strategically in terms of the governance around IT and OT: how to get the best out of the overlap and make those two exist in a secure and profitable way.
I suppose organisations are looking for the magic formula and unfortunately there isn't one. It took strategic thinking and a will to change things for organisations that have succeeded and it did not happen overnight.
The biggest hurdle in working towards an OT/IT coexistence in an organisation is the huge amount of change it will provoke. Each organisation has to find out their own way and has to help people through that change curve.

The key thing is to take the first step!