Governance Institute of Australia

# Cyber health and safety: Directors' duties

*by* **BLARE SUTTON** *Partner, McGrathNicol Advisory*

- Operational technology is being adapted for competitive benefit but it is not subject to the same level of scrutiny as traditional IT.
- Changing the lens of cyber resilience must include the safety of people.
- Understanding true cyber risk requires bringing both IT and OT together.

Almost every week a new cyber incident hits the media — personal information released on the dark web, Silicon Valley tech giants causing public outrage due to unethical collection or use of data, or accusations of state sponsored espionage.

Locally, we are seeing wave after wave of high profile cyber incidents, from Melbourne Heart Group's targeted malware attack encrypting the medical records of 15,000 patients, to the valuation records of Landmark White 137,500 customers being released on a dark web forum, and even the Australian parliament computing network being breached. While the media appears to be focused on high profile issues involving privacy, interference or financial losses, there is a disturbing lack of publicity about the increasing risk to what we should all hold most dear — the potential impact on human life.

It is not difficult to see examples of operational technology (OT) being adapted for competitive benefit — it is now commonplace for utility suppliers to fit remote flow and valve sensors to its distribution network to improve maintenance cycles and reduce field operation overheads, or transport companies to deploy internet enabled GPS transponders to vehicles to collect and improve delivery routes and response times, and even construction firms implementing remote electronic control systems to reduce operating costs. Each of these is an example of new technology being deployed by operations to drive efficiency, and more often than not, done outside of the standard IT controls framework.

> ...as technology is deployed more frequently outside the boundary of traditional IT environments to enhance the efficiency of those workplaces, directors and their boards can't assume that the controls they have in place are being applied to OT.

There should be no doubt that the increasing use of technology in the race to be faster to market and more efficient in the manufacturing, sale and supply of goods is changing the ownership of the cyber issue from the IT manager's office to the boardroom. Since Safe Work Australia released a set of model laws through the introduction of the federal Work Health and Safety Act in 2011, company directors throughout Australia have had a direct legal duty to implement and monitor systems to ensure safe working conditions in their workplaces. This includes a positive obligation to demonstrate due diligence in relation to workers health and safety, and as technology is deployed more frequently outside the boundary of traditional IT environments to enhance the efficiency of those workplaces, directors and their boards can't assume that the controls they have in place are being applied to OT.

We can tell that OT is not subject to the same level of scrutiny as traditional IT simply by looking at the many industry surveys that are conducted each year on the occurrence and impacts of cyber incidents. Last year more than 25 per cent of businesses experienced a cyber incident. However, if we examine organisations that have deployed OT (such as Industrial Control Systems or ICS, connected sensors and monitoring systems, controlling or providing information about manufacturing, production and supply), this exposure increases dramatically to almost 75 per cent. In fact, last year 15 per cent of cyber incidents affecting operational networks resulted in damage to the equipment it was connected to. What this tells us is that while efforts are being made to protect traditional IT systems, we are not seeing the same level of maturity applied to technology deployed in the field or on the factory floor.

With the media firmly focused on popular topics like data privacy and state sponsored espionage or political influence, you could be forgiven for thinking that the risks to OT are not real. However, in between the populist cyber noise you may have missed the reported OT cyber issues that the cyber researchers and hackers have picked up on:

- In 2015 Chrysler was forced to recall 1.4 million vehicles because their engines could be remotely turned off via a security vulnerability. At the same time, a UK-based firm demonstrated that they could compromise braking systems of cars through their entertainment systems by injecting commands into a digital radio station. 2016 saw US authorities urging caution for consumers and organisations connecting aftermarket products into vehicles' onboard diagnostic ports, subsequently followed up by Argus Cyber Security remotely stopping the engine of a moving vehicle using the Bosch Drivelog device connected to a vehicle's ODBII port.
- We saw the advent of the 'NotPetya' attack in 2017, which took the radiation monitoring system at a nuclear power plant offline and crippled the operations of several large organisations including Maersk, Saint-Gobain, DHL and Mondelez International. The cost of the attack is estimated in the tens of billions, from which others still have not learnt, with security firm INSINIA demonstrating in 2018 that they could take control of 'modern' industrial control systems using only four lines of malicious code, potentially costing millions in lost productivity. These ongoing vulnerabilities were highlighted by the devastating ransomware attack on Norsk Hydro in March this year, forcing the company to switch to manual operations for months while systems were restored from backup.

> This rapid adoption of technology that is blurring of lines between IT and OT now means that the physical safety and wellbeing of people can be directly impacted by the level of security in place throughout an organisation.

Changing the lens of cyber resilience to include the safety of people — because not only are people an important part of ongoing resilience, they are now directly and potentially physically impacted by cyber incidents — should not be a new concept. Throughout history the introduction of new technologies has changed the way we work, requiring organisations to identify risks to people the technology poses and to mitigate them accordingly. In the nineteenth century technological advancements brought us industrial machines, and the serious threats that they posed to people's lives in the process. In response, a variety of laws, regulatory bodies and workers' rights were established across western society to deal with the negative impacts that they pose. Today the threats we are facing are designed to first leverage a weakness in people, in order to then leverage a technology weakness, which either has a direct financial (such as theft or fraud), reputational (through defacement or data theft), or physical impact (through failure or misuse of physical equipment).

This rapid adoption of technology that is blurring of lines between IT and OT now means that the physical safety and wellbeing of people can be directly impacted by the level of security in place throughout an organisation. To date, the focus of cyber resilience has been largely on financial or reputational risk, and with the adoption of inter-connected OT this focus needs to change. By now, most organisations should be well down the path of executing their cyber resilience strategy or, at least, are asking the right questions to begin that journey, such as:

- What critical or 'high value' data do I have?
- How is it integrated in my business and in particular, my approach to technology?
- Who has access to it?
- What governance framework, controls and technical capability do I have to adequately protect myself?

Knowing all of this, an organisation can then develop a plan that takes into account current capabilities and seeks to mitigate the identified risks. But how does this journey remain agile and evolve as a business grows and adopts technologies that might be outside the remit of IT? As we have already identified, effective evolution requires a broader cyber risk lens and an investment in people to collaborate collectively across the organisation and the entire supply chain. This can be summarised in three further questions:

- Do I have a holistic view of how technology is used throughout my entire organisation?
- Is the use of technology increasing the risk of harm to my people, or the people around me?
- Are my people and trusted parties adequately prepared to help me defend myself?

Understanding true cyber risk requires bringing both IT and OT together so that they can understand each other's systems, operating priorities, vulnerabilities and what the actual enterprise attack surface is. Once this has been achieved, the organisation is then able to apply a consistent application of risk and governance standards to improve enterprise wide resilience. Importantly, taking this approach will require an investment in your people — you will need to cross-train your IT and OT professionals (either formally or informally) — but as a result they will each bring their own unique perspectives to each other's domain.

The industry trends, backed by available data and current events, all indicate that a well-constructed cyber resilience strategy should include a dedicated stream aimed at increasing people's awareness of the cyber risks associated with the use of OT and should evolve as the risks and threats to a business evolve. If this is approached from a health and safety angle, then we are more likely to see our people take a personal interest in protecting themselves and their colleagues, resulting in heightened awareness and improved resilience across the entire organisation. This outcome is not only desirable, it will protect company directors from the penalties for not complying with their obligations.

Blare Sutton can be contacted (03) 9038 3190 or by email on bsutton@mcgrathnicol.com

McGrathNicol

*Material published in Governance Directions is copyright and may not be reproduced without permission. The views expressed therein are those of the author and not of Governance Institute of Australia. All views and opinions are provided as general commentary only and should not be relied upon in place of specific accounting, legal or other professional advice.*