# Interview

## How businesses can get ahead of critical infrastructure requirements

Paul Zalai, Director at Freight & Trade Alliance (FTA) recently sat down with Steve McSweeney, Director Strategic Accounts at Certis Security Australia to look at the above topic.

**1. Paul Zalai – Steve, last year Certis hosted a briefing with the Australian Border Force and freight forwarding executives. Have there been any major security developments on your radar since then?**

The biggest security development has to be the recent changes to the Critical Infrastructure (CI) Bill, which are specific to multiple industries, including freight. This Bill is continuously being discussed and tweaked, but as you can imagine, is a very important focus for Australia. Part of the new requirements for relevant organisations (i.e., those that manage critical infrastructure) include submitting a risk assessment to the government each year, incorporating cyber and physical attacks. As part of this risk assessment, organisations will have to outline various strategies to reduce risks.

In addition, real-time acknowledgement and reporting of cyber breaches to CCTV software and Electronic Access Control Systems are paramount to the new requirements of the CI Bill.

**2. Paul Zalai - What kind of organisations does the Critical Infrastructure Bill refer to?**

The regulation of critical infrastructure under the Security of Critical Infrastructure Act 2018 (the SOCI Act) now places obligations on specific entities in the electricity, communications, data storage or processing, financial services and markets, water, healthcare and medical, higher education and research, food and grocery, transport, space technology, and defence industries, so almost everyone is affected!

The SOCI Act was amended to strengthen the security and resilience of critical infrastructure by expanding the sectors and asset classes the SOCI Act applies to and to introduce new obligations. The Department of Home Affairs website has some great fact sheets to help understand who is affected and how.

**3. Paul Zalai - How is Certis helping customers meet these requirements?**

We're working closely with our customers and partners to ensure they're compliant and have all the resources to mitigate risks. For example, we provide access to real-time data for accuracy and ease of reporting. This includes access control information and CCTV recordings, which help to identify breaches and issues in a timely manner. Additionally, we can assist with physical security reviews & assessments, helping identify vulnerabilities for remediation.

**4. Paul Zalai - Is security simply a case of supplying enough personnel and CCTV cameras, or have we evolved from this with other technologies?**

Security has evolved significantly to go beyond just having security personnel and CCTV cameras. It's much more complex and integrated now with broader business operations. For example, we're using analytics as part of our security solutions to glean insights on how sites can be pro-actively secure, or operational response times can be improved. Additionally, we're also incorporating drone usage into our patrol services to increase safety for frontline personnel and gather additional CCTV data for further operational insights.

Technology is evolving rapidly, and we're constantly innovating and looking at ways the latest technological advancements can be integrated to improve the solutions customers' experience. While ripping things up and starting from scratch is sometimes the solution, it's not always the answer; in many cases, it can be a matter of tweaking existing solutions so they are utilised more efficiently

**5. Paul Zalai - It's not just customers who need to pivot. How has Certis adapted to recent policy changes?**

Security is an always-on task, and whether you're talking about physical or cyber, it can't be a set-and-forget approach. As such, we're working with customers to help them establish a culture of proactivity in relation to physical and cyber breaches, just as we have done. This requires having clear visibility across all aspects of the business and access to real-time data so potential issues or breaches can be addressed as a priority. The use of real-time data is imperative today; there's no room for weekly reporting as the information becomes outdated and damage can be done, whether physical or cyber, so quickly. The biggest change we've implemented over the last few years, and one we're working through with customers, is to build a culture of security that is ingrained into all levels, from frontline personnel to management.

**6. Paul Zalai - Who should be involved in security planning? What would their role be?**

Security of people, systems and property impacts the entire business operations, so it's a conversation that should involve leaders of all facets of the business. Obviously, if we're talking about cyber security then people such as the CISO or CIO should be a part of the conversation, but equally so should the CEO or COO and Risk Manager.

The security planning should also be communicated to every individual of the business so there is visibility across the whole company, not just the leaders.