COME TOGETHER

Lucas Young *examines the importance of managing security risks with partnerships and reveals how customers and manufacturers can cooperate*

Critical National Infrastructure (CNI) operators face the perennial challenge of developing and managing a security strategy in a complex and ever-changing landscape. Security managers have to consider both current needs while ensuring an operational capability to face future threats. A long-term approach to technology and manufacturer selection is fundamental to success, but this is sometimes forgotten, with added weight given to technology specification and price.

When working for many years as a security consultant in hostile environments and as a segment lead for one of the larger security tech firms, one gets familiar with the tendency for clients to embark upon a procurement path for a technology that they might not fully understand. This problem is on occasion further exasperated by procurement teams who might not either understand the security landscape, the threat or the potentially devastating consequences of getting it wrong.

Part of the problem starts early during the request for information (RFI) stage when the organisation shares with potential suppliers their 'problem statement' and a framework of technical specifications with which the respondents need to comply. Problem statements have improved significantly in recent times, providing the respondents with a much clearer idea of what the real challenge is. However, the technical requirements remain a challenge.

> PROOF OF CONCEPT IS A GREAT WAY FOR ORGANISATIONS TO TEST OUT NEW CONCEPTS

These requirements are understandably written around two knowns: firstly, the technology that is either known to exist or to have worked in the past and secondly, the known challenges which the technology must provide a solution for. This invariably results in potential suppliers proposing outdated technology. This increases the risk of excluding precisely those manufacturers and technologies needed to solve the security challenges.

An increasingly popular approach to the challenge of gaining an appraisal of what technology is available and reducing the 'unknown' is a pre-procurement market engagement exercise. Market engagement allows the buyer to reach out to a broad market and gain an appreciation of the solutions available today, but rarely does this process allow for respondents to expand on what technology will be available in the future, be it next month or next year. And when you consider how lengthy procurement processes can be, particularly in the public sector, it will invariably mean the selected technology is outdated and offers poor value for money by the time it is procured, installed and finally commissioned.

Like any challenge in security, there is no single solution. It is more about adopting a process. In the case of security technology, an organisation wanting to be able to make the right procurement decision needs to adopt an approach of developing trusted partnerships with their supply chain and particularly the manufacturers. Manufacturers, who want to understand their market, their customers and specifically those challenges affecting their customers, will be keen to form a relationship which is mutually open and breeds trust.

A direct relationship with any end-user, but particularly in a key strategic market like critical infrastructure, is invaluable to a manufacturer. Even more so to those whose route to market is through an extended supply chain. Meetings and conversations held with customers are a golden opportunity to gain an appreciation of the operating environment, challenges, constraints and concerns faced by the customer. It is this information that shapes product development, feature sets and standards. And nowhere are these more important than in critical infrastructure.

Critical infrastructure operators and owners will share many challenges, but individual organisations and even individual sites will also often have their own unique requirements to mitigate common threats. Manufacturers want to be able to produce devices at scale. This will typically mean producing technology which has multiple purposes. To design a device that's applicable in numerous use cases manufacturers must take into account a broad scope of possible customer applications and requirements. For airports that could be a deeper understanding of other operational technologies and sensors with which the security sensor cannot interfere. In utilities, it could be the issue of remote sites and lack of connectivity and in the energy sector it might be understanding the threat of the equipment causing an explosion. The best way to get this level of insight is undoubtedly to hear it directly from the customer.

Picture credit: Axis Communications

Sharing with the manufacturer means customers can have the most effective long term security solution

What organisation wouldn't benefit from a close relationship with its suppliers? What is there to lose? It is a reciprocal arrangement and for the relationship to be truly fruitful, both parties must be willing to be as open and honest as possible.

For the customer, this might mean sharing details around security vulnerabilities and other sensitive information. The manufacturer also needs to be willing to share everything from limitations on capabilities of its technology to potential supply challenges and even quality issues. But this all amounts to the correct solutions being applied for the right challenges and the associated risks being effectively managed by both parties, resulting in an effective security strategy.

Another significant benefit for the critical infrastructure customer is access to sensitive manufacturer technology roadmaps. We talk a lot about an evolving threat and the types of technology required to meet the industry's needs. Customers can read journals and white papers about new technology on the horizon and what amazing capabilities it has (AI immediately springs to mind).

However, what customers often see in the press are concepts and theoretical applications to an 'almost ready' technology. The reality is often somewhat different. Security practitioners need to know what is genuinely possible and soon available, and few are better placed to do that than the manufacturers. While manufacturers are understandably sensitive about what is contained in their product roadmaps, close end-user partners are uniquely placed to gain insight, allowing them to adjust their security strategy based on what they know is on the horizon.

These relationships go further than just passive access to the technology. Some manufacturing teams work with end customers, with the view to directly impact the development of the technology. Everything from product form factor to feature sets and even pre-launch integration with complementary tech, has been directly influenced by this collaborative approach. This level of sharing with the manufacturer means customers can have the most effective long-term security solution.

We have touched on some of the pre-production development work that goes into designing and

▶

producing a product and how customers might be part of that process. What the market doesn't often see is the amount of field testing the technology is exposed to.

Customers can play a significant role in this phase too, and it is often highly beneficial to both parties. The manufacturer gets the obvious benefit of testing the technology in a real-life environment, or as close as is possible, and can make pre-launch adjustments based on vital customer feedback. The customer gets a first look at cutting-edge technology. Often referred to as a Proof of Concept (PoC) or a Technology Trial, it is a great way for organisations to test new technology concepts with the view to helping shape the security strategy and influencing the procurement process.

INDIVIDUAL SITES OFTEN HAVE THEIR OWN UNIQUE REQUIREMENTS TO MITIGATE THREATS

So, why are these manufacturers so keen to share and partner with the industry? Well, first they are out there, you just need to know what to look for. The advice to any operators in critical infrastructure would be to first truly understand their own security strategy, which will highlight the threats one is facing as a business. It may even indicate the types of technology a company should be looking for.

The next step is making a shortlist of those brands that meet any internal policy requirements that might exist around supplier selection criteria and to then take a closer look at those companies to find out who has successfully worked with large corporations in the past. It is unlikely that any manufacturer will have critical infrastructure case studies publicly accessible on their website, but many large companies, financial institutions and banks, for example, have very stringent supplier selection processes and evidence of their custom is a strong indicator of their suitability.

After this research, it's useful to talk to the manufacturer, ensuring they have local representation and technical support on a scale that will meet your needs. Reaching out to them helps to understand how long it takes for them to respond. A fast and positive response at least indicates they are set up to service end users.

It's also key to establish if the manufacturers have a 'dedicated end-user' team and get a feel for their knowledge and experience of the sector. Most organisations will have a Pre-Qualification Questionnaire to dig deeper into a supplier's suitability, but at the very least they must ascertain what policies the manufacturer has in place to inform their customers of any of their vulnerabilities. What does their supply chain security look like? Can they evidence their compliance to the regulatory framework?

Lastly, talking to one's point of contact in government, who is responsible for Critical National Infrastructure, can help to be pointed in the right direction.

The vast majority of procurement and security professionals in critical infrastructure are leaders in their respective fields. But as the threat evolves, so must our security. In an environment where the only thing that might move faster than the threat is the technology to counter it, the industry must demand more from manufacturers. But like any relationship, it needs to be mutually beneficial and based on openness and trust ●

Lucas Young, Segment Lead, Critical Infrastructure (Northern Europe) at Axis Communications is responsible for critical infrastructure and transportation verticals for Axis Communications in the UK. Lucas comes from a risk management and security consultancy background and has worked around the globe in both operational and commercial roles.

It is vital the correct solutions are applied for the right challenges and the associated risks are effectively managed by both parties

Picture credit: Axis Communications