tyco | Cyber Solutions

White Paper

Selecting a Trusted Cybersecurity Partner

In the physical security industry, there is a general perception that cybersecurity is someone else's responsibility. From the end-user's perspective, the integrator is required to install and configure equipment that meets their security policy. From the integrator's point of view, the end-user is responsible for specifying their particular cybersecurity requirements. Therefore if there is a gap in the requirements the deployment is also likely to have gaps in protection. While some products include cybersecurity features, proper configuration may require action by the integrator to enable the protection. Furthermore, security updates most be applied as they become available.

The truth is that cybersecurity is a shared responsibility where everyone owns a part of ensuring that a system is properly protected from cyberattacks. The media is constantly reporting on new cyber attacks on security and Internet of Things (IoT) products.

Many of these products have not been properly secured – becoming easy targets for hackers. In addition, as today's news headlines demonstrate, these products are not just targets but can become weapons hackers can use for formidable attacks against others. To reduce the risk to your organization and others, a physical security system needs to be specified, designed, configured and maintained in a secure manner that is effective in reducing its vulnerability to attacks.

To be effective, you need to understand the capabilities of the suppliers' equipment and the processes they have in place. The key areas to learn more about are the supplier's processes regarding secure development and response support.

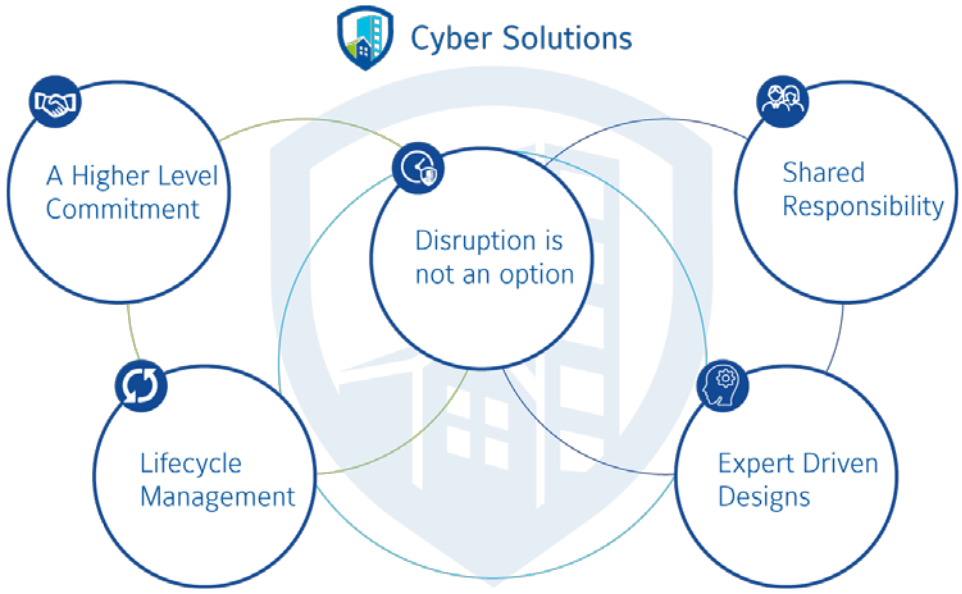
Supplier and Product Selection

Secure Development

Including cybersecurity during the development phase of a product is critical. The intent is to create a product which is designed to:

- Include necessary security features and capabilities
- Minimize the attack surface
- Reduce product vulnerabilities

The manufacturer should follow a Secure Development Lifecycle. This ensures that the right security requirements and analyses occur at appropriate times in the product development lifecycle. This ensures that security is designed into the product and is not an afterthought.



Product Security Incident Response

Cyber threats are ever evolving as such products need to evolve to address new challenges. Independent of a well-designed and hardened system security events can still occur and the support of the supplier is crucial. When a security issue is suspected the supplier should have the capabilities to investigate and provide guidance such as mitigation steps, and if necessary issue a software update or patch. Suppliers with more mature response programs incorporate active threat intelligence into their security operations.

Conclusion

Integrators and end-users should take a proactive role regarding the specification, selection, and deployment of physical security systems. With a strong cybersecurity component within project specifications more capable suppliers and products can be selected to reduce the risk associated with cyber threats. It is also important to align with integrators that can sufficiently design and deploy the physical security solutions to maximize protection. When validating a suppliers cybersecurity capabilities and practices the following questions maybe used to start the conversation:

- Do you have a dedicated product security team?
- Does your security team include cybersecurity experts?
- Do you follow a Secure Development Lifecycle (SDL) process?
- Do you have a dedicated Product Security Incident Response Team (PSIRT)?
- Do you publish product security advisories?

With these questions, you can get an understanding of the capabilities and processes the supplier has in place to develop, test and support the products you need.

tyco

Cyber Solutions From a Trusted Partner

Gain peace of mind with cyber-resilient systems focused on your security needs. Johnson Controls takes a holistic, organization-wide approach:

- Cyber Solutions tailored for the unique needs of buildings
- Emphasis on cyber protection at every phase – design, deployment and maintenance
- Secure product development
- Daily tracking of potential threats
- Rapid incident response
- Investment in continually evolving capabilities

Above all, we execute with rigorous discipline – because we understand what's at stake for you.

Johnson Controls

At Johnson Controls, we transform the environments where people live, work, learn and play. From optimizing building performance to improving safety and enhancing comfort, we drive the outcomes that matter most. We deliver our promise in industries such as healthcare, education, data centers and manufacturing. With a global team of 105,000 experts in more than 150 countries and over 130 years of innovation, we are the power behind our customers' mission. Our leading portfolio of building technology and solutions includes some of the most trusted names in the industry, such as Tyco®, York®, Metasys®, Ruskin®, Titus®, Frick®, Penn®, Sabroe®, Simplex®, Ansul® and Grinnell®.

For additional information, please visit www.johnsoncontrols.com/cyber-solutions or follow us on Facebook, Twitter, and LinkedIn.

Johnson Controls