TÜVRheinland®
Risktec

RISKworld / The Newsletter of Risktec Solutions / Autumn 2020 p4-5

Cyber Essentials – A holistic approach to reducing the risk of cyber-attacks

It may be surprising to learn that a well-designed computer system that is not connected to the internet can still be compromised by a cyber-attack. For example, 'sleeper' malware implanted during the design of a digital system can manifest itself many years later. The damage caused by such cyber-attacks can be significant and has been well documented following high profile incidents in recent years. As cyber-attacks become more sophisticated and continue to evolve, how can we best reduce the risk and assure ongoing cyber security?

WHAT IS CYBER SECURITY?

Cyber security is a collective term used to describe the measures put in place to reduce the risk associated with cyber-attacks. It has been around for about half a century since the advent of computers and the invention of the internet. Initially focused on the protection of Information Technology (IT), cyber security has evolved to embrace Operational Technology (OT) as digitalised industrial automation and control systems have become prevalent.

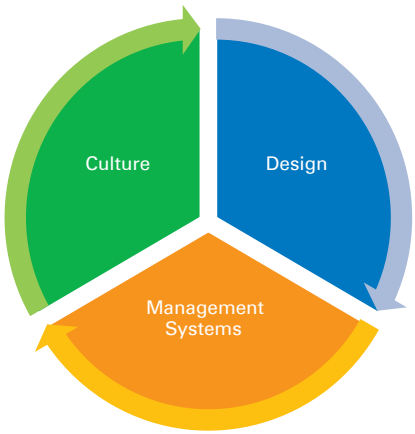

Figure 1 – Cyber security risk reduction enablers

Over the years considerable effort has been expended in managing the cyber threat via design measures, such as air gaps and fire walls, but with the ever changing landscape of cyber-threats, which are evidently able to infiltrate IT and OT, it is essential to widen the focus if we are to effectively manage the risk.

The holistic approach incorporates the three complementary cyber security risk reduction enablers illustrated in Figure 1, namely design, management systems and culture, applied throughout the IT or OT lifecycle; and integrates with physical aspects of security.

SECURE BY DESIGN

Design is potentially the most effective of the three enablers. It is best considered alongside a cyber security hierarchy of controls (see Figure 2) to help prioritise possible cyber security measures.

The preferred option during design is to eliminate the potential for a cyber-attack (e.g. design analogue or passive OT systems) or eliminate paths for cyber-attacks (e.g. system not connected to the internet or other IT systems). Next, consideration should be given to reducing cyber-attack paths in the design of the system (e.g. reduced number of logical entry points).

Design robustness is crucial. It includes the design of a defensive system architecture as well as software programming measures to ensure system confidentiality, integrity and availability. A Cyber Security Risk Assessment (CSRA) of the system design against a broad range of threat actors and sources, including blended cyber and physical attacks, will identify the need for any additional requirements.

These may lead to active systems (e.g. system monitoring) and/or control measures (e.g. procedural security measures or applying the principle of least privilege) and/or physical security measures (e.g. hardened cabinet for digital equipment or physical port blockers for connection points).

MANAGEMENT SYSTEMS

Effective cyber security requires cyber security processes and procedures to complement the design measures. These need to be in place and followed not only during the use of the OT/ IT system but throughout its entire lifecycle, from initial concept, design and manufacture, right through to operation, upgrade and eventual removal.

Furthermore, the procedures should be embedded not just within the organisation operating the system but also its associated supply chain. During the system design or build, for example, a latent cyber threat introduced into the system by a supplier may remain undetected and can be exploited years later as the basis for a cyber-attack during operations. During maintenance or upgrade, portable devices used to upgrade software can provide a convenient path for a cyber-attack on systems that have been air-gapped from the internet.

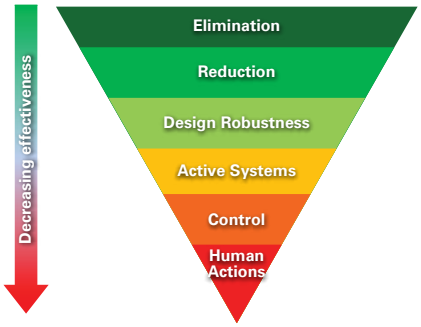

Figure 2 – Cyber security hierarchy of risk controls

The management system specifies when the CSRA should be carried out. Typically, this would be periodically at set intervals but should also be considered in response to known developments in the cyber threat, any internal or external cyber security incidents, or system upgrades and modifications.

Informed by the CSRA, a broad range of cyber security processes and procedures will be required. These will cover the use of the digital OT system, the use of the IT platforms on which the design, maintenance or upgrade of the digital system is carried out, as well as personnel vetting and aftercare, and regular testing of the system. Particular attention needs to be given during the development of these processes to address the insider intent on causing harm, either directly via a cyber-attack or via a combined cyber and physical attack.

CULTURE

The effectiveness of a robust system design and management system in reducing the risk of cyber-attacks can be compromised by the actions of people interfacing with the system, whether intentional or not. This could include inadvertently opening up a phishing email or connecting an infected USB stick to an IT or OT system, or simply not adhering to logical access control procedures.

A proactive security culture will drive the desired behaviours within the operating organisation and associated supply chain. Effective security requires motivating people to comply with well-defined procedures. Crucial to success here is the visible commitment of leaders to security, as well as providing cyber security awareness and refresher training for all personnel. Developing a mature security culture does not happen overnight; it takes time and continuous effort, but is as important as the other elements of the holistic approach.

INTEGRATION WITH PHYSICAL SECURITY

Overall security against the many potential cyber threats will depend to differing degrees on both cyber security and physical security. For instance, a knowledgeable insider (e.g. a disgruntled, radicalised or coerced employee), can present a specific challenge to cyber security which may only be effectively countered by non-cyber security measures. These could include physical security measures (e.g. hardened buildings or rooms, and access control), procedural measures (e.g. two-person rule), or may involve the deployment of the site security force.

More generally, understanding the defence in depth offered jointly by cyber security and physical security against specific threats and the trade-offs available can help optimise the overall solution.

CONCLUSION

Cyber-attacks on digital systems have the potential to cause significant loss. Rapidly changing and sophisticated cyber-attacks present an increasing challenge against which robust cyber security design and testing of digital systems is no longer sufficient.

A holistic approach which considers the three risk reduction enablers of design, management systems and culture throughout the different stages of the system lifecycle, in a way that also integrates physical security, is required to effectively reduce the risk of today's evolving cyber-threats.

Contact: John Llambias
enquiries@risktec.tuv.com

Information: Cybersecurity Trends 2020, https://www.tuv.com/landingpage/en/cybersecurity-trends/