Cybersecurity in the Nuclear Industry The Need for Strategic Cyber Risk Management

By **Rhonda Evans, Jean Llewellyn OBE, Roger Howsley,**

SUMMARY

In a global survey of over 700 security practitioners in 98 countries, the World Institute for Nuclear Security (WINS) found that the top priority across all continents and demographics was cybersecurity. The results, published in February 2020 [1], found that a cyberattack on a nuclear facility was considered much more likely than a physical attack. This conclusion points to the need for greater understanding of cybersecurity threats amongst nuclear facility staff and the professional capability to prepare for and, if necessary, respond to cyberattacks. The paper sets out the importance of cybersecurity risk reduction in the nuclear industry and the means by which this can be achieved, highlighting the approach and recommendations developed through WINS' research and publications on cybersecurity [2] as well as its professional development programme about cybersecurity in the nuclear industry [3].

The paper in brief:

- establishes the context of cybersecurity for the nuclear industry having regard to cyberthreats, cyber targets, cyberattack vectors and the nature of cyberattacks
- highlights the importance of raising awareness among all stakeholders within the nuclear industry of the vulnerabilities that may be exploited by cyberthreats to mount successful cyberattacks
- recognises the increasing digitisation of systems and the evolution of human technological interface as a key risk to be managed
- directs attention to the importance of risk reduction through attention to cyber risk, risk mitigation and assurance processes that organisations should undertake to reduce risk and promote cyber resilience.

1. RELIANCE ON COMPUTERS AND COMPUTER-BASED SYSTEMS

The nuclear industry has invested heavily in automation, remote monitoring and control, and real-time analysis. As ageing systems [4] in existing nuclear facilities have been modernised and new facilities constructed, computers and digital technologies are now integrated into almost all aspects of nuclear facility operations, including those supporting nuclear security, nuclear safety, nuclear material accountancy and control and emergency response.

Cybersecurity is a key strategic risk that organisations must manage to increase cyber resilience in a dynamic and rapidly evolving environment.

2. CYBERSECURITY - PROTECTING INFORMATION AND OPERATIONAL TECHNOLOGIES FROM BECOMING CYBER TARGETS

Cybersecurity is the protection of organisations, their information technology (IT) and operational technology (OT) systems from cyberattack. Specifically, the confidentiality, integrity and availability of information on these systems must be protected.

While cybersecurity is well defined in relation to IT systems (in the ISO 27000 series of standards, for example), these controls cannot necessarily be used in the same way to protect OT systems. OT systems generally control and/or monitor physical processes. Industrial control systems (ICS) is the term used to broadly describe operational technologies (both analogue and digital) that support industrial processes [5]. The main specialised ICS that are used in the nuclear industry are supervisory control and data acquisition (known as SCADA) and distributed control systems (DCS) [6].

Most ICS used for the complex processes at nuclear power plants are DCS. The term instrumentation and control system is commonly used to describe the DCS used in safety systems. These are examples of complex control architectures. However, nuclear power plants also contain simple control systems that are dedicated to very specific and simple tasks and are not usually monitored centrally or continuously. Examples of these common control systems include automated building systems (heating, ventilation and air conditioning), building management control systems, and interior and exterior lighting systems.

Both simple and complex systems within a nuclear power plant can be subject to a cyberattack. These systems have become more and more automated and digitised to provide remote monitoring and increase system efficiencies. The remote availability of these systems, whether for maintenance or viewing, can provide a possible entryway for cyberattack [7]. All these systems, whether complex architecture or simple control systems, should be protected from cyberattack in order to ensure their availability and reliable operation.

3. CYBERTHREATS - INFORMED AND AGILE ADVERSARIES THAT MAY BE INSIDE OR OUTSIDE YOUR ORGANISATION

Individuals and groups with malicious intentions, both insiders and external adversaries, have recognised that the nuclear industry's migration from analogue to digital systems has increased the number of potential cyberattack targets. Adversaries have embraced computer-based systems as both a target and a means of cyberattack. The attackers may have

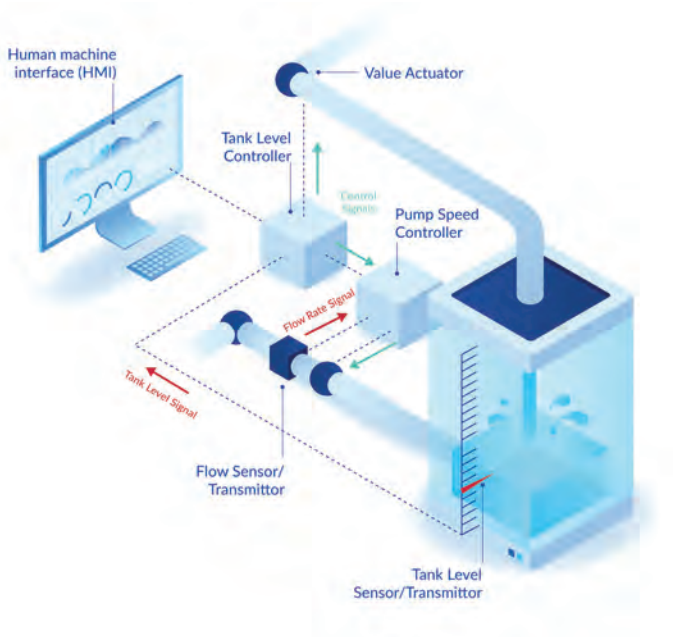

FIGURE 1: Example control system operation on a physical system

criminal, terrorism-related or hacktivism motives. They aim to affect the confidentiality, integrity and availability of information or the availability of information related to the operation of digital assets - such as controllers, actuators, human machine interface - and other key components of systems which support safety, security, nuclear material accounting and emergency response.

4. CYBERTHREATS EXPLOIT VULNERABILITIES IN SYSTEMS, PROCESSES AND CULTURE

A *cyberthreat* may be an insider, an individual with authorised access who could commit or facilitate a malicious act, or an external threat or adversary. A cyberthreat is not limited by proximity to the location of a planned cyberattack, the number of attackers they have available, or the physical security measures implemented at the facility containing a target or targets. The cyberattack may come from anywhere at any time.

Understanding the characteristics of a cyberthreat as well as possible cyberattack scenarios provides valuable information for the design and implementation of protection, detection and response measures [8]. However, identifying a person or group of people who may be a cyberthreat is quite difficult. Often cyberattacks are so sophisticated that it is difficult to determine who carried it out. The only way an organisation can deal with this uncertainty is to develop a set of cyber profiles based on an understanding of how cyberthreats may carry out their cyberattacks and the typical profiles of cyberthreats. There is no room for complacency as cyberthreats—and their associated tools, tactics, and targets—change frequently. Cyberthreat profiles used as planning tools must be updated frequently.

For a cyberattack to succeed, the system must have a vulnerability that can be exploited. A vulnerability is a flaw or weakness in a system that can leave it open to cyberattack. Cyberattacks are designed to exploit one or more system vulnerabilities. The sum of vulnerabilities of a system form its attack surface.

Many OT systems, including ICS, were designed to support engineering processes and qualities such as reliability, maintainability and availability. Cybersecurity was not necessarily an initial design consideration in many of these systems. Therefore, OT systems, especially legacy systems, have inherent vulnerabilities which may be exploited by a cyberthreat during a cyberattack.

Due to design requirements and operational restrictions, these vulnerabilities often cannot be addressed in the same way that vulnerabilities in an IT system can, as it may adversely affect the performance of the OT system. For example, numerous OT systems include computers that run outdated versions of the Windows operating system that Microsoft no longer provides patches for. In an IT environment the solution would be to update the computer to the latest version. This may be impractical for OT systems, which are normally the integration of many complex systems. A simple change in operating systems could cause the system to fail. Additionally, any change would result in downtime, lost production and lost revenue.

5. THE ANATOMY OF A CYBERATTACK

A cyberattack is often the result of extensive planning and preparation. A cyberattack can be broken down into several distinct phases that form an attack sequence [9].

The first step is reconnaissance. The goal of reconnaissance is to collect information on the potential target(s), the users and the processes from which vulnerabilities for exploitation can be identified. The cyberthreat seeks to identify vulnerabilities that can be used as an entry point or a source of information.

The next step is for the cyberthreat to establish a foothold with access to some part of the target organisation. This could be carried out by exploiting vulnerabilities discovered during the reconnaissance phase, such as in internet-connected workstations or servers or by introducing malware into internal systems. The route by which a cyberthreat exploits a vulnerability is referred to as the attack vector. Common attack vectors include phishing attacks that introduce malware or redirect users to malicious websites or introduction of malware through removable media.

Even the most sophisticated and resource-rich cyberthreats will still use one of the above methods coupled with social engineering to achieve the initial compromise. Training is crucial to make personnel aware of and vigilant against these simple methods which allow cyberthreats to establish a foothold.

Once a foothold is established, typically an externally located cyberthreat will create a connection that allows them to manually run commands to control the cyberattack or to establish routes for removing information from target systems. This covert communication is normally accomplished via a remote-access Trojan, a special piece of software providing administrative control and backdoor communications that include data exfiltration and updates to the exploit software. The internet servers supporting this communication may cause the communication to be bounced around in multiple countries, making the identity of the cyberthreat hard to determine.

Once command and control is established, the cyberthreat's next step is to gain control of the systems required to complete the mission. The cyberthreat then escalates their privileges. This process could be as simple as stealing an IT administrator's username and password, but it could also comprise a lengthy process to exploit multiple systems and bypass several layers of defence.

FIGURE 2: Illustration of cyberattack sequence

After escalating privileges, e.g. using stolen user or system credentials, the cyberthreat may move laterally through one or multiple computer systems and networks within the organisation. The goal may be to better understand the environment to craft additional exploits, to collect information, and/or search for the ultimate target.

Cyberthreats seeking to disrupt the operations of a nuclear facility may initially target the IT networks while seeking to identify a network/communications path to the engineering or physical protection systems. While a common approach to protect sensitive systems and associated assets is to make them physically isolated, or 'air gapped', pathways to compromise of the system still exist. These isolated networks can be bridged, for example during maintenance operations by test equipment and mobile media. Mobile media interchange between isolated systems, known as 'sneaker net', occurs when data or software is manually carried from one digital device to another and transferred using a physically transportable storage medium, such as floppy disks, thumb drives, portable hard disks, or other modes of data transfer. This introduces a potential vulnerability which has been recognised by regulators who generally impose specific requirements on the management of portable or removable devices [10].

Mission completion and subsequent action by the cyberthreat will depend on their motivation and intent. Mission objectives could include information collection, extortion, propaganda, sabotage, support for theft of material, and/or denial or destruction of information.

The timeframe to complete these missions varies greatly. In some cases, the intention may be to maintain a permanent presence within a targeted system. An advanced persistent threat may exist within organisations' networks for extended periods of time.

If the cyberthreat is interrupted or is conducting an event designed to have a significant adverse impact on an organisation, the cyberthreat may seek to cover its tracks and remove evidence of its presence in the network of systems. This could include wiping, encrypting or damaging systems to hide evidence of its presence or its activity. External servers will likewise be abandoned and information deleted.

6. CYBER RISK REDUCTION - WHAT CAN AND MUST BE DONE

All organisations should ensure that they have a robust approach to cybersecurity risk management that addresses cyberattack as part of their organisational approach to risk management. Cybersecurity should be an integrated part of board discussions within the organisation's overarching security strategy and treated by boards with the same focus as safety. Effectively communicating cybersecurity risk to all stakeholders is essential for informed decision making about cybersecurity protective measures and building cybersecurity awareness within the organisation.

The perception of risk drives priorities and behaviours, including the amount of money spent on risk reduction or decisions about what actions will reduce risk. An inaccurate perception of risk can lead to poor decision making and poor risk reduction outcomes.

When assessing the likelihood of a cyberattack, the following can be considered:

- **Will the cyberthreat undertake a cyberattack?** A cyberthreat may have the intention and the capabilities, but for a variety of reasons may not initiate a cyberattack. Factors such as the fear of being caught or even retaliation may deter the cyberthreat from initiating a cyberattack.
- **Will the cyberattack succeed?** Not every cyberattack succeeds in causing system compromise. The exploit developed to take advantage of a certain vulnerability in the targeted IT or OT system may not work. This can be due to a lack of capability of the cyberthreat, errors in the exploit, conditions that did not support the cyberattack, or even control measures that identify and prevent the success of the cyberattack.

When assessing the consequences of a cyberattack, the following can be considered:

- **Will the cyberattack cause damage? What degree of damage will the cyberattack cause?** Cybersecurity control measures, including cybersecurity incident response, or even an ineffective exploit, may limit the intended damage of the cyberattack.

A comprehensive risk management strategy is an essential element of a cybersecurity programme. The risk management strategy should address cybersecurity across the entire organisation and set out specific objectives, such as reducing the risks of cyberattack to the organisation while remaining consistent with wider organisational security strategy. The strategy should also identify the methodology for meeting such objectives, including aligning staff, processes, budgets and controls into a single framework. Finally, the strategy should include evaluation measures that will help to assure performance against objectives and assess the contribution of the measures to overall risk reduction. Cyber risk management must allow the organisation to provide timely and accurate information to the board and senior management team about cyber risk, risk mitigation and ultimately the effectiveness of the organisation's approach to risk reduction.

Organisations need to assure themselves that they have successfully implemented—and continue to implement—risk management in a way that is consistent with their overall risk strategy. They also need to ensure that the mitigation measures in place are proportionate to the risk and continuing to function correctly.

A capability maturity model is one tool that can be used to assess the cybersecurity programme status and progress over time. A maturity model is a set of characteristics, attributes, indicators or patterns that represent capability and progression in a discipline. Model content typically exemplifies best practices

and may incorporate standards or other codes of practice of the discipline. The maturity model thus provides a benchmark against which an organisation can evaluate its current practices, processes and methods as well as for setting goals and priorities for improvement.

Communicating risk effectively can be challenging. However, to influence real improvement in cybersecurity, it is important not only to be able to communicate risk but also the risk management actions being taken, the overall performance of the risk management programme, and the desired end goals.

If decision makers who own risks do not adequately understand cybersecurity risks, they will be unprepared to put such information into the wider business context with the actions that are being taken. Instead, they will likely depend on their personal biases to make decisions, which could be inappropriate or even counter-productive to cybersecurity. Therefore, the communication of risk management performance is as important as risk management performance itself. This communication should be undertaken in a consistent and thoughtful way.

7. PROFESSIONAL DEVELOPMENT FOR THE DIGITAL AGE

Raising awareness of cybersecurity and the nature of cyber threats and risks throughout an organisation is paramount, and professional development plays a key role. The WINS Academy Cybersecurity Programme positions cybersecurity as an important and dynamic subject that requires dedicated attention.

While it is not necessary for all levels of an organisation's leadership and management to become cybersecurity experts, all need to understand the nature of cyber risks in order to make informed decisions for overall risk reduction.

A common approach to cybersecurity is the application of cybersecurity standards and associated controls with the goal of seeking process maturity. This approach is effective at establishing a certain level of assurance against the potential adverse impacts of a cyberattack, but it may not be the most efficient approach. As more systems become digitised and connected, the potential for cyberattacks grows. Understanding risks and implementing appropriate risk management processes are necessary to account for the possibility of cyber compromise and to implement mitigation controls to reduce any potential impact.

As organisations mature in effective cyber risk management, efforts can be tailored and focused on the areas with the most risk, specifically in protecting against the most impactful events. Process and prevention should eventually be replaced by a model of effective risk reduction and cyber resilience through appropriate training and development.

8. CONCLUSION

Digital technologies will continue to be enablers of business and operational processes now and in the future. New technologies are constantly being introduced and some are replacing roles previously performed by staff. The interface between people and technology is constantly evolving. In addition, the move toward remote work and outsourced/contracted IT and OT services, such as cloud-based information storage and applications, is also changing the way we work. These innovations bring us greater work efficiencies, near instantaneous visibility into processes and information, enhanced safety and other benefits. Cybersecurity needs to be a strong consideration in the development and implementation of new technologies. People and their behaviour are often cited as the key vulnerability that may be exploited in any system.

Decisions on new technology integration should be risk informed and evaluated on cybersecurity impact as well as economic factors. Some technology changes have great potential for enhancing the protection against and detection of cyberattacks. Organisations must ensure that the evolution in technologies also pays due regard to new vulnerabilities that may be exploited.

REFERENCES

- [1] The State of Nuclear Security in 2020, WINS, February 2020.
- [2] The Security of IT and IC Systems, Revision 3.1, WINS, 2019
- [3] Cybersecurity for the Nuclear Industry: Nuclear Security Management Certification Programme, WINS, 2020
- [4] IAEA, Implementing Digital Instrumentation Control Systems in the Modernization of NPPs No. NP-T-1.4, Nuclear Energy Series, 2009
- [5] Stouffer, K, Lightman, S, Pillitteri, V, Abrams, M, Hahn, A, Guide to Industrial Control Systems (ICS) Security Special Publication 800-82 Rev 2, NIST, 2015
- [6] IAEA, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants No. N-P-T-3.12, Nuclear Energy Series, 2011
- [7] Jaikumar, V. Target breach happened because of a basic network segmentation error. ComputerWorld. 6 February 2014.
- [8] IAEA, Computer Security at Nuclear Facilities NSS 17, Nuclear Security Series of Publications, 2011
- [9] Dudenhoeffer, D, et al, NS 22 Computer Security for Nuclear Security Professionals, IAEA, 2013
- [10] USNRC, Regulatory Guide 5.71 Cybersecurity Programme for Nuclear Facilities, January 2010

Rhonda Evans

Rhonda Evans, WINS' Head of Engagement and Sustainability, brings over 20 years of international and national experience in the field of nuclear safety and nuclear security to her position with WINS. Before joining WINS in August 2017, she served as a senior nuclear security officer at the IAEA in the Division of Nuclear Security. Rhonda also has extensive experience in capacity building in 171 IAEA Member States; 30 years of experience in regulation, governance and assurance; and is a lawyer specialised in nuclear law and regulation.

Jean Llewellyn, OBE

Jean Llewellyn, OBE, established the UK National Skills Academy for Nuclear and was as its CEO for 10 years. This initiative built on a career involving senior management, leadership and policy development roles in both the private and public sector. Ms Llewellyn also served as a member of the UK Government's Nuclear Industry Council and as Chair of the Nuclear Energy Skills Alliance. In 2019 Ms Llewellyn was appointed to the rank of Chevalier de l'Ordre national du Mérite by the French President. She is a Non-Executive Director of WINS.

Roger Howsley

Dr Roger Howsley is the Co-Founder and Executive Director of WINS. During 30-plus years of international experience relating to nuclear non-proliferation and security across the nuclear fuel cycle, Roger has worked with the IAEA, Euratom, national police forces and security organisations. Prior to WINS, he served as Director of Security, Safeguards and International Affairs (SSIA) for British Nuclear Fuels Ltd. He also established and directed the SSIA function across the BNFL Group of companies (16 countries, 17,000 employees).