WORKING GROUP 1 REPORT

Managing Cyber Threats

March 30, 2016

TABLE OF CONTENTS

1. MANAGEMENT SUMMARY

Since the first Nuclear Industry Summit (NIS) in Washington in 2010, the industry has made substantial steps in further improving cyber security in the nuclear industry. The NIS 2012 in Seoul put the topic of information protection clearly on the table. The NIS 2014 in Amsterdam added a focus on the protection of Industrial Automation Systems, and on the need to collaborate between government and industry to develop effective counter measures in the cyber domain.

The NIS 2016 embraces these thoughts and continues to deepen the focus on cyber security within the nuclear industry. Furthermore, it promotes activities for the nuclear industry to remain ahead of the dynamic cyber threat curve. In doing so, it enables the nuclear industry to continue providing benefits to society in a secure manner, such as carbon free electricity and the supply of medical isotopes.

The NIS 2016 Working Group on Managing Cyber Threat condensed its work into 27 Working Group recommendations, which can be found in chapter 7 of this report. Those 27 recommendations have been further condensed into a summary for the NIS Joint Statement in five conclusion statements, as described in chapter 8. These five conclusion statements of the Working Group are:

1. The threat of cyber-attacks is substantial and continues to increase over time.
2. The threat encompasses not only sensitive nuclear information, but also the Plant Control Systems managing and controlling the nuclear processes within nuclear facilities.
3. Developing robust defenses against cyber-attacks is about more than meeting regulatory requirements.
4. Transparency must be promoted to ensure that the trust of the society is maintained.
5. The nuclear industry is advised to move from a culture of compliance to a culture of excellence in cyber security.

2. INTRODUCTION

The nuclear industry brings great value to society in a wide variety of forms. Nuclear energy delivers safe, reliable and affordable electricity without producing greenhouse gases, thus yielding significant economic and environmental benefits. Similarly, radiological sources are key enablers for advanced medical diagnostics, food safety and industrial applications. For society to continue to capitalize on these benefits, the nuclear industry must continue to demonstrate that it can operate securely without endangering the populations that we serve. The application of advanced digital technologies in the nuclear industry continues to yield significant benefits in terms of safety, reliability and efficiency. While these benefits are both highly desirable and imperative for the long-term success of the industry, the level to which critical infrastructures are now interconnected can create cyber security vulnerabilities if not properly and vigilantly managed.

Nuclear facilities are typically hardened to a degree that makes cyber compromise difficult to achieve, but complacency is the enemy of excellence. However, the sophistication of exploitation tools continues to increase, and access to these tools and techniques becomes more widespread – thus the industry must remain vigilant. Cyber defenses must continue to evolve commensurately with the evolution of threat they defend against. A variety of initiatives has been undertaken to address this evolving threat. The International Atomic Energy Agency (IAEA), as a collaboration of States, has increased its efforts in this domain. Governments have used the IAEA guidance to further develop their regulatory frameworks. On the industry side, the World Institute for Nuclear Security (WINS) has also increased their efforts in this domain. The industry itself continues to improve its defensive posture further against cyber threat.

These improvements are evident from the progress that has been made against the recommendations contained within the 2010, 2012 and 2014 Nuclear Industry Summits. The principle challenge of the 2016 NIS is to build upon this progress.

3. WORKING GROUP MEMBERS

The members of the NIS 2016 Working Group on Managing Cyber Threat are:

NAME	TITLE	ORGANISATION	COUNTRY
Amir Shahkarami **(Chair)**	President & CEO	CASe Global Partners, Inc.	USA
Anno Keizer **(Vice Chair)**	Manager Security	URENCO Nederland B.V.	The Netherlands
Philippe Bosquet	Deputy VP Site Protection	AREVA	France
John Connelly	Fleet Cyber Security Program Manager	Exelon	USA
Scott Hilts	Manager IT Security	Bruce Power	Canada
Barry Kaufer	Director	WNA – Cordel	International
Pierre Legoux	Head of Program	WINS	International
Ernani Peas de Barros	Manager IT Governance & Security	Eletronuclear	Brazil
Jean Luc Trolle	Nuclear Security Information Advisor	EDF	France

Table 1: NIS 2016 Working Group members

4. DEVELOPMENTS SINCE THE NIS 2014 IN AMSTERDAM

4.1 Statements made at the NIS 2014 in Amsterdam

The Cyber Security Working Group of the 2014 NIS developed four key recommendations[1], which are summarized below:

Nuclear industry participants of the [NIS 2014] Working Group are proposing the following recommendations (or good practices) to increase the level of cyber security:

1. *Pursue discussions at the IAEA level with a view towards establishing common guidelines related to the cyber security of Nuclear facilities and supporting infrastructures and ultimately extend these discussions to eventually include generally accepted standards providing a common framework for the industry;*

2. *Acknowledging that States retain regulatory oversight of their nuclear infrastructures, continue to support national initiatives to define appropriate regulations and measures that are commensurate with cyber security risks and threats and do not adversely affect plant operations;*

3. *Reinforce industry collaboration on cyber security by establishing regular discussions on cyber security topics (inside WANO and/or WNA) with the objective of sharing good practices and risk reduction efforts in response to known and potential cyber security threats duly taking into account national requirements for protection of sensitive information;*

4. *Improve the cyber security culture and capability within their organizations by analyzing and applying a wide range of solutions addressing cyber security skills, knowledge, practices and overall awareness at all levels of the organization.*

[1] Reference www.nis2014.org

Figure 1: The NIS 2014 participants in the Beurs van Berlage in Amsterdam, the Netherlands

4.2 Progress on NIS 2014 statements

Section 4.2 illustrates the progress made on these recommendations since March 2014, and how it enhances and further strengthens the industry's defensive posture.

Progress on NIS 2014 recommendation 1

With respect to Recommendation 1, the IAEA has conducted multiple activities over this period which included a) the development of guidance, b) conducting expert meetings, c) conducting global information exchanges for stakeholders, and d) conducting training courses at the international, regional, and national levels.

In June 2015 the IAEA organized the "International Conference on Cyber Security in a Nuclear World: Expert Discussion and Exchange" which brought together over 700 experts representing 92 countries and 17 international organizations. The goal of this conference was to provide an international forum for information exchange and discussion on both the challenges and progress with regards to cyber security in the nuclear industry. Multiple sessions were conducted focused on the industry perspective.

National Training Courses (NTC) conducted by the IAEA have been one of the most productive forums for raising awareness and building cyber security competence. The NTCs also provided an excellent basis for engaging both competent authorities (i.e. State representatives) and industry (operators and vendors) in joint discussions aimed at enhancing cyber security for the nuclear industry within the State.

The IAEA has published multiple documents related to information and computer security. These include: **Nuclear Security Series No 17 (NSS17) Computer Security at Nuclear Facilities**, which provides guidance for implementing a cyber security program, evaluating existing programs, assessing critical digital assets, identifying appropriate risk reduction measures and designing robust digital systems. **Nuclear Security Series No 23-G Security of Nuclear Information** provides guidance on the classification and protection of information in all forms including electronic format, and the systems associated with this information.

The IAEA is developing additional guidance documents as listed below.

DOCUMENT	STATUS
TECDOC NST 037 - Conducting Computer Security Assessments Provides good practices for organizing and conducting cyber security assessments associated with nuclear security.	Document Complete Publication in 2016
TECDOC – NST038 Computer Security Incident Response Provides good practices for implementing cyber security incident response processes between competent authorities, operators, and technical support organizations.	Document Complete Publication in 2016
Nuclear Security Series Technical Guidance – NST036 Computer Security of Instrumentation and Control Systems at Nuclear Facilities. Provides guidance on implementing cyber security controls across the life cycle of nuclear instrumentation and control systems.	Approved for Publication Publication in 2016
Nuclear Security Series Implementing Guide – NST045 Computer Security for Nuclear Security Provides overarching guidance to assist Member States in implementing cyber security as a component of their nuclear security regime.	Under Development
Nuclear Security Series Technical Guidance – NST047 Computer Security Techniques for Nuclear Facilities Provides discussion on good practices for implementing cyber security associated with digital technologies at nuclear facilities.	Under Development

Table 2: Overview of IAEA cyber security guidance.

Progress on NIS 2014 recommendation 2

NIS recommendation 2 can be characterized as a statement, and it remains true. The statement was:

Acknowledging that States retain regulatory oversight of their nuclear infrastructures, continue to support national initiatives to define appropriate regulations and measures that are commensurate with cyber security risks and threats and do not adversely affect plant operations.

Progress on NIS 2014 recommendation 3

Industry collaboration on matters of cyber security continues to gain momentum through a variety of venues at national and international levels. Examples include:

1. WINS[2] has expanded its efforts to identify, consolidate and disseminate best practice guides on topics relevant to those with responsibility for the security of nuclear materials and associated facilities and transport. WINS has published 35 Guides on various topical security areas, and two of these "Security of IT and IC Systems at Nuclear Facilities" and "Effective Integration of Physical and Cyber Security" focus on cyber security. Each of these guides contains key survey questions for practitioners, and a Maturity Model for evaluating the effectiveness of their security arrangements.
2. In April of 2014, WINS initiated the WINS Academy. The Academy offers online courses focusing on the needs of specific audiences, such as Board Members, Executive Managers, Security Directors, Scientists/Technicians/Engineers, and Regulators, who have responsibility and accountability for nuclear security.
3. In coordination with its members and sponsors, WINS has developed a comprehensive program of professional development activities for 2015 and 2016. This includes producing new Best Practice Guides, undertaking revisions of current Guides, conducting workshops and/or roundtables around the world on an almost monthly basis, and continuing the development of new Academy modules that offer growing opportunities for professional certification in nuclear security. Program of activities will promote the development of comprehensive nuclear security program and the convergence of the

[2]www.wins.org

various security related disciplines (physical protection, cyber security, emergency preparedness, etc.) into an integrated risk management framework.

4. The organizations WNA and WANO have acknowledged the importance of the topic of cyber security, and have agreed that cyber security will be one of the aspects that WNA and WANO will include in their primary activities. For instance, in the safety related guidance of WANO, the cyber security aspects impacting safety will be taken into consideration.

5. In 2014, the Electric Power Research Institute (EPRI) chartered the Cyber Security Technical Advisory Committee (CTAC) to address specific technical issues with the implementation of Cyber Security best practices.

6. INPO specifically reviews Cyber Security compliance as an element of Configuration Management.

Progress on NIS 2014 recommendation 4

WINS has delivered the WINS Academy in which staff responsible for nuclear security can be trained and certified against an international recognized standard.

WNA Working Group on Security of the International Fuel Cycle has its role adding cyber security to its four main subgroups. In addition the WNA CORDEL Task Force and Digital I&C has listed cyber security as one its priorities.

As most of nuclear security systems are designed, managed, and operated by humans; the ultimate success of the nuclear security regime relies on the people involved. The impact of individuals and management must be addressed in order to maintain effective nuclear security. Nuclear security culture plays an important role in motivating individuals to remain vigilant and take sustainable measures to protect against credible insider and outsider threats. Cyber security culture, education, and awareness continue to improve in international community and countries have adopted several measures on this important aspect of security as a whole.

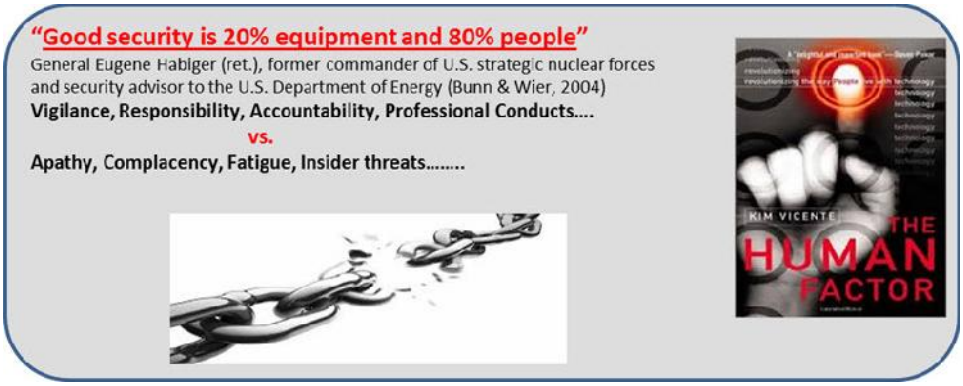

Figure 2: Example of a cyber security culture activity

5. EFFECTIVELY ADDRESSING CYBER THREAT

5.1 Developments in threat

While Stuxnet was a watershed event in the application of malware and targeting of nuclear facilities, the targeted attack against Korea Hydro and Nuclear Power (KHNP) in December of 2014 further illustrates that the nuclear industry is being targeted by very capable adversaries. Currently there are multiple cyber campaigns occurring that are specifically seeking out industrial control systems common to many nuclear facilities. These attacks have demonstrated a high level of sophistication, and a high degree of persistence by the attackers. Examples include:

- **KHNP Attack**: As noted above, this attack led to the exfiltration and public release of large volumes of data from a South Korean nuclear operator. One possible goal of the attack was to create social chaos regarding the safety of the nuclear power plants. The attack involved targeting of not only employees, but also of retirees and vendors.

- **Havex**: A reconnaissance virus that targets and enumerates a common Industrial Control System (ICS) protocol. The entity mounting this campaign is actively collecting intelligence on connectivity and relationships between ICS components for reasons that are not currently known. This is a concern as understanding relationships between the ICS components is the first step in an attack.

- **REGIN**: An exceptionally sophisticated and modular suite of malware tools that targets ICS components. While the total suite of modules is not currently understood (it is the subject of ongoing research), the capabilities identified thus far range from simple reconnaissance to device destruction.

- **BlackEnergy**: A sophisticated framework currently being used in both the “sandworm” and “crouching yeti” campaigns, which specifically target ICS platforms. In January 2016 BlackEnergy was identified as a key part of the attack on the electricity grid in the Ukraine that caused an electricity outage of several hours to tens of thousands of customers.

- The **German Still Mill** Control System Compromise: As reported in Die Lage der IT-Sicherheit in Deutschland 2014, a cyber-attack at the German steel mill allowed attackers to gain access to the control system for the production facility. The report further indicates that the attackers had not only a high level of knowledge of cyber security, but also a good understanding of the operation of the control systems. The result of the attack was massive physical damage, caused when the attackers prevented a normal system shutdown from occurring.

When considered in aggregate, it is clear that ICS platforms are being specifically targeted by adversaries whose intent is unclear, and can be vulnerable if not properly protected.

5.2 Effectively addressing cyber threat

In order to effectively address the cyber threat, an organization must assign responsibility for the cyber security function. The cyber security program should be integrated as much as possible in the company's overall risk-governance structure. Additionally, the cyber security program must integrate different functions, including (at a minimum) physical security, engineering, information technology, maintenance and emergency preparedness. These groups must work together to identify, assess and manage the cyber threat.

Furthermore, security and cyber security should be managed on a graded risk-based approach, meaning cyber security risk should be understood. There are several guidance and best practice guides available that can be used to assist in this process. The fundamental steps are:

1. Understand the risk and attack vectors;
2. Understand the facility's vulnerabilities; and
3. Determine the consequences of a hypothetical attack.

Based on the risk analysis, a comprehensive framework of security measures should be implemented consisting of both technical and organizational measures. Technical measures include, for example, segmentation of networks, restricting access and monitoring access. Organizational measures include, for example, procedures, awareness, exercising and testing.

The figure below shows the relationships of the various entities that share and hold a stake in matters of cyber security.

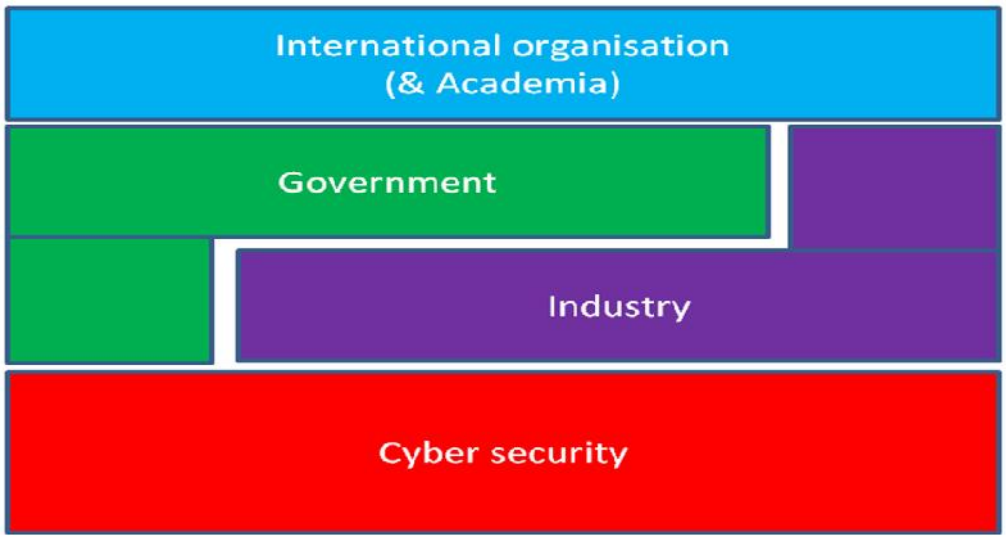

Figure 3: Relationship of different stakeholders towards cyber security.

5.3 Governance, oversight and assessment

The nuclear industry strives for excellence in many areas, such as the quality of primary processes, safety performance and operational performance. Nuclear security should be considered by management as one of the areas where the nuclear industry must also excel. This approach goes beyond simply meeting regulatory requirements.

Management in the nuclear industry is advised to incorporate nuclear security into the governance processes they already utilize. The manner in which management maintains oversight of cyber security should be similar to the manner in which management maintains oversight over nuclear safety, since the consequences of a cyber security attack can also be serious.

The industry must move from a 'reactive' mode of cyber security operations to a 'proactive' mode. This requires the nuclear industry to move from the compliance mentality to one of excellence in cyber security. Below are examples of Board of Directors responsibilities and an assessment method.

Corporate Board:

Corporate boards are faced with the challenge of needing to use technology to grow and maintain their enterprises without creating undue risk or jeopardizing hard-won public trust.

The *National Association of Corporate Directors' Cyber Security Handbook* identified five core principles for corporate boards to enhance their cyber-risk management.

1. Understand that cyber security is an enterprise-wide risk management issue. Thinking of cyber security as an IT issue to be addressed simply with technical solutions is an inherently flawed strategy. The single biggest vulnerability in cyber systems is people – insiders. Cyber security costs are managed most efficiently when integrated into core business decisions such as product launches, M&A and marketing strategies. Moreover, in an integrated world, organizations must take into account the risk created by their vendors, suppliers and customers as their weaknesses can be exploited to the detriment of the home system.

2. Directors need to understand the legal implications of cyber risk. The legal situation with respect to cyber security is unsettled and quickly evolving. There is no one standard that applies, especially for organizations that do business in multiple jurisdictions. It is critical that organizations systematically track the evolving laws and regulations in their markets.

3. Boards need adequate access to cyber security expertise. Although cyber security issues are becoming as central to business decisions as legal and financial considerations, most boards lack the needed expertise to evaluate cyber risk. Many boards are now recruiting cyber professionals for board seats to assist in analyzing and judging staff reports. At a minimum,

boards should regularly make adequate time for cyber security at board meetings as part of the audit or similar committee reports.

4. Directors need to set an expectation that management have an enterprise-wide cyber-risk management framework in place. At a base level, each organization ought to have an enterprise-wide cyber-risk team led by a senior official with cross-departmental authority that meets regularly, has a separate budget, creates an organization-wide plan and exercises it.

5. Based on the plan, management needs to have a method to assess the damage of a cyber event and therefore establish a robust recovery plan. They need to identify which risks can be avoided, mitigated, accepted or transferred through insurance. This means they need to identify which data, and how much, the organization is willing to lose or have compromised. Risk mitigation budgets need to then be allocated appropriately between defending against basic and advanced risks.

If an organization follows these principles, it should be well on its way to establishing a sustainable and secure cyber-risk management system.

Independent Assessment:

There are several assessment tools already available that can be utilized. In its 'Transforming Cyber Security Using COBIT 5', global association ISACA recommends starting with these eight principles:

1. Know the potential impact of cybercrime and warfare. Make sure you are aware of the potential damage a cyber-attack can cause and the wide-ranging impact it may have. The organization must decide the risk level it can tolerate in order to ensure the appropriate level of cyber security governance.

2. Understand end users, their cultural values and their behavior patterns. As the ISACA guide notes, "Business impact and business risk relating to cyber security arrangements are strongly influenced by organizational and individual culture." The culture – and the resulting end-user behavior and patterns – should be accounted for in the enterprise's strategic, tactical, and operational security measures.

3. Clearly state the business case for cyber security and the risk appetite of the enterprise. The business case outlining expected value and tolerable risk will drive the overall cyber security strategy. As a result, the business case must have depth and definition. Among its contents, it must include cost-benefit considerations and the organization's culture and values pertaining to cyber security.

4. Establish cyber security governance. There is no need to reinvent the wheel here. Adopting and customizing a governance framework such as COBIT will give you the tried, tested and proven governance guidance you need. By effectively governing cyber security, an organization provides a clear sense of direction and boundaries.

5. Manage cyber security using principles and enablers. The principles and enablers will help the organization ensure end-to-end governance that meets stakeholder needs.

6. Know the cyber security assurance universe and objectives. Cyber security covers multiple areas and aspects within cyber security. To provide adequate assurance over cyber security, the cyber security universe must be well defined, and the assurance objectives must be clear and manageable.

7. Provide reasonable assurance over cyber security. This principle requires all three lines of defense within an enterprise to be defined and managed. This includes monitoring, internal reviews, audits and, as needed, investigative and forensic analysis.

8. Establish and evolve systemic cyber security. Cyber-attacks target the weakest link in the system. As a result, cyber security must be looked at as a system of interdependent elements and the links between them. To optimize cyber security, the enterprise must have complete understanding of this dynamic system and must be fully aware that security governance, management and assurance cannot be viewed in isolation.

5.4 Management and procedures

Continued general management attention is an essential prerequisite for effective cyber security. Cyber security should be seen as one of the areas in the overall company's risk management process. As much as possible cyber security should be treated as any other risk the business needs to manage.

Besides adopting cyber security in the holistic risk management approach of the company, it is also imperative that cyber security related concepts, standards, best practices, and advice available outside of the company are adopted.

Aspects that are to be considered are allocation of responsibilities, competencies of staff, quality of architectural design, and effectiveness of cyber security management including effective monitoring.

5.5 Enhancing cyber security culture and capabilities

Cyber security has become one of the most important and challenging issues facing today's organizations. With pervasive use of technology and widespread connectedness to the global environment, organizations increasingly have become exposed to numerous and varied threats. Technical controls can provide substantial protection against many of these threats, but they alone do not provide a comprehensive solution. As Kevin Mitnick notes in his book, "The Art of Deception:

Controlling the Human Element of Security," these technological methods of protecting information may be effective in their respective ways; however, many losses are not caused by a lack of technology or faulty technology but rather by users of technology and faulty human behavior. It stands to reason than that people not only can be part of the problem, but they can also and should be part of the solution. People must be an integral part of any organization's cyber security defense system.

Keeping information secure is not only the responsibility of information technology (IT) security professionals, but also the responsibility of all people within the organization. Therefore, all users should be aware not only of what their roles and responsibilities are in protecting information resources, but also of how they can protect information and respond to any potential security threat or issue. Security awareness programs must address the need to educate all people in an organization so they can help to effectively protect the organization's information assets. But just how well are organizations doing implementing security awareness programs and training their employees[3]?

The nuclear industry already has reached a consensus that cyber security will not solely rely on technology and internal IT teams, but will require human performance improvements. Furthermore, raising awareness of cyber security issues amongst nuclear operators' senior management will be necessary to enhance the overall security level. This awareness will be partially driven by states through their regulatory body. It will also be driven by independent organizations such as corporate audit and standards organizations. Nuclear facilities will continue to be responsible to implement robust cyber security cultures and capability, similar to what they have achieved in nuclear safety.

Culture:

It must be universally agreed in the nuclear industry, including by senior management, that cyber security is everyone's responsibility. Any action that anyone can take (such as clicking on a web link, using a personal USB device…) may lead to a potential security breach. Cyber security must be as important as safety and physical security in the minds of all employees, from operators to managers to support personnel. It must be systematically integrated into the organization's policies and procedures.

Enhancing cyber security awareness and culture across nuclear industry organizations represents a challenge that will require dedicated and knowledgeable teams, as well as tailored training and awareness activities.

Capabilities:

As previously stated, cyber security will not rely only on IT departments but will have to include management and operational measures. Cyber security must be integrated with existing security policies and procedures, with clearly delineated but integrated roles and responsibilities within the organizations. A dedicated cyber security multidisciplinary team with appropriate delegated authorities and responsibilities should be employed to achieve this level of integration.

[3] Glenda Rotvoid, PhD. "How to Create a Security Culture in Your Organization", Information Management, Nov/Dec 2008

Industries outside of nuclear are acknowledging that the skills required for cyber security are not the same as the skills required for general information technology management and that their current teams may lack these capabilities; the nuclear industry is no different. Since cyber security has recently emerged as a critical imperative for all industries and is very fast moving, resources are scarce. As a result, a recognized challenge for the industry (extending to national / international organizations and regulatory bodies) will be to find qualified resources, whether within their organizations or through third parties. Each nuclear operator must decide whether cyber security is a competency that is core to its required capabilities, or a competency that can be acquired as an external service. In making this decision, operators must consider that while third parties may bring expertise to enhance nuclear operators' capabilities on cyber security, it also increases the risk of disclosing potentially sensitive information.

Any plan for establishing cyber security capabilities should therefore address the type of capabilities required, but also a strategy for sourcing the capability (internal or external).

5.6 Extra considerations for existing facilities

Like all industries, the nuclear industry is enjoying the benefits of significant improvements in information and digital technology. As control systems are refurbished or modernized with digital controls and sensors, reliability and efficiency of operations as well as safety and security can be improved. This trend is supported by new generations of engineers and managers who have been trained and even helped design these new capabilities using these new digital technologies.

What was formerly done via purpose-built information technology and engineering solutions is now done by non-proprietary solutions using available software and hardware connected via internet-based protocol or other widely available standard protocols. This proliferation of 'commercial-off-the-shelf' (COTS) technology in the nuclear industry, while efficient, has its negative side: the use of COTS products has made it easier for attackers to craft exploits against known vulnerabilities of such systems. The problem is further complicated as greater connectivity is applied to such systems, for example, when they are connected to corporate intranets that have access to the Internet. The security of nuclear facilities will depend on a thorough exploration and understanding of how physical and cyber assets are connected, how physical and cyber threats are vulnerable and how they relate to each other. As States and industries have improved their understanding of cyber security risks, and ultimately threats, they have been prompted to establish guidelines and take specific actions to increase the overall level of cyber security at existing facilities.

From a safety perspective, the nuclear industry's response to the Fukushima event could be taken as a successful example of how the nuclear industry succeeded in:

- Assessing or reassessing the level of safety of existing plants and facilities with shared common rules and under national oversight (stress tests performed under national regulatory oversight).
- Enhancing the safety of existing reactors with the development of new products and services.

To prevent a cyber-security or malicious event, a similar effort should be made to reach the common objective of enhancing cyber security and integrating it into an overarching effective security program, bearing in mind that:

- A balanced approach is necessary to ensure that measures taken are commensurate with the risks and that they do not create adverse effects with respect to the plant operation and maintenance in particular with regard to safety,
- Required regulatory oversight needs to be effective and pragmatic.

Today, it is important to have in mind that new international recommendations or standards for the nuclear industry have been published or are being developed after the previous Nuclear Industry Summit held in Amsterdam, in particular by IAEA (NSS 13, NSS 23-G, NSS 17, IPPAS Chapter 6 Cyber Security Review, NST036, NST 037) and IEC (62645, 62689 which is in development, or even 61653, 62138, 61226, 60880 which are safety-focused). Documents already published, as well as those in development at the IAEA and/or IEC, are the result of long-term development processes. Such documents provide a good overview of key success factors to build a comprehensive security program, as well as detailed guidelines to be applied to increase the level of security against cyber threats. These new international recommendations or standards, consistent with nuclear safety standards, explain defense-in-depth concepts such as the graded approach, security levels, security zones, independence of the cyber security organization, and a dedicated cyber security team. These new international recommendations or standards are already used by some nuclear operators and vendors.

In conclusion, IAEA recommendations, implementing guide or technical guidance and other new emerging international standards (e.g., from the IEC) for cyber security in the nuclear industry could serve as a strong reference basis to improve and harmonize the national regulatory environment in nuclear security. This will lead to a solution that balances risks while ensuring effective and pragmatic regulations. For example, to promote a high level of cyber security protection and confidence, IAEA advocates PR articles of periodic tests, self-assessment of an operator with its own independent audit organization, benchmarking with other operators and industries, and assessment by regulatory authorities. Cyber security assessments could be conducted, for example, by using IAEA guidelines (IPPAS Module and/or/with adjunction of NST037 “Conducting Computer Security Assessments at Nuclear Facilities”).

5.7 Additional considerations for new facilities

While existing facilities enjoy increased capabilities from new generation information technology, new facilities have these new technologies built-in for both safety and operational systems. During the design phase of new facilities, a structured approach to integrating cyber security capabilities should also be applied to ensure adequate protection of the systems. Since some new Gen3 reactors are currently in construction phase, any modification or change will be critical as they may affect licensing processes and cause delays in the construction of these new reactors.

Similar to existing facilities, an alignment of authorities on a common set of internationally recognized recommendations could ensure an agreement on a common ground between reactor manufacturers and regulatory authorities. This would bring about balanced cyber solutions and allow effective oversight, corresponding to each State's level of need.

Additionally, improvements made in new Gen3 designs could also benefit the revamping of current I&C systems, as those operations are often associated with life extension of existing facilities.

6. DEVELOPING A FORUM FOR THE INDUSTRY TO EXCHANGE INFORMATION ON CYBER SECURITY TOPICS

As enumerated throughout this report cyber security is both an emerging and a fast-moving topic. To enhance the level of cooperation, at the national and international levels, between nuclear operators and between the nuclear industry and other sectors, it would be worthwhile to build on existing international nuclear platforms. These include WANO-INPO and/or WNA, where actors of the nuclear industry already regularly meet to exchange their views, best practices or concerns on operational practices and nuclear safety arrangements.

This forum could be hosted within the current organizations or members could meet under the auspices of frequent international meetings held throughout the year (for example, AtomExpo, WNA). However, It's also necessary to take into account the fact that information about security measures actually implemented at nuclear facilities is sensitive, and must be also protected in an appropriate manner.

Cyber-attacks can, by their nature, be used to wage a form of asymmetric warfare to achieve nationalistic, ideological, or criminal objectives. An adversary capable of delivering a properly targeted attack can achieve results that were once the exclusive domain of a military operation, thus opening the door to a broader range of attackers with a variety of motivations and objectives. The non-linearity of the threat is further exacerbated by the reality that an adversary can focus intently on a single vulnerability or weakness. As is often stated, the attacker need be successful once, whereas the defender must be vigilant across all fronts and must be successful at all times.

Digital technology and connectivity are revolutionary in terms of reliability, efficiency and system performance. While these technologies carry substantial operational and safety benefits, there are attendant risks that must be properly managed. Nuclear facilities must ensure a level of cyber security that is commensurate with the sectors obligation to protect the health and safety of the public, and to provide a reliable source of power to the communities we serve.

Open-source information makes it clear that:

- The sophistication of exploit tools continues to grow exponentially thereby lowering the barrier of technical sophistication necessary to mount a successful attack.
- Nations continue to invest heavily in the development of advanced cyber capabilities as a mechanism to achieve military and political objectives.

- Criminals are achieving greater sophistication in cyber-attacks.
- General threat and vulnerability information is becoming more widely available through Internet searches and information sharing portals.
- The cyber security ecosphere is exceptionally dynamic and is perpetually evolving.

The fluidity of the threat makes it imperative that information be shared among key stakeholders within the nuclear community quickly and efficiently as an enabler for closing potential gaps before they can be exploited. Mechanisms exist today for this purpose (ICSCERT, DHS, INPO, et al) but they have inherent limitations and in many cases lack information that exists within the intelligence community, as information sharing mechanisms do not currently exist on a universal basis.

Using non-classified information, it is recommended that key decision makers are informed of the following broad issues:

- Current readiness of the international nuclear community.
- Adversary capabilities.
- Existing mechanisms for sharing information across the international nuclear community and their inherent limitations.
- Strategies for improving information sharing as an enabler to improving the industries defensive posture.
- The need to establish metrics and methods to measure and establish shared information quality.
- Strategies to develop and share best practices related to vulnerability identification and mitigation of cyber-attacks.

The following is a review of possible contributions by different organizations as platforms for future discussions for the industry.

IAEA

The IAEA is the undisputed leading organization in the field representing governments. The nuclear industry is using the products, including guidance and training that the IAEA is providing. But since it is an organization of States, it is not the logical choice as a future platform for industry discussions.

However, it may facilitate Industry/State discussions, especially those centered on threat and incidents response by hosting periodic expert meetings, and possibly other information sharing platforms. The IAEA is currently investigating cyber security incident and threat sharing platforms and protocols. This is in part based on and in response to the outcomes of the 2015 conference.

WINS

WINS provides an international forum where organizations and individuals who are accountable for nuclear security can learn, share and promote the implementation of security best practices. WINS is playing a leading role in professional development and certification for nuclear security management. In its current form (budget and staffing), WINS could not take on the role of unique industry platform for future discussion on nuclear cyber security. However, such a platform could be established through an effective cooperation and coordination between organizations such as WANO, WNA, WNTI and WINS.

WANO/INPO

WANO is the leading industry organization on safety for Nuclear Power Plants. In cases where safety would be at risk because of security issues, WANO seems to have an interest in security as well. However, WANO has not shown interest in taking on security as an independent topic. Also WANO only represents the Nuclear Power Plants (NPPs) and few nuclear fuel cycle facilities (reprocessing plants) so a substantial part of the nuclear cycle is not in their scope.

WNA

The World Nuclear Association is the international organization that promotes nuclear energy and supports the many companies that comprise the global nuclear industry. WNA participates through its various Working Groups and can also provide a wide communications network through its World Nuclear News (WNN).

7. WORKING GROUP RECOMMENDATIONS

In summary, the NIS 2016 Working Group on Cyber Security proposes the following 27 recommendations.

Industries

1. Shift from a culture of cyber security compliance to a culture of excellence in cyber security, as regulatory requirements are unlikely to keep pace with the evolution of the cyber security threat.

2. Reinforce industry collaboration on cyber security by establishing regular discussions on cyber security topics (inside WANO and/or WNA) with the objective of sharing good practices and risk reduction strategies for known and potential cyber security threats, taking into account national requirements for the protection of sensitive information.

3. Strengthen the multi-disciplinary approach needed to ensure effective cyber security, especially in the plant control systems domain.

4. Strengthen active collaboration with the IAEA in developing guidance, and in conducting awareness and training activities to support the nuclear industry.

5. Verify the effectiveness of cyber security measures where possible by exercising and testing (i.e., adoption of the Plan-Do-Check-Act model).

6. Explicitly focus on cyber security practices in the execution of properly crafted specifications, and in the procurement of products and services to ensure that supply chain vulnerabilities are effectively mitigated.

7. Improve the cyber security culture and capability within their organizations by analyzing and applying a wide range of solutions addressing cyber security skills, knowledge, practices and overall awareness at all levels of the organization.

8. Ensure that every staff with cyber security accountabilities is demonstrably competent.

9. Strengthen the communication and cooperation between cyber and physical security staff and coordinate their respective strategies, policies and reporting mechanisms.

10. Fully integrate experts from nuclear operations, engineering and maintenance in addressing cyber security. Integrations of third party staff involved in these fields should be considered as well.

11. Pursue the formation of an organization that will foster the exchange of information in a meaningful and confidential manner.

12. Treat self-assessments and peer reviews as a necessary mechanism to acquire assurance of an effective security structure, and as a means to share good practices.

International organizations

13. Organizations like the IAEA and WINS (et al) are encouraged to further increase their respective efforts in developing technical, programmatic and managerial guidance in the cyber domain. These activities should actively engage the industry as a key stakeholder and implementer of cyber security.

14. Industry organizations like WNA, WANO, NEI, EPRI and others are encouraged to establish platforms whereby cyber security issues receive appropriate attention, and relevant information can be shared by all across sectors and national borders. Cyber security has no 'end state'. Therefore, it is likely that this effort will need to continue in some form in perpetuity. Such a platform could be a working group coordinated under a single entity, or as a joint effort executed in a coordinated fashion among multiple entities. The platform should not only involve its members, but also others in the industry via, for instance, the organization of conferences.

15. Other international organizations involved in Nuclear Cyber Security (e.g., WINS) should also play a role in exchanging general practices and training in the field of cyber security.

16. Further develop and / or further promote the idea of internationally recognized common knowledge levels for cyber security practitioners. Examples of certified knowledge levels for security people are the 'CISSP' for Cyber security professionals or 'CPP' for security managers. Specific to the nuclear sector, international or national accreditation schemes could be used.

17. Recognize the unique position and the role of the IAEA in the international field of nuclear security, and especially cyber security in the area of establishing recommendations and guidance at different levels, and ensuring coherence between safety and security. This is key in the domain of Instrumentation & Control, and of nuclear materials. Those recommendations and guidance can be further detailed by other international standards elaborated under their robust processes, such as those of the International Electrotechnical Commission (IEC).

18. The industry encourages States in all countries to request IAEA International Physical Protection Advisory Service (IPPAS) missions. The IAEA developed a cyber security module in IPPAS, a critical step in helping develop a common cyber security review specialized for nuclear activities. The industry acknowledges value of the IAEA IPPAS missions as independent objective assessments of both nuclear security arrangements on facilities, and also the nuclear security framework of the State. The current IPPAS mission focus on cyber

security is not sufficient in terms of resources and time to provide the level of review desired. The industry encourages the IAEA to enhance IPPAS missions or develop advisory missions dedicated to support the assessment of plant industrial control systems, especially those used for safety.

Governments

19. Incorporate cyber security in the Design Basis Threat (DBT) to ensure effective cyber resilience at the facilities for which they have regulatory authority.

20. Provide pragmatic definitions of the cyber equivalent of the concepts of "Beyond DBT" and "remote armed response" (used in the physical world).

21. Recognize the dynamic nature of cyber threat, and develop appropriate mechanisms through which information can be shared with key stakeholders as threats emerge and mitigations need to be undertaken. Absent of the sharing of this information, vulnerabilities are less likely to be addressed expeditiously.

22. Ensure that regulators and inspectors acquire the cyber skills necessary to effectively regulate and inspect cyber security plans.

23. Establish a mechanism whereby cyber incident information and lessons learned can be shared across different vital/critical industry sectors, whilst protecting the identity and interests of the organization that reported the incident as well as taking into account the obligation for the protection of sensitive information.

24. Coordinate threat information internationally, as while States retain regulatory authority, the threat is not constrained by national borders.

Academia, research centers and vendors

25. Develop tools for assessing the effectiveness of cyber security measures, since analogous concepts from the physical world like attribution, deterrence, delay time, detection rate and armed response don't easily translate to the cyber world.

26. Develop operating systems and security concepts that strengthen resilience, especially in the Industrial Automation Systems domain.

27. Further enhance collecting of information, and analyze this data to develop practical and usable conclusions on what the level of cyber threat actually is, what the trend is and how it fluctuates over time.

8. WG1 SUMMARY FOR NIS 2016 JOINT STATEMENT

For the purpose of the NIS 2016 Joint Statement the advice of the Working Group 1 given in this report can be summarized in the following five items.

1. The threat of cyber-attacks is substantial and continues to increase over time

Experience gained over the last two years demonstrates that the number of cyber security related events and the aggressiveness of those events continue to increase. Attacks on nuclear facilities have occurred and were executed by capable adversaries, which likely included nation States.

Unlike more typical cyber security attacks, the adversaries do not focus on the theft of information, but seek to damage the reputations of our industry. This could ultimately extend to sabotage of the installation possibly resulting in major risks for the environment and substantial financial losses.

2. Nuclear facilities are protecting sensitive nuclear material, protecting their Industrial Control Systems and managing their controlled nuclear processes

Earlier views concerning cyber security focused on protecting sensitive nuclear information regarding the protection of nuclear sites. This view has developed over time to reveal that Industrial Control Systems that manage and control nuclear processes can also be a target for adversaries, and need focused and stringent protection.

3. The nuclear industry developing robust defenses against cyber-attacks is more than a regulatory requirement

Regulatory requirements may be met by the nuclear industry, but the commitment to managing cyber security risk extends beyond minimal compliance. A successful cyber-attack could have implications that would be intolerable from a financial and public confidence perspective. Facility operators recognize their interest and responsibility to share lessons learned and best practices with the balance of the nuclear community. Efforts are ongoing to create a framework that allows this information sharing to occur.

4. Transparency will be promoted to ensure that the trust of the society is maintained

Nuclear technology is sustainable only if society trusts that it is safe and secure. In order to maintain this trust, the nuclear industry is committed to transparency and will continue to develop processes and methods for ensuring that public trust is maintained. This includes regulatory inspections and

peer-reviews, which provide confidence in the quality, objectivity and thoroughness of cyber security practices.

5. The nuclear industry must move from a culture of compliance to a culture of excellence in cyber security

We must look for excellence as we have done with institutionalizing the nuclear safety culture. Given the dynamics and risks of the connected world, we must do the same with the cyber security culture.

APPENDIX 1: Acronyms

ABBREVIATION	MEANING	FURTHER EXPLANATION
IEC	International Electronical Commission	A non-profit, non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies
IPPAS	International Physical Protection Advisory Service	An IAEA service to States to independently advise on the states regulatory framework for Nuclear Security and Nuclear security at facilities
OSART	Operational Safety Review Teams	The operational safety services provide advice on selected operational aspects and on safety management and safety culture of nuclear power plants
WANO	World Association of Nuclear Operators	An international, non-profit group of nuclear power plant operators whose primary emphasis is on achieving the highest possible standards of nuclear safety
WINS	World Institute for Nuclear Security	An international non-profit organization of nuclear facilities focused on increasing nuclear security
WNA	World Nuclear Association	An international organization that represents the global nuclear industry whose mission is to promote a wider understanding of nuclear energy among key international influencers by producing authoritative information, developing common industry positions, and contributing to the energy debate.

APPENDIX 2: Advised further reading

Please find below a list of possible interesting sources if you want to access advice on a more detailed level:

DOC / ADDRESS	WHAT
www.iaea.org	Guidance documents developed by IAEA
www.wins.org	Guidance documents developed by WINS
ISO27001	Internationally recognized ISO standard on IT Security
ISA99	Industrial automation and control systems standard.