5. Cultural Challenges

Summary

This chapter describes a cultural divide between nuclear plant personnel, or OT engineers, and cyber security personnel, or IT engineers. Their different ways of thinking result in different priorities that are incompatible and can lead to frictions. One such consequence is that nuclear plant personnel often do not understand the cyber security procedures. Additionally, the procedures are not always clearly written, so that nuclear plant personnel may not know whom to call in the event of a cyber security incident, and may therefore not interpret the recommendations or requirements in the way intended by the IT engineers. These communication problems are exacerbated by limited interaction, as those responsible for cyber security are not based on-site. Furthermore, cyber security training at nuclear facilities is often inadequate, and the lack of drills means that nuclear plant personnel have no opportunity to practise these procedures.

Another concern expressed by those interviewed is that security at nuclear facilities is reactive rather than proactive. While this might work in other areas, in terms of cyber security, personnel at nuclear facilities might not become aware of a cyber attack until it is already substantially under way. The combination of factors discussed above suggests that nuclear plants may lack preparedness for a large-scale cyber security emergency, in particular if one were to occur after normal working hours.

Conflicting priorities and cultural divides

Nuclear plant personnel, who are primarily OT engineers, and cyber security personnel, who are considered IT engineers, often have conflicting priorities. The OT discipline concerns itself primarily with the operations of a plant – such as the industrial control systems, including the remote management of pumps and valves – whereas IT is primarily concerned with computers and networks. Each group has different priorities and ways of thinking. In many cases, these different frames of reference will clash, leading to conflict between the two camps. They may often not even realize that their approaches are different and that this will inevitably lead to clashes.

Safety versus cyber security. Historically the main priority of OT engineers has been to ensure the safe and efficient running of the plant; but for cyber security personnel (or IT engineers), security has been the priority.

Source 5 describes a recent IAEA meeting in which the OT engineers (also termed 'safety engineers') and the IT engineers (also called 'security engineers') were approaching the discussions from such different perspectives that they could not understand each other:

> The safety engineers wanted the security engineers to add security to a system, but were telling the security engineers, 'You can't touch the rest of the tests. We have done 19 tests. You're the last test, test 20.' They were bent on making sure that the security engineers did not invalidate any of the previous safety tests. They were essentially saying, 'Just make sure it is right for us and don't violate any of the previous tests.'

In reality, it is simply not possible to treat security as a bolt-on extra to safety in this scenario, because the IT engineers cannot introduce security without risking a change that would invalidate the safety case. For example, a valve controller may have a detailed safety case that has been approved by the plant, but with little or no security to protect the device from interference. If the plant decides to add security to this valve controller, doing so may invalidate some of the safety tests that have already been done, or there might even be unexpected incompatibilities between the security system and the safety system. The system might then behave in such a way that it would no longer be safe. This would be especially true if the nuclear plant wanted to connect the valve controller to the network, in order to gain easier access to data generated by the equipment.

> The reason that the security engineers don't understand is that it is not practical, not possible; you cannot defend a system without altering its state. And so when the safety engineers say, 'You can't alter the state,' the security engineers say, 'In that case we can't defend it.' (Source 5)

Availability versus security. OT engineers prioritize maintaining availability (in other words, keeping the plant running continuously), while cyber security personnel (or IT engineers), as discussed above, regard security as their key focus.

Yet it is not always possible to promote availability and security at the same time. For example, 'patching' a system against a known vulnerability might mean that the system will be unavailable during installation and testing (see Chapter 6). Rather than reducing the system's availability, the OT engineers will often prefer not to patch. From an IT engineer's perspective, patching is a way to improve security against the growing number of cyber security threats. On a larger scale, IT engineers could be in a position where, to maintain the security of a facility's systems, they might require a shutdown of the plant in order to eliminate a cyber security threat – which directly conflicts with the needs of OT engineers.

> On one side, nuclear wants availability as key priority. Cyber wants security as key priority. And often they can't cohabit well. That's the real fight. (Source 25)

Unintentional (accidental) versus intentional (malicious). OT engineers are primarily concerned with preventing accidents and other unintentional acts. This concern derives directly from their focus on safety. By contrast, cyber security personnel (or IT engineers) tend to focus on preventing intentional acts which might harm the plant, namely malicious attacks (although they are also concerned about unintentional events).

OT engineers' long-standing focus on safety and guarding against accidents means that they have developed rigorous methods of statistical analysis. They approach problems by doing a causal fault analysis, which allows them to look at everything that could theoretically go wrong, the probabilities that all possible events might occur, and what the underlying causes could be. This approach is so central to their culture that they expect the IT engineers to show them the same kind of causal analysis. But IT engineers are not trained to approach problems in this way. The need to consider the intentional threat means that there are simply too many potential, unpredictable events for such an analysis to be undertaken. For example, attackers could make use of zero-day vulnerabilities and other attack technologies that have never been seen before, and new threat actors could emerge.

Frictions between nuclear plant (OT) personnel and cyber security (IT) personnel

Given the conflicting goals and mindsets of nuclear plant personnel and cyber security personnel, it is not surprising that at times some degree of animosity manifests itself between the two. Interviews with personnel from both camps have provided useful anecdotes that further illustrate these frictions and explain some of the underlying causes.

Source 8 emphasized that OT engineers' general dislike of IT engineers is a major part of the cyber security challenge:

> The problem is as much cultural and sociological as it is technical. One of the biggest problems we have is that – as in any industry – the operations people dislike IT.

Source 25, an IT engineer, attempted to view the situation from the OT engineers' perspective:

> I can understand why nuclear plant managers don't like us, because they think we are painful. We come in at the end of a procedure that works [and say that all of these cyber security measures must be added]. We add in cyber security in order to protect them, but from their perspective they don't see the benefit.

Part of the problem can be attributed to the belief among some nuclear plant personnel that cyber security does not pose a real threat; they thus tend to regard the cyber security measures imposed on them by IT engineers as a nuisance, rather than as an important contribution to the security of the plant.

Source 6, an OT engineer who worked for over 10 years in two different nuclear plants in the United States, expressed a number of frustrations with IT engineers. He does not trust their qualifications, particularly as they are rarely nuclear engineers, and believes that they do not understand how a nuclear plant functions. He noted:

> I've never been convinced that if we ever implemented the [cyber emergency] procedure, the guy was even qualified. Certainly not qualified to the extent I was, where I had to go through schools. He might be the biggest computer wizard in the world, he had no idea how a nuclear plant worked.

Without this fundamental understanding, in his view, IT engineers cannot understand why stabilizing the reactor is so essential. As a result, many IT engineers would be unhappy if nuclear plant personnel prevented them from working on an IT problem because the nuclear plant personnel first needed to stabilize the reactor; the IT engineers would not understand why it should take priority.

The extent of the mistrust is such that Source 6 expressed doubts about whether he could rely on the IT engineers in the event of an emergency. He suggested that the IT engineers do not have enough of a work ethic, commenting that 'They want to get the job done as fast as possible so that they can go home. They are not 24/7 workers like we are' – the implication being that IT engineers were less likely to be available in an incident occurring outside standard working hours. Unlike nuclear plant personnel, who are accustomed to receiving urgent calls in the middle of the night, the cyber security personnel tasked with responding tend to be corporate middle managers who are not normally required to deal with out-of-hours calls, and it was felt they might not fully appreciate their critical nature.

The same source observed that IT engineers often wish to know the full extent of a problem before making a decision, or in some cases need to seek permission from the appropriate authority in their management structure before taking action – meaning they might not be able to make decisions quickly enough in the event of an incident. Moreover, unlike nuclear plant personnel, cyber security personnel do not have the requirements on fitness for duty (including working-hour limitations and rules governing alcohol consumption before reporting for a shift), so an OT engineer would not know if an IT engineer responding to a cyber incident had been up all night or was unwell.

Source 6 recounted how in the nuclear plants in which he had worked, the IT engineers developed cyber security procedure documents for the nuclear plant personnel that directed them to stop what they were doing in the event of a cyber incident, to touch nothing, and to call in the cyber security personnel. They did not explain to the nuclear plant personnel the nature of the cyber security risks, how to deal with them, or the rationale behind the procedures:

> The safety of the reactor was always firmly my responsibility. For all the other procedures, for example, if there was a problem with a feed pump, the person in charge fully understood every step and why they were doing it. The reason for that is, in case you got to that step and there was a problem with the equipment, you could devise a solution. So the stuff about 'Stop what you're doing, don't touch any critical control systems' [is surprising].

In addition to the tone being perceived as somewhat offensive by nuclear plant personnel, one problem with such an approach is that in some cases it may be clear that an incident has occurred but the source – whether due to a cyber security incident or otherwise – may be unknown. Therefore, nuclear plant personnel cannot know whether they should call in the cyber security personnel, and the limited information they receive on dealing with cyber security incidents will make it harder for them to diagnose the cause.

Unclear procedures

The interviews also revealed that **nuclear plant personnel often do not understand the cyber security procedures, including those to follow in a cyber-related emergency.** Even the most experienced nuclear plant personnel reported difficulty in understanding the procedures as communicated in the documentation.

> The procedures are confusing as hell … I didn't really understand the procedures. What I knew is that if a cyber incident happened, the first step was that I was supposed to tell the operators to stop what they are doing and not touch any critical control systems. And then the second step, after informing security, was that I was supposed to call whomever the cyber person on call was. (Source 6)

Often, **this is because the procedures are not clearly written.** Nuclear plant personnel report finding the cyber security procedures so hard to understand that they do not always know whom to call in the event of a cyber security incident. In one case, while the procedures documents provided a flow chart of who among the cyber security personnel should be called in such an event, the chart was unclear. Source 6 added:

> It would be like, 'call the director of engineering, who will call someone else, who will then call someone else'. I had no idea who they were and was never sure who the right guy was, who the cyber expert to call was.

In fact, the difficulty understanding the procedures is not limited to OT engineers. The **physical security personnel at nuclear plants,** who must implement IT requirements at times, also **have difficulty understanding cyber security procedures.** Source 7 commented:

> What is frustrating for the [nuclear] security professional is that some of the recommendations are badly written, unclear, and just don't make any sense. Sometimes it is hard to understand what the recommendations are.

Given that the procedures documents were written by IT engineers, with their very different approach and ways of thinking, this is hardly surprising. The nuclear plant personnel's difficulties in understanding the documents are a clear manifestation of the cultural divide. As Source 8 explains, 'One reason the guidelines are unclear is that they were written from an IT security perspective.'

The consequence of this is that the **interpretation of recommendations or requirements by nuclear plant personnel may be very different from that intended by the IT engineers.** OT and IT engineers literally often take different meanings from the same phrase. For example, for OT engineers a 'denial of service' might mean that a 10,000 horsepower main coolant pump in a nuclear plant has shut down. For IT engineers, a 'denial of service' occurs when a malicious flood of data makes a computing resource unavailable.

As another example, although the cyber security procedures instruct nuclear plant personnel not to touch any 'critical control systems' in the event of an incident, it does not detail which system or systems should be regarded as critical. Nuclear plant personnel are thus expected to use their discretion, and their conclusions may be very different from those envisaged by the authors of the cyber security procedures.

Similarly, physical security personnel at nuclear plants might interpret the phrase 'intrusion detection system' as a gate monitor or a card reader. To an IT engineer, an 'intrusion detection system' monitors a network for suspicious traffic.

> The security professional and the IT professional will have a different interpretation of what exactly IT security compliance means; a security professional and an IT professional may have different views on what a control actually is because the documents are badly written. (Source 7)

Another consequence of the cultural divide is that **personnel at nuclear facilities often have difficulty determining what their critical cyber assets are.** For example, in one plant, one of the most critical controllers – the pumps that are used to bring water back into the plant after a loss of feed water event – had its push button located in the highly secure control room but its PLC was in a building that required key card access but was not a vital area. In the United States, there have been some promising recent initiatives to encourage nuclear plant personnel to work with cyber security personnel in order to agree on which assets are cyber critical and need to be prioritized for protection, but more such efforts are needed.

Limited interaction

These communication problems between nuclear plant personnel and cyber security personnel are magnified by the limited interaction between the two. A significant part of the challenge is that **those responsible for cyber security at nuclear facilities are not based on-site** and in fact are often located some distance away; there are thus limited opportunities for the nuclear plant and cyber security personnel to interact in person. Moreover, among the latter, responsibility is often highly dispersed. Thus for most nuclear plant personnel their main contact with the IT engineers is when they come out to the plant on occasion to make repairs. However, these would be unlikely to be the same people who would be responding to a cyber incident.

> No plants in the country have cyber expertise on site. I think that it's all corporate people and that they are not even around. I had no idea who they were. I just knew that they worked in an office that was maybe 100 miles away. (Source 6)

Training issues

It appears that **the level and quality of cyber security training at nuclear facilities are often low compared with the mandatory training for nuclear personnel in other areas.** In particular, some organizations undertaking the training may not have sufficient expertise to do so. Source 23 commented:

> Many companies propose training sessions, but not all of them are equally rigorous. The right people are not always doing the training. Many companies and foundations take norms and say that they can train people, without there being any accreditation process.

Source 6 commented that his training consisted of watching a film (which was not particularly informative) once a year, reading the cyber security procedures documents, and taking an exam based on these procedures. As such, the training also did not address what was happening from a cyber security perspective or how to coordinate with the cyber security personnel. This inadequacy of training is very likely to stem from the nuclear industry's perception that cyber threats are not a high risk.

In particular, the **lack of drills** is a problem since there is no opportunity for nuclear personnel to practise cyber security incident procedures. By contrast, nuclear facilities have regular drills for other scenarios, including integrated drills with the physical security personnel to prepare for the event of an attemped invasion.

The inadequacy of the training is such that when nuclear plant personnel are tested on the cyber security procedures, they may not understand the questions properly and often fail, whereas they obtain high scores in the frequent tests they must take on other procedures.

A reactive rather than proactive approach

Another concern is that **cyber security at nuclear facilities is reactive rather than proactive;** in other words, the focus is on reacting and responding to incidents as they arise, rather than proactively seeking to prevent attacks. In general, defences at nuclear facilities (e.g. physical security) rely on receiving warnings of an imminent attack. For example, if a plane were heading towards a nuclear facility located in the United States, the Federal Aviation Administration would call the facility to alert personnel there.

> Many procedures for reacting to events at nuclear facilities are based on warnings of either an imminent threat or of an event that has occurred … It's all reactive, based on somebody in the plant seeing that something has happened. (Source 6)

> We're reactive to a large extent, something happens in the industry and we learn from it. I can assure you that what happened in South Korea back in December [2014] is going to cause a lot of changes in the way operators and states think of cyber security. (Source 3)

When it comes to a cyber attack, however, there are no such warning mechanisms in place. In fact, as discussed above, **a nuclear facility might not know of a cyber attack until it is already substantially under way.** For example, a hacker could introduce a logic bomb that lies dormant until it is activated to cause physical damage. In the case of the Natanz and Bushehr nuclear facilities in Iran, the nuclear plant personnel knew that their centrifuges were breaking apart. However, it was only months later that they realized that the Stuxnet worm was the cause. In addition, the ease with which malicious code can be hidden makes implementing such a warning system more difficult than in other domains, and in some cases it may be impossible.

Lack of preparedness for a large-scale cyber security emergency

The combination of factors discussed above suggests that **nuclear plants lack preparedness for a large-scale cyber security emergency,** and there would be considerable problems in trying to coordinate an adequate response.

A large-scale cyber security emergency occurring at night could be particularly dangerous. The most confusing time for a system to go out of service is during this time. Of course, there might be an on-call team doing virus scans or other diagnostics, but these are only basic measures, and as Source 6 explained:

> When we have to call people in the middle of the night for other issues that are just as important, like a pump breaking, the response can be slow. If you're calling people at 1 am, it takes them a few minutes to wake up. And say you have 10 people who need to be on the call. By the time you get everyone to dial in, it can take over an hour.

6. Technical Challenges

Summary

This chapter assesses some of the technical challenges involved in providing cyber security at nuclear facilities. Above all, early designs of nuclear facilities – before cyber attacks were a concern – means that they are insecure by design, lacking basic safeguards including authentication and encryption. This means that cyber security at nuclear facilities depends in large part on the successful defence of the network perimeter – all the more so because the flexibility of code means that any attacker who can get past the perimeter defences would be able to make logic changes in the code that are almost impossible to observe. Furthermore, some cyber security techniques such as patching that are standard in home or office IT environments are difficult to implement within nuclear facilities. Lastly, it is extremely difficult to guarantee the integrity of the supply chain.

'Insecure by design'

A major challenge for the nuclear industry, as for most critical infrastructure, is that **cyber security measures were not designed into industrial control systems from the beginning.** The control systems in most nuclear facilities were developed in the 1960s or 1970s when computing was in its infancy and designers gave no thought to the possibility that an actor with a malicious agenda might deliberately try to attack a computer system using electronic means. Against this background, systems were not designed and built with protection against cyber attack in mind, and 'retrofitting' cyber security measures to these original systems now is technically challenging and expensive. Source 3 observed:

> A couple of minor tweaks in how you think about a system right at the very beginning can have huge implications for its security. If security wasn't built in at conception, it is difficult to bolt on after the fact. Actually, it is going to require a redesign.

One example of the 'insecure by design' nature of industrial control systems is the **lack of authentication and verification.** That is, field devices do not require authentication that a command sent to them is a valid command, or verification that it comes from a legitimate source. They are designed to do what they are told without question. This means that any attacker who is able to gain access can just send a command to the device and it will comply. As a result, industrial control systems are particularly vulnerable to man-in-the-middle attacks that alter the communication between two devices:

> The field devices accept the message immediately, without asking. The receiving device does not have to authenticate. Control systems are thus very fragile due to man-in-the-middle attacks. (Source 29)

> You can tell the field device to do whatever you want and it will just say, 'OK, you command, I'll do it.' … The most skilled attackers won't even bother with finding vulnerabilities, they'll use features instead. (Source 13)

Furthermore, **the flexibility of code means that an attacker can change the logic,** or the set of programming instructions, for a piece of equipment in order to cause it to behave differently. This was exploited by the Stuxnet worm. Logic changes are difficult to detect and are therefore a major concern. While it would be technically feasible to examine the code to determine whether any lines had been changed, in practical terms the task would be immense because a typical system could contain billions of lines of code.

This difficulty is exacerbated by the lack of cyber forensics for control systems. For example, they do not generally have log files that maintain records of which parts of the system have been accessed, who accessed them, which information was viewed, and at what date and time. Without a log, it is much more difficult for cyber specialists to determine whether a hacker has gained access or changed anything in the code.

A major implication of the existence of 'insecure by design' systems at a nuclear facility is that such systems rely entirely on network perimeter defence to protect them from attack. If a hacker is able to breach the network perimeter, then the lack of authentication and the flexibility of code provide a number of opportunities to inflict significant damage on the facility.

> It is almost impossible to protect the system once someone gains access to it. That means that right now, we're entirely reliant on the perimeter to stop hackers. (Source 13)

Patching difficulties

The unique aspects of industrial environments (and particularly nuclear facilities) mean that **standard cyber security measures used in everyday home or office IT environments are not necessarily applicable.** Cyber security experts urge home and office users to install patches that will address vulnerabilities discovered in software. Yet patching at nuclear plants presents unique challenges, and is therefore infrequently used.

> Patching is really challenging, and the reality is that very few people are actually installing any patches. (Source 3)

First, unlike in everyday home and office IT environments, patches are less likely to be available for the systems being used. Since these are predominantly legacy systems kept in service for at least 20–30 years, unlike those in home or office environments, many are no longer supported by the vendor. A number of facilities have very old MS-DOS or Windows NT operating systems, for which Microsoft no longer issues patches (or at least, not at a reasonable cost). In some instances the vendor may no longer be in business.

Furthermore, patches risk breaking the system that they are trying to protect. A patch may not be compatible with other software or hardware on a system, thereby causing the entire system to malfunction, or it might have unintended and unforeseen effects. Since the utmost priority is maintaining the availability of the plant, and a patch which does not perform as expected could take an entire plant offline, some operators consider the risk of patching to be too high. Source 3 noted: 'I've seen patches break systems, where they actually disable the system.' In home and office environments the consequences are much less severe and can usually be corrected fairly quickly.

Since the utmost priority is maintaining the availability of the plant, and a patch which does not perform as expected could take an entire plant offline, some operators consider the risk of patching to be too high.

Even if a patch has been approved for software that runs on a vendor's equipment, this does not necessarily guarantee that it is safe to install. The mere presence of one additional piece of software, such as a plug-in, running on a system in a nuclear facility can create an incompatibility with the patch and break the system. The vendor will have tested that the patch is safe in several standard cases, but cannot possibly test every combination of software that a nuclear facility might be running.

> Just because your automation vendor has certified a patch, you don't know whether, because you've got that system with some other plug-in, it's going to have a negative impact. (Source 26)

The unique characteristics of industrial environments like nuclear facilities mean that even patching a facility's commercial network could have significant consequences. It might be reasonable to assume that a facility's commercial network is an 'everyday' office IT environment and that a patching problem there would only affect that network. Yet its interconnectedness with the industrial control systems means that a problem with a patch could affect both systems. As noted in Box 1, at the Hatch nuclear plant in Georgia in 2008, a patch was applied to the business network in order to synchronize it with the industrial control system network. Unfortunately, it introduced incorrect data onto an industrial control system, triggering an automatic plant shutdown.

Owing to the risk of a patch breaking a system, nuclear facilities, again unlike everyday home and office IT environments, must test patches extensively and intensively before they can install them. Patches that affect key systems cannot be applied and tested on the system directly without the risk of taking an entire plant offline. Instead, nuclear facilities often need to set up a costly partial or complete duplicate system to serve as a test bed.[8]

> Having a duplicate system is enormously expensive. And even then, you'll never literally have two identical nuclear reactors. Yet, to have absolutely accurate testing, you would need literally the exact same thing twice. (Source 9)

Even if a patch is available and has been tested, finding a time window in which to apply it is often difficult. Nuclear facilities operate 24 hours a day, but the plant would need to be shut down in order to apply patches, especially if they affect key systems. Some systems provide such essential capability for the running of the facility that even taking them temporarily out of service would compromise the plant's safe operation. Nuclear power plants might typically shut down for maintenance every two years, so installing a patch may not be possible until a scheduled shutdown occurs. Again, this is in contrast to everyday home and office IT environments, where patches can easily be installed during downtime.

> You have to be assured that you have even got a change window. Now, if you have a change window, then potentially the organizations themselves have to take a break from operations, and you are talking about a 24/7 operation. (Source 26)

> Operators are not going to be willing to shut a unit down for three days to install a patch for a vulnerability that somebody might or might not exploit. (Source 3)

Since patching changes the configuration of a system, in a nuclear plant it also makes it harder to monitor the system for unusual behaviour that might indicate infection by malware. Among nuclear operators, the instinct is to avoid making changes to a system so that the operator can acquire a deep understanding of how that system works; the moment a patch is installed, however, the system has changed and the operator no longer has the same depth of understanding of its behaviour. Patching would thus considerably reduce the effectiveness of monitoring techniques, which look for behavioural anomalies. Yet again, this is in marked contrast to changes to the configuration of systems in everyday

[8] Creating a test-bed for a nuclear facility is particularly complex because of the prevalence of legacy systems. Many of the components used at nuclear facilities are no longer manufactured, so operators must try to purchase them on markets for old equipment. Moreover, the equipment must be absolutely identical in order to test a patch properly, since just one difference in a component could cause the duplicate system to react in an entirely different manner. For example, if a computer in a nuclear facility is running Windows 98, then an operator must obtain a Windows 98 computer that has exactly the same graphics card, network card and other elements for the test bed. In procuring components for a test bed, for either legacy or new equipment, part substitutions made by the device manufacturers can present real problems. For example, if an operator buys a personal computer in January and then purchases exactly the same model in March, it is possible that the manufacturer could have changed a small number of components in those three months: even if the two computers are seemingly the same model from the same manufacturer, they may not be identical. Yet even small differences such as these could cause the duplicate system to react in a different manner during testing.

home and office IT environments, which change (and are patched) regularly.

> The default position is that, as you develop and field test a system, that's the way it stays. Industrial operators do that because it works. Every change you make introduces uncertainties and always will. (Source 9)

Finally, patching is a never-ending cycle with new vulnerabilities always being discovered and with them the requirement for new patches.

> You could spend all this time patching your systems and, tomorrow, they will be just as outdated as they were before you patched. (Source 27)

This challenge is magnified by the large number of systems that need to be patched in a nuclear facility. For patching to be effective, an operator could be faced with the requirement to patch every single device in that facility on a regular basis, but there will always be a significant period after the discovery of a vulnerability when a system will be known to be vulnerable while the vendor develops a patch, which then has to be tested. This process could at best take weeks or months, but in many cases it could take years.

> In order to limit your exposure, you need to patch everything. You need to patch your switches, you need to patch your firewalls, you need to patch embedded devices. (Source 27)

It seems, therefore, that each nuclear facility must carefully assess the advantages and disadvantages of patching in each instance. Many appear to have decided that the risks outweigh the benefits and choose not to patch.

Supply chain challenges

Supply chain vulnerabilities are a growing concern since the equipment used at a nuclear facility (and in critical infrastructure more generally) could be compromised at any stage. Backdoor access or exploits could be introduced, for instance, at the vendor's facility, when the equipment is being designed and assembled, or at the locales of any of the subcontractors. For reasons of cost efficiency, vendors are likely to make use of sub-components from other sources, including those produced in other countries. Even the transportation phase is liable to tampering. The Snowden revelations[9] provided evidence that the United States' National Security Agency (NSA) intercepted routers and other network devices being shipped overseas and implanted backdoors, or means of obtaining unauthorized remote access to computer systems (Greenwald, 2014). Source 28 comments:

> We really have no way to defend against supply chain risks in a cyber warfare situation: a computer or system could be compromised in transit or at the place of manufacture.

Although supply chain threats are at present primarily confined to a small number of state actors seeking to prepare the terrain for cyber conflict scenarios, it is possible that terrorist groups or even hackers could adopt such tactics as well.

Of course, intelligence agencies across the world are concerned by these vulnerabilities – particularly in the wake of the Snowden revelations – and a number of countries are increasingly seeking to nationalize their supply chains. However, the reality of globalization is that very few countries are capable of producing all the required parts of a nuclear plant themselves. According to Source 5:

> The US would like to do that [produce all its own components], but I don't think the US can do it anymore. I don't think anybody's in a position to do this.

For instance, just one computer used at a nuclear facility is comprised of thousands of parts. Among these, it is almost inevitable that there might be, say, a tiny chip made in Taiwan, or some other foreign sub-component.

[9] In May 2013 former NSA contractor Edward Snowden leaked tens of thousands of sensitive and classified documents involving US-led surveillance activities.

7. Meeting the Challenges: the Way Forward

Summary

Meeting the challenges described in the previous chapters will require a blend of policy and technical measures. This chapter proposes a series of solutions centred around several key themes. There is above all a need for improved risk assessment guidelines on cyber security at nuclear facilities, which will provide a solid economic underpinning for investment. The 'human factor' can best be handled through a combination of better communication about the risks of poor 'cyber hygiene' and stronger enforcement measures.

Improving disclosure and information-sharing could be achieved by encouraging anonymous sharing, fostering personal contacts at international conferences, and the establishment of industrial CERTs. There is also a need for regulatory standards and more funding for agencies like the IAEA. The cultural divide might be bridged by measures such as encouraging IT engineers to visit nuclear plants, cross-disciplinary educational programmes, and improving cyber security training.

Technical measures such as avoiding the use of non-essential digital features, implementing whitelisting (authorization) technologies, network monitoring, and encouraging the adoption of data diodes can all enhance cyber security. Countries can mitigate supply chain risk by reducing their dependency on foreign components.

Assessing the risk – and attracting investment

Given that many in the nuclear industry do not believe that cyber security poses a real risk to nuclear facilities, a first step is to raise awareness of the challenge. One way to do so would be through the **development of guidelines on ways of measuring cyber security risks in the nuclear industry.** Since at present there is no risk assessment methodology that would permit a nuclear facility to perform a combined safety risk and security risk assessment (only a safety risk assessment and a separate security assessment, which includes cyber security risk), such guidelines include the need for a **combined risk assessment methodology for safety and security.** Developing a methodology will require reflection within the industry, perhaps led by the IAEA's Interface Group, which was formed to address conflicting priorities between safety and security.

A greater understanding of the risk will also help to tackle the challenge of insufficient spending on cyber security in the industry. In addition to **raising awareness of the need to invest in cyber security,** it will **make cyber security more commercially attractive** and provide a clear economic rationale for CEOs and corporate boards to increase expenditure on it.

Since the insurance industry requires solid risk assessments, promoting the further development and adoption of cyber insurance in the nuclear sector might also be beneficial in helping develop these guidelines to measure cyber risk; **cyber insurance may therefore be an important tool to enhance cyber security.** The French government has been conducting a major study on this question. An early conclusion is that to succeed (and to find the right level of underwriters' exposure when measured against the cyber security risk), a key need is the accurate calculation of that risk based on metrics agreed between insurers and the insured.

> What underwriters need is an understanding of the risk and that really comes down to, do organizations have the right people in the right places, with the right authorities, to make the right decisions and have the right policy and operational structures in place? (Source 9)

Insurance may also make cyber security more commercially attractive and drive the process of implementing appropriate measures, by providing the necessary financial incentives (in the form of lower premiums) to persuade owner-operators to invest in them.

> If an insurance company tells an owner-operator that their insurance premium would be very high because they don't have adequate cyber security measures, the owner-operator might just conclude, 'if I spend $100,000 on cyber security measures, I can save $200,000 on the insurance premium'. (Source 10)

Handling the 'human factor'

Given that part of the challenge stems from the 'human factor' – such as engineers or contractors who set up rogue or unauthorized connections or those who plug their home laptops directly into nuclear facility networks – **raising awareness among the personnel involved** of the inherent dangers in doing so will be key.

There is also a need for nuclear facilities to **establish rules where they are not in place already.** For instance, in countries or facilities where personal devices are not already expressly forbidden within nuclear facilities, engineers should be required to hand in any personal devices such as laptops when they enter the facility; the devices should only be returned to the engineers when they depart.

> Engineers should be required to turn in any personal laptops that they bring to the plant. (Source 7)

> If you are going to do any testing and have any kind of device of your own, you should have to turn it in and we will issue it back to you when you bring our laptop back. (Source 6)

There is also a need for rules requiring nuclear plant personnel to **change the default passwords on equipment** to secure passwords; this should apply to both existing equipment and to any new equipment installed.

In order to ensure that engineers actually follow such policies, **enforcement** is key. In particular, independent verification methods, in which multiple personnel check compliance with procedures, should be rigorously followed for cyber security issues. Source 6 suggested that if a device has been signed out, an assigned person should independently check that it is the correct device before it is hooked up to a nuclear plant; a person should also be assigned to run a virus scan on the device.

Technical means can also be used to help enforce compliance. For example, given that nuclear plant personnel may plug USB devices into the nuclear facility computers even though this is not allowed, owner-operators may want to glue USB ports.

> People working in nuclear plants might be more willing to put up with glued ports than they would in a standard IT environment. Glued ports within a plant room probably do not impact productivity; they just make it hard for someone to charge his iPhone. On the other hand, glued USB ports in an IT environment would definitely impact the effectiveness of employees. (Source 26)

Another option is to ensure that USB devices are checked for malware and cleaned before they are allowed into nuclear facilities. One company has developed a technology to do so.

> There is company down in the south of France that has developed technology that provides USB cleaning devices. So we're not saying don't bring your USB to work, but can we at least plug that USB into a special device that will examine all of the data that's on it, it will execute the files that are executable and make sure that there's no malicious software on them before the person plugs that USB stick directly into a critical asset. (Source 26)

Promoting disclosure and information-sharing

Since the industry reluctance to share information about cyber attacks that have occurred stems partly from concern about potential damage to reputation, encouraging nuclear facilities to **share threat information anonymously** would promote greater disclosure. Anonymity could be achieved by asking facilities to **share 'indicators of compromise',** which are traces left on a network or system that indicate a malicious actor has been in the system. These might include phishing emails, the IP addresses from which an attack was launched, or the malware code itself. In sharing indicators of compromise, nuclear facilities do not have to reveal their identity, nor what the impact of the attack has been.

> Sharing indicators of compromise can help the whole industry and improve security. We could anonymously share indicators of compromise without knowing who it was that was breached. (Source 26)

Given that nuclear facilities tend to focus on reacting to attacks as they unfold, another benefit of sharing indicators of compromise is that it would **encourage a proactive approach** to preventing attacks. In communicating valuable information about prevalent attacks – including the types of vulnerabilities exploited by hackers, attack pathways used to gain access, and systems targeted – sharing indicators of compromise would provide others with an early warning of such an attack. This would enable them to put defensive countermeasures in place, perhaps by increasing monitoring or by deciding to patch systems that are identified as particularly vulnerable.

Anonymous sharing has been successful in other fields. As Source 5 commented:

> The airline industry … has set up a platform in which pilots and other industry personnel can anonymously report incidents (for example, if two aircraft come too close to each other); this approach has helped increase disclosure and enhance the safety of the industry.

Such mechanisms could be copied and adapted in the nuclear industry and in the industrial sector more generally.

Fostering personal contacts, which are central for the trust-building required for information-sharing, is also key for promoting the exchange of information at both national and international levels. People may not trust other companies – or governments, for that matter – but they do trust other individuals with whom they have developed strong personal relationships; they are therefore prepared to take the risk of sharing information with them. International conferences can be an important avenue for building these relationships, and more such initiatives in the nuclear industry (and critical infrastructure more broadly) should be encouraged.

> Personal contacts are always best for information-sharing; these trusted environments work best where they co-align common interests of countries or organizations and also personal relationships. (Source 5)

> Conferences where people meet with each other are very important, because when people personally know one another they will not want to attack each other in a cyber warfare scenario. There are not that many nuclear plants in the world, so this should be possible to implement; there needs to be a sense of community. (Source 11)

Although governments are concerned that sharing threat information with other governments could jeopardize national security and thus are reluctant to collaborate at the international level, they recognize that at the national level such sharing is a key priority for defence. Governments can therefore play a key role in encouraging information-sharing within their own countries by **leading the establishment of national Computer Emergency Response Teams specialized in industrial control systems.**

The unique characteristics of industrial control systems mean that CERTs specifically dedicated to industrial control systems will be more effective. In fact, the United States has achieved success with its Industrial Control Systems

CERT (or ICS-CERT) established in 2009, which operates in addition to the national CERT (referred to as US-CERT). Of course, for countries that have yet to establish national CERTs, doing so is a first priority and ICS can be handled as a division within these as a first step.

Regulators need to understand that in order to foster a more proactive cyber security culture in the nuclear sector, they should be content to stay remote from some of the necessary dialogue between stakeholders.

Some measure of government-backed international sharing can also take place between close allies. One avenue for this is the national CERTs; **encouraging greater information-sharing between national CERTs could prove beneficial.** At present, there is only limited information-sharing between CERTs on an informal, ad hoc basis (Sources 19–22). Even though some governments will take more information than they contribute, this will still strengthen cyber security. Many in the industry feel that any information-sharing, however limited, is still better than the current minimal situation.

> It would be helpful to have greater information-sharing between the CERTs. Of course, most countries will want to take information but not give it. But if you allow countries to give what they want and take what they want, it's not ideal, but it's much better than what we have today because today we don't have anything. (Source 25)

Furthermore, given that owner-operators can be wary of disclosing cyber security breaches or incidents in case they are held liable, creating an environment where they feel they can speak candidly without fear of repercussions is key to increasing the level of reporting to ICS-CERTs (or CERTs more generally). The **regulator should reassure owner-operators that they will not be penalized** for any information they share – provided they show good faith – and that, if they disclose a cyber security problem or incident that arose because they violated the code, they will not be prosecuted. According to Source 20: 'To enable information-sharing, you need to develop a culture where whatever you say will not be used against you.'

Regulators thus need to understand that in order to foster a more proactive cyber security culture in the nuclear sector, they should be content to stay remote from some of the necessary dialogue between stakeholders; that their prime focus is on outcomes, rather than on the mechanics of delivering a minimum level of security. They also need to be aware of the difficulties of security in the electronic medium, and take a pragmatic approach to enforcement. Every system, whether it is air gapped, patched or otherwise protected, is liable to intrusion; as long as the root cause of a particular breach is not negligence or purposeful violation of rules, then regulators should only be concerned that the nuclear sector should learn from its experiences as the cyber security culture develops over time and corresponding capabilities are developed.

Developing international policy measures

A number of policy measures would be beneficial as well. Given that only a small number of nations have implemented regulations regarding cyber security at nuclear facilities, the remaining countries should be encouraged to **adopt regulatory standards.** Since a large number of countries follow IAEA guidance, the agency's further development of its work on cyber security at nuclear facilities will prove beneficial. This can be encouraged by **allocating more resources to the IAEA (and other agencies)** to enable them to deal more effectively with cyber security threats.

Particular attention should be dedicated to helping developing countries improve their cyber security readiness in the nuclear sector, given their greater vulnerability. These countries are likely to require funding assistance as well to enable them to achieve this.

Bridging communication gaps

In order to overcome the communication barriers between nuclear plant personnel (OT engineers) and cyber security personnel (IT engineers), **fostering face-to-face communication between the two groups** will be essential. For example, it is important that the cyber security personnel physically visit nuclear facilities on a regular basis. As cost-saving measures, they will be tempted to use methods of remote collaboration, but face-to-face contact is key to promoting mutual understanding between the two cultures. In particular, **encouraging nuclear plant personnel and cyber security personnel to work together on integrated projects** would allow them to gain greater appreciation of each other's ways of thinking. This might involve working together on joint vulnerability analyses or risk assessments, for example. It would also help raise general awareness of cyber security risks among nuclear plant personnel.

> Actually getting the IT guys to work in the plant, to sit with the engineers and work with them, to deploy stuff in OT environments is how you ensure that IT and OT understand each other. (Source 26)

> You need an IT security professional to talk to the on-site security professional so that they can understand the same language. (Source 7)

It will be important to **improve cyber security training at nuclear facilities.** Given that one problem identified is that some of the training may be conducted by groups without sufficient qualifications, there may be a need for **accreditation of training programmes.** Source 24 suggests that the IAEA would be the one vehicle that could provide international accreditation.

In addition, training quality and frequency could be enhanced by **holding integrated drills** on a regular basis. This will also provide an additional avenue for communication between the two groups that will help reduce the cultural divide.

There is also an urgent need for more **cross-disciplinary university and professional programmes.** Interdisciplinary programmes on the cyber security of industrial control systems within the nuclear industry, which include both computer science and engineering disciplines, are now being established, and the creation of more such programmes should be promoted in order to help bridge the cultural gap and start to usher in cultural change within the industry (IAEA, 2014a).

Another initiative to improve communication, in view of the limited dialogue between cyber security companies and vendors, is to **encourage more partnerships between cyber security specialists and vendors.** Deeper knowledge of how vendors' propriety protocols work will enable cyber security companies to provide better security protection for these products. According to Source 25, the cyber security company McAfee has recently signed partnership contracts with vendors such as Alstom and Schneider for this purpose.

Enhancing security

Given that most industrial control systems were designed without considering cyber security requirements – and that, as noted above, it is difficult to 'add on' cyber security at a later date – it is essential that the designers of future generations of control systems take cyber security into account during the initial conception phase. For example, ICS should **avoid the inclusion of non-essential digital features** that could introduce cyber security weaknesses; otherwise, removing such features will require partial or complete redesign. In practical terms this may mean that particularly important functions should not be digitized.

> A couple of minor tweaks in how you think about a system right at the very beginning can have huge implications for the security. If a certain function is particularly important, you might make the decision that you don't even want a computer involved. (Source 3)

Additionally, given that the growing uptake of digital systems is leading to a reduction in redundancy, it is important for nuclear facilities to realize this and to **ensure that sufficient redundancy is retained.** This may involve, for example, making certain that there are manual backups for critical systems in the event of a failure.

Encouraging the greater adoption of authentication and encryption technologies in future generations of ICS will also be key, since their lack contributes to making SCADA systems 'insecure by design'. Adding authentication when sending and receiving communications or commands means that the different parts of a SCADA system have to prove their identity to each other – and that the communication or command being transmitted is legitimate. It makes it harder to carry out cyber attacks that send an unauthorized command to a device that automatically accepts it, or that falsify communications (as happened with Stuxnet, for example). And adding encryption to authentication would also make the contents of the communications or commands unintelligible to hackers, providing an even greater level of security. Source 29 confirms: 'The solutions to the 'insecurity by design' challenge will involve encryption and authentication.'

Given that the unprecedented flexibility of the current generation of ICS also makes them 'insecure by design', it will be vital to restrict their malleability. While the specific nature of industrial environments means they face particular cyber security challenges that do not exist in everyday home or office IT environments – such as patching difficulties – these special characteristics also permit unique cyber security solutions that would not be possible in the latter. **Promoting the adoption of 'whitelisting'**, for example, could therefore be an important way to bolster cyber security at nuclear facilities. As an information exchange protocol that only permits actions or traffic if they are on an authorized list known to be safe, whitelisting contrasts with traditional 'blacklisting' methods of cyber defence, a model under which all actions or traffic are permitted unless they are on a blocked list.

Whitelisting can be done both at the device level and at the network level. At a device level, the methodology involves authorizing the device to carry out only a narrow set of actions that are necessary for its role. The computer would only be allowed to run certain types of pre-approved executable files, rather than, as now, any executable files on a USB key. This would reduce the risk of infection carried across an air gap by insertion of a USB device (which was the likely pathway used by Stuxnet).

Whitelisting at a network level involves only authorizing traffic between specific points that are needed for its activities. For example, instead of allowing a computer to talk to all of the computers on the network, whitelisting would only allow it to talk to a small number of other previously identified computers with which it needs to communicate.

Industrial environments are particularly suited to whitelisting because they are predominantly static in functionality, making it possible to determine exactly what actions or traffic should be authorized. Most everyday home or office IT environments are in constant flux. At the device level, users regularly download new software on their computers – either new applications or software updates to existing applications. At the network level, computers are regularly added to or removed from parent networks. These computers also generate a lot of unfamiliar traffic, as they visit new websites and receive and send numerous emails to and from new people all over the world. This results in a high level of unpredictability.

By contrast, the industrial world is relatively fixed. At the device level, patching is rare (particularly in the nuclear environment), so device configurations change little. At the network level, industrial control systems primarily involve computers talking to computers; thus the communications and commands that different parts of such systems must exchange with other parts should follow relatively stable patterns. This predictability makes it possible to determine what actions and communications should be authorized in industrial environments.

> Within an industrial control system environment, especially a nuclear environment, actually being able to secure these environments is infinitely easier, not harder, than it would be for an IT environment. (Source 26)

Whitelisting can also provide a solution to the patching challenges experienced by nuclear facilities: by restricting the functionality of a device or network, it becomes less important to patch systems, and this in turn facilitates whitelisting.

> If you compare the effort of doing whitelisting with the effort of patching and vulnerability management, they are not even vaguely related in scope. (Source 9)

In order to implement whitelisting, if the programmable logic controllers are modern, purchased within the last 10 years or so, and as long as they are digital, only a firmware upgrade to them or a new ethernet card would be needed. The financial expense of an upgrade would be manageable. In fact, the largest share of the cost would be the additional testing and planning needed to make the upgrade safely.

If a system is older, perhaps 20–30 years old, then whitelisting may not be possible. In this case, other options that can add security include active management, the deployment of intrusion protection systems, and intrusion detection systems which monitor the electronic traffic within a nuclear facility for anomalous behaviour. Some of these are discussed further below.

Intrusion detection systems such as network monitoring, which involves examining the traffic within a nuclear facility for anomalous behaviour, would enable nuclear facilities to take a more proactive approach to cyber security. When the system detects unusual traffic that does not fit the established pattern, it alerts the owner-operator.

For many facilities (nuclear and otherwise), the first step in network monitoring is to map the expected traffic between devices in order to establish a standard baseline. Many nuclear facilities have yet to do this, and others may not have undertaken the mapping at a sufficiently detailed level.

> It is vital that operators identify the devices they have, identify how they communicate with each other, and put in place technical systems that will immediately alert the operators as soon as any of that ever changes. This is typically not done in industrial settings. It is done to a greater degree, but far from ubiquitously, in nuclear. (Source 9)

> Because people are not thinking about security, they are not doing the data flows at the level that is needed for security. The way data flows are currently documented is, for example, that this computer sends data every 10 minutes over to that computer. But what we need to know is the communication between IP addresses or ports and the data format. For example, if a computer is trying to access an IP address outside my company on port 80, that would be a red flag because it is indicative of a backdoor access Trojan sending data back to a command and control server. (Source 3)

The **use of virtualization** – the creation of a virtual version of a device, operating system or network – may be a useful process in helping understand the data flows and serve as an effective way to map out those connections. By virtualizing the entire network, it is possible to learn about the data flows without the degree of risk involved in actual experimentation.

> We can use virtual environments to learn about the data flows without having to experiment with our real network and worrying that we are going to mess it up. (Source 3)

Furthermore, **monitoring needs to be done on the entire industrial control system network, not just on the perimeter.** Since personnel at nuclear facilities (and, in fact, critical infrastructure more generally) too often concentrate only on perimeter defence, allowing malware to operate undetected if it is able to get past the perimeter, they need to recognize that they must monitor *all* networks.

> Most people focus all of their security on prevention and they do very little for detection and containment. Network monitoring tends to be on the perimeter and very little [on] any form of network monitoring within the control system. So people need to monitor all their networks, not only the perimeters. (Source 27)

In addition, encouraging **the adoption of secure optical data diodes** where not already implemented would significantly enhance cyber security. This is key given that there are some nuclear facilities that may have only a firewall to protect the industrial control system network.

With regard to supply chain challenges, the globalization of manufacturing means that resolving vulnerability remains difficult. However, some countries are taking important **steps towards the nationalization of their supply chains** (in the nuclear sector and beyond).

Japan has had the greatest success here in enabling indigenous companies to build the entire product range for its nuclear power plants. Although of course microchips from foreign sources may be used, Source 18 states that Japanese power plants are 'almost 100% national; they make the products that they need'.

The best option for countries that lack the required extensive national industry is to **reduce their supply chain vulnerability** to the maximum extent possible. Russia, for example, views the nationalization of its supply chain as a priority, including in the nuclear sector. Given the difficulty of manufacturing all of its products domestically, in the short term Russia is seeking to reduce its dependency on components manufactured in countries that it considers 'less friendly'; instead, it is substituting them with components from China, which it considers a 'more friendly' country at present. Russia views this as an intermediate step while it continues to build up its own national industry. In the long term, it hopes to be able to replace the majority of components with Russian products.

> Throughout all of last year, there was a big discussion in Russia about the need to urgently replace foreign components and hardware with Russian ones. This attitude extends to all spheres and sectors of the Russian economy. (Source 12)

Of course, for financial reasons it will be important for nuclear facilities to identify the most crucial parts of the plant from a cyber security perspective (notably, their critical cyber assets) in order to grant those the highest levels of protection. As Source 3 states, 'It needs to be a graded approach; we can't afford to do everything for every system.' **Prioritization of the cyber risks is therefore key.**

8. Developing an Organizational Response

Summary

This chapter sets out a series of proposals for the development of a response regime in the civil nuclear industry. This regime would be aimed at mitigating cyber security problems identified above, and at addressing others. It would be based on an organizational methodology that is scalable and flexible, and able to act with confidence and authority, but that would be driven by the overriding need to keep providing nuclear-sourced energy rather than by the sometimes commercially restrictive requirements of the security profession.

The need for organization

In cyber security, organization is a prerequisite for everything. Technological responses on their own have failed. So have data-centric responses. Without organization, communication and cooperative actions involving stakeholders and individuals will always be inefficient and ineffective. Without organization, a strategic cyber response does not work.

Acting coherently, stakeholders involved in a future civil nuclear cyber security regime should have as their goals to turn the components of cyberspace that are key to achieving strategic sectoral aims into a self-governing eco-system, instead of, as now, an ungoverned environment made up of disparate components, each engaged in tactical battles with a variety of threats. The comprehension involved must also reach beyond simply cyber security into physical security, personnel security and safety. In addition, meaningful and persistent dialogue between IT and OT stakeholders must be incorporated as a fundamental necessity.

Cyber security is a multi-dimensional concept that cannot readily be accommodated within traditional security policy-making. In the nuclear sector, both safety and physical security measures have developed incrementally and in tandem over time, but the rapidity in the development of cyber dependency creates dissonance within a security regime. Three essential components (physical, virtual and personnel) are evolving at different rates, in terms of both threat manifestation and countervailing capability development. This leads to a twisting complexity in the management of overall security (with additional complications of insider threats posing problems across all areas of risk).

This environment must continue at all times to establish the appropriate balance between regulated and self-determined actions to avoid any tendency towards overall stagnation, which is a condition attractive to organized groups and individuals aiming to challenge the welfare of the nuclear energy supply chain.

Communication

The various illicit uses of cyberspace amount to a system-level challenge to the civil nuclear sector. As it is currently configured, however, the sector does not act and respond as a coherent eco-system where cyber security is concerned. This is despite fifty years' experience of developing a safety-related (and more recently a security-related) culture. Stakeholders in the nuclear cyber domain remain largely segregated, despite having a satisfactory set of enabling computer security policy documents that act as a potential operational glue. As a result, agencies within the sector may well fail to see that they are affected by another stakeholder's cyber security, or, more often, by the lack of it. This is a matter of communication, both horizontally between nuclear energy producers, but also vertically throughout the entire supply chain.

Improved coordination

At a simple level, the priorities for a cyber security regime are nothing but traditional: deterrence, prevention, detection and response. But it is how these activities are coordinated that will set the tone of the nuclear sector's cyber security culture, closely allied by absolute necessity to the safety culture already at the core of the industry.

Hitherto challenges in the cyber domain, no matter in which industrial sector, have been managed generally by a patchwork of technological responses. The nuclear sector is no different from any other. However, there is ample evidence to suggest that the main challenge, affecting the entire sector, requires an equally far-reaching response mechanism to achieve higher overall levels of security, thus providing confidence in the use and maintenance of electronic control and information systems. Without appropriate controls in behaviour, the potential for technology to deliver future efficiencies in the nuclear energy life-cycle will become limited; the threat picture begins to build, but awareness on its own does not act as a catalyst for the technological design of operational and defensive systems, which fail to keep pace with the real world.

In order to attempt to correct this imbalance, cyber security policy within the sector needs to be extended to fuse two approaches: the largely reactive and bottom-up concerns with computer and network security, along with information security and assurance; and the top-down approach driven by the needs of sector-level responsibility to deliver nuclear-sourced energy safely and at commercial prices. If this organizational transformation is achievable, it should be possible to shape future cyber security policy to align with strategic perspectives – primarily the needs of the nuclear business, but also progressive strategies on governance and regulation, cost-effectiveness and, particularly, inclusiveness.

The term cyber security and other related expressions are widely used as though their meaning were clear and incontrovertible, but the primary research for this report confirms that there is no consistency in approach to cyber issues across the international stage, and the nuclear sector is no exception. The lack of an international cyber lexicon continues to hinder multilateral responses in all sectors, particularly when applied across linguistic barriers. Even within individual states, the interpretation of 'cyber' can mask a range of inconsistencies and unanswered questions, posing a serious difficulty for policy-makers and those tasked with ensuring security. In several languages, for example, there is only a single word for both safety and security.

Even within individual states, the interpretation of 'cyber' can mask a range of inconsistencies and unanswered questions, posing a serious difficulty for policy-makers and those tasked with ensuring security.

One way to achieve alignment across and within all stakeholder groups might be to put one set of stakeholders (such as the technical cadre) at the centre of the problem and then organize the response around it. However, the foundations of a more integrated and robust regime in any sector require a common idea of cyber security – as regards both the problem and responses to it. At the top of the IAEA policy tree there is some very sound advice already being developed, but at the centre of the downstream problem is the lack of a common baseline in building a potential cyber response. This makes development of a unified approach to cyber issues all the more challenging. Creating a common lexicon for cyber security, and hence a common threat picture, as well as acknowledging differences in national cultures in terms of risk management, security vetting and operational responses, are all issues for further and immediate consideration.

Regulation

The threat that the nuclear sector faces in cyberspace is fast-changing, sophisticated and potent, suggesting that a response mechanism needs to be equally powerful and agile. However, meeting an unresponsive and arguably obsolete regulatory requirement being enacted in a highly regulated environment (which is the cultural norm in the nuclear industry) would only be counter-productive. Such an approach would quickly strangle the vitality of a potential response based on the mature culture that the nuclear sector enjoys in the matter of safety. Instead, there needs to be a well-judged and informed balance in policy, regulation and communication. A potential solution would be to support regulatory authorities with accredited specialist cyber security expertise that can act with appropriate agility and speed.

A strategy that shifts the risk of cyber-related harm to proactive rather than reactive measures would serve to deter cyber adversaries by increasing the degree of difficulty they will encounter if attacking the sector. This approach would deflect threats to easier targets, while also ensuring that any determined adversaries would have to invest more to achieve their aims. A nuclear-cyber security regime needs to be put in place to make the sector hostile to saboteurs, while maintaining the delicate balance between prescriptive regulation and the empowerment of knowledgeable people to take appropriate mitigating action where necessary.

This approach would need to be high on vision, doctrine and knowledge, and moderate on control. The development of cyberspace with its embedded insecurities will always outpace any internationalized hierarchical structure designed for policy development rather than operational response. Such a regime would allow the fullest of freedoms to those who have a role to play in countering risks to the security of the sector, while also contributing to a broader approach to cyber security through a policy of inclusiveness. It will rely to a much greater extent on creating a shared awareness of cyberspace, its threats and operating methods, as well as the spectrum of available security capabilities, including collective protection, to mitigate risk.

Technological responses

Such a security regime would have to incorporate a technical response to address the issues described earlier (such as patching or air gapping). This would fit into an organizational approach to risk reduction, which can be bought into action rapidly and uniformly to raise the level of security to address critical vulnerabilities across the sector. Thus an appropriate overall response would comprise an eco-system in which the activities of different responding agencies and bodies complement one another and are mutually reinforcing, rather than conflicting; this would include a very close cooperation with the safety cadre and the physical security teams on sites. An approach to cyber security that draws in a wide range of people from across the sector and also further afield (national regulatory bodies, for example), scarcely lends itself to centralized control. Cyber security operations at nuclear facilities therefore need to be self-informed, self-governing and spontaneous, but to act within an agreed framework that is coordinated more centrally, most probably by the IAEA.

There is limited evidence of cyber attacks on the civil nuclear sector, most likely owing to lack of disclosure (as is common in other reputation-sensitive sectors such as finance, but also perhaps from a lack of discovery. Current responses to the exploitation of cyberspace by adversaries characteristically lack both agility and organization, making it difficult to improve security systematically and efficiently. Organized threats require organized responses by the whole sector, which necessarily includes leadership at the highest level (supported by up-to-date advisory bodies) with energetic and knowledgeable inputs from the various internal and external stakeholders. Technological capability involved in protection, detection and response capability needs proportionate investment, gearing to risk registers and recognition of the guidance and recommendations for cyber security that the IAEA is developing on behalf of its member states.

Governance

The governance of cyber security in the sector has to be able to promote debate around two key factors. First, responses need to be managed in a way that creates a norm that supports the use of information and communications technology (ICT) to ensure safe and efficient nuclear energy production, while increasing the difficulties for threat actors.

Second, cyber security management must have a collective dimension, involving all the key stakeholders and organizations. Clearly, where vulnerabilities remain in infrastructure protection or information assurance, these are likely to be discovered (whether by accident or design) and exploited by the ill-disposed. A collective approach would enable cyber security to become a self-taught, dynamic process based on common operating principles to counter evolving threats, and benefiting from a doctrinal loop based on the 'Boyd cycle' of continual process improvement (observe, orientate, decide, act). If each stakeholder were to be given the opportunity to learn from the experience of others, the overall level of cyber security across a chosen sector should increase (and has been demonstrated to do so in the UK financial services through concepts such as the virtual task force (Home Office, 2010)).

Effective and durable responses in cyberspace therefore require a shared awareness, an appetite for collaboration and the development of an instinct for risk, which might alternatively be described as a culture of cyber security. But achievement of this relies once again on developing a truly knowledgeable leadership at the very top of the eco-system, and then within its subsections too.

Risk management

To achieve absolute security in cyberspace would require all threats, their toolsets and their attack paths to be identified and isolated, and certain interactions to be interdicted before they became critically dangerous.

However, taking into account the complexity of the internet, the rapidity with which malware is developed and the unpredictability of the human component of the environment, such perfect security is a fantasy – and perhaps not even a desirable one at that, given the constraints that would place on the industrial processes involved.

Thus the requirement for a civil nuclear cyber security regime must be to manage and mitigate rather than eliminate threats from cyberspace and to assess these threats relative to vulnerabilities, the likelihood of an attack and the potential impacts if an attack is successful. Cyber security therefore becomes a matter of risk management, within an environment in which the key element of the responsive entity is the development of pace and agility.

Inclusiveness

A technological approach alone will not be sufficient to resolve the complexity of the security space. An approach to cyber security which is entirely or largely technological will lack depth and deny the defender the ability to develop an interlinked series of layers of security, each representing another hurdle for an attacker to overcome. Understanding the intersection between the technical, human, organizational and regulatory aspects goes to the heart of solving, or even merely mitigating, the problem of cyber security in any sector, let alone the politically sensitive theatre of nuclear energy production

Given the technological sophistication of the cyber medium, the pace of change and the way in which user demand on the internet catalyses high degrees of innovation, security within ICT infrastructures could be seen as just too great a security problem for analysts, industrialists and policy-makers. This condition exists nationally, internationally and within industrial sectors themselves, with complex sets of regulatory authorities trying to make their respective marks on the structure of cyber security within their own ambits. But this does not necessarily have to be the case in the nuclear sector, where there are fewer stakeholders, they are generally acquainted with one another, and the culture of 'collectivism' is more clearly accepted (principally through the traditional lens of 'safety'). This fundamental principle in the delivery of nuclear safety has the potential to extend to a complementary development of cyber security in the sector, given the appropriate push by regulators and the development of a workable model of the response required.

Configuring the future response

Within this difficult concept of cyber security, some capabilities can be identified as simply common sense, aligned to general principles in risk management systems where most resources are expended on the most critical vulnerabilities. However, the philosophy of taking proactive action to mitigate risks when they are identified rather than focusing on responses when they occur – often called 'left-shifting' risk management (Jonas 2011) – also points usefully to the less resource-intensive (and less expensive) preventive activities of education, training and exercising.

The key features of the response will be agility and initiative; and taking both an actor-neutral and a risk-based approach.

Agility and initiative. As described earlier, the range of cyber threats is so broad and the spectrum of threat actors so diverse that a 'line in the sand' cyber defence philosophy will mean two things. First, the agile and intelligent (and well-resourced) cyber adversary, who is unencumbered by long-winded business processes, will enjoy a good deal of initiative in the contest, and will not have to compete particularly vigorously to gain or maintain the initiative. Second (as is borne out by our interviews for this project), the response to cyber threats will tend to be reactive rather than anticipatory, with reaction only occurring when an attack hits the firewall or is detected inside it (if it is detected at all). In other words, the point at which response mechanisms of the sector begin to address cyber threats is when those threats are fully developed and at their most powerful. Before such an event occurs, attacks may even have been rehearsed on other sectors, nationally or internationally, particularly those containing a preponderance of industrial control systems. The nuclear sector's cyber security response should therefore seek to be as agile as possible and should focus on unbalancing an opponent by winning and maintaining the initiative, and where possible activity should be intelligence-led. The intelligence component, which includes horizon scanning, research and development (R&D), and information from other actors in the sector, thus helps to determine the triggers which invoke the response mechanisms.

An actor-neutral approach. An 'actor-neutral' approach in which capability is developed irrespective of particular (and known) threat actors would be preferable, given that these are so diverse and can change quite quickly. What is important is the knowledge of what an adversary (any adversary) could do, and to have the policies, procedures and equipment necessary to meet (or anticipate) that challenge, whatever its origin and whenever it occurs.

A risk-based approach. It would not be reasonable to expect to eliminate all cyber threats permanently, nor would it be possible to filter out all criminal or hostile use (actual or potential) of the global ICT infrastructure. However, a risk-based approach to cyber-security will:

- Indicate that legitimate use of ICT should not be assumed to be free of plausible adverse consequences;
- Enable cyber security to be assessed on the basis of proportionality: perceived benefits can be set against possible penalties, and benefits can therefore be prioritized;
- Encourage agility and adaptability: as cyber security challenges evolve, priorities can be recalibrated;
- Allow cyber security policy to be framed at an overall or system level, with risks and dangers in one sector being offset by benefits and advantages in another.

A cyber security regime

In transforming cyber security management in the direction proposed in this report, it becomes reasonable and useful to describe these efforts as aspects of a sector-level cyber security 'regime'. Such a regime will define a methodology to organize efforts through the national and international development of enabling policy, while acknowledging that successful cyber operations will need to remain delegated to power plants via their commercial parents.

A successful and durable regime is one that functions intelligently and responsively within its area of concern, remaining absolutely current with the threat picture, concomitant risks and the arsenal of available countermeasures.

Any management system that remains centrally driven or over-prescriptive would risk reducing pace and agility in the response, leading to ever-widening capability gaps between threats and responses and thus higher risks. A successful and durable regime is one that functions intelligently and responsively within its area of concern, remaining absolutely current with the threat picture, concomitant risks and the arsenal of available countermeasures. The regime method offers the most suitable basis for a sectoral cyber security strategy because it can include and empower (not direct, as to do so would cause resistance and impose delays) a wide variety of actors, agencies and stakeholders. It can also be sufficiently agile (yet without losing focus) to meet a rapidly evolving and transforming security challenge.

An active strategy for cyber security can thus be developed in a series of steps:

- by establishing an agile organization;
- by articulating a sectoral policy;
- by careful planning and deconfliction; and
- through developing responsiveness.

On the basis of the analysis above, an effective sectoral cyber security management regime would:

- Promote a sectoral-level approach, from the highest levels down to the individual;
- Support a progressive environment which is designed to sustain tempo, and set out to establish the appropriate balance between regulation and the need to foster a culture of organizational and personal responsibility;
- Draw inputs from all available sources of cyber expertise;
- Incorporate a formal and properly funded environment for the promotion and fostering of cyber security within the sector;
- Enable the free flow of information between all stakeholders, creating a knowledgeable group in which the key tenets of leadership, responsibility and accountability can be clearly identified;
- Incorporate the necessary mechanisms to enable in-depth preparation for cyber security challenges, however these may arise, and an agile and coordinated response, including horizon scanning and R&D to extend the boundaries of the regime to the maximum extent possible;
- Define unambiguous communications channels to national and international specialist agencies.

While society at large is becoming more engaged in the cyber security problem, progress in the nuclear sector has been more laboured. Although the IAEA has developed some sound guidance on computer security, hitherto the culture of the sector has remained focused on the issue of safety. This has left the implementation of cyber security largely passive, defensive and uncoordinated; both ‘agility’ and ‘organization’ seem in short supply. This has led to considerable inconsistencies in technical implementation.

The organized way in which threats are manifested through the internet requires an organizational response by the civil nuclear sector, which includes, by necessity, knowledgeable leadership at the highest levels, combined with dynamic contributions by management and staff and the entire stakeholder group, including members of the wider security and safety communities. Energetic and knowledgeable inputs from internal communities and individuals and also external agencies such as government bodies will be welcomed by the cyber security regime. Each of these stakeholders has a role to play in a system which must generate ‘tempo’, be agile, and create an environment in which innovation is allowed to flourish and inefficient processes are challenged.

9. Conclusions

This report has examined the range of cyber security challenges at nuclear facilities and proposed a number of specific solutions to the challenges identified, as well as various actionable recommendations for the nuclear industry on a more general level. (For convenience these are listed at the end of the Executive Summary.)

Perhaps the greatest cyber security issue facing the nuclear industry is that many in the sector do not fully understand the risk, and therefore a key first step is to develop guidelines to assess and measure this risk as accurately as possible. This will help CEOs and company boards to understand what is at stake, and also provide them with a clear economic rationale to invest in cyber security. The development of cyber insurance, with its strong reliance on risk metrics, may be an important tool for promoting the development of cyber risk guidelines. In tackling the challenges related to the 'human factor', it will also be important to raise awareness among both engineers and contractors of the risks involved in setting up unauthorized connections or plugging in personal USBs at nuclear facilities. Measures that promote disclosure and information-sharing can also play an important role in enhancing cyber security, as can regulatory standards and other policy measures, improved communication to bridge cultural divides and the implementation of technical solutions.

The nuclear industry as a whole needs to develop a more robust ambition to take the initiative in cyberspace and to fund the promotion and fostering of a culture of cyber security, determining investment priorities and ensuring that sufficient and sustained funding is allocated to effective responses to the challenge. It also needs to establish an international cyber security risk management strategy and encourage the free flow of information between all stakeholders. This will require the industry to develop appropriate mechanisms and coordinated plans of action to address the technical shortfalls identified, as well as to find the right balance between regulation and personal responsibility.

The report has also highlighted some important areas for future research. Given that developing countries have been found to be particularly vulnerable, their specific needs should be assessed so that resources can be allocated more efficiently to combating the particular risks identified. The apparent lack of preparedness for a large-scale cyber security emergency, particularly one that occurs outside normal working hours, also suggests that scenario-based planning studies and exercises would lead to a better understanding of how a situation might unfold in a crisis – and to the development of effective response plans across the industry.

A number of the findings in this report may have a wider relevance, beyond the nuclear sector, since many of the challenges described here are common to critical infrastructure more generally. Examples of solutions that could apply across all sectors are initiatives to bridge communication gaps, the adoption of whitelisting techniques and the creation of industrial CERTs.

The main purpose of this research initiative has been to contribute practical and valuable ideas for decision-makers in the spirit of increasing safety and security in the nuclear industry. We hope that the findings and conclusions will stimulate lively discussion in the nuclear sector about the risks of – and responses to – a wide range of potential cyber attacks, thus benefiting the industry as a whole and the societies that it serves.