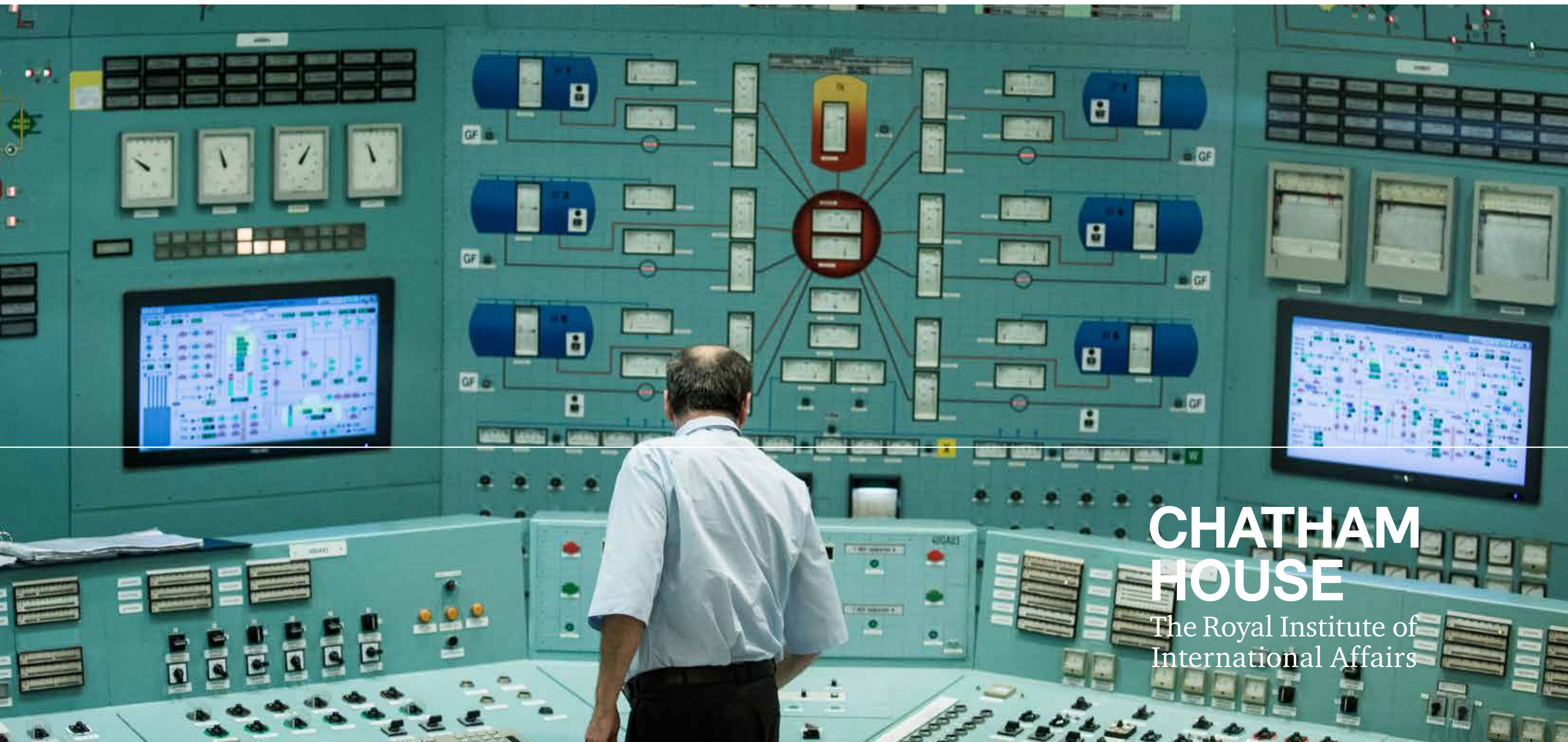
Research Paper

Éireann Leverett
International Security Department | May 2019

Cyber Insurance for Civil Nuclear Facilities
Risks and Opportunities



CHATHAM HOUSE
The Royal Institute of International Affairs

Summary

- Civil nuclear facilities and organizations hold sensitive information on security clearances, national security, health and safety, nuclear regulatory issues and international inspection obligations. The sensitivity and variety of such data mean that products tailored for insuring the civil nuclear industry have evolved independently and are likely to continue to do so.

- ‘Air-gaps’ – measures designed to isolate computer systems from the internet – need to be continually maintained for industrial systems. Yet years of evidence indicate that proper maintenance of such protections is often lacking (mainly because very real economic drivers exist that push users towards keeping infrastructure connected). Indeed, even when air-gaps are maintained, security breaches can still occur.

- Even if a particular organization has staff that are highly trained, ready and capable of handling a technological accident, hacking attack or incidence of insider sabotage, it still has to do business and/or communicate with other organizations that may not have the essentials of cybersecurity in place.

- Regardless of whether the choice is made to buy external insurance or put aside revenues in preparation for costly incidents, the approach to cyber risk calculation should be the same. Prevention is one part of the equation, but an organization will also need to consider the resources and contingency measures available to it should prevention strategies fail. Can it balance the likelihood of a hacker’s success against the maximum cost to the organization, and put aside enough capital and manpower to get it through a crisis?

- All civil nuclear facilities should consider the establishment of computer security incident response (CSIR) teams as a relevant concern, if such arrangements are not already in place. The existence of a CSIR team will be a prerequisite for any facility seeking to obtain civil nuclear cyber insurance.

- Preventing attacks such as those involving phishing and ransomware requires good cyber hygiene practices throughout the workforce. Reducing an organization’s ‘time to recovery’ takes training and dedication. Practising the necessary tasks in crisis simulations greatly reduces the likelihood of friction and the potential for error in a crisis.

Introduction

Obtaining cyber insurance is an option for organizations that are unable or unprepared to handle cyber risks by themselves. This could be perhaps because the expense of employing full-time staff dedicated to mitigating cyber risks is hard to justify, or because the risk cannot be quantified sufficiently well for the organization to be confident in assessing its response capabilities.

Several organizations in the civil nuclear sector currently 'self-insure' against technological accidents, insider threats to computer systems and information, and external hacking. Self-insuring involves setting aside internal funds and resources to cover risks, rather than contracting with an insurance company, and is a natural extension of the use of in-house information security and privacy teams. However, other options also exist for addressing cyber risks. This paper sets out a roadmap for how organizations in the civil nuclear sector can explore their options and review their cyber risk exposure.

Major categories of cyber risk

Information disclosure

Perhaps the most well-known of information management problems is an information disclosure event or 'breach'. This occurs so frequently that people have become quite numb to the issue. In the civil nuclear sector, the causes might include staff or contractors leaving storage media on trains and in taxis; disgruntled employees taking proprietary data with them when they resign (or are terminated); an organization being hacked electronically; and users being tricked through social engineering into giving away sensitive nuclear documents.

The first concern is to understand the different types of data that an organization holds, and how this can determine regulatory fines in the case of a breach. The broad categories of sensitive data can be defined as follows: personally identifiable information (PII), sensitive personal data (SPD), payment card and credit card information (PCI), protected health information (PHI), commercially confidential information (CCI), financially sensitive information (FSI) and value-sensitive information (VSI).[1] PII and SPD usually consist of personal details and other information about an individual, such as financial status or religious affiliation. Disclosure of such information can be damaging to an individual, for example because it enables financial fraud or violates privacy. PCI is usually a concern in respect of breaches that can involve fraud affecting a person or institution. PHI breaches can lead to disclosures of medical data: for example, information about a pregnancy or terminal illness can affect job prospects or loan approvals. Protection of CCI is typically a more organizational concern. This category could include information on proposed mergers and acquisitions, or – specifically in the civil nuclear sector – plans for a new reactor vessel that is soon to be commercialized. FSI and VSI often refer to trades or asset valuations. Breaches of each of the seven types of data outlined above carry different average costs to the victim, due to variations in the sensitivity of the data concerned and the size of regulatory fines in differing jurisdictions. While a lot is known about such fines in the US, and even in Europe, the numbers vary widely according to geography and jurisdiction.

[1] Coburn, A., Leverett, E. and Woo, G. (2019), *Solving Cyber Risk: Protecting your company and society*, Hoboken, NJ: Wiley, pp. 35–36; and Palmetto Security Group (2016), 'All The PXI's (PCI/PII/PHI): Putting the P Back In Protection of the Enterprise', 8 September 2016, https://www.palmettosecuritygroup.com/single-post/2016/09/08/All-The-PXIs-PCIPIIPHI-Putting-the-P-Back-In-Protection-of-the-Enterprise.

Civil nuclear facilities and organizations also hold sensitive information on other categories, namely security clearances, national security, health and safety, nuclear regulatory issues and international inspection obligations. The variety and sensitivity of these data mean that products tailored for insuring the civil nuclear industry have evolved independently and are likely to continue to do so.

There exists a great deal of available data about data breach risk, which is a well-studied phenomenon. This means that data breach risks to organizations can be estimated with increasing accuracy. A crucial but simple estimation approach in any organization is to examine the list of types of information (see Table 1) and estimate or categorize the number of records held in each category. These estimates need not be exact: indeed, the Cambridge Centre for Risk Studies has developed a simple logarithmic scale from P1 to P9 for studying past breaches.[2]

Table 1: How to estimate data breach risk to an organization

Severity	Number of records lost	Number of recorded US events (2012–18)	% of events
P1	0 to 100	Below reporting threshold	0
P2	100 to 1,000	Below reporting threshold	0
P3	1,000 to 10,000	2,022	58
P4	10,000 to 100,000	918	26
P5	100,000 to 1 million	324	9
P6	1 million to 10 million	162	5
P7	10 million to 100 million	50	1.4
P8	100 million to 1 billion	19	0.5
P9	More than 1 billion	2	0.1

Source: Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016), *Managing Cyber Insurance Accumulation Risk*, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf (accessed 28 Jan. 2019); and Coburn, Leverett and Woo (2019), *Solving Cyber Risk*.

To estimate costs in a given scenario, an organization should start by anticipating the likely worst-case outcome, as this provides the upper limit in terms of projected data loss. The next step is to make a list of the seven above-mentioned categories of information type in one column (PII, SPD, PCI, PHI, CCI, FSI, VSI), then leave space for a numeric estimate in another. For each category, a rough guess should be made as to how many records are held (corresponding to the same P1–P9 data-loss scale shown in Table 1). A relatively straightforward example might involve payroll data, for which each organization would obviously hold records for each employee. A reasonable starting assumption would be that the number of records is at minimum equal to the number of employees – with the caveat that many organizations potentially hold data on past as well as current employees. This exercise need not be time-consuming: the number of records can be estimated on the logarithmic scale, and easily refined later as and when more accurate numbers are discovered through interviews with different organizational units. Similarly, estimates can be made for other types of data, although some estimates may fall into the P1 category (0–100 records), for example if the organization does not hold that type of data (though organizations are often surprised to discover that they hold more data than expected).

[2] Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016), *Managing Cyber Insurance Accumulation Risk*, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf (accessed 28 Jan. 2019).

The next step is to imagine the maximum cost based on this information, which is why the number of records for different categories of information needs to be listed. For example, a PCI event can cost 1.5 times as much as a PII event, and 5.5 times as much as a PHI event.[3] Some up-to-date information on the average cost per record may be available for a specific category. Failing that, a good first estimate is IBM's 2017 cross-record average of $141 per record (in other words, an organization can arrive at a rough estimate of its exposure by multiplying the number of its employees by $141 if better, more localized data are unavailable). It may be necessary to add a shareholder loss estimate (i.e. reflecting reputational damage), ranging from 0 to 25 per cent of the share price in the case of a publicly listed company. This contingency should be kept separate from the costs of incident response for a period of a few days or weeks while the affected organization seeks to understand the source of the breach. A good base assumption for incident response costs is to allow $400 per hour for a period of one day to three weeks. The resulting estimate is likely to be a worst-case scenario, but this is a realistic way of understanding the size of loss the organization hopes to prevent. Over time, a more accurate picture may emerge of the probability distribution of a range of scenarios, allowing mitigation contingency measures and self-insurance to be funded at a higher level of confidence.

A good base assumption for incident response costs is to allow $400 per hour for a period of one day to three weeks. The resulting estimate is likely to be a worst-case scenario, but this is a realistic way of understanding the size of loss the organization hopes to prevent.

Another simple method of breach cost estimation is to rely on the parameters in the EU's General Data Protection Regulation (GDPR), which provides for fines of up to €20 million or 4 per cent of an organization's global turnover, whichever is higher. If an organization holds any data on Europeans, this figure also provides an easy answer to the question: 'How much it might cost us?' Of course, there may very well be someone in a particular organization who has much better data and can thus offer more accurate analysis than is possible via these two simple methods; in addition to enabling a more realistic projection of exposure, this would offer the opportunity to boost in-house expertise in cyber risk management.

Compromise of industrial systems

> Technological advances and the human factor mean it is no longer sufficient (or perhaps even possible or desirable) to isolate computer systems from the internet, a process known as air-gapping. The Stuxnet attack on Iranian 'air-gapped' nuclear centrifuges, for instance, illustrated the ability to infiltrate sensitive systems through a simple thumb drive and therefore the unreliability of air-gaps.[4]

'Air-gaps' – IT measures designed to isolate computer systems from the internet – need to be continually maintained for industrial systems. Yet years of evidence indicate that proper maintenance of such protections is often lacking (mainly because very real economic drivers exist that push users towards keeping infrastructure connected). Indeed, even when air-gaps are maintained, security breaches can still occur, as evidenced by an incident at the Davis-Besse nuclear generation facility in the US state of Ohio in 2003.

[3] See, for example, Ponemon Institute LLC (2018), *Cost of a Data Breach Study: Global Overview*, https://www.ibm.com/security/data-breach.
[4] Unal, B. and Lewis, P. (2018), *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences*, Research Paper, London: Royal Institute of International Affairs, p. 17, https://www.chathamhouse.org/publication/cybersecurity-nuclear-weapons-systems-threats-vulnerabilities-and-consequences.

The plant's network was breached by the Slammer worm,[5] which gained access via a consultant's data connection, exploiting the infrequency of security patches at the facility. Although the plant was offline for maintenance at the time of the incident, the worm disabled a safety parameter display system – a safety-critical feature even when the plant is not operating – for five hours. The security breach underlined the fact that systems such as that at Davis-Besse are vulnerable to randomly scanning worms, and that an air-gap offers limited protection (although its presence may delay infection by mitigating the core vulnerability that is the root cause of a worm attack). Engineers are known to use air-gaps to avoid patching, but the myth that this alone offers sufficient protection can lead to a dangerous tendency to deal with symptoms and not root causes. Such examples remind us that even air-gapped industrial systems still carry a residual risk of infection by virus, worm, Trojan or insider hacking attack, and that organizations are well advised to calculate such risk no matter how effective they believe their air-gaps to be.

The Davis-Besse incident was also a reminder of the potential safety-critical implications of malware for supervisory control and data acquisition (SCADA) systems, even when malware is not specifically designed to target such systems.[6]

> In the civil nuclear sector, reports of computer glitches date back at least as far as 1991, though the earliest recorded *malicious* attack on a nuclear plant occurred in Lithuania in 1992.

Over the years, a great number of cybersecurity incidents at industrial facilities have resulted in physical effects. One of the earliest on record occurred in Maroochy Shire in Queensland, Australia in 2000, when a hacker released a large sewage spill.[7] In the civil nuclear sector, reports of computer glitches date back at least as far as 1991,[8] though the earliest recorded *malicious* attack on a nuclear plant occurred in Lithuania in 1992.[9] Even worms and viruses intended for other targets can sometimes have impacts on civil nuclear facilities, as has been reported in the US.[10, 11] Japan has also experienced computer security problems with its civil nuclear facilities.[12] Glitches continue to cause problems with control systems to this day.[13, 14, 15]

[5] Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S. and Weaver, N. (2003), 'Inside the Slammer Worm', *IEEE Security and Privacy*, 1(4):33–39.

[6] The Davis-Besse example is adapted from Leverett, E. P. (2011), 'Quantitatively assessing and visualising industrial system attack surfaces', MPhil thesis, Cambridge: Darwin College.

[7] Repository of Industrial Security Incidents (undated), 'Maroochy Shire Sewage Spill', https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill (accessed 28 Jan. 2019).

[8] Repository of Industrial Security Incidents (undated), 'Computer Error at Sellafield Nuclear Plant in UK', https://www.risidata.com/Database/Detail/computer-error-at-sellafield-nuclear-plant-in-uk (accessed 28 Jan. 2019).

[9] Repository of Industrial Security Incidents (undated), 'Computer Sabotage at Nuclear Power Plant', https://www.risidata.com/Database/Detail/computer_sabotage_at_nuclear_power_plant (accessed 28 Jan. 2019).

[10] Repository of Industrial Security Incidents (undated), 'Slammer Impact on Ohio Nuclear Plant', https://www.risidata.com/Database/Detail/slammer-impact-on-ohio-nuclear-plant (accessed 28 Jan. 2019).

[11] Repository of Industrial Security Incidents (undated), 'Browns Ferry Nuclear Plant Scrammed (Shut Down)', https://www.risidata.com/Database/Detail/browns_ferry_nuclear_plant_scrammed_shut_down (accessed 28 Jan. 2019).

[12] Repository of Industrial Security Incidents (undated), 'Japanese Nuclear Company Virus Attack', https://www.risidata.com/Database/Detail/japanese_nuclear_company_virus_attack (accessed 28 Jan. 2019).

[13] Repository of Industrial Security Incidents (undated), 'Georgia Nuclear Power Plant Shutdown', https://www.risidata.com/Database/Detail/georgia_nuclear_power_plant_shutdown (accessed 28 Jan. 2019).

[14] Repository of Industrial Security Incidents (undated), 'Circuit card shuts down nuclear plant', https://www.risidata.com/Database/Detail/circuit_card_shuts_down_nuclear_plant (accessed 28 Jan. 2019).

[15] Repository of Industrial Security Incidents (undated), 'Computer Glitch Leads to Shutdown of Nuclear Reactor', https://www.risidata.com/Database/Detail/computer_glitch_leads_to_shutdown_of_nuclear_reactor (accessed 28 Jan. 2019).

Note that most of these events occurred before the emergence in 2010 of Stuxnet, one of the most famous examples of a malicious computer program that has caused physical damage.[16] There have also recently been two cyberattacks in Ukraine that have led to power outages,[17] as well as an incident at an unspecified location in the Middle East involving malware that specifically altered the safety systems of industrial facilities.[18]

In many jurisdictions, the regulatory regime does not provide for compensation to victims of radiation released as a result of a cybersecurity incident.[19] Plenty of data exist about cybersecurity incidents at civil nuclear facilities, but information of specific relevance for an insurance context (and codified in actuarial calculations) is not very easy to acquire. One reason for this information gap is that incidents resulting in radiological environmental impacts are much rarer than events involving data breach, distributed denial of service (DDoS) and ransomware.

Supplier digital business interruption

Even if an organization's staff are highly trained, ready and capable of handling any technological accident, hacking incident or case of insider sabotage, it still faces the challenge of having to communicate and/or do business with other organizations, some of which may have less stringent safeguards in place. To illustrate, let's consider a relatively simple ransomware event in which a computer system is deliberately infected with software that encrypts all the files with a malicious hacker's secret cryptographic key. In theory, this means that the files can only be unlocked by the hacker, who charges a ransom to do so.

Now, imagine such an infection occurring in a global shipping company. The inability of that company to unlock files containing shipping manifests, legal certificates, insurance documentation or payment processing systems could hold up its global shipping for weeks or months. Such an event might in turn delay, disrupt or cancel the shipment of materials necessary for the safe operation of a nuclear facility, even though that facility may, in isolation, be appropriately protected against cyberattacks. Despite such crises sounding like remote possibilities, cyber-related disruptions to supply chains have already happened. In 2018, container shipping giant Maersk was hit by a ransomware attack that cost the firm an estimated $300 million.[20] Yet what was even more interesting about the incident was the cost of the resultant disruption to Maersk's *downstream* customers, estimated at nearly $3 billion.[21]

Thus, while an organization's own security and privacy teams may be top-notch and without fault, it still might need to consider using insurance to cover the risks of disruption to its suppliers, whether these be for digital or physical assets. If an upstream supplier is hacked, this can cost the downstream organization time, money and effort, regardless of the state of the latter's security measures. Insurance products are now evolving that are designed to cover contingent business interruption from cyberattacks. For some organizations, such arrangements may be worth discussing either within their internal risk teams or with cyber insurance specialists.

[16] Zetter, K. (2015), *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Broadway Books, https://dl.acm.org/citation.cfm?id=2886120 (accessed 28 Jan. 2019).
[17] ICS-CERT (2018), 'Cyber-Attack Against Ukrainian Critical Infrastructure', 23 August 2018, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (accessed 28 Jan. 2019).
[18] Dragos Inc. (2017), 'TRISIS Malware: Analysis of Safety System Targeted Malware', https://dragos.com/wp-content/uploads/TRISIS-01.pdf (accessed 28 Jan. 2019).
[19] Stimson Center (2018), *Shaping Strong Security Norms: "Duty Of Care" for Security in Nuclear Facilities Through Organizational Governance*, https://www.stimson.org/sites/default/files/file-attachments/Shaping%20Strong%20Security%20Norms%20Report.pdf (accessed 28 Jan. 2019).
[20] Olenick, D. (2018), 'NotPetya attack totally destroyed Maersk's computer network: Chairman', *SC Magazine*, 26 January 2018, https://www.scmagazine.com/home/news/ransomware/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/ (accessed 28 Jan. 2019).
[21] The Insurer (2018), 'PCS: NotPetya insured losses now $3bn+', 4 September 2018, https://www.re-insurance.com/news/pcs-notpetya-insured-losses-now-3bn/1627.article.

Risk conclusions

> Solutions to these risks, therefore, should go beyond applying cybersecurity policies because, in this context, cyber risk reduction is actually about nuclear risk reduction.[22]

The insurance of civil nuclear facilities has a long and complicated history, but two events that stand out are the use of probabilistic risk assessment techniques in the 1975 *Reactor Safety Study* (widely known as the *Rasmussen Report*);[23] and the establishment of the Price–Anderson Act in 1957. The *Rasmussen Report* accomplished the herculean statistical task of estimating risk in the absence of an actuarial history of civil nuclear safety, which in turn gave the US Congress the confidence in reactor safety to provide $560 million in insurance above and beyond that available from the private market (which was only prepared to offer $60 million).[24] Counterintuitively, as systems achieve greater safety levels, the more difficult it can be to calculate the insurance risks associated with them, given the consequent rarity of incidents on which to base assessments. For example, for nuclear reactors built in the 1960s, statistically it would be necessary to wait 30–40 years for enough near misses and incidents to occur that could inform actuarial calculations.[25] As a relatively new field, cyber risk is at a very similar point in history today.

To insure or self-insure?

Self-insurance for most large corporates often involves the creation of a 'risk captive' – a subsidiary devoted to handling the risks of the parent company – without resorting to commercial insurance. Another option is to work with other organizations that share a similar profile of risk in mutual non-profit cooperative risk groups, via what are known as 'risk swaps' (wherein a company or organization trades risks with another that has similar exposures). In relation to cybersecurity, risk swaps can be useful because participants receive independent and mutual evaluations of their cyber risk posture.

Regardless of whether an organization chooses to buy external insurance or to self-insure (i.e. by putting aside revenues in preparation for costly incidents), the approach to cyber risk calculation should be the same. Prevention is one part of the equation, but each organization also needs to consider what resources will be needed should prevention strategies fail. Can the likelihood of a hacker's success be balanced against the maximum potential cost to the organization, and can enough capital and manpower be set aside to get the organization through a crisis? A useful first step is for an organization to ask its chief information security officer (CISO) what resources are set aside and available for incident mitigation as opposed to incident prevention.

Incident response

All civil nuclear facilities should consider establishing computer security incident response (CSIR) teams if such capabilities are not already in place. The existence of a CSIR team is a prerequisite for obtaining civil nuclear cyber insurance and also essential for organizations that choose to manage

[22] Unal and Lewis (2018), *Cybersecurity of Nuclear Weapons Systems*.
[23] U.S. Nuclear Regulatory Commission (1975), *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Powerplants, WASH-1400 (NUREG 75/014)*, http://webcache.googleusercontent.com/search?q=cache:qGBQNnFH7sQJ:journeesdetudes.org/atomescrochus/recherche/rapport-rasmussen.pdf+&cd=2&hl=en&ct=clnk&gl=uk&client=firefox-b-ab.
[24] Klüppelberg, C., Straub, D. and Welpe, I. (eds) (2014), *Risk – A Multidisciplinary Introduction*, New York: Springer.
[25] Starr, C. (1969), 'Social Benefit versus Technological Risk', *Science*, Vol. 165, No. 3899, pp. 1232–38.

their security programmes without external insurance. A competent CSIR team is capable of answering questions about the integrity of computer systems, investigating where and when systems were or might have been hacked, and how to respond to such attacks.

If an organization or facility does not have a CSIR team, it should aim to expand its knowledge of what such teams do, and of how their work is distinct from preventative measures such as installing anti-virus software, managing firewalls and setting password policies. Just as first-aid training and eyewash stations are provided to reduce the impact of physical safety incidents, CSIR teams focus on remediation, rather than on merely preventative measures, when a cybersecurity incident occurs. A good guide to incident response for policymakers can be found in the FIRST.org training section.[26]

Overview of cyber insurance coverage

Cyber insurance myths and facts

The most commonly cited reason for not buying cyber insurance is the idea that the policy will not pay out. Indeed, there have been high-profile legal cases in which the provider of cyber insurance has chosen to fight a claim in court. However, this is the exception rather than the rule, and insurers would soon cease to exist if they didn't pay out on claims. Independent reviews of cyber claims data show that most claims are paid and provide insight into what kinds of claims have been made going back to 2011.[27]

The mean total cost of a security breach between 2014 and 2016 was $394,000, with the median being $56,000.[28] Forty-seven per cent of claims came from companies with less than $50 million in revenue.[29] The cost of notifications was 176 per cent higher in 2016 than in the previous year.[30]

> Forty-seven per cent of claims came from companies with less than $50 million in revenue.

The second most common misperception about cyber insurance is that it is a waste of security spending. Yet cyber insurance premiums should come out of contingency budgets, not from prevention budgets. It is reasonable for management to ask how much money and manpower can be called on during a cybersecurity crisis, rather than comparing the cost of cyber insurance with that of a full-time prevention team. In short, money spent on firewalls does not contribute to the payment of regulatory fines, and budgeting should reflect a difference between prevention and response spending. Given the above numbers, an organization should be prepared to cover an average of $400,000 in the case of a data breach. If an organization is prepared to do this, then cyber insurance is perhaps unnecessary, though prudent contingency planning might also take into account the possible size of maximum payouts, which are significantly higher.

[26] Forum of Incident Response and Security Teams (FIRST) (2019), '2019 Incident Response for Policymakers', 22 January 2019, https://www.first.org/events/training/tallinn2019/.

[27] NetDiligence (2017), *2017 Cyber Claims Study*, https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition-1.3.pdf (accessed 25 Mar. 2019).

[28] Ibid., p. 5.

[29] Ibid., p. 2.

[30] Ibid., p. 3.

Types of coverage

The first thing to understand about insurance coverage is whether it is intended to address first-party or third-party exposures. First-party cyber insurance attempts to cover losses to the insured organization specifically, including those arising from extortion via DDoS or ransomware, business interruption from network downtime, notification fees (for example, due to regulatory requirements), theft of money or digital assets, and of course reputational damage.

Third-party cyber insurance is designed to cover costs to the insured party's customers; the costs of investigating their concerns; liability for the insured organization's own negligence or the negligence of those providing services to it; and loss of data or system access that prevents others from doing business, for example if the insured party fails to deliver fuel on time.

Note that a computer emergency response team (CERT) typically concerns itself with one of these types of risk over another, and cyber insurance may therefore be useful for the risks the CERT is *not* prioritizing. Outlined below are a number of different insurance types, many of which will offer both first-party and third-party variations. An organization should consider whether it has capital reserves to cover both the first-party and third-party risks listed.

It is possible to obtain standalone cyber coverage for both first-party and third-party risks. The costs will depend on the particular insured business, and on the desired coverage limit. Most common cyber insurance policies will be suitable for covering disruptions to business operations, but *not* for material damage arising from an industrial control system (ICS) or SCADA incident. Most standalone cyber policies are designed to cover data breaches, DDoS (a specific cyber risk) or credit card fraud. They are not designed to cover the costs of physical damage to engineering environments.

> Most common cyber insurance policies will be suitable for covering disruptions to business operations, but not for material damage arising from an ICS or SCADA incident.

Luckily, engineering lines of insurance, and even some civil nuclear pools, have started to offer cyber insurance tailored towards cyber risk in nuclear environments. Some key questions to ask of any provider offering such insurance are as follows:

- Does the insurance cover incident response and forensic investigation costs for ICS/SCADA environments?
- Does the insurer offer discounted rates or increased limits if the insured facility submits to an audit or security assessment?
- Can the digital forensics and incident response services be delivered at short notice?
- Do these service providers maintain the safety certifications and security clearances required for the civil nuclear regulatory jurisdiction in question?[31]

[31] Note that transport and logistics organizations (for nuclear materials) will have different concerns, as these often operate in more than one jurisdiction and may accordingly have special insurance needs.

Categories of coverage include the following:

Errors and omissions. This category of third-party coverage focuses on the insured party's liabilities in the event that it suffers a breach. It primarily focuses on payouts to other parties – such as regulatory bodies, personnel, customers or business partners – affected by a cyber event at the insured organization.

Commercial property all risks. This may cover physical damage to a facility from hacking, such as that demonstrated by Stuxnet. Many insurers are increasingly excluding cybersecurity coverage from this line of insurance. However, purchasers can still discuss having cybersecurity risks included, via a process known as 'write-back' that involves payment of an additional risk premium. Even if an organization's existing insurer offers a write-back clause, shopping around for explicit cybersecurity insurance may be advisable, in order to compare prices between one option and the other.

Personal lines insurance. This is less likely to be of interest for organizations, as it usually focuses on homeowners. However, this type of insurance increasingly comes with coverage for cyber risks such as ransomware. Small business insurance can also include similar protections.

Workers' compensation, safety and environmental lines of insurance. These are offered by a variety of insurers. Cyber issues are not always considered in these types of policy, but of course cyber exposures remain present and exacerbate the core named risks in ways that cannot always be anticipated. For example, it would not be uncommon for someone to think that environmental risk has no cyber component. However, on closer examination this assumption is mistaken. Much environmental modelling is done using sensors and networks, and data veracity is critical to monitoring and managing an organization's environmental footprint. Workers also routinely use computers to monitor their exposure time to radiation; denial of access to such data at a critical time can open an employer up to liability.

Cyberterrorism insurance. Cyberterrorism has become a concern in recent years, and both the UK and Australia have developed reinsurance products that cover material damage caused by cyber means. In particular, Pool Re, a UK firm, has created a flexible and adaptive approach that avoids attribution problems and investigation from getting in the way of prompt payouts. This, in turn, gives confidence to those responding to the problem, without burdening them with wider investigations into who was behind a cyberattack until a later time.

Specialist civil nuclear insurance. Specialist providers in this sector have shown an interest in providing cyber insurance to cover a variety of impacts. The civil nuclear pools are likely to be the most suitable places to look for coverage if an organization requires external cyber insurance. Even going through the questionnaire process for such coverage can provide valuable insight into the preparations an organization has made and/or issues it needs to attend to.

Cyber insurance for civil nuclear facilities

Key questions for civil nuclear facilities concern *whether* to buy cover, *how much* to buy, and *how much is available* in the market.

On average across the general (non-civil nuclear) cyber insurance market, a $120,000 premium buys coverage up to a limit of $10 million. Coverage for $50 million or more can be bought for $1 million in yearly premiums, but small and medium-sized companies can get $1 million in coverage for just a few thousand dollars.[32] The cost scale may, of course, change over time as risks are recalibrated from actuarial evidence. However, the estimates shown here capture the state of the market as of March 2019. Premiums and coverage specifically for civil nuclear risk may also diverge significantly from these estimates, but the above scale provides a baseline for research and back-of-the-envelope discussions.

One form of cover that is hard to find in standard policies is for **environmental damage**. It can only be found in 4 per cent of policies,[33] yet is a category that should interest civil nuclear facilities and organizations (in particular, within the civil nuclear transport sector). The ability to access liquidity and receive rapid assistance during a transport-related crisis might significantly reduce an incident's costs.

Policy wordings

The term 'all risks' in property damage insurance often used to include cyber coverage, but over time insurers have started removing it. This is because they have seen rising claims, and do not know how to manage the risk unless it is covered by a more specific cyber insurance product. However, for a small additional fee, cyber exclusions can be voided and cyber coverage returned to the same policy (as mentioned, this process is known as 'write-back'). A commercial property insurance policy that contains a CL380, LMA3030, NMA2912 or NMA2914 clause[34] specifically excludes any loss shown to be caused by accidental or malicious technological or computer-related means.

Table 2: Exclusion clauses, with focus and possibility of write-back

Exclusion clause	Focus	Write-back possible?
CL380	Computers/war	Yes
LMA3030	Computers/weapons	Yes
NMA2912	Data/virus	Yes
NMA2914	Data/virus	Yes

Before considering cyber insurance, an organization should review its traditional policies to see if any of the above clauses are present. If these exclusion clauses are not present, some cybersecurity risks may be covered already, and it is worth checking whether the insurer covers the specific cyber risk that the purchaser is concerned about. On the other hand, if any of the exclusions *are* present, it may still be possible to request a write-back or consider buying standalone cover.

Now that it is clear that traditional insurance sometimes covers common cybersecurity-relevant incidents such as computer theft or loss, breach, ransomware and GDPR notifications, it is also necessary to consider in greater detail cyber-specific insurance as well as specialized products for the civil nuclear sector. The latter are specifically designed to cover the impacts of hacking and technological accidents for civil nuclear facilities, whether in generation, research, transport or storage in operations.

[32] Coburn, Leverett and Woo (2019), *Solving Cyber Risk*, p. 237.

[33] Event held under the Chatham House Rule.

[34] These are standard insurance market cyber exclusion clauses. See, for example, Lloyd's Market Association (2018), *Cyber Risks and Exposures: Model Clauses – Class of Business Review*, https://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=c3910476-c5d4-47b1-bf3c-8b7e12e08299&iFileTypeCode=PDF&iFileName=Cyber%20Clauses%20Review.

Cyber insurance has many varieties in terms of its coverage, including GDPR and incident response assistance after a breach, DDoS mitigation, ransomware clean-up and assistance, financial fraud, CEO phishing, physical damage from hacking or technological accidents, and even cyberterrorism. Insurance tailored to civil nuclear facilities has only recently started coming on to the market. Such products offer tailored security audit and incident response features.

Strategies for buying cyber insurance

A prospective purchaser of cyber insurance should do the following:

1. Check if coverage is included under existing insurance policies, and also check the exclusion clauses in these policies;
2. Ask if a potential insurer can provide write-backs on exclusions, and check the price for such write-backs;
3. Ask how much standalone cover would cost, and what capacity would be offered; and
4. Review the two prices (write-backs vs standalone cover) to decide whether it makes more financial sense to fund the necessary capacity internally.

An introduction to calculating cyber risk

Ideally, the risk to the public from civil nuclear facilities should be below the risk of disease,[35] which is a bellwether of acceptable risk in society. The singular term 'risk' discussed here refers in reality to multiple civil nuclear risks – such as accidents, environmental hazards and hacking – all rolled into one. Nonetheless, a simplified concept provides a benchmark to aim at. Much is known about the 'safety' risks in civil nuclear plants,[36] due to probabilistic risk analysis and a well-recorded history of failures and near misses, but these are not the same as 'security' risks. Events such as employees losing laptops or breaching firewall rules (albeit with good intentions) fall into the latter category and can be modelled just as safety risks are. Increased dialogue between safety and security modelling teams should be encouraged, even when the two do not agree. Progress sometimes requires argumentation.

> Ideally, the risk to the public from civil nuclear facilities should be below the risk of disease, which is a bellwether of acceptable risk in society.

There is also the question of how to quantify the probability and severity of malicious hacking, where an intelligent adversary is trying to adapt to and avoid an organization's defences. Clearly, the adversary changes its approach as the defences change. Historically, game theory has been successfully applied to similar problems. This is less daunting than it sounds. The first step is to ask the safety team what is the most severe safety case that it has modelled. The cost of that event can form the basis of a stress test for a computer security incident, using the worst-case scenario to determine maximum severity.

[35] Starr (1969), 'Social Benefit versus Technological Risk'.

[36] 'Nuclear safety' refers to the protection of people and the environment against radiation risks; it also involves the safety of nuclear installations. In contrast, the term 'nuclear security' refers to 'the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities'. See International Atomic Energy Agency (2007), 'Introduction: Background Terminology in IAEA safety standards', https://www-ns.iaea.org/downloads/standards/glossary/glossary-introduction2007-07-06-21.pdf (accessed 25 Mar. 2019).

Taking the safety case as a starting point, a team can be brought in to discuss whether such a scenario could be caused maliciously through hacking. It is essential to bring penetration testers or CSIR teams into the discussion, as they will provide useful descriptions of the methods that might be used to achieve malicious ends. Otherwise, a supposedly 'expert' group is likely to remain under the impression that the scenario cannot happen, because its members cannot imagine how the hack would work.

Assuming that the scenario could indeed be brought about by hacking or technological failure, the challenge will be to understand the probability of such an event occurring. While most people attempt an actuarial approach, in the context of the civil nuclear industry it is well known that not all catastrophic events can be found in history, and that therefore the likelihood of occurrence must be analysed using other methods such as probabilistic risk assessment, counterfactual analysis, crisis simulation, stress testing and safety drills. It is worth considering a simple scenario, such as what happens when an operations room's communications (email/phone/fax) are compromised and used to subvert control of a facility.

Once there exists a scenario, created by experts and assigned levels of severity and probability respectively, it should be possible to start to look at the calculated risk, and at how much fiscal capacity will be needed to respond to the incident should it occur. This process can be repeated over time using a variety of hypothetical incidents. Such experiences will give staff confidence in calculating and responding to cyber risks. This is crucial as an organization builds capacity and starts to understand its exposure.

Should a civil nuclear facility, on the basis of the above scenario modelling, choose specific cyber insurance, then it will need to demonstrate that it is following various standards and has established a full-time and capable CERT. Guidance on how to do this can be found at the FIRST.org website.[37]

Transitional use of cyber insurance

One important general point about insurance is that coverage can be purchased for specific projects and specific points in time. For example, imagine that a civil nuclear facility managed by a given organization is scheduled to be decommissioned within three years. It is known that this facility carries a higher cyber risk than newer facilities because of its age, because the software in use there is older and harder to manage, and because there are fewer staff who can respond to a crisis. To train a new security team dedicated to this facility, only to let the team go three years later, would not be reasonable. Instead, extra training could be provided to the existing team and an insurance policy taken out to cover the three years to the transition. This in turn would help with the migration of staff and equipment to a new facility.

The specific sorts of transitional phase in which cyber insurance could be relevant include the following: during construction, before a facility goes live, while it is being wound down, or while one organization is being merged with another.

It is also possible to use cyber insurance, rather than technological solutions, during times of increased risk: for example, if new vulnerabilities have been discovered in the control system used by a nuclear facility and a patch is not expected because the product has reached end-of-life stage. Another example is that a facility might take out temporary cyber insurance if a known hacking group were targeting other similar facilities; such cover might allow the insured party to get through the crisis while security and privacy teams were trained to the higher standard demanded by the new threat.

[37] FIRST (2019), 'Trainings', https://first.org/education/trainings#Conducting-Exercises-to-improve-Incident-Response (accessed 28 Jan. 2019).

Capping the unmanageable risk

Cyber risk is constantly evolving, and some risks cannot be prevented, yet facilities still have a duty to manage civil nuclear risks. Risk cannot simply be 'air-gapped' away. Phone calls have to be taken, safety designs emailed and software used to model quality. Even if a facility is perfectly secure in theory, it must do business with organizations that may not be operating at the same level of security, privacy and safety. Not only does prudence dictate the creation of contingency plans for situations in which incidents compromising a facility's systems and security have an impact on its customers and business partners; it is also necessary to plan for situations when the reverse applies, and the facility is itself impacted by virtue of being a customer or business partner of an organization that is compromised.

> Risk cannot simply be 'air-gapped' away. Phone calls have to be taken, safety designs emailed and software used to model quality. Even if a facility is perfectly secure in theory, it must do business with organizations that may not be operating at the same level of security, privacy and safety.

For an illustration of this concept, imagine an email system that is in principle perfectly secure, and would not accept a spoofed email or divulge the contents of an email to an unauthorized party. However, that is only half the story. The emails which the system sends and receives must also be secure. If a hacker can read the counterparty's email (for example, by stealing his or her laptop), then the hacker can see any messages sent to that user (an eventuality that constitutes 'breach'). And if the hacker can send messages as the user – in effect impersonating that user – then the hacker can also potentially convince the recipient to perform various actions or tasks. So, a facility is only as secure as its partner organizations; everyone depends on each other to collaboratively manage cyber risk. Simply informing colleagues and external parties that a hacker has been detected and that any emails sent or received between two given dates may have been compromised is in itself enormously useful in managing cyber risk, even for a hypothetically perfectly secure facility.

The key point here is that not all cyber risks are manageable, especially on a unilateral basis. An organization's data are in the hands of business partners, whose security and privacy are their own concern. This is literally a risk that is outside one's control: a classic externality, and one that takes a lot of collaboration to address. Moreover, there will always be nation-state hackers that can exceed the level of defence that an organization has available. This leaves any organization with a residual risk that must be accepted and cannot always be prevented.

Response

Organizations can set aside capital for incident response and/or purchase protection in the form of cyber insurance. They need contingency plans for a variety of threats and risks, ranging from the loss of laptops to actions by disgruntled employees, ransomware and espionage by nation states. Many organizations can benefit from simple role-playing exercises among board members about how to handle incidents. It is possible either to create scenarios in-house (breach or ransomware incidents are good starting points) or to hire specialists to provide training.

Such processes often make it clearer to senior executives (who may or may not be accustomed to dealing with technical risks on a daily business) how responding to cybersecurity threats is not as simple as a password change. It involves communication and coordination across the organization, and often with many other organizations as well.

Scenario exercises provide an opportunity for organizations to review how much money, manpower and time are available for responding to a cyber incident. Alternatively, or in addition, an organization can perform 'risk transfer' by engaging specialist civil nuclear cyber risk and insurance professionals. The key goal of this process is to discover the limit of coverage offered, and on the basis of this information to produce a flexible plan for decision-making and resource allocation in the event of a crisis. Many cyber incidents last longer and require more work to resolve than expected, so it is worth asking how quickly the contingency budget can be refilled. Internally, an organization might refill the contingency budget faster than the insurance policy is able to make a second payout. Nonetheless, if it is not feasible to keep large amounts of capital in reserve or hire permanent, full-time security and privacy staff, turning to the growing cyber insurance market provides an alternative option.

Recommendations

Civil nuclear facilities should consider the following steps to review and strengthen their cyber risk response capabilities.

1. Quantify the risk

Each organization should examine how much it spends on cybersecurity. It should compare this amount to the sums spent by organizations of similar size in similar sectors, where such data are available, and should see how often breaches, ransomware attacks and DDoS events occur for them. This investigative exercise may offer scope to improve on the base risk calculations supplied by other entities (although in many cases the calculations are likely to be similar). Incident response reports, where available, should be examined to determine how much other organizations tend to spend in a crisis. It is worth comparing such documents to the fire, safety, HR and/or geopolitical risk budgets for one's own organization, thus starting a dialogue between risk and finance managers about cyberattacks.

2. Measure response capacity

Each organization should find out what proportions of its cybersecurity and cyber risk budgets are divided between prevention and mitigation/response. Money spent on firewalls does not help when notifications of breach need to be sent to all employees or customers. The process of budget 'discovery' should therefore be followed by the division of the cybersecurity budget into prevention and response components. The money set aside for response can be compared against the claims figures cited in reports such as the *Cyber Claims Study*, published by NetDiligence.[38]

[38] NetDiligence (2017), *2017 Cyber Claims Study.*

3. Use training to shorten recovery time

Even if enough money is set aside, a crucial activity in cyber response is training staff to reduce the 'time to recovery'. How quickly can employees reset email passwords? How quickly can hackers in a network be detected? How quickly can a crucial employee's computers be rebuilt from backup?

Preventing attacks such as those involving phishing and ransomware requires good cyber hygiene practices throughout the workforce. Reducing the time to recovery for an organization takes training and dedication. Practising tasks in simulation settings can greatly reduce subsequent friction and the potential for errors in a crisis, just as safety training does in other areas. Crisis simulations help identify communication channels and define the roles and responsibilities of different personnel and departments. The lessons from crisis simulations can boost organizational resilience. Board-level support is preferable for attempting such exercises – although, failing this, a training exercise involving crisis role-playing for senior managers can still be of benefit. Many boards think they are ready for crises, but rapidly discover they don't know what phone numbers to dial, or what communication path to activate to achieve the desired outcome. In this context, it is useful to find a supportive internal stakeholder and create a scenario around hackers compromising or disabling key parts of the organization. Such practice improves essential understanding of risks and capabilities.

> Crisis simulations help identify communication channels and define the roles and responsibilities of different personnel and departments.

There are many places to look for cybersecurity training, from the solutions approved by the UK's National Cyber Security Centre (NCSC)[39] to the SANS Institute, a professional security personnel certification organization.[40] The Forum of Incident Response and Security Teams (FIRST) offers training on running computer incident response teams.[41] It has an Industrial Control System Special Interest Group (ICS-SIG) and a Cyber Insurance Special Interest Group (CI-SIG). It also provides training in technical incident response and digital forensics. For more specific civil nuclear computer security advice, the U.S. Nuclear Regulatory Commission has useful documentation on how to apply computer security practices and principles to safety instrumentation systems.[42] This is especially relevant now that evidence has emerged of actual threat actors using malware to target safety system integrity, rather than malware's capabilities simply being demonstrated by the 'white-hat' research community (members of which use their knowledge and expertise in computer security systems for ethical coding and hacking).[43]

One organization dedicated to all types of civil nuclear security is the World Institute for Nuclear Security (WINS).[44] It offers online training on issues from physical site security to information risk management.[45] To build on these activities, programmes such as those offered by WINS for board-level personnel could be utilized to deliver bespoke training at a high level within the duty-holder community.

[39] IT Governance (2019), 'Certificated Cyber Security Training', https://www.itgovernance.co.uk/cybersecurity-training (accessed 28 Jan. 2019).
[40] SANS Institute (2019), SANS homepage, https://www.sans.org/ (accessed 28 Jan. 2019).
[41] FIRST (2019), 'FIRST Training', https://www.first.org/events/training/ (accessed 28 Jan. 2019).
[42] U.S. Nuclear Regulatory Commission (2011), 'Criteria for Use of Computers in Safety Systems of Nuclear Power Plants', https://www.nrc.gov/docs/ML1028/ML102870022.pdf (accessed 28 Jan. 2019).
[43] National Cyber Security Centre (NCSC) (2017), 'TRITON Malware Targeting Safety Controllers', 22 December 2017, https://www.ncsc.gov.uk/information/triton-malware-targeting-safety-controllers (accessed 28 Jan. 2019).
[44] For more information regarding WINS Academy training programmes, see https://wins.org/.
[45] World Institute for Nuclear Security (WINS) (2019), 'The leaders in knowledge exchange and certification for nuclear security management', https://wins.org/ (accessed 28 Jan. 2019).

Board-level engagement is crucial for budgeting decisions, but also because executives will be decision-makers during a crisis. A cybersecurity crisis is significantly different from other types of crisis; management and decision-making during a cybersecurity crisis can present unexpected challenges. Organizational training and board-level crisis simulations, as mentioned above, can aid understanding and budgeting both for prevention and for response.

The Safety Directors' Forum provides frank discussions and sharing of information and practices among senior-level civil nuclear executives.[46] In the UK, initiatives include a CISO working group that is co-chaired (on rotation) by the government, industry and the Office for Nuclear Regulation.[47]

It is known in certification circles that sometimes people undergo training, neglect to sit the requisite exams, then claim the training on their CVs. Accreditation organizations are exploring better ways of verifying that people have passed the exams. Pearson, for example, is exploring the use of digital badges. It is also important to verify organizations in the supply chain, as well as employees and consultants. One method of doing so is to examine chairs' reports on security performance, but increasingly a number of cyber risk telemetry and metrics companies offer simple cyber health check scoring systems. These companies may currently offer only shallow views of cyber risk (focused on online presence security, instead of control system security), but such offerings will improve in time and are useful leading indicators of poor practices.

In conclusion, training is an essential part of cyber risk management and response. It should be leveraged at the individual, organizational and board levels simultaneously. Crisis simulations can provide cost-effective ways of building a culture of security within an organization. They offer potential improvements in the management of, and response to, the future challenges of cyber risk for civil nuclear facilities.

[46] The Nuclear Institute (2019), 'About the Safety Directors' Forum', https://www.nuclearinst.com/Safety-Directors-Forum (accessed 28 Jan. 2019).
[47] http://www.onr.org.uk/.

About the author

Éireann Leverett is a senior risk researcher with the University of Cambridge Judge Business School's Centre for Risk Studies. His research covers a variety of cyber risks and technological disasters. He is the co-author, with Gordon Woo and Andrew Coburn, of *Solving Cyber Risk: Protecting your company and society* (Wiley, 2018); and CEO of Concinnity Risks, a cyber risk consulting company. Previously he was an ethical hacker of industrial control systems with the esteemed IOActive team. He is also chair of the Cyber Insurance Special Interest Group at FIRST.org.

Acknowledgments

Thanks to the International Security Department at Chatham House for assisting me in this study. Special thanks go to Dr Patricia Lewis, Dr Beyza Unal, David Livingstone, Erwin Kooi, Franky Thrasher and Frederic Gatte for their support and contributions.

Thanks also to the peer reviewers of the paper and all those who gave me comments and suggestions, the Chatham House editorial team and Calum Inverarity in the International Security Department at Chatham House.

Independent thinking since 1920

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Cover image: The control room inside the Paks nuclear power plant in Hungary, 10 April 2017.

Photo credit: Copyright © Bloomberg/Contributor

ISBN 978 1 78413 326 9

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223