Cybersecurity in Indian Nuclear Facilities
Neeraj B R

Abstract
Nuclear facilities have revolutionised renewable energy worldwide. However, the use of highly radioactive raw materials, capable of causing extensive damage if mismanaged, has made them a priority in national security along with other critical infrastructure facilities. Given this background, the importance of nuclear facilities for national security has strengthened with cases of cyberattacks on nuclear facilities worldwide. This paper analyses the ability of India's cybersecurity framework, both legislative and executive, to fend off cyberattacks on its nuclear facilities, drawing from experiences of cyberattacks worldwide and internationally recommended good standards and practices. Additionally, the paper also looks at how India could mitigate insider threats to its nuclear facilities and cultivate a cybersecurity culture within its nuclear facilities.

Keywords: Cybersecurity, Nuclear, India, Kudankulam, Nuclear Energy, Legislation, Prevention

Introduction
Nuclear energy has become an increasingly used source of renewable energy worldwide. Nuclear Power Plants (NPP), with their numerous interconnected systems, structures, parts, networks, and gadgets, work together to carry out a series of processes that tap into the uranium fuel fission in the reactor core to generate electricity. Multiple tightly connected yet individually operated process and safety systems keep the uranium fuel 'cooled' and the fission products contained in the core (Ayodeji, Mohamad, Li, Di Buono, Pierce & Ahmed, 2023). Digital systems have mostly superseded outdated analogue systems in NPPs due to the manufacturers' discontinuation of analogue goods during the past decade. However, software-based systems face cybersecurity issues that could jeopardise their ability to perform safety-related tasks (Park, Suh & Park, 2016).

This paper analyses the cybersecurity threats NPPs worldwide face and reviews cyber-attacks on nuclear facilities worldwide, international standards of cybersecurity and best practices followed to counter such attacks. The implications of a cyberattack on nuclear facilities and the

1 Neeraj BR is a postgraduate student at the Department of Humanities and Social Sciences at IIT Madras, India.
robustness of the cybersecurity measures adopted by India to protect its nuclear facilities are also reviewed. Additionally, the paper analyses ways of mitigating insider threats in Indian NPPs and cultivating a culture of cybersecurity among employees.

Cyberattacks on Nuclear Facilities

Raiyn (2014) elaborates on the various types of cyberattacks prevalent, including denial of service (DoS), remote-to-local (user) attacks, user-to-root (U2R) attacks and probing attacks, which could be traced to motives including stealing critical technology, cyber-activism, a disgruntled employee, or a nation-state or terrorist organisation-funded investigation. The attackers could exploit a system vulnerability by conducting harmful assaults, including imitating, man-in-the-middle (MITM) attacks, network spoofing, packet sniffing and modification, sensor masking, or malicious software like viruses, worms, and ransomware. False data injection (FDI) assaults, which could induce minor deviations in genuine signals and make them challenging to identify by traditional anomaly detection systems, are also possible in industrial control systems (ICS). Modern digital instrumentation and control (DI&C) systems face significant difficulty from exploitation by well-intentioned, well-resourced, and knowledgeable attackers. Moreover, the attack's intricacy reflects the intended impact of cyberattacks on nuclear ICS (Ayodeji et al., 2023).

The need to secure hardware and software used in NPPs obtained through the global supply chain has become necessary due to the shifting geopolitical landscape and national security concerns. Counterfeit goods, dubious products, and supply chain compromise have forced nations to be prepared for hardware compromise via supply links and accidental or intentional cyber exploits. Supply chain vulnerabilities emerge when data tampering, false data injection, product quality degradation, and counterfeiting are carried out in ways that make attribution difficult to install embedded malware that creates a backdoor for data exfiltration (Nissen, Gronager, Metzger & Rishikof, 2018), as illustrated by the following cases of cyberattacks on nuclear facilities.

Cases of Cyberattacks on Nuclear Facilities

Davis-Besse, USA (2003)

On January 25, 2003, users on Davis-Besse's corporate network began to experience poor service after the Slammer worm started affecting networks worldwide. The poor service was due to the congestion in the plant's corporate and control networks by the worm's traffic. It first
entered an unnamed Davis-Besse contractor's unsecured network. Then, it found its way through a T1 wire connecting that network and Davis-Besse's corporate network. Investigators eventually discovered that the T1 line was one of numerous entry points into Davis-Besse's corporate network that sidestepped the plant's firewall, which was set up to prevent the port Slammer utilised from spreading (Poulsen, 2003). A firewall was in place at Davis-Besse to guard its internal network from external internet traffic, and it would have prevented the slammer attack had a consultant not established a link to the consultancy's office network from behind the firewall (Kesler, 2011).

The worm rendered the Safety Parameter Display System (SPDS), which would indicate meltdown conditions by displaying sensitive information about the reactor core gathered from coolant systems, temperature sensors, and radiation detectors, inaccessible to plant staff for four hours and fifty minutes. Subsequent investigations state that plant computer engineers failed to apply the patch for the MS-SQL flaw that Slammer took advantage of. Surprisingly, these engineers were unaware of such a patch, which Microsoft released six months before the attack (Kesler, 2011).

**Natanz, Iran (2010)**

Stuxnet, a combined Israeli-American operation, is credited with causing around 1000 centrifuges at Natanz- a fifth of Iran's nuclear centrifuges, to spin out of control and explode in 2010. The worm replicated itself and attacked networks and computers running on Microsoft Windows, following which it looked for Siemens Step7 software, a Windows-based industrial control system used to operate centrifugal machinery. Then, it damaged the plant's Programmable Logic Controllers (PLCs) (Kushner, 2013). Stuxnet kept replaying the plant's protection system values throughout the attack, giving the impression that everything was normal while incrementally increasing the pressure on spinning centrifuges (Kelly, 2013).

Without the knowledge of the plant's human operators, Stuxnet's creators could spy on the industrial systems and even trigger the fast-spinning centrifuges to break apart. Stuxnet could covertly spread among Windows-powered machines, even those not connected to the Internet, and could get its way onto an infected machine if a worker inserted a USB thumb drive into it (Kushner, 2013).

On the condition of anonymity to discuss the classified operation code-named Olympic Games, U.S. officials stated that the operation was initially developed under the George W. Bush administration and was intended to gradually weaken Iran's nuclear capability while confusing
Iranian scientists regarding the cause of accidents at a nuclear plant. The officials state that the cyberattack was carried out on the secret orders of President Obama, who was eager to halt Iran's ostensible progress towards developing an atomic bomb without launching a conventional military attack. (Nakashima & Warrick, 2023).

Gundremmingen, Germany (2016)

The "W32.Ramnit" and "Conficker" viruses were found in a computer system of Gundremmingen's B Unit that had been upgraded in 2008 with data visualisation software connected to apparatus for transporting nuclear fuel rods. W32.Ramnit is intended to steal files from affected machines and targets Microsoft Windows software. It was first identified in 2010 and is disseminated using removable data storage devices. Conficker, which has infected millions of Windows computers worldwide since 2008, spreads through networks and duplicates itself onto removable data storage devices. W32.Ramnit and Conficker were discovered on 18 detachable storage drives, mostly USB sticks, on office computers with operating systems that were luckily kept separate from those of the plant, preventing attackers from gaining remote control over the plant's operations (Steiz & Auchard, 2016)

Kudankulam, India (2019)

The cyberattack of the Kudankulam Nuclear Power Plant (KNPP) came to light when a former National Technical Research Organisation (NTRO) analyst, Pukhraj Singh, tweeted about it on 27 October 2019 after having reported the attack to the Indian National Cyber Coordination Centre on 4 September 2019. KNPP officials refuted Singh's claims in an official statement on 29 October 2019, stating that such an attack could not occur. However, the KNPP's parent company, Nuclear Power Corporation of India Limited (NPCIL), acknowledged the security lapse in a separate statement within 24 hours. It stated that the Computer Emergency Response Team-India (CERT-In) informed them about the breach on 4 September 2019, and experts from the Department of Atomic Energy (DAE) looked into the situation. An inquiry pointed out that a user who joined the internet-connected network for administrative purposes was the owner of the infected PC, and he was an expert in research on thorium-based reactors (Mallick, 2019)

Russian Cybersecurity Company Kaspersky pointed out that the DTrack malware used to attack the KNPP was created by Lazarus, "an umbrella term that typically describes hacking activity that advances Pyongyang's interests." Further investigation suggested that the KNPP attack could be attributed to Lazarus' Group B and C. Group B deployed the Dtrack malware on the plant's IT systems, whereas Group C engaged in surveillance during the previous year and had
sent malware to senior nuclear experts. Group C turned over the information they gathered to Group B once they gained authority by conducting reconnaissance on individuals connected to KNPP (Mallick, 2019).

The North Korean hackers sent the email with the malware link to the official BARC-issued email address and personal email address of two prominent scientists (Mallick, 2019). The hackers, who already knew the KNPP's IP address, gained access to the KNPP's IT system when the scientists clicked the infected link while using the KNPP's domain, stealing technology-related data while not sending any destructive code. The Hi-Tech Crime Trends 2020/2021 report by the Singapore-based Group IB pointed out that the main file with the compromised data was dated 30 January 2019, which meant the hackers went unnoticed in the victim's network for almost eight months (John, 2020).

Regarding the KNPP cyberattack, the Union Minister for Atomic Energy stated that the Computer and Information Security Advisory Group – Department of Atomic Energy (CISAG-DAE) and CERT-In had investigated the breach (PIB, 2022). In a written response to a question in the Rajya Sabha on 8 December 2022, the Union Minister for Atomic Energy stated that the government had implemented security measures to safeguard India's NPPs against cyberattacks through authorisation, authentication, and access control techniques, stringent configuration management, and surveillance. Furthermore, the Minister replied that additional steps had been taken to improve information security in administrative networks at nuclear power plants, including improving internet and administrative intranet connectivity, limiting the use of portable devices, and restricting websites and IP addresses (PIB, 2022).

These case studies share common trajectories that are relevant when approaching the issue of cybersecurity in nuclear facilities. The cyberattacks in Natanz, Hanford and Kudankulam demonstrate how nuclear facilities, given their status as a critical infrastructure, could become targets of cyber warfare ascribed to or orchestrated by external actors. Moreover, the modus operandi of the attacks, in the case of David-Besse, Gundremmingen and Kudankulam, show the dangers of insider threat caused by mundane actions like using a personal pen drive or not updating the software could have on the security of nuclear facilities and by extension, on national security.

The lapses that could be attributed to the attack in each of the above cases are illustrated in Table 1:
Table 1: Cyberattacks on Nuclear Facilities Worldwide

<table>
<thead>
<tr>
<th>Year</th>
<th>Location</th>
<th>Event</th>
<th>Weakness discovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>David-Besse, USA</td>
<td>Five-hour loss of safety management due to traffic overload caused by slammer worm attack</td>
<td>Computer engineers failed to install the latest security patch for Microsoft Outlook 2000, available for six months.</td>
</tr>
<tr>
<td>2010</td>
<td>Natanz, Iran</td>
<td>Centrifugal damage due to speed variations caused by Stuxnet</td>
<td>Possibility of malware spread through using USB storage devices</td>
</tr>
<tr>
<td>2016</td>
<td>Gundremmingen, Germany</td>
<td>No damages were reported since the affected computer was isolated from the Internet</td>
<td>18 removable storage devices on another part of the plant operations were found to contain the malware</td>
</tr>
<tr>
<td>2019</td>
<td>Kudankulam, India</td>
<td>Stole technology-related data</td>
<td>Remote access to use the plant's domain provided to scientists</td>
</tr>
</tbody>
</table>

Source: Compiled by author from multiple sources

Implications of Cyberattacks on Nuclear Facilities

Cyberattacks at crucial industrial facilities like NPPs always lead to physical harm. A cyberattack could also induce misoperation in NPPs- for example, when attacking one of the plant's non-safety critical systems leads to an inadvertent operator's action affecting the availability of the safety-critical system. Depending on the plant's status, operators can manually override automatic control functions, and attackers can directly spoof or corrupt either the human-machine interface (HMI) or the sensor signal, misleading the operator into sending an incorrect control signal (Ayodeji et al., 2023). Cyberattacks on nuclear facilities worldwide, comprehensively covered by Kim (2013), show the potential damages a cyberattack could cause in an NPP.

Moreover, a cyberattack could pull a country's nuclear programme down, even though no human lives may be lost, following which recovery may be slow. Regarding the Stuxnet attack
on Iran's Natanz nuclear facility, Paul Roberts from Kaspersky Labs estimated that the attack could cost Iran's nuclear programme by at least five years. Charles Ferguson, President of the American Association of Atomic Scientists, stated that the Stuxnet attack was a setback for Iran's nuclear programme and added that Iran continued uranium enrichment but at a slower pace than before the attacks (Barzashka, 2013)

**Literature Review: Cybersecurity for Nuclear Facilities**

Poletykin, Promyslov, Jharkov and Semenkov (2022) put forth vital pointers when ensuring the security of an information system (which applies to nuclear facilities as well). They are referred to as the concept of Defence in Depth (DiD), which includes ensuring multiple protection measures in a progression that must be circumvented for cyberattacks to progress and affect the subsystem of the automated process control systems (APCS) for NPPs and its functions. Ayodeji et al. (2023) have also made similar suggestions to improve the protection of NPPs against cyberattacks by studying scenarios like false data injection attacks, supply chain risks, and attacks through cyberspace. Other scholars like Bhamare, Zolanvari, Erbad, Jain, Khan and Meshkin (2020) and Zhang and Coble (2020) have studied the security infrastructure in NPPs and made recommendations. Furthermore, Camp and Williams (2019) studied insider threats at nuclear facilities and recommended preventive measures.

**International Good Practices**

The spread of potentially harmful programs into PLCs can be stopped by ensuring that flash update schemes include an authentication mechanism, implementing appropriate access control to safeguard firmware images while being stored, forbidding remote updates, and disabling removable media like thumb drives. Moreover, creating a security policy, which offers a framework from which the staff of an NPP can identify the critical network components and develop a plan to secure network access and its operation, is a crucial countermeasure for defending the safety system against malicious cyber threats (Kim, 2013). Moreover, the existence of a backdoor account with permission to access and modify all library and source code files is a vulnerability for a nuclear system, which must be deleted immediately (Park et al., 2016)

Some measures that can be implemented include limiting physical access to the system, monitoring and documenting physical access, requiring staff identification, installing a hardware lock on the system cabinet, and announcing an open cabinet status (Park et al., 2016).
Code signing, the process of producing a cryptographic-based digital signature, is a crucial safeguard against infection in a computer system, and applying the software limitation policy is another method for preventing malware (Kim, 2013).

This is taken up in India's Central Electricity Authority (CEA) (Cyber Security in Power Sector) Guidelines, 2021, which advises all actors in the power sector, including NPPs, to ensure that their OT systems are hard isolated from any internet-facing IT systems. If necessary, they may only keep one internet-facing IT system at any site, provided it is kept in a separate room, isolated from all OT systems, and supervised by the Chief Information Security Officer (CISO). Moreover, communication between the OT systems must be carried out through a secure channel and all Information and Communication Technology (ICT) equipment must be sourced from 'trusted sources' as drawn by the Ministry of Power or the CEA (Central Electricity Authority, 2021). The Operational Safety Experience Feedback on Nuclear Power Plants Guide issued by the Atomic Energy Regulatory Board of India recommends organising an NPP's storage system to contain records of each component, system flaw, or human action involved in the reported occurrence for easy retrieval and evaluation of information (Atomic Energy Regulatory Board, 2006).

The CEA Guidelines recommend that only identifiable permitted devices should be used to download or upload any data from an NPP's internet-facing IT system, and both should be scanned for vulnerabilities and malware. Digital logs must be maintained for all such activities, kept in the CISO's care for at least six months, and prepared on demand for forensic analysis. Furthermore, the CISO must maintain a list of permitted IP addresses for each firewall, and each firewall is configured to allow communication with the permitted IP addresses only (Central Electricity Authority, 2021).

The 2021 CEA Guidelines mandate a cyber risk assessment and mitigation plan in the CSP for all power-generating facilities, including NPPs, and authorised by the board of directors. The NPP must specify the standards to declare a cyber security incident(s) as a cyber crisis in their system in their CSP. Moreover, a Cyber Crisis Management Plan must be created and submitted to its sectoral CERT for assessment with notification to the Ministry of Power or the CISO of the Ministry of Power (CEA Guidelines, 2021). The risk assessment and mitigation plan should clearly define how the cyber risk in IT and OT environments will be evaluated, along with the risk acceptance criteria (Atomic Energy Regulatory Board, 2006).
Furthermore, the Guide issued by the Atomic Energy Regulatory Board recommends conducting in-depth studies about the root cause of problems during breaches. A thorough investigation should include, among other procedures, forming a team of experts from other groups or organisations to evaluate the events, such as those involving equipment damage, unplanned shutdowns, excessive radiation exposure for plant workers or the public, unusual releases of radioactive material from the plant, and other high-profile incidents. These specialists must come from various specialities related to the research. The fundamental cause of the event, its chronology, safety significance, design flaws, operation and maintenance, correlation to prior events, and actions taken are a few of the things the Guide advises investigators to watch for. Safety system failures, or failures of any system that could harm the facility's operation and cause the release of hazardous, radioactive material, must be investigated. The Guide suggests suitable actions while examining and repairing human faults but does not entirely rule out the potential for human error (Atomic Energy Regulatory Board, 2006).

The information gathered in the Operational Safety Experience Feedback (OSEF) database and other software is effectively screened to guarantee that all safety-related issues, which should be prioritised for analysis, are selected. Lessons learned should be instantly communicated to other plants, and the necessary corrective steps should be taken swiftly to prevent the recurrence of similar occurrences that the exact underlying root causes may cause. Moreover, the Guide recommends constituting regular safety review committees so that no aspect of safety regarding NPPs is overlooked (Atomic Energy Regulatory Board, 2006).

**International Standards**

To combat the growing menace of cyberattacks, the International Atomic Energy Agency (IAEA) offers technical recommendations to tackle computer security issues and implement cyber security programmes necessary to safeguard NPPs. Additionally, the IAEA Nuclear Security Series (NSS) 17 comprehensively covers the establishment and enhancement of programmes to protect computer systems, networks, and other digital systems essential for the safe and secure operation of nuclear facilities and the prevention of theft, sabotage, and other malicious acts (IAEA, 2011). The international standard for cybersecurity in nuclear facilities set by the Institute for Electrical and Electronics Engineers (IEEE) in 2004 and 2010 also states that system security features should be addressed appropriately throughout the lifecycle phases and that potential security vulnerabilities should be addressed during the appropriate phase of the development process for digital safety systems (Park et al., 2016).
The IAEA Nuclear Security Guide 17 requires that the Cyber Security Plan (CSP) and the physical security plan of an NPP should work in tandem. The Nuclear Security Guide mandates communication and coordination between the teams in charge of the CSP and the physical security plan to maintain consistency throughout the development and review process of the NPP. The security plan must provide a thorough inventory of those assets vital to the NPP's security and safety. It also calls for a 5-fold classification of the safety systems in the NPP, with Level 1 requiring the highest level of security, whereby remote maintenance access should not be provided, physical access to the critical systems and the number of staff provided access are heavily regulated (IAEA, 2011). The successor Nuclear Security Guide 17-T builds on the standards set by Nuclear Security Guide 17 (IAEA, 2021). Furthermore, the CEA Guidelines mandate that the Cyber Security Audit follow ISO/IEC 27001, industry-specific standards ISO/IEC 27019 and ISO 16335, and any additional regulations issued by the relevant authority, if applicable (CEA Guidelines, 2021).

**Analysing current Cybersecurity mechanisms to protect Indian Nuclear Facilities**

**Cybersecurity Acts Information Technology Act, 2000**

Section 43 of the Information Technology (IT) Act, 2000 lists the offences pertaining to the damage to the computers, computer systems and networks, including accessing or securing access to the systems, extracting data, introducing malicious software into the system, causing disruption, or denying access to authorised personnel invites repairs to the maximum of one crore. Sections 65 and 66 of the Act enlist the two cybercrimes that are generally relevant but particularly relevant to nuclear facilities: Tampering with the Computer Source Documents and Hacking into the System. Another provision in the Act is Section 72, which calls for punishing offenders charged with gaining access to classified information and disclosing the same without authorisation to do so with a penalty amounting to no more than one lakh or imprisonment up to two years or both, except otherwise required under the Act or any other law at the time.

However, these provisions run into problems when applied to cyberattackers, because they rarely leave authentic traces, making it difficult to pinpoint a particular actor as the offender. The lack of clarity about who the offender could be, even if the actor is based in India, renders the entire redressal process moot.

Additionally, under Section 49 of the Act, a single-member Cyber Regulatory Appellate Tribunal comprising the Residing Officer appointed by the Government of India is established.
Furthermore, a Cyber Regulations Advisory Committee shall be established under Section 88 of the Act to advise the Central Government on information technology issues under this Act.

**Information Technology (Amendment) Act, 2008**

A vital change pertaining to the cybersecurity of critical infrastructure in India was brought about by changes under the new Section 66D, which orders a punishment of up to three years in prison or a fine of up to one lakh for impersonation while using a computer resource. However, far-reaching changes in India's cybersecurity governance are brought out under Section 66F, which defines what constitutes 'cyber terrorism' and the punishment for indulging in cyberterrorism. Under the Amendment, attacks aimed at harming the unity, integrity and sovereignty of India, unauthorised access to computer resources and introducing 'computer contaminants' into critical infrastructure as defined by Section 70 of the IT Act, 2000, and those actions in the cyberspace that could detrimentally affect India's foreign relations constitute cyber terrorism. Furthermore, Section 66F(2) states that life imprisonment is punishment for indulging in cyberterrorism.

Despite elaborately defining the criteria for cyber terrorism and the associated punishments, it suffers from the same shortcoming as its predecessor: how to enforce the punishments when the offender cannot be easily identified. Therefore, the Amendment Act falls short in the enforcement area.

**National Cyber Security Policy, 2013**

The National Cyber Security Policy recognises the types of cyberattacks India's critical infrastructure is vulnerable to and the consequences, should one occur. It is the umbrella guidelines that cater to all actors involved in cyberspace, including NPPs.

The Policy addresses the issue of cybersecurity by combining both organisational-level initiatives. At the organisational level, the Policy mandates the presence of a Chief Information Security Officer, a dedicated information security policy compliant with international standards, and the allocation of funds for the proper implementation of cyber security initiatives.

Apart from strategies aimed at strengthening the regulatory framework and encouraging open standards, the Policy calls for the operation of a Computer Emergency Response Team (CERT-In) as the Nodal Agency that would coordinate all matters on cyber security and the establishment of a 24/7 National Critical Information Infrastructure Protection Centre.
The National Cybersecurity Policy (NCIIPC). The NCIIPC would act as the nodal agency for all cybersecurity issues on critical infrastructure (including NPPs) under the Policy. Additionally, the Policy mandates periodic audits of the cybersecurity initiatives, certification of all those involved with the critical infrastructure and carrying out secure application or software development process in line with global security processes. Additionally, the National Cyber Security Policy provides comprehensive precautions and actions to be taken during a cybersecurity breach in any part of cyberspace, mainly when it involves critical infrastructure, evident from its specific emphasis on its security in the provisions.

Mechanisms to implement the Policy in India

Computer Emergency Response Team (CERT-in)

The Central Government, under a Gazette-published notification dated October 27, 2009, appointed the "Indian Computer Emergency Response Team (CERT-In)" under sub-section (1) of section 70B of the Information Technology (IT) Act, 2000. The CERT-In serves as the national agency for carrying out cybersecurity functions, according to the provisions of subsection (4) of section 70B of the IT Act, 2000. It is responsible for gathering, analysing, and disseminating data on cyber incidents; forecasting and alerting of cyber security incidents; formulating emergency measures for handling cyber security incidents; coordinating cyber incidents response activities; and publishing guidelines, advisories, vulnerability notes, and whitepapers about information security practices, procedures, prevention, response, and reporting of cyber incidents, among others (CERT-In, 2022).

The National Cyber Security Policy ascribes great importance to CERT-In in India's cybersecurity. Apart from improving communication and coordination efforts in response to cyber crisis scenarios, the Policy makes CERT-In the umbrella organisation that enables the development and operationalisation of sectoral CERTs round the clock for all coordination and communication efforts within the appropriate sectors for efficient incident response and resolution and cyber crisis management (Department of Electronics and Information Technology, 2013).

Moreover, CERT-In is authorised to request information from and issue directives to service providers, intermediaries, data centres and government bodies for carrying out the activities outlined in sub-section (4) of section 70B of the IT Act, 2000. Any relevant party, including government institutions, must report cyber incidents to CERT-In within six hours of becoming
aware of them or bringing them to their attention. According to this regulation, operators of nuclear plants must submit a cyber security plan for the Commission's inspection and approval. The Ministry of Electronics and Information Technology (MEiTY) Guidelines list the 'cyber incidents' that must be immediately reported to the CERT-In: compromise of critical systems or information, malicious code attacks, DoS and DDoS attacks, unauthorised access of IT systems or data, attacks on critical infrastructure, data breach, and data leak, that are of relevance for a nuclear facility's cybersecurity (CERT-In, 2022).

The CERT-In Guidelines state that relevant organisations must act or provide information or assistance to CERT-In as required by the CERT-In's order or direction for cyber incident response, protective and preventive actions related to cyber incidents, and cyber incident response planning. This assistance may help with cyber security mitigation actions and improved cyber security situational awareness. All service providers, intermediates, data centres, and governmental entities must, by law, enable logs of every ICT system they use, retain them securely every 180 days, and keep them under Indian law. These should be sent to CERT-In reports or whenever CERT-In requests or directs them (CERT-In, 2022).

Moreover, the CERT-In Guidelines state that apart from protecting the cyber infrastructure, an Information Technology Security Policy should contain measures for people security, including personnel security through background checking, security in job definition and resourcing, and education on IT security measures, among others (Department of Information Technology, 2003). Similarly, the U.S.-based Nuclear Sector Coordinating Council of the Cybersecurity & Infrastructure Security Agency requires that individuals working with digital plant equipment are subject to background checks, extensive security screening, cybersecurity training, and behavioural observation. The Defence-in-Depth (DiD) approach requires that strict controls over the use of thumb drives, laptops, and other portable media are maintained, and these devices are regularly scanned for malware. Furthermore, supply chain risks must be minimised by being aware of evolving cyber security threats, assets must be purchased only from approved vendors with a trusted distribution path, and testing assets prior to installation to ensure they operate securely as essential components of the Defence-in-Depth approach to be adopted (Nuclear Sector Coordinating Council, n.d.).

National Critical Information Infrastructure Protection Centre (NCIIPC)

U.S.-based Nuclear Threat Initiative (NTI) highlighted four broad priorities that they believe would significantly lower the probability of harmful cyber-attacks on nuclear sites:
institutionalising cyber security, mounting an aggressive defence, decreasing complexity, and promoting transformation (Pickering & Davies, 2021).

National Cyber Security Policy, 2013, aims to enhance the cybersecurity of India's critical infrastructure by operating a round-the-clock National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating related to the design, acquisition, development, use and operation of information resources (Department of Electronics and Information Technology, 2013). The NCIIPC, created in 2014 by the Government of India, mandates that organisations examine the Vulnerability-Threat-Risk assessment reports used to implement the infrastructure protection security controls. The NCIIPC Framework states that an organisation must assess if the security controls defined in Phase I (Clearly defining and understanding the various components of an NPP and the interlinking between them) are accurate, consistent, and comprehensive compared to the security measures mentioned in the established international standards, like the ISO 27001 standard or the North American Electric Reliability Corporation (NERC) and the National Institute of Standards and Technology (NIST) (National Critical Information Infrastructure Protection Centre, n.d.). Other international and country-specific standards regarding cybersecurity for nuclear facilities are covered in Arinze, Eneh and Longe (n.d.).

A similar initiative was carried out in the 2000s when the U.S. Nuclear Regulatory Commission (NRC) began including cyber requirements and eventually published the 10 CFR 73.54 Cyber Security Rule (which was fully implemented in 2017) for nuclear facilities in the U.S. (Pickering & Davies, 2021). In India, organisations from the critical sectors must inform the NCIIPC of their cyber security audit results and their strategies for maintaining a sufficient level of cyber security (National Critical Information Infrastructure Protection Centre, n.d.)

Threats to Nuclear Facilities

Given the damages a nuclear facility could cause, its safety is a vitality. Like other industries, safety depends on careful planning, proper design with minimal margins, backup provisions, high-quality components, and an operational safety culture (World Nuclear Association, 2022). Three incidents could be attributed to flaws in the reactor design: Three Mile Island (1979), Chernobyl (1986) and Fukushima (2011). The Three Mile Island incident saw the reactor getting severely damaged, without any human casualties, as the radiation was quickly contained. The Fukushima accident happened in the aftermath of the 2011 Japan tsunami, when three nuclear reactors, which were written off due to the loss in cooling, were inadequately
contained. Luckily, there was no loss of lives owing to radiation exposure. However, the 1986 Chernobyl disaster resulted in the death of 2 individuals, and 28 others followed due to radiation exposure (World Nuclear Association, 2022).

Thankfully, the nuclear industry has successfully avoided similar incidents- in the 61-year history of nuclear energy, these are the only three significant accidents at NPPs. (World Nuclear Association, 2022). The Royal United Services Institute, the world's oldest security and defence think-tank, adds another source of threat to NPPs: a plane crash into a nuclear facility by terrorists, especially after the 9/11 attacks. The industry believes a plane crash could breach the containment around an NPP, causing a fire. (Royal United Services Institute, 2023). However, insider threats pose a greater perennial threat to nuclear facilities, compared to a terrorist attack.

**Mitigating Insider Threats**

Cappelli, Moore and Trzeciak (2012) define an insider as:

> A current or former employee, contractor, or business partner who has or had authorised access to an organization's network, system, or data and intentionally exceeded or misused that access in a way that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems (p.xx)

Georgiadou, Mouzakis and Askounis (2022) outline various criteria for categorising insider threats. Employees could be vulnerable to insider acts due to negative events at work, personal circumstances, and life events. Cole (2008, as cited in Colwill, 2009) points out that organisations disregard insider threat either because they are unaware of it occurring, they are afraid of negative publicity, or is easy to remain in denial. Colwill (2009) adds another reason to the list: organisations recognise the existence of the insider threat but are unsure how to respond. Given the scale of the damage an insider threat could have, organisations dealing with critical infrastructure aim to implement measures to detect, deter, and avoid the insider threat. Insiders may jeopardise information confidentiality, integrity, and availability; therefore, unintentional and intentional risks must be considered (Colwill, 2009).

Dealing with insider threats is a top-priority security issue for any organisation handling critical infrastructure. In this regard, organisations ought to adopt a preventive and protection approach. Behavioural changes could act as an important clue to identifying insider threats. Changes ranging from overt physical actions supported by evidence, consistent shifts in usual behaviour or attitudes that may be apparent to other team members, boasting or even
threatening others about the intended act, and the language used in email correspondence are some pointers towards identifying an 'insider act' (Bell, Rogers, & Pearce, 2019).

Fundamental measures that could mitigate insider threats include enforcing baseline security policies and procedures, extending traditional policy and guidance, conducting personnel checks, and implementing focused risk assessments. Organisations, in plain, unified terms, must outline the expectations of insiders. Using business property for personal use while on the job must be strictly prohibited by restricting network access to critical applications and regulating access to websites irrelevant to the work must be in place to maintain legal compliance, cut down on time wastage, and lower the danger of malware infections. This is particularly important since the KNPP attack was carried out because two scientists were provided remote access to the plant's database, which the hackers exploited. Employee classification must be in place to specify granularity in access permissions for all insiders, including third-party people, attention should also be paid to effective employee classification (Colwill, 2009).

Strict rules must also exist regarding using portable devices inside critical infrastructure premises. 89% of employees in the UK reportedly connected a personal portable device to their company network at least once a week, and more than half of UK businesses had no controls to manage the use of removable media devices. Similarly, people in the security-conscious financial services industry in London loaded free CDs onto systems despite prominent warnings printed on the CDs to check company guidelines before loading. Furthermore, people have been tricked into using an abandoned USB memory stick with a 'friendly' Trojan (Colwill, 2009). The source of the cyberattack in Natanz and Gundremmingen serves as a reminder for India regarding the dangers posed by using personal portable devices within the premises of its NPPs.

However, these measures run into problems in implementation. Bell et al. (2019) show that screening is unlikely to reveal shifts in attitude, loyalty to the company, or employee discontent, even if repeated throughout the job lifespan. When organisations try to increase security against external threats without considering its impact on its employees, this adds another layer to the insider threat problem as it could affect employees in terms of increased stress and longer completion times for routine tasks, and it may unintentionally increase the insider threat if the worker tries to get around security or becomes more susceptible to social engineering as a result.
Furthermore, the biggest problem regarding insider threats is that the 'insider' may not have done an 'insider act' to cause harm. Research by the UK's Centre for the Protection of National Infrastructure (CPNI) shows that only 24% of insider acts in critical infrastructure organisations analysed were committed by people exploited by outside parties or joining with the intent. This means that 74% of the time, the 'insider' did not indulge in the act deliberately (Bell, Rogers & Pearce, 2019). Even in the case of the KNPP cyberattack, the scientists did not open the infected links to harm the plant. It would be morally incorrect to accuse someone of doing something they did not intend to do. Therefore, the best way out for India is to inculcate a culture of cybersecurity among the employees working in its various nuclear facilities.

Organisational Culture

Organisational culture refers to the shared values, beliefs, and presumptions among employees within an organisation, which emerges through interactions between members and their surroundings through myths, symbols, and artefacts that are unique to that organisation (Roy, Newman, Round, & Bhattacharya, 2023).

Chye and Boo (2004) discovered a significant relationship between organisational ethical culture, job satisfaction and organisational commitment in Singaporean managers. This relationship was measured by Singaporean managers' perceptions of top management support for ethical behaviour and the relationship between ethical behaviour and career success. Similarly, Treviño, Butterfield and McCabe (1998) found a favourable relationship between employees' organisational commitment and the ethical culture. However, most studies about the organisational culture and their associated effects reviewed in Roy et al. (2023) revolve around private organisations, and the nuclear industry is highly likely (if not certainly) in government control. In a government organisation, leadership cannot be expected to create a long-lasting example of ethical leadership because they only have a fixed tenure. In such cases, the best way to cultivate an organisational culture is from the bottom up: inculcating core values and practices of the organisation among employees who have a longer tenure than those in the higher levels of the hierarchy.

Organisational Culture and Security

A shared identity or the common presumptions about "who we are" is paramount for developing an organisational culture. Thus, recommendations made by members will not be followed unless they align with the organization's presumptions about itself. These may not always be especially conscious, but they may become apparent if we look closely at the organization's
strategic choices. For a group to have a sense of mission and concrete goals within their work restrictions, it needs a common language and shared assumptions about the fundamental logistical procedures. The agreed fundamental presumptions about how things should be done and how goals are to be met are some of an organisational culture's most crucial components. Once procedures are accepted as routine, they become the cultural tenets that may be the most difficult to alter (Schein, 2010).

An essential component within an organisational culture is the organisational subculture. According to Schein (2010), organisational culture is defined as shared basic assumptions influencing how members feel and act. It is also an essential element for the safety of high-risk organizations. However, opinion is mixed about the impact of organisational subgroups on the overall functioning (and safety). The IAEA (as cited in Badia, Navajas, & Losilla, 2020) believes that the existence of subcultures is not an element that has a positive or negative impact. However, the man-made disaster theory puts forth that a lack of information flow causes accidents, and accidents could be prevented when warning signs are detected, and these warning signs are likely to be known to an organisational subgroup. Therefore, the existence of subcultures is not necessarily negative; acknowledging and managing them could prevent 'safety blind spots' (Badia et al., 2020).

Boisnier and Chatman (as cited in Badia et al., 2020) also consider that subcultures can develop within a robust and integrated culture while strengthening the organization's flexibility to change and adapt to external contingencies. Thus, organisations with increased cultural variety are better prepared to respond to complex environments. According to Wahlström (1999), cultural differences should be considered vital factors of safe evolutions in nuclear facilities, meaning research should focus on how safety is built due to cultural interactions. Nuclear facilities fall under the category of what Mintzberg (1979, as cited in Badia et al. 2020) defines as 'machine bureaucracy', which comprises highly specialised, routine operational activities, an abundance of rules, regulations, and large-sized units of the organisation, formalised communication across the operational level, the use of functional foundation for task grouping, relative centralization of decision-making authority and a complex administrative structure that separates line employees from staff, driven primarily by a particular need for safety.
Cultivating a Cybersecurity Culture within Nuclear Power Plants

Organisational culture is the foundation upon which the safety culture. According to the IAEA (1991, p. 4 as cited in Ylönen & Björkman, 2023), safety culture in the nuclear context is an "assembly of characteristics and attitudes in organisations and individuals which establish that nuclear plant safety issues receive the attention warranted by their significance as an overriding priority." It is a widely accepted concept in the nuclear industry and many other high-risk industry sectors. However, the term "security culture" is far more recent and less used (Ylönen & Björkman, 2023).

ISO/IEC 27034-2 contains the principles, elements, procedures, and ideas intended to aid facilities in incorporating security into the entire application lifecycle. Each nuclear facility should have a clearly defined organisation for reporting security incidents in the nuclear domain. The security culture should also include the extent and methods of reporting and the required training. Staff must possess the minimum knowledge and abilities required to perform expected standard functions. For specific job profiles, like system administrators, specialised technical security training is required, in addition to awareness training for the employees at a nuclear plant (Gupta & Bajramovic, 2017).

Additionally, the RACI (Responsible-Accountable-Consulted-Informed) charts used by ISO/IEC 27034-3 to carry out process operations are essential in inculcating a cybersecurity culture in nuclear facilities. Distinguishing between 'Responsible (R)' and 'Accountable (A)' roles is a crucial component of the RACI jobs: Technical managers who can enforce local cybersecurity organisation and technical implementation, including relationships to external specialists, should be given the responsibility (R function) to coordinate the implementation of security policies and application security controls, while those who ensure that security is accounted for the entire scope, that resources are available, and that recurring operations are carried out should be given the 'Accountable (A)' function. Moreover, the 'C' (Consulted) function mandates that specific cybersecurity-related decisions must be consulted with the indicated experts (Gupta & Bajramovic, 2017).

The NCIIPC Cyber Security Framework recommends personnel screening, termination, and accountability, with a proper redressal system for resolving cases of personnel-induced cybersecurity breaches (National Critical Information Infrastructure Protection Centre, n.d.). Moreover, the Standard Operating Procedures mandated in the CERT-In (2022) Guidelines (and other guidelines on cybersecurity) adopt a tone of authority that does not leave exceptions...
since the nation's integrity and territorial security are at stake. Thus, unquestioned compliance with the regulations becomes and ought to be part of the work culture in an NPP. The stringent screening process to get employed in an NPP, the strict system of checks there, the punitive punishments for violations mandated by the Information Technology (IT) Act, 2000, and its subsequent amendments internalise compliance with the rules among employees (Ministry of Defence, 2019).

Furthermore, increasing employees' knowledge of security hazards is the goal of security awareness, for 'Security is everyone's responsibility' must be the driving force behind all education and training initiatives. Staff members must comprehend how poorly educated and inexperienced personnel might imperil sensitive information and nullify any technical security measures or processes in place (Gupta & Bajramovic, 2017). Routines, norms, and standardised practices support system maintenance and gradual advancement. Members can avoid confusion and mistakes with the support of top-down communications and clear instructions, which helps to achieve uniform results and shared objectives because 'doing things right' is valued in a culture of hierarchy (Oh & Han, 2020). To achieve a positive safety culture, everyone in the organisation has a responsibility to make all reasonable efforts to prevent accidents and injuries, and a shared set of standards—a "way of life"—that transcends individual members is created through the blending of role behaviours and the solidification of social norms (Lee & Harrison, 2000).

Discussion

This study sought to explore how robust India's cybersecurity framework is to protect its NPPs by reviewing the existing mechanisms considering international good practices and standards and the causes and results of cyberattacks on various nuclear facilities worldwide. Moreover, it sought to look at what India could do to mitigate insider threats and cultivate a cybersecurity culture in its NPPs.

The study finds that legislation on cybersecurity falls short because of difficulties in identifying the perpetrator of a cyberattack. However, the operating procedures placed by CERT-In and NCIIPC are found to be significantly robust. The various case studies analysed in the paper show that a human element created a vulnerability in the facility's cybersecurity framework, which cyber attackers eventually exploited. This, coupled with practical difficulties in identifying a cyberattacker, shows that the best protection for Indian NPPs comes from within-by mitigating intentional and unintentional insider threats and cultivating a cybersecurity
culture. This study does not recommend implementing more control on nuclear personnel, as it will likely bring down productivity. Instead, it recommends a balance between the opportunities for employees to display their adherence to operational safety standards while sticking to the core safety values within the nuclear facility.

Conclusion

This paper attempted to determine how robust India's cybersecurity framework is when protecting its nuclear facilities. The study found that legislation on the issue of cybersecurity is robust in punishments but suffers from an inability to identify the perpetrator, which India has compensated with the establishment of the CERT-In and the NCIIPC. Moreover, the study believes mitigating insider threats and cultivating a cybersecurity culture is the best solution for India, and every other nuclear power, to protect its nuclear facilities from cyberattacks.

References


Press Information Bureau. (2022, December 8). Union Minister Dr Jitendra says, security arrangements are in place to secure India's nuclear power plant systems from cyber-attack. Retrieved on 7 August 2023, from https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1881733


