WELCHMAN KEEN

SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE

RISKS & OPPORTUNITIES

Whitepaper by Welchman Keen

Contents

Introduction

The protection of Critical Infrastructure (CI) has always been a key concern for states' national security. CI refers to key infrastructure which are employed for the supply of essential services such as energy, drinking water, government, finance, and transportation. Although there is not a universal definition, CI commonly designate infrastructure which are essential for the functioning, maintenance and resilience of vital societal functions that protect the safety, security, economic or social well-being of people, and the disruption or destruction of which would result in significant impact (CIPedia, 2020). As nations globally continue to develop and grow, critical services are becoming increasingly complex and interconnected, with consequential challenges for their security. The extensive integration of Information and Communication Technology (ICT) has introduced new vulnerabilities and created new categories of risks in the CI landscape. Not only has it increased the likelihood and potential reach of technical failures, but it has also made CI liable to be targeted by malicious attacks via cyberspace. The need for effective cybersecurity strategies, policies and activities tailored to each country becomes evident. However, designing an effective protective measure for CI is challenging as several factors have to be taken into consideration. First, due to the growing interconnectedness of essential services, it is important to adopt intersectoral approaches aimed at increasing the maturity of cybersecurity strategies in an organic manner. Second, CI which traditionally had been purely government-owned, has now evolved into a multi-stakeholder environment which includes government agencies, privately-owned companies, academia, defence agencies, and international organisations. Hence, there is the need to ensure cooperation and dialogue between the different actors to implement an all-encompassing cybersecurity posture in a coordinated manner.

As countries are accelerating the digitisation of their CI landscape to increase reliability and to cope with the growing demand for cybersecurity services, cybersecurity has become a foundational element underpinning the achievement of socio-economic objectives of modern economies. This whitepaper will outline a set of general principles for establishing a holistic cybersecurity approach to CI. It will first explore how digitisation has changed the focus from the protection of CI to the protection of essential services. It will then discuss general guidelines which can serve as a useful tool to all stakeholders, which includes both national actors with cybersecurity responsibilities and private sector operators.

CI and CII

The term Critical Information Infrastructure (CII) appeared in the early 2000s (Wenger, Metzger, & Dunn, 2002) and refers to the "material and digital assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of a country's government" (Brunner & Suter, 2010). Although the concept of CII has been widely employed at a governance and academia level, there is still little agreement regarding a widely accepted definition and a distinction with the broader category of Critical National Infrastructure (CI). In fact, there are two sides to CII: on the one hand, it considers ICT and digital assets as a stand-alone CI; on the other hand, it needs to take into account the intersectoral aspect of ICT which are employed and constitute an essential asset within each of the CIs (Energy, Water & Food, Finance etc.) as shown in Diagram 1.

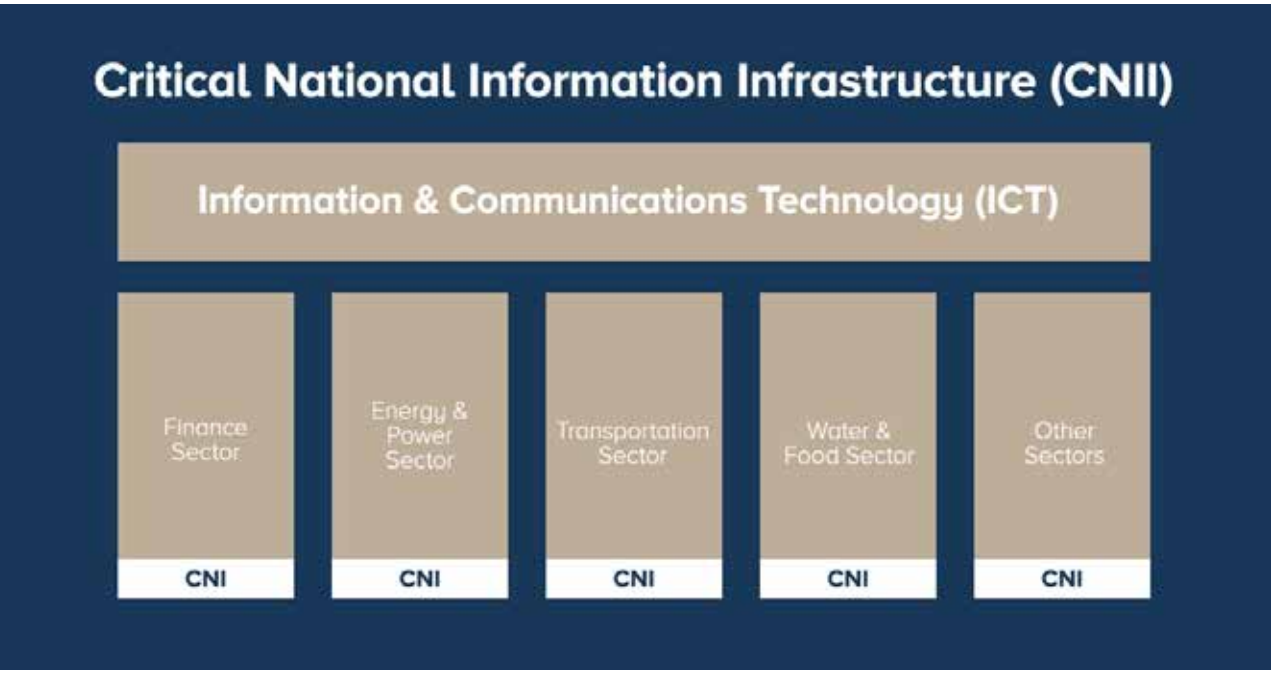

Diagram 1: CNII

In recent times, the complexity of extrapolating the concept of CII has become even more evident as CI is increasingly reliant on digital assets, where the exchange of data between different CIs is essential to the operation of infrastructure as well as to the supply of services. Generally, we can affirm that CI is broader than CII, but CII constitutes the backbone of CI. In any case, the two concepts are strictly interconnected and recent frameworks for defending critical sectors have adopted a "service-oriented approach", which is a more holistic approach that focuses on protecting the supply of essential services against cybersecurity threats. This approach goes beyond the mere protection of information infrastructure that supports these services (OECD, 2019).

For the purposes of this study, we will adopt this "service-oriented approach" and we will generally refer to Critical Information Infrastructure (CII) as the economic and social activities that depend on digital-physical assets and therefore need protection against cybersecurity threats.

CII Cyber Risk Landscape

Over the last few decades, the exponential growth and rapid adoption of Information and Communication Technologies (ICTs) has transformed critical sectors of modern societies. To benefit from improved productivity, efficiency and supply capacity, today's essential services rely on CIIs with an increasingly pervasive cyber component. As we move forward to the wide adoption of the industry 4.0 paradigm, ICTs are bound to become even more integral for increasing the supply and reach of critical services. The usage of IoT devices, together with 5G technology, is becoming pervasive in many verticals with an estimated 41.6 billion connected devices around the world by 2025 (IDC, 2019). Cloud solutions have also become critical to operations with 94% of businesses worldwide relying on them (Weins, 2020). Artificial Intelligence, given the growing availability and preponderance of data, will find unprecedent applications in several domains including critical sectors for national security, well-being, and economy. According to the World Economic Forum, we are now entering a new era referred to as "Globalization 4.0", with digital assets and services constituting the backbone of the economy (Schwab K. , 2018).

"The exponential growth and rapid adoption of Information and Communication Technologies (ICTs) has transformed critical sectors of modern societies."

While the reliance on digitised CII is growing, technology remains inherently vulnerable due to the increase in cyber risks. According to the 2020 Global Risks Report (World Economic Forum, 2020), cyber-related risks stands in the top 10th categories of risk to modern societies. These include not only accidental events capable of tampering physical and digital assets, but also malicious attacks to CII via cyberspace.

The growing connectivity has significantly broadened the vulnerable and attackable surface. Furthermore, due to their strategic nature, CII makes an appealing target for an extensive spectrum of malicious actors. Possible attackers range from so called “script-kiddies”, disgruntled workers, petty criminals, organised criminals, hacktivists and terrorists, to state sponsored groups (Rudner, 2013).

While attackers can be motivated by personal reasons, political beliefs, economic goals or geopolitical interests, due to the high complexity of the CII landscape any theft, manipulation and destruction of critical data can escalate and result in significant impacts and major disruption of essential services with serious repercussions on the country’s economy, stability, and social well-being.

One of the earliest, and most used, case studies is the 2007 Estonian episode (Davis, 2007). Estonia fell victim of an extensive Distributed Denial of Service (DDoS) attack which targeted institutional portals, banks, transportation, newspaper, and broadcasting stations, causing prolonged disruptions. Though services were restored without long-term or catastrophic consequences, this attack showed the vulnerability of CII and that cyber-attacks are possible and capable of affecting the supply of essential services.

The vulnerability of CII also poses a risk to the economic wellbeing of a country. In 2017, ransomware called NotPetya spread across the globe affecting government agencies and companies, resulting in more than $10 billion in total damages (Greenberg, 2018). NotPetya has been largely declared as the most devasting cyberattack in history (White House , 2018). Most affected were large organisations such as FedEx, Durex, Maersk, and Merck (Maloney, 2019) which suffered nine-figures losses.

The disruption of essential services might also pose a critical risk factor to public health. In 2017, ransomware known as WannaCry infected thousands of computers worldwide. Although it was not designed to target the healthcare sector, a significant number of hospitals fell victim to the attack. The United Kingdom was particularly impacted, and because medical data could not be accessed, the national service provider had to cancel over 19.000 medical appointments. Similarly, in September 2020, a hospital in Germany whose databases were under attack was obliged to turn away emergency patients, resulting in the death of a woman who did not make it to the closest hospital twenty miles away (Eddy & Perlroth, 2020).

The outbreak of the Covid-19 pandemic has further intensified the exposure to cyber risks as there is an unparalleled increase in the usage of internet through teleworking. A recent assessment revealed that the Covid-19 pandemic has seen not only a general increase of malicious activities but also a shift of attacks from small businesses to critical infrastructure and government networks (INTERPOL, 2020). Since the onset of Covid-19, not only has the number of incidents increased, but the reach of the incidents has increased as well. With greater reliance on connectivity and digital assets, even minor disruptions can cause significant inconvenience. Now more than ever, the transformational power of technology and its ability to be an enabler for social stability, wellbeing and economic growth is at stake. Implementing a solid cybersecurity posture is essential to reap the benefits of digitalization.

Global Cybersecurity Attacks

2007 Estonian Episode

Estonia fell victim of an extensive Distributed Denial of Service (DDoS) attack which targeted institutional portals, banks, transportation, newspaper, and broadcasting stations, causing prolonged disruptions.

2017 NotPetya Ransomeware

In 2017, ransomware called NotPetya spread across the globe affecting government agencies and companies, resulting in more than $10 billion in total damages (Greenberg, 2018).

2017 WannaCry Ransomeware

Although it was not designed to target the healthcare sector, a significant number of hospitals fell victim to the attack. The United Kingdom was particularly impacted, and because medical data could not be accessed, the national service provider had to cancel over 19.000 medical appointments.

2020 Germany Hospital

in September 2020, a hospital in Germany whose databases were under attack was obliged to turn away emergency patients, resulting in the death of a woman who did not make it to the closest hospital twenty miles away (Eddy & Perlroth, 2020).

Operational Technology and Cybersecurity

Many critical sectors such energy, water supply and production, rely on Operational Technology (OT), which refers to a set of technologies that connect physical elements, networks, and communication protocols to execute industrial operations. Typical examples of OT are SCADA (Supervisory Control and Data Acquisition), ICS (Industrial Control Systems) and DCS (Distributed Control Systems) etc.

OT is inherently insecure as it interfaces with physical processes (warming, cooling, chemical reactions, liquid flow etc.) and needs to respond to "hard real-time" requirements where the availability of data becomes more important than its security. This means that applying standard cybersecurity measures in an OT environment will be particularly challenging (Roberto Setolaa, 2019). In fact, incorporating control routines such as antivirus, firewalls and encryption might delay the immediate exchange of data, and affect the readiness of a system. Similarly, patching and updating requires downtime of the infrastructure which needs to be planned long in advance (Cook, Janicke, Smith, & Maglaras, 2017).

For a long time, OT has been protected by so-called "security through obscurity", which means that control systems were "air-gapped" i.e. not connected to the internet, but rather employed legacy systems and proprietary networks (Berinato, 2002). In other words, malicious actors not only had to have an extensive knowledge of the system in use, but also physical access to the site. However, to respond to the primary need of operability and reduce reliance on custom and legacy systems vendors, many CI sectors have turned to off-the-shelf systems and have increased their connectivity. Today, industrial assets are largely equipped with internet connection (the so-called Industrial Internet of Things) (Setola, Oliva, Assenza, & Faramondi, 2020).

While the integration of IT protocols and internet connection have significantly improved the performance of OT-based CII, it has also exposed IT systems to cyberspace threats with a dramatic increase in the number of attacks. A survey of security professionals in six countries found that 90 per cent of OT-based CII had been impacted by at least one successful attack (Gary, 2019). Another report highlights that half of the organisations relying on operational technology (OT) experienced downtime as a result of a cyber-attack over the past two years (Ashford, 2019). Similarly, A study of 320 cybersecurity professionals on OT/IT, commissioned by Kaspersky Labs, revealed that 77% of companies put cybersecurity as a major priority while 32% said that it is very likely that their organisation will become a target of a cyberattack involving industrial control systems (ICS) (Schwab & Poujol, 2018). The study further revealed that only 23% of the organisations were complaint with mandatory industry or governmental regulations and guidance.

In fact, the most critical aspect of OT vulnerability is that attackers can manipulate normal operations of a system to induce failures and mechanical break points (Setola, Oliva, Assenza, & Faramondi, 2020), potentially causing major damages, disruption of services and even harm. For example, in 2010 Stuxnet tampered with the industrial process of a nuclear plant in Natanz; in 2014 a malware prevented a furnace from properly shutting down in a German steel mill; in 2015 and 2016 BlackEnergy3 and Crashoverride caused power blackouts in Ukraine (Dragos Inc., 2017); and in 2017 Trisis shut down a chemical plant in the Middle East (Dragos Inc., 2017). 2020 has been a particularly intense period for OT as at least five cyberattack episodes resulted in physical complications for industrial operations including the blockage of productions lines in a Honda (Japan) and Lion (Australia) site, or even the shutdown of the whole infrastructure as experienced by a natural gas operator in the US (Dragos Inc., 2020). Similarly, in May 2020 the State of Israel thwarted an attack targeting its water supply system (Times of Israel, 2020). The operation was aimed at increasing the proportion of chemical agents in the country's water source, making it unpotable and leaving a significant proportion of the population without water in the midst of the COVID-19 pandemic.

While OTs are the most complex targets and attacking them requires considerable sophistication and resources, the employment of Artificial Intelligence and Machine Learning significantly reduces the training duration within the targeted network. These open up new ways to transform cyber means into tactical tools that can quickly be deployed not only in geopolitical scenarios, but also for economic and financial purposes.

Human Factor & Skills Shortage

As individuals are becoming increasingly interconnected through the digital environment, security cannot be perceived and managed as a mere technological issue. On the contrary, the human component is one of the main challenges in cybersecurity. People are routinely considered the weakest link of the cybersecurity chain and are the cause of a large proportion of security breaches (Corradini, 2020).

It is reported that malicious actors prefer to target people rather than infrastructure. A recent study shows an extensive use and refinement of social engineering techniques and reports that more than 99% of analysed attacks required at least one point of interaction with an employee to succeed (Proofpoint, 2019). It is evident that an essential measure to reduce cyber risk is to build a strong security culture and awareness among CII operators.

The digital environment has also become significantly complex and specialised. Consequently, the demand for skilled cybersecurity professionals has increased exponentially while the cybersecurity industry faces a critical shortage of skilled and diverse personnel. Estimates report that there will be approximately 3.5 million vacant cybersecurity jobs by 2021 around the globe, which means that in order to meet the demand, the cybersecurity talent pool needs to increase at a near-impossible rate of 145% per year (Morgan, 2018). Thus, it becomes a crucial area of action for countries worldwide to meet this demand of professional skills.

Addressing Critical Information Infrastructure Protection (CIIP)

Considering the increase in infrastructure vulnerability and sophistication of the threat, the need for Critical Information Infrastructure Protection (CIIP) has become increasingly prominent. An effective CIIP needs to consider both the expansion of the threat spectrum in terms of new capabilities and asymmetric actors, and the new vulnerabilities of digital and interconnected societies. The unpredictability of cybersecurity challenges due to uncertainty concerning the identity of adversaries, their capabilities and the contingencies that can be caused by the exploitation of vulnerabilities, calls for a security posture built around the concept of "risks", which are by definition "indirect, unintended, uncertain and situated in the future" (Eriksson & Giacomello, 2009). Risk oriented security strategies guide defenders in their allocation of resources to prioritize security measures and adopt a posture which is commensurate to the existing risk. While there is a tendency to consider cyber threats as a risk to business, and there fore a "Risk Business," it is essential to look at this risk from the perspective of national (and to some extent international) security. A compromised CII can have a far-reaching impact that jeopardises the stability, economy, daily-life and prosperity of a country (Luiijf, Schie, Ruijven, & Huistra, 2016). Therefore, there is an increasingly important need to elaborate CIIP posture not only at the operator level, but also to foster resilience and preparedness from the top at a national level. Countries should develop cybersecurity strategies, policies, and activities to ensure, in a common effort with CII operators, the resilience of critical sectors. The following sections will provide general guidance on how to elaborate cybersecurity posture at both a national and operators levels.

"The unpredictability of cybersecurity challenges calls for a security posture built around the concept of risks."

CIIP for Countries

While it is essential for all countries to develop their own CIIP strategy, there is no one-size-fits-all approach that suits every nation. Each nation needs to tailor its CIIP strategy based on the context in which it will be applied. Countries differ in legal (and regulatory) structure, governance over CII, level of integration of digital technology, resources, culture, role of stakeholders etc. If it is not possible to build an ultimate CIIP model, all effective national security postures need to address a set of necessary building blocks. This section will indicate and analyse key areas of intervention for states, namely:

1. Institutional architecture
2. National Risk Assessment
3. Identification of Critical Information Infrastructure
4. Strategies, policy, regulations, and standards
5. Public-Private Cooperation
6. Education and capacity building
7. Development of a trusted market
8. National crisis management
9. Monitoring and improvement

Institutional architecture: Addressing the complexity of CIIP requires states to establish an efficient institutional architecture which clearly defines mandates, roles, responsibilities and accountable bodies or people. The CIIP posture can be appointed to one or more agencies which cover both strategic and operational levels. The first relates mostly to governance aspects and political will, and entails the identification of priorities, elaboration of strategies and policies as well as the establishment of dialogue and coordination with stakeholders (both in the national and international scenarios). The operational level, which is normally delegated to national Computer Incident Response Teams (CIRTs) is more practical. It entails the production of technical standards, guidelines and best practices, the organisation of educational activities and the coordination of networks to share information about vulnerabilities, threats and related remediations. Another key activity is developing incident response capabilities and supporting CI operators when an incident occurs. Even if the CIIP mandate is clearly appointed to specific national agencies, the multiplicity of dimensions, correlations and interdependencies of the CI landscape calls for the adoption of multi-agency and Whole-of-Government governance architecture. These aim to join up and coordinate all relevant stakeholders such as ministries, regulators, agencies, regional and local bodies etc. Typical settings are roundtables, inter-agency councils or coordination committees.

National risk assessment: One of the key activities for CIIP is conducting a systematic national risk assessment in order to create an extensive understanding and awareness of the existing risks the state faces in terms of threats, hazards and vulnerabilities. Risks should be assessed using standard metrics based on likelihood of occurrence and potential impact. Building a national risk profile is the first step to elaborate national prevention and remediation measures. It is a good practice to involve all relevant stakeholders in the assessment in order to reach an all-encompassing understanding of the national risk profile. This will allow stakeholders to acquire not only the expertise, but also the acceptance of key national actors. The assessment should be regularly updated to reflect changes in the national risk panorama.

Identification of Critical Information Infrastructure: A key stage of any CIIP is to identify what is critical to a country in order to allocate more resources for the protection of assets, services, processes and infrastructure where failure would result in serious consequences. As discussed previously, nations have different interpretations of criticality and its definition varies from country to country. While it is helpful to look at bolrrowing definitions elaborated by other subjects (preferably politically, demographically, geographically, and economically similar), nations need to identify their own CII. There are various methodologies to identify critical assets. Typically, they can be broken down in three steps:

i) Identifying critical sectors (energy, health, transport, water etc.)
ii) Identifying the critical services in each sector (electricity, gas, hospitals drinking water etc.)
iii) Identifying the assets, operators, infrastructure, and processes which are essential for the supply of these services

For the third step, infrastructure can be filtered using a set of sectoral and intersectoral criteria such as:
- Market share
- Affected geographic area
- Amount of people depending on the infrastructure
- Recovery time

A key criterion to consider is the correlation in terms of dependencies (where the functioning of an infrastructure is essential for the functioning of another) and interdependencies (where infrastructure are mutually essential to each other) (Eric Luiijf, 2008). CII are highly interconnected, and failures can easily generate an unpredictable and debilitating cascade effects on different services and sectors. Therefore, assets with a higher level of correlation and the potential of affecting other infrastructure should be deemed particularly critical.

Strategies, policy, regulations and standards: An organic and homogenous CIIP should be guided from the top through the adoption of strategies, policies, regulations and standards which outline and enforce appropriate principles in addressing cyber risks and convert national security priorities into actionable and auditable requirements. These documents have different level of specification. While strategies and policy normally express principles and general guidelines, regulations and standards outline specific conditions and requirements that operators should meet. Not all standards will or should be enforced, but they can serve as an indication of the best practices to address specific risks. It is important that enforced disciplines consider the existing risk landscape (also in relation of specific sectors), as well as constraints and reasonable applicability. The aim of this component of CIIP is to ensure that all critical sectors benefit from a minimum level of cybersecurity to create a status of systemic resilience.

Public-private cooperation: While national authorities have a role in outlining the high-level CIIP strategy, most operational aspects and cybersecurity decisions are implemented by single operators which are often private or semi-private entities. In such a scenario it is essential to promote cooperation within and between operators and public entities in the format of Public-Private Partnership (PPP). Different stakeholders must operate together in a coordinated manner as in the complex net of correlations operators are to some extent dependent and responsible for actions implemented by another entity. Cooperation is useful to develop an intersectoral view of the CII panorama and can be implemented through various initiatives such as through regulations, information sharing, mutual support, sharing of best practices, pooling of resources, trainings and capacity building, inter-organisational networks of collaboration and joint decision making.

Development of a trusted ICT market: CII is increasingly integrating a wide variety of new technology such as virtualization, cloud, sensors, networks, adopting open software and enlarging the ecosystem of service partners. This raises concern about the security of the supply chain. Supply chain cybersecurity risk refers to the possibility of weak or compromised vendors, partners, and service providers. This category of risk is broad and includes partners with poor cybersecurity hygiene used as an attack vector, but also the risk that a supplier could maliciously embed in its products concealed backdoors and software, or critical zero-day flaws. The relation between the supply chain, CIIP and national security is evident, as the security of a chain is as strong as its weakest link. Public authorities should address this supply chain risk by developing a secure market for digital products and services while imposing minimum standard requirements and establishing certification systems. This would help with the creation of a trusted pool of providers from where CII operators can select partners with a verified and auditable cybersecurity maturity.

National crisis management: Since risks can be mitigated but never completely eliminated, a thorough national CIIP should contain not only a preventive approach, but also measures and mechanism to manage crisis and incidents at a national level. These typically include the prior elaboration of plans for dealing with significant disruptions, related actions to ensure the supply of minimum levels of impacted services and remediation to restore normal operation in a timely manner. The elaboration and implementation of such plans, as well as the decision-making during crisis should be coordinated at the national level, possibly through the establishment of a responsible team which can represent all relevant stakeholders, national CIRT and public authorities. It is important to periodically test the preparedness of the CIIP structure in dealing with crisis. For example, many countries, regions, and international organisations including ITU engage in cyberdrills where major incidents are simulated.

Monitoring and improvement: The implementation of the CIIP posture is as important as its definition. Countries should establish formal processes and mechanisms to constantly monitor its effectiveness. To be monitored, CIIP related activities need to clearly define their objectives and identify a set of indicators to measure and track their implementation. Also, the security posture should be reviewed by integrating lessons learned and adjustments which emerge from critical elements identified during implementation. Since the cyber landscape is constantly evolving, and new threats are always emerging, countries should continuously monitor and improve the adequacy of their CIIP. The security posture should clearly identify the appointed authority responsible for monitoring the implementation of the CIIP.

CIIP for Operators

CII operators need to develop corporate policies to support a security posture to ensure that the right people, technologies, processes, and programmes are employed and deployed to prepare, protect, defend and respond to cyber risks. Adopting a structured and repeatable risk management approach is key to make certain the CII is protected both physically and virtually. Some key activities critical operators should include in their security posture are:

1. Define a risk management framework
2. Build and test emergency plans
3. Training and education
4. Supply chain security
5. Information-sharing and cooperation
6. Legal compliance
7. Continuous monitoring and assessment of cybersecurity posture

Define a risk management framework: CII operators should adopt and apply a risk management framework. Such a document elaborates a continuous and repeatable methodology for identifying, assessing, and responding to cybersecurity risks. Managing risk entails understanding the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine their risk tolerance, thus the acceptable level of risk for achieving their supply and organizational goals. Once the risk tolerance is determined, operators are able prioritize remediations and make informed decisions about cybersecurity investments. In fact, risks can be managed by employing various solutions, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the supply of critical services. A typical example of risk management methodology is the framework published by The National Institute of Standards and Technology (NIST) (NIST, 2018). The document is designed for CII operators and is based on security controls grouped around five categories: identify, protect, detect, respond, and recover.

Build and test emergency plans: A complete cybersecurity program cannot be limited to the implementation of preventive controls, but must also entail incident response, business continuity and recovery plans. Broadly, this includes capabilities to proactively detect and respond to incidents in order to mitigate their effects, ensure minimum services supply during a crisis, and facilitate the prompt restoration of normal operations. The emergency response program should be tailored according to the cyber risk landscape and should clearly outline roles, responsibilities, and practical actions to be implemented in relation to potential incident scenarios and include communication with relevant stakeholders. To define plans, operators can look at lessons learned from past incidents and existing standards, guides, and best practices. Also, emergency plans need to be periodically tested, for example by engaging in cyber-drills or other exercises, to test their effectiveness and the preparedness of the infrastructure.

Training and education: This is an ongoing process for all organisations, and operators must continuously ensure employees have the right skills, knowledge, and attitude to address evolving risks, threats, and attacks. Cybersecurity awareness training, exercises, and educational activities should be delivered periodically to all personnel. Similarly, technical staff should receive training that is tailored to their operations. A key component is security awareness as a large portion of incidents are caused by human behaviour. Employees must be made aware of information security policies and the importance of adhering to them. Communicating this to all employees is vital to ensure they know, understand, and comply. The key outcome of security awareness programs and activities is to create a culture of security, change of behaviour and attitudes.

Supply chain security: Due to extensive outsourcing, today's supply chain is increasingly complex and externalized, with subsequent additional risks. The resilience of a supply chain is dependent on its weakest link and operators are secure only if their entire ecosystem of partners and vendors is secure. Adversaries can use poorly protected partners as attack vectors to compromise critical operators. Similarly, digital assets might come with intrinsic bugs and vulnerabilities. Therefore, an integrated and sustainable supply chain security objective must be included in business plans, contracts, and operations. Operators need to ensure that all third parties have adequate cybersecurity measures in place and respond to specific cybersecurity criteria to be included as a binding condition in the contracts.

Information sharing and cooperation: Because of increasing complexity and correlations, no single CII operator can individually deal with cyber risks. On the contrary building trusted and frequent communication channels with other stakeholders is a core element of CIIP. Sharing information about threats, vulnerabilities, standards, best practices, remediations etc, before during and after incidents is a vital aspect for ensring security and preparedness in the CII landscape. Through information sharing, critical sector organisations can reduce and prevent the spread of the incidents and minimise the damage to the infrastructure and country. Because this kind of information can be highly sensitive also for national security concerns, it is essential to engage only in trusted networks preferably with the involvement of public authorities. Information sharing can be performed within and across public and private sectors, and at the national and international levels.

Legal compliance: Critical operators should conduct their activities according to legal guidelines. Regulations are generally based on type of industry, sector, service, customers, location etc. They typically include cybersecurity and data protection/privacy requirements. Legal compliance ensure that operators meet critical security standards identified by national decision makers, and also ensures that responses to cyberattacks fall within national and international norms, particularly when it comes to attending to offending servers physically located in other countries or activities designated as “hacking back.”

Continuous monitoring and assessment of cybersecurity posture: Given that the digital risk landscape is in a constant state of evolution, CII operators need to build repeatable processes to monitor and assess their cybersecurity maturity level on an ongoing basis, with objectives and constraints in mind. The assessment should consider the risk-related adequacy of the processes, people, and technology, to identify substantial gaps and determine appropriate remedies to resolve weaknesses. Assessment processes should examine the general preparedness of the operator, including the ability to detect and to respond to incidents and ensure business continuity. The assessment should also consider a wide variety of potential cybersecurity incident scenarios and their potential consequences

Conclusion

The rapid digitisation and connectivity of CII has introduced new vulnerabilities and significantly broadened the categories and reach of risks threatening the resilience of modern essential services. Similarly, the CII landscape has become considerably complex because of global trends which have led private stakeholders to play a crucial role in the supply of essential services. Although the necessity of CIIP has been largely acknowledged, many countries are still lagging in the definition and implementation of strategies, policies, and activities to protect essential services. The general principles as outlined for establishing a holistic CI tailored cybersecurity approach can serve as a useful risk-mitigating tool for all stakeholders, including both national actors with cybersecurity responsibilities and private sectors operators.

References

Abercrombie, K. (2019, May 8). ICS Security - IT vs OT. Retrieved May 21, 2020, from Context: https://www.contextis.com/us/blog/ics-security-it-vs-ot
Ashford, W. (2019, April 5). Critical infrastructure under relentless cyber attack. Retrieved May 4, 2020, from computerweekly.com: https://www.computerweekly.com/news/252461202/Critical-infrastructure-under-relentless-cyber-attack
Bailes, A. J. (2007). Introduction: A World of Risk. In A. J. Bailes, SIPRI Yearbook 2007: Armaments, Disarmament, and International Security. Solna: Oxford University Press. Retrieved from https://www.sipri.org/sites/default/files/SIPRI%20Yearbook%202000.pdf
Berinato, S. (2002, March 15). Debunking the Threat to Water Utilities. Retrieved from CIO.com: https://www.cio.com/article/2440931/debunking-the-threat-to-water-utilities.html
Brunner, E. M., & Suter, M. (2010). INTERNATIONAL CIIP HANDBOOK 2008 / 2009. Zurich, Switzerland. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf
Check Point Software Technologies. (2020, July 22). Check Point Research: COVID-19 Pandemic Drives Criminal and Political Cyber-Attacks Across Networks, Cloud and Mobile in H1 2020. Retrieved from Check Point: https://www.checkpoint.com/press/2020/check-point-research-covid-19-pandemic-drives-criminal-and-political-cyber-attacks-across-networks-cloud-and-mobile-in-h1-2020/
CIPedia. (2020, January). Critical National Infrastructure. Retrieved May 4, 2020, from Fraunhofer: https://websites.fraunhofer.de/CIPedia/index.php/Critical_National_Infrastructure
Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017, September). The industrial control system cyber defence triage process. Computers & Security, 70, 467-481. doi:10.1016/j.cose.2017.07.009
Corradini, I. (2020). Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. Cham: Springer.
CREST. (2019). What is Cyber Threat Intelligence and how is it used? Retrieved May 21, 2020, from Crest: https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf
Davis, J. (2007, August 21). Hackers Take Down the Most Wired Country in Europe. Retrieved from Wired.com: https://www.wired.com/2007/08/ff-estonia/
Deloitte. (2020). The Impact of Cyber on “Critical Infrastructure” in the Next Normal. Deloitte. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/gx-deloitte-global-cyber-covid-19-critical-infrastructure-release-date-4.29.2020.pdf
Dragos Inc. (2017). CRASHOVERRIDE: Threat to the Electric Grid Operations. Dragos. Retrieved from https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf
Dragos Inc. (2017). TRISIS Malware: Analysis of Safety System Targeted Malware. Dragos. Retrieved from https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
Dragos Inc. (2020, June 18). EKANS Ransomware Misconceptions and Misunderstandings. Retrieved from Dragos: https://www.dragos.com/blog/industry-news/ekans-ransomware-misconceptions-and-misunderstandings/
Eddy, M., & Perlroth, N. (2020, September 18). Cyber Attack Suspected in German Woman’s Death. Retrieved from New York Times: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
Eric Luiijf, A. N. (2008). Empirical findings on critical infrastructure dependencies in Europe. International Workshop on Critical Information Infrastructures Security (pp. 302-310). Berlin: Springer.
Eriksson, J., & Giacomello, G. (2009). Who Controls the Internet? Beyond the. International Studies Review, 11, 205-230. doi:10.1111/j.1468-2486.2008.01841.x
FIRST. (2020). About FIRST. Retrieved from FIRST: https://www.first.org/about/
Gary, T. (2019, April 5). Cybersecurity Pros Face Significant Challenges with OT Security: Ponemon Report. Retrieved from Tenable: https://lookbook.tenable.com/ponemonotreport/ponemon-ot-report-blog
Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
Hilt, S., Huq, N., Kropotov, V., McArdle, R., Pernet, C., & Reyes, R. (2018). Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries. Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.pdf
IDC. (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Framingham: IDC. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS45213219
INTERPOL. (2020, August 4). INTERPOL. Retrieved from INTERPOL report shows alarming rate of cyberattacks during COVID-19: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
i-Scoop. (n.d.). Operational technology (OT) – definitions and differences with IT. Retrieved May 20, 2020, from i-Scoop: https://www.i-scoop.eu/industry-4-0/operational-technology-ot/
Lee, R. M. (2019, May 3). Two sides of IT vs. OT Security and ICS Security Operations. Retrieved May 18, 2020, from Dragos: https://www.dragos.com/blog/industry-news/two-sides-of-it-vs-ot-security-and-ics-security-operations/
Luiijf, E., Schie, T. v., Ruijven, T. v., & Huistra, A. (2016). The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. Global Forum on Cyber Expertise (GFCE). Retrieved from https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf
Maloney, P. (2019, October 25). Cybersecurity focus has shifted to critical infrastructure. Retrieved May 4, 2020, from American Public Power Association: https://www.publicpower.org/periodical/article/cybersecurity-focus-has-shifted-critical-infrastructure
Morgan, S. (2018). Cybersecurity Jobs Report. Herjavec Group. Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/11/HG-and-CV-Cybersecurity-Jobs-Report-2018.pdf
NIST. (2011). Information Security Continuous Monitoring for Federal Information Systems and Organizations. National Institute of Standards and Technology, Department of Commerce. NIST.

NIST. (2017). An Introduction to Information Security. doi:10.6028/NIST.SP.800-12r1
NIST. (2018). Cybersecurity Framework. NIST. Retrieved from https://www.nist.gov/cyberframework/framework
NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. doi:https://doi.org/10.6028/NIST.CSWP.04162018
OECD. (2019). Policies For The Protection of Critical Information Infrastructure - Ten Years Later. OECD. Retrieved from http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP/SPDE(2017)14/FINAL&docLanguage=En
Osborne, C. (2019, August 5). ZDNET. Retrieved from Cyberattacks against industrial targets have doubled over the last 6 months: https://www.zdnet.com/article/cyberattacks-against-industrial-targets-double-over-the-last-6-months/
Proofpoint. (2019). Human Factor Report 2019. Proofpoint. Retrieved from https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf
PWC. (2020). Managing the impact of COVID-19 on cyber security. Retrieved from https://www.pwc.com/my/en/assets/publications/2020/pwc-malaysia-impact-of-covid-19-on-cyber-security.pdf
Ramachandran, R. (2018). Envisioning the 2019 Cybersecurity Landscape. ISACA. Retrieved March 26, 2020, from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/envisioning-the-2019-cybersecurity-landscape
Reed, S. (2018, December 3). Which cyber threats do critical national infrastructure, defence and public organisations face most frequently? Retrieved May 20, 2020, from Nominet: https://nominetcyber.com/which-cyber-threats-do-critical-national-infrastructure-defence-and-public-organisations-face-most-frequently/
Roberto Setolaa, L. F. (2019, Spetember 30). An overview of Cyber Attack to Industrial Control System. Chemical Engineering Transactions, 77, 907-912. doi:10.3303/CET1977152
Rudner, M. (2013). Cyber-Threats to Critical NationalInfrastructure: An Intelligence Challenge. International Journal of Intelligence and Counter Intelligence, 26(3), 453-481. doi:10.1080/08850607.2013.780552
Schwab, K. (2018, November 5). Globalization 4.0 – what does it mean? Retrieved from World Economic Forum: https://www.weforum.org/agenda/2018/11/globalization-4-what-does-it-mean-how-it-will-benefit-everyone/
Schwab, W., & Poujol, M. (2018). The State of Industrial Cybersecurity 2018. Retrieved from https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf
Setola, R., Oliva, G., Assenza, G., & Faramondi, L. (2020). Cyber Threats for Operational Technologies. International Journal of System of Systems Engineering, 10(2). doi:10.1504/IJSSE.2020.10026809
Simmons, D. (2019, April 5). Cyber-attacks 'damage' national infrastructure. Retrieved May 4, 2020, from bbc.com: https://www.bbc.com/news/technology-47812479
Suter, M. (2007). A Generic National Framework For Critical Information Infrastructure Protection (CIIP). ETH Zurich , Center for Security Studies. Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
Tagle, P. (2019, January 25). Five Steps to Protect National Infrastructure. Retrieved May 22, 2020, from CSO: https://www.csoonline.com/article/3500649/five-steps-to-protect-national-infrastructure.html
Times of Israel. (2020, June 1). Iran cyberattack on Israel's water supply could have sickened hundreds – report. Retrieved from https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/
Toshiba. (2019, July 31). "The Front Lines of Cybersecurity" – Fending Off Hackers and Keeping Our Infrastructure Safe! Retrieved May 19, 2020, from Toshiba: https://www.toshiba-clip.com/en/detail/7338
Trend Micro. (2015). Report on Cybersecurity and Critical Infrastructure in the Americas. Retrieved from https://www.sites.oas.org/cyber/Documents/2015%20-%20OAS%20Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf
Trend Micro. (2019). Cybercrime and Exploits: Attacks on Unpatched Systems. Trend Micro. Retrieved May 25, 2020, from https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cybercrime-and-exploits-attacks-on-unpatched-systems
U.S. Department of State. (2019). A Guide to Critical Infrastructure Security and Resilience. U.S Department of Homeland Security. Retrieved May 22, 2020, from https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf
Weins, K. (2020, May 21). Cloud Computing Trends: 2020 State of the Cloud Report. Retrieved from Flexera: https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/
Wenger, A., Metzger, J., & Dunn, M. (2002). CIIP Handbook - An Inventory of Protection Policies in Eight Countries: Critical Information Infrastructure Protection. In A. Wenger, J. Metzger, & M. Dunn, CIIP Handbook - An Inventory of Protection Policies in Eight Countries: Critical Information Infrastructure Protection. Center for Security Studies and Conflict Research.
White House . (2018, February 15). Statement from the Press Secretary. Retrieved from White House: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/
World Economic Forum. (2020). The Global Risks Report 2020. Geneva: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
Zaballos, A. G., & Jeun, I. (2016). Best Practices for Critical Information Infrastructure Protection (CIIP) - Experiences from Latin America and the Caribbean and Selected Countries. Inter-American Development Bank, New York.

WELCHMAN KEEN

contact@welchmankeen.com

+65 6592 7634

10 Anson Rd, #27-15 International Plaza
Singapore 07990