ieema
your link to electricity

Smart Grid Division

Cyber Security Imperatives

for

INDIA's Electricity Infrastructure

A Comprehensive Study Report

IEEMA's initiative towards a resilient, sustainable and secure Electricity infrastructure

About IEEMA:

Indian Electrical & Electronics Manufacturers' Association (IEEMA) is an Apex Industry Association of the Indian electrical equipment, industrial electronics and allied equipment manufacturers – representing a combined turnover of $42 Billion. First ISO certified industry association in India, represents businesses encompassing the complete value chain in generation, transmission & distribution equipment. IEEMA has more than 900 members who have contributed to more than 90% of the power equipment installed in India. A platform for constructive interactions between Industry, Utilities and Policy Makers.

Acknowledgements:

IEEMA places on record its sincere thanks to, Mr. Deepak Pandey, Vice Chairman, IEEMA Smart Grid Division and Director, Business Operations GE-Digital India and Mr. N. Kishor Narang, Mentor & Principal Design Architect, Narnix Technolabs Pvt. Ltd. for developing and editing this White Paper and accompanying comprehensive Study Report. We also recognize the active support and contributions by Mr. Mayank Sharma, Schneider Electric, Mr. Rohit Sharma, Siemens Ltd, Mr. Amit Golhani, L&T Ltd, Mr. Anil Mehta, Secure Meters Ltd and the coordinating officer from IEEMA Mr. Akeel Khan for their contributions for the White Paper.

IEEMA further place on record the guidance and supervision of Mr. Sunil Singhvi, Chairman IEEMA Smart Grid Division and CEO, Secure Meters Ltd and Mr. Vikram Gandotra, Past Chairman IEEMA Smart Grid Division and General Manager Siemens Ltd for his inputs.

Disclaimer:

This report is the compilation of study, findings and views of the members of the Cybersecurity focused group in IEEMA Smart Grid Division. This paper has been prepared as a Study by the Members and to be considered as a guiding document only. The views/analysis expressed in this report/document do not necessarily reflect the official view of IEEMA. Efforts have been taken to ensure the accuracy and authenticity of the information presented in the report; however, IEEMA does not guarantee the accuracy of any data included in this publication, nor does it accept any responsibility for the consequences of its use.

FORWARD

IEEMA views Smart grid as an integral yet one of the most critical components of a nation-wide Integrated Smart Infrastructure. Thus, it believes that its architecture and the framework must not be considered or designed in isolation; rather it must form an integral part of the structured, Nation-wide Homogeneous Framework and architecture defined and harmonized to the finest granularity. It must take into consideration the implications of other concurrent infrastructures and/or services running for the consumers/stakeholders to optimize the Life Cycle (Total) cost of all the infrastructures for a given geographical territory.

To ensure a comprehensive and structured deployment of nation-wide smart grid infrastructure, it's Imperatives to address the current challenges like 'energy security', 'Electricity for all', and 'financial health of distribution utilities' along with 'Modernization of the Grid' in a holistic and sustainable manner.

IEEMA Smart Grid Division by virtue of its comprehensive members base covering the whole spectrum of the electricity infrastructure is uniquely positioned to support, advise and hand hold the government, utilities, policy makers, funding agencies and regulators in their endeavours to implement their restructuring, modernization and up gradation plans. IEEMA Smart Grid Division has taken upon itself to proactively support and enable the various government departments, ministries, utilities and other interested stakeholders to implement various relevant initiatives like National Smart Grid Mission (NSGM), National Mission for Enhanced Energy Efficiency (NMEEE), National and System Management (NSM) from IEC, National Electric Mobility Mission (NEMM).

To support the utilities and the government in their respective smart grid initiatives IEEMA Smart Grid division has formed Focus Groups in critical areas, which need immediate co-operation amongst the various stakeholders to enable realization of Smart Grid Vision and Roadmap of Ministry of Power. The goal is to reach out to all the direct and indirect stakeholders in various government departments, research and academic institutions, industry associations, regulators and standards developing organizations to have inclusive deliberations and actionable insights to resolving the various challenges being faced by all the stakeholders in their respective endeavours to make our nation 'smart green & secure'. Initial few Focus Groups:

- ⇨ Smart Grid Architecture and Framework FG
- ⇨ Smart Grid Interoperability, Standards and Harmonization FG
- ⇨ Cyber Security FG
- ⇨ Policy and Regulations FG

This report comprehensively covers challenges due to Cyber Security threats in Smart Grid landscape and suggest technical, commercial and process related action which can be taken to address the threat. The paper also explains references of Indian and International standards, Security controls that needs to be put in place, which can be further referred for adoption by Transmission and Distribution Grid Companies, Policy Makers, national security agencies and other entities concerned with Grid security and safety.

EXECUTIVE SUMMARY

Challenges that all economies are facing today in safeguarding the security and privacy of its ecosystem including citizen are - Transnational Nature of Cyber Crime, 'Cultural' Vulnerabilities, Internet Resilience and Threat Landscape.

The new paradigm of Smart Grid, Smart Building, Smart Home, Smart City, Smart Manufacturing already complicated by the 'Internet of Things' & Internet of 'Everything' made further complex by the Artificial Intelligence, Machine Learning Blockchain & Quantum Computing, make it truly complex to develop & embed comprehensive Security, Privacy and Trustworthiness attributes in the products, systems and solutions for any use case or application - be it consumer, commercial, industrial, automotive or strategic domains like critical infrastructure, defense and aerospace.

The recent evolution of disruptive technologies and digitalization compounded by the Covid 19, changing geopolitical situations and increasing cyber-attacks from not-so-friendly nations; bring a whole new set of challenges for the Security and Security Evaluation Methodologies for complex nature & architectures of Critical Infrastructures of the nation leveraging IT & Communication Networks evolving to meet these rising needs of the Society.

On one hand, we have the highly protected Networks for the 'Critical Information Infrastructures'; on the other hand, these very 'highly protected networks' need to give access to the consumers for Consumer Engagement and Participation in these Smart (Digital) Infrastructures to meet the true drivers of setting them up. These large Smart Networks are actually highly complex 'Systems of Systems' and "Networks of Networks', and thus create fresh challenges in the Security Paradigm and development of Protection Profiles.

Ransom demands have been growing larger with time. Tactics are becoming more cutthroat. Established criminal organizations are busy expanding their respective operations, and affiliates of the Ransomware-as-a-Service (RaaS) malware developers are adopting BGH attacks. Malware-as-a-Service (MaaS) developers have introduced ransomware modules. Banking trojans are continuing to be repurposed for Download-as-a-Service (DaaS) operations — a trend started to distribute malware families associated with BGH. Even targeted eCrime appears to be in a state of change, apparent by the recent activities of adversaries, notable for their high-volume spam campaigns and limited use of ransomware.

Analysis in recent years revealed a focus by some neighbourhood adversaries on the telecommunications sector, which could support both signals intelligence and further upstream targeting. Content related to defense, military and government organizations remains a popular lure for targeted intrusion campaigns.

India is among the top 10 countries facing cyber-attacks. There was an almost 56% rise in malicious traffic on internet during the lockdown period also on account of the culture of work from home. This might be just the beginning, which suggests even more increased interest in exploiting cyber breaches. While security teams are encouraged to strive to meet the BREAKOUT TIME metrics of the 1-10-60 rule: detecting threats within the first minute, understanding threats within 10 minutes, and responding within 60 minutes. However, the average breakout time for all observed intrusions rose from an average of 4 hours 37 minutes in 2018 to 9 hours in 2019.

The Smart Grid being the convergence of IT, Communication & Power Technologies, designed to cater to a nation's Integrated Energy Infrastructure requirements comprehensively, is a mission critical deployment needing the highest possible grade of security.

Widespread connection of distributed energy resources (DERs) (e.g., demand response, generation including from wind and solar, energy storage, electric vehicles and energy control devices) will increase digital complexity and attack surfaces, and therefore require more intensive cybersecurity protection. A multi-pronged approach to cybersecurity preparedness is required. System operators must have the capacity to operate, maintain, and recover a system that may never be fully protected from cyber- attacks.

Utilities purchase information, hardware, software, services, and more from third parties across the globe. And threat actors can introduce compromised components into a system or network, unintentionally or by design, at any point in the system's life cycle. This may be through software updates or "patches," which are downloaded frequently, or through firmware that can be manipulated to include malicious codes for exploitation at a later date. Adversaries may also compromise the hardware that utilities install in their operating systems.

The Contrast - It is easy to see why IT security and industrial control security are facing challenges when it comes to integration. These two Titans clash because at the lowest level the security considerations their entire design structures are based on, are at odds.

Blurring line between Cyber and Physical Attacks - This targeting of ICS, which has developed over a decade, is blurring the lines between cyber and physical attacks, prompting national security concerns in many countries. ICS attacks have evolved in scope and purpose across the globe. Attackers began by exploiting software developed for legitimate purposes, such as Shodan and Metasploit, to find components and devices connected to the internet, and to target supervisory control and data acquisition (SCADA) and other ICS software.

AI is a tool that can be used for offensive as well as defensive cybersecurity applications. Just as organizations can use artificial intelligence to enhance their security posture, cybercriminals may begin to use it to build smarter malware.

Key Cybersecurity Concepts Applicable to Electric Power Operations can be summed up as Resilience, Security by Design, the IT & OT interplay, Risk Assessment, Risk Mitigation & continuous update of Processes and Cyber Security Standards & Best Practices Guidelines. Security requirements and processes essentially comprise of Security Policy, Security Assessment, Security Deployment, Security Training and Security Audit (Monitoring).

Since, it is believed that Security will **ALWAYS** be breached at some time – there is no perfect security solution, Security Defense-in-Depth Concept strategy that provides multiple, redundant defensive measures in case a security control fails, or a vulnerability is quite effective. To ensure a secure environment, a strategy to protect the organization's cyber space is required for managing risks and boosting resilience. Organizations must build and implement a risk based cyber security policy with clear priorities, minimum ICT security baseline with threat and vulnerability information, build incident response capabilities and create awareness, educating and training opportunities.

We don't need to reinvent the wheel. We need a Cyber Risk Management Information System that has a user-friendly interface. It should integrate the best, most recent data from our own sources. It has to be a lean machine. At the same time, it should give us more transparency than we have today. Step by step, we can make the cyber risk MIS our own. The whole process takes less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the shelf solution.

The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure demand a top-down approach to standardization starting at the system or system-architecture rather than at the product level. Therefore, the systemic approach in standardization work can define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported. It promotes an increased co-operation with many other standards-developing organizations and relevant non-standards bodies needed on an international level. India needs to define and develop its own globally harmonized framework and architecture for the Electricity Infrastructure keeping in mind the new paradigm of Integrated Critical Infrastructure, where Smart Grid shall be one of the key (but not the only) component to meet the imperative of a 'smart, green and secure community'.

CEA is formulating a comprehensive strategy to address the cyber security issues that Power Sector faces. A National policy doctrine to address cyber security for national critical infrastructure and a regulatory framework that provides guidance to the industry players across generation, transmission and distribution - To review preparedness with respect to advisories on Cyber Security Framework and to vet self-assessment of gaps vis-à- vis baseline security & resilience requirement; To prepare the requirement for setting up of C-SIRT (eligibility criteria, scope of work etc.); To design and develop Cyber Security Policy (CSP) & Procedures along with CCMP; Security Policy and Management; Security Organization; Security Mandates for the Corporate IT Systems; Domain Specific security standards for Control Systems; Business Continuity Planning and Disaster Recovery; Customer Data Protection; Physical Security Requirements; Periodic Assessments and Reporting; Data Sharing and Collaboration…

Though government of India has put measures in place to check for any mal-intentioned bug or subcomponent in these equipment / systems, but these are not providing high level of assurance from intentional built in mechanism meant to compromise security of system. This is due to following reasons/constraints: Sheer volume of equipment and their subcomponents; Gaps of Standards; Gaps in Capacity Skill set in Utilities/DISCOMs and budget provisions… Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

THE WAY FORWARD for INDIA is to develop Internet Resilience for the nation. It is of utmost importance to ensure the security and resilience of the INTERNET within the country to enhance cyber security capabilities to better protect Indians and defend critical government and private sector systems. National Electricity Infrastructure - There is a need to develop Resilient, Secure and Trustworthy Grid which to a large extent is immune to cyber-attacks. Cyber Security - as the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace.

One of the proposed solutions could be that all utilities form a cyber division of experts & take ownership of complete security instead of relying on different vendors for their respective deliveries. Some of the issues that are critical for securing the Smart

Infrastructure are: Best Security Practices for Protecting Big Data; Approach to Address Security of data in Cloud and Standards for Emerging Technologies, Data Management - Minimum security assurance in Devices & systems; Mandatory certification of Devices before bringing it in market; Increase in numbers of testing labs; India specific protection profile of new devices coming up in emerging technologies…

Power systems are among the most complex and critical infrastructures of a modern digital society, serving as the backbone for its economic activities and security. It is therefore in the interest of every country to secure their operation against cyber risks and threats.

It is imperative to delve into the security, privacy & trustworthiness aspects and implications of the new paradigm of "Critical Information Infrastructure" and "Internet of Things" that the pervasive computing has enabled, thus raising new challenges for the 'IT & Communication Security' Development & Evaluation Eco-system. Hence, needing a new rigorous and vigorous effort in developing a "Comprehensive Cyber Security, Resilience & Trustworthiness" Strategy Framework encompassing all the critical domains and Stakeholders classifications and their respective imperatives from Cyber Security, Resilience & Trustworthiness Perspective.

Considering the current and future evolving Cyberthreat Landscape, it would be absolutely critical to have Two National Documents:

i. A concise yet comprehensive 'National Cyber Security Strategy' that sets clear, top-down directions to enhance the cyber resilience for the ecosystem that includes government, public and private sectors, the citizenry, and also addresses international cyber issues.
ii. A separate 'National Cyber Security Policy' based on principles laid down in the 'Strategy'. It must be outcome-based, practical and globally relevant, as well as based on risk assessment and understanding of cyberthreats and vulnerabilities. The security framework must include the compulsory testing of cyber products, infrastructure skill capacity development, responsibilities of entities and individuals, and public-private partnerships.

An accountable integrated national cybersecurity apparatus to be structured/ restructured and it must be provided clear mandates and be empowered adequately. It must be able to supervise and enforce policies across India, including policies regulated by independent regulators.

India needs its own National Charter of Trust to develop an ecosystem of Trustworthy vendors that Electricity Utilities and other Critical National Infrastructure agencies can TRUST absolutely by establishing the best practices in the domain of cyber security that are globally harmonized in Standards, Strategy, Innovation, Certification, Transparency and all other core characteristics required to build an absolutely TRUSTWORTHY ecosystem.

As per recommendations of Telecom Regulatory Authority of India (TRAI) in September 2017 National Trust Centre (NTC) must be set up without any further delay.

This NTC must be geared up to undertake the Security Testing and Evaluation comprehensively including but NOT limited to Devices, Systems, Networks, Application & System Softwares, Firmwares, Communication Stacks to ensure that the deployed Devices, systems and solutions are completely Trustworthy.

Improving cyber safety and resilience requires all stakeholders to act together at scale and in a coordinated way, including governments, the engineering professionals, operators of critical infrastructure and other systems, and developers of products and components. The evolving nature of the challenges will require continual responsiveness and agility by governments and other stakeholders.

The only approach would be to adopt top-down approach to standardization starting at the system or system-architecture rather than at the product level. We need to Study & Analyze the diverse Use Cases, Applications and corresponding Stakeholders & their respective requirements to understand their respective Characteristics and concerns. Develop a Granular Smart Grid Architecture followed by developing a Cyber Security Architecture mapping all the security, privacy, safety, resilience characteristics with the Granular Smart Grid Architecture.

It is evident that Cyber Security is a very complex paradigm, and with evolving new technologies, requirements and ever-increasing Attack Surface the vulnerabilities are rising many folds with time. In such a dynamic scenario, how do we develop a Cyber Security Strategy to make our Critical Infrastructure comprehensively Safe, Secure, Resilient and Trustworthy?

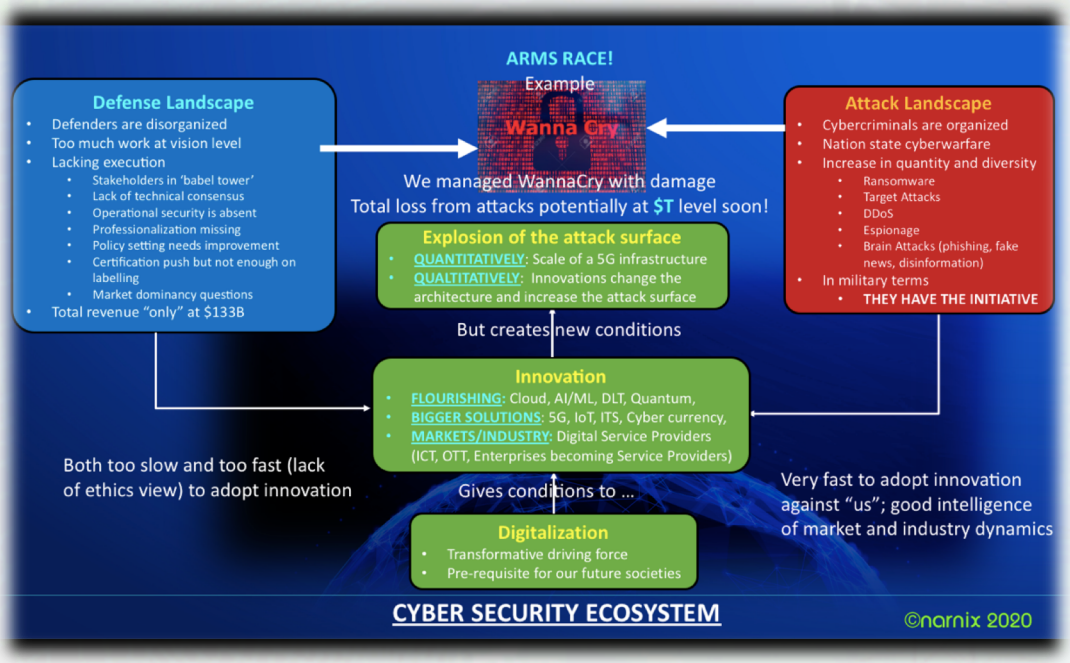
Table of Content

CONTEXT

Challenges that all economies are facing today in safeguarding the security and privacy of its ecosystem including citizen are - Transnational Nature of Cyber Crime, 'Cultural' Vulnerabilities, Internet Resilience and Threat Landscape.

The new paradigm of Smart Grid, Smart Home, Smart Building, Smart Manufacturing, Smart City already complicated by the 'Internet of Things' & Internet of 'Everything' made further complex by the Artificial Intelligence, Machine Learning, Blockchain & Quantum Computing, make it truly complex to develop and embed comprehensive Security, Privacy and Trustworthiness attributes in the products, systems and solutions for any use case or application - be it consumer, commercial, industrial, automotive or strategic domains like critical infrastructure, defense and aerospace.

The recent evolution of disruptive technologies and digitalization compounded by the Covid 19, changing geopolitical situations and increasing cyber-attacks from not-so-friendly nations; bring a whole new set of challenges for the Security and Security Evaluation Methodologies for complex nature & architectures of Critical Infrastructures of the nation leveraging the IT & Communication Networks evolving to meet these rising needs of the Society.



On one hand, we have the highly protected Networks for the 'Critical Information Infrastructures'; on the other hand, these very 'highly protected networks' need to give access to the consumers and citizens for Consumer/Citizen Engagement and Participation in these Smart (Digital) Infrastructures to meet the true drivers of setting them up. These large Smart Networks are actually highly complex 'Systems of Systems' and "Networks of

Networks', and thus create fresh challenges in the Security Paradigm and development of Protection Profiles.

International law defines Four Global Commons (natural assets outside national jurisdiction) which are the earth's natural resources i.e. the High Seas, the Atmosphere, Antarctica and Outer Space. Cyberspace is the 5th Global Common. It is also considered as the 5th Dimension beyond the 3 dimensions of Space & 4th dimension being the Time.

The imperatives of building a sustainable and secure planet have given rise to new paradigms like the green movement, DC power, renewables, microgrids, sustainable transportation, networking devices, network & cyber security, smart homes, smart buildings, smart grids and smart cities. All these shifting and rising paradigms are ultimately converging into the new & much larger paradigm of 'Sustainable and Trustworthy' Digital Infrastructure.

The power sector is one of the most frequently targeted and first to respond to cyber threats with mandatory controls. But threats continue to evolve, reaching into industrial control systems and supply chains, and requiring even greater efforts to manage risk. The network of power plants and lines connecting to homes and businesses is widely considered to be among the most critical infrastructure in the world. Power systems are among the most complex and critical infrastructures of a modern digital society, serving as the backbone for its economic activities and security. It is therefore in the interest of every country to secure their operation against cyber risks and threats.

The Indian Electricity Infrastructure is also going through a paradigm shift in the wake of Global Initiatives in the fields of Energy Security, Renewable Energies, Smart Grids, Energy Efficiency, Electric Mobility etc. in order to make our planet Earth Green and Sustainable. Electric utilities now find themselves making three classes of transformations:

- ⇨ Improvement of Infrastructure, also called the *Strong Grid*;
- ⇨ Addition of the digital layer, which is the essence of the *Smart Grid*; and
- ⇨ Business process transformation, necessary to capitalize on the investments in smart technology.

It must take into consideration the implications of other concurrent infrastructures and/or services running for the consumers/stakeholders to optimize the Life Cycle (Total) cost of all the infrastructures for a given geographical territory. To ensure a comprehensive and structured deployment of nationwide smart grid infrastructure, it's Imperative to address the current challenges like 'energy security', 'Electricity for all', and 'financial health of distribution utilities' along with 'Modernization of the Grid' in a holistic and sustainable manner.

India is among the top 10 countries facing cyber-attacks.

CYBERTHREAT LANDSCAPE

Those of us who have worked in cybersecurity for many years often start to think we've "seen it all". We haven't. Recent years have ushered in a host of new adversaries, new attack methods and new challenges for those of us in the cybersecurity industry.

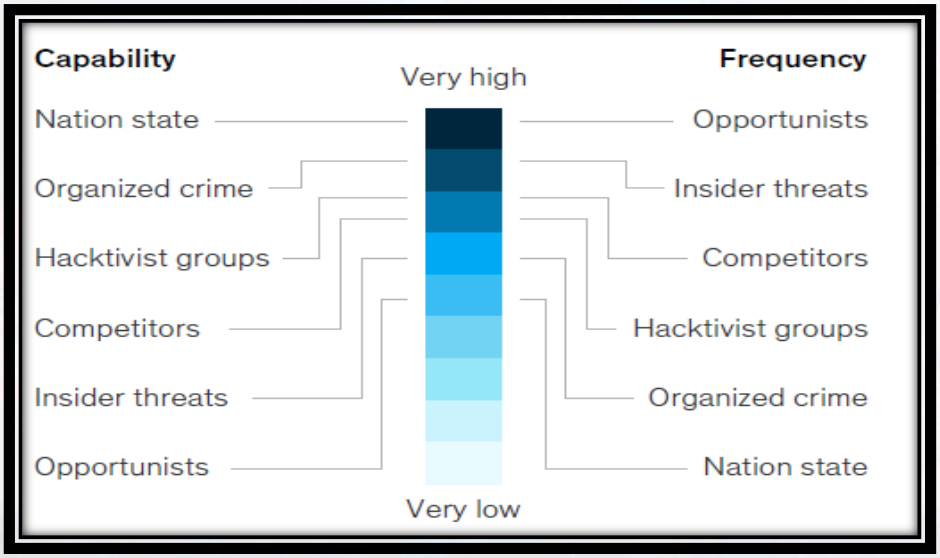
Challenges that all economies are facing today in safeguarding the security and privacy of its ecosystem including citizen are - Transnational Nature of Cyber Crime, 'Cultural' Vulnerabilities, Internet Resilience and Threat Landscape. The constituents that are responsible for the ever-evolving 'Threat Landscape' include (but not limited to) the following:

- ⇨ Confluence of Emerging Technologies
- ⇨ Quantum Computing and Quantum Key Distribution
- ⇨ Cyber Influence
- ⇨ Malwares & Ransomwares - Targeted Ransomwares
- ⇨ Mobile-focused Malware and Banking Trojans
- ⇨ Web Skimming Attacks
- ⇨ Supply Chain Attacks
- ⇨ Crypto mining and cloud-based Attacks
- ⇨ Weak Cyber Security Practices …

While criminals are relatively predictable in their tendency to always choose the path of least resistance, the activities of nation-states are frequently more relentless and sophisticated — and as a result, more challenging for cyber-defenders. In recent times, numerous adversaries specializing in the delivery or development of malware benefited from supporting customers or partners conducting BGH (Big Game Hunting) operations.

Disruption in recent years was not punctuated by a single destructive wiper; rather, it was plagued by sustained operations targeting the underpinnings of our society. Intelligence anticipated that big game hunting (BGH) — targeted, criminally motivated, enterprise-wide ransomware attacks — was expected to continue at least at the 2018 & 2019 pace. However, what was observed was not just a continuation but an escalation. Ransom demands have been growing larger with time. Tactics are becoming more cutthroat. Established criminal organizations are busy expanding their respective operations, and affiliates of the Ransomware-as-a-Service (RaaS) malware developers are adopting BGH (Big Game Hunting) attacks.

Numerous adversaries specializing in the delivery or development of malware benefited from supporting customers or partners conducting BGH operations. Malware-as-a-Service (MaaS) developers have introduced ransomware modules. Banking trojans are continuing to be repurposed for Download-as-a-Service (DaaS) operations — a trend started to distribute malware families associated with BGH. Even targeted eCrime appears to be in a state of change, apparent by the recent activities of adversaries, notable for their high-volume spam campaigns and limited use of ransomware.



McKinsey on Risk, November 2019

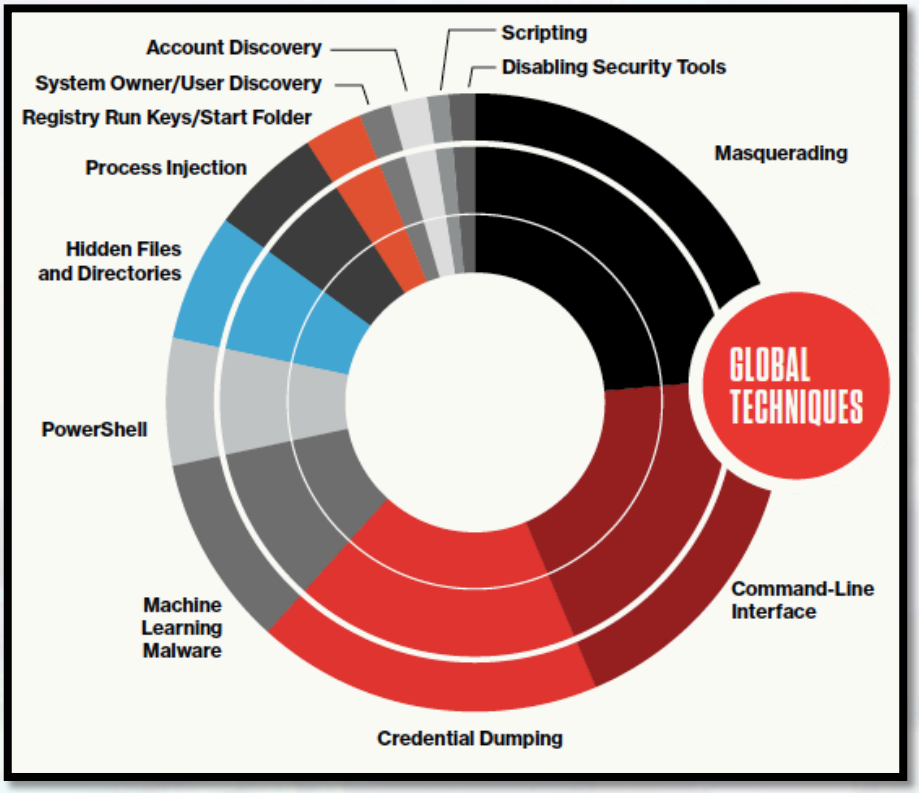
As in years past, the majority of state-sponsored targeted intrusions appeared to be motivated by traditional intelligence collection needs. Analysis in recent years revealed a focus by some neighbourhood adversaries on the telecommunications sector, which could support both signals intelligence and further upstream targeting. Content related to defense, military and government organizations remains a popular lure for targeted intrusion campaigns.

A structured analysis of the most significant events and trends in the recent years of cyber threat activity can demonstrate how threat intelligence and proactive hunting can provide a deeper understanding of the motives, objectives and activities of these actors — information that can empower swift proactive countermeasures to better defend your valuable data now and in the future. Before examining tactics and techniques observed from individual adversaries, it's instructive to take a broad view of the threat landscape and how it continues to shift over time. One useful lens is comparing the types of attacks that leverage malware and those that do not.

The new data points highlight a continuing trend in attack techniques that approximately 60% of attacks were Malware related. The trend toward Malware-Free Attacks is accelerating with these types of attacks surpassing the volume of Malware Attacks.

GLOBAL ATT&CK TECHNIQUE TRENDS: Moving past the initial intrusion vector, attackers employed a wide range of tactics and techniques in order to achieve their goal, whether that goal was financial gain, political advantage or disruption of services. The MITRE ATT&CK™ framework provides a very useful taxonomy of attackers' TTPs (Tactics, Techniques & Procedures) that we can use to catalogue observed behaviours in order to better understand methods in common use and how those methods have changed over time.

The MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) framework is an ambitious initiative that is working to bring clarity to how the industry talks about cyberattacks. It breaks intrusions into a series of 12 tactics that adversaries may employ, each with a number of different techniques that have been observed to be in use.



TTPs (Tactics, Techniques & Procedures) used by attackers in 2019 (www.crowdstrike.com)

A notable change in the most prevalent overall techniques used by attackers in 2019 was the significant increase in the use of "masquerading". This uptick can be explained by a rise in the use of the EternalBlue exploit in the wild. This is not necessarily indicative of a particular trend but instead highlights that this is still an active exploit in use by threat actors. (Masquerading occurs when the name or location of an executable, whether legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation).

The remaining techniques mirror those observed in previous years, with heavy reliance on hands-on-keyboard techniques (command-line interface, PowerShell), as well as, theft of credentials (credential dumping, valid accounts, account discovery) and defense evasion (masquerading, hidden files and directories, process injection). These techniques feature prominently in many sophisticated attacks, where a human adversary is engaged in the intrusion and is actively working toward an objective.

BREAKOUT TIME: Breakout time is important for defenders, as it sets up the parameters of the continuous race between attackers and defenders. By responding within the breakout time window, which is measured in hours, defenders are able to minimize the cost incurred and damage done by attackers.

BREAKOUT TIME:

Security teams are encouraged to strive to meet the metrics of the 1-10-60 rule: detecting threats within the first minute, understanding threats within 10 minutes, and responding within 60 minutes. However, the average breakout time for all observed intrusions rose from an average of 4 hours 37 minutes in 2018 to 9 hours in 2019.

This key cybersecurity metric measures the speed from an adversary's initial intrusion into an environment, to when they achieve lateral movement across the victim's network toward their ultimate objective. Security teams are encouraged to strive to meet the metrics of the 1-10-60 rule: detecting threats within the first minute, understanding threats within 10 minutes, and responding within 60 minutes.

This year, the average breakout time for all observed intrusions rose from an average of 4 hours 37 minutes in 2018 to 9 hours in 2019. This increase reflects the dramatic rise in observed eCrime attacks, which tend to have significantly longer breakout times compared with nation-state adversaries. It's important to note that defenders should still focus on speed, as data attributable to nation-state activities recently does not suggest any major changes in breakout times among state affiliated adversaries.

India is among the top 10 countries facing cyber-attacks. These incidents have increased manifold during the lockdown period — almost three times increase in cases of phishing, spamming and scanning of ICT systems, particularly of critical information infrastructure.

There is significant increase in incidents relating to hacking, injecting malware through spam mails and other forms of exploiting vulnerabilities.

There was an almost 56% rise in malicious traffic on internet during the COVID-19 lockdown period also on account of the culture of work from home. This might be just the beginning, which suggests even more increased interest in exploiting cyber breaches.

A news daily too reported massive "denial of service" attacks on financial institution in the country which, however, could not be verified. The border stand-off has further increased worries about enhanced cyber-attacks from the bordering rogue nation and its close allies. Several advisories have been published by the Indian Computer Emergency Team and media about possibilities of cyber-attacks from China.

Many cyber hackers — state, non-state, professional, freelancer's groups, so-called "anonymous groups" — operate worldwide and conduct attacks internationally. Approximately more than one third of all cyber-attacks worldwide are launched from unfriendly nations. These countries have been accused of perpetrating state-sponsored attacks for a variety of purposes.

Recently, the Australian Prime Minister expressed concerns over Chinese cyber-attacks. About 38% of Advance Persistent Threat Vectors like APT40, APT3, APT10 and APT17 have been reported to be developed and deployed by China for espionage, stealing of data and IP. Some APTs are general purpose tools but others are customised for specific countries and purposes.

The techniques and tools like APT1, APT3, APT10, APT15, APT17, APT26 etc. have been deployed against India too. The rogue nations are in the process of developing technology to penetrate the internet through satellite channels. Under the influence by rogue nations, our bordering country too has deployed APT 36 targeting Indian entities. The role of hacker group called LAZARUS is well known in carrying out attacks on financial targets in India, Bangladesh and other South Asian countries.

"The current situation is very tricky. We do not have the facts to decide on actions. This paralysis puts our critical infrastructure at risk."

CYBERTHREAT for GRID

The Smart Grid being the convergence of IT, Communication & Power Technologies, designed to cater to a nation's Integrated Energy Infrastructure requirements comprehensively, is a mission critical deployment needing the highest possible grade of security. This is because, once these Smart Grid Deployments are complete, you shall not need to possess nuclear weapons to bring a Nation Down, but would simply need a bunch of good Hackers who could penetrate thru the Smart Grid network of a nation and shut down the power to the nation.

With utilities around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyber-attacks on the electric grid continue to grow in frequency and sophistication. The potential for malicious actors to access and adversely affect physical electricity assets of electricity generation, transmission, or distribution systems via cyber means is a primary concern for utilities.

Widespread connection of distributed energy resources (DERs) (e.g., demand response, generation including from wind and solar, energy storage, electric vehicles and energy control devices) will increase digital complexity and attack surfaces, and therefore require more intensive cybersecurity protection. A multi-pronged approach to cybersecurity preparedness is required. System operators must have the capacity to operate, maintain, and recover a system that may never be fully protected from cyber- attacks.

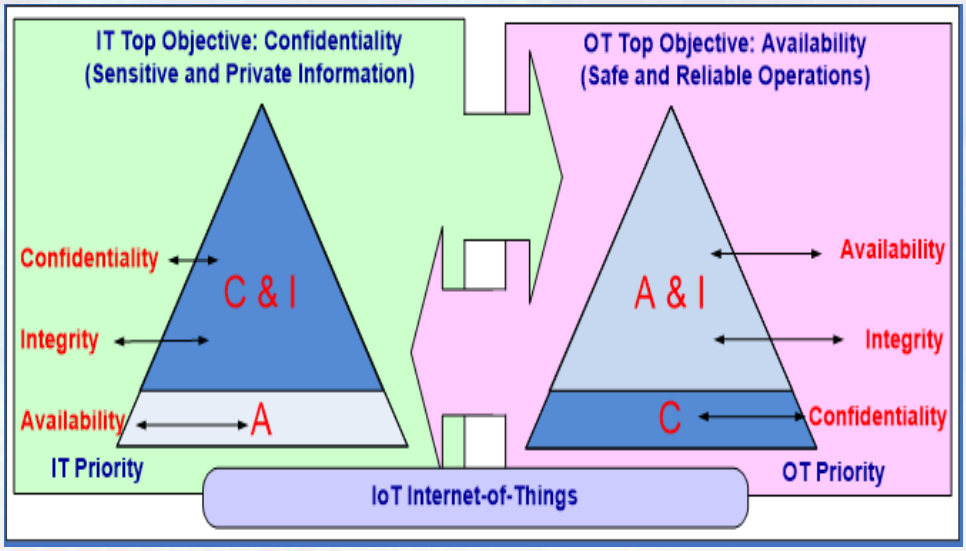
Utilities used to consider cyber risk in terms of the vulnerability of either IT systems - meaning software, hardware, and technologies that process data and other information, or *Operational Technology*(OT) systems - meaning software, hardware, and technologies that help monitor and control physical devices, assets, and processes, including the ICS (Industrial Control Systems). In recent years, however, the two systems have been converging as companies digitize and build the power sector's version of the Industrial Internet of Things, including the "Smart Grid". And, as challenging as it may be for utilities to identify their own critical assets and protect them, the challenge seems to be expanding exponentially, since today's interconnected world also requires them to secure vast, far-flung, and increasingly complex global supply chains.

The Contrast

It is easy to see why IT security and industrial control security are facing challenges when it comes to integration. These two Titans clash because at the lowest level the security considerations their entire design structures are based on, are at odds:

- ⇨ IT industry has been developed around the asynchronous behavior of humans, while industrial controls require a synchronous component to communications.
- ⇨ Control systems' primary concern for security is operational availability while providing highly accountable authentication of devices. The primary concern for IT systems is to separate, secure and provide authenticated access for each user to their data.
- ⇨ IT systems are based around storage and access to user's data, while embedded systems and control networks for the most part do not require so much data storage.
- ⇨ Many control system networks operate independent of users, thus the user-to-data authentication required for IT systems is less relevant.

- Control systems rely on a high accountability that control commands are authentic and the communicating systems are trusted, while IT systems rely on a trusted environmental perimeter and assume the machine's physical boundary is an extension of the user and thus is uncompromised.
- Exploiting simple control system operating software, and root secrets is often very trivial and becomes a target because of its perceived minimal size and easy access to root code through built in debug ports.
- IT systems run on virtual machines and allow anonymous systems to implement secure transactions between Application Softwares. Virtual machines, anonymous communications, and untrusted systems are the nemesis of highly accountable authentication and the system trust required for control networks.
- Finally, the IT paradigm expects to follow Moore's law and have twice the system resources for the same cost with each upgrade cycle. However, control networks enable business systems to be more efficient; their designers strive to provide long life expectancy and attempt to reduce cost while increasing the number of control devices on a network with each design cycle.



The Contrast - It is easy to see why IT security and industrial control security are facing challenges when it comes to integration. These two Titans clash because at the lowest level the security considerations their entire design structures are based on, are at odds.

Bridging the Gap

The two industries being contrasted are very large and have developed with such a degree of separation that often the terminology between the two is not the same.

In many cases, security for industrial controls has not developed to nearly the same level as in the IT industry. Since the IT security industry is noticeably much more defined, many IT-related security leaders have brought mature solutions to market attempting to push the same solutions directly into industrial controls/embedded systems environments. While

some of these have had success, in general they have missed the defining concepts they will need to address the gap between the security bases of the two industries.

In order to create a robust encompassing security basis to cover both IT and Industrial Controls, the root cause must be addressed. The security basis for each type of network must be addressed by a method, which combines the base security needs of both types of networks.

Blurring line between Cyber and Physical Attacks

In another unsettling but growing trend, cyber attackers are increasingly targeting industrial control systems (ICS), sometimes potentially laying the groundwork to do physical damage to the grid. Previously, attackers primarily targeted utilities' information technology (IT) systems to steal data or launch ransomware for financial gain. The threat is now becoming even more insidious, with reports of hackers tied to nation-states and organized crime trying to burrow their way into utility ICS, seeking to learn how systems operate, and positioning themselves to control critical physical assets, such as power plants, substations, transmission, and distribution networks, and to potentially disrupt or destroy them.

This targeting of ICS, which has developed over a decade, is blurring the lines between cyber- and physical attacks, prompting national security concerns in many countries. ICS attacks have evolved in scope and purpose across the globe. Attackers began by exploiting software developed for legitimate purposes, such as Shodan and Metasploit, to find components and devices connected to the internet, and to target supervisory control and data acquisition (SCADA) and other ICS software. A common thread is that all of these attacks are either known or suspected to have been carried out or supported by nation-states to further political goals, and such activity appears to be on the rise. There are innumerable examples of attacks on the critical infrastructures of nations right from Aurora (2007), Shodan (2009), Stuxnet (2010), Metasploit (2010), Shamoon (2012), BlackEnergy (2016), Shamoon 2 (2017) to Trisis/Triton (2017) - a particularly disturbing ICS-targeted attack that penetrated the safety systems of a Saudi petrochemical plant. Investigation revealed that the attack, which was foiled only by a bug in the computer code, was likely intended to cause an explosion that could have killed and injured people.

A few Challenges in Smart Grid Security

- Pervasive digitization of the grid (without designing security into the products)
  - Smart Meters
  - Digital Relays/Intelligent Electronic Devices (IEDs)
  - Phasor Measurement Units (PMUs)
- Proprietary and legacy Systems – lack of updates
- Lack of clear patch management policy for power system equipment
- Devices in remote (insecure) locations
- Supply chain contamination (including AMC personnel)
- Different National / State / Local regulatory authorities
- Extensive communication without properly enforced security policies could result in attacks/faults cascading from one part of the system to other
- Rapidly emerging threats (days/weeks) versus power system lifecycle (decades)
- Lack of security awareness & expertise among utilities.

Risks with AI and Machine Learning

The processing speed of smart grid devices, coupled with the use of AI systems, also presents a potential cybersecurity vulnerability. AI systems learn from experience, and some observers say that these systems may be of limited use in cybersecurity defenses. Machine learning decisions are made based on the data the machine learning is trained and tested on. Machine learning is also subject to bias inherent in the data used to train the machines, as the coding reflects the preconceptions of the coding's programmers.

AI systems are typically only as good as the data on which they are trained. They crystallize any biases or falsehoods found in their training data. The application of AI to surveillance or cybersecurity for national security opens a new attack vector based on this data diet vulnerability. Adversaries may learn how to systematically feed disinformation to AI surveillance systems, essentially creating an unwitting automated double agent.

Thus, the bias of the programming can restrict how the machine learning addresses a situation. However, AI is a tool that can be used for offensive as well as defensive cybersecurity applications.

The next generation of situation-aware malware will use AI to behave like a human attacker: performing reconnaissance, identifying targets, choosing methods of attack, and intelligently evading detection. Just as organizations can use artificial intelligence to enhance their security posture, cybercriminals may begin to use it to build smarter malware.

Adversaries may discover how to use AI to stage future attacks on the grid, designed to disguise the intrusion and then overwhelm defenses.

One factor restricting intelligence in malware is the need for small malware payloads to prevent detection… But it is conceivable that future developments in swarm or distributed AI may result in strategic botnets with small malware payloads but devastating effects.

Purchase, Upgrades & Patches:

Utilities purchase information, hardware, software, services, and more from third parties across the globe. And threat actors can introduce compromised components into a system or network, unintentionally or by design, at any point in the system's life cycle. This may be through software updates or "patches," which are downloaded frequently, or through firmware that can be manipulated to include malicious codes for exploitation at a later date. Adversaries may also compromise the hardware that utilities install in their operating systems.

Human Factor in Cybersecurity

Many cybersecurity breaches are caused by individuals falling prey to phishing or similar attacks which are used to gain credentials to access utility systems. The human factor is thus considered by many to be the weakest link in cybersecurity. This was the case in Ukraine, as hackers sent out malware-carrying emails. After links in the emails were opened by legitimate users, hackers acquired the credentials needed to access control and operations systems to cause blackouts at regional distribution utilities. Development and deployment of better tools to secure the human interface could potentially reduce

cybersecurity threats via email systems, in particular. In the meantime, targeted phishing attacks are reported to be increasing.

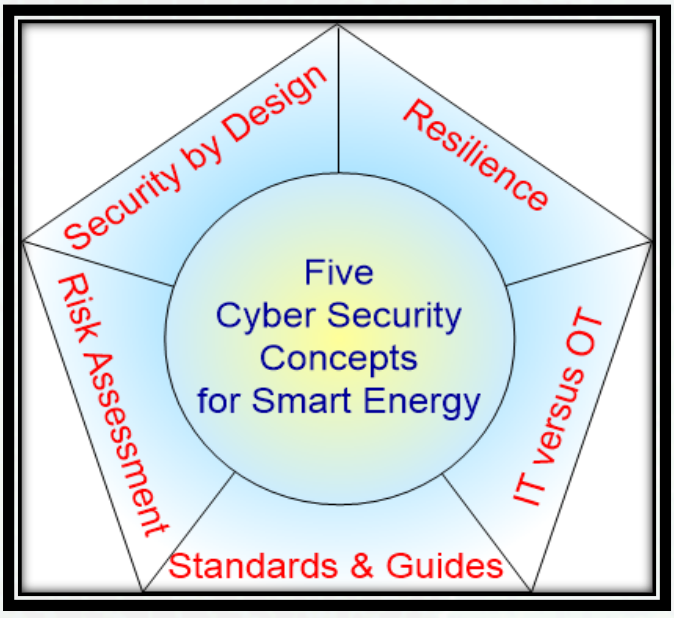
THE FIRST LINE OF DEFENSE IS THE EMPLOYEES THEMSELVES

CYBER SECURITY CONCEPTS FOR SMART GRID

With the introduction of digital smart grid technologies to enhance and modernize grid operations, the speed and processing power of microprocessor-based ICS networks enhances the efficiency and control of power production and flows across electricity transmission and distribution systems. While the benefits to the electric power system and its users are many, there are potential risks, as many IT and OT systems are connected to the internet to improve data collection and information sharing. However, this exposure to the internet leads to increased cybersecurity risks.

Key Cybersecurity Concepts applicable to Electric Power Operations

- Concept #1: Resilience should be the overall strategy for ensuring business continuity: When focusing on resilience in general, organizations must consider safety, security, and reliability of the processes and the delivery of their services. Resilience includes security measures that can mitigate impacts, not only before incidents (identify & prevent), but also during such incidents (detect & respond) and after incidents have been resolved (recover).
- Concept #2: Security by Design is the most cost-effective approach to security: Security is vital for all critical infrastructures and should be designed into systems and operations from the beginning, rather than being applied after the systems have been implemented.
- Concept #3: IT and OT are similar but different: Technologies in Operational environments (called OT) have many differing security constraints and requirements from Informational Technologies (IT) environments.
- Concept #4: Risk assessment, risk mitigation, and continuous update of processes are fundamental to improving security: Based on an organization's business requirements, its security risk exposure must be determined (human safety, physical, functional, environmental, financial, societal, reputational) for all its business processes.
- Concept #5: Cyber security standards and best practice guidelines for energy OT environments should be used to support the risk management process and establish security programs and policies: at the right time.



Security Requirements for Utility Operation: Security Processes

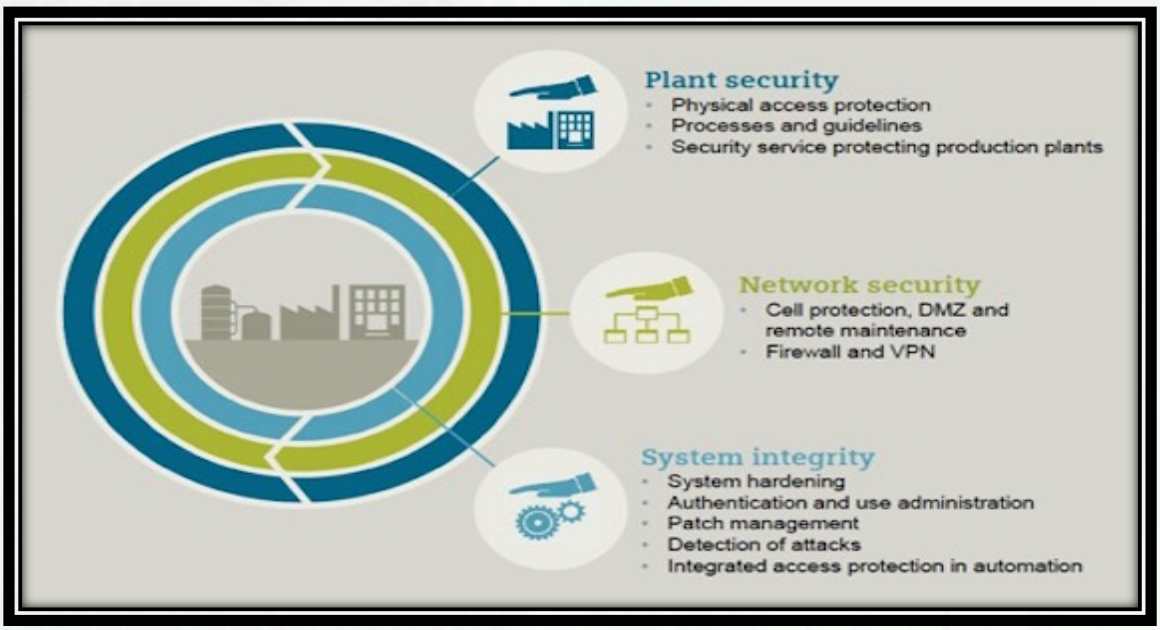
- Security Policy,
- Security Assessment,
- Security Deployment,
- Security Training and
- Security Audit (Monitoring).

Security Requirements for Utility Operations: Security Process

- Security Policy – Security policy generation is the process of creating policies on managing, implementing, and deploying security within a security domain. The recommendations produced by security assessment are reviewed, and policies are developed to ensure that the security recommendations are implemented and maintained over time.
- Security Assessment – Security assessment (risk assessment) is the process of assessing assets for their security requirements, based on probable risks of attack, liability related to successful attacks, and costs for ameliorating the risks and liabilities. The recommendations stemming from the security requirements analysis leads to the creation of security policies, implementation of security procedures, and the deployment of security technologies: products and services.
- Security Deployment – Security deployment is a combination of purchasing and installing security products and services as well as the implementation of the security policies and procedures developed during the security policy process.
- Security Training – Continuous training on security threats, security technologies, corporate and legal policies that impact security, Security measures analysis (which is a periodic activity), and best practices is needed. It is this training in the security process that will allow the security infrastructure to evolve and stay relevant with changing Threat Landscape.
- Security Audit (Monitoring) – Security audit is the process responsible for the detection of security attacks, detection of security breaches, and the performance assessment of the installed security infrastructure. However, the concept of an audit is typically applied to post-event/incursion.

Security Defense-in-Depth Concept

Security will ALWAYS be breached at some time – there is no perfect security solution.



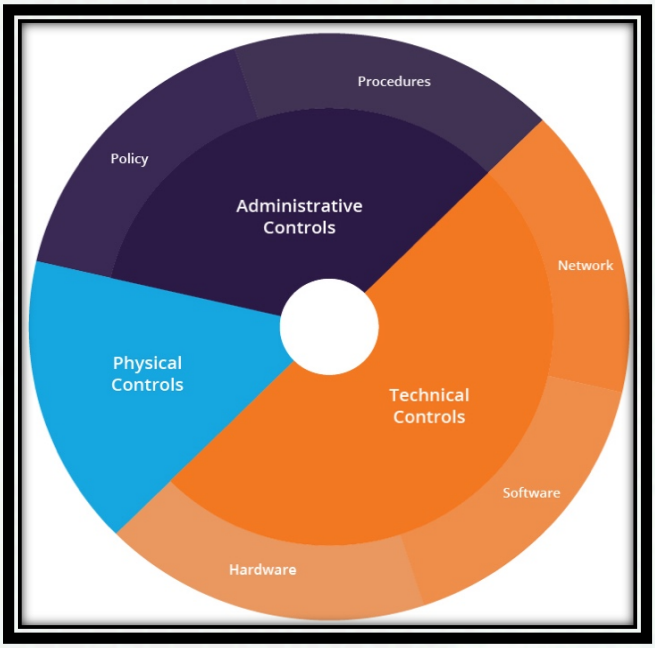
Defense-in-Depth is an information assurance strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is

exploited. Defense-in-depth cybersecurity use cases include end-user security, product design and network security. A defence-in-depth security architecture is based on the idea that any one point of protection can, and probably will, be defeated. It implies layers of security and detection, even on single systems. Deterrence and delay, to try to avoid attacks or at least delay them long enough for counter actions to be undertaken. This security is implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response. This is the primary defense but should not be viewed as the only defense. Detection of attacks, primarily those that were not deterred, but could include attempts at attacks. Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Intrusion detection capabilities can play a large role in this effort. Assessment of attacks, to determine the nature and severity of the attack. For instance, is the entry of a number of wrong passwords just someone forgetting or is it a deliberate attempt by an attacker to guess some likely passwords? Communication and notification, so that the appropriate authorities and/or computer systems can be made aware of the security attack in a timely manner. Network and system management can play a large role in this effort. Response to attacks, which includes actions by the appropriate authorities and computer systems to mitigate the effect of the attack in a timely manner. This response can then deter or delay a subsequent attack.

Security Defense-in-Depth Concept

Since, it is believed that Security will ALWAYS be breached at some time – there is no perfect security solution. Security Defense-in-Depth is an information assurance strategy that provides multiple, redundant defensive measures in case a security control fails, or a vulnerability is quite effective.

7 Layers of Security



7 Layers of Security

Information Security Policies. These policies are the foundation of the security and well-being of our resources:

- ⇨ Physical Security;
- ⇨ Secure Networks and Systems;
- ⇨ Vulnerability Programs;
- ⇨ Strong Access Control Measures;
- ⇨ Protect and Backup Data;
- ⇨ Monitor and Test Your Systems.

Cybersecurity Requirements for Communication Protocols

The first five rely primarily on cryptography and require key management methods, while availability may rely more on engineering strategies and other non-cryptographic methods.

1. Authentication of the systems, devices, and applications that are sending and receiving data - Generally, the most important security requirement for power system operations and every interaction should ensure both the sender and receiver are authenticated.
2. Authorization for interactions such as viewing, reading, writing, controlling, creating, deleting - Access Control Lists (ACL) in routers and gateways and Role-Based Access Control (RBAC) for applications and databases.
3. Data integrity of all interactions and of information within the systems - Data integrity of messages usually implies detecting tampering since it is not possible to prevent messages from being destroyed or modified, but it is possible to detect these actions. Hashing using cryptographic keys is the most common method to detect tampering
4. Accountability / Non-repudiation ensures that some entity cannot deny having received or acted upon a message - Often necessary for interactions linked to contractual requirements. Digital signatures using cryptographic keys are a common method for providing non-repudiation.
5. Confidentiality is usually required for financial, market, corporate, or private data - Usually not necessary for normal power system operational data exchanges. Encryption of messages with cryptographic keys is required to avoid eavesdropping.
6. Availability of the interactions can range from milliseconds to hours or days - Unlike the other cyber security requirements, availability generally relies on engineering design, configuration management, redundancy, functional analysis, communication network analysis, and engineering practices.

Cybersecurity Requirements for Communication Protocols

- ⇨ Authentication
- ⇨ Authorization
- ⇨ Data Integrity
- ⇨ Accountability/ Non-repudiation
- ⇨ Confidentiality
- ⇨ Availability.

Data Analytics

Electric utilities are collecting massive amounts of data from ICS networks and customer-information systems. Generally, this accumulation is referred to as "big data". Big data refers to the growth in the volume of structured and unstructured data, the speed at which it is created and collected, and the scope of how many data points are covered. Big data often comes from multiple sources and arrives in multiple formats.

Using data analytic techniques, big data can be turned into useful information. High-performance computing can take advantage of fast processing to examine data sets collected from smart grid systems into operational information, providing insights into

customer behaviour. It can also be used to recognize (or potentially predict) patterns or trends in data of new physical or cybersecurity threats to the grid.

Artificial Intelligence for Cybersecurity

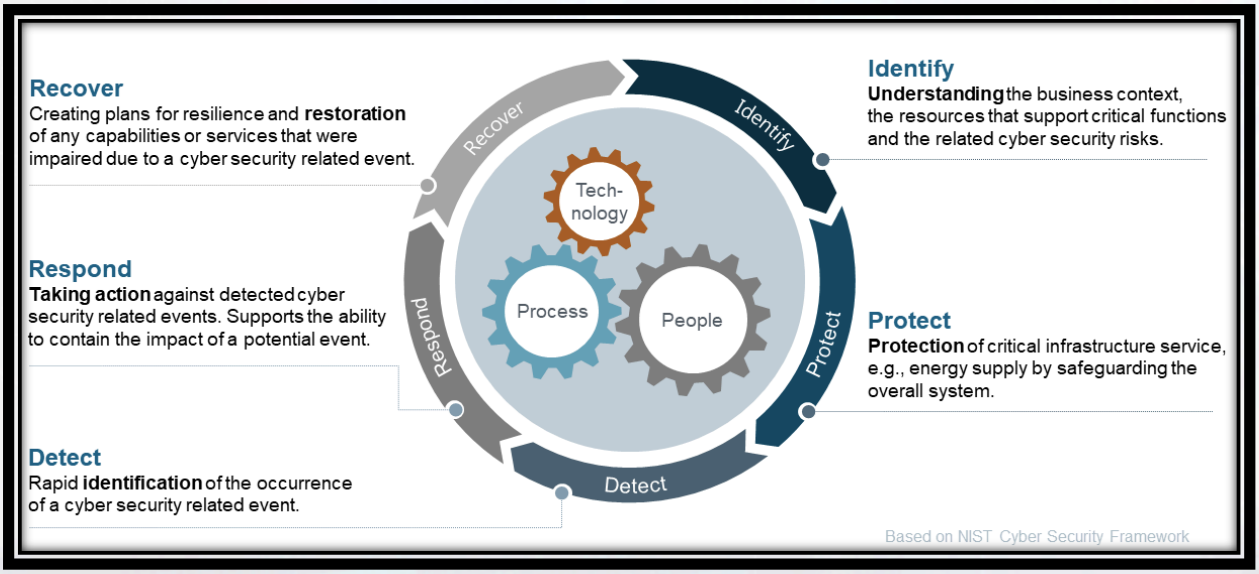
Artificial Intelligence (AI) is one of the technologies being deployed to mitigate cybersecurity risks. AI is a combination of computational technologies, machines, and software which have the capability to learn from inputs and be self-directed. AI allows computer systems to simulate human learning and problem solving.

Artificial intelligence algorithms are designed to make decisions, often using real-time data. They are unlike passive machines that are capable only of mechanical or predetermined responses. Using sensors, digital data, or remote inputs, they combine information from a variety of different sources, analyze the material instantly, and act on the insights derived from those data. With massive improvements in storage systems, processing speeds, and analytic techniques, they are capable of tremendous sophistication in analysis and decision making.

The speed of processing of AI systems is currently seen as providing protection for ICS and other networks that human operators may not be able to match, especially as cyber-attackers are employing increasingly sophisticated methodologies.

One form of AI is machine learning—algorithms based on statistical techniques—which gives computer systems the ability to learn from a set of situations and make decisions based upon alternative scenarios in reaction to those situations rather than from programmer instructions. The algorithms also adapt in response to new data and experiences to improve efficacy over time. Under these circumstances, AI can potentially respond to a cyberattack scenario far more quickly than a human decisionmaker.

The speed of processing of AI systems is currently seen as providing protection for ICS and other networks that human operators may not be able to match, especially as cyber-attackers are employing increasingly sophisticated methodologies. AI can potentially respond to a cyberattack scenario far more quickly than a human decisionmaker.



security management cycle for an organization

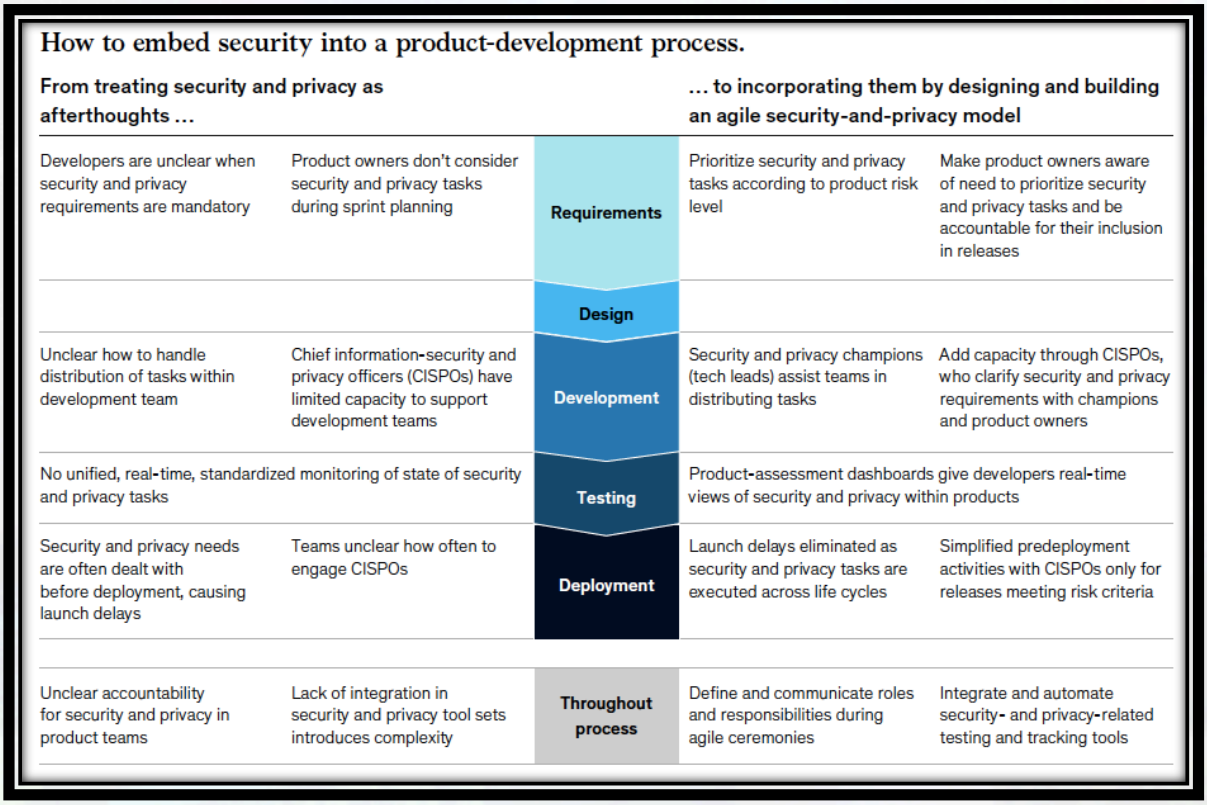
CHAIN IS AS STRONG AS THE WEAKEST LINK

Smart Meters

Networked embedded equipment, like Smart Energy Meters and Controllers found throughout the Smart Energy Grid need to be protected from a variety of security threats to avoid the possibility of significant financial losses due.

Side-Channel Analysis is one of the most sophisticated forms of attack on cryptographic systems that uses information that leaks, unintentionally, from the real-world implementations of cryptographic hardware. For example, an attack might examine the characteristics of a cryptographic device when a variety of security keys are presented. Measurements and analysis of the power use (called Differential Power Analysis, or DPA), timing responses or electromagnetic radiation given off could provide clues as to the nature of the protected keys used within the hardware.

Possible solutions - Tamper Resistant secure MCU, Secure element, Secure library (Crypto Library + Secure Storage)



How to embed security into a product-development process.

From treating security and privacy as afterthoughts …			… to incorporating them by designing and building an agile security-and-privacy model	
Developers are unclear when security and privacy requirements are mandatory	Product owners don't consider security and privacy tasks during sprint planning	Requirements	Prioritize security and privacy tasks according to product risk level	Make product owners aware of need to prioritize security and privacy tasks and be accountable for their inclusion in releases
		Design		
Unclear how to handle distribution of tasks within development team	Chief information-security and privacy officers (CISPOs) have limited capacity to support development teams	Development	Security and privacy champions (tech leads) assist teams in distributing tasks	Add capacity through CISPOs, who clarify security and privacy requirements with champions and product owners
No unified, real-time, standardized monitoring of state of security and privacy tasks		Testing	Product-assessment dashboards give developers real-time views of security and privacy within products	
Security and privacy needs are often dealt with before deployment, causing launch delays	Teams unclear how often to engage CISPOs	Deployment	Launch delays eliminated as security and privacy tasks are executed across life cycles	Simplified predeployment activities with CISPOs only for releases meeting risk criteria
Unclear accountability for security and privacy in product teams	Lack of integration in security and privacy tool sets introduces complexity	Throughout process	Define and communicate roles and responsibilities during agile ceremonies	Integrate and automate security- and privacy-related testing and tracking tools

Enhancing the Threat/Risk Assessment

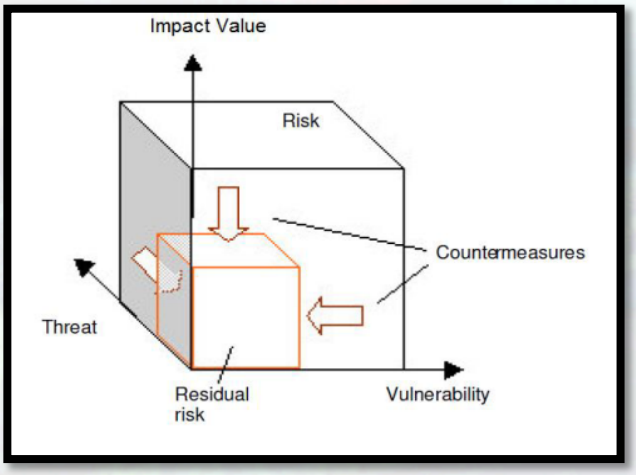
Many cybersecurity actions are reactive to the last threat discovered. While intrusion detection is considered a priority, some experts say that mitigation of cyber threats requires a focus on attackers, not the attacks, to address their motivations (e.g. - to extort money or to cause damage). Others might differ, saying that the focus should be on the attack and the system vulnerability exploited. Some utilities are undertaking security improvements in modernization programs, while other improvements would potentially have to be undertaken as special projects because of limitations for cost recovery under traditional cost-of-service ratemaking regulations under state government jurisdiction. In such instances, the improvements may have to be justified as "used or useful" in providing electricity service to customers in utility rate cases.

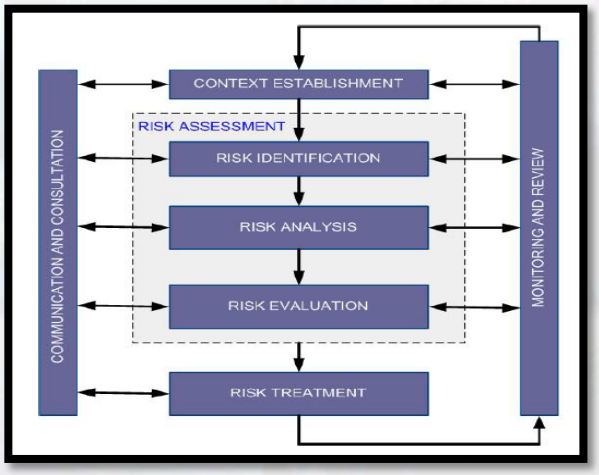
Very often, the relative level of sophistication of the threat is related to the origin of the threat. Since many cyberthreats appear to originate from foreign entities (including some with nation state affinities), intelligence on the existence and nature of the threat, as well as the capability of dealing with the threat, often relies on the federal government's national security apparatus. Therefore, the information communicated from the government is generally more useful when it is both timely and relevant as to the severity of a threat and communicates whether a need exists for immediate action. The electricity industry then provides the expertise necessary for understanding the relative risk to the grid of the potential threat, and the appropriate avenues for communicating the threat information.

Risk Assessment and Risk Management of Cyber-Physical Systems: Risk-Based Cyber Security

In the power sector, cyber space security is the protection of data, systems, and

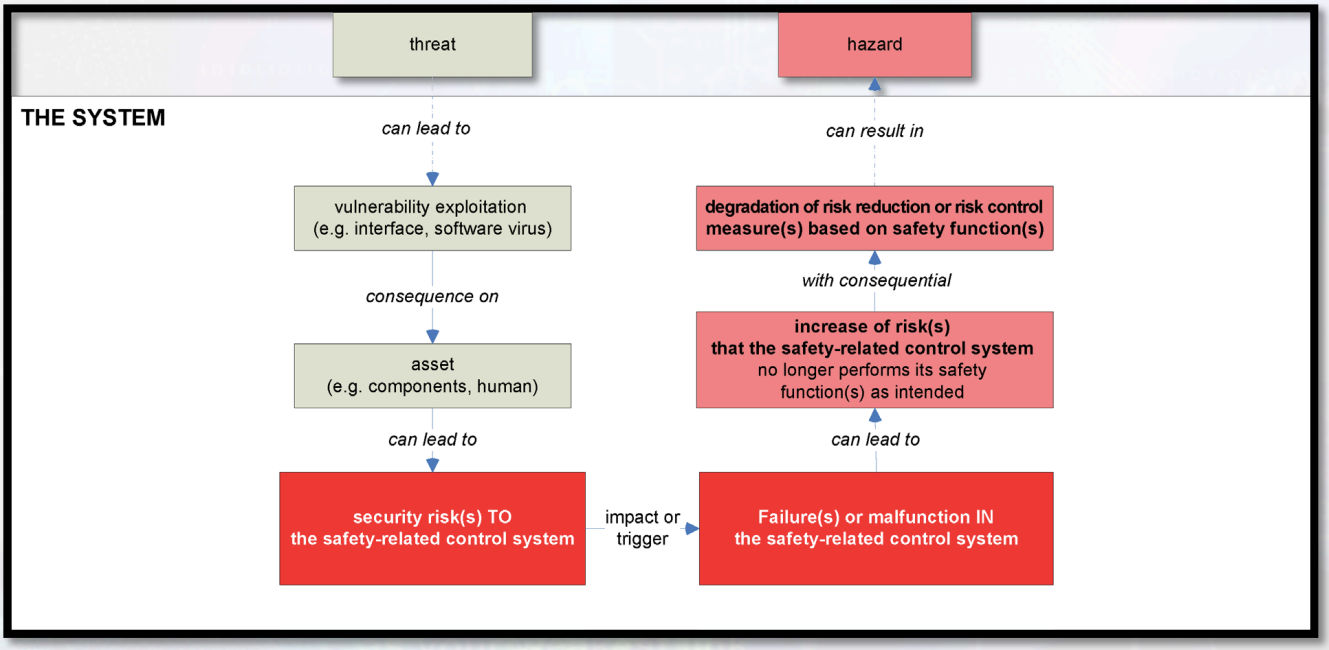
infrastructure vital for the organization's operation. Organizations are increasingly depending on Information and Communication Technology (ICT). Along with the growing economic value of ICT for organizations, threats to it are all growing because of the increased connectivity. To ensure a secure environment, a strategy to protect the organization's cyber space is required for managing risks and boosting resilience. Organizations must build and implement a risk based cyber security policy with clear priorities, minimum ICT security baseline with threat and vulnerability information, build incident response capabilities and create awareness, educating and training opportunities. Residual risk is a risk that remains after all efforts have been made to mitigate or eliminate risks associated with a business process or investment. After a risk assessment, a residual risk may be known but not completely controllable, or, in some cases, it may not be known.





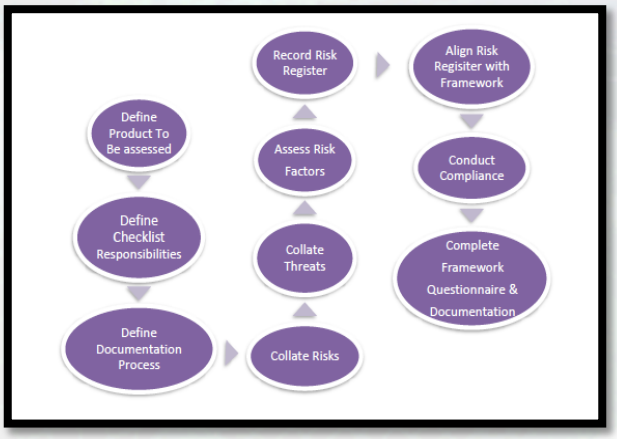
Risk Assessment comprises of Assessment of Threats, Vulnerabilities, Likelihood of Attack, Failure, Event, Impact (safety, reliability, financial, reputation, societal). And,Risk exposure (RE) of a threat is the likelihood (LI)(probability) of an attack "times" the impact (IM) if such an attack were to take place - **RE = LI * IM.**

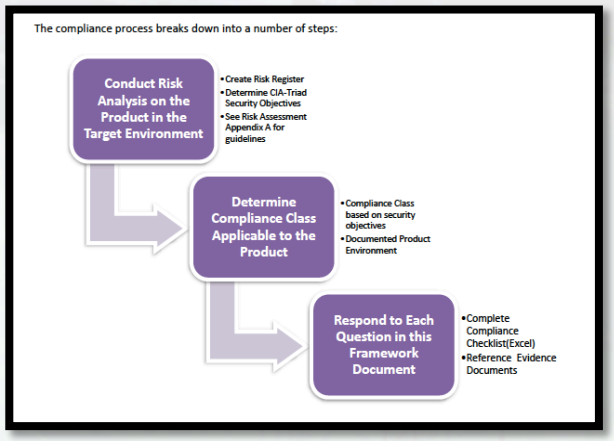
We don't need to reinvent the wheel. We need a Cyber Risk Management Information System that has a user-friendly interface. It should integrate the best, most recent data from our own sources. It has to be a lean machine. At the same time, it should give us more transparency than we have today.



Possible impact of security risk(s) on the safety-related control system

RISK ASSESSMENT STEPS





Cyber Threat Intelligence

Cyber Threat Intelligence *(CTI)* is analyzed information about the capabilities, opportunities and intent of adversaries that meets a specific requirement determined by a stakeholder. Organizations with CTI programs focus on understanding the threats TAKEAWAYS they face and providing specific information to help defend against those threats. In the past few years, CTI has evolved from small, ad-hoc tasks performed disparately across an organization to, in many cases, robust programs with their own staff, tools and processes that support the entire organization.

On the basis of security infrastructure, smart grid information security system provides security for smart grid from technology and management. The need is to establish a comprehensive security system from the four directions of physical and environmental

security, system security, network security, and data and application security on technical level. Aiming at each layer's unique security risks of sensing layer, communication layer, data layer and application layer, implement appropriate solutions respectively, to achieve prevention and control of smart grid - layer upon layer. Protect the whole Electricity Infrastructure and safeguard the security of smart grid.

"Step by step, we can make the cyber risk MIS our own. The whole process takes less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the shelf solution."

STANDARDIZATION IMPERATIVES

> "The beauty of standards is that there are so many to choose from!"
>
> Andrew S. Tanenbaum (1990)

In an ideal world, we would have exactly one standard for each task or interface. In reality, there are often overlapping or rivalling standards, driven by different vendor "camps", in case of Cyber Security, Standards by different Global, regional & National SDOs.

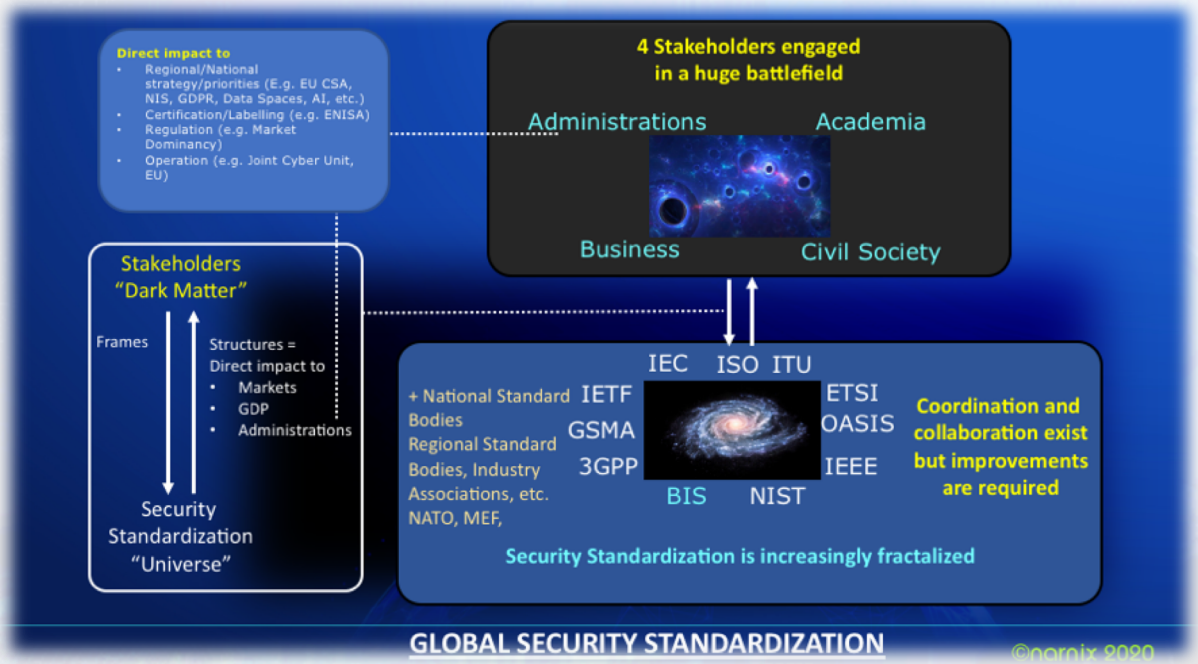
Innovation and technology development are accelerating. Strategic plans and roadmap are needed to help ensure that the market is suitably served with best practices that is pertinent to the goals and context of this very large market. The world has never been as competitive as today, yet cooperation is a must to deliver solutions for increasingly complex systems.

The Standards support our need to balance agility, openness and security in a fast-moving environment. The Standards provide us with a reliable platform from which we are able to innovate, differentiate and scale up our technology development. They help us control essential security and integrate the right level of interoperability. Standards help ensure cyber security in ICT and IoT systems (Digital & Cyber Physical systems).

Given the scale, moving forward through the labyrinth of Disruptive Technologies cannot be successfully, efficiently, and swiftly accomplished without standards. The role of standards to help steer and shape this journey is vital. Standards provide a foundation to support *innovation*. Standards capture tacit *best practices* and standards set *regulatory compliance requirements*, which is crucial for the sustainable Digital Transformation of the National Critical Infrastructure.

One of the most challenging Imperatives for "Standard Development Organizations" is Harmonization of Standards. "Standards & even SDOs are not at the forefront of Critical Infrastructure planners', utilities' or users' minds". There are misconceptions on what standards are for, and, the case for use of standards has not been made. Liberalization and Markets have a lot of great virtues, but they cannot create their own conditions of existences: they must be designed!

The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure demand a top-down approach to standardization starting at the system or system-architecture rather than at the product level. Therefore, the systemic approach in standardization work can define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported. It promotes an increased co-operation with many other standards-developing organizations and relevant non-standards bodies needed on an international level. India needs to define and develop its own globally harmonized framework and architecture for the Electricity Infrastructure keeping in mind the new paradigm of Integrated Critical Infrastructure, where Smart Grid shall be one of the key (but not the only) component to meet the imperative of a 'smart, green and secure community'.

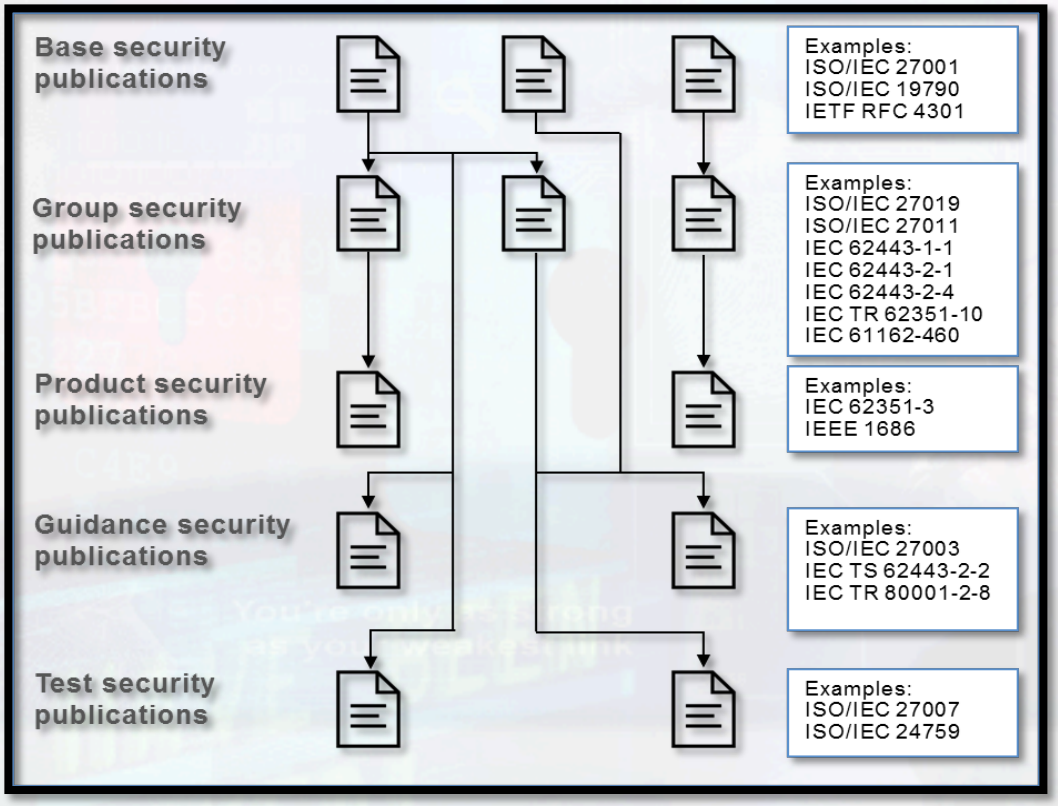


In last few years, there have been numerous Smart Grids and other Technology Initiatives (including R-APDRP, Smart Grid Pilots, IPDS etc.) aimed to help transform the Indian Electricity Infrastructure. While the roadmaps and even Pilots have focused on functionality, there is limited clarity on Technology Solutions, Architectures and Protocols that may best meet the goals of open standards, modularity, inter-operability and price-performance. The claim of "following standards" is insufficient because it doesn't answer the question of *which standard* and *why*. In fact, it is unlikely to be which standard, rather which standards since most architectures (e.g., NIST's & ETSI's frameworks) do not pick one standard but have a layered approach capable of using multiple standards in the portfolio. India needs to define and develop its own globally harmonized framework and architecture for the Electricity Infrastructure keeping in mind the new paradigm of Integrated Critical Infrastructure, where Smart grid shall be one of the key (but not the only) component to meet the imperative of a 'smart, green and secure community'.

The increasing complexity and connectivity of systems, products, processes and services entering the market requires that the consideration of security aspects be given a high priority. Inclusion of security aspects in standardization provides protection from and response to risks of unintentionally and intentionally caused events that can disrupt the functionality/operation of products and systems.

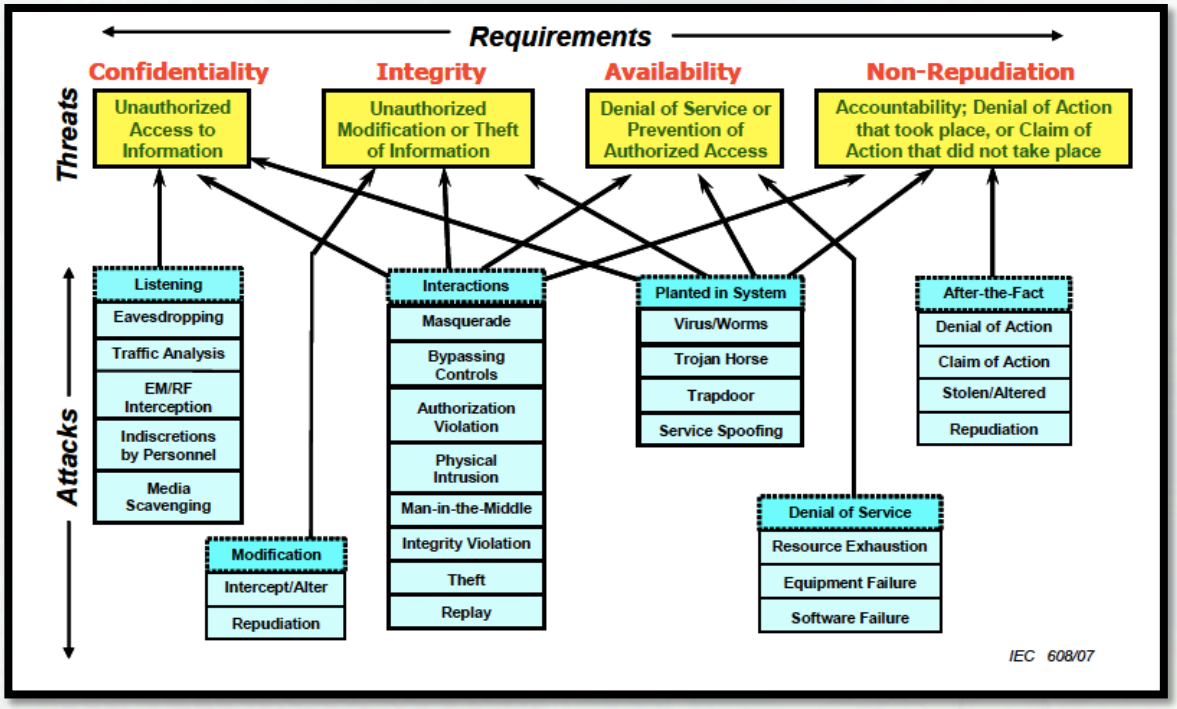
Publications for security can be categorised as one of the five types listed below:

- ⇨ Base Security Publication;
- ⇨ Group Security Publication;
- ⇨ Product Security Publication;
- ⇨ Guidance Security Publication;
- ⇨ Test Security Publication.



Types of publications

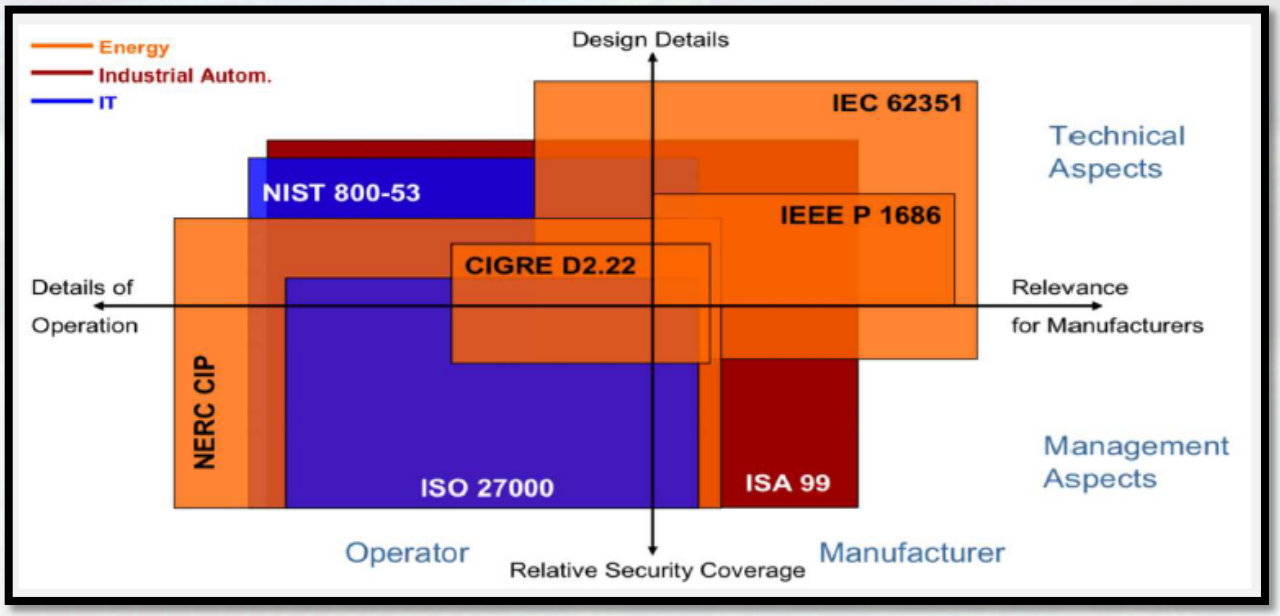
However, it is also important to understand the co-relation amongst different attributes of Cyber Security being illustrated below:



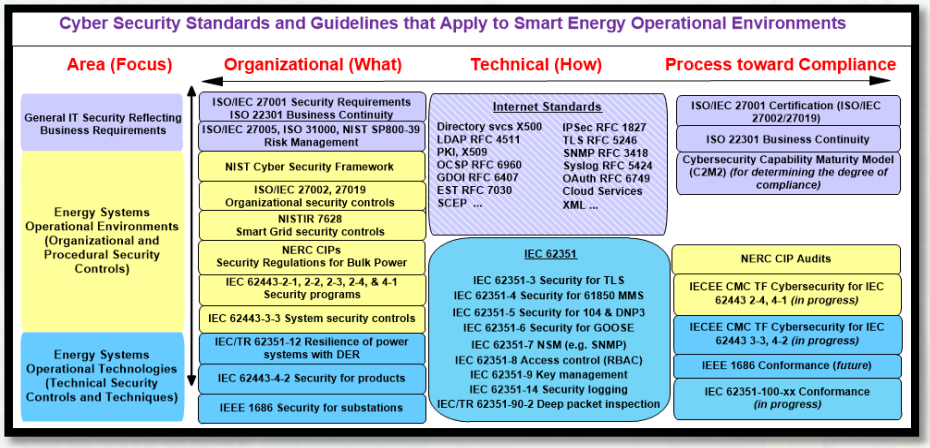
The relationships between security requirements, threats, and attacks

Another aspect that needs to be understood is that different SDOs (Standards development Organizations) have developed the Cyber Security Standards for different aspects of this complex paradigm with their respective perspectives which is determined by their respective domain focus and interest/requirements of their members/stakeholder. An illustration below explicitly demonstrates this inherent disconnect amongst stakeholder SDOs and their focus:

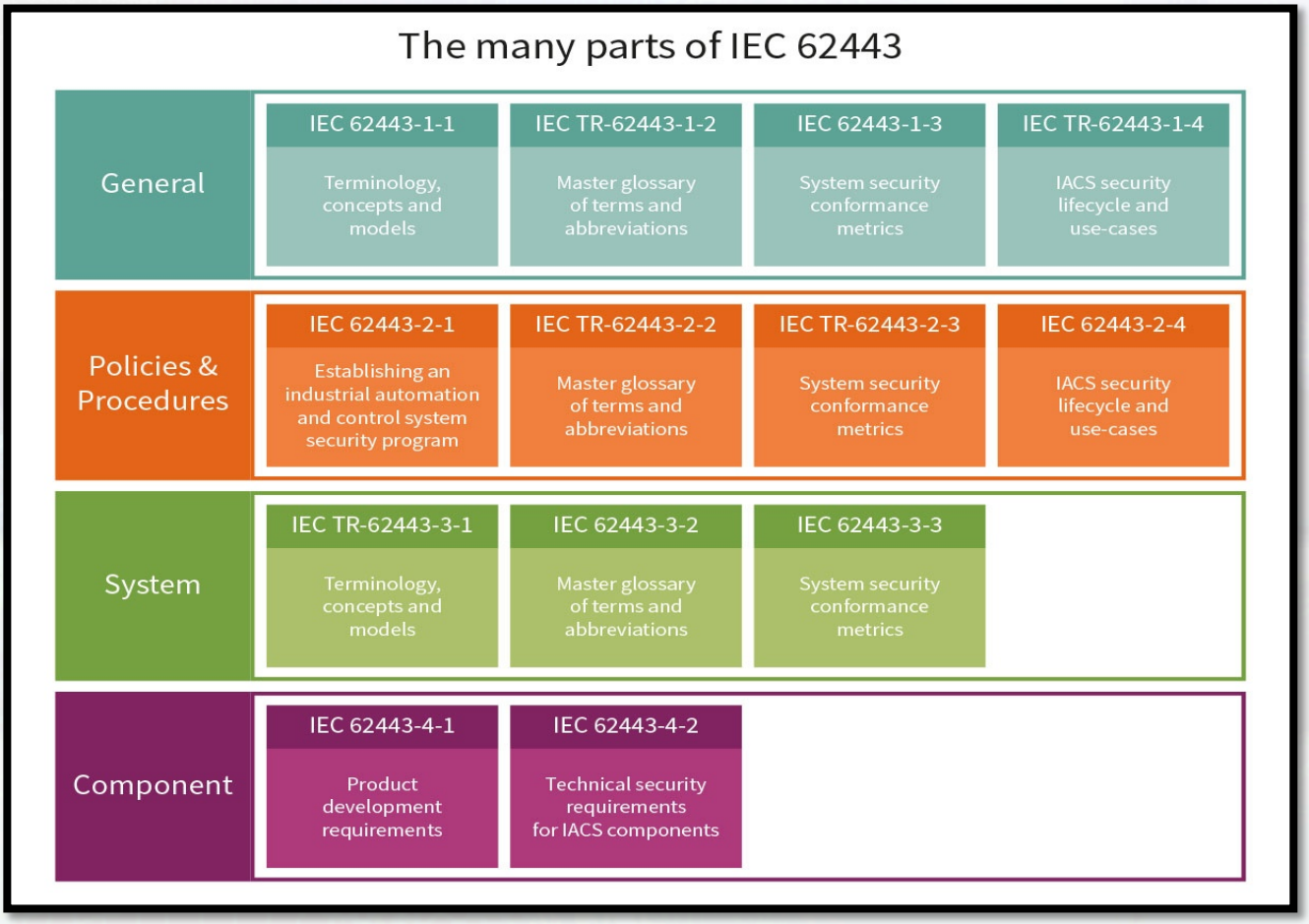
IEC 62443-2-4	Security program requirements for IACS service providers
IEC 62443-3-3	System security requirements and security levels
IEEE 1686 - 2013	IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
BDEW Whitepaper	Requirements for Secure Control and Telecommunication Systems
IS 16335	Power Control Systems – Security Requirements
ISO 27001	Information Security Management System (ISMS)
NERC-CIP	Critical Infrastructure Protection



The key IEC, ISO, IEEE, NIST, and IETF cyber security standards and best practices are shown in the diagram below, organized by type (What, How, Process towards Compliance) and by level (High general level, High energy-specific level, Detailed technical level).



It would be interesting and insightful to map further the different Series of Standards developed by different SDOs with granular aspects within the domain or aspect under focus to help get a comprehensive understanding about Cyber Security Concerns with corresponding Standards.



IEC 62443 Series for Industrial Control Systems

ISA/IEC62443 Security Levels

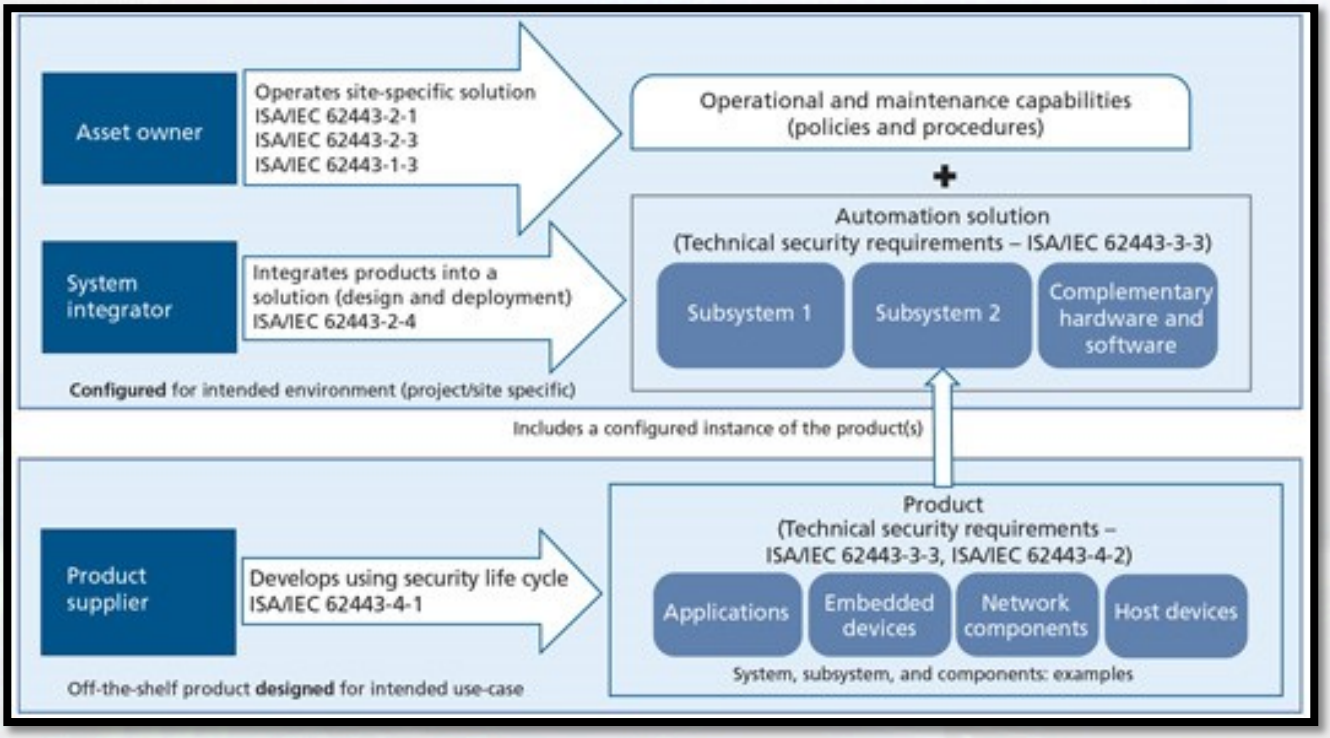
Three Types of Security Levels (SL)

- SL-T – Target Security Level for a specific asset or zone. Determined based upon results of a risk assessment.
- SL-C – Capability Security Level of component or system. Based on component or systems security capabilities (Security Features).
- SL-A – Achieved Security Levels – The actual level of security for a particular system.

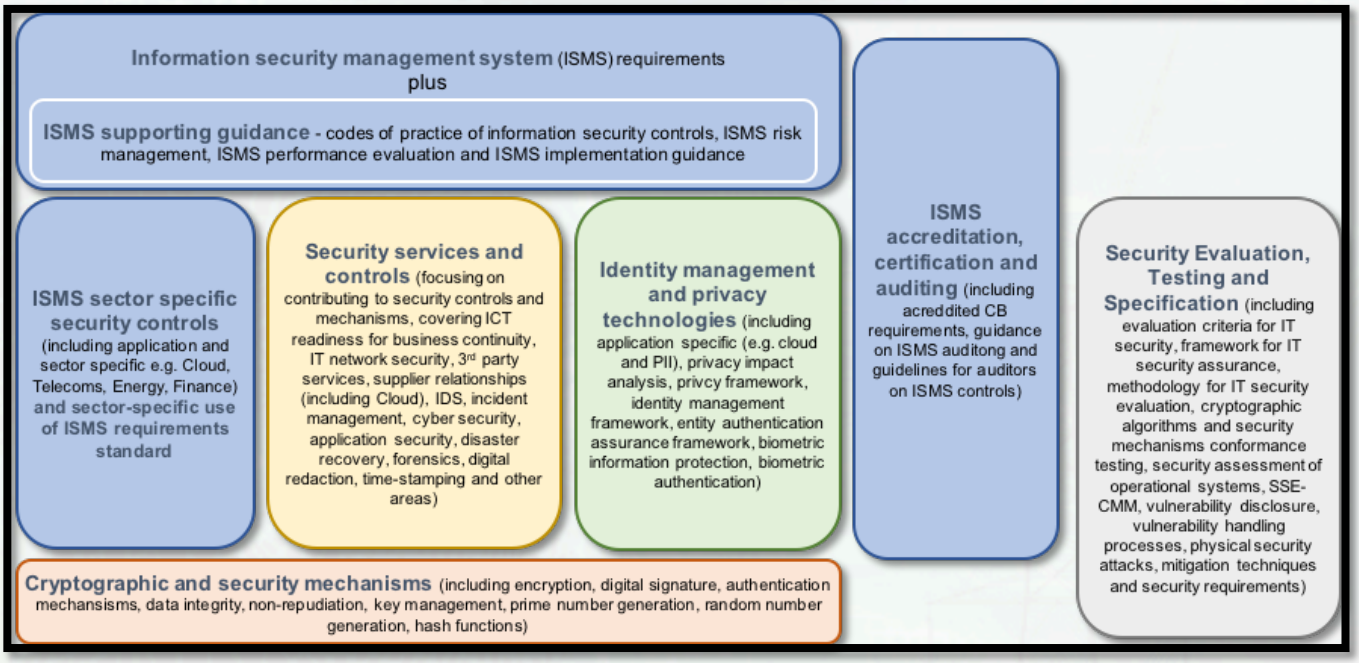
Five Security Levels (SL) – draft Version

- SL 0: No specific requirements or security protection necessary.
- SL 1: Protection against casual or coincidental violation
- SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation.

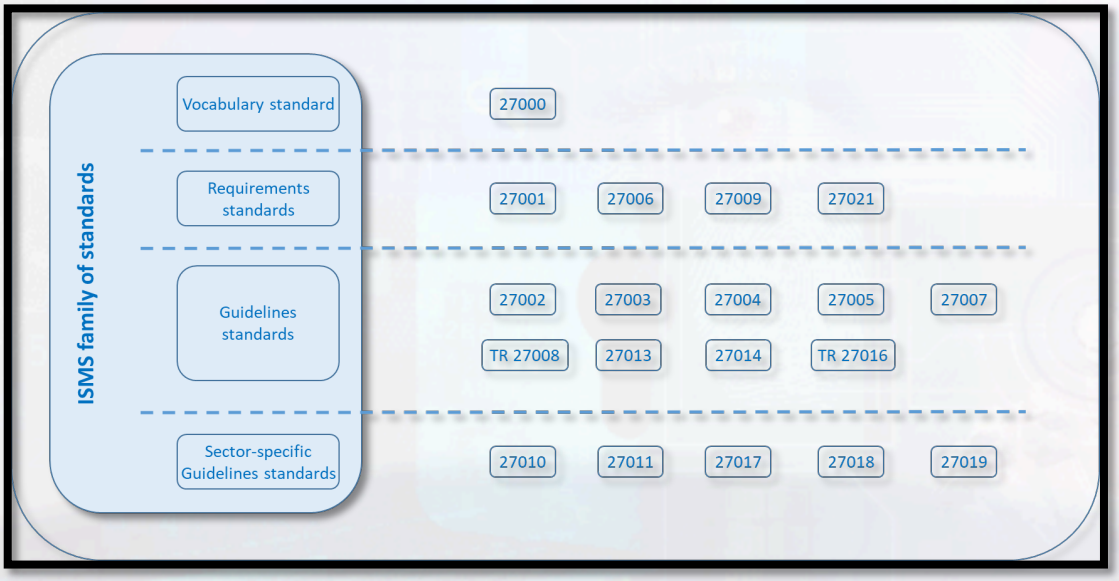
- SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.



IACS Value Chain



Security & Privacy Aspects in ISO/IEC 27000 Series Standards



ISO/IEC 27000 Series (*Information Security Management System: ISMS)*

Standards of penetration test for Firmware level security:

- Penetration testing is a part of the vulnerability discovery resource set at product and system application levels. The reference of penetration testing is found in IEC 62443 series (62443-2-1, *Clause A.3.4.3.5.5 System Testing*, 62443-2-3 *Clause C.2.1*).
- Within a vendor organization, the testing teams develop their own test cases to perform the penetration testing. There are no standard testing procedures available and the use cases are prepared as per the requirements. Hence, each testing is unique and depends upon the type of product and system configuration.
- There are 2 ways to address the identified vulnerabilities.
- Within a vendor organization, the vulnerabilities, as and when detected, are reported to the product owner to improve the quality of the product before its release or make a patch release later based on the severity of the vulnerability.
- Academic researchers, 3rd party companies may report the vulnerabilities to following global bodies:
  I. The National Vulnerability database (NVD).
  II. ICScert (https://www.us-cert.gov/ics) for Industrial Control System (ICS) related products.

IF YOU THINK TECHNOLOGY CAN SOLVE YOUR SECURITY PROBLEMS, THEN YOU DON'T UNDERSTAND THE PROBLEMS AND YOU DON'T UNDERSTAND THE TECHNOLOGY.

It is evident that Cyber Security is a very complex paradigm, and with evolving new technologies, requirements and ever-increasing Attack Surface the vulnerabilities are rising many folds with time. In such a dynamic scenario, how do we develop a Cyber Security Strategy to make our Critical Infrastructure comprehensively Safe, Secure, Resilient and Trustworthy?

CYBER SECURITY REGULATIONS & POLICIES LANDSCAPE

Cyber Security Initiatives in India

- 17.10.2000: Information Technology Act,2000 (No. 21 of 2000) – IT Act notified. This was amended in 2008. It is the primary law in India dealing with Cyber Crime and electronic commerce.
- National Cyber Security Policy notified in 2013. The strategies mentioned in NCSP 2013 are:
    - Creating a secure cyber ecosystem;
    - Creating an assurance framework;
    - Encouraging Open Standards;
    - Strengthening the Regulatory framework;
    - Creating mechanisms to address security;
    - Securing E-Governance services;
    - Protection and resilience of Critical Information Infrastructure;
    - Promotion of R & D;
    - Reducing supply chain risks;
    - Human Resource Development;
    - Creating Cyber Security Awareness;
    - Developing effective Public Private Partnerships; and
    - Information sharing and cooperation

- 10.01.2014: National Critical Information Infrastructure Protection centre (NCIIPC) was created by Government of India under section 70 A of IT Act.
- Two important documents of NCIIPC:
  Guidelines for protection of critical Infrastructure (CII)
  Framework for evaluation of Cyber Security
- Computer Emergency response Teams (CERT-In) under section 70(B) and sector specific CERTs constituted.
- As per Rule 12(1) (a) of IT Rules 2013, it is mandatory to report specific cyber security incidents to CERT-In.
- ISO: 27001: The Government of India, under the Information Technology Act, 2000 and the Rules therein for Reasonable Security Practices published in 2011, require all organisations to implement ISO:27001 as the recommended Information Security Management System for legal compliance.

Cyber Security in Power sector

- Indian Electricity Grid code Clause 4.6.5

  "All utilities shall have cyber security framework to identify the critical cyber asset and protect them so as to support reliable operation of the Grid."

- IS-16335 :2015 Power Control Systems-Security Requirement

  It specifies requirement for identification and protection of critical assets for all entities involved in generation, transmission, distribution and trading of electric power.

- CERC (Communication System for inter-State transmission of Electricity) Regulations, 2016.

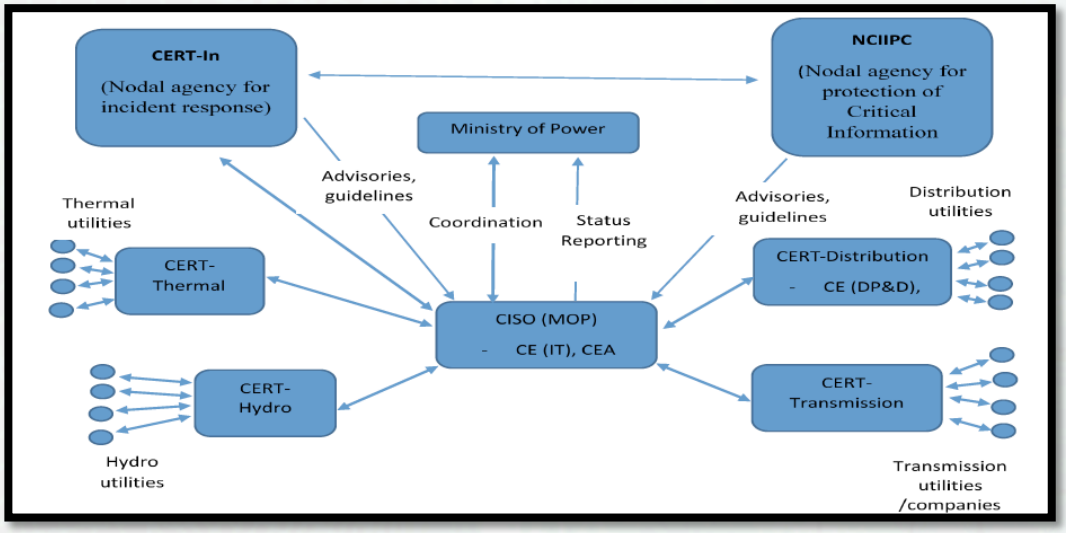
- "CEA shall formulate and notify technical standards, cyber security requirements, protocol for the communication system for Power Sector within the country including the grid integration with the grid of the neighbouring countries".
- Cyber Security: Communication infrastructure shall be planned, designed and executed to address the network security needs as per standard specified by CEA.

National Policy Doctrine

CEA is formulating a comprehensive strategy to address the cyber security issues that Power Sector faces:

- ⇨ A National policy doctrine to address cyber security for national critical infrastructure and a regulatory framework that provides guidance to the industry players across generation, transmission and distribution
- ⇨ To review preparedness with respect to advisories on Cyber Security Framework and to vet self-assessment of gaps vis-à- vis baseline security & resilience requirement
- ⇨ To prepare the requirement for setting up of C-SIRT (eligibility criteria, scope of work etc.) υ To design and develop Cyber Security Policy (CSP) & Procedures along with CCMP
- ⇨ Security Policy and Management
- ⇨ Security Organization
- ⇨ Security Mandates for the Corporate IT Systems
- ⇨ Domain Specific security standards for Control Systems υ Business Continuity Planning and Disaster Recovery
- ⇨ Customer Data Protection
- ⇨ Physical Security Requirements
- ⇨ Periodic Assessments and Reporting
- ⇨ Data Sharing and Collaboration

Organization structure for Cyber Security in Power system



Courtesy CEA dated presentation (2017)

NATIONAL TRUST CENTRE

Telecom Regulatory Authority of India (TRAI) in its Recommendations on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" released on 5th September 2017 advised DoT that –

- ⇨ A National Trust Centre (NTC), under the aegis of TEC, should be created for the certification of M2M devices and applications (hardware and software).
- ⇨ The government should provide comprehensive guidelines for manufacturing/ importing of M2M devices in India.
- ⇨ Device manufacturers should be mandated to implement "Security by design" principle in M2M device manufacturing so that end-to- end encryption can be achieved.

However, it is yet to be set up…

> It is evident that Cyber Security is a very complex paradigm, and with evolving new technologies, requirements and ever-increasing Attack Surface the vulnerabilities are rising many folds with time. In such a dynamic scenario, how do we develop a Cyber Security Strategy to make our Critical Infrastructure comprehensively Safe, Secure, Resilient and Trustworthy?

It is evident that Cyber Security is a very complex paradigm, and with evolving new technologies, requirements and ever-increasing Attack Surface the vulnerabilities are rising many folds with time. In such a dynamic scenario, how do we develop a Cyber Security Strategy to make our Critical Infrastructure comprehensively Safe, Secure, Resilient and Trustworthy?

Though government of India has put measures in place to check for any mal-intentioned bug or subcomponent in these equipment / systems, but these are not providing….

Lack of high level of assurance from intentional built in mechanism meant to compromise security of system due to following reasons/constraints: Sheer volume of equipment and their subcomponents; Gaps of Standards; Gaps in Capacity Skill set in Utilities/DISCOMs and budget provisions… Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

National Cyber Security Strategy 2020 (NCSS 2020)

The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25).

Pillars of Strategy - various facets of cyber security are under examination under the following pillars:

- ⇨ **Secure** (The National Cyberspace)
- ⇨ **Strengthen** (Structures, People, Processes, Capabilities)
- ⇨ **Synergize** (Resources including Cooperation and Collaboration)

Proposed vision is to ensure **a safe, secure, trusted, resilient** and **vibrant cyber space** for our **Nation's prosperity.**

GAPS & CHALLENGES

IF YOU THINK TECHNOLOGY CAN SOLVE YOUR SECURITY PROBLEMS, THEN YOU DON'T UNDERSTAND THE PROBLEMS AND YOU DON'T UNDERSTAND THE TECHNOLOGY.

The power sector cyberthreat landscape is rapidly evolving and expanding, with more frequent attacks, more numerous and varied threat actors, and increasingly sophisticated malware and tools that are more widely available and sometimes indiscriminately deployed. Power companies are among the most frequently attacked targets, increasingly by nation-state actors aiming for disruption and even destruction through Industrial Control System (ICS). One of the most challenging vulnerabilities to address is cyber supply chain risk, given the increasingly far-flung and complex nature of the supply chain. Cyber supply chain accountability and ownership are not well-defined within companies, most CISOs have no control over their enterprises' supply chain, and they may have little access to supply chain cyber risk intelligence or visibility into suppliers' risk management processes. Add to that a lack of manpower and the sheer number of suppliers and transactions, and you begin to appreciate the scope of the challenge. Most companies are just beginning to make suppliers more aware and accountable, and to demand supplier integrity.

Though government of India has put measures in place to check for any mal intentioned bug or subcomponent in these equipment / systems, but these are not providing high level of assurance from intentional built in mechanism meant to compromise security of system. This is due to following reasons/constraints:

Sheer volume of equipment and their subcomponents:

It is difficult for 100% full proof testing/ scrutiny while consuming. There is also lack of required infrastructure to handle such volumes. It becomes even more challenging, when majority of Indian companies import this equipment which are seldom just sample checked.

Gaps of Standards:

There is lack of holistic efforts and pro-activity on parts of countries and OEMs to participate in standards development which provides an open and democratic approach to product development and ensures compliance with regulatory and national testing procedures.

The problem is not the lack of standards, but lack of understanding on relevance and usage of the right standard for Indian ecosystem. Internationally there are too many standards available and very often having duplicities, hence, these required to be simplified and modelled for Indian Utilities. Utilities shall spec-in such standards which are drafted by national organization.

There is a need for standard cyber security framework. Though international organizations like IEC, ITU, ISO, IEEE etc. have framed standards to be followed for electrical and communication equipment, but these do not cover most of internal architecture, design & software, which remain propriety in nature even today. This in general is exploited by OEMs for commercial reasons. However, countries with mal intentions use this loophole to impregnate their equipment and devices for spy wares. Understanding or detecting these

proprietary and intentional applications is a big challenge. List of standard and their intended coverage /use is elaborated in the preceding section.

Gaps in Capacity Skill set in DISCOM and budget provisions:

To deal with vulnerabilities and gaps, it is required that DISCOMs should have structured programs for skill development. DISCOMs should take full ownership of Cyber Security compliance rather can delegating it to vendors and/or other agencies through contracts. Usually technologies are evolving at a fast pace and from cyber security perspective this pace becomes even more challenging as nature of threats & resolutions keep on changing. Utilities are either not updated with latest technologies or there are no budget provisions to explore cyber security solutions. Hence, a dedicated focus and ownership is required with in DISCOMs.

Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

Some key Challenges in Protecting CII (Critical Information Infrastructure):

- Lack of **"**visibility over, and classification of CII**"**
- Identify and document incoming/outgoing dependencies on other infrastructure.
- Gap analysis of dependencies on other infrastructure.
- Evolve overall CMP for CII sectors at NCIIPC level.
- Lack of **"**a standardized framework or metrics to identify and classify critical information infrastructure**"**
- Lack of **"**standard, nation-wide practices, for defining the baseline metrics" for identification of critical information infrastructure
- Lack of **"**knowledge and awareness about factors**"** impacting critical information infrastructure
- **Inadequacy of "**relevant and workable information to take decision at the national level**"**
- Inability **in "**Activating, driving, ensuring desired actions and seeking conformance from the entities on the specific terms**"**

Challenges in Digital Infrastructure Security:

- Pervasive digitization of the infrastructure (without designing security into the products) - Smart Meters; Digital Relays/Intelligent Electronic Devices (IEDs); Phasor Measurement Units (PMUs)
- Proprietary and legacy Systems – lack of updates
- Lack of clear patch management policy for power system equipment
- Devices in remote (insecure) locations
- Supply chain contamination (including AMC personnel)
- Different National / State / Local regulatory authorities
- Extensive communication without properly enforced security policies could result in attacks/faults cascading from one part of the system to other
- Rapidly emerging threats (days/weeks) versus power system lifecycle (decades)
- Lack of security awareness & expertise among utilities.
- How do we address the Security Issues of the Eco-systems, which are still evolving?
- How do we develop the Protection Profiles for the use cases, when even users have not defined their Requirements and concerns?

- The majority stakeholders of these new Eco-systems have absolutely NO CLUE about the identity & existence of the Security Evaluation frameworks like COMMON CRITERIA.
- How do we educate the Utilities about the Security Paradigm, who do not have a CISO on board yet, or even have any inkling of the devastating implications of the vulnerabilities of their ICT Infrastructures?
- The integrating Information Technology, so vital to the Smart Grid, will introduce traditional cyber weakness.
- In order to have appropriate protection, the new generation Smart Grid's Information Infrastructure could deploy measures similar to that used in securing a cloud and implement security as a wrapper.
- The Smart Grid essentially deploys SCADA systems. There has been a perceptible shift towards running such smart applications on COTS non-embedded computing systems running on OS that are either open source or commercial in nature. Such systems traditionally run in client - server mode. These, in particular need to be protected. All best practices relevant to a large IT base network will have to be incorporated.

One of the most challenging vulnerabilities to address is cyber supply chain risk, given the increasingly far-flung and complex nature of the supply chain. Cyber supply chain accountability and ownership are not well-defined within companies, most CISOs have no control over their enterprises' supply chain, and they may have little access to supply chain cyber risk intelligence or visibility into suppliers' risk management processes. Add to that a lack of manpower and the sheer number of suppliers and transactions, and you begin to appreciate the scope of the challenge. Most companies are just beginning to make suppliers more aware and accountable, and to demand supplier integrity.

- Volume of equipment and Sub-Components:
- Lack of Testing Infrastructure
- Gaps in Standards: Simplification and Relevance
- Skill set in DISCOM - Approach to handle Contractually rather Technically
- Budget Constraints
- Protecting CII (Critical Information Infrastructure)
- Digital Infrastructure Security

The problem is not the lack of standards, but lack of understanding on relevance and usage of the right standard for Indian ecosystem. Internationally there are too many standards available and very often having duplicities, hence, these required to be simplified and modelled for Indian Utilities. Utilities shall spec-in such standards which are drafted by national organization.

ONLY AMATEUEURS ATTACK MACHINES, PROFESSIONALS TARGET PEOPLE

Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

SOLUTIONS FOR INDIA

Secure Cyberspace Assurance – Promise of a trustworthy Cyber-ecosystem

Internet Resilience of India - It is of utmost importance to ensure the security and resilience of the INTERNET within the country to enhance cyber security capabilities to better protect Indians and defend critical government and private sector systems.

Secure Cyberspace Assurance - Promise of a trustworthy Cyber-ecosystem entails the following:

Cybersecurity expectations of users:

i. Availability of system and network resources to legitimate users;
ii. Convenient recovery from successful attacks;
iii. Control over and knowledge of one's computing environment;
iv. Confidentiality of stored information and information exchange;
v. Authentication and provenance of information;
vi. The technological ability to exercise fine-grain control over the flow of information in and through systems;
vii. Security using computing directly or indirectly in important applications, including financial, health care, and electrical transactions, as well as in real-time remote control of devices that interact with physical processes;
viii. The ability to access any source of information safely;
ix. Awareness of the security being delivered by a system or component; and
x. Redress for security problems caused by another party.
xi. Citizen's privacy and protection on Social Media - Protecting users of the cyber commons, nationally or globally.

Defensive actions cover at least four dimensions:

i. Data protection an essential component of security strategy.
ii. Mandatory protection of cyber domains essential to the economic health and quality of life - Responsible entities should not be able to opt out of compliance with mandatory Reliability Standards. Remove - acceptance of risk language from the CIP Reliability Standards and technical feasibility from the CIP Reliability Standards, only that the term be interpreted narrowly and without reference to considerations of business judgment. Interconnected control-system networks are susceptible to infiltration by a cyber intruder and that responsible entities should protect themselves from whatever is outside their control systems. Issues and concerns that

a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.

iii. National strategies, plans, and programs, helping coordinate protection of the commons - Regulation is necessary for protecting important parts of the cyber commons and a necessary tool for protectors. But one must recognize that the entities so regulated will accept it only after avoiding it through every possible legal and political channel available to them. Regulation of digital identities would eliminate anonymity from users in order to facilitate accountability for actions in the cyber commons. Acceptance of communications from unlicensed users would be at the receivers' risk.

iv. international legal regimes and their supporting international structures, encouraging and assisting defense of the commons; and monitoring compliance by the signatories to maintain their trust and confidence; enforcing the agreement should signatories depart from agreed-upon norms; resolving disputes among the signatories; addressing technical issues of definitions, standards, and forensic collection; and rendering assistance to signatories to respond to technical challenges expeditiously.

v. Technology to warn, prevent and thwart misuse of the commons

Internet Resilience of India

It is of utmost importance to ensure the security and resilience to enhance cyber security capabilities to better protect Indians and defend critical government and private sector systems. Some actionable insights to achieve these imperatives shall entail:

- ⇨ Thwart abuse of Legitimate Services for Command and Control for Cyber espionage and financially motivated actors.
- ⇨ Making available Public DNS for use by general public.
- ⇨ Diverting query of root DNS to a DNS in the country, which will be acting as root DNS in case of any eventuality.
- ⇨ Public National Time Protocol (NTP) need to be implemented and it will be used by all ISP and organization for synchronization of time in digital space.
- ⇨ All the ISPs in the country should peer through NIXI so that domestic traffic does not go out of India.
- ⇨ All the critical sectors such as financial, power, governance etc. should use '.in' based domains for websites or web-based services. The access of '.in' based domains can be ensured during any eventuality.
- ⇨ CNI (Critical National Infrastructure) Protection shall need completely indigenously designed and maintained - Information Network, Search Engines, National Switch, National OS, Social Media Platform, Collaboration Platforms, Secure Chip, Digital Forensics, Cloud & SDC's, Domain Name System & Registry etc.
- ⇨ Further, India needs development of indigenous critical component of Internet infrastructure such as - e-mail, Search Engine, Root Servers, Operating Systems, Messaging services.

National Electricity Infrastructure

There is a need to develop Resilient, Secure and Trustworthy Grid which to a large extent is immune to cyber-attacks.

Widespread connection of distributed energy resources, smart appliances, and more complex electricity markets increases the importance of cybersecurity and heightens

privacy concerns. Robust regulatory standards for cybersecurity and privacy are needed for all components of an interconnected electricity network. To keep pace with rapidly evolving cybersecurity threats against large and complex electric power systems, electric utilities, vendors, law enforcement authorities, and governments should share current cyber threat information and solutions quickly and effectively.

Maintaining a data hub or data exchange would serve several purposes: securely storing metered data on customer usage, telemetry data on network operation and constraints, and other relevant information; allowing non-discriminatory access to this data to registered market participants; and providing end consumers with timely and useful access to data on their own usage of electricity services. Responsibility for this function should also be carefully assigned, with priority given to data security and consumer privacy considerations.

Utilities will need resilience and will need to be prepared to contain and minimize the consequences of cyber incidents. Future power systems with high penetration of DERs and Electric Vehicles are envisioned to have features that are favorable for their resilient operation. For instance, microgrids, with DERs, are helpful for resilience, and with "islanding" operations can assist in "black-start" or continued operations if the broader grid goes down due to a cyber or physical incident.

Privacy is also a growing concern, as ever expanding private personal and corporate information is gathered and stored by utilities and their affiliated companies. With expanding connection of electric and telecommunications devices, vastly more information will become available. Data analytics and the opportunity for outside organizations to have access to large quantities of data will increase the amount of information held by electric utilities and their affiliated partners. If electric utility companies expand their services beyond just delivering electricity, by interacting with DER aggregators, for example, specific procedures to protect data breaches and exfiltration of information will be needed.

To build a stronger and smarter grid, continuous efforts to check authenticity of equipment, implement secure communication, follow relevant standards, regular upgrades and maintenance of devices, centralized repository of knowledge data base and role-based access etc. are some of the guidelines to adopt and run smart grid project successfully.

Communication medium and equipment:

Communication plays a vital role in not only connecting the GENCO, TRANSCO and DISCOM but also sharing the vital information across various devices. This data is then turned into an information and helps to control and manage the system. Any disruption of the flow of data or insidious tampering of data in transit would have vicious consequences if perpetrated by unfriendly entities. These systems have life, spanning 10-15 years or more and so there is greater concern of attack with respect to time. The solution is to reduce the risk by removing untrusted elements from root and expect a robust level of security over the communication network consisting of network devices and network infrastructure including application servers at back end.

Connecting field devices in DISCOM e.g. Must have end to end security and must comply the security standards *(refer Annexure-I)*. It is recommended to use managed devices, Zone Based Firewall etc.

Standard protocols and certifications should be used for critical infrastructures application.

Communication Equipment TRANSCO: TRANSCO plays major role in transmitting the power across regions, states and districts. These transmission power relies on control event generated from ahead substation to share faults and control data. These substations are connected via OPGW and terminated over a Fiber Optic Terminal Equipment (FOTE) communication equipment. These FOTE should be certified by TEC under Department of Telecommunication over and above international certifications.

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE.

Cyber Security:

Cyber security is primarily the critical part of the Power Grid system. Cyber Security is amalgamation of People, Process and Technology. All the devices which are enabled to be part of smart Grid infrastructure should have cyber security features in place, e.g. Devices which are connecting substations should have firmware free from any known vulnerability and all vulnerabilities should be duly exposed and regularly updated in these devices.

Communication on encrypted channel: Communication across sites should be via devices enabled with encrypted channel. While in TRANSCO network SDH or WAN Devices, routers should be transmitting encrypted and fully secure data using OT Security in place.

Process related Actions:

Following actions recommended:

a) Cyber Laws: It is recommended that Cyber law must be refined considering utility needs.
b) Trusted Vendor List: It is suggested to develop a "National Charter of Trust" under NSA, which should publish a list of trusted vendors for Critical infrastructure landscape.
c) Policy Level actions: India can follow policy level decisions taken by other countries including USA, Australia & New Zealand to protect their power systems as per reference below:
https://www.zdnet.com/article/trump-bans-acquisition-of-foreign-power-grid-equipment-citing-hacking-threats/
https://www.scmp.com/news/asia/australasia/article/2002313/deal-australia-ban-chinese-investment-power-grid
d) Blocking unreliable vendors: Policy makers, funding agencies and Utilities should be vigilant on blocking following vendors:
    i. Who have been debarred by international agencies due to fraudulent practices e.g.:https://www.worldbank.org/en/news/press-release/2019/06/12/world-bank-group-debars-dongfang-electronics-co-ltd
    ii. Vendors belonging to countries having restrictive clause for mission critical applications which does not allow use of equipment of any other country for mission critical applications like power & telecom sectors.
e) Physical Security processes: End user should have stringent process for Document Control, Access control, User authentication and password protection to prevent access of any unauthorized person or leakage of information. Security education and training programs need to be developed as well as policies on sharing security vulnerabilities, threats, and solution information.

One of the proposed solutions could be that all utilities form a cyber division of experts & take ownership of complete security instead of relying on different vendors for their respective deliveries.

In addition to the above, following Technical and Commercial conditions can be considered to be part of the bids for new Smart Grid Infrastructure:

COMMERCIAL:

1. If any company acquires Indian company, then new entity can supply old product of acquired company to the utilities and should maintain spares & provide support to utilities for at least 10 years.
2. Bidder must have license to manufacture the product within India with compliance to standards like BIS, IEC, IEEE & ITU etc.
3. In Bidder manufacturing facility, more than 80% employee strength should be from Indian origin.
4. Bidder must have service support team within India to handle the defects or repair.
5. Employees working in critical infrastructure projects should be Indian citizens and security cleared by Govt nominated agency.
6. Govt should release security guidelines for security processes to be followed by all constituents of Power sector.
7. It should be mandatory for utilities to conduct annual security audit /penetration testing for systems.
8. Security audit of processes and systems of company supplying systems and solutions should be done by approved Cyber Security Audit agencies.
9. Quality and cost-based selection (QCBS) criteria must be considered for all tenders and bidder should get advantage if offered solution complies to “Make in India”.
10. Indian bidder should get chance to match L1 price in case tender allows global players.
11. Global companies which have registered offices for engineering, design, integration, testing, equipment inspection in India should only participate.
12. Limit participation of neighbouring countries having national boundary conflict as there can be increased incentive of such countries to create cyber-attack.

TECHNICAL:

1. CERT-In guideline must be followed for all component and push for IEC 62443 and ISO 27019 must be given to meet OT/IT cybersecurity requirement.
2. Products should be certified by Cyber security test facility in India e.g. CPRI, STQC (under MeitY), TEC (under DOT) or designated test agencies across the world. The infrastructure for testing on cyber vulnerabilities should increase in India.
3. The hardware shall be CE or equivalent international standard compliance.
4. All configuration of products / application should be in English language.
5. Origin of Source code of application must be declared. It should not be from non-friendly country as denoted in Sl. 13 of commercial section.
6. Firmware shall be readily available on support sites for supporting different versions of OS.
7. Data Centre need to be available for Smart Grid application and they should comply to minimum Tier-3 level security along with comprehensive SOC capability.
8. Reference architecture of Smart Grid application as published by IEEE / BIS / IEEMA should be used.

Some critical issues for securing the Smart Infrastructure:

- Design the Smart Infrastructure Information & Communication Infrastructure with security inbuilt. This should include the use of appropriate encryption for authentication and securing information at rest, and in transit.
- The Smart Infrastructure ICT Infrastructure should be scalable, so as to allow networks that comply with established standards, validated through a functional and security audit, to quickly integrate with the main grid network. (There is no question that the Smart Infrastructure is going to be a complex infrastructure and also consist of multiple smart Infrastructure domains.) More interconnections also increase the surface area for Denial-of-Service attacks and introduction of malware / compromised hardware.
- Integrate strong encryption systems for securing communications within the grid. Integration of a PKI solution for a role-based access control and authentication mechanism.
- Hardening of systems, both client as well as server. There should be a clear role-based security policy pushed to the client systems in a domain environment. This would include a policy for hardening network devices.
- Design the Smart Infrastructure Information & Communication Infrastructure with security inbuilt. This should include the use of appropriate encryption for authentication and securing information at rest, and in transit.
- The Smart Infrastructure ICT Infrastructure should be scalable, so as to allow networks that comply with established standards, validated through a functional and security audit, to quickly integrate with the main grid network. (There is no question that the Smart Infrastructure is going to be a complex infrastructure and also consist of multiple smart Infrastructure domains.) More interconnections also increase the surface area for Denial-of-Service attacks and introduction of malware / compromised hardware.
- Integrate strong encryption systems for securing communications within the grid. Integration of a PKI solution for a role-based access control and authentication mechanism.
- Hardening of systems, both client as well as server. There should be a clear role-based security policy pushed to the client systems in a domain environment. This would include a policy for hardening network devices.
- The new generation SCADA systems are mostly running on COTS Hardware and software (OS either windows or Linux).
- The shelf life of Operating systems is far lesser than the applications designed to run on them.
- There is a need to take the issue into account, as some applications may be built specific to a type and version of OS, so that seamless migration of SCADA applications to newer operating systems becomes possible.
- It is also important to lay down the standard for hardening of such systems, whilst the actual procedure /process can only be defined when the architecture and its components / specific solutions and technologies are finalized.
- Secure implementation of COTS based SCADA systems. The security of networking components, their secure configuration, hardening and administration.
- Standards for regulating the transfer of data or malware through various interfaces like USB or LAN etc. is critical.
- To study and define the Security Life Cycle of the IT based components of the Smart Infrastructure Systems.

- ⇨ To study the impact of mobile devices i.e. Laptops/ palm tops that will most likely be used within the Grid and how to secure the Infrastructure from them and these official devices from cyber threats as well. Must look at BYODs aspect, as well.
- ⇨ To Evaluate the NISTIR 7628 and its Gap analysis.
- ⇨ There is a need to deliberate whether we need to insist on the Common Criterion evaluation /grading of IT components.
- ⇨ We need to engage with the "Common Criteria" and "Information Security" domain professionals as well as the new stakeholders of these New & Rising Paradigms to make our planet earth Safe and Secure along with making it Smart n Green.

Best Security Practices for Protecting Big Data:

- ⇨ Secure computation in distributed programming frameworks
- ⇨ Secure data storage and transaction logs
- ⇨ Real time security and compliance monitoring
- ⇨ Privacy protecting data mining and analytics
- ⇨ Access control and secure communications
- ⇨ Effective audits
- ⇨ Data provenance (ability to trace and verify the creation of data, how it has been used or moved among different databases, as well as altered throughout its lifecycle)

Approach to Address Security of data in Cloud:

- ⇨ Data Classification and Accountability
- ⇨ Application Level Controls
- ⇨ Operating System Controls
- ⇨ Host Level Controls
- ⇨ Identity and Access Management
- ⇨ Network Controls
- ⇨ Physical Security
- ⇨ Compliance
- ⇨ Data isolation techniques to logically separate cloud tenants and create an environment where customers can only access their own data

Standards – Emerging Technologies, Data Management:

i. Minimum security assurance in IoT devices
ii. Mandatory certification of IoT devices before bringing it in market
iii. Increase in numbers of testing labs
iv. India specific protection profile of new devices coming up in emerging technologies.

Regulation & Policy

i. Increase efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime.
ii. Efficient and effective long-term whole-of-government response to cybercrime, including national coordination, data collection and effective legal frameworks, leading to a sustainable response and greater deterrence;
iii. Strengthened national and international communication between government, law enforcement and the private sector with increased public knowledge of cybercrime risks.

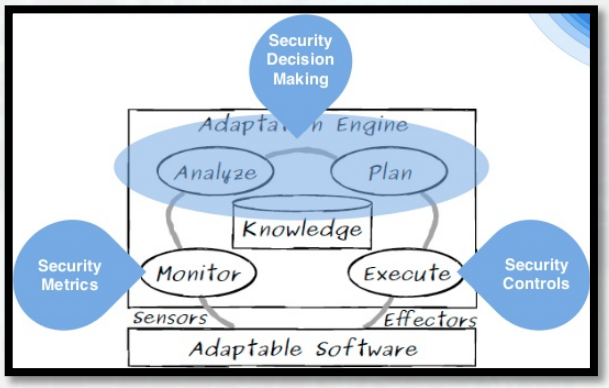
Legislations

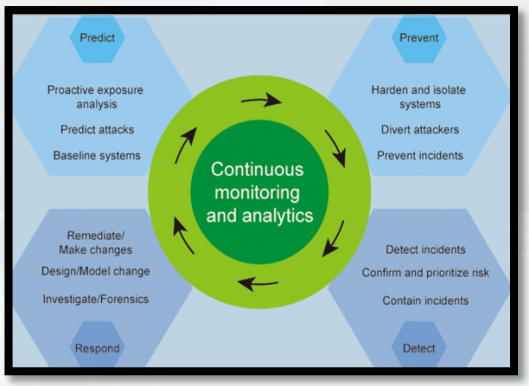
a. **IT Act & Amendment**
b. **Data Protection Act**

ONLY AMATEUEURS ATTACK MACHINES, PROFESSIONALS TARGET PEOPLE

Security Strategy: Adaptive Security Architecture:

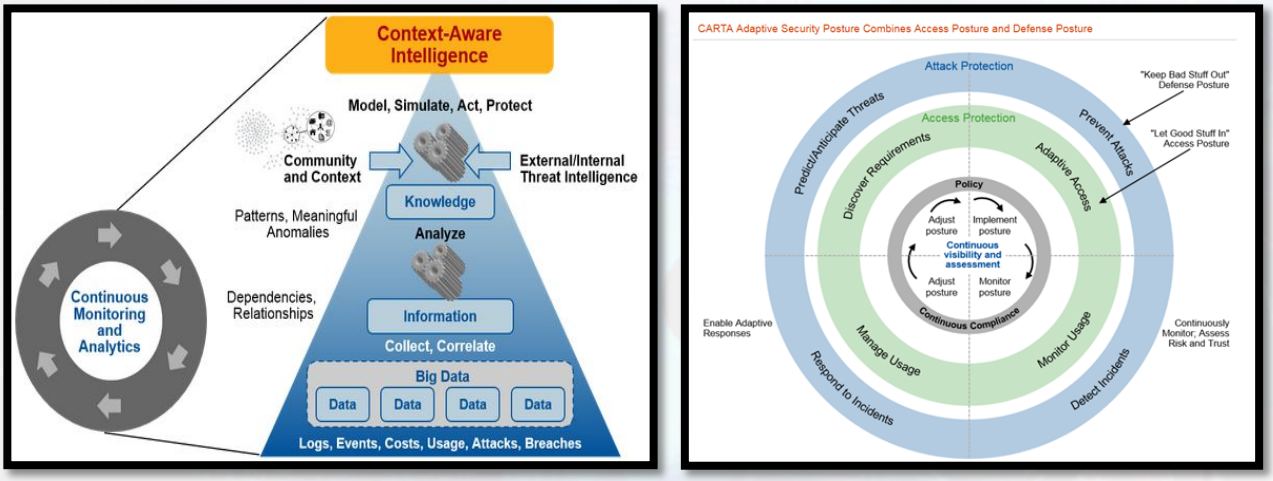
- It is an information security approach that employs modern tactics and tools to thwart the attack on the network by cybercriminals.
- It can be considered as a way of "beating the cybercrime masters in their own game".
- Thus, organizations should not solely rely on preventative mechanisms as cybercriminals are continuously "upping" their game and not giving up in launching attacks on vulnerable networks.
- In simpler terms, Adaptive Security Architecture means having flexible security measures in place to be able to protect an organization's information.
- This goes beyond the traditional perimeter defense from potential threats.





CARTA (Continuous Adaptive Risk and Trust Assessment) **Approach** –

- CARTA represents a critical strategy for forward-thinking CIOs and CISOs. With digital trust as a key concept, CARTA enables you to recognize the changing risk landscape and place only the trust appropriate at a given time in your employees and entities. Security is not a set-it-and-forget-it thing; it's a process that has to be always reviewed and adjusted based on ongoing real-time assessments of risk and trust.
- A CARTA approach goes beyond yes/no questions and assesses risk and trust related to both the user and the entity (in our case, a folder), at the exact point in time when the decision has to be made — all based on continuous top-to-bottom visibility.
- CARTA approach balances risk and trust, minimizing the risk of a "good guys gone bad" situation.



CARTA – Continuous Adaptive Risk and Trust Assessment

NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020)

The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25).

India was one of the first few countries to propound a futuristic ***National Cyber Security Policy 2013(NCSP 2013)***. Since the adoption of NCSP 2013, the technologies, platforms, threats, services and aspirations have changed tremendously. The transformational Digital India push as well as Industry 4.0 is required to be supported by a robust cyberspace. However, Cyber intrusions and attacks have increased in scope and sophistication targeting sensitive personal and business data, and critical information infrastructure, with impact on national economy and security. The present cyber threat landscape poses significant challenges due to rapid technological developments such as Cloud Computing, Artificial Intelligence, Internet of Things, 5G, etc. New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime & cyber terrorism, and so on. Threats from organised cybercriminal groups, technological cold wars, and increasing state sponsored cyber-attacks have also emerged. Further, existing structures may need to be revamped or revitalised. Thus, a need exists for the formulation of a National Cyber Security Strategy 2020.

Proposed vision is to ensure **a safe, secure, trusted, resilient and vibrant cyber space for our Nation's prosperity.**

Pillars of Strategy - various facets of cyber security are under examination under the following pillars:

- ⇨ **Secure** (The National Cyberspace)
- ⇨ **Strengthen** (Structures, People, Processes, Capabilities)
- ⇨ **Synergise** (Resources including Cooperation and Collaboration)

One of the proposed solutions could be that all utilities form a cyber division of experts & take ownership of complete security instead of relying on different vendors for their respective deliveries. Some of the issues that are critical for securing the

Smart Infrastructure are: Best Security Practices for Protecting Big Data; Approach to Address Security of data in Cloud and Standards for Emerging Technologies, Data Management - Minimum security assurance in Devices & systems; Mandatory certification of Devices before bringing it in market; Increase in numbers of testing labs; India specific protection profile of new devices coming up in emerging technologies…

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE.

CONCLUSION & RECOMMENDATIONS

Cyber risk is challenging to address, but utilities can start by identifying and mapping critical assets across the extended enterprise; using a cybersecurity maturity model to assess the maturity of the control environment; and building a framework that is secure, vigilant, and resilient. After reducing their own cyber risk profiles, utilities can collaborate with peers, governments, suppliers, and other industrial sectors to share intelligence, participate in practice exercises, develop new standards and frameworks, and pilot new technologies. New tools are increasingly available, and the capability to monitor networks in real time, discover threats, and address them is also advancing rapidly. If electricity utilities seize these opportunities, they can reduce risk significantly for themselves, the power sector, and, given the critical nature of the service they provide, society as a whole.

Power systems are among the most complex and critical infrastructures of a modern digital society, serving as the backbone for its economic activities and security. It is therefore in the interest of every country to secure their operation against cyber risks and threats.

Key vulnerabilities in energy infrastructure that malicious actors seek to exploit, including common security gaps that are created as utilities rely on digitalization to leverage data analytics, artificial intelligence and balance the grid with intermittent renewable energy and distributed power generation. As utilities increasingly adopt business models that connect OT power generation, transmission and distribution assets to IT systems, critical infrastructure is more vulnerable to cyber attacks

Most surveyed global utilities say that cyber threats present a greater risk to critical infrastructure—compared with IT systems—and are concerned with unique industry challenges, including ensuring availability, reliability and safety of electricity delivery. Industry-wide, readiness to address cyber-attacks is uneven and has common blind spots, especially with regards to the unique cybersecurity requirements for OT, and the importance of distinguishing between security for OT and security for IT. This remains a major challenge for many organizations across the industry.

Power systems are among the most complex and critical infrastructures of a modern digital society, serving as the backbone for its economic activities and security. It is therefore in the interest of every country to secure their operation against cyber risks and threats.

Among the findings of this report, several key elements are:

- ⇨ Growth of networks and communication protocols used throughout ICS networks pose vulnerabilities that will continue to provide attack vectors that threat actors will seek to exploit for the foreseeable future. The interoperable technologies created for a shift toward a smart grid will continue to expand the cyber-attack landscape.
- ⇨ Threat actors on multiple fronts continue to seek to exploit cyber vulnerabilities in the U.S. electrical grid. Nation-states like Russia, China, and Iran and non-state actors, including foreign terrorist and hacktivist groups, pose varying threats to the power grid.

A determined, well-funded, capable threat actor with the appropriate attack vector can succeed to varying levels depending on what defences are in place.

- ⇨ Utilities often lack full scope perspective of their cyber security posture. Total awareness of all vulnerabilities and threats at all times is improbable, but without enough cyber security staff and/or resources utilities often lack the capabilities to identify cyber assets and fully comprehend system and network architectures necessary for conducting cyber security assessments, monitoring, and upgrades.
- ⇨ Some utilities require financial assistance in creating or shaping their cyber strategy, both to meet regulatory standards and for business security. While regulatory requirements for the bulk electric system are clear about what compliance outcomes utilities should achieve, utilities desire guidance about how to best achieve cyber security outcomes, as well as how to develop active defenses capable of addressing a highly targeted cyber-attack.
- ⇨ The assortment of regulatory standards and guidelines applicable to utilities regarding cyber security practices produces varied methods of adoption. This causes some overlap and confusion in jurisdictional applicability (federal vs. state) and has produced a wide range of differing practices by utilities in meeting standards, making an evaluation of industry-wide best practices difficult.
- ⇨ Utilities expect more qualitative, timely threat intelligence from existing federal information sharing programs. Utilities also seek clarity about the conditions of information sharing programs based on new national cyber security policy.

It is imperative to delve into the security, privacy & trustworthiness aspects and implications of the new paradigm of "Critical Information Infrastructure" and "Internet of Things" that the pervasive computing has enabled, thus raising new challenges for the 'IT & Communication Security' Development & Evaluation Eco-system. Hence, needing a new rigorous and vigorous effort in developing a "Comprehensive Cyber Security, Resilience & Trustworthiness" Strategy Framework encompassing all the critical domains and Stakeholders classifications and their respective imperatives from Cyber Security & Resilience & Trustworthiness Perspective.

Every company in a cyber security domain has set up transparency centres that might help them and their client, but not for society or the nation at large. We need a consolidated transparent centre at the national level where all the things can be looked at together simultaneously lawfully.

In India, the private sector has started playing a significant role in operating critical information infrastructure, particularly in power, transportation and healthcare. It is now more necessary than ever before to take cognizance of new directions and shifts in policies across the world.

It will be necessary to undertake a thorough risk and gap assessment of the current cyber resilience of India's various economic sectors, as well as that of the governance structure that enforces and manages the cybersecurity policy and framework. National cybersecurity strategic initiatives such as the National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC) and the Computer Emergency Response Team (CERT) need to be strengthened manifold and reviewed for their effectiveness in addressing the national imperatives comprehensively.

A national cybersecurity strategy outlines a country's cybersecurity vision and sets out the priorities, principles and approaches to managing cybersecurity risks. However, India has

only a National Cyber Security Policy (2013), which also is long overdue for comprehensive revision and update.

Considering the current and future evolving Cyberthreat Landscape, it would be absolutely critical to have Two National Documents:

iii. A concise yet comprehensive 'National Cybersecurity Strategy' that sets clear, top-down directions to enhance the cyber resilience for the ecosystem that includes government, public and private sectors, the citizenry, and also addresses international cyber issues.
iv. A separate 'National Cybersecurity Policy' based on principles laid down in 'strategy'. It must be outcome-based, practical and globally relevant, as well as based on risk assessment and understanding of cyberthreats and vulnerabilities. The security framework must include the compulsory testing of cyber products, infrastructure skill capacity development, responsibilities of entities and individuals, and public-private partnerships.

An accountable integrated national cybersecurity apparatus to be structured/restructured and it must be provided clear mandates and be empowered adequately. It must be able to supervise and enforce policies across India, including policies regulated by independent regulators.

NATIONAL TRUST CENTRE

As per recommendations of Telecom Regulatory Authority of India (TRAI) on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" released on 5th September 2017 National Trust Centre (NTC) must be set up without any further delay.

This NTC must be geared up to undertake the Security Testing and Evaluation comprehensively including but NOT limited to Devices, Systems, Networks, Application & System Softwares, Firmwares, Communication Stacks to ensure that the deployed Devices, systems and solutions are completely Trustworthy.

National Charter of Trust:

Following the example of "Charter of Trust" founded in 2018 by a group of Global Technology Vendors. India needs its own National Charter of Trust to develop an ecosystem of Trustworthy vendors that Electricity Utilities and other Critical National Infrastructure agencies can TRUST absolutely by establishing the best practices in the domain of cyber security that are globally harmonized in Standards, strategy, innovation, certification, transparency and all other core characteristics required to build an absolutely trustworthy ecosystem.

Improving cyber safety and resilience requires all stakeholders to act together at scale and in a coordinated way, including governments, the engineering profession, operators of critical infrastructure and other systems, and developers of products and components. The evolving nature of the challenges will require continual responsiveness and agility by governments and other stakeholders.

The only approach would be to adopt top-down approach to standardization starting at the system or system-architecture rather than at the product level. We need to Study & Analyze the diverse Use Cases, Applications and corresponding Stakeholders & their respective requirements to understand their respective Characteristics and concerns. Then develop a Granular Smart Grid Architecture and then develop a Cyber Security Architecture mapping all the security, privacy, safety, resilience characteristics with the Granular Smart Grid Architecture.

The only approach would be to adopt top-down approach to standardization starting at the system or system-architecture rather than at the product level. We need to Study & Analyze the diverse Use Cases, Applications and corresponding Stakeholders & their respective requirements to understand their respective Characteristics and concerns. Develop a Granular Smart Grid Architecture followed by developing a Cyber Security Architecture mapping all the security, privacy, safety, resilience characteristics with the Granular Smart Grid Architecture.

* * * * *

REFERENCES:

- Ministry of Electronics & Information Technology - http://meity.gov.in/#
- Ministry of Telecommunication - http://www.dot.gov.in/
- Telecom Engineering Centre, DoT - http://www.tec.gov.in/
- NIST: www.nist.gov
- IEEE: www.ieee.org
- IETF: www.ietf.org
- IEC: www.iec.ch
- ISO: www.iso.org
- TIA: www.tiaonline.org
- BIS: www.bis.org.in
- ITU: www.itu.int
- CEN: www.cen.eu
- CENELEC: www.cenelec.eu
- ETSI: www.etsi.org
- OMA: www.openmobilealliance.org
- GSMA: www.gsma.com
- OneM2M: www.onem2m.org
- OASIS: www.oasis-open.org
- ISA: www.isa.org
- http://www.trai.gov.in/sites/default/files/Recommendations_M2M_05092017.pdf
- http://www.bis.org.in/other/USR_ICT_FSI_V_1_0.pdf
- http://meity.gov.in/content/guidelines-0
- https://www.gsma.com/iot/wp-content/uploads/2019/10/CLP.11-v2.1.pdf
- https://www.csa.gov.sg/news/publications/iot-security-landscape
- https://www.gov.uk/government/collections/secure-by-design
- https://www.internetsociety.org/iot
- https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf
- http://tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20Iot%20M2M%20Security.pdf
- https://www.itu.int/en/publications/Documents/tsb/2017-Trust-in-ICT-2017/mobile/index.html
- https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

The IEEMA Vision Electricity for All and Global Excellence leading to Human Enrichment – is based on the five building blocks viz. Credibility with Stakeholders, Excellence, Global Presence, Environment and Enabling Power to All.

The relevance - Ieema's membership base comprehensively covers the multitude of different aspects of the Smart Grid paradigm. Ieema has been major contributing stakeholder and partner in the Indian electricity ecosystem growth story for more than last six decades and, is in sync with the ground realities of electricity infrastructure deployments. Ieema smart grid division members have extensive pool of Individual and organizational competencies, knowledge base and understanding of Indian Power Systems and Utilities.

Ieema's perspective – Ieema views Smart grid as an integral yet one of the most critical components of a nationwide Integrated Smart Infrastructure. Thus, it believes that its architecture and the framework must not be considered or designed in isolation; rather it must form an integral part of the structured, Nationwide Homogeneous Framework and architecture defined and harmonized to the finest granularity. It must take into consideration the implications of other concurrent infrastructures and/or services running for the consumers/stakeholders to optimize the Life Cycle (Total) cost of all the infrastructures for a given geographical territory.

IEEMA Smart Grid Division Mission Enabling Indian Electricity infrastructure to become resilient, sustainable and secure…

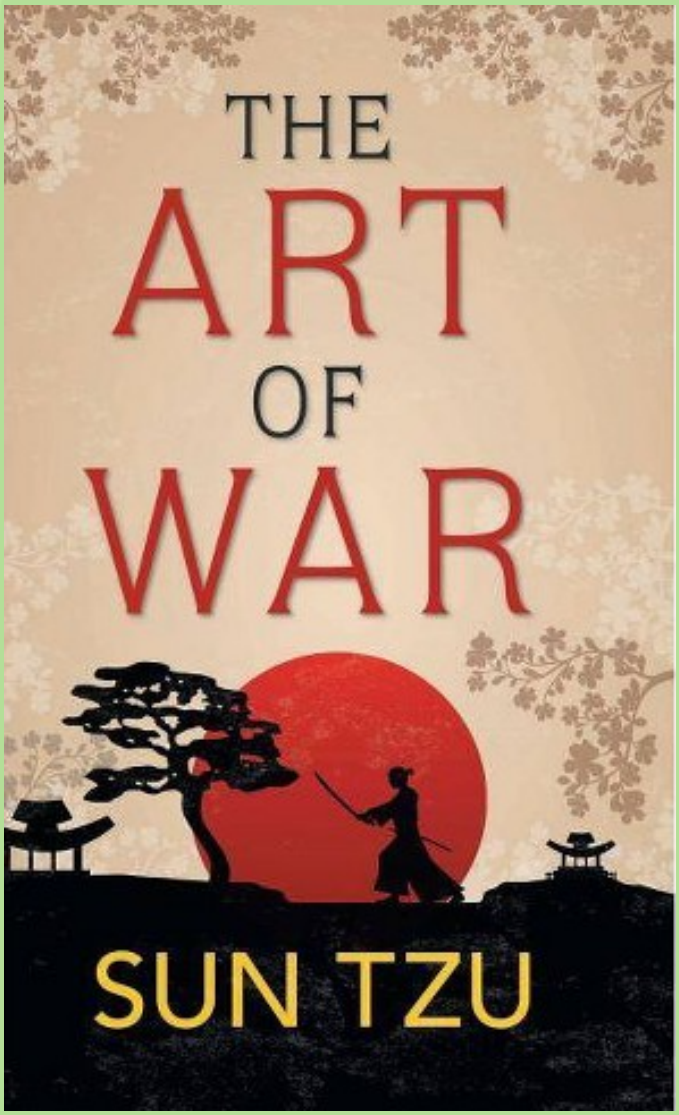
To ensure a comprehensive and structured deployment of nationwide smart grid infrastructure, it's Imperatives to address the current challenges like 'energy security', 'Electricity for all', and 'financial health of distribution utilities' along with 'Modernization of the Grid' in a holistic and sustainable manner.

Objective – Ieema smart grid division by virtue of its comprehensive members base covering the whole spectrum of the electricity infrastructure is uniquely positioned to support, advise and hand hold the government, utilities, policy makers, funding agencies and regulators in their endeavors to implement their restructuring, modernization and up gradation plans. Ieema smart grid division has taken upon itself to proactively support and enable the various government departments, ministries, utilities and other interested stakeholders to implement various relevant initiatives like National Smart Grid Mission (NSGM), National Mission for Enhanced Energy Efficiency (NMEEE), National and System Management (NSM) from IEC, National Electric Mobility Mission (NEMM).

Action Plan - To support the utilities and the government in their respective smart grid initiatives Ieema Smart Grid division has formed Focus Groups in critical areas, which need immediate co-operation amongst the various stakeholders to enable realization of Smart Grid Vision and Roadmap of Ministry of Power. The goal is to reach out to all the direct and indirect stakeholders in various government departments, research and academic institutions, industry associations, regulators and standards developing organizations to have inclusive deliberations and actionable insights to resolving the various challenges being faced by all the stakeholders in their respective endeavors to make our nation 'smart green & secure'. Initial few Focus Groups:

- ⇨ Smart Grid Architecture and Framework FG
- ⇨ Smart Grid Interoperability, Standards and Harmonization FG
- ⇨ Cyber Security FG

Cyber Security : Many Battles & A War



If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle."

Each of these 3 points of 5th Century B.C. book directly applies to the world of Cyber Security.