iNTELEGRID

Newsletter

MAY, 2024

CYBER-ATTACK AND INCIDENT REPORTING

CERT-IN'S SIX HOUR REPORTING RULE FOR CYBER SECURITY

Any person affected by a cyber-security incident is required to mandatorily report such incident to the Indian Computer Emergency Response Team ("CERT-In") if it is of a specified type. With effect the June 27, 2022, the deadline for such reporting has been fixed at 6 (six) hours of the incident being noticed or being brought to the attention of the concerned person.

Obligation to report cyber security attacks

Rule 12(a) of the Cert-In Rules deals with incident reporting, response and information dissemination. Rule 12 requires CERT-In to operate an Incident Response Help Desk on a 24 hour basis on all days including government and other public holidays to facilitate reporting of cyber security incidents. Rule 12(a) reads as follows:

Reporting of incidents: Any individual, organisation or corporate entity affected by cyber security incidents may report the incident to CERT-In. The type of cyber security incidents as identified in Annexure shall be mandatorily reported to CERT-In as early as possible to leave scope for action. Service providers, intermediaries, data centres and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action.

Therefore, Rule 12(a) provides for two types of reporting, which are:

1.Any individual, organisation or corporate entity affected by a cyber-security incident may, at its option and sole discretion, report the incident to CERT-In.

2.If any individual or organization, if affected by a cyber-security incident which is of the nature as detailed in Annexure of the Cert-In Rules, such cyber security incident has to be mandatorily reported to CERT-In as early as possible to leave scope for action.

The time limit for reporting cyber security incidents to CERT-In has been updated to six hours. The new directions, which came into effect on June 27, 2022, mandate that any service provider, intermediary, data center, body corporate, and government organization must report cyber incidents to CERT-In within six hours of noticing such incidents or being brought to notice about such incidents1234. This change aims to ensure a swift response and mitigation of cyber threats, enhancing the overall security of the Indian cyberspace. It's important for all entities to comply with this directive to facilitate timely action against cyber security incidents.

The Annexure to the Cert-In Rules lists the following types of cyber security incidents which needs to be mandatorily reported to CERT-In:

1.Targeted scanning/ probing of critical networks/ systems;

2.Compromise of critical systems/ information;

3.Unauthorised access of IT systems/ data;

4.Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.;

5.Malicious code attacks such as spreading of virus/ worm/ Trojan/ Botnets/ Spyware;

6.Attacks on servers such as Database, Mail and DNS and network devices such as Routers;

7.Identity Theft, spoofing and phishing attacks;

8.Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.

9.Attacks on Critical infrastructure. SCADA Systems and Wireless networks

10.Attacks on Applications such as E-Governance, E-Commerce etc.

The various types of cyber security incidents do overlap and more importantly over a wide array of nefarious activities. The terms used in the Annexure are not defined, but even laypersons would be able to understand most of them. Terms such as "identity theft", "spoofing" and "phishing" are now everyday terms and there is little ambiguity about them. Denial of Service (DoS) and Distributed Denial of Service (DDoS) may not be so well understood and these mean as follows:

1.Denial of Service (DoS):A DoS attack is a type of cyber-attack in which a perpetrator attempts to render a computer resource dysfunctional, so as to make it unavailable for its intended users. This may also be done by temporarily or permanently damaging the services of a host connected to a network.

2.Distributed Denial of Service (DDoS):In a DDoS attack, the perpetrator renders an internet network unusable for genuine users and prevents them from accessing online services and sites available on such network by overflowing the network with internet traffic.

CERT-In's website details the incident reporting mechanism and provides a form to fill in while reporting an incident. The webpage detailing the incident reporting mechanism can be accessed here. The form on CERT-In's website can be accessed here.

Rule 11(1)(a) of the Cert-In Rules state that, "CERT-In shall address all types of cyber security incidents cyber incidents which occur or are expected to occur in the country".

Impact of new deadline on incidents prior to June 27, 2022

The new 6 (six) hour deadline does not have retrospective effect and will apply only to cyber security incidents that take place on or after June 27, 2022.

However, new 6 (six) hour deadline has exposed CERT-In's thought process and it is now clear that CERT-In believes that it is possible for every organisation affected by a cyber security incident to report such incident to CERT-In within 6 (six) hours of noticing such incident. In light of this, it is interesting to see how CERT-In will view cyber security incidents that took place prior to June 27, 2022 and were required to be reported to CERT-In under the 'as early as possible standard', but were reported to CERT-In without undue haste.

Consequences of non-compliance with reporting obligation

PENALTY FOR NON-COMPLIANCE

The Cert-In Rules do not prescribe any penalty for breach of the reporting obligation in Rule 12 of the Cert-In Rules. However, Section 70B(7) of the IT Act provides that any service provider, intermediary, data center, body corporate or person who fails comply with any direction issued by Cert-In shall be punishable with imprisonment for a term which may extend to 1 (one) year or with fine which may extend to Rs. 1,00,000 (Rupees one lac) or with both.

Preventing cyber-attacks and safeguarding patient data requires diligence, security investment, and proactive measures. Let us hope that conditions in India would also get better with the enactment of the DPDP Act.

HEALTHCARE IN INDIA IS UNDER ASSAULT: REPORT THE INCIDENTS TO CERT In, ELSE IT IS PUNISHABLE

A CEO of a hospital should be well-versed in the incident reporting process related to cyber-attacks. A hospital CEO plays a crucial role in ensuring effective incident reporting related to cyberattacks.

The process involves verifying and gathering incident details, using secure communication channels, and involving third parties in serious cases. Cyber terrorism, defined under Section 66F of the Information Technology Act, 2000, refers to acts with the intent to threaten India's unity, integrity, security, or sovereignty. If a cyber-attack is suspected to be state-sponsored or from another nation, the hospital should promptly file an FIR under Section 66F. Section 66F prescribes punishment for cyber terrorism, including imprisonment that may extend to life, to deter acts that threaten national security or disrupt essential services.

Failing to report a cyber-attack to CERT-In, especially one of such severity as the attack on a hospital, is indeed a violation of the legal requirements under the Information Technology Act, 2000. According to the directions issued under Section 70B(6) of the IT Act, service providers, intermediaries, data centers, body corporates, and government organizations are required to report cyber security incidents to CERT-In within six hours of noticing such incidents or being brought to notice about such incidents[12].

If the attack, involving the theft of a large volume of patient data, the hacking of critical medical software, and the disruption of treatments, are significant cyber security incidents. Not reporting this incident to CERT-In could result in legal consequences, including imprisonment of up to one year and a fine which may extend to 1 lakh rupees.

Therefore, it is crucial for the affected hospital to comply with the reporting requirements to avoid legal repercussions and to ensure a coordinated response to the cyber-attack.

Digital Personal Data Protection (DPDP) Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, is an essential piece of legislation for hospitals and other healthcare facilities. The DPDP Act's goal is to protect personal data, especially sensitive health information. Hospital CEOs must be aware of these standards in order to ensure patient confidentiality and compliance. The Act mandates that express consent be acquired before processing personal data. CEOs of hospitals need to understand the regulations controlling the collection, use, and sharing of data. If hospitals don't comply, they risk fines. CEOs must be aware of the potential legal consequences of managing data improperly. CEOs can implement robust data security protocols by comprehending the Act. Hospitals need to protect patient data against cyber-attacks and security lapses. In conclusion, patient trust, regulatory compliance, and effective data management depend on hospital CEOs having a solid understanding of the DPDP Act.

Cyber-attacks on Major Public Sector Hospitals in India

Cyber-attacks on hospitals have become a significant concern globally. Healthcare institutions in India are increasingly being targeted by hackers due to the vast amounts of sensitive patient data held by these institutions.

The country's push for digitization has increased the potential attack surface for hackers, as healthcare systems become more connected. Resource constraints, outdated legacy systems, ransomware attacks, and regulatory compliance make public healthcare an attractive target for cyberattacks. To protect against these threats, healthcare institutions must enhance their cybersecurity measures. Hackers are targeting public healthcare systems in India due to the vast amounts of sensitive patient data held by these institutions. The country's push for digitization

has increased the potential attack surface for hackers, as healthcare facilities often prioritize patient care over cybersecurity. Many healthcare institutions rely on outdated systems that are difficult to secure against modern cyber threats. Ransomware attacks are also a trend where hackers lock systems and demand payment, exploiting the urgency of healthcare services to resume operations. Compliance with regulations like the DPDP Act adds complexity to cybersecurity measures, making public healthcare an attractive target for cyberattacks. The following are a few significant cyberattacks that target public health organizations:

National Institute of Mental Health and Neurosciences, Bangaluru

The cyber incident involving the National Institute of Mental Health and Neurosciences (NIMHANS) on March 23, 2022, was a ransomware attack that significantly impacted the institution's computer systems and data. The attack led to the encryption of numerous computer files and systems, rendering them inaccessible to authorized personnel. This event compelled NIMHANS to file an official complaint with the Bengaluru City Police on April 30, 2022, about a month after the initial attack occurred. Dr. Pratima Murthy, the director of NIMHANS, was responsible for submitting the complaint to the police. However, it took more than a month after the NIMHANS faced a ransomware attack before the administration filed a complaint with the Bengaluru City Police. This will make gathering digital evidence more difficult, which gives cybercriminals—especially insider attackers—a way out. It is not widely understood that the IT Act of 2000 and the Indian Digital Evidence Act. The most important thing is to promptly report incidents to CERT In, which is something that most of the time does not happen and causes concerns. The majority of offenses are not registered in line with the relevant IT Act provisions as a consequence.

After about a month after the cyber-attack, that too was under the severe pressure of the Nimhans Employees' Association only she filed the complaint. In addition, the Employees' Association strongly urged that professionals should be appointed to the organization's IT division. One member of the association said, "There is an IT department that does nothing but exist for show. No cyber safety assessment has been carried out, and no proper cyber professionals have been hired out."

Safdarjung Hospital, Delhi

Safdarjung Hospital is a public hospital in Delhi. In terms of total beds, it is the largest central government hospital in India, run by the Ministry of Health and Family Welfare. The hospital offers a range of medical services and is affiliated with Vardhman Mahavir Medical College. It is well known for providing beneficiaries with lower treatment costs and is backed by several programs, such as CGHS, ECHS, and others. In the heart of New Delhi, it is located on the Ring Road across from the All India Institute of Medical Sciences (AIIMS). Safdarjung Hospital in Delhi experienced a cyber-attack in November, which was reported in December 2022. The hospital's server was down for a single day due to the attack. However, the data was secured, and the impact was not as severe as the cyber-attack on AIIMS Delhi. The hospital's Outpatient Department (OPD) services, which are run manually, were not badly affected. The IT department and the National Informatics Centre (NIC) managed to revive the systems promptly. It was also noted that the cyber-attack was not a ransomware attack, and the hospital's IP was blocked during the incident.

All India Institute of Medical Sciences (AIIMS), Delhi

The All India Institute of Medical Sciences (AIIMS) in Delhi was targeted by a cyber-attack on November 23, 2022. The attack, originating from China, infiltrated 5 physical servers out of 100. The data in the affected servers was successfully retrieved, but the e-hospital service, which manages patient data systems, went offline. The attack led to a rush at AIIMS, causing services to be operated manually. The incident underscored the need for robust cybersecurity measures for institutions handling sensitive data.

Indian Council of Medical Research (ICMR): *Data Breach (81 million people's data on the dark web)*

It was a shocking incident, in which the Indian Council of Medical Research (ICMR) has been breached. The breach occurred on October 9, 2023, exposing sensitive information of 81 million people on the dark web. It could be the largest data breach in India's history. The data breach noticed by the US-based cybersecurity and intelligence firm Resecurity informed that "on October 9, a threat actor going by the alias ‘pwn0001’ posted a thread on Breach Forums brokering access to 815 million 'Indian Citizen Aadhaar and Passport' records". consquently, it has been understood that this massive data breach, details of over 81.5 crore citizens with the Indian Council of Medical Research (ICMR) are on sale on the dark web, which contains crucial information such as Aadhaar and passport details, along with names, phone numbers, and addresses, according to the reports.

Regional Cancer Centre (RCC), Thiruvananthapuram

The Regional Cancer Center (RCC) in Trivandrum has been targeted by a cyber-attack that compromised its radiation treatment software and servers storing health information of over 20 lakh patients. This attack occurred 28/04/2024. As per the reports, the attack halted radiation treatment, demanded a ransom in cryptocurrency worth billions of rupees, and the hackers claimed responsibility via an email abroad and demanded a ransom in cryptocurrency worth billions of rupees. There is suspicion that the attack may have been carried out by Chinese and North Korean hackers. The Cyber Police and Computer Emergency Response Team of Kerala took emergency measures to reload the data which was stored in the magnetic tapes to resume the functionality.

Of course, hospital cyber-attacks have become a major global concern, and incidents targeting **private hospitals** in India are not exempt from this trend. A noteworthy instance involved the online sale of 1.5 lakh patients' personal information from Tamil Nadu's **Sree Saran Medical Center** following a cyberattack. The data breach was discovered by a cybersecurity firm and was traced back to a compromised third-party vendor, **Three Cube IT Lab.** Sensitive data, including names, dates of birth, residences, guardians' identities, and medical information, were among the disclosed files.

Private hospitals in India often conceal cyber-attack details due to privacy concerns, reputation management, operational security, legal and regulatory implications, and negotiation with attackers. Disclosure could damage trust, expose vulnerabilities, and expose potential liabilities and penalties. Confidentiality is crucial for maintaining patient trust, preventing further attacks, and avoiding legal penalties.

These incidents highlights the vulnerability of healthcare institutions to cyber threats and the importance of robust cybersecurity measures to protect patient data. It also underscores the potential consequences of supply chain attacks, where attackers target less secure elements in the supply chain to gain access to larger organizations.

AIIMS stands alone as the sole hospital, among those affected, to have instituted the requisite security protocols to fend off future cyber onslaughts. They have adopted a comprehensive defense-in-depth strategy, reinforced by multiple layers of security measures. Furthermore, they have established a robust 3-2-1 backup strategy to ensure disaster recovery resilience. However, in the wake of the recent RCC cyber-attack, it remains to be seen how they will enhance their post-incident responses to prevent such breaches from recurring. Vigilance and continuous improvement in cybersecurity practices are imperative to safeguard against the ever-evolving threat landscape.

Cyber Sleeper Cells

Sleeper cells are clandestine groups of operatives that remain inactive until activated by their parent organization. They engage in violent actions, often with indiscriminate targeting, such as bombings or assassinations. In cyber terrorism, sleeper cells take on a different form, consisting of skilled hackers, insiders, or cyber operatives. They infiltrate networks, gain access to critical systems, and launch cyber-attacks, disrupt infrastructure, steal sensitive data, or spread propaganda. Front-end operators, the visible face of an organization or movement, engage with the public, spread ideology, recruit new members, or carry out low-level cyber-attacks. Both traditional and cyber terrorism rely on

sleeper cells and front-end operators, with vigilance and intelligence efforts crucial to identifying and countering these threats.

The term “cyber sleeper cells” refers to malicious cyber actors who infiltrate an organization’s network and remain dormant, waiting for the right time to execute a cyberattack. They can be formed within any organisation most secretly and operates in silence. These entities can be particularly concerning within government sectors due to the sensitive nature of the information and systems involved. They steal sensitive data, intellectual property, credentials, and financial information using various techniques like phishing, malware, insider threats, and network reconnaissance. Cyber sleeper cells do not physically steal mobile devices or storage media, other cyber assets, but the traditional sleeper cells do it for their parent organization, and handed over to cyber sleeper cells through them.

Cyber sleeper cells are skilled hackers who infiltrate networks, gain access to critical systems, and disrupt operations. They covertly gain intelligence, study network architecture, identify vulnerabilities, and execute cyber-attacks, stealing sensitive data and financial information. Both traditional and cyber sleeper cells serve their parent organizations' goals, with traditional cells using cyber sleeper cells for information gathering or disruption, while cyber sleeper cells indirectly support traditional cells by weakening infrastructure or stealing sensitive data.

Stealing information from critical infrastructure and providing it to state actors is a serious offense, especially by front-end operators, which is a reality today. These individuals attired as common man, often belong to cybercriminal or state-sponsored groups and carry out cyber-attacks, gathering intelligence, and compromising critical systems. The stolen information can be exploited for espionage, economic disruption, or physical attacks. If these operators hand over the stolen data to state actors, it becomes a matter of national security, allowing them to use it for strategic advantage, cyber warfare, or coercion. Law enforcement must not be the sitting ducks but rather be vigilant against these activities.

CYBER CRIMES: THE PURSUIT FOR FAIR INVESTIGATION & JUSTICE

Recent cyber-attacks have specifically targeted critical infrastructure sectors, including nuclear plants, load dispatch centres, and space agencies, exposing vulnerabilities and underscoring the need for robust protective measures. In this context, the pursuit for fair investigation and justice becomes paramount. Ensuring the security and resilience of critical infrastructure is not only a matter of national interest but also directly impacts public safety, economic stability, and national security.

As India grapples with cyber threats, it must navigate complex legal, technical, and operational landscapes to safeguard its critical systems. This chapter explores the pursuit for fair investigation and justice in cyber-attacks on critical infrastructure in India. It highlights the challenges faced by investigators, prosecutors, and judges in upholding justice in the digital realm. The chapter also discusses the need for tech-savvy judges and lawyers to bridge the gap between legal principles and digital evidence. Vulnerability Assessment and Penetration Testing (VAPT) plays a pivotal role in securing critical infrastructure, but it must be handled with care to ensure security improvements occur without compromising confidentiality. The chapter also discusses a cautionary tale of VAPT and the unpardonable catastrophic lapse of incident reporting. The text encourages readers to navigate the intricate web of investigation, justice, and resilience in the face of cyber threats targeting critical infrastructure. Join us on this journey as we delve into the intricacies of cyber investigations, legal frameworks, and the pursuit of justice in the face of evolving threats.

The Crying Need for Tech-Savvy Judges and Lawyers

The crying need for tech-savvy judges and lawyers cannot be overstated, especially in the context of combating cyber terrorism. Without a deep understanding of technology, our legal system risks being ill-equipped to address the evolving threats in the digital realm. Cyber terrorism poses a severe danger to global security, and it is imperative that legal professionals embrace technological literacy. International cooperation and a global legal framework are essential to prevent cyber terrorism from flourishing in India and beyond.

Cyber security officers in cyber cell play a crucial role in combating cyber threats through technical training, understanding cyber threats, and seamless support. They need to understand network security, forensics, malware analysis, and incident response. Collaboration with other agencies, private sector, and international bodies is essential for shared threat intelligence. They must also understand privacy laws, evidence handling, and ethical dilemmas. In summary, a well-trained and supported cyber cell is essential for effective defense against cyber threats.

In this digital age, cyber law awareness and training are crucial for judges to effectively handle cases related to technology, data breaches, and cybercrimes. Here are some initiatives that focus on providing training to judicial officers:

The Advanced Centre for Research, Development and Training in Cyber Laws and Forensics at the National Law School of India University in Bangalore offers specialized training for judicial officers, public prosecutors, judges, investigative agencies, and cyber security personnel. The center focuses on legal aspects and technical issues related to cyber law, aiming to prevent misuse of technology and enhance law enforcement. Other courses include Digital Evidence for Judges, National Cybercrime Training Centre, UNESCO's Massive Open Online Course on AI and the Rule of Law, and an Online Certificate Course on Cyber Law by the Indian Law Institute.

*The Supreme Court of India recognizes the critical importance of judges and lawyers being tech-savvy. The court emphasized that every judge in India needs to be technologically adept to ensure efficient legal proceedings and adapt to the changing landscape of legal practice. The integration of technology in the legal system enhances efficiency, accessibility, and connectivity within courtrooms, benefiting lawyers, litigants, and other stakeholders. Therefore, staying abreast of technological advancements is crucial for ensuring fair investigation and justice.

Read more at:
*https://economictimes.indiatimes.com/news/india/judges-need-to-be-tech-friendly-supreme-court/articleshow/104223430.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

*https://www.hindustantimes.com/india-news/techsavvy-cji-chandrachud-plays-mentor-to-fellow-judges-insupremecourt-101673519238531.html

SIGNIFICANCE OF VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) plays a crucial role in safeguarding sensitive data and preventing the potentially devastating consequences of data breaches. Let’s delve into why VAPT is considered restricted data, particularly when it comes to critical infrastructure like the National Power Grid.

- Understanding VAPT: Vulnerability Assessment: This step involves identifying potential vulnerabilities in a system, network, or application.
- Penetration Testing: It goes beyond assessment by actively simulating attacks to exploit vulnerabilities and assess the system’s resilience.

Severity Levels: VAPT assessments categorize vulnerabilities by their severity levels. High-severity vulnerabilities demand immediate attention and remediation. Assessing severity helps prioritize actions based on the potential impact.

Types of VAPT: Different types of VAPT focus on specific aspects:

- Network VAPT: Assesses network infrastructure vulnerabilities.
- Application VAPT: Identifies code, design, or configuration vulnerabilities.
- Wireless VAPT: Evaluates wireless network weaknesses.
- Mobile VAPT: Analyzes mobile app and device vulnerabilities.

Impact on Critical Infrastructure: A breach in critical infrastructure can have severe consequences, like attacks disrupting power supply, affecting lives and essential services, and compromising national security. In fact, VAPT for critical infrastructure is severe because it safeguards against vulnerabilities, ensures compliance, and protects essential services. Prioritizing VAPT helps prevent catastrophic consequences.

Why VAPT Is A Restricted Data?

The National Power Grid is a lifeline for a nation, providing electricity to homes, businesses, and essential services. Any disruption can have severe consequences. The power grid relies heavily on interconnected systems, software, and communication networks. Vulnerabilities could lead to blackouts, financial losses, and even endanger lives. The grid contains sensitive data, including operational details, network configurations, and user information. Unauthorized access could compromise its integrity. Protecting critical infrastructure is a matter of national security. A successful cyberattack on the power grid could cripple an entire country. A compromised power grid affects industries, commerce, and daily life. Ensuring its security is vital for economic stability.

In essence, Vulnerability Assessment and Penetration Testing (VAPT) is crucial for ensuring the security and integrity of critical infrastructure. It is essential to protect sensitive data, prevent unauthorized access, and maintain operational efficiency. Disruption to critical infrastructure can have severe consequences on society and the economy. Governments and governing bodies define rules for managing critical infrastructure, and Presidential Policy Directive 21 emphasizes maintaining secure, resilient infrastructure. Techno-legal challenges include managing interconnected components, protecting sensitive data, and detecting false indicators.

If critical infrastructure data is stolen by a criminal/cybercriminal, immediate action is crucial. Report the incident to law enforcement, provide details, notify relevant authorities, invoke legal measures, preserve evidence, mitigate further risks, change access credentials, and assess the impact on security. Collaboration with law enforcement and authorities is essential to address the theft effectively. The role of VAPT in cyber security defenses is essential to assess statistics and risks.

VAPT is a crucial process for identifying potential vulnerabilities in systems, networks, or applications. It involves two main steps: vulnerability assessment and penetration testing. VAPT categorizes vulnerabilities by severity levels, allowing for immediate attention and remediation. Different types of VAPT focus on specific aspects, such as network, application, wireless, and mobile app vulnerabilities. Benefits of VAPT include identifying vulnerabilities, ensuring compliance, and protecting reputation. However, breaches in critical infrastructure can have severe consequences, such as disrupting power grids or compromising national security. Prioritizing VAPT helps prevent catastrophic consequences.

Vulnerability Assessment and Penetration Testing (VAPT) of critical infrastructure especially power grids is a valuable commodity in the dark web, with cyber criminals targeting critical infrastructure, state-sponsored attacks, and historical incidents like Ukraine's 2015 power outage. Cyber-attacks can lead to dark age scenarios, disrupt daily life, economic impact, national security, and the Internet of Energy (IoE). As power infrastructure evolves, cyber criminals find more entry points and a larger attack surface for malicious actors. The potential for Cyber-attacks on power grids is a global concern, highlighting the importance of security measures.

In essence, VAPT is restricted data because it directly impacts national security, economic stability, and the well-being of citizens. Safeguarding critical infrastructure requires rigorous assessments and proactive measures to prevent vulnerabilities from being exploited.

CYBER TERRORISM INVESTIGATION IN UNITED STATES (US)

The United Nations (UN) is focusing on protecting critical infrastructure against terrorist attacks, emphasizing the vulnerability of essential services like

energy facilities and transportation networks. The UN has established an Inter-agency Working Group to address this challenge. International cooperation and public-private partnerships are also being developed to create a global safety net. Key steps include mapping vulnerabilities, cooperation on prevention, and capacity building. The UN Office of Counter-Terrorism (UNOCT) updates the Compendium of Good Practices on the Protection of Critical Infrastructure, providing guidance for safeguarding critical assets.

Investigation teams for critical infrastructure security vary across nations, each with unique strengths and challenges. Notable players include the US, Israel, UK, Germany, Russia, and China. The US has advanced cybersecurity capabilities and a strong focus on protecting critical assets, while Israel has a skilled intelligence community and elite military unit. The UK's National Cyber Security Centre leads critical infrastructure defense, while Germany's Federal Office for Information Security focuses on resilience. Russia's FSTEC and FSB play key roles in cybersecurity, but their reputation is often tied to state-sponsored cyber activities.

US is the nation which faces maximum number of industrial cyber-attacks especially to their critical infrastructure. Colonial Pipeline ransomware attack, Crashed Ohio Nuke Plant Network by Slammer Worm, Taum Sauk Hydroelectric Power Station Failure, Cyber Incident on Georgia Nuclear Power Plant, Penetration of Electricity Grid of US by Spies, etc. are some them. The US power sector has prevented millions of cyber-attacks in 2020- that takes 24/7 commitment.

Presently FBI is the lead federal agency for investigating cyber-attacks and intrusions and also predestined as their number one priority to protect the United States from terrorist attacks. They are committed to remaining agile in its approach to the terrorism threat, which has continued to evolve since the September 11, 2001 terror attacks. The Bureau works closely with its partners to neutralize terrorist cells and operatives here in the United States, to help dismantle extremist networks worldwide, and to cut off financing and other forms of support provided to foreign terrorist organizations. The FBI's cyber strategy is to impose risk and consequences on cyber adversaries. Their goal is to change the behavior of criminals and nation-states who believe they can compromise US networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves. To do this, they use their unique mix of authorities, capabilities, and partnerships to impose consequences against their cyber adversaries. Whether through developing innovative investigative techniques, using cutting-edge analytic tools, or forging new partnerships in their communities, the FBI continues to adapt to meet the challenges posed by the evolving cyber threat.

- The FBI has specially trained cyber squads in all their field offices, working hand-in-hand with inter-agency task force partners.
- The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents.
- With cyber assistant legal attachés in embassies across the globe, the FBI works closely with their international counterparts to seek justice for victims of malicious cyber activity.
- The Internet Crime Complaint Center (IC3) collects reports of Internet crime from the public. Using such complaints, the IC3's Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cybercrime.
- CyWatch is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country.

It is important for people to protect themselves both online and in-person, and to report any suspicious activity they encounter by:

- Remain aware of their surroundings.
- Refrain from oversharing personal information.
- Say something if see something.

The insular nature of today's violent extremists makes them difficult for law enforcement to identify and disrupt before an attack. Many times, a person's family or friends may be the first to notice a concerning change in behaviour that may indicate a person is mobilizing to violence.

The most attractive feature of the US cyber terrorism investigation system is the optimally organised combination of the cyber aware and trained judges, legal experts and cops to comprehend, analyse and act quickly as each moment is very important in cyber terrorism investigation.

In US the following technical experts are usually be the part of such cyber terrorism investigations.

Critical Infrastructure Protection

1. Senior Emerging Technology Security Researcher
2. Senior Director, Critical Infrastructure Protection
3. Senior Critical Infrastructure Analyst
4. Operational Technology Specialist
5. Senior Application Security Engineer

Critical Infrastructure Threat Management

1. Third Party Cyber Risk Program Manager
2. Cyber Sr. Strategic Analyst
3. Cyber Strategic Analyst
4. Cyber Technical Analyst
5. Counter Threat Automation Engineer
6. Counter Threat Automation Engineer (Developer)
7. Counter Threat Automation - Associate Developer
8. CERT Specialist

The cyber-terrorism issues in India also need to be investigated by team comprising appropriate technical experts, Indian IT Act legal experts and techno savvy police officers. The minimum domain expertise requirements for the team investigating critical infrastructure cyber-terrorism issues are listed below.

I. KNOWLEDGE SET REQUIREMENTS

- Deep understanding of computer networking and industrial networking concepts and protocols.
- Knowledge of electronic devices used in ICS control room, industrial process, access control devices, digital cameras, memory cards, modems, hard drives, network components, printers, copiers, storage devices, etc.
- Knowledge of Defense-in-Depth architecture and policies of Critical Infrastructure Protection (CIP),
- Knowledge of Security Operations Center (SOC) and its functions,
- Knowledge of SCADA, ICS and modern automation devices used especially PLC, RTU, DCU, MU, WSN, BCU etc.,
- Knowledge of communication protocols deployed such as IEC 101, 102, 104, IEC 61850, DNP3, Modbus, Profibus, etc.,
- Knowledge of security standards such as ISA 99/IEC 62443, NERC CIP, NIST SP-800-53, ISO/IEC 27001 etc.,
- Knowledge of defining Electronic Security Perimeter (ESP) especially in power sector automation,
- Knowledge of cyber threats and vulnerabilities to automated critical infrastructure, SCADA systems and deployment of IDS, IPS and Firewalls.
- Knowledge of industrial network perimeter security,
- Knowledge of system and application security threats and vulnerabilities,
- Knowledge of insider threat investigations, reporting, investigative tools, laws and regulations,
- Knowledge of physical and physiological behaviors of employees that may indicate suspicious or abnormal activity,
- Knowledge of crisis management protocols, processes and techniques,
- Knowledge of IT act 2000, regulations, policies and ethics related to cyber security,
- Knowledge of cyber security principles and privacy principles,
- Knowledge of crisis management protocols, processes and techniques, and
- Knowledge of covert communication techniques

II. LEGAL PROCEDURE REQUIREMENTS

1. Knowledge for processes for seizing and preserving proper digital evidence,
2. Knowledge of legal governance related to admissibility of digital evidences,
3. Knowledge of processes for collecting, packaging, transporting and storing electronic evidence while maintaining chain of custody,
4. Knowledge of types and collection of persistent data,
5. Knowledge of electronic evident law,
6. Knowledge of legal rules of evidence and court procedures, and
7. Knowledge of judicial process, including the presentation of facts and evidence.

III. SKILL SET REQUIREMENTS

1. Skill in preserving evidence integrity according to standard operating procedures or national standards,
2. Skill in collecting, processing, packaging, transporting and storing electronic evidence to avoid alteration, loss, physical damage or destruction of data,
3. Skill in using scientific rules and methods to solve problems, and

4. Skill in evaluating the trustworthiness of the supplier and product.

IV. ABILITIES REQUIRED

1. Ability to find and navigate the dark web using the TOR network to locate markets and forums.
2. Ability to examine digital media on multiple operating system platforms.

Thus, the United States has a dedicated team for investigating cyber terrorism and protecting critical infrastructure. The FBI leads the investigation, collecting and sharing intelligence, engaging with victims, and working to unmask malicious cyber activities. The National Cyber Investigative Joint Task Force (NCIJTF), led by the FBI, coordinates efforts against cyber threats, focusing on key cyber threat areas. The FBI collaborates with foreign partners and private sector partnerships to seek justice for victims of malicious cyber activity. The US invests significant resources in combating cyber terrorism and safeguarding critical infrastructure.

Revolutionizing Legal Practice in India: The Impact of Generative AI and Large Language Models on Criminal Law

Criminal attorneys put a lot of effort into writing documents and doing manual case law research. Large Language Models (LLMs) for attorneys, however, are now capable of completing these jobs far more swiftly and effectively. According to a Goldman Sachs analysis that examined the US legal business in early 2023, up to 44% of the work that attorneys do now may one day be automated by AI tools.

LLMs can be used to enrich precedents in a number of ways, including:

1. Finding pertinent precedents: Artificial intelligence (AI) can be used to search through enormous databases of court records and find precedents that are pertinent to a certain case. Lawyers will no longer need to spend a lot of time and energy manually searching through case law thanks to this.
2. Precedent analysis: AI can be used to find important legal ideas and arguments by analyzing precedents. This can aid attorneys in comprehending precedents more fully and making greater use of them in their own cases.
3. Legal argument generation: AI is capable of producing legal arguments based on prior decisions. This can make it easier and faster for attorneys to create compelling legal arguments.
4. Case outcome prediction: AI is capable of making case outcome predictions based on historical data. This can assist attorneys in making well-informed decisions regarding the course of their cases.

Examples - AI-Assisted CoCounsel from Reuters.

LexisNexis has a Lexis+ AI tool which is a re-trained version of out-of-the-box LLMs

The future of the legal profession is likely to be even more technology driven. As artificial intelligence (AI) and other modern technologies become more sophisticated, they will be able to automate even more legal tasks. Lawyers may become more engaged in prompting and reviewing AI outputs, advising on more complex or emergent matters and building client relationships.

But it's important to remember that technology is just a tool. It can't replace the human touch that is essential to the legal profession. Even terms of the OpenAI API usage policy clearly states that these models should not be used for providing legal services without a review by a qualified person. Lawyers will always need to be able to think critically, solve problems, and communicate effectively.

NEED CYBERSECURITY CONSULTANCY IN YOUR ORGANISATION?

Intelegrid ECC (P) Ltd offer personalized and managed security services, gap analysis, security maturity, risk and cyber vulnerability assessment, **Purdue model security architecture**, **CIE, layered security with DiD and security policy development**, **SCADA, IT-OT segregation and integration, design of digital substations**, **IEC 61850, DNP 3, NERC CIP, IEC 62443 consulting**, and implementation.

In the digital age, cyber security is inextricably linked to our transformative journey. Imagine a digital realm devoid of robust security measures—it stands as precariously as a pyramid without its base, vulnerable to collapsing at the slightest disturbance. In today's dynamic data-driven economy, adaptability is not just an asset but a necessity. For C-suite(CEO, CIO, CFO, etc.) executives—the trailblazers at the helm of innovation—navigating this ever-shifting landscape is akin to taming a wild tiger. It is imperative, therefore, that they arm themselves with the latest cyber security insights from seasoned experts. C-suite leaders seeking to fortify their knowledge with cutting-edge updates on cyber space intricacies and associated legal frameworks are invited to explore Intelegrid. Embark on a journey of empowered security with us. A platform

for research, design, build and maintain cyber security-capable health delivery organizations (HDO), operational technology (OT) and critical infrastructure (CI) with visibility and security.

Published by Intelegrid ECC(P) Ltd. TF3, Galaxy Delight, Trivandrum-12, INDIA.
www.intelegridecc.com, jayamohan@intelegridecc.com, 8547018797, 0471 3577774.