iNTELEGRID

Newsletter

APRIL, 2024

CYBERSECURITY ROLE OF CEO IN HOSPITALS

The role of **CEOs and directors** in hospital cybersecurity is multifaceted and critical. Their responsibilities and impact are:

1. **Understanding the CEO's Influence on Cybersecurity**:
   - **CEOs** play a pivotal role in **cybersecurity strategy** and promoting awareness within the organization.
   - As the highest-ranking executive, the CEO sets the tone for cybersecurity efforts and must prioritize the allocation of resources to address risks.
2. **The CEO's Responsibility in Safeguarding the Organization**:
   - **CEOs** must actively engage in cybersecurity efforts, demonstrating their commitment to protecting sensitive data and mitigating risks.
   - This proactive approach is essential in today's digital landscape, where cyberattacks continue to evolve and pose significant threats to organizations.
3. **Assessing the CEO's Awareness of Cybersecurity Risks**:
   - **CEOs** should regularly assess their understanding of cybersecurity risks.
   - Staying informed about emerging threats, regulatory changes, and best practices is crucial for effective decision-making.
4. **The CEO's Role in Prioritizing Cybersecurity Initiatives**:
   - **CEOs** must prioritize cybersecurity as a strategic imperative.
   - Allocating resources for security measures, incident response planning, and employee training demonstrates their commitment to protection.
5. **Examining the CEO's Online Presence and Vulnerabilities**:
   - **CEOs** should be aware of their online presence and potential vulnerabilities.
   - Cybercriminals may target CEOs directly, using social engineering or other tactics to gain access to sensitive information.
6. **The CEO's Potential as a Target for Cyberattacks**:
   - **CEOs** can be a potential security risk due to their lack of prioritization of cybersecurity and unawareness of their online exposure.
   - Their susceptibility makes them attractive targets for cyberattacks.
7. **The CEO as a Gateway for Breaches: Mitigating the Risk**:
   - **Employee training** is crucial in reducing susceptibility to cyberattacks.
   - Educating employees about risks, threat recognition, and incident response enhances their ability to protect company data.
8. **The CEO's Role in Cultivating a Culture of Security**:
   - **CEOs** should foster a culture of security awareness within the organization.
   - Regular training, communication, and emphasizing the importance of cybersecurity contribute to a vigilant workforce.
9. **Company Obligations: Providing Cybersecurity Training**:

iNTELEGRID

- Organizations have a responsibility to provide **cybersecurity training** for all employees.
- Investing in resources to protect against attacks and regularly updating security measures is essential.

10. **Collaboration and Prevention: Maximizing Cybersecurity Under the CEO's Leadership**:
    - **Collaboration** between organizations and sharing information about cyber threats enhances overall cybersecurity.
    - Regular assessment and improvement of security measures are crucial for proactive prevention and effective response to cyber threats.

Conclusion

In conclusion, hospital CEOs' choices and actions have a big influence on cyber security readiness. 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: EXPOSING VULNERABILITIES

Healthcare data is a prime target for hackers due to its richness, permanence, and potential for extortion. It contains comprehensive personal information, such as name, address, and medical history, which allows hackers to build a more complete picture of an individual's identity. Personal health information (PHI) is hardcoded and unchangeable, making it valuable for extortion or compromise by nation-states or cybercriminal groups. The sensitive nature of health issues makes it a prime target for hackers, making protecting patient data crucial for safeguarding privacy and preventing misuse.

Health data is highly valuable on the dark web due to its comprehensive personal information, high market price, diverse use cases, and complexity. Health records, including names, addresses, Social Security numbers, medical histories, and insurance details, are hard-coded and constant, making them more valuable to threat actors. They are sold for $250 to $1,000 per record on the dark web, indicating the demand for health data. Criminals exploit health data for identity theft, tax fraud, exortion, and fraudulent medical services. The 21st Century Cures Act and interoperability standards add compliance complexity, making health data a prime target for hackers.

Health data is a valuable resource for pharmaceutical companies, enabling critical applications such as drug discovery, supply chain optimization, personalized medicine, sales and marketing strategies, quality control and compliance, clinical trials optimization, post-market surveillance, and social media analytics. By analyzing patient records, genetic information, and clinical data, companies can identify potential drug targets, design novel therapies, and optimize formulations. Machine learning algorithms process vast datasets to predict drug efficacy and optimize formulations. Health data also aids in supply chain management, ensuring timely availability of medications to patients. It also enables personalized medicine, tailoring treatments to individual needs, and enhancing sales effectiveness. Overall, health data fuels innovation, informs decision-making, and shapes the future of pharmaceutical research and patient care.

Within the intricate realm of hospital cybersecurity, a disconcerting pattern emerges: CEOs and directors—often physicians themselves—display a

disquieting ignorance when it comes to safeguarding against cyber threats. A recent Accenture report casts a stark light on this issue: a staggering 74% of CEOs express apprehension about their hospitals' capacity to thwart or mitigate damage from cyberattacks. Curiously, 96% of these same CEOs acknowledge the paramount importance of cybersecurity for organizational resilience and growth. Yet, therein lies the paradox: many CEOs treat cybersecurity as an afterthought, relegating it to a post-active concern. This shortsighted approach amplifies risk and escalates the costs associated with incident response and remediation.

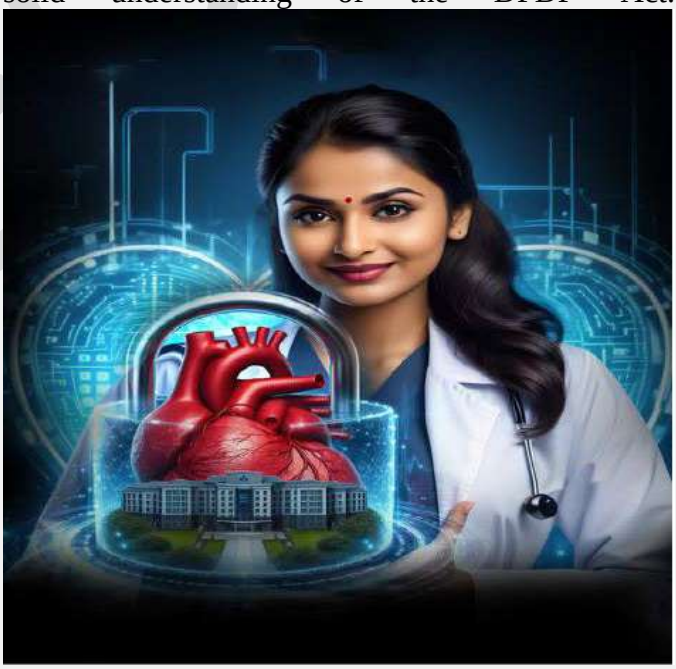
CEOs are in charge of making sure hospitals have strong cybersecurity protocols in place.
Poor information technology security policies, poor procedural and technical safeguards, and a failure to preserve patient data are examples of negligence. Cybercriminals may be able to access hospital systems as a result of such carelessness.

Incident Reporting

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.

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.



INTERRD

The Growing Peril of Healthcare Ransomware

Ransomware groups are increasingly targeting vulnerable remote access systems in healthcare, with several high-profile incidents in recent months. Ransomware attacks can cripple a hospital's ability to serve patients by cutting off access to or manipulating essential technologies and patient data. Hackers can exploit remote systems to divert emergency vehicles, cancel appointments, and in worse-case scenarios, shut down entire facilities.

It's common for hospitals to grant remote access to their networks, including for hybrid or remote employees; for physicians accessing patient records; and for radiologists reading studies etc. Vendors are also given access to remote hospital systems to run financial operations such as bill payments; or to support medical devices, IT systems, or to access & control BMS. Attackers can exploit these entry points—gaining access to and moving throughout the network—if remote access systems are not protected.

The consequences of these attacks can be devastating: vital medical records held hostage, treatment plans in disarray, and potentially deadly delays in care. Each unchecked vulnerability is a threat to patient safety. To grow complacent about cybersecurity in healthcare is to play fast and loose with patients' lives.

Recommendations for healthcare leaders to address ransomware attacks on remote access systems:

- Consider blocking network traffic to internet-facing systems from potentially adversarial countries with which your organization does not conduct business.
- Develop incident response plans that include ransomware contingencies and recovery.
- Do not ignore other attack vectors such as phishing and password compromise.
- Ensure that Internet-facing systems (e.g., remote access systems, VPNs) are configured securely and that security updates are applied.
- Identify who to contact at law enforcement agencies.
- Identify your primary vendor contacts for clinical and IT systems.
- Include downtime and offline procedures for operating without an electronic medical record (EMR) and all other networked medical systems and devices.
- Include policies on patient diversion.
- Maintain backup and recovery methods for all IT systems, and periodically test restoration from backups.
- Prioritize remediation of any systems affected by vulnerabilities listed in the KEV catalog.
- Routinely audit against the CISA Known Exploited Vulnerabilities (KEV) catalog.
- Routinely audit logs and traffic from remote access systems.
- Routinely scan perimeter networks for vulnerabilities. Cybersecurity & Infrastructure Security Agency (CISA) offers vulnerabilities scanning to health delivery organizations (HDOs) at no cost.
- Consult legal counsel in the event of a data breach or ransom demand.
- Consider that payment of a ransom incentivizes future attacks, and that payment is not a guarantee that systems will be restored, either in part or in full.

INFOSEC

CERT In AND INCIDENT REPORTING

As per the Information Technology Act, 2000 (IT Act, 2000), a cyber-incident is defined as: *"Any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy, resulting in unauthorized access, denial of service, disruption, unauthorized use of a computer resource for processing or storage of information, or changes to data or information without authorization."* In essence, a cyber-incident encompasses any event related to cybersecurity that compromises the confidentiality, integrity, or availability of electronic information, systems, services, or networks.

The Indian Computer Emergency Response Team (CERT-In) is the national incident response center for major computer security incidents in India. Its functions include collecting, analyzing, and disseminating information on cyber incidents, forecasting and alerts, emergency measures, coordination of response activities, and issuing guidelines, advisories, and vulnerability notes. It also tracks security threats, issues security alerts and advisories, conducts security workshops and awareness programs, promotes security best practices, and collaborates with various stakeholders to enhance India's overall cybersecurity. The Information Technology Act, 2000 (IT Act, 2000) and the Indian Computer Emergency Response Team (CERT-In) together contribute to a safer digital environment.

CII includes systems, networks, and databases vital for a nation's functioning and whose compromise could lead to severe consequences. The Indian Computer Emergency Response Team (CERT-In) plays a crucial role in incident reporting related to CII.

Once court directions are issued, the police are responsible for reporting cyber incidents to the appropriate authority when an FIR is registered under Section 66F of the Information Technology Act, 2000. They should gather evidence, identify suspects, and pursue legal action. Reporting the incident to CERT-In is mandatory part of the investigative process. Collaboration between the police and CERT-In is essential for enhancing overall cyber security and contributing to a safer digital environment.

Reporting channels include email, helpdesk, and fax. Incident reports should include details such as the time of occurrence, affected system/network information, observed symptoms, and technical details. CERT-In verifies the report's authenticity and goes through stages like triage, incident response, and recovery. The Research Analysis Wing (RAW) and National Investigation Agency (NIA) collaborate with CERT-In and law enforcement to investigate cyber terrorism incidents.

An FIR (First Information Report) registered under Section 66F of the Information Technology Act (IT Act) requires an investigation officer to follow specific procedures, including mandatory reporting to the Indian Computer Emergency Response Team (CERT-In). CERT-In handles cybersecurity incidents in India and provides support and advice but does not physically deploy members to incident sites. The investigation officer should collaborate with relevant agencies such as the NIA and RAW to investigate cyber terrorism cases and ensure national security. Reporting to CERT-In is crucial for effective

INTELORD

incident handling and collaboration with investigation agencies enhances the overall response to cybercrime incidents.

In the event of a complaint or litigation filed against a cyber-attack/breach on critical infrastructure, the **first step** taken by the relevant authority should indeed be to **report the incident to CERT-In**. CERT-In plays a crucial role in handling and mitigating cyber security incidents in India. Whether it's **law enforcement officers (COPs)** or **Courts**, mandatory reporting cyber-attacks on critical infrastructure to **CERT-In** is indeed a crucial step to ensure the genuineness of the crime or litigation. By involving CERT-In, authorities can access expertise, collaborate with other agencies, and follow established protocols for handling such incidents. Filing an FIR is crucial for law enforcement and evidence collection in cyber-attacks on critical infrastructure. It treats the attack as a criminal offense, allowing necessary action. Reporting to CERT-In, a national organization specializing in cyber security, provides expertise, guidance, and coordination during incident response. Both steps are essential for timely intervention and legal proceedings, with authorities often reporting to both simultaneously.

Belated incident reporting to the Indian Computer Emergency Response Team (CERT-In) can have significant consequences, including legal and regulatory implications, delayed incident response, increased impact on systems and networks, missed threat intelligence sharing, reputational damage, loss of evidence, and impact on national security and economy. Non-compliance with reporting requirements may result in legal penalties or fines, as mandated by the Information Technology Act, 2000. Organizations should prioritize reporting within the stipulated timeframe to mitigate risks and protect the digital ecosystem. Legal analyses and guidelines on CERT-In's reporting rules can provide further details.

National security is put at risk when important incidents are kept secret. A catastrophic event might jeopardize defense systems, interrupt vital services, or put populations in danger. Inadequate reporting could result in fatalities and tangible harm to vital infrastructure. A cyberattack on transportation or electrical grids, for instance, might have disastrous effects. A major national disaster has an impact on the economy. Events that go unreported could cause protracted disruptions that impact trade, enterprises, and the stability of the financial system. Public confidence in institutions and the government is damaged by secrecy. Sustaining the public's trust requires openness and prompt reporting. Incidents that are kept under wraps could result in accountability, questions, and legal investigations. Political figures and groups could come under investigation for carelessness. International relations are impacted by hidden calamities. Transparency and cooperation are expected during times of crisis by neighboring countries and global partners. Better readiness and preventive measures are made possible by timely reporting. CERT-In can improve overall cyber resilience, coordinate responses, and send out notifications.

INTEGRID

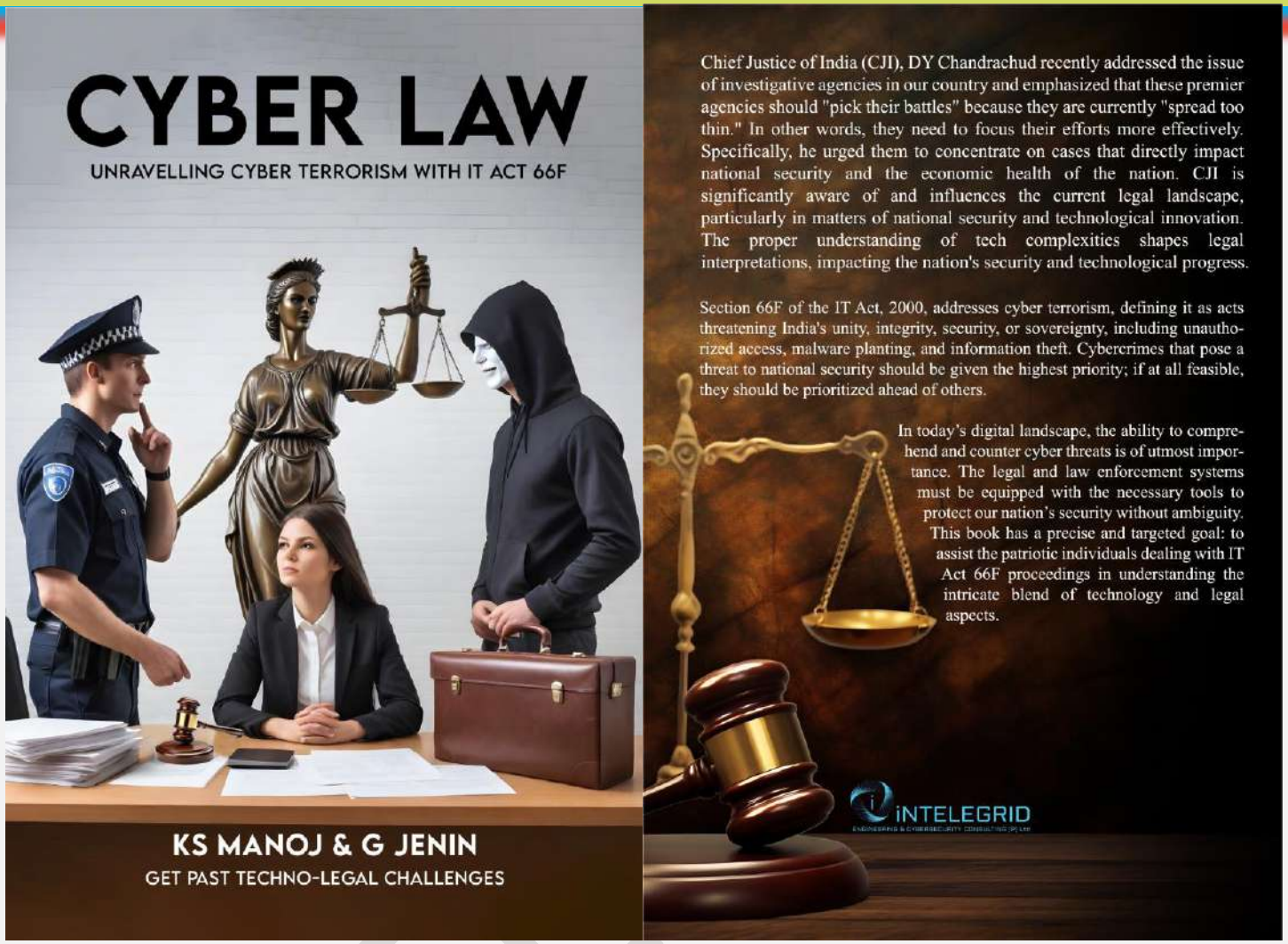
Published by Intelegrid ECC(P) Ltd. TF3, Galaxy Delight, Kesari Lane, Trivandrum-12, INDIA.
www.intelegridecc.com, jayamohan@intelegridecc.com, 854761 1741, 8547018797, 0471 3577774.

SECURING THE LIFELINE: AIIMS' RESPONSE TO CYBER TERRORISM

In response to the cyber-attack on the All India Institute of Medical Sciences (AIIMS), several **remedial measures** have been taken to enhance security and prevent further incidents. And they are:

1. **Network Segmentation**: AIIMS has implemented network segmentation to isolate critical systems and sensitive data from potential threats. By dividing the network into smaller segments, they can limit lateral movement for attackers and reduce the impact of breaches.
2. **Endpoint Hardening**: Strengthening endpoints (such as computers, servers, and devices) by applying security configurations, regular updates, and patches. This helps prevent vulnerabilities that attackers might exploit.
3. **Firewall Policies**: AIIMS has reviewed and tightened its firewall policies to control incoming and outgoing traffic. Properly configured firewalls can block unauthorized access and protect the network.
4. **Regular Software and System Updates**: Keeping all software, operating systems, and applications up-to-date is crucial. Patches often address security vulnerabilities, so timely updates are essential to prevent exploitation.
5. **Security Audits**: Regular security audits and vulnerability assessments help identify weaknesses in AIIMS' systems. These audits allow them to address any gaps promptly.
6. **Employee Education**: Creating awareness among staff about cyber threats, phishing, and safe practices is essential. Training employees to recognize suspicious emails, avoid clicking on malicious links, and follow security protocols can significantly reduce risks.
7. **Effective SIEM Solution**: Implementing a Security Information and Event Management (SIEM) solution helps monitor and analyze network activity. It detects anomalies, alerts administrators to potential threats, and facilitates incident response.

Remember that cybersecurity is an ongoing process, and AIIMS must remain vigilant, adapt to emerging threats, and continuously improve its defenses to safeguard sensitive patient data and critical systems.



https://www.amazon.in/dp/B0CW1KVQ67

Available in Amazon

CYBER LAW: Unravelling the Cyber Terrorism with Section 66F of the IT Act" is a comprehensive book that delves into the complex world of cyber terrorism, legal frameworks, and techno-legal investigative challenges. It covers key topics such as the 66 F of IT Act 2000, investigation challenges of cyber attacks on critical infrastructure, the Indian Digital Evidence Act, safeguarding critical infrastructure, the far-reaching impact of cyber-attacks, raising awareness and preparedness, investigating critical infrastructure cyber-attacks, the current cyber threat landscape, and the pursuit for fair investigation and justice.

The book emphasizes the importance of raising awareness among investigation officers, lawyers, and judges, enhancing cyber resilience, and promoting digital forensics, incident response, and collaboration. It also highlights the need for agility and adaptability in the cyber threat landscape. . This book has a precise and targeted goal: to assist the patriotic individuals dealing with IT Act 66F proceedings in understanding the intricate blend of technology and legal aspects.

Embracing Change: The Paradox of Learning and Resistance

The AIIMS cyber-attack has sparked increased awareness among Indian hospitals, prompting a focus on robust cybersecurity measures. Hospitals are ramping up their cybersecurity infrastructure, with demand increasing 10x to 15x since the attack. Experts propose management solutions that integrate cybersecurity into business and patient care, and government agencies are urged to comply with compliance requirements and establish secure policies.

The cyber-attack on AIIMS has indeed served as a wake-up call for hospitals across India. The incident has underscored the critical need for robust cybersecurity measures in the healthcare sector. Here's how hospitals in India are responding:

- **Increased Awareness**: The widely-publicized AIIMS cyber attack has heightened awareness among hospital executives, prompting a sharper focus on security solutions[1].
- **Strengthening Infrastructure**: Hospitals are ramping up their cybersecurity infrastructure, with some reporting a 10x to 15x increase in demand for security solutions since the AIIMS attack[1].
- **Management Solutions**: Experts have proposed management solutions that integrate cybersecurity factors into business and patient care to meet acceptable standards[2].
- **Government Involvement**: Government agencies involved in healthcare are urged to abide by compliance requirements, create awareness about cyber threats, and set up secure policies[3].

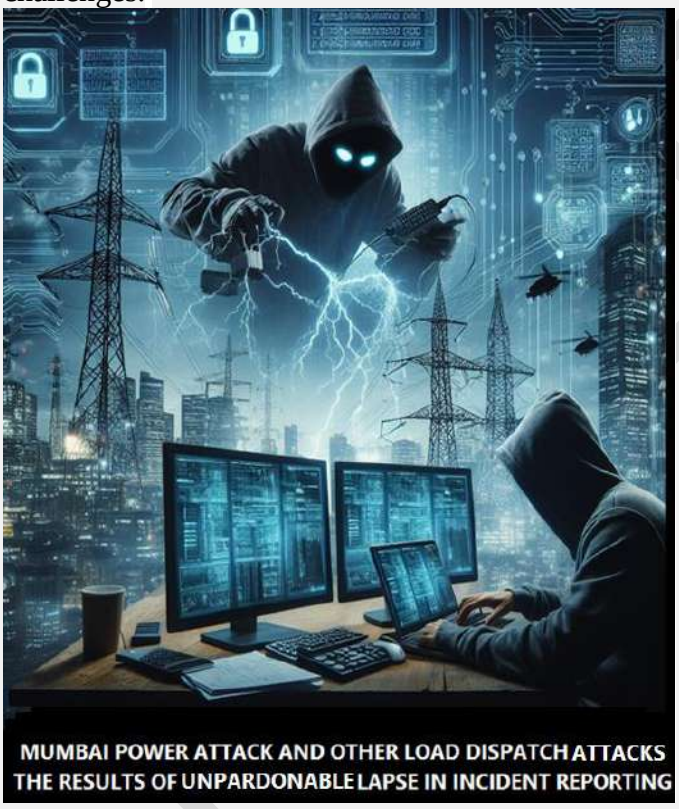
These steps indicate a concerted effort to prevent similar incidents in the future and protect the sensitive data of patients and healthcare workers. It's a positive sign that the healthcare industry is taking serious strides towards improving cybersecurity in light of the AIIMS cyber-attack.

Though, the increasing number of cyber-attacks highlights the importance of cybersecurity, many hospitals, often hesitate to adopt cybersecurity measures due to budget constraints, lack of expertise, underestimation of risks, and complexity of implementation. The cost of a cyber-attack can far exceed the investment in preventive measures, affecting patient trust and institutional reputation. The healthcare sector must collectively work towards creating a secure digital environment to protect against such threats. Indian hospitals must conduct annual cybersecurity audits.

INTERPID

An Indefensible Catastrophic Lapse of Incident Reporting

The **Mumbai power outage** in **2020** was a significant incident that affected the city and its surrounding areas. The power outage in Mumbai on October 12, 2020, caused significant disruptions to transportation, traffic, and business operations. Trains and metro services halted, affecting daily commuters. Traffic signals failed, leading to traffic congestion and heavy road jams. Businesses faced disruptions, and hospitals had to switch to emergency power supply to continue critical medical services. Essential services, such as emergency response units and communication centers, faced challenges.

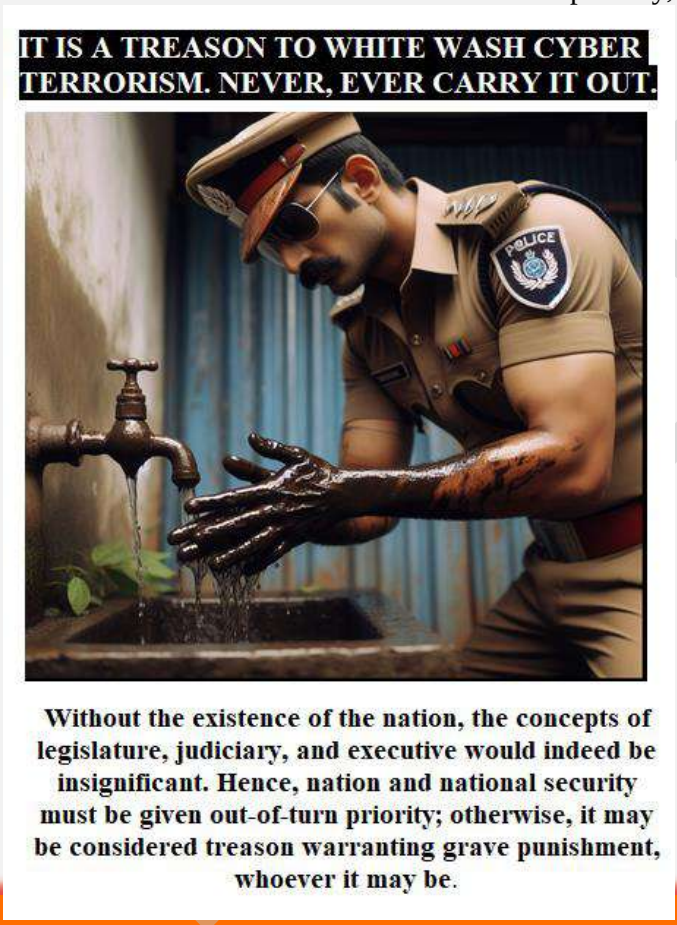


Under Section 70B (6) of the Information Technology Act, 2000, the specific reporting requirements for cyber incidents to CERT-In are clearly specified. Yet, it's still unclear why the authorities chose not to disclose or manipulate the information of power grid attack, despite the court's direction, but it's possible that the Mumbai power attack and other load dispatch center cyber-attacks could have been prevented if the situation had been thoroughly looked into. Here are some potential scenarios:

- Early Detection and Mitigation: Had the compromised VAPT details been promptly detected and acted upon, the vulnerabilities in the R APDRP SCADA/DMS systems might have been patched or remediated. Timely intervention could have prevented the attackers from exploiting these weaknesses during the power outage.
- Enhanced Security Measures: An investigation could have led to strengthened/implemented security protocols NERC CIP without compromise. Authorities might have implemented additional layers of protection, such as intrusion detection systems, access controls, end point security, network architectural flaws, ESP, and network segmentation. These measures could have thwarted any attempts to infiltrate the critical infrastructure.
- Increased Vigilance: Knowledge of the compromised VAPT details would have put the MSEB and other SEBs on high alert. Regular monitoring and proactive threat hunting could have been initiated. Suspicious activities or anomalies might have been detected earlier, allowing for timely action.
- Collaboration and Information Sharing: An investigation would likely involve collaboration with cybersecurity experts, government agencies, and international bodies. Sharing insights and threat intelligence could have led to a more comprehensive understanding of the threat landscape.
- Public Awareness and Preparedness: Transparency about the breach could have raised awareness among other critical infrastructure operators. Preparedness drills, scenario-based training, and crisis management protocols might have been put in place.
- Attribution and Deterrence: Investigating the attack could have led to attribution—

identifying the perpetrators. Knowing the source of the attack could serve as a deterrent and enable legal action against the responsible parties.

Deliberate hiding of cyber breaches by the cops raises serious legal concerns. Reporting cyber incidents promptly is crucial for preventing further harm and ensuring accountability. In India, there is a mandatory reporting requirement for certain cyber incidents, such as the National Cyber Crime Reporting Portal and CERT In. Failure to report promptly can have legal implications. Deliberate hiding and misdirecting of incidents especially by the law enforcement could constitute obstruction of justice or misconduct, specifically if it impacts critical infrastructure like the power grid. Legal consequences include obstruction of justice, negligence, conspiracy, and exacerbated situation. Authorities must ensure transparency, accountability, and timely reporting to prevent further harm and protect society.



In essence, the failure to promptly report the incident, particularly by law enforcement, resulted in significant and catastrophic incidents. Obviously none other than this negligence directly contributed to the attacks on the load dispatch centre. Intentionally concealing a cyber-breach incident, especially when it leads to severe consequences, is unacceptable and could potentially be considered a criminal act. Authorities must prioritize transparency, accountability, and timely reporting to prevent further harm and safeguard society. Clearly, this incident reporting failure is inexcusable and necessitates proactive measures to prevent similar incidents in the future.

Unified Threat Management (UTM) and Hospital Security

Unified Threat Management (UTM) systems are generally not considered suitable for OT-IT segregation and integration in hospitals due to several factors such as:

1. **Complexity and Specialization**: OT environments are complex and often use specialized protocols and devices that may not be fully supported by UTM systems. UTMs are typically designed with IT security in mind, which can lead to gaps in protection when applied to OT networks.
2. **Different Security Objectives**: The primary goal of IT security is data confidentiality and integrity, while OT security focuses on system availability and safety. UTM systems may not adequately address the nuanced requirements of OT security, such as the need for real-time response and minimal system downtime.
3. **Legacy Systems**: Many OT systems are legacy systems that were not designed to be connected to IT networks. UTMs may not be compatible with older OT technologies, and retrofitting them can be challenging and risky.
4. **Network Segmentation Needs**: Effective OT-IT integration requires detailed network segmentation to limit the spread of cyber threats. UTM systems may not offer the granular control needed for proper segmentation and microsegmentation of OT networks.

5. **Cultural and Operational Differences**: There are significant cultural and operational differences between IT and OT teams. UTMs require a unified approach that may not align with the distinct operational practices and responsibilities of OT environments.
6. **Regulatory Compliance**: Healthcare facilities, including hospitals, must comply with strict regulatory standards for cybersecurity. UTM systems may not meet all the regulatory requirements specific to healthcare OT environments.

For these reasons, it's important for hospitals and other healthcare facilities to consider cybersecurity solutions that are specifically tailored to the unique needs of OT environments, ensuring both the protection of sensitive health data and the uninterrupted operation of critical medical devices and systems.

A single entry-level Unified Threat Management (UTM) system for a large hospital's cybersecurity is not at all sufficient due to its inability to address the complex cybersecurity demands of healthcare institutions. A robust, risk-based cybersecurity strategy is crucial for managing sensitive health data and ensuring uninterrupted system operations. Hospitals should seek cybersecurity professionals' expertise to protect patient well-being and data integrity in the digital age.

Role of OT security expert in building Security Capable Hospitals

Consulting with an Operational Technology (OT) cybersecurity expert is crucial when establishing cybersecurity in hospitals. OT cybersecurity experts have specialized knowledge in securing systems that interact with the physical environment, such as medical devices and hospital infrastructure[1]. Their expertise is essential for:

- **Assessing Risks**: Identifying and evaluating potential vulnerabilities within the hospital's OT systems.
- **Designing Security Architecture**: Creating a robust framework that protects against cyber threats while ensuring device availability and reliability.
- **Implementing Best Practices**: Applying industry-standard security measures tailored to the unique needs of healthcare OT environments.
- **Maintaining Compliance**: Ensuring that the hospital's cybersecurity practices meet regulatory requirements.

The need for OT cyber security specialists is critical given the growing integration of IT and OT systems in healthcare and the significant risks associated with safeguarding patient information and safety. However, there is a severe shortage of these specialists in India. Their engagement is a high goal for any hospital's cybersecurity plan since they play a crucial role in protecting against disruptions that could result in serious morbidity or even death.

INTERCOM

Written in an easy tounderstand style, this book provides a comprehensive overview of the physical-cyber security of Industrial Control Systems benefitting the computer science and automation engineers, students and industrial cyber security agencies in obtaining essential understanding of the ICS cyber security from concepts to realization. The Book

-> Covers ICS networks, including zone-based architecture and its deployment for product delivery and other Industrial services.

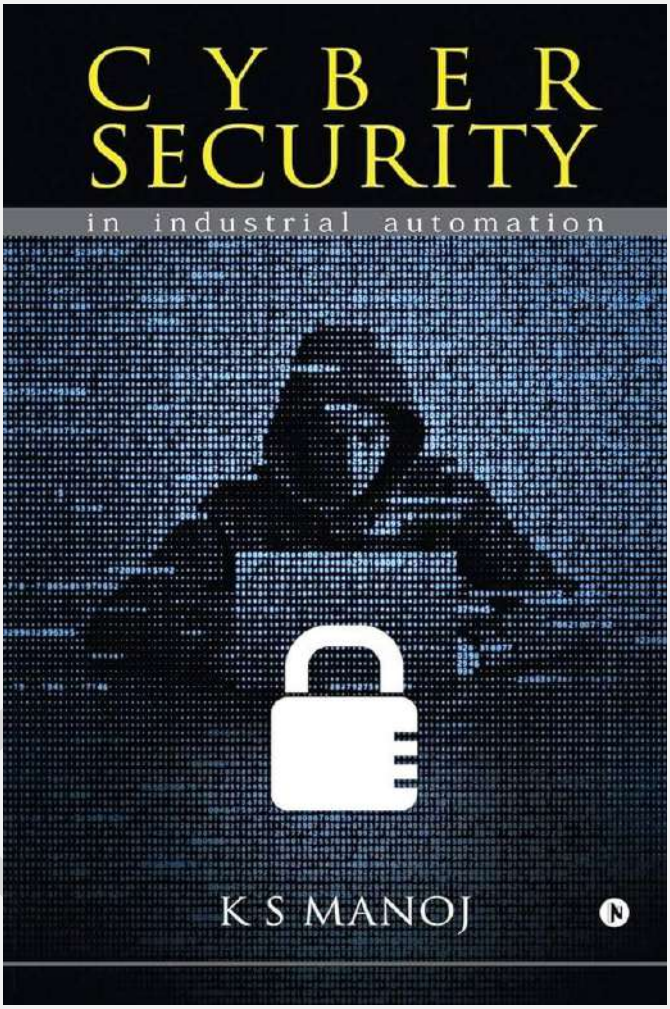
-> Discusses SCADA networking with required cryptography and secure industrial communications.

-> Furnishes information about industrial cyber security standards presently used.

-> Explores defence-in-depth strategy of ICS from conceptualisation to materialisation.

-> Provides many real-world documented examples of attacks against industrial control systems and mitigation techniques.

-> Is a suitable material for Computer Science and Automation engineering students to learn the fundamentals of industrial cyber security.



Available in Amazon, Flipkart, Kobo, Etc.

Protect Your Digital Future

A Platform for Research, Design, Build and Maintain Cybersecurity-Capable Health Delivery Organizations(HDO), Operational Technology(OT) and Critical Infrastructure(CI) with Visibility and Security

NEED CYBERSECURITY CONSULTANCY IN YOUR ORGANISATION?

Intelegrid Virtual CISO consultancy acts as your own Security Engineer

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.

Published by Intelegrid ECC(P) Ltd. TF3, Galaxy Delight, Kesari Lane, Trivandrum-12, INDIA.
www.intelegridecc.com, jayamohan@intelegridecc.com, 854761 1741, 8547018797, 0471 3577774.