iNTELEGRID

Newsletter

February, 2024

Burning Out in Bytes

The Alarming Stress Experiencing on Indian Cybersecurity Professionals

According to a recent Times of India article, over 80% of Indian cybersecurity experts are experiencing dangerously high levels of burnout, which poses a risk to their organizations. It is alarming that Indian cybersecurity professionals have experienced burnout. Let's examine the causes of this occurrence in more detail.

1. **High Demand and Stress**:

Cybersecurity professionals face significant stress due to the constant threat landscape, rapid response demands, skill gap, business continuity at risk, emerging threats, zero-day attacks, compliance with regulations, 24/7 monitoring and incident handling, human factor stressors, and emotional toll. The constant threat landscape, rapid response demands, and scarcity of skilled professionals put organizations at risk. Cybersecurity professionals must also manage compliance with industry-specific regulations, which can result in fines, legal actions, and reputational damage. Balancing technical expertise with effective communication can be stressful, and the emotional toll of constantly thwarting attacks can lead to anxiety, frustration, and burnout.

2. **Weak Security Architecture and Poor Design Expertise:**

Cybersecurity architecture is the design and structure of an organization's security measures, consisting of network segmentation, access controls, firewalls, encryption, intrusion detection/prevention systems, endpoint security, application security, and incident response plans. Layers provide redundancy and resilience, with examples including perimeter, network, host, application, and data layers. A defense-in-depth strategy involves deploying multiple layers of security controls, assuming no single measure is fool proof. Benefits include redundancy, diverse protection, early detection, and resilience. A robust architecture ensures better threat detection and incident handling, with layers like IDS/IPS, endpoint security, and network monitoring identifying anomalies.

The majority of industry 4.0 Indian organizations still use outdated perimeter security techniques to secure their networks. It's assumed that protecting the exterior boundary is sufficient. Nevertheless, current threats can now bypass traditional perimeters (firewalls, gateways) because to lateral movement, insider threats, and phishing. Cybersecurity receives small expenditures from many

WHY CYBER INSURANCE?

K S Jayamohan,
Cyber Insurance Consultant

A cyber insurance policy covers businesses from any financial loss that may arise due to cyber crimes, online data breaches, malware, ransomware, and other digital risks. This policy offers overall protection to your business from data losses, unauthorized access, and various costs such as forensic costs, PR costs when any data breach occurs in your system. Key Features of Cyber Insurance

Covers financial losses caused due to online attacks such as cyber breaches
Plans designed for business entities of all sizes
Covers a variety of costs such as defence costs, investigation costs and other related expenses
What Does Cyber Insurance Cover?
1. Covers costs of lawsuits arising out of data breach, failure to protect sensitive information
2. Covers the cost of any legal liabilities arising against the third party such as:

Private & network security liability protection
Multimedia liability
Reputational liability
IPR Infringement
3. Covers various first-party costs arising due to security breaches or data failures. Some of these costs include:

Business Interruption Costs
Legal and defence costs
Crisis Management Costs and Public Relations Costs
Ransomware Payments
Credit Monitoring to customers due to breach / Notification Cost
Loss of funds due to fraudulent communication
Forensic Expenses
Cyber extortion
Reward expenses
Fines/penalties
Cyber Terrorism

jayamohan@intelegridecc.com

firms. Some businesses either don't know about international standards or consider them to be optional. Outdated Frameworks: Retrofitting antiquated systems to meet modern specifications is challenging. Organizations frequently place a higher priority on compliance than a strong security framework. It can be dangerous to put compliance above a robust security framework since it doesn't provide effective protection and can result in breaches. Risk assessment, comprehensive planning, and strong security procedures should be given top priority by organizations. Unquestioning faith in credentials might be deceiving because they do not imply real-world expertise. Effective risk management and compliance are both ensured by a balanced strategy. In order to analyze security posture beyond certifications, organizations need regularly undertake assessments, move beyond compliance, and adapt to threats.

The shortage of skilled cybersecurity professionals is a pressing issue in India, particularly in the context of Industry 4.0 and securing SCADA systems. This shortage is due to the increased vulnerability of critical infrastructure, the complexity of protecting it, the skill gap, and the industry-specific expertise required. The shortage also impacts proactivity, forcing organizations to be reactive rather than proactive. Urgent measures needed include upskilling, talent acquisition, and collaboration between industry, academia, and government. Protecting critical infrastructure is vital for national security and addressing the cyber-terrorism threat is crucial. Organizations, policymakers, and educational institutions must work together to build a robust workforce capable of safeguarding critical infrastructure.

3. **Complexity of Attacks**:

The complexity of cyber-attacks and resource constraints pose significant challenges for cybersecurity professionals. Advanced techniques, diverse attack vectors, and lateral movement make detection and prevention challenging. Incident response is complex, and resources are limited due to budgets, staff shortages, time constraints, and technology limitations. Balancing security measures with business needs is essential. Organizations must invest wisely, prioritize tasks, and support their teams to manage these pressures effectively.

4. **Skill Gap and Training**:

The skill gap in cyber security is a significant issue, as professionals must stay updated to defend against new threats. Lack of regular training can lead to outdated skills, which can result in missed vulnerabilities and burnout. 24/7 monitoring and incident response are also crucial, as threats don't adhere to office hours. Professionals must investigate, contain, and remediate incidents, which can be time-sensitive and strain their mental and physical health. Organizations must invest in training, support their teams, and prioritize well-being to maintain effective security operations. Cyber threats are constantly monitored and responded to by security teams, who constantly monitor networks and logs. However, they face challenges in investigating, containing, and resolving incidents, which can be time-sensitive and cause stress on mental and physical health.

5. **Balancing Act**:

Indian cyber security professionals face burnout due to a high-pressure environment, resource constraints, lack of training, and the need to balance security with business needs. The challenges include balancing security with business needs, risk assessment, and resource allocation. The high-pressure environment also leads to constant threats, skill gaps, and a critical impact on an organization's reputation, financial stability, and compliance. Resource constraints include insufficient budgets, staff shortages, and time constraints. The emotional toll of constantly thwarting attacks, lack of training, outdated knowledge, and 24/7 monitoring and incident response contribute to burnout. Organizations must prioritize well-being, invest in training, and support their teams to mitigate burnout.

6. **Emotional Toll**:

Indian cyber security professionals face a high-pressure environment, constantly thwarting attacks, which can lead to burnout. The emotional impact of this work is significant, as they must constantly monitor networks, detect anomalies, and respond to incidents. Burnout factors include stress, anxiety, long hours, and negative attitudes towards work and colleagues. Symptoms include exhaustion, cynicism, reduced effectiveness, and health issues. Mitigating burnout involves self-care, work-life balance, peer support, training, and recognition. Organizations must prioritize well-being and support cyber security teams to maintain resilience. To combat high-pressure burnout among Indian cyber security professionals, a holistic approach including regular training, robust security architecture, work-life balance, and community collaboration is recommended.

CYBER-ATTACKS ON OPHTHALMIC HOSPITALS

R RENJITH

Cyber attacks on Opthalmic hospitals like any healthcare institution, pose significant risks to patient data, medical devices, and overall operations. Here are some potential cyber-attacks that ophthalmic hospitals may face:

1. **Ransomware Attacks:** Ransomware attacks involve malicious software that encrypts hospital data, making it inaccessible until a ransom is paid. Ophthalmic hospitals may face disruptions in patient care, scheduling, and access to critical medical records if their systems are compromised by ransomware.
2. **Data Breaches:** Data breaches involve unauthorized access to patient records, including personally identifiable information (PII) and medical histories. Ophthalmic hospitals store sensitive patient data related to eye health, treatments, and surgeries, making them valuable targets for cybercriminals seeking to steal personal information.
3. **Phishing Attacks**: Phishing attacks involve fraudulent emails, text messages, or phone calls designed to trick hospital staff into revealing sensitive information or clicking on malicious links. Ophthalmic hospital employees may inadvertently disclose login credentials or other confidential data in response to phishing attempts, leading to security breaches. Medical Device Compromise: Ophthalmic hospitals rely on specialized medical devices and equipment for diagnostic imaging, surgery, and treatment. Cyber attacks targeting medical devices could disrupt patient care, compromise patient safety, and potentially result in irreversible harm to patients' vision.
4. **Distributed Denial of Service (DDoS) Attacks**: DDoS attacks involve flooding hospital networks or websites with a high volume of traffic, causing system slowdowns or outages. Ophthalmic hospitals may experience disruptions in electronic health record (EHR) systems, imaging platforms, or telemedicine services if they become victims of DDoS attacks.
5. **Insider Threats:** Insider threats involve malicious actions or negligence by hospital employees, contractors, or vendors. Ophthalmic hospital staff with access to patient data or medical systems could intentionally misuse their privileges or inadvertently cause security breaches through careless actions.
6. **Supply Chain Attacks:** Supply chain attacks target vulnerabilities in third-party vendors, suppliers, or service providers connected to hospital networks. Ophthalmic hospitals may be at risk if their suppliers or vendors experience security breaches that compromise the integrity of medical devices, software, or data transmission channels.
7. **Zero-Day Exploits:** Zero-day exploits target previously unknown vulnerabilities in hospital software, operating systems, or network infrastructure. Ophthalmic hospitals may be vulnerable to zero-day exploits if they fail to promptly apply software patches, updates, or security fixes to mitigate emerging threats.

To mitigate the risk of cyber attacks, ophthalmic hospitals should implement robust cybersecurity measures, including network segmentation, encryption, access controls, employee training, threat monitoring, incident response planning, and regular security assessments. By adopting a proactive approach to cybersecurity, ophthalmic hospitals can safeguard patient data, protect medical devices, and preserve the trust of their patients and stakeholders.

Do you know? The following pieces of hardware comprise a digital cloud?

Servers: Servers are the core components of a cloud computing data center. They handle user requests and run virtualized workloads. Servers provide the computational power needed to process data, execute applications, and manage cloud services.

Storage Systems: Cloud computing data centers require robust and scalable storage systems. These systems store and manage vast amounts of data. Storage solutions include various technologies like hard disk drives (HDDs), solid-state drives (SSDs), and network-attached storage (NAS).

Networking Equipment: Networking components play a crucial role in connecting cloud services over the internet. These include switches, routers, firewalls, load balancers, and other devices. Network infrastructure ensures data transmission both internally and externally.

Power and Cooling Systems: Data centers need reliable power sources to keep servers running. Backup power supplies (such as generators or uninterruptible power supplies) prevent disruptions during outages. Efficient cooling systems maintain optimal temperatures to prevent hardware from overheating.

Management Infrastructure: Management software helps maintain and configure the entire infrastructure. It monitors and optimizes resources, data, applications, and services. Deployment software assists in deploying and integrating applications within the cloud. Security Measures:

Security is paramount in cloud infrastructure. Measures include access controls, encryption, intrusion detection systems, and firewalls. Compliance with data laws and regulations is also essential. Remember, these hardware components work together to create a robust and efficient digital cloud environment, enabling businesses to deliver services, store data, and scale seamlessly.

EMR Vs EHR

The difference between **Electronic Health Records (EHR)** and **Electronic Medical Records (EMR)**:

1. **EMR (Electronic Medical Record)**:
   - An EMR is a digital version of the paper charts used in a clinician's office.
   - It contains the **medical and treatment history** of patients within a single practice.
   - Advantages of EMRs include:
     - Tracking data over time.
     - Identifying patients due for preventive screenings or checkups.
     - Monitoring specific parameters (e.g., blood pressure readings, vaccinations).
     - Improving overall quality of care within the practice.
   - However, EMRs have limitations—they don't easily share information outside the practice. Sometimes, patient records need to be printed and physically delivered to specialists or other care team members.
2. **EHR (Electronic Health Record)**:
   - EHRs focus on the **total health** of the patient, going beyond clinical data collected within a provider's office.
   - Key differences:
     - EHRs include information from **all clinicians** involved in a patient's care.
     - They are designed to **share information** with other healthcare providers, laboratories, and specialists.
     - EHR data can be accessed by authorized clinicians across **multiple healthcare organizations**.
     - The information **travels with the patient**, even across different states or countries.

In summary, EHRs provide a more comprehensive view of a patient's health and facilitate seamless communication among healthcare providers.

"WILL THE SMART FRIDGE TELL MY MOTHER THAT I HAD STOLEN THE PUDDINGS?"

Ardent Health Cyber-attack US, 2023

A cyber-attack has shut down emergency rooms in at least three states, a hospital operator warned on November 2023, forcing the organization to divert patients to other facilities. Ardent Health, which oversees 30 hospitals in states across the US, including New Mexico, Texas and Oklahoma, reported it had been targeted by a ransomware attack over the Thanksgiving holiday. The attack had shut down a significant number of its computerized services.

The hospital administrator informed the cyber-attack has affected computer programs that track patients' healthcare records, among others. Later Ardent informed that the ransomware attack had taken its network offline. They also informed that it had reported the issue to law enforcement and retained third-party forensic and threat intelligence advisers. Attacks commonly occur during holiday periods as hackers believe there are fewer security staff on duty. Ardent is believed to be the largest health operator to be hit so far. While there are no cases of patients dying as a result of this attack, studies have shown that there is a link between ransomware attacks on hospitals and increased mortality rates.

Adopt NERC CIP and be secured.

NERC CIP is a crucial security regulation for the electric power industry, ensuring the reliability and security of the bulk electric system (BES). It mandates compliance with standards for utility operators connected to the BES. The regulation mitigates risks to critical infrastructure, standardizes utilities, ensures audits and accountability, requires industry cooperation, and requires continuous improvement. Balancing compliance with effective security practices is essential for resilience.

SMART APPLIANCES

Smart appliances are Wi-Fi-enabled devices that connect to a smart hub, voice command system (such as Google Assistant or Amazon Alexa), or a smart home app. These appliances offer convenience, automation, and remote control. Here are some examples:

1. **Smart Refrigerators**:
   - Receive alerts when you're out of specific groceries.
   - Adjust temperature settings remotely.
   - Some have touchscreens for managing shopping lists and recipes.
2. **Smart Ovens and Microwaves**:
   - Preheat your oven remotely.
   - Control cooking times and temperatures from your phone.
   - Get recipe recommendations based on available ingredients.
3. **Smart Washing Machines and Dryers**:
   - Schedule laundry cycles.
   - Receive notifications when a load is done.
   - Some models even auto-order detergent when supplies are low.
4. **Smart Dishwashers**:
   - Monitor water usage and energy efficiency.
   - Start or pause cycles remotely.
   - Receive maintenance alerts.
5. **Smart Vacuum Cleaners (Robotic)**:
   - Map your home for efficient cleaning.
   - Set cleaning schedules.
   - Some models integrate with voice assistants.
6. **Smart Thermostats**:
   - Adjust home temperature remotely.
   - Learn your preferences and create energy-saving schedules.
   - Some models detect occupancy and adjust accordingly.
7. **Smart Lighting Systems**:
   - Control lights individually or in groups.
   - Set timers or schedules.
   - Change colors and brightness levels.
8. **Smart Blinds and Curtains**:
   - Open or close blinds remotely.
   - Schedule adjustments based on time of day.
   - Some models respond to voice commands.
9. **Smart Coffee Makers**:
   - Brew coffee from your bed or while driving home.
   - Set wake-up routines with freshly brewed coffee.
10. **Smart Air Purifiers and Fans**:
    - Monitor air quality and adjust purification levels.
    - Control fan speed and oscillation remotely.

Remember, smart appliances enhance convenience, save time, and improve energy efficiency. They're a key part of the modern connected home.

STOP CYBER HAEMORRHAGE

G Jenin, Security Analyst and Auditor

Cyber Haemorrhage is a term that denotes a cyber-attack that causes either a breach of patient data or a malfunction of medical devices such as IoMT, surgical robots, etc., which may lead to fatal incidents for patients. Patients who utilize medical devices for their care may be oblivious to the cyber vulnerabilities of these devices, whether they are in the hospital for a routine examination, monitoring their heart rate with a wearable device on a morning jog, or undergoing surgery on the operating table. However, the rapid advances in the use and capabilities of connected health also entail potential risks to cybersecurity. For instance, a cyber-incident affecting a hospital elevator control system may impair patient transportation and delay care. A change in temperature or humidity in the operating theatre may compel procedures to be postponed. Shutting down a blood or organ refrigerator may have dire consequences for patients awaiting a transplant or infusion.

The security and safety of medical devices have emerged as a global healthcare challenge as medical devices have progressed from the initial applications of electricity and radiation to a highly interconnected system of systems with intricate data flows not only among devices but also between devices and hospital IT systems. Clinical engineers recognized that these devices were not only susceptible and arduous to safeguard but also that the security breach of any of them could result in patient harm or impede healthcare delivery, in addition to the conventional security concerns around data confidentiality, integrity, and availability.

Stopping cyber hemorrhage is crucial in today's digital landscape due to rising cyber threats, unique challenges in healthcare, and the need for comprehensive risk assessments. Healthcare organizations handle vast amounts of sensitive data, complex networks, and compliance with regulations. Practical solutions include risk assessments, security awareness, robust defenses, and leadership engagement. Proactive measures, informed leadership, and a holistic approach are essential for safeguarding sensitive data and maintaining healthcare services. Ensuring compliance with regulations and implementing robust defenses is essential for preventing cyber risks.

Digital Innovations in Legacy Hospitals in the AI Era

Digital Innovations in Legacy Hospitals in the AI Era: Retrofitting Challenges

As legacy hospitals embrace digital innovations and integrate AI technologies, retrofitting poses both opportunities and challenges. Let's explore the complexities involved:

Operational Decision-Making:
Digital transformation impacts not only clinical decision-making but also various operational aspects. Hospitals can leverage AI to enhance patient flow management, staffing, scheduling, and supply chain optimization. Improved operational decisions lead to better quality of care and enhanced patient access.

Workforce and Expertise:
Retrofitting legacy hospitals requires expertise in both healthcare and technology. Not every hospital can afford new AI talent or access sufficient data for meaningful algorithms. Collaboration within innovation clusters can benefit smaller organizations.

Balancing Old and New Technology:
Retrofitting involves combining new AI solutions with existing infrastructure. Challenges arise when proprietary solutions from different manufacturers cannot seamlessly communicate. Interoperability and integration are critical.

Financial Constraints:
Deep retrofits can be expensive. Hidden costs, such as Value Added Tax (VAT), further impact affordability. Financial incentives and support schemes are essential to encourage retrofitting.

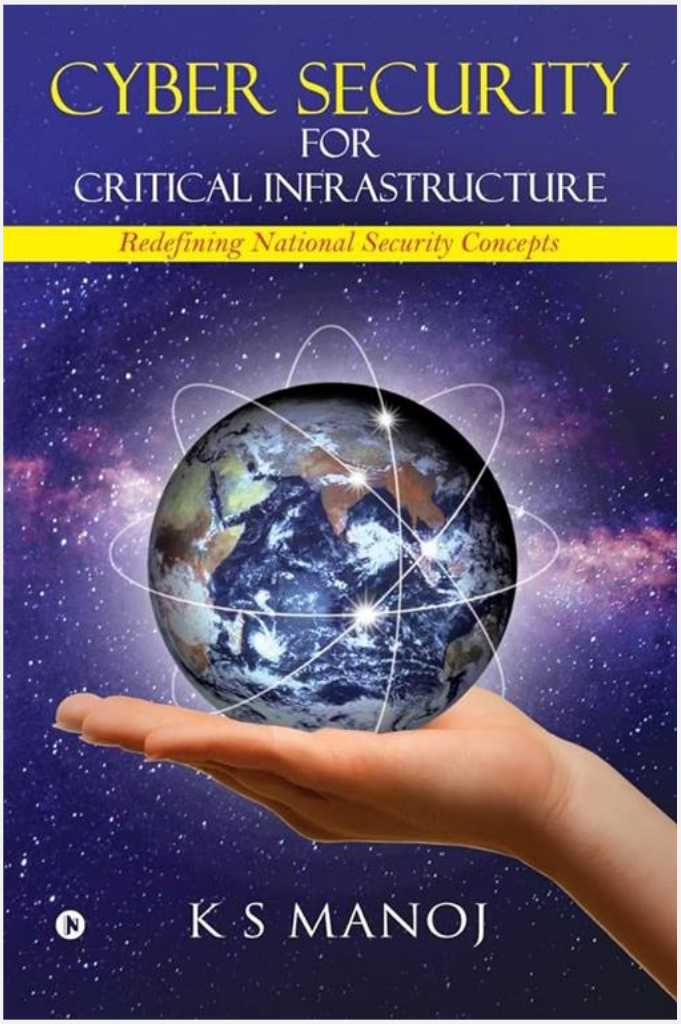
Environmental Impact and Embodied Carbon:
Demolishing and rebuilding properties may seem cost-effective, but it releases embodied carbon. Remodeling existing homes is crucial for sustainability. Retrofitting reduces waste and conserves resources.

In summary, retrofitting legacy hospitals with digital innovations requires a strategic approach, financial support, and collaboration across disciplines. Balancing cost, environmental impact, and patient care is key to successful implementation.

THE PURDUE MODEL

The Purdue Model for Industrial Control Systems (ICS) security provides a structured framework for segmenting networks from corporate enterprise networks and the internet. It divides networks into zones, ensuring a hierarchical flow of data between layers. Layered security involves deploying multiple security controls to protect vulnerable areas, including administrative controls, physical controls, and technical controls. Cyber-informed engineering (CIE) integrates cybersecurity considerations into the design, development, and operation of physical systems, ensuring resiliency and engineering out potential risks. Network segmentation and communication control are also crucial. Regular assessments and audits are necessary to identify vulnerabilities and ensure compliance. Collaboration and training with industry peers and experts can enhance cybersecurity defenses.

Today, cyberspace has emerged as a domain of its own in many ways, like land, sea, and air. Even if a nation is small in land area, low in GDP per capita, low in resources, less important in geopolitics, or weak in the strength of its armed forces, it can become a military superpower if it is capable of launching a cyberattack on critical infrastructure of any other nation, including superpowers, and crumbling that nation. In fact, cyberspace is redefining our security assumptions and defense strategies. This book explains the current cyber threat landscape and discusses the strategies being used by governments and corporate sectors to protect critical infrastructure (CI) against these threats.



Available in Amazon, Flipkart, Kobo, Etc.

Published by Intelegrid ECC(P) Ltd. TF3, Galaxy Delight, Kesari Lane, Trivandrum-12, INDIA.
www.intelegridecc.com :ksjayamohank@gmail.com, 8547611741, 8547018797, 0471 3577774.

iNTELEGRID

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.

LACK A CYBERSECURITY ENGINEER IN YOUR ORGANISATION?

Intelegrid Virtual CISO consultancy acts as your own Security Engineer

Intelegrid ECC offer personalized and managed security services, security architecture and policy development, security maturity, risk and cyber vulnerability assessment, IT-OT segregation and integration consulting, and implementation.