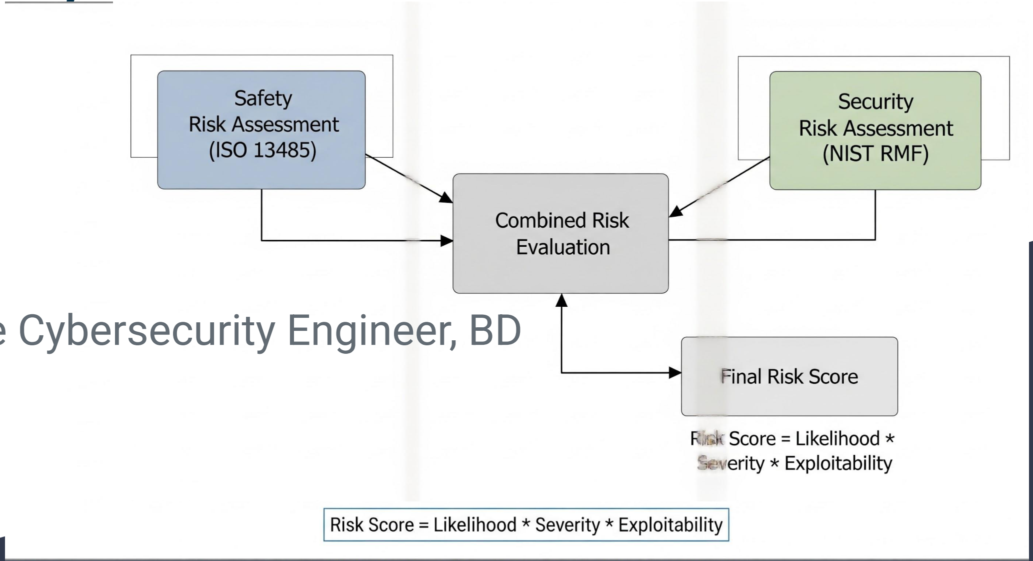
Medical Cybersecurity - Research Seminar , Kathmandu University, Dec 2025



Safety
Risk Assessment
(ISO 13485)

Security
Risk Assessment
(NIST RMF)

Combined Risk
Evaluation

Final Risk Score

Risk Score = Likelihood *
Severity * Exploitability

Risk Score = Likelihood * Severity * Exploitability

Ravi Dhungel
Staff Medical Device Cybersecurity Engineer, BD

MedicSec

About me

B.E. Computer Engineering Kathmandu University
M.S (Dual major - Computer science /GIS) - Southern IL University, Carbondale

Former Major of Nepalese Army / 23 years of experience on cyber security.
https://www.linkedin.com/in/ravidhungel/

More than 25 articles and white papers published on cyber security in the local and global publications.

Research Paper , Graduate School - **Web Mapping and Application Towards a Cloud: Enabling a WebGIS Prototype in an Open Source** Environment
https://opensiuc.lib.siu.edu/cgi/viewcontent.cgi?article=1372&context=gs_rp

www.medicsec.com - personal collection

Hobbies - HIgh Altitude Hiking, Blogging, Mountain Biking, playing so

Few publications – Not peer reviewed

The Rising Nepal www.therisingnepal.org.np

DETOUR

2019 September 29 | 7
2076 B.S. Asoj 12 Sunday

Information & Technology

Cyber security in banking and financial sectors

Ravi Dhungel

Two recent data security incidents in Nepal - the breach of Nepal Electronic Payment Systems (NEPS) and the furor of the public against the teleconferencing of Prime Minister Oli from a hospital in Singapore has reinvigorated the debate on cyber security and national security. While these two incidents are completely different in nature, they share commonalities in current state and challenges ahead in cyber security vis-a-vis national security.

Nepal need to build strategies that are actionable and far reaching.

1. Short term strategy and actionable items

Cyber risk assessment of governance, systems, and processes are very important to identify the gaps in cyber security. Engaging security professionals, who have in-depth knowledge on global regulatory compliance, governance, cyber security frameworks, and security architecture is the first step. All security artifacts, findings, reports, and processes should be secured and encrypted. An assessment like this is a starting point to develop multiyear cyber security programs.

2. Long term strategy and plans

Strategy, governance, and

and secure development lifecycle - Banks should invest in vulnerability management programs and processes. Software systems are composed of millions of lines of code and hundreds of functions. If the banks have internal development teams, process should be developed for static scanning, code reviewing, and identifying top ten vulnerabilities by Open Web Application Security Project (OWASP). Bug bounty programs should be developed to engage external security researchers.

Cyber Insurance - The banks should buy cyber insurance to transfer the monetary risks to the insurance in the case of a breach. Cyber security policy offered by insurance largely depends upon the investment on cyber security programs.

Bridging the digital divide

By Ravi Dhugnel

Information Technology (IT) is becoming the common hub for most of our activities whether it be using smart machines or using WAP (Wireless Application Protocol)

and Communication Technology) age emphasis "any to any" connection, that is the ability of any network operator to

The 240 page ITU report entitled "Trends in Telecommunication reform 2000-2001, Interconnection Regulation " explains

pagers, mobiles and cable TVs are not only bringing the world closer but also giving the choice to customers to have the service they need the best. Thus, it increases the overall communications networks, and beneficiaries include workers, economies and governments. Different types of networks and service providers are emerging day by day in the hope of better interconnection and services among different networks so that they can serve a wide range of customers and offer them the different types of services they need. In

Mitigating COVID-19 Cyber Security Challenges

Ravi Dhungel

THE COVID crisis is a for bad actors to comm The bad actors can be criminals, or rogue employee introduces unique challenges health and cyber security cri times because of ubiquitous increase in penetration of the i the globe and the challenge social distancing and quarant This makes it a global

authentication (2FA) are technical controls for remote access. Beside that the cyber hygiene of the devices should be maintained that includes patching of the operating system, antivirus and anti-malware systems.

Use of personal computers, mobile devices, and managed systems: All the devices should be managed at the enterprise level. The hard drives should be encrypted and mobile device management (MDM)

should be done with the vendor before using applications. The organisation risks losing the intellectual property if proper controls are not placed on the video and audio data.

Training and awareness: Enterprise should periodically provide the training to the employees on the best practices of cyber security, data security and the regulations pertaining to the telecommuting. More specifically, training and awareness should

Organisations and individuals should refrain sharing the video conferencing URL in public and invites should be sent to the attendees emails. The phenomenon is called "Zoom Bombing".

In Nepal, the availability of COVID-19 applications by different government agencies shows the importance of technology services in the race against time.

We should praise the government

The Rising Nepal www.risingnepaldaily.com

NATION

2020 July 18 | 3
2077 B.S. Saun 3 Saturday

Developing Next Generation Border Security System

Durga Kunwar
Ravi Dhungel

Ever since the stand-off between Kathmandu and New Delhi erupted, the question of border security management in Nepal took an alter and steered debates ranging from sealing the border with a physical fence to lock horns deploying soldiers eyeball to eyeball.

Today, border management expands from physical security to the cyberspace where the demarcation of digital borders in cyberspace is nonexistent and global rules of engagement are yet to be written. The hacking of the Civil Aviation Authority of Nepal website and a couple of educational institutions by an alleged Indian hacker in the last week of May 2020 is an example of how the border crisis escalates to cyberspace and information warfare in the social media.

The presence of Rohingya

unmanned autonomous systems and predictive analytics will take border management to the next level of national security. It should also justify the limitation of physical geography and the financing for armed forces.

Virtual monitoring of borders using unmanned autonomous systems provides real time monitoring of the activities across the borders. The scale of

enforcement agencies. This kind of unified approach to build a next generation information system will provide real time border and intelligence information to the central government. On the basis of this data, the central government can make informed security and diplomatic interventions.

Next generation border management system helps proactively engage in diplomacy.

Cyber Security: Awareness And Training

Ravi Dhungel

THE recent banking security breaches in Nepal highlight the gap in technology, processes, and people in managing critical information technology infrastructures. More importantly, there have been gaps in training and awareness of cyber security. All financial institutions and banks should establish multi-year cyber

threat. Hence, training and awareness are critical controls in mitigating cyber risks. To develop effective cyber security training and awareness, banking and financial sectors need to clearly address certain action items. Some key ones are discussed below.

Assessment of training needs: What kind of cyber security training is needed for organisations? Training needs assessment is the first step in identifying the requirements of cyber security training. It varies from basic cybersecurity 101 to advanced training on applications and Applications Programming Interface (API) security as well as vendor specific tools and technologies.

on computer hygiene, data security, roles and responsibilities, physical security, and do's and don'ts. This kind of training should be given during the onboarding of new employees and refreshed yearly or bi-yearly.

Trainings on privacy and compliance: Regulatory data compliance is important in any industry. A data compliance and privacy team should adhere to the regulatory requirements of the Nepal Rastra Bank (NRB), Payment Card Industry (PCI).

management (SIEM) intrusion detection system (IDS), file integrity monitoring, endpoint security, data loss prevention system etc.

Phishing and simulation training: This is one of the most popular cyber security trainings in an organisation. Phishing has a large attack surface, the threat of malware, adware, and ransomware can be largely reduced by this kind of training. Organisations should invest heavily in email security and training so that phishing emails don't reach the individual mailbox and helps to reduce the attack surface.

Internal processes and policies: Organisations should continuously train and monitor individuals

advantages and innovation in financial products by enabling security and privacy in financial technologies. It is a known fact that most phishing emails are targeted to C-level executives who should be trained on phishing and work with cyber security teams to mitigate phishing attacks.

Establishing cyber security as a shared responsibility: It is the responsibility of management to establish a culture of security as a shared responsibility through training and awareness. A culture of cyber security should share values between different organisational units and accountability across the business units. Cyber security is not merely an IT problem but is the complex amalgamation of people, processes, and technologies.

AI To Develop Safe Medical Devices

Ravi Dhungel

Generative AI is set to revolutionise the medical device industry by enabling the creation of innovative, safe, and secure devices. This technology uses advanced algorithms to rapidly generate design prototypes, ensuring that devices meet stringent safety and efficacy standards while improving the verification and validation of patient needs. By leveraging generative AI, manufacturers can accelerate the secure development process, tailor devices to individual patient needs, improve security posture, automat the regulatory compliance and enhance overall healthcare outcomes.

In the pre-market phase, generative AI plays a crucial role in the design and development of medical devices. AI algorithms can analyse vast amounts of data, including patient records, clinical trial results, and existing device performance metrics, to generate optimised design prototypes. This process significantly reduces the time required to develop new devices, moving from years to months. It also substantially improves the verification and validation process for both clinical and security user needs.

Additionally, AI can simulate various scenarios to predict device performance, identify potential risks, and ensure com-

devices and improving the security posture of the devices.

Device performance

Once a medical device is on the market, generative AI continues to provide value by monitoring device performance and patient outcomes. AI systems can analyse real-world data to detect any anomalies or adverse events, enabling manufacturers to address issues promptly. This continuous monitoring helps maintain device safety and efficacy, ensuring that any necessary updates or recalls are managed efficiently. Furthermore, AI can assist in post-market surveillance by predicting long-term device performance and patient outcomes, contributing to ongoing improvements in device design and functionality. The ability to continuously fetch performance data not only enhances the AI model but also improves the security posture and threat intelligence, ensuring that devices remain safe and secure throughout their lifecycle.

Despite its potential, leveraging generative AI in medical device development comes with challenges. One significant hurdle is ensuring the transparency and explainability of AI algorithms. Securing AI algorithms is a complex issue, as outlined in my article "Challenges of AI in Cybersecurity," which discusses the cybersecurity challenges in AI and machine learning applications. Regulatory bodies require a clear understanding of how AI systems make decisions to ensure patient safety. Additionally, integrating AI into existing clinical workflows can be complex, requiring collaboration between AI developers, healthcare professionals, and regulatory agencies.

This technology can significantly improve the precision, customization and security of medical devices, tailoring them to individual patient needs more effectively than ever before.

are secure and compliant with regulations is paramount to protecting patient data and maintaining trust. The opportunities presented by generative AI in medical device development are vast. AI can create highly personalised devices tailored to individual patient anatomies, improving treatment outcomes and reducing complications. The technology also enables rapid iteration and testing of device prototypes, facilitating next-generation verification and validation processes at scale thus maturing secure software development life cycle.

This accelerates innovation and brings new devices to market faster. Moreover, AI-driven insights can enhance post-market surveillance, leading to continuous improvements in device safety and performance. The continuous collection of performance data will refine AI models, while security data will bolster the security posture and threat intelligence. As AI technology advances, its integration into the medical device industry promises to revolutionise healthcare delivery and secure patient care, ultimately leading to better health outcomes and more

medical device industry can harness AI to enhance patient outcomes and drive innovation in healthcare. This technology can significantly improve the precision, customization and security of medical devices, tailoring them to individual patient needs more effectively than ever before.

Regulatory burdens

Moreover, generative AI can streamline the development process by reducing the time required to bring new devices to market. This is achieved by decreasing regulatory burdens through improved and automated compliance mechanisms, enhancing the development process with rapid prototyping, and enabling next-generation verification and validation processes at scale. These advancements ensure that devices are not only developed faster but also meet the highest standards of security, safety and efficacy.

In the post-market phase, continuous surveillance powered by AI ensures that devices remain effective and secure throughout their lifecycle. Real-time monitoring and data analysis allow for prompt identification and resolution of any security issues, maintaining the trust and safety of patients. This ongoing vigilance helps in refining AI models and improving the security posture, ultimately leading to better health outcomes and more efficient healthcare systems. By embracing generative AI, the medical device industry can achieve unprecedented levels of innovation, safety, and security, paving the way for a future where medical devices are more effective, personalised, and

Agendas

Cyber Security, Data Security and Privacy - Revisiting

Data Regulations

- by industry - Healthcare, Education, Children
- by region - EU GDPR, US

Similarities and differences among industries.

Safety and Cybersecurity risk score

Potential data sources

MedicSec

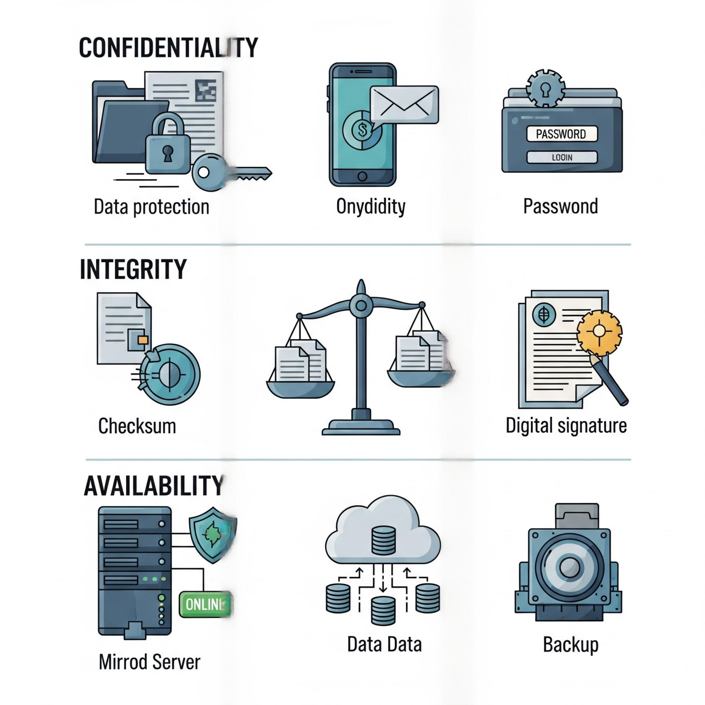
Cyber Security and Data Security

- Broad - National security, critical infrastructure, cyber warfare
- Digital Data
- Stored in computers, mobiles, memory chips etc.
- Internet, websites, Apps
- Operating Systems, Networking, Internet
- Browsers - Edge, Internet Explorer, Chrome, Firefox etc .

Data security and privacy regulations

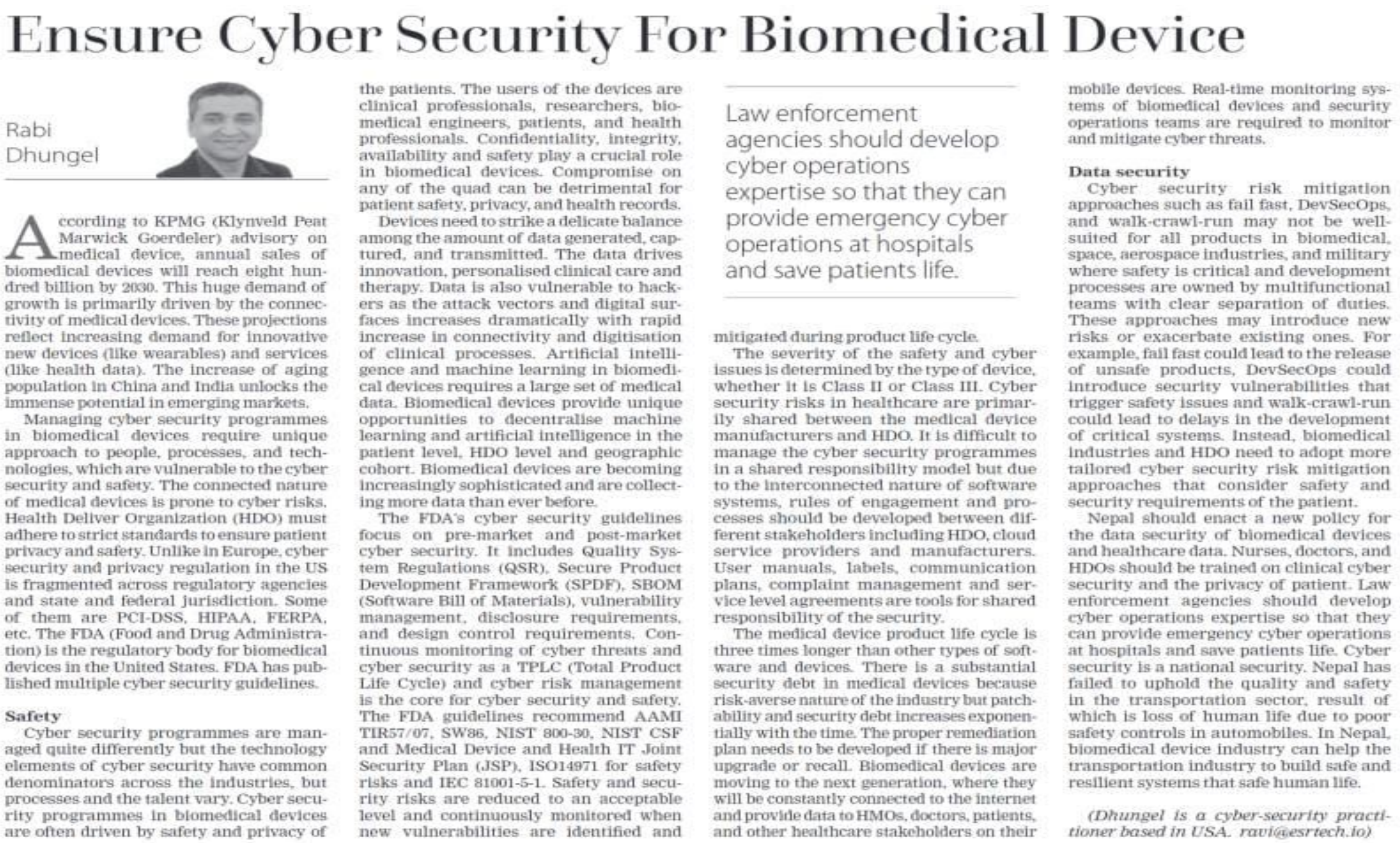
- COPPA - Children Online Privacy Protection Rule < 13 yrs of age - US
- FERPA - Higher Education (Transcripts, grades etc.) - US
- GDPR - European Union - parental consent <16 yrs of age
- PCIDSS - Credit Card consortium - Global
- HIPAA - Personal Health Information - US
- Child sexual abuse material - download etc.
- FDA’s - post market and pre-market guidances.

Cybersecurity – CIA triad



MedicSec

Cybersecurity in medical device



Ensure Cyber Security For Biomedical Device

Rabi Dhungel

According to KPMG (Klynveld Peat Marwick Goerdeler) advisory on medical device, annual sales of biomedical devices will reach eight hundred billion by 2030. This huge demand of growth is primarily driven by the connectivity of medical devices. These projections reflect increasing demand for innovative new devices (like wearables) and services (like health data). The increase of aging population in China and India unlocks the immense potential in emerging markets.

Managing cyber security programmes in biomedical devices require unique approach to people, processes, and technologies, which are vulnerable to the cyber security and safety. The connected nature of medical devices is prone to cyber risks. Health Deliver Organization (HDO) must adhere to strict standards to ensure patient privacy and safety. Unlike in Europe, cyber security and privacy regulation in the US is fragmented across regulatory agencies and state and federal jurisdiction. Some of them are PCI-DSS, HIPAA, FERPA, etc. The FDA (Food and Drug Administration) is the regulatory body for biomedical devices in the United States. FDA has published multiple cyber security guidelines.

Safety

Cyber security programmes are managed quite differently but the technology elements of cyber security have common denominators across the industries, but processes and the talent vary. Cyber security programmes in biomedical devices are often driven by safety and privacy of the patients. The users of the devices are clinical professionals, researchers, biomedical engineers, patients, and health professionals. Confidentiality, integrity, availability and safety play a crucial role in biomedical devices. Compromise on any of the quad can be detrimental for patient safety, privacy, and health records.

Devices need to strike a delicate balance among the amount of data generated, captured, and transmitted. The data drives innovation, personalised clinical care and therapy. Data is also vulnerable to hackers as the attack vectors and digital surfaces increases dramatically with rapid increase in connectivity and digitisation of clinical processes. Artificial intelligence and machine learning in biomedical devices requires a large set of medical data. Biomedical devices provide unique opportunities to decentralise machine learning and artificial intelligence in the patient level, HDO level and geographic cohort. Biomedical devices are becoming increasingly sophisticated and are collecting more data than ever before.

The FDA's cyber security guidelines focus on pre-market and post-market cyber security. It includes Quality System Regulations (QSR), Secure Product Development Framework (SPDF), SBOM (Software Bill of Materials), vulnerability management, disclosure requirements, and design control requirements. Continuous monitoring of cyber threats and cyber security as a TPLC (Total Product Life Cycle) and cyber risk management is the core for cyber security and safety. The FDA guidelines recommend AAMI TIR57/07, SW86, NIST 800-30, NIST CSF and Medical Device and Health IT Joint Security Plan (JSP), ISO14971 for safety risks and IEC 81001-5-1. Safety and security risks are reduced to an acceptable level and continuously monitored when new vulnerabilities are identified and mitigated during product life cycle.

> Law enforcement agencies should develop cyber operations expertise so that they can provide emergency cyber operations at hospitals and save patients life.

The severity of the safety and cyber issues is determined by the type of device, whether it is Class II or Class III. Cyber security risks in healthcare are primarily shared between the medical device manufacturers and HDO. It is difficult to manage the cyber security programmes in a shared responsibility model but due to the interconnected nature of software systems, rules of engagement and processes should be developed between different stakeholders including HDO, cloud service providers and manufacturers. User manuals, labels, communication plans, complaint management and service level agreements are tools for shared responsibility of the security.

The medical device product life cycle is three times longer than other types of software and devices. There is a substantial security debt in medical devices because risk-averse nature of the industry but patchability and security debt increases exponentially with the time. The proper remediation plan needs to be developed if there is major upgrade or recall. Biomedical devices are moving to the next generation, where they will be constantly connected to the internet and provide data to HMOs, doctors, patients, and other healthcare stakeholders on their mobile devices. Real-time monitoring systems of biomedical devices and security operations teams are required to monitor and mitigate cyber threats.

Data security

Cyber security risk mitigation approaches such as fail fast, DevSecOps, and walk-crawl-run may not be well-suited for all products in biomedical, space, aerospace industries, and military where safety is critical and development processes are owned by multifunctional teams with clear separation of duties. These approaches may introduce new risks or exacerbate existing ones. For example, fail fast could lead to the release of unsafe products, DevSecOps could introduce security vulnerabilities that trigger safety issues and walk-crawl-run could lead to delays in the development of critical systems. Instead, biomedical industries and HDO need to adopt more tailored cyber security risk mitigation approaches that consider safety and security requirements of the patient.

Nepal should enact a new policy for the data security of biomedical devices and healthcare data. Nurses, doctors, and HDOs should be trained on clinical cyber security and the privacy of patient. Law enforcement agencies should develop cyber operations expertise so that they can provide emergency cyber operations at hospitals and save patients life. Cyber security is a national security. Nepal has failed to uphold the quality and safety in the transportation sector, result of which is loss of human life due to poor safety controls in automobiles. In Nepal, biomedical device industry can help the transportation industry to build safe and resilient systems that safe human life.

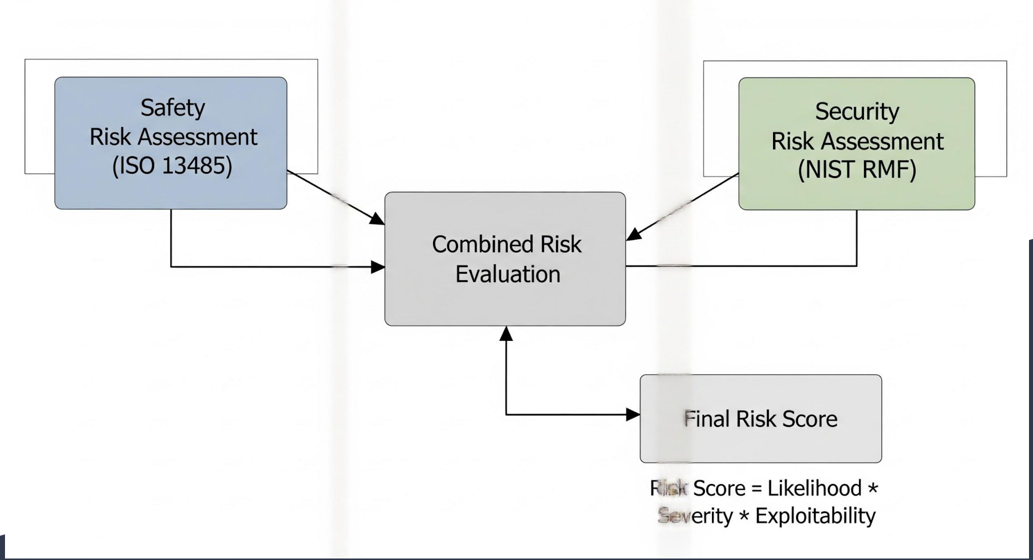
(Dhungel is a cyber-security practitioner based in USA. ravi@esrtech.io)

MedicSec

Challenges on medical cybersecurity

- **Increased system complexity** - embedded systems, clouds, integration
- **Severe patient impact** - services or directly through the device.
- **Vulnerability and patch management** - time is of essence, legacy system
- **Multi Patient harm potentials**

Risk Scoring – Security Vs. Safety



Safety
Risk Assessment
(ISO 13485)

Security
Risk Assessment
(NIST RMF)

Combined Risk
Evaluation

Final Risk Score

Risk Score = Likelihood * Severity * Exploitability

MedicSec

Cybersecurity in AI

Data Poisoning - Training Data sets

Prompt Injection / Input manipulation modify AI system inputs in realtime to alter the responses.

Generative AI facilitates advanced deep fake for fraud and impersonation

AI hallucinations occur when the model produces inaccurate or misleading information.

Model stealing involves attackers replicating an AI model by exfiltrating input and output data.

Re-identification of anonymized data can lead to privacy violations a sensitive information.

Medical Cybersecurity – potential research topics

1. Finding **cyber posture** of medical devices in the hospital - patch , updates, encryption, MFA etc

2. Systemic challenges on vulnerability management of medical devices.

3. Balancing privacy, security and usability in medical devices

4. Developing risk classifier for security and safety risk assessment

MedicSec

Data Sources for Research

Health care delivery organization (HDO) - Hospital, Clinics

FDA - Food and Drug Administration - Warning Letters, Recalls of devices

- Device Types, Clinical Use

Threat Intel Sources - H-ISAC feed

White Papers - Medical Device Manufacturers

UCSD - Center of Healthcare Cybersecurity - leader in clinical cybersecurity space

MedicSec

Summary

- Covered data security regulations across various industries

- Challenges on medical device cybersecurity.

- Foundations of security and safety risk assessment.

- Discussed research topics for medical device cybersecurity

MedicSec

Questions ?

Contact me at linkedin
ravi.dhungel@gmail.com