enGAge

Cybersecurity Special Edition

Oct 23

“If opportunity doesn’t knock, build a door.”

– Milton Berle

Introducing

Dr. Dilip Nath

AVP & Deputy CIO

SUNY Downstate Health Science University

CLIENT SPEAK

" GS Lab | GAVS has been a great partner from the start. They have helped us during the initial phases of SOC. The team is just amazing, and they work on 24/7 rotational shifts smoothly. We are slowly moving forward to the next phases of SOC and GS Lab | GAVS team is playing a huge role in this movement.

Thanks to the complete GS Lab | GAVS team and special thanks to Karthikeyan and Kannan who have taken time to hear us out and made this happen. Last but not the least, a huge thanks to Balaji for giving us such a wonderful team. "

- Kumudha Padmanabhan,
Sr. Manager,
Cyber Security Operations (CSOC),
Oportun

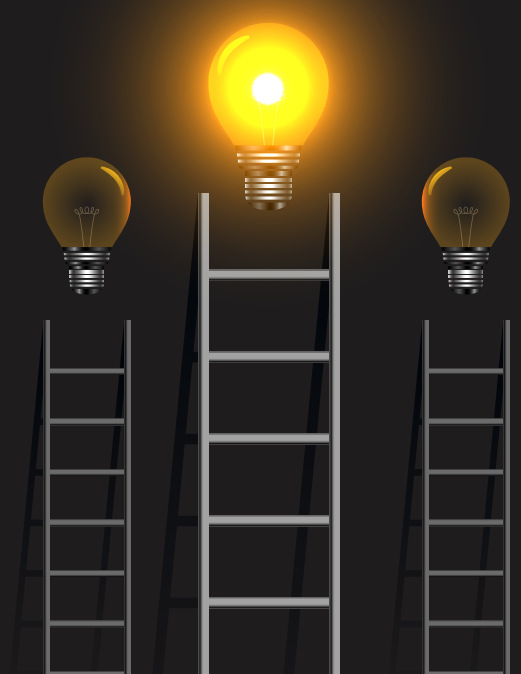


Table Of Content

Editor's Note

Soumika Das

Welcome to the **Cybersecurity special edition** of enGAge!

In the realm of cybersecurity, the advent of AI marks a significant shift, promising a potent and versatile tool that could revolutionize the entire paradigm. This transformative technology not only alters the landscape of prevailing threats but also presents novel challenges that necessitate our attention.

The rise of AI has streamlined cybercrime processes, automating malicious activities and lowering entry barriers, thus enabling larger-scale attacks with ease. Tools like WormGPT, a sizable language model trained on malware data, exemplify this advancement by facilitating phishing attacks through a nuanced understanding of persuasive communication strategies. Another concern is the use of AI to develop new types of malware.

To mitigate these risks, organizations must take a proactive approach to cybersecurity. Focus must be on recalibrating employee training to encompass responsible AI tool usage within the workplace. A heightened awareness of evolving social engineering techniques, propelled by generative adversarial networks and large language models, should be integrated into training modules. Moreover, enterprises embracing AI technologies should rigorously test their implementations to identify and mitigate common vulnerabilities and errors, ensuring a robust security posture. Stringent code review processes, especially for code developed with the aid of LLMs, must be in place, coupled with effective mechanisms to identify vulnerabilities within existing systems.

GS Lab | GAVS with its end-to-end Cyber Security Services, helps clients manage risk and build an effective cyber security program. Please visit our website to know more –> Cybersecurity Services

Team enGAge spoke with **Dr. Dilip Nath, AVP & Deputy CIO, SUNY Downstate Health Science University,** on his journey and his thoughts on success and leadership. He has also written on **'Ransomware Preparedness for Healthcare: Enhancing Resilience Amid Growing Threats'.**

We have a lineup of insightful articles in this edition.

Kannan Srinivasan has written, **ChatGPT: A Security Guide for Healthcare and BFSI Industries.**
Yuvaraj Arumugam has written, **IoT Security in Healthcare.**
Karthikeyan M has written, **Securing Medical Devices: Safeguarding Healthcare in the Digital Age.**
Praveenkumar Jothi has written, **Cyber Insurance: Preparing for the Inevitable.**
Madhumitha K has written, **Multi-level Approach to Access Security.**
Anitha R has written, **Building Trust through Risk and Controls.**

Messages from Cybersecurity Leaders at GS Lab | GAVS

"Practising situational awareness in Cybersecurity world and taking simple yet effective security precautions in our everyday life will help us to create a safer environment for us and those around us."

- Anitha R
Group Manager,
Customer Success,
Cybersecurity PMO

"Cyber Resilience can be thought of as digital fitness. Focusing on traditional cybersecurity measures and protections is no longer adequate to protect businesses from the spate of sophisticated attacks."

- Subhakala K
Technical Manager,
SOC

"This moment is the future, let's face it. We need to stop denying or denying the impact of the cyber society in which we already live."

- Yuvaraj Arumugam
Technical Manager,
Information Security

"Your password is the key to your digital life. Keep it safe."

- Karthikeyan Manoharan
Sr. technical Manager,
Cybersecurity

"Cybersecurity is not just a technology issue; it's also a people issue. The chain is only as strong as its weakest link, and often, that weakest link is human error. By staying aware and vigilant we can be secured."

- Bhavani Damodaran
Technical Manager,
Information Security

Introducing Dr. Dilip Nath

AVP & Deputy CIO, SUNY Downstate Health Science University

Please tell us something about your journey from Bangladesh to having a successful career in the US.

I was born in Bangladesh and grew up with a sense of ambition, hunger for knowledge, along with a deep appreciation for my cultural heritage and a strong sense of community. However, I recognized that to fulfill my aspirations and make a difference in the world, I needed to venture beyond the borders of my homeland.

At the age of 16, I relocated to the US, becoming the first member of my family to do so. However, this venture was not undertaken just to fulfil my dreams of education and success but was also fueled by a burning desire to contribute to society.

After arriving in the United States, I had to face some inevitable challenges that come with immigration – adjusting to a new culture, language, and way of life. Language was a significant obstacle. I had to master English, which was essential for communication and building a successful life here. I tackled this challenge head-on, enrolling in English language classes and practicing tirelessly to improve my proficiency. Financial constraints were yet another hurdle. I took on various jobs, often working long hours to support myself and pursue my educational goals simultaneously.

My experiences as an immigrant instilled in me a deep appreciation for the opportunities the United States offered and a strong desire to give back to the community that had welcomed me.

It taught me the value of adaptability, the importance of community support, and the significance of embracing diversity.

Dr. Dilip Nath

How would you define success?

Success to me is making a difference in the lives of people, whether is providing easy access to education or healthcare and close the equity gap. After I came to the US, I became involved as an activist addressing the following issues: affordable health care, hate crimes, immigrant rights, domestic violence, environmental issues, improving elderly care, improving the public educational system, child day care and after school programs, affordable housing and transportation efficiency. These are a few causes that are near to my heart, and I continue to participate in several collaborative organizations to give back to the community.

What has been your approach to building trust with your team and how do you build credibility as a leader?

My approach has been to lead the team from the front and to believe in them. Leading from the front means being visible and accessible to your team and being willing to roll up your sleeves and work alongside them. Also, believing in them gives themV the autonomy and resources they need to succeed, and being supportive when they make mistakes. When you believe in your team, they are more likely to believe in themselves and in their ability to achieve their goals.

How do you maintain engagement and morale during challenging times?

Staying focused on the mission is a critical way to maintain engagement and morale during challenging times. When people know what they are working towards and why it is important, they are more likely to stay motivated and engaged, even when things are tough.

What is the one thing you wish someone had told you when you were at the start of your career?

Do not look for the perfection, rather focus on the continuous improvements.

Ransomware Preparedness for Healthcare

Enhancing Resilience Amid Growing Threats

Introduction

Ransomware attacks have become a significant problem in the healthcare sector. These criminal operations have become a formidable foe that need a concerted response from healthcare groups. The recent high-profile cyber-attacks on prominent institutions like as UHS, Common Spirit Health, Johns Hopkins Health, and HCA have highlighted the critical need to tighten cyber security in the healthcare business. Proactive efforts are required since ransomware attacks not only endanger patient data but also considerably raise the risk to medical care.

Preparing for Ransomware Attacks

In view of the increasing threat of ransomware attacks, healthcare companies must take a proactive approach to preparation. Thorough risk assessments are a critical component of this planning. These evaluations provide the core of ransomware mitigation strategies. At this stage, organizations in the healthcare industry carefully identify system flaws and analyzes the dangers associated.

Organizations can build a plan for delivering successful mitigation measures by appropriately identifying potential vulnerabilities in their cyber security architecture (Neprash et al., 2022).

Developing a robust response strategy is also critical to their ransomware preparedness. Healthcare institutions that use this strategy will be directed like a compass through the turbulent waters of a ransomware attack. In the event of an attack, it provides precise, logical procedures that must be taken. This action plan includes procedures for isolating contaminated systems, an efficient reporting method for law enforcement, and an effective patient and staff communication approach. It is impossible to overstate the importance of having a well-organized reaction strategy since it ensures a coordinated and effective response when time is of the essence.

Furthermore, the value of the human aspect in cyber security cannot be emphasized. Employee training initiatives are a key priority for healthcare firms to equip their first line of defense. These courses provide healthcare personnel with the knowledge and skills they need to recognize specific ransomware threats.

Employees are trained on how to identify phishing emails, which are regularly used as entry points for ransomware attacks, and how to report any suspicious behavior immediately.

Last but not least, proactive security deployment is critical for mitigating ransomware attacks. For this, reliable technologies like as firewalls, antivirus software, and intrusion detection systems must be used. These layers of defense increase detection and mitigation, making it more difficult for hackers to infiltrate the system (Neprash et al., 2022).

Responding to Ransomware Attacks

In the unfortunate event of a ransomware attack, a rapid and well-planned response is critical to reducing damage and regaining control.

Isolating Infected Systems

The first line of defense is to isolate vulnerable systems as quickly as possible. This precaution is required to prevent ransomware from spreading throughout the network. By isolating the susceptible systems, healthcare institutions can limit the attack's reach and prevent further data compromise. Isolation is the first step in regaining control of the situation (Crespo & Driscoll, 2022).

Collaborating with Law Enforcement

Cooperation with law enforcement is critical when responding to ransomware attacks. Their knowledge and resources aid in the investigation, mitigation, and monitoring of cybercriminals, which helps the overall reaction and pursuit of justice while also avoiding new attacks. Miller 2022).

Effective Communication with Stakeholders

Managing the aftermath of a ransomware attack necessitates open communication and fast information sharing. Personnel and patients must be informed as soon as possible about the incident's impact on data security and medical services. Maintaining confidence, managing expectations, and ensuring a coordinated response all contribute to a lower overall effect.

Data Restoration from Backups

Reliable data backup and recovery are critical for mitigating the effects of ransomware. They enable data restoration in order to sustain care and minimize long-term impacts. According to Crespo and Driscoll (2022), updated backups serve as a safety net, allowing for recovery without giving in to hackers' demands and, eventually, resuming normal corporate operations.

Balancing Innovation and Security

While technologies such as generative AI and data modernization have immense potential, it is critical that cyber security is not jeopardized in the process. Given the rapid speed of technological advancement, the healthcare business cannot afford to remain complacent regarding security. Finding this balance is critical because it allows healthcare organizations to adopt developing technology while still ensuring the availability, confidentiality, and integrity of critical data and services.

In this day and age, healthcare must emphasize effective cyber security. This necessitates the deployment of cutting-edge technology, thorough risk analysis, and stringent standards. Leveraging innovation without accepting unnecessary risks is made feasible by improving cyber security while embracing technology. This harmony preserves patient information, maintains trust, and ensures the continuance of healthcare services (Miller, 2022).

Strategies for Ransomware Preparedness

A comprehensive strategy to ransomware preparation includes a number of critical tactics:

- **Rigorous Risk Assessment:** The identification of vulnerabilities and threats via rigorous assessments is the cornerstone of resilience (Kancherla, 2023).
- **Effective Response Planning:** Prepares for every ransomware event. Regular response strategies should be developed and maintained.
- **Employee Education:** Ongoing training programs enable employees to be proactive in spotting and resolving hazards.

- **Employee Education:** Ongoing training programs enable employees to be proactive in spotting and resolving hazards.
- **Strong Security Infrastructure:** Investing in cutting-edge security practices and technology builds a strong protection against cyber threats.
- **Patient-Centric Approach:** Maintaining patient trust and resolving patient concerns about data security are crucial in the healthcare sector.
- **Continuous Improvement:** Continuous improvement is made feasible by frequently reviewing protection, detection, reaction, and recovery capacities (Kancherla, 2023).

Healthcare facilities are becoming vulnerable to ransomware attacks, which is a major problem that must be addressed immediately. Proactive actions must be done to build defenses against these dangers in order to protect patient care and the general public's health. By conducting thorough risk assessments, developing specific response plans, educating employees, implementing advanced security measures, addressing patient concerns, and embracing technology while fortifying cyber security, healthcare organizations can successfully prepare for and respond to ransomware threats. These strategies are critical to ensuring that the healthcare business remains a reliable guardian of patients' well-being in the face of evolving cyber threats.

This article was originally published in The Generation.

References

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., ... & Nikpay, S. S. (2022, December). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. In JAMA Health Forum (Vol. 3, No. 12, pp. e224873-e224873). American Medical Association.
URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9856685/

Crespo, M., & Driscoll, K. (2022, February 19). Addressing Ransomware in Healthcare. Managed Healthcare Executive.
URL: https://www.managedhealthcareexecutive.com/view/addressing-ransomware-in-healthcare

Miller, E. (2022, November 21). The Growing Threat of Ransomware Attacks on Hospitals. BitLyft.
URL: https://www.bitlyft.com/resources/the-growing-threat-of-ransomware-attacks-on-hospitals

Kancherla, S. (2023, September 7). Ransomware Attacks: What the Healthcare Industry Can Do. VMware Blogs.
URL: https://blogs.vmware.com/industry-solutions/2023/09/07/ransomware-attacks-what-the-healthcare-industry-can-do/?utm_campaign=ransomware-attacks-what-the-healthcare-industry-can-do&utm_medium=rss&utm_source=rss

About
the Author

Dr. Dilip Nath is a distinguished leader in higher education and healthcare, known for his advocacy in voting and human rights. As a Harvard Kennedy School alumnus, he's celebrated for his transformative leadership.

With 30+ years of strategic planning expertise, Dr. Dilip focuses on using technology to bridge equity gaps in healthcare and education.

At 16, Dr. Dilip Nath emigrated from Bangladesh to the US, becoming the first in his family to attend college. He's lived in Queens for 33 years, earning the trust of his community as a dedicated leader and activist.

Recognizing the importance of knowledge in politics, he embarked on a self-learning journey about US government and principles of democracy. He earned degrees from the State University of New York, including an MBA and a DBA

Dr. Dilip Nath is know for his visionary, team-oriented, and compassionate leadership. He's a respected advocate for various community issues, including healthcare, immigrant rights, and education. He founded NAVA and co-founded ABHF to further his endeavors.

ChatGPT

A Security Guide for Healthcare and BFSI Industries

ChatGPT is a natural language processing tool driven by AI technology that allows you to have human-like conversations and is considered more advanced than the chatbot.

Ever since the launch in November 2022, there are lots of security concerns raised by the CISO organization and many organizations have blocked the usage of ChatGPT.

Resistance to use new inventions citing risk is quite common and, in this article, we are going to highlight those security challenges and guide you on how to address those.

60% of the organizations have explored ChatGPT in some form or other. In that 60% of organizations 12% use this technology extensively. The key use cases are for Analytics, marketing and analysis, research and development and fraud detection.

Here are some sample use cases for Healthcare and BFSI industries.

Healthcare

- **Patient triage:** ChatGPT can be used to triage patients' health by asking the right questions about their symptoms and medical history to determine the urgency and severity of their condition.
- **Virtual assistants for telemedicine:** ChatGPT can be used to develop a virtual assistant to help patients schedule appointments, receive treatment details, and manage their health information.
- **Medical recordkeeping:** ChatGPT can be used to generate automated summaries of patient interactions and medical histories, which can help streamline the medical recordkeeping process. With ChatGPT, doctors and nurses can dictate their notes, and the model can automatically summarize key details.
- **Remote patient monitoring:** ChatGPT can be used to monitor patients remotely by analyzing data from wearable devices,sensors, and other monitoring devices, providing real-time insights of patients' health.

BFSI

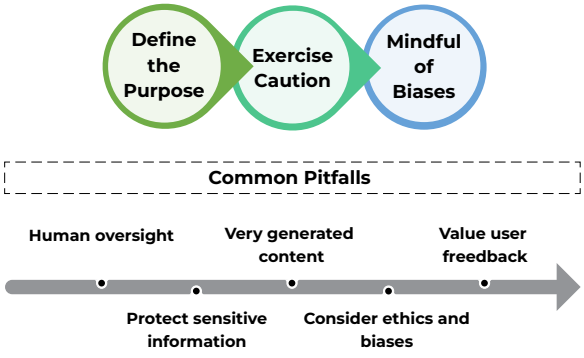
- **Customer onboarding:** It can help in reducing the time taken to onboard a client and simplify the KYC process by asking relevant and assist in guiding the users in a right way.
- **Marketing:** Banks can use ChatGPT to analyze customer data and build personalized marketing campaigns that target specific customer segments.
- **Customer service:** ChatGPT can assist the human agent in answering customer questions, improving efficiency and response time, and providing more accurate and detailed information. This can improve customer service and satisfaction and employee onboarding.

Here are some of the key issues that organization will face due to ChatGPT if proper security measures are not taken

- Exposing Personally Identifiable Information (PII) or Personal Health Information (PHI) through chatbot conversation.

- Employees sharing organization's classified information resulting in losing of competitive advantage.
- Generating malicious code which either sends the data to external entities or waits to create an attack at later point in time.
- Generating code that has malware which can infect the developer's machine.
- Sophisticated phishing attacks.

Best Practices



Organizations implementing ChatGPT use cases should define the purpose, understand the security/data privacy implications, and keep in mind that output is prone to bias. Here are some best practices to be considered while implementing ChatGPT

- There should be human oversight resulting in context irrelevant information not being shared with users
- Ensure sensitive data like PHI or PII or financial data is not shared
- Validate if generated data is right and relevant
- It shouldn't result in ethics, gender or racial biases
- Have a feedback mechanism where users can share their inputs and relevant ones are taken care of in the subsequent sprints

Security measures

Consider the following key security measures for the successful implementation of ChatGPT use cases.

Data Encryption (both in transit & at rest)

Enforching strict Access Control

Audit Trail & Monitor the users' activites

Collect minimal data required to process the application functionality (Data Miinimization)

Regular Updateds & Patchess of hardware and network devices

Audit third parties who store and process your data

Regularly backup the data as per business requirement (Recovery Point Objective [RPO])

About
the Author

Kannan Srinivasan has over 23 years of experience in Cybersecurity and Delivery Management. He is a subject matter expert in the areas of Cloud security, infra security including SOC, Vulnerability Management, GRC, Identity and Access Management, Managed Security Services. He has led various security transformation engagements for large banks and financial clients.

Kannan Srinivasan

Building Trust through Risk and Controls

Building trust through risk and controls involve establishing transparency, reliability, and accountability in all the actions that we perform.

We would cover the following in this topic:

- Common risks in multi-Cloud environments.
- Some countermeasures that can be implemented to mitigate risks.
- Understand when it is the right time to think about security and controls during a large business and technology transformation.

To start with, we need to first understand risks around cloud applications. Implementing the digital trust around Cloud applications is a major step and to continuously monitor the risk becomes the key for success.

When it comes to Cloud, it is a shared responsibility across the delivery models. As organizations increase their dependence on cloud-based solutions, they often struggle with adapting to the nuances that come with governing and protecting their environments. The cloud introduces a paradigm shift in technological possibilities, requiring organizations to evolve their compliance and security models. 77% of executives globally agree that new solutions exist to secure cloud infrastructures better than they have ever been in the past. 99% of cloud security failures will be the customer's fault.

When it comes to SaaS environment

- 35% fail rate against configuration of security best practice settings.
- 30% Compliance violations.
- Over 95% of companies over-provision external users.
- 55% of companies have sensitive data exposed on the Internet.

Leveraging cloud technologies presents new and different risks requiring the organization to understand the compliance. To manage unique risks, we need to know 'Who' you are; 'What' you do; 'What' applications, platforms and infrastructure are in the Cloud, 'What' Cloud provider(s) and provider technologies are used.

Cloud environments break the mould with dynamic new possibilities. This potential brings unique challenges, risks, and threats.

The below are some of the common risk and threats in cloud environments:

- Improper protection of cloud credentials
- Misconfiguration of cloud storage services
- Weaknesses in the cloud's perimeter, and improper configurations in cloud environments
- Inadequate hardening of cloud infrastructure services
- Improper or insufficient tagging of cloud resources
- Failure to architect and engineer infrastructure and applications to meet resiliency needs.

It is important to develop and implement robust controls and safeguards to mitigate these risks. This could include policies, procedures, security measures, and compliance mechanisms.

- Communicating openly and transparently about the risks and the controls that are in place.
- Assigning responsibilities and accountability for risk management and control implementation is a key step.
- Continuously monitoring and assessing the effectiveness of the controls. This involves regular audits, reviews, and evaluations to ensure they are working as intended.
- Keeping the stakeholders informed about the results of risk assessments and control evaluations.
- Being adaptable and responsive to changing circumstances.
- Demonstrating consistency in our approach to risk management and control implementation. This consistency builds trust by showing that we take these matters seriously over time.
- Ensuring our controls are aligned with industry standards and regulatory requirements.
- Maintaining a thorough documentation of the risk assessments, control measures, and compliance efforts. This documentation can serve as evidence of our commitment to managing risks effectively.
- Ensuring we do invest time in training and awareness programs to ensure that the team understands the importance of risk management and the controls in place.
- Finally, creating a feedback loop for stakeholders to provide input and express concerns about risk and control measures. This demonstrates the willingness to listen and improve.

By consistently implementing these steps, we can build trust by showing that we are proactive in managing risks and ensuring that effective controls are in place to protect against them. Trust is essential for any organization that wants to succeed. By building trust, we can create a more secure and resilient environment for our customers, partners, and employees.

About
the Author

Anitha R is a seasoned leader with overall 24+ years of experience in multiple domains with a diversified Industrial background. She has 14+ years of experience in Delivery managing Project Management, Governance, Transitions, Complex Partner Negotiations for Banking, Financials, Telecom and Insurance. She also has 5 years of experience in Cyber Security, Auditing and Risk management, Internal Audit and Control, third party audits and compliance audits for Retail, Life Science, Healthcare, Energy and Resource, Utilities, Manufacturing, Banking, Insurance and Financial services comprising for 17,000 employees for US, Australia and New Zealand geography.

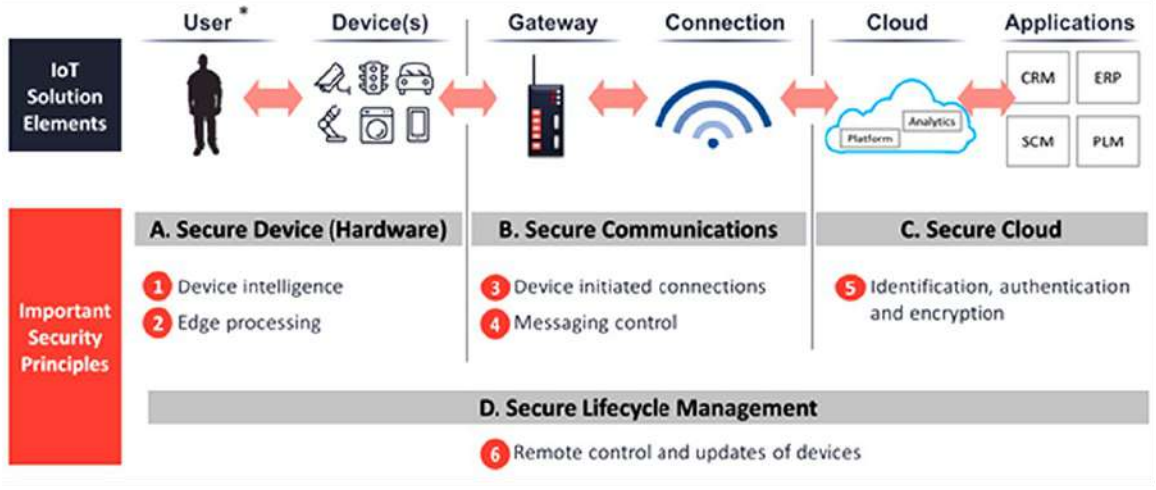
Anitha R

IoT Security in Healthcare

When it comes to IoT security for healthcare the stakes are high and crucial. IoT devices are becoming increasingly prevalent in healthcare, from medical implants to medical devices. These devices will revolutionize the patient care and has the potential to introduce new security risks.

What is IoT Security?

Security in IoT is the act of securing Internet devices and the networks they're connected to from threats and breaches by protecting, identifying, and monitoring risks all while helping fix vulnerabilities from a range of devices that can pose security risks to your business.



What is IoMT Devices?

Rather than security, these days medical devices are designed with functionality and comfort in mind, this leads them becoming easy targets for attackers. If an attacker compromises a medical device, they can potentially exploit it to steal sensitive ePHI data or disrupt critical operations.

For an effective business model and process management, the IoT has become a powerful weapon for individuals/businesses to leverage by connecting the medical devices to a network that can be utilized to generate huge volumes of crucial health care information.

Nowadays in healthcare institutions the IoT devices are like regular networked devices, but these medical devices are crucial and has to be kept safe as part of cyber security practices in the industry.

Major IoMT Devices in Industry

On-body devices - can be separated into clinical-grade wearables and consumer health devices. The devices at consumers' end are used mainly for personal wellness or fitness, such as sports watches, activity trackers and smart clothing.

In-home IoMT devices - These devices are designed to ensure that patients are monitored always to get medical care even when mobility is an issue. This includes telehealth systems, personal emergency response systems (PERS) and remote patient monitoring (RPM).

Community IoMT Systems

This segment of IoMT devices consists of:

- **Mobility services** in which passenger vehicles monitor a patient's health in transit.
- **Emergency response intelligence systems** to help first responders, paramedics, and ER personnel.
- **Kiosks** with touchscreen displays that can provide healthcare products or services, such as connecting patients with healthcare professionals.
- **Point-of-care (PoC) devices** used by healthcare professionals in non-traditional settings.
- **Logistics systems** to improve the transport and delivery of healthcare products and services, such as sensors to measure temperature, humidity, and other elements.

In-clinic IoMT systems – These are designed to perform clinical and administrative functions that allow healthcare professionals to deliver service remotely and receive all the necessary patient data.

In-hospital IoMT systems – These devices are for various management solutions like environment and energy monitoring, inventory management, patient flow management, asset management and personnel management.

Benefits of IoMT in Healthcare Industry

- IoMT reduces errors and helps in making more accurate diagnoses. Also, it reduces healthcare costs and supports healthcare professionals to monitor diseases and prevent/manage chronic illnesses.
- IoMT improves patient experience by reducing the in-person visits of patient which provides better experience and reduces stress and costs for the patient.
- These devices help researchers develop more effective treatments, e.g. smart pills, contain microscopic sensors that provide invaluable real-time data to scientists.
- IoMT collectively makes healthcare providers to save lives easily. Regular monitoring helps professionals to direct preventative care for life-threatening events, and critical care when needed.

IoMT - a Unique Target

- In the above devices we covered, it has to be mentioned that these devices are the most targeted by the threat actors, which may lead to access to the critical ePHI data along with a chance of breaching sensitive financial information that can be a massive payload to the attackers.
- Ransomware attacks are one of the most common cyber security attacks aimed at Medical IoT devices. That leads healthcare institutions to cooperate with threat actors to avoid patient lives endangered.
- Often IoT devices are used to target/launch attacks on other devices. For example, the WannaCry ransomware attack on England's NHS exploited a flaw in Windows XP that had been previously identified by the NSA. The impact of this was global, causing cancellations of appointment and disrupting patient care.
- Although the trend is changing, most healthcare institutions don't necessarily care whether devices are HIPAA compliant, or whether they are sufficiently encrypted, this makes the healthcare IoT devices an easy target.
- Medjacking is a type of security threat used for implementation in a medical device to gain access to its software. This attack will hijack medical devices like infusion pump, which injects drugs into the patient directly. Attackers get the device access and manipulate them with fatal outcomes. Devices with various malware can also lead to stealing of critical healthcare information.

Most Vulnerable Areas

- **Debug port -** In all the devices the debug port exists to facilitate the development/ debugging, which is either hardware/software or it is usually not removed to avoid additional costs while design changes. This is where attackers take advantage to connect the debug port virtual or physical, and give access to read, hijack or modify the software/ firmware.
    - Sometimes physical devices are insecure, which means some models allow us to connect with specific ports using special commands without authentication. If threat actors gain access to these commands, we will be an easy target for attacks such as hardware attacks, medjacking or any reverse engineering attacks.
- **Interception of insecure traffic -** When sensitive information is transmitted in an unsecure manner to the hospitals' IoT devices, there is a risk of data interception. This attack is possible only when the attacker is physically close to the device or plant a beacon like Raspberry Pi that reads medical data with sensors and sends it to the attacker server.
- **Authentication and Authorization -** Hacking attempts are possible in all the stages of interaction, so this has to be implemented end-to-end. Both authentication and authorization are required for devices which contact the data transmitter. We should implement this in an infrastructure level to prevent access from outside.

Being Responsible

- **Healthcare Workers:** Those who deal with software and devices daily need to be educated on how to use them. eg: We should not use devices with a browser to surf internet or watch videos that will infect them with viruses. Healthcare institutions allows people to bring your own devices (BYOD) for their convenience but allowing this can cause breaches and exploits which is caused by mismatch of personal devices with security requirements. This is how attackers gain access to critical information not through IoT appliances but through employees' devices.
- **Healthcare institutions:** There is an increase in connectivity of medical gadgets, so more attention is required for security and privacy of such devices.

We should monitor devices that are reachable through internet for Threats, Malware and apply latest patches/software. Also, we have to ensure that when updating/upgrading the IoT device security will not conflict with any system and not harm any patient indirectly.

- **Cloud Service Providers:** Healthcare institutions take care of secure data storage and encryption, cloud services fill the gap on transmission control and data access. Depending on the devices connected to the network an increase at security risk occurs, and only the providers can monitor the processes of data transfer.
- **Regulatory Authorities:** Regulatory bodies should ensure reasonable and clear legislation for transmitting and storing PHI data securely.

Best Practice to secure the IoMT Devices

- **Asset inventory -** Maintaining the IoMT asset inventory is the first step towards best practice for security. You can't protect when you don't know what you have.
- **Strong Password Policy -** Every IoMT device comes with default password and settings. The attackers will find these default passwords and when adding a new device to their network they will target it. So, while adding a new device, the first step is to create a new strong unique password for each device.
- **Multi-Factor Authentication (MFA) -** is the next level for mitigating credential theft risks. Even if attackers get successful log on attempt into the device, MFA will be the second layer for authentication for logging into the device.
- **Network Segmentation -** isolates sensitive data from unauthorized access by physically or logically separating networks. This process can be done by storing sensitive information on a different data centre from public internet-facing applications or by using firewalls to limit access to the network containing sensitive data. The data breach impact is also reduced because malicious actors won't be able to move from one network to another.
- **Security Updates -** will fix for known vulnerabilities in OS, Software and Firmware. Often, threat actors use these vulnerabilities to gain access to devices, networks, and applications. Critical IoMT devices and their applications should be updated regularly to mitigate risk.

This should include prioritizing any network devices or components associated with any IoMT-connected network.

- **Network Traffic Monitoring** will provide more visibility for devices whether they are sending or receiving more data than usual. eg: IoMT devices can be used as a botnet. In this attack the botmaster gains access to the compromised devices and distribute malicious commands to the bots. When we overwhelm the request and response of the servers that leads to DoS (Denial of Service). By monitoring for abnormal traffic, the healthcare organizations can detect compromised IoMT devices and reduce the attack's impact.
- **Encryption -** IoMT transmits ePHI to a connected application. eg: The insulin pump shares the data to the application to monitor the patient glucose levels, and the application will connect to the public internet. So, encrypting the data-in-transit at network level reduces the impact of man-in-the-middle attacks. Encryption is a process that scrambles data making it unreadable without proper decryption technology, so even when attackers gain access, they won't be able to use the information until decrypted.
- **Intrusion detection systems (IDS)** can be signature-based, specification-based, or anomaly-based. For IoMT, anomaly-based provides the best defence. IDS usually monitors the network for any unusual activity. It includes ML [Machine Learning] so that we can be aware of new risks. The primary benefit of IDS, is that it has the ability to detect zero-day attacks. Since IoMT is new, many devices are not linked with known vulnerabilities that has to be taken care of.

Conclusion

The truth is that the healthcare industry will remain a high-level target for threat actors and healthcare institutions need to ensure that they do everything in their power to keep IoT devices safe from breaches.

References

https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/

About the Author

Yuvaraj Arumugam is a Technical Manager, Information Security at GS Lab | GAVS. He held numerous positions of responsibility in areas of Information Security such as Red Team, Vulnerability Management, Infra Security Audit, VAPT, PCI Audits & HIPAA, Compliance, Devsecops, etc.

He is passionate about reading technical blogs, listening to music & driving.

Yuvaraj Arumugam

Securing Medical Devices

Safeguarding Healthcare in the Digital Age

In recent years, the healthcare industry has undergone a digital transformation, with medical devices playing a pivotal role in patient care and treatment. These devices, ranging from insulin pumps and pacemakers to infusion pumps and MRI machines, have become integral to modern medicine. However, this increasing reliance on medical devices has also exposed vulnerabilities that can be exploited by cybercriminals, potentially endangering patients' lives and compromising the integrity of healthcare systems. This article explores the importance of securing medical devices and provides an overview of strategies and best practices to ensure their safety and confidentiality.

Shared Responsibility between Device Manufacturer and Healthcare delivery Organization

The Growing Significance of Medical Device Security

The Pervasive Nature of Medical Devices

Medical devices are ubiquitous in healthcare settings, encompassing a wide range of and functions. From monitoring vital signs to delivering precise doses of medication, these devices are essential for diagnosing and treating patients. With the advent of the Internet of Things (IoT) and the integration of these devices into larger healthcare systems, their security is of paramount importance.

The Threat Landscape

The increasing connectivity of medical devices exposes them to a myriad of cybersecurity threats. These devices are vulnerable to unauthorized access, data breaches, and even potential manipulation of their functionality. Malicious actors can exploit these vulnerabilities to gain access to patient data or, in some cases, directly harm patients by tampering with device settings.

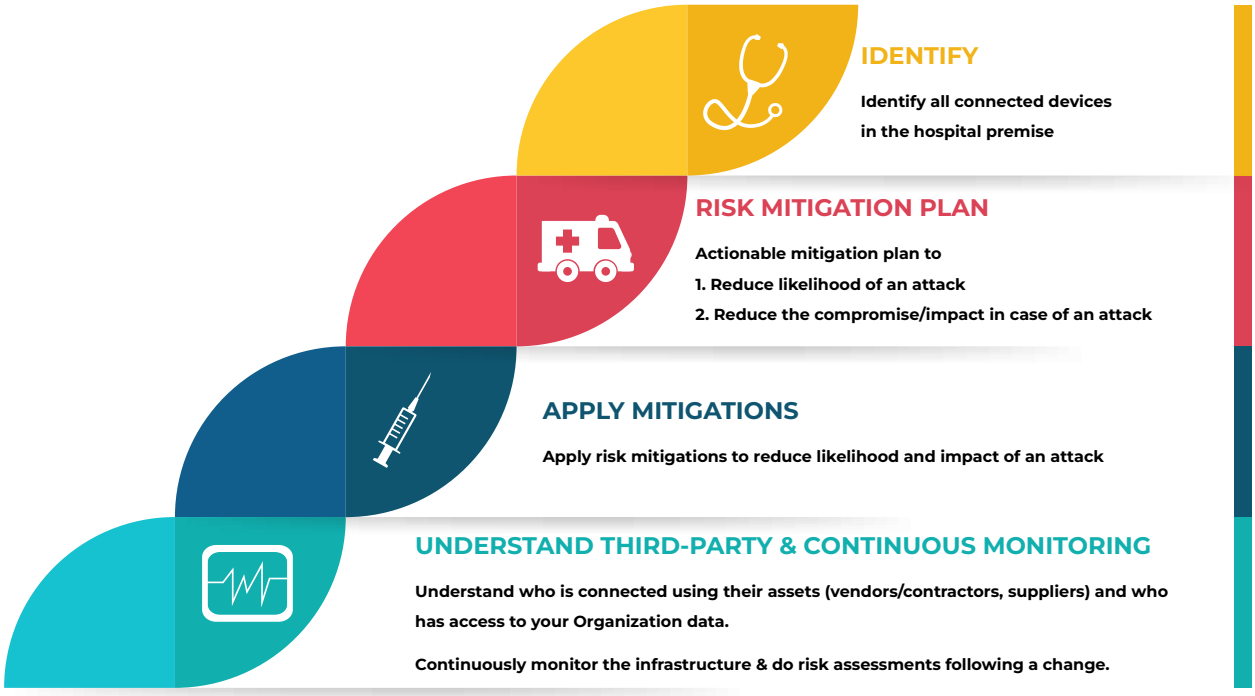
Securing Medical Devices: Best Practices

Risk Assessment

A thorough risk assessment is the first step in securing medical devices. Healthcare organizations must identify and evaluate the potential risks associated with each device. This includes assessing the device's intended use, data handling capabilities, and potential impact on patient safety. A risk assessment should also consider the device's exposure to network vulnerabilities and the level of protection required.

Secure Design and Development

Manufacturers should adopt secure design principles and adhere to cybersecurity best practices during the development of medical devices. This includes implementing encryption protocols, access controls, and regular software updates to patch vulnerabilities. Additionally, manufacturers should consider the entire lifecycle of the device, from design to disposal, and plan for secure end-of-life procedures.



Network Segmentation

Healthcare organizations should implement network segmentation to isolate medical devices from the broader hospital network. This limits the potential attack surface and ensures that even if one device is compromised, the entire network is not jeopardized. Segmentation should be complemented by strict access controls and monitoring.

User Authentication and Access Control

Robust user authentication mechanisms, such as biometrics or two-factor authentication, should be enforced for accessing medical devices. Access control policies should restrict device access to authorized personnel only, reducing the risk of unauthorized tampering.

Regular Updates and Patch Management

Software vulnerabilities are a common entry point for cyberattacks. Regularly updating and patching both the operating systems and software of medical devices is essential to mitigate these risks. Manufacturers should provide a mechanism for easy and secure updates, and healthcare organizations must prioritize timely installation.

Intrusion Detection and Monitoring

Implementing intrusion detection systems and continuous monitoring of medical devices and their network connections can help identify suspicious activities in real-time. This proactive approach allows for rapid response to potential security incidents.

Incident Response Plan

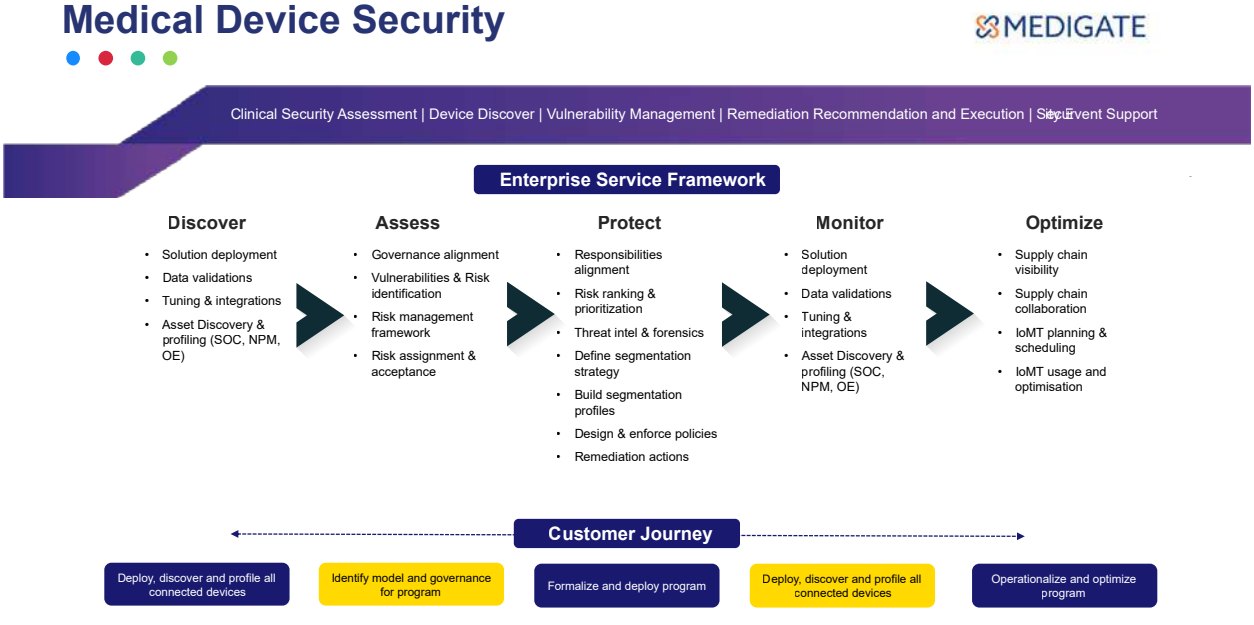
Having a well-defined incident response plan is crucial for mitigating the impact of security breaches. Healthcare organizations should establish clear protocols for reporting and responding to security incidents involving medical devices. This plan should encompass communication, isolation of compromised devices, forensic analysis, and patient notification if necessary.

Training and Awareness

Healthcare staff should receive regular training on cybersecurity best practices and be aware of the potential risks associated with medical devices. Creating a culture of security awareness among employees can significantly reduce the likelihood of human error leading to security breaches.

Leading Medical device security tools

- Medigate
- Asimily
- ORDR



About
the Author

Karthikeyan Manoharan is an accomplished Cybersecurity Architect with over 19 years of experience in the field. Karthik has successfully delivered several Cybersecurity projects viz Security Operations Center implementation, and compliance-related programs for reputed organizations across the Globe. Apart from Cybersecurity, he is a numismatist and interested in learning about several cultures.

Karthikeyan Manoharan

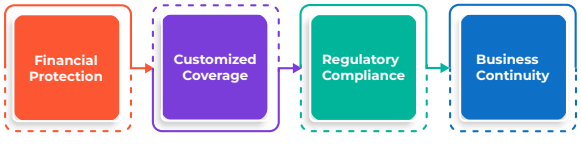
Cyber Insurance

Preparing for the Inevitable

In today's digital age, cyber threats are a stark reality for businesses of all sizes. From data breaches to ransomware attacks, no organization is immune to these potentially devastating events. This article will delve into some major areas of cyber insurance, highlighting its crucial role in modern risk management strategies.

The Role of Cyber Insurance

Cyber insurance plays a pivotal role in addressing and mitigating the consequences of cyber incidents, outlining four essential roles.



What does Cybersecurity Insurance Cover?

1st Party Damage

- **Forensic Analysis:** Costs to hire forensic experts to investigate and understand the breach.
- **Legal Guidance:** Expenses for legal consultants to navigate breach response laws and customer notifications.
- **Credit Monitoring:** Costs of providing credit monitoring to affected customers.
- **Public Relations:** Expenses to restore public trust in your organization.
- **Cyber Extortion:** Fees related to ransomware attacks under specific conditions.
- **Business Interruption:** Loss of revenue, customers, and system recovery costs due to a successful attack.

3rd Party Damage

- **Re-issuing of Credit Cards:** Costs borne by financial institutions.
- **Stolen Intellectual Property:** When your breach affects a third party.
- **Stolen Licensed Property:** Disclosure of licensed property after the breach.
- **Stolen Documents:** Including libelous/slanderous content about a third party.

What isn't Covered by Cybersecurity Insurance?

- **System Improvement:** Costs for vulnerability fixes and system redesign.
- **Hardware Damage:** Damage to physical hardware.
- **Mental Distress:** Executive, employee, or customer distress.

Application Process

The application process for cyber insurance involves submitting information on risk, data, security, and more.

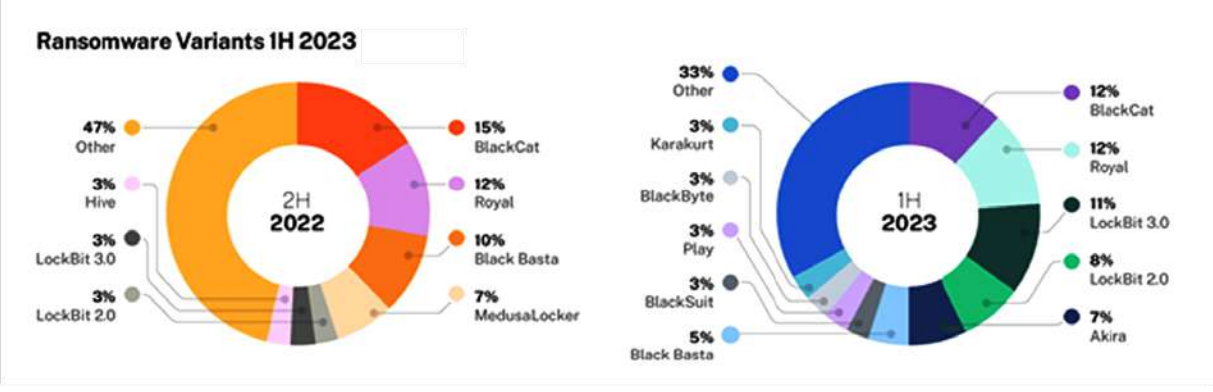
- **Policy Selection:** Define the coverage you need.
- **Industry and Revenue:** Share your industry and annual revenues.
- **Data Handling:** Describe the type and volume of data you manage.

- **Security Measures:** Provide details on firewalls, system updates, encryption, and more.
- **Device and Employee Policies:** Explain your policies on third party and employee devices.

What are Insureds' Responsibilities?

After obtaining cybersecurity insurance, individuals and businesses aim to avoid using it by maintaining strong security measures. Insurance providers typically require minimum-security controls such as MFA, EDR, encryption, backups, awareness training, patch management, email filtering, access controls, network segmentation, BCP/DR/IR plans, and more. Some insurers even offer cyber assurance security tools to reduce the risk of an attack.

A cyber insurance firm reported a sharp rise in claims during H1 2023, attributing it to increased damages from cyberattacks. Ransomware, accounting for 12% more claims than the previous year, was a major driver of this surge. May recorded the highest number of ransomware claims ever in Coalition's history. Large firms with revenues over $100 million experienced a 20% uptick in cyber incidents. Funds transfer fraud claims increased by 15%. However, business email compromise claims decreased by 15%, providing a rare positive note. Cyber insurance is a rapidly expanding industry, predicted to reach $50 billion by 2030.



Source: https://shorturl.at/rxRYZ

Real-World Scenarios

IBM's latest Cost of a Data Breach report discovered that, in 2023, the average cost of a data breach globally reached an all-time high of $4.45 million. This figure represents a 2.3% increase from the previous year and a 15.3% rise from 2020.

A Wall Street analyst said the losses MGM Resorts International is experiencing from a cyberattack on the company's hotel-casino operations in eight states could be covered by a $200 million cyber insurance policy covering ransom payments and business interruption.

University of California, San Francisco, faced a ransomware attack that encrypted critical data, including COVID-19 research. Cyber insurance helped cover expenses, facilitating data recovery, legal matters, and ensuring uninterrupted healthcare and research operations during the pandemic.

Final Thoughts

In tandem with technological progress, cybercriminal tactics evolve, emphasizing the need for proactive measures by individuals and organizations. Cyber insurance provides financial security, mitigating the impact of unforeseen cyber incidents. Investing in cyber insurance safeguards digital assets and ensures confidence in navigating the digital era's challenges.

About
the Author

Praveenkumar Jothi is a cybersecurity lead with 11 years of experience in the IT industry. His expertise encompasses IT infrastructure, Identity and Access Management (IAM), and the last five years have been dedicated to Governance, Risk, and Compliance (GRC). Additionally, Praveen is an active traveler and motorcycle enthusiast. He channels his passion for biking by running a biking club in the state.

Praveenkumar Jothi

Multi-level Approach to Access Security

When it comes to access management, identity is the common thing behind some of the breaches in the past few years. But the question is what approaches do we take to ensure secure access is applied in an organization. Let's dig into the concept of multi-layered approach to securing access.

First Things First – Authentication

SSO (Single Sign On) allows users to access what they want with a single set of credentials, without a requirement for repeated logins. But how will the tool know whether the person authenticating is a legitimate user? The same applies to MFA (multi-factor authentication) - attackers are finding ways to break the legacy MFA policies, such as 'MFA bombing'.

Some solutions that can address these issues:

- Automation-driven workflows – from an SSO that knows when to block a user's access, to an MFA that moves users to low-risk roles, after repeated failed login attempts.
- User behaviour analytics tool – Threat detection and the capability to respond

High-level protection to passwords

Nowadays employees have significant access to critical resources. What is standing between organization's resources and the attackers targeting those? The answer is passwords which lack visibility. What can be done regarding this? Below are the few areas to focus on.

Password Storage and Retrieval • Control over how credentials are stored, managed, and retrieved. • End-to-end encryption in transit or at rest for passwords. • Ability to host passwords in a secure cloud location or self-hosted vault.	**Sharing Passwords and Account Management** • Control over who can share, view, and edit passwords. • Set time limits for how long users can access shared passwords. • Settings to restrict saving passwords in browsers.
Secure User Experience • Ability to recognize when users are entering credentials into apps login forms and take automated action. • Offering to save them in a secure vault. • Securely auto-filling credential fields. • Ability to generate strong, complex, unique passwords.	**Audits and Reporting** • Insights on which employees have accessed specific apps during a particular time period. • Reporting capabilities to fulfil compliance and audit requirements.

Monitoring and Auditing user activities

How much visibility do we have into our employees' ability to change, delete, modify data within an app? Many organizations lack centralized visibility and tools for mitigating incidents like these.

The solution lies in having the ability to monitor an admin's sessions. Below is how we can do it.

- Continuously monitoring and recording user's activities in an application by capturing a step-by-step view of actions taken, with a clear audit trail.
- Automated function to identify when a session is left open and require re-authentication to help ensure an attacker hasn't compromised the user's device and identity.
- Controls for preventing specific actions like downloading or copying data.

Secure access for external vendors

External vendors also play a key role in helping organizations grow, compete, and see digital initiatives. Just as any employee's identity can become privileged, the same applies to external vendors. When they gain access to an organization's apps, services, they're also gaining access to high-risk resources. This provides another opportunity for attackers and yet another layer for IT security teams to protect. Few things to be consider here.

- When vendors log into apps containing sensitive data, do they have the same level of protection given to employees?
- When team members working for a third-party vendor start or leave their jobs, are you able to manage their identities with the same checks you'd apply to your own workforce?

Below are how we can reduce these risks:

- Ensure SSO and MFA layer of protection is followed even for vendors.
- Review the access granted at regular intervals.
- Ensure the provisioning and deprovisioning through automated workflows instead of manual to avoid risk.

Wrapping it up

In an era where it takes just one mismanaged identity or compromised credential for an attacker to break into the system, no single tool or solution can protect every identity, resource, environment. It is important for us to uncover security gaps and add layers of IAM capabilities on top of the existing solutions. Adopting to a multi-level approach can greatly reduce the enterprise attack surface and help us mitigate vulnerabilities before attackers can take advantage of them.

About
the Author

Madhumitha K has 3+ years of experience in IT and is a InfoSec engineer. Her areas of expertise include Identity and Access Management and network security. Outside of work she is passionate about travel based content creation and food with a hunger to explore the unexplored.

Madhumitha K

InfoSec Champions

We would like to thank all those who have helped us in identifying suspicious cyber activities.

- Anand Somisetty
- Nirmala Mary
- Swagata Khanolkar
- Antraj Khaire
- Tanmayee Joshi
- Jayesh Prajapati
- Sumit Deokar
- Devashree Brahme
- Farha Khan
- Amol Jain
- Vijayraj Chingunde
- Tushar Kadu
- Akhtarjahan Mulla
- Ajay Rege
- Amogh Sherkar
- Shubham Nandi
- Anay Khangan
- Giriraj Shete
- Aniket Nimkar
- Balamurugan Gopal
- Julian Picardo
- Karthik Manoharan
- Rahul Garapaty
- Ramya Subramaniam
- Sabarish R
- Srinath Mohanraj

Note: This is not an exhaustive list.

enGAge

www.gslab.com | www.gavstech.com

Follow us on: