CONNECT

MAGAZINE

OCT ‘24

CYBERSECURITY SPECIAL EDITION

#SECUREOURWORLD

Security is always excessive until it’s not enough.

- Robbie Sinclair

Welcoming Our New CEO

Harmeet Chauhan

Featuring

Madhumita Sarkar

Director, Information Security, Englewood Hospital

Ramana Chamarti

Chief Architect, Frontier Airlines

Table Of Content

Editor’s Note

Soumika Das

Welcome to the Cybersecurity Special Edition of CONNECT!

This October, as we observe Cybersecurity Awareness Month, it's crucial to remember that our strongest defense against cyber threats isn't just sophisticated software or complex algorithms—it's us. Humans are both the greatest asset and the weakest link in the cybersecurity chain.

Statistics paint a stark picture: according to a study, a staggering 95% of cybersecurity breaches are caused by human error. This underscores the critical role we play in safeguarding our digital world. Cybercriminals are masters of manipulation, exploiting our natural tendencies through sophisticated phishing attacks and social engineering tactics. They prey on our trust, curiosity, and even our desire to help, tricking us into clicking malicious links, downloading infected files, or revealing sensitive information.

But we are not helpless. By cultivating a culture of awareness and vigilance, we can become powerful human firewalls. Throughout October, we will be hosting a series of cybersecurity awareness activities in our office, including polls, webinars, and interactive sessions. These events are designed to keep you informed about the latest threats and best practices in cybersecurity. Your participation is crucial in building a security-conscious environment—stay informed, ask questions, and apply what you learn in your daily work. Together, we must align our actions to the best practices that #SecureOurWorld.

Fostering a security-conscious mindset is key. Remember, cybersecurity is not just an IT issue; it's a human issue. By recognizing our role in the fight against cybercrime, we can transform ourselves from potential vulnerabilities into powerful agents of protection. Let's embrace Cybersecurity Awareness Month as an opportunity to strengthen our human firewall and build a safer digital future for all.

For this edition, we spoke to **Madhumita Sarkar, Director, Information Security, Englewood Hospital**. She has penned a note on the role of senior leaders in shaping, supporting and promoting cybersecurity. We also spoke with **Ramana Chamarti, Chief Architect, Frontier Airlines**, who discussed the cybersecurity implications of emerging technologies like edge computing, wearable devices, AI, and cloud adoption.

We have insightful articles lined up for this edition.

Kannan Srinivasan has written, **Improving Healthcare Cybersecurity Maturity**.

Dheepanraj K has written, **Deepfake Phishing Using AI: A Growing Threat**.

Kumaresan Periyasamy has written, **Level Up Your Android's Defenses: A Practical Guide**.

Bhavani Damodaran has written, **BSOD and the World: Risks of Unverified Updates to Production**.

Shalini J and **Sri Priyadharshini A** have written, **Understanding Data Loss Prevention (DLP)**.

Hashini Yuvaraj has written, **The Impact of Generative AI on Cybersecurity: Navigating Opportunities and Challenges**.

Anitha R has written, **3 Forward-thinking Practices to Manage IT Risk**.

Happy Reading!

Accelerating Growth

Welcoming Our New CEO, Harmeet Chauhan

“I am excited and truly honored to join GS Lab | GAVS at this inflection point in its journey. I deeply resonate with the Company’s values of **Respect**, **Integrity**, **Trust**, and **Empathy**, its commitment to purpose-led growth, and will build on their AI-led strategy to deliver exceptional outcomes for our clients.”

Congratulating Sumit Ganguli on his new role as Vice Chairman

“All of us will immensely benefit from Harmeet’s stewardship at GS Lab | GAVS. He will be a strong force multiplier in GS Lab | GAVS’ purposeful growth and value creation journey. I will continue to serve our clients and colleagues as the Vice Chairman and Board Member of GS Lab | GAVS. I am extremely excited about the future of GS Lab | GAVS.”

Click here to know more

Leader's Perspectives

"Several emerging technologies will significantly impact cybersecurity in the coming years. Edge computing and Edge AI, for example, are enabling more processing and decision-making to occur closer to where data is generated. This can improve performance and reduce latency, but it also creates new security challenges. Wearable devices are also becoming increasingly common, and many of these devices collect sensitive data. This data can be valuable to attackers, so it is important to ensure that wearable devices are properly secured. AI is also playing an increasingly important role in cybersecurity. AI can be used to automate many security tasks, such as threat detection and incident response.

IoT is prevalent and in aviation it is being used to improve efficiency and safety of operations. For example, we send details on the gradient of the flight that the pilot should take to avoid overconsumption of fuel. Continuous monitoring is important to ensure security.

Cloud adoption is also increasing rapidly. Cloud providers offer a variety of security features including encryption, but it is important for customers to understand these features and to configure them properly. It is also important for customers to understand their own security responsibilities when using cloud services."

Ramana Chamarti
Chief Architect,
Frontier Airlines

Introducing
Madhumita Sarkar

Director, Information Security, Englewood Hospital

1. Tell us something about your childhood. What values had been instilled in you that helped you excel later in your life?

I come from a very humble background where my parents worked hard to raise me and my two younger siblings and our cousin, who stayed with us when we were kids. So, they were raising 4 kids at the same time with limited income. This was the perfect recipe to instill traits like sharing, being considerate, helping others and being sensitive toward any life around you, and having a sense of responsibility towards society and nation.

As the oldest among my siblings, I was closest to my mom who was talented, hardworking, kindhearted, and a smart housewife, my dad was working in a government organization but was honest and hardworking and never compromised with his ethics. Both of my parents were incredibly skilled and versatile individuals who enjoyed engaging in various tasks, ranging from cleaning the house and crafting small furniture to sewing clothes, tending to the garden, and repairing electronic devices. They were adept at handling almost every household chore and DIY project imaginable. Hence, I got this love for doing everything on my own from both and that helped me to be independent.

I also drew inspiration from the stories of moral science books that were part of the curriculum for 80-90 kids, and I wanted to do the best and be the best. I grew up in Kanpur, UP, India, a multicultural society and always had my parents' support to do what I loved to do. I studied Home Science but after my bachelor's degree, computer science especially hardware, network and security of digital world caught my attention, and I did Diploma and then a few years later master's in computer science.

The person I am today is the product of every moment of my parent's guidance and their life examples, friends and family and many of my colleagues who taught me how to deal with the life and souls around you, to be a better self in your personal and professional life.

2. How would you define success?

For me success is something that I feel deep down, and that feeling comes as a result of the pursuit of reaching the goal, no matter how big or small that goal is. However, success could be short and long term and it requires it shares of hard work, grit, perseverance & passion. You succeed when you do what you love to do. I am yet to achieve my ultimate Success!

3. What motivated you to pursue a career in digital security?

I loved the job of fixing things, specially dissecting and investigating the facts and details around anything that is unknown to many and needed revelation for justice. I would have loved to become an investigating officer but when that did not happen, I told myself it is never too late, get into digital world, protect organizations, and fix it when something goes wrong. Cybersecurity is not just my job; it is my passion.

4. Could you please tell us about some of the social causes you support?

Absolutely, till today I have raised funds by selling my artwork that includes realistic paintings, sketching, portraits, wood & mirror crafts & fashion jewelries. I also contribute to fund these, and they are:
Rehabilitation of riots/accident victims
Assistance to families from low-income groups to start small businesses.
Families facing difficulties in covering medical expenses.
Students struggling to pay their fees for education.
Providing funding for initiating projects for self-help groups.
My non-financial work includes:
Free career guidance to the youth in India over phone.
Free online art and cyber security classes.
Provide voluntary services to elderly living in old age homes (in the US).

5. Looking back on your journey and knowing what you know now, what is the one piece of advice you would have given yourself along the way?

“Mita, learn the art of communication and language, this will help articulate yourself better and you can achieve anything with all other qualities and skills you have.”

I strongly believe the art of selling is important too. Unfortunately, I currently lack proficiency in this area, which limits my ability to effectively monetize my artwork for funding my endeavors in social causes. However, I am not giving up and remain determined to improve them for better results in future.

6. What advice would you give to young women who are starting their careers now?

Dream big, follow your heart, give your 100% and never hesitate to ask for help, there are many angels looking to help you!

Madhumita on the involvement of senior leaders in shaping and supporting cybersecurity policies and in promoting cybersecurity awareness within their organizations.

The involvement of Senior Leadership varies from organization to organization and the industry type. However, in general best practices recommends that since the landscape of Cyber Threat keeps evolving, we need to keep educating our leaders so that they understand the importance of Cybersecurity Awareness and Training in order to train the entire organization so they act as the first line of defense.

A new trend has been observed recently in the Cybersecurity pitch that senior leaders are taking initiative in hiring Cybersecurity consulting firms and vCISO services to address the policy gap that is arising because of the fast-pacing evolution of IT technologies, specifically AI based services in all segments of IT services and tools.

It is recommended that each organization that is onboarding new technologies, IT solutions, applications and tools to service their business needs should have a mandatory cybersecurity awareness program with focus on top-down approach. Cybersecurity should be discussed in every Department meeting to ensure that Cybersecurity is not only IT/Security responsibility but everyone's responsibility.

University of California, Riverside (UCR) has published a paper that recommends leaders to leverage various leadership styles to an advantage when it comes to combating cybersecurity challenges in their organizations. Some of the leadership they recommended are:

- Collaborative leaders promote cross-functional communication and cooperation, breaking down silos that may impede the sharing of crucial information. This open communication facilitates a more comprehensive understanding of potential threats and vulnerabilities, enabling a more robust cybersecurity strategy.
- Transformational leadership - In the context of cybersecurity, this style encourages a proactive approach towards identifying and addressing potential threats. Such leaders foster a transformational environment to instill a sense of responsibility and accountability among team members, promoting a collective effort to safeguard sensitive information
- Transactional leaders - In the cybersecurity context, adhering to established protocols and compliance measures is the priority. Such leaders ensure that team members follow standardized security practices, reducing the likelihood of human error and exploitation of vulnerabilities.
- Situational Leaders adapt an approach based on the specific challenge at hand, whether it's a sudden breach or a sophisticated attack, these leaders guide their teams through effective crisis management and response strategies.
- People-first leaders can contribute to a strong cybersecurity posture by prioritizing the well-being and development of team members. In the context of cybersecurity, this can translate to a workforce that is more vigilant and committed to upholding security best practices.

Apart from these leadership practices to develop a healthy and effective cybersecurity culture, it is important that an effective Cybersecurity program and tool is implemented to educate ever employee, contractor and consultant who has access to the organization's assets at any capacity..

About Madhumita Sarkar

As a seasoned digital security executive, Madhumita brings 25 years of corporate leadership across technology, healthcare, education, retail, and banking. Renowned for leading cyber-security teams and developing IT risk management programs, she has driven business growth. Her key areas of expertise include information security strategy, website security, global data protection, technology solutions, and project management. She is also an artist and social worker.

Enabling Education Through Inclusion and Infrastructure

We undertook a project at **Government Higher Secondary School, Vennangupattu, Tamil Nadu**, to construct new classrooms for the school for the underprivileged, to provide a more conducive learning environment for young children, thereby encouraging improved enrolment for the academic year and better educational outcomes. The contribution from the CSR team was end-to-end, including site selection, design, planning, and construction of the classrooms. We are proud and humbled by the positive impact that this project has had through our commitment to giving back to society.

Our project focused on two remote schools, **Shiravali Madhyamik Vidyalaya and ZP Primary School, Ramoswadi, Hatmoshi**, situated deep within the hills of Bhor, 85 km from Pune, which are serving 14 villages within a 20 km radius for the educational needs of young children. Recognizing the significant challenges faced by students who had to walk long distances to reach school, we implemented several initiatives to improve their learning environment. These improvements have not only enhanced the overall learning experience for the students but have also contributed to the overall development of the community.

Improving Healthcare Cybersecurity Maturity

A Comprehensive Approach

In today's fast-changing healthcare environment, keeping patient information safe and making sure healthcare systems stay secure is crucial. To defend against cyber threats effectively, healthcare organizations need a clear plan that includes understanding their cybersecurity maturity, tracking their progress, and setting clear Service Level Agreements (SLAs) and Key Performance Indicators (KPIs). This article will break down these elements and show how they can help improve cybersecurity.

Understanding Cybersecurity Maturity Levels

Cybersecurity maturity is about how well an organization can spot, defend against, find, respond to, and recover from cyber threats. Maturity models offer a way to evaluate and improve these skills. These models are usually divided into different levels to help organizations understand their progress.

01. Initial (Ad Hoc): At this level, cybersecurity practices are often inconsistent and reactive. There is a lack of formal processes, and security measures are implemented as issues arise rather than proactively.
02. Developing (Repeatable): Organizations at this stage have begun to establish and document cybersecurity policies and procedures. Security practices are becoming more consistent, but there may still be gaps in implementation and adherence.
03. Defined (Established): Cybersecurity processes are well-defined and integrated into the organization's overall risk management strategy. There is a clear understanding of roles and responsibilities, and practices are routinely reviewed and updated.
04. Managed (Quantitatively Managed): At this level, cybersecurity practices are quantitatively managed. Metrics and KPIs are used to measure the effectiveness of security controls, and there is a strong emphasis on continuous improvement based on data-driven insights.

05. Optimizing (Adaptive): The organization continuously optimizes its cybersecurity practices based on emerging threats and technologies. There is a focus on innovation and adaptive strategies to stay ahead of evolving risks.

Tracking Cybersecurity Maturity

Tracking cybersecurity maturity involves assessing progress against the maturity model and identifying areas for improvement. This can be achieved through:

01. Regular Assessments: Conduct periodic maturity assessments using established models like the NIST Cybersecurity Framework or the CMMI Cyber Maturity Platform. These assessments help identify current maturity levels and areas that need enhancement.
02. Internal Audits: Regular internal audits help ensure that cybersecurity policies and procedures are being followed and identify potential gaps or weaknesses in the implementation.
03. Third-Party Reviews: Engaging external experts to review and assess cybersecurity practices provides an unbiased perspective and can uncover issues that internal teams might overlook.
04. Documentation and Reporting: Maintaining detailed records of cybersecurity practices, incidents, and improvements helps track progress over time and provides a basis for reporting to stakeholders.

Service Level Agreements and Key Performance Indicators

SLAs and KPIs are critical in managing and measuring cybersecurity performance. They help set expectations, monitor effectiveness, and drive improvements

Service Level Agreements

Incident Response Time: Specifies how quickly the organization must respond to and fix security problems.

System Availability: Sets the expected level of system uptime and how often the system should be operational.

Data Breach Notification: Details how quickly the organization must inform stakeholders and regulators if there's a data breach.

Key Performance Indicators

Incident Detection Rate: Shows how many security incidents are caught by the organization's monitoring systems.

Incident Response Time: Measures the average time taken to address and resolve security issues.

Patch Management: Evaluates how quickly and effectively security updates and patches are applied.

Employee Training: Tracks the percentage of employees who have completed required cybersecurity training.regulators if there's a data breach.

Implementing an Improvement Strategy

To improve cybersecurity maturity effectively, healthcare organizations should consider the following strategies:

Service Level Agreements

Incident Response Time: Specifies how quickly the organization must respond to and fix security problems.

- Buy-in from senior management for cybersecurity: Getting buy-in from senior management for a cybersecurity improvement strategy is crucial for its success. Senior leaders must understand the value of cybersecurity investments and how they align with the organization's overall goals.
- Create a Strong Cybersecurity Plan: Develop a clear strategy that matches your organization's goals and tackles identified risks. Include regular reviews and updates to keep improving.
- Invest in Staff Training: Provide ongoing training to ensure all employees understand their role in protecting sensitive information and staying up-to-date with cybersecurity practices.

- Use Advanced Technology:
  Implement cutting-edge cybersecurity tools and automation to improve threat detection, response, and overall security management.
- Build a Security-Focused Culture:
  Encourage everyone in the organization to take responsibility for cybersecurity and adopt proactive security practices.
- Update Policies Regularly:
  Frequently review and revise cybersecurity policies and procedures to address new threats and changes in regulations.
- Communicate with Stakeholders:
  Keep open lines of communication with patients, partners, and regulatory bodies to maintain transparency and trust in your cybersecurity efforts.

Improving healthcare cybersecurity maturity is crucial for several key reasons

Protecting Sensitive Data:
Safeguards patient information from breaches and unauthorized access.

Adapting to Threats:
Keeps pace with evolving cyber threats and sophisticated attacks.

Reducing Financial Impact:
Mitigates the costs associated with breaches and cyberattacks.

Ensuring Patient Safety:
Protects interconnected systems that are vital to patient care.

Compliance:
Ensures adherence to regulations like HIPAA, avoiding legal and financial penalties.

Maintaining Trust:
Preserves patient trust and protects the organization's reputation.

Improving Incident Response:
Enhances readiness and response to security incidents.

Encouraging Innovation:
Supports secure adoption of new technologies.

Preventing Disruptions:
Minimizes the risk of operational shutdowns and delays in patient care.

A mature cybersecurity approach is essential for maintaining secure, reliable, and compliant healthcare operations.

Toolkit: Tabletop Exercise for Ransomware Response

01. Preparation
    Objective Setting: Define goals (e.g., assess incident response, identify gaps).
    Participants: Include IT, management, legal, and communications.
    Scenario Development:
    Create a realistic ransomware scenario.
    Materials: Gather the incident response plan, contact lists, and relevant policies.
    Facilitator: Appoint someone to guide the exercise.

02. Exercise Design
    Scenario Overview: Outline the ransomware attack details (type, infection method, impact).
    Injects: Plan key events to introduce during the exercise.
    Role Definitions:
    Assign roles (e.g., Incident Commander, IT Lead).

03. Conducting the Exercise

Briefing: Explain objectives, rules, and scenario.
Scenario Walkthrough: Present the scenario and
use injects to simulate evolving conditions.
Discussion: Facilitate discussions on responses, decisions, and actions.
Documentation: Record decisions, actions, and identified issues.

04. Post-Exercise Activities

Debriefing: Review what worked, what didn't, and lessons learned.
Evaluation: Assess response effectiveness and identify improvements.
Action Plan: Develop a plan to address gaps, with timelines and responsibilities.
Report: Summarize findings and recommendations, and share with stakeholders.
Follow-Up: Plan meetings to review progress and ensure preparedness.

This streamlined approach helps ensure your organization is well-prepared for ransomware attacks.

Streamlined Survey of Organizational Cyber Maturity

Objectives:

- **Evaluate Practices:** Assess cybersecurity maturity across industries.
- **Identify Gaps:** Spot strengths and weaknesses.
- **Benchmark:** Compare against established frameworks.
- **Provide Recommendations:** Offer actionable improvement insights.

Design:

- **Industry Focus:** Target sectors like healthcare, finance, and manufacturing.
- **Criteria:** Evaluate policies, risk management, incident response, and training.

Key Areas:

- **Governance:** Policies, oversight, risk management.
- **Technical Controls:** Firewalls, encryption, vulnerability management.
- **Incident Response:** Planning, testing, recovery.
- **Compliance:** Adherence to regulations (e.g., HIPAA, GDPR).
- **Training:** Quality and frequency of cybersecurity training.
- **Threat Intelligence:** Use of threat monitoring and intelligence.

Data Collection:

- **Methods:** Online surveys, interviews, workshops.
- **Questionnaire:** Develop a detailed questionnaire.
- **Sources:** IT staff, cybersecurity leaders, management.

Analysis and Reporting:

- **Analyze:** Identify trends and gaps.
- **Benchmark:** Compare best practices.
- **Report:** Summarize findings and recommendations.

Recommendations:

- **Improvement Strategies:** Tailor recommendations for each industry.
- **Best Practices:** Suggest industry-wide practices.
- **Action Plans:** Outline steps to address identified weaknesses.

Follow-Up:

- **Reassessments:** Recommend periodic reviews.
- **Collaboration:** Encourage sharing insights across industries.

This approach provides a clear picture of cybersecurity maturity and helps organizations enhance their defenses relative to industry standards.

About the Author

Kannan is the Head of Cybersecurity & Data Privacy at GS Lab | GAVS. He 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

Live **Webinar**

gslab | GAVS

Navigating Security Challenges in the Age of AI:

Best Practices and Emerging Threats

Speaker
Ryan Yardis
VP, IT Infrastructure and Security, embecta

Speaker
Howard Estcourt
Director, Information Security Engineering, embecta

Speaker
Kannan Srinivasan
Head, Cybersecurity and Data Privacy, GS Lab | GAVS

Moderator
Bhavani Damodaran
Senior Technical Manager, Information Security, GS Lab | GAVS

18 OCT
9:00 AM **EST**
6.30 PM **IST**

#SecureOurWorld

Webinar

The digital landscape is rapidly transforming with the rise of artificial intelligence (AI). While AI offers tremendous opportunities for innovation and efficiency, it also introduces new and complex cybersecurity challenges.

Join our panel of industry experts as they delve into the critical topic of cybersecurity awareness in this AI-driven era.

Agenda

- The Evolving Threat Landscape
- Opportunities and Challenges of AI
- Managing AI and Personal Data
- Protecting Organizational Data
- User Awareness for Safe AI Sharing

Register Here

Deepfake Phishing Using AI: A Growing Threat

As technology evolves, advancements are rapidly being made in fields such as medicine, research, and more. However, it is not without concerns. In recent times, artificial intelligence (AI) has been increasingly leveraged across various industries, providing numerous benefits. Unfortunately, hackers are also exploiting AI, using it to create realistic but fake audiovisual content designed to deceive individuals into divulging sensitive information.

What is Deepfake Phishing?

Deepfake phishing is a sophisticated scam where attackers use AI-generated deepfake technology to create convincing but fake audio or video content. This content is designed to impersonate someone you trust—such as your boss, a colleague, or a service provider—with the goal of tricking you into revealing sensitive information or transferring funds.

How Does Deepfake Phishing Work?

Deepfake phishing operates on the same core principle as other social engineering attacks: confusing or manipulating users, exploiting their trust, and bypassing traditional security measures. Attackers can weaponize deepfakes for phishing attacks in several ways:

- Impersonation in Video Calls:
  Attackers can employ video deepfakes during Zoom or other video calls to convincingly pose as trusted individuals. This can lead to victims disclosing confidential information, such as credentials, or authorizing unauthorized financial transactions.
- Voice Cloning:
  By cloning someone's voice with near-perfect accuracy, attackers can leave voicemail messages or make phone calls that sound convincingly real.

Real-Life Example
One notable instance of deepfake phishing involved a scammer in China who used face-swapping technology to impersonate a trusted individual. The scammer successfully tricked the victim into transferring $622,000. Such incidents underscore the growing danger of video deepfakes in phishing attacks.

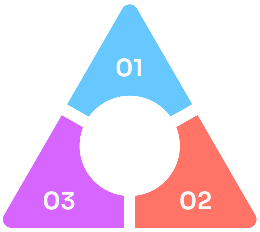
Why Should Organizations be Concerned about Deepfake Phishing?

It's a Fast-Growing Threat

Deepfake technology is becoming increasingly sophisticated and accessible thanks to generative AI tools. In 2023, incidents of deepfake phishing and fraud surged by an astounding 3,000%.

It's Difficult to Detect

AI can mimic someone's writing style, clone voices with near-perfect accuracy, and create AI-generated faces that are indistinguishable from real human faces. This makes deepfake phishing attacks extremely hard to detect.



It's Highly Targeted

Attackers can create highly personalized deepfake attacks, targeting individuals based on their specific interests, hobbies, and network of friends. This allows them to exploit vulnerabilities that are unique to select individuals and organizations.

How Can Organizations Mitigate the Risk of Deepfake Phishing?

01. Improve Employee Awareness of Synthetic Content: Employees should be made aware of the increasing proliferation and distribution of synthetic content. They must learn not to trust an online persona, individual, or identity solely based on videos, photos, or audio clips on an online profile.
02. Train Employees to Recognize and Report Deepfakes: Human intuition is a powerful tool in phishing prevention and detection. Employees should be trained to recognize and report fake online identities, visual anomalies (such as lip-sync inconsistencies), jerky movements, unusual audio cues, and irregular or suspicious requests. Organizations that lack this training expertise might consider phishing simulation programs that use real-world social engineering scripts.
03. Deploy Robust Authentication Methods to Reduce Identity Fraud Risk: Using phishing-resistant multi-factor authentication and zero-trust architecture can help reduce the risk of identity theft and lateral movement within systems. However, security leaders should anticipate that attackers may attempt to bypass authentication systems using clever deepfake-based social engineering techniques.

Improving Solutions to Detect Deepfake Threats

McAfee has introduced a significant upgrade to its AI-powered deepfake detection technology. Developed in collaboration with Intel, this enhancement aims to provide robust defense against the escalating threat of deepfake scams and misinformation. The McAfee Deepfake Detector leverages the advanced capabilities of the Neural Processing Unit (NPU) in Intel Core Ultra processor-based PCs to help consumers distinguish real content from manipulated content. Deepfake phishing represents a rapidly growing threat that is difficult to detect and highly targeted. As attackers continue to refine their methods, organizations must be proactive in enhancing their defenses. By raising awareness, training employees, and deploying advanced security measures, organizations can mitigate the risks associated with deepfake phishing and protect their sensitive information from this evolving threat.

About the Author

Dheepanraj K has over 6 years of experience in the field of cybersecurity. His career has been dedicated to safeguarding digital assets, identifying vulnerabilities, and implementing robust security measures to protect organizations from cyber threats. With a deep understanding of the evolving landscape of cybersecurity, he is passionate about staying ahead of emerging threats and leveraging advanced technologies to ensure the highest level of security. His expertise spans across various domains, including threat detection, risk assessment, and incident response, enabling him to effectively mitigate risks and safeguard critical information.

Dheepanraj K

Level Up Your Android's Defenses: A Practical Guide

In today's digital age, smartphones are integral to our daily lives, storing a wealth of personal and sensitive information. As such, securing these devices is paramount. Android, being one of the most widely used operating systems, requires particular attention to security hardening. This comprehensive guide will walk you through the essential steps to secure your Android device against potential threats.

01. Update Operating System and Applications

Regular updates are crucial for security. They not only enhance functionality but also address vulnerabilities that could be exploited by attackers.

Check for system updates:
Go to
Settings → System → Advanced → System update.

Update apps regularly:
Enable automatic app updates in the Google Play Store settings to ensure all applications are running the latest versions.

02. Install Trusted Security Software

Install a reputable antivirus and security app to add an extra layer of defense against malware, viruses, and other malicious activities.

Choose a trusted antivirus:
Look for well-reviewed security apps on the Google Play Store.

03. Enhance Lock Screen Security

Securing your device with a robust lock screen is your first line of defense against physical access.

Use strong authentication:
Opt for a combination of a PIN, pattern, or password that is difficult to guess. Consider using biometric options like fingerprint scanning or facial recognition if available.

04. Enable Full Device Encryption

Encryption ensures that your data remains secure, making it unreadable without the proper decryption key.

Activate encryption:
Newer Android devices are encrypted by default, but you can check this under Settings → Security.

05. Manage App Permissions

Apps can request access to various functions and data on your device, which can be a major privacy concern.

Review permissions:
Regularly audit app permissions by going to Settings → Apps & notifications → Advanced → Permission manager.

06. Disable Installation from Unknown Sources

Preventing installation from unknown sources mitigates the risk of inadvertently installing malicious apps.

Restrict app installation:
Navigate to Settings → Security → and ensure the option to install apps from unknown sources is disabled.

07. Use Secure Networks

Using public Wi-Fi can expose your device to interception by cybercriminals.

Avoid public Wi-Fi for sensitive transactions:
Use trusted networks or a VPN service when performing sensitive operations like online banking.

08. Turn off Bluetooth and NFC When Not Needed

Wireless technologies can be exploited to gain unauthorized access to your device.

Manage connectivity settings:
Disable Bluetooth and NFC from the quick settings menu when not in use.

09. Regular Data Backups

Backing up your data regularly ensures you can recover your personal information in the event of a device compromise.

Use cloud backup:
Android offers integrated backup options through Google Drive which can be configured under
Settings → System → Backup.

10. Limit Ad Tracking

Limiting the amount of personal data collected by advertisers is crucial for privacy.

Adjust ad settings:
Opt-out of personalized advertising in Google settings to enhance privacy.

11. Review and Configure Security Features

Android comes with built-in security features that need to be activated and configured properly.

Enable features like 'Google Play Protect' and 'Find My Device':
These can be found under
Settings → Security.

12. Stay Informed About Phishing and Scams

Awareness is key in combating phishing and scams. Educate yourself about common tactics used by cybercriminals to steal personal information.

Be cautious:
Avoid clicking on suspicious links or downloading attachments from unknown sources.

Securing an Android device involves a combination of keeping the software updated, managing permissions, and using security features effectively. By following the steps outlined in this guide, you can significantly enhance the security of your Android phone and safeguard your personal information from potential threats. Regular vigilance and adherence to these practices are essential in the evolving landscape of mobile security.

About the Author

Kumaresan has more than 17+ years of Technology experience in Cyber Security, IT Infrastructure Audit, Risk Management, Compliance and Project Management. He has done his MBA in IT Systems. Kumaresan has rich experience in Information Security, GRC, Information Technology Audit, Compliance Audits and Program Management.

Kumaresan Periyasamy

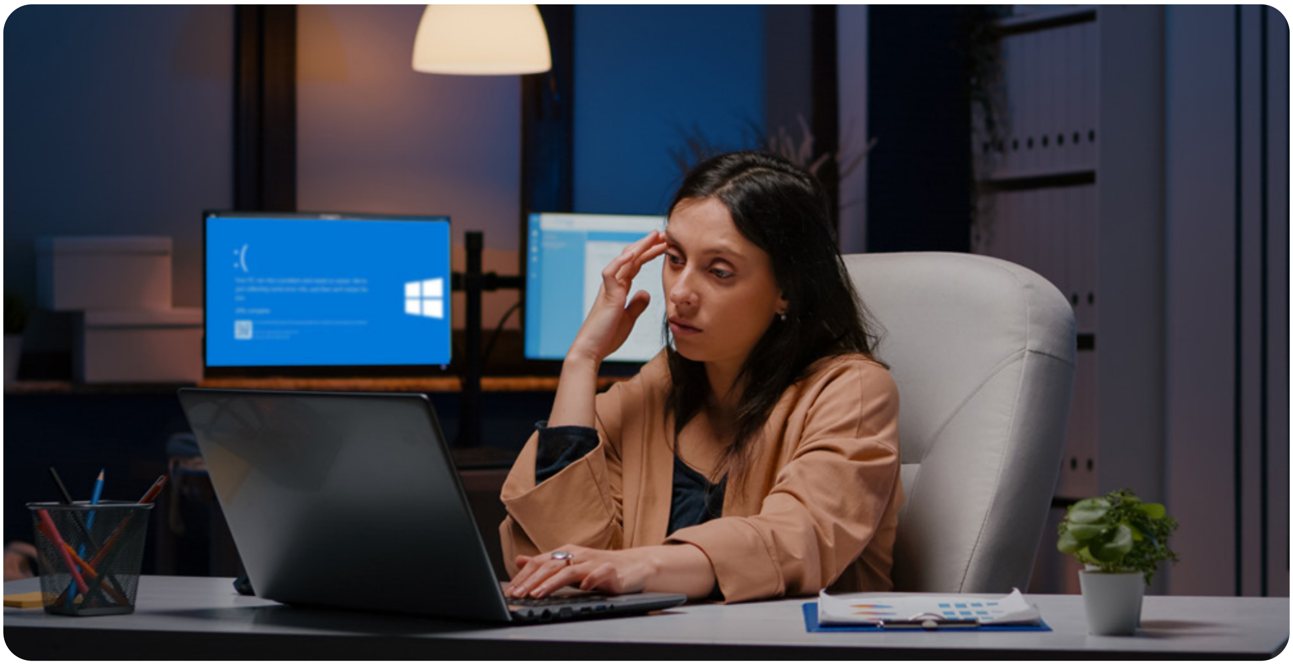
Cybersecurity Awareness Month

October 2024

Browse **Smart,** Stay **Safe.**

Use **Secure Connections** & Encrypt **Sensitive Data**.

#SecureOurWorld



BSOD and the World: Risks of Unverified Updates to Production

In the world of software development and IT operations, ensuring the stability and reliability of updates before they are deployed across all systems is critical. This principle is especially important for cybersecurity solutions like CrowdStrike Falcon, where updates must be meticulously tested to prevent issues such as the recent Blue Screen of Death (BSOD) incident. This article explores why testing production updates is crucial and outlines best practices for mitigating risks associated with widespread deployment.

On July 19, 2024, an update to CrowdStrike's Falcon endpoint detection and response (EDR) platform caused a Blue Screen of Death (BSOD) on many Windows computers globally. Most users' day started with an error screen and inability to access their asset. The issue caused significant disruption across various sectors. Though the root cause of the issue was identified on the same day, a workaround was done by IT professionals who physically booted every Windows machine into safe mode and removed a channel file to get the system to boot normally again. This took anywhere between a few hours for smaller organizations to a couple of days for large organizations.

The Risks of Unverified Updates

When updates are pushed to all machines without adequate testing, several risks arise:

1. System Instability: Unverified updates can cause crashes, slowdowns, or other instability issues. This is particularly problematic for systems that rely on continuous uptime, such as those in a business or production environment.
2. Data Loss: Unexpected crashes or system failures due to faulty updates can lead to data loss, especially if there are no recent backups.
3. Security Vulnerabilities: Inadequate testing might introduce new vulnerabilities or fail to address existing ones, potentially exposing systems to cyber threats.
4. Operational Disruption: For organizations, widespread issues resulting from faulty updates can lead to significant operational disruptions, impacting productivity and service delivery.
5. User Frustration: Frequent issues or downtime due to problematic updates can lead to frustration among users, affecting morale and trust in the software.

Best Practices for Testing Updates

To minimize the risks associated with deploying updates, organizations should adhere to the following best practices:

- **Staging Environment Testing:** Before rolling out an update to the entire production environment, test it in a staging environment that mimics the production setup. This helps identify potential issues without affecting live systems.
- **Phased Rollout:** Implement updates in phases or using a gradual rollout strategy. Start with a small group of users or systems and monitor the performance before expanding the deployment to the broader user base.
- **Automated Testing:** Utilize automated testing tools to run regression tests and verify that new updates do not break existing functionalities or introduce new issues.
- **Beta Testing:** FEngage a select group of users to test the update in real-world conditions. Collect feedback and monitor for any issues that might not have been caught in earlier testing phases.
- **Monitoring and Rollback Mechanisms:** Implement robust monitoring systems to quickly identify any problems arising from new updates. Ensure that rollback mechanisms are in place to revert to a previous stable version if necessary.
- **Communication Plan:** Clearly communicate with users about upcoming updates, including potential impacts and any required actions on their part. Provide timely updates on any issues and resolutions.
- **Documentation and Feedback:** Maintain thorough documentation of testing procedures and results. Gather feedback from users who experience issues and use this information to refine future updates.

Case Study:
CrowdStrike Falcon Update Incident

The recent CrowdStrike Falcon update incident, highlights the critical need for comprehensive testing protocols:

- **Issue Identification:** The problem was identified when users began reporting system crashes following the update.
- **Resolution Efforts:** CrowdStrike had to quickly develop and release a fix while guiding affected users through temporary measures and rollback procedures.
- **Lessons Learned:** The incident underscores the importance of pre-deployment testing and phased rollouts. It also highlights the need for effective communication and support channels to manage and resolve issues promptly.

Testing production updates before they are deployed to all machines is not just a best practice but a necessity for maintaining system stability, data integrity, and operational efficiency. By adopting a rigorous testing approach, including staging environments, phased rollouts, and automated testing, organizations can mitigate risks and ensure a smooth deployment process. Learning from past incidents, such as the CrowdStrike Falcon BSOD issue, can help refine these practices and enhance overall software reliability and user satisfaction.

About the Author

Bhavani is a Senior Technical Manager, Information Security at GS Lab | GAVS. She has held numerous positions of responsibility in areas of Information Security such as risk management, IT controls, audits and compliance. Her expertise involves handling IT risks, security control framework designing and assessing digital tools. She is an avid traveler and is passionate about driving.

Bhavani Damodaran

Understanding Data Loss Prevention (DLP)

In today's hyper-connected world, data has become the new currency, making preventing accidental leaks or malicious theft a top priority. Data Loss Prevention (DLP) is a critical security strategy designed to ensure that sensitive or essential information is not transmitted outside the organization's network. These strategies incorporate a range of tools and software solutions that provide administrative control over the secure transfer of data across networks.

DLP products utilize business rules to categorize and safeguard confidential and sensitive information, preventing unauthorized users from unintentionally or deliberately leaking or sharing data, which could expose the organization to risk. Organizations are increasingly implementing DLP solutions due to the growing threat of insider risks and the demands of stringent data privacy laws, many of which enforce strict data protection and access controls. Beyond monitoring and regulating endpoint activities, certain DLP tools are capable of filtering data streams across the corporate network and securing data in transit.

Types of DLP Threats

- Insider Threats: Individuals within an organization who misuse their authorized access to data, either maliciously or unintentionally. Malicious insiders steal or sabotage data, while negligent insiders cause exposure through errors.
- External Attacks: Perpetrated by individuals or groups outside the organization, including phishing (deceptive messages), malware (viruses, ransomware), and hacking (exploiting vulnerabilities).
- Human Error: Mistakes such as accidental data sharing or configuration errors that unintentionally expose data, requiring corrective actions to mitigate impacts.
- Data Theft: Unauthorized acquisition of sensitive information through physical theft (e.g., stolen devices) or digital theft (hacking into systems).
- Data Breaches: Occur when unauthorized individuals access sensitive data, leading to exposure or theft via network or application breaches.

- **Ransomware Attacks:** Malware that encrypts data, making it inaccessible until a ransom is paid, potentially causing operational disruptions.
- **Social Engineering:** Manipulating individuals into divulging confidential information or performing actions that compromise data security, such as pretexting or baiting.
- **Advanced Persistent Threats (APTs):** Long-term, targeted attacks by sophisticated actors to gain and maintain access to systems, causing significant and sustained damage.

Types of DLP

Since attackers employ various methods to steal data, an effective DLP solution must address how sensitive information is exposed. Below are the types of DLP solutions:

Email DLP

- Analyze email content and attachments for sensitive data like personal identifiers, financial info, or proprietary business details, ensuring confidential information isn't accidentally shared.
- Automatically encrypt emails with sensitive data during transmission, and block those that violate data protection policies, such as sending restricted information to unauthorized recipients or external domains.

Network DLP

- Continuously monitors and analyzes network activity, including email, messaging, and file transfers, to identify any violations of data security policies across both traditional networks and cloud environments, ensuring protection of business-critical information.
- Establishes a comprehensive database that logs when sensitive or confidential data is accessed, who accessed it, and, if applicable, where the data moves within the network, providing the security team with complete visibility into data whether it's in use, in motion, or at rest.

Endpoint DLP

- Monitors all network endpoints, including servers, cloud storage, computers, laptops, mobile devices, and any other device where data is used, transferred, or stored, to prevent data leakage, loss, or misuse.
- It also helps classify regulatory, confidential, and business-critical data to simplify compliance and reporting. Additionally, it tracks data stored on endpoints both within and outside the network for comprehensive protection.

Cloud DLP

- Protects cloud-based data by scanning and auditing information stored in cloud repositories to automatically detect and encrypt sensitive data before it is uploaded. It maintains a list of authorized cloud applications and users who can access this sensitive information and alerts the infosec team to any policy violations or unusual activities.
- Tracks and logs cloud data access by recording when confidential information is accessed and identifying the user involved. It provides end-to-end visibility for all data in the cloud, ensuring comprehensive protection and compliance.

DLP in Healthcare

Protecting Patient Privacy:

Healthcare organizations handle sensitive data, including personal health information (PHI) and electronic health records (EHRs). DLP helps ensure that this data is not exposed or misused, maintaining patient confidentiality.

Compliance with Regulations:

Healthcare organizations must comply with regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the U.S. DLP solutions help meet these compliance requirements by enforcing data protection policies and preventing unauthorized access.

Patient Records
- ePHI
- EHRs
- PII
- Thirdparty Lab Results
- Imaging Results
- Data from connected Medical Devices

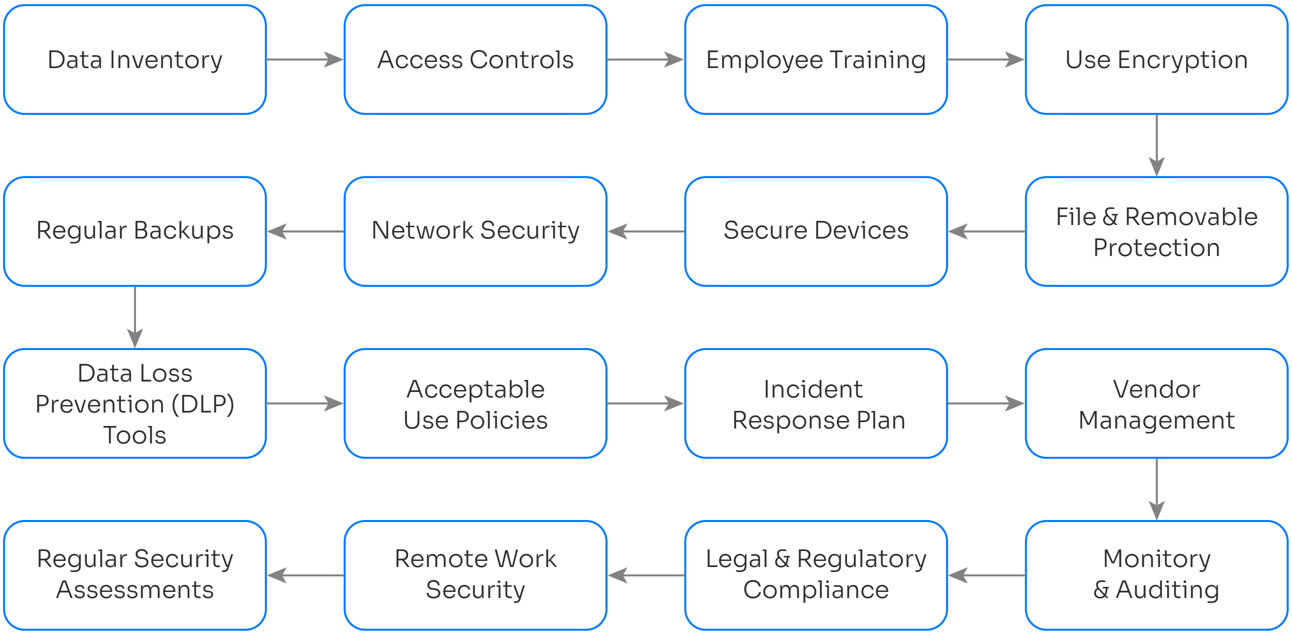
Research
- Clinical Trails
- Surveys & Research Findings
- Unpublished Medical Papers

Finance
- Payer Fillings & Records
- Financial Reports
- Compensation Plans

Legal
- Payer Agreements
- HIPAA & GDPR Audits

Steps for Preventing Data Leakage

To protect against these threats, organizations should adopt a multi-layered approach that includes deploying DLP solutions, educating employees, and continuously monitoring and analyzing data flows.



Data Inventory

Access Controls

Employee Training

Use Encryption

File & Removable Protection

Secure Devices

Network Security

Regular Backups

Data Loss Prevention (DLP) Tools

Acceptable Use Policies

Incident Response Plan

Vendor Management

Monitory & Auditing

Legal & Regulatory Compliance

Remote Work Security

Regular Security Assessments

How do DLP Tools Work?

DLP solutions leverage a blend of standard cybersecurity practices—such as firewalls, endpoint protection, monitoring services, and antivirus software—alongside advanced technologies like artificial intelligence (AI), machine learning (ML), and automation. This combination helps prevent data breaches, detect unusual activities, and provide context for security teams.

Typically, DLP technologies support various cybersecurity functions:

- Prevention: Conduct real-time reviews of data flows to instantly block suspicious actions or unauthorized access.
- Detection: Enhance data visibility and monitoring to swiftly identify irregular activities.
- Response: Improve incident response by tracking and documenting data access and movement throughout the organization.
- Analysis: Provide context for high-risk activities or behaviors, aiding security teams in strengthening preventive measures or addressing issues effectively.

Key Security Tools to Integrate with DLP

Security Information and Event Management (SIEM)

- Prevention: SIEM tools collect and analyze log data from various sources to detect and respond to security incidents.
- Integration Benefits: Integrating DLP with SIEM provides centralized visibility into data security events, allowing for real-time analysis and correlation of DLP alerts with other security data. This enhances threat detection and incident response capabilities.

Endpoint Protection Platforms (EPP)

- Role: EPPs protect endpoints from malware, ransomware, and other threats.
- Integration Benefits: When DLP is integrated with EPP, data security policies can be enforced directly on endpoints. This ensures that sensitive data is protected from internal and external threats and provides an added layer of security.

Cloud Access Security Brokers (CASBs)

- Role: CASBs manage and secure cloud service usage within an organization.
- Integration Benefits: Integrating DLP with CASBs enhances cloud data protection by providing visibility into applications and enforcing security policies for sensitive data across cloud services.

Identity and Access Management (IAM)

- **Role:** IAM solutions control user access to systems and data based on their identity and roles.
- **Integration Benefits:** Integrating DLP with IAM ensures that data protection policies are applied based on user roles and permissions. This helps in preventing unauthorized access to sensitive data and ensures that data protection measures are aligned with user access controls.

Conclusion

Data Loss Prevention (DLP) is essential for a strong cybersecurity strategy, addressing the increasing risks of data breaches and theft. DLP solutions help organizations protect sensitive information, meet regulatory requirements, and manage both internal and external threats. Integrating DLP with technologies like SIEM, EPP, CASBs, and IAM, ensures comprehensive protection across IT infrastructures. However, effective DLP also requires advanced tools, continuous monitoring, employee training, and robust policies. The goal is not only to prevent data loss but to enable secure, confident use of data. A well-implemented DLP strategy is a proactive measure for building trust and maintaining a strong security posture.

About the Authors

Shalini is a dedicated Security Operations Center (SOC) Analyst specializing in threat analysis, incident response, and security operations. She is recognized for her strong analytical skills and effective incident management. Shalini is committed to advancing cybersecurity measures and adapting to emerging threats.

Sri Priyadharshini A is a seasoned Security Operations Center (SOC) analyst with a passion for cybersecurity and a commitment to enhancing digital defenses. She enjoys exploring new cybersecurity technologies

The Impact of Generative AI on Cybersecurity: Navigating Opportunities and Challenges

Generative AI (GenAI) is transforming cybersecurity. As organizations rely more on digital systems, cyber threats rise, demanding advanced defenses. GenAI improves threat detection, vulnerability management, and incident response, but also introduces new risks. Organizations must adapt their cybersecurity strategies to leverage AI's strengths while addressing evolving threats. Understanding this balance is crucial for developing robust defenses.

The Impact of GenAI on Cybersecurity

Below is a detailed exploration of GenAI's implications in this field:

01. Enhanced Security Measures

Automated Threat Detection: GenAI can process and analyze vast amounts of network data in real time, significantly improving the identification of anomalies and potential threats. Unlike traditional methods, which may rely on predefined signatures, GenAI can learn from patterns and adapt to evolving threats, leading to quicker and more accurate detections.

Advanced Malware Detection: AI-driven systems leverage ML algorithms to recognize and respond to emerging malware patterns. By continually updating their knowledge base, these systems can adapt to new forms of malware that evade traditional detection methods, thus enhancing overall security.

02. Vulnerability Management

Proactive Risk Assessment: GenAI tools can simulate various attack scenarios to uncover vulnerabilities before they can be exploited. This proactive approach allows organizations to strengthen their defenses and minimize the risk of breaches.

Dynamic Vulnerability Scanning: GenAI can perform continuous assessments of systems for weaknesses, adapting its scanning strategies based on new intelligence about vulnerabilities and evolving threat landscapes. This dynamic capability ensures that organizations remain vigilant against potential security gaps.

03. Phishing and Social Engineering Defense

Content Generation for Detection: GenAI can be trained to recognize phishing attempts by analyzing linguistic patterns, visual designs, and other characteristics. This enhances detection rates, making it harder for malicious actors to succeed with deceptive tactics.

User Training Simulations: Personalized training modules can be developed using GenAI, helping users recognize various social engineering tactics. These simulations can adapt to individual learning curves, thereby improving overall security awareness and resilience within organizations.

04. Automated Incident Response

Rapid Response Systems: GenAI can automate responses to detected incidents, significantly reducing response times. This capability limits the potential damage from breaches and allows security teams to focus on strategic tasks rather than manual interventions.

Root Cause Analysis: GenAI can aid in pinpointing the root cause of incidents by analyzing data and identifying patterns. This insight is invaluable for preventing future occurrences and strengthening security protocols.

05. Cyber Threat Intelligence

Intelligent Data Analysis: GenAI can process vast amounts of threat intelligence data from diverse sources, providing organizations with actionable insights about emerging threats. This capability enhances situational awareness and helps in making informed decisions regarding security measures.

Trend Prediction: By analyzing historical data and patterns, GenAI can predict potential attacks. This foresight allows organizations to take proactive measures and adjust their security strategies in anticipation of threats.

06. Challenges and Risks

Sophisticated Attack Techniques: Cybercriminals can exploit GenAI to develop advanced attacks which evades traditional security measures, including realistic deepfakes and highly convincing automated phishing campaigns.

AI-Powered Malware: Attackers may use AI to create malware that evolves and adapts in real time, effectively bypassing existing security protocols. This evolution of malware represents a significant challenge for cybersecurity professionals.

07. Ethical Considerations and Governance

Bias and Reliability: There is a risk of bias in AI systems, which can lead to misidentification of threats or vulnerabilities. Developing governance frameworks is essential to ensure that AI operates fairly and reliably, avoiding discriminatory outcomes.

Accountability: As AI systems become more autonomous in decision-making, establishing accountability for breaches or errors becomes critical. Organizations need to create clear guidelines for accountability in AI-driven actions and outcogmes.

08. Future Directions

Collaborative Defense Strategies: Organizations may need to collaborate more closely, sharing AI-driven insights and data to enhance collective security. This approach fosters a community of defense, where information is shared to better anticipate and mitigate threats.

Integration with Other Technologies: Combining GenAI with other emerging technologies, such as blockchain, can create more resilient security frameworks. For example, blockchain can enhance the integrity of data used by AI systems, ensuring that threat intelligence is both reliable and tamper-proof.

Defending Against Next-Generation Threats from GenAI

To effectively defend against the next generation of threats posed by GenAI, organizations must adopt a comprehensive strategy. Below are key areas to focus on:

01. Advanced Threat Detection

Behavioral Analytics: Organizations should leverage machine learning to identify unusual patterns in user behavior. This approach helps detect potential security breaches before they escalate.

Real-Time Monitoring: Implementing AI-driven systems for continuous surveillance of networks and endpoints ensures that any suspicious activity is quickly identified and addressed.

02. Proactive Vulnerability Management

Regular Vulnerability Assessments: Conduct frequent penetration tests and audits using GenAI tools to uncover potential weaknesses in systems. This proactive approach allows organizations to address vulnerabilities before they can be exploited.

Automated Patch Management: Utilizing automated solutions for timely updates and patching of vulnerabilities is essential in maintaining robust cybersecurity defenses.

03. Enhanced Phishing Protection

AI-Enhanced Email Filters: Advanced AI can be employed to detect phishing attempts through content analysis and context recognition, significantly reducing the risk of successful attacks.

Employee Training Programs: Regular training sessions should be conducted to equip staff with the skills to recognize and report phishing attempts and other social engineering tactics.

04. Robust Incident Response Plans

Automated Response Mechanisms: Developing protocols that enable rapid isolation and remediation of threats is crucial for minimizing damage during an incident.

Simulation Drills: Conducting regular incident response exercises will ensure that teams are prepared and can respond efficiently when real threagts arise.

05. Intelligent Threat Intelligence

Collaborative Networks: Organizations should participate in information-sharing platforms to exchange threat intelligence with peers, enhancing collective security.

AI-Driven Analysis: Utilizing AI to process and analyze threat data can provide better situational awareness and predictive insights, enabling proactive measures against potential attacks.

06. Ethical AI Practices

Bias Audits: Regular reviews of AI systems are necessary to identify and mitigate biases that could lead to erroneous threat detections.

Transparency and Accountability: Ensuring transparency in AI decision-making processes is vital for maintaining trust and reliability within the organization.

07. Security-Aware Culture

Continuous Learning: Fostering a culture of security awareness through ongoing education and training helps employees stay informed about the latest threats.

Clear Reporting Channels: Establishing easy-to-use mechanisms for employees to report suspicious activities encourages vigilance and prompt action.

08. Investment in Advanced Technologies

Multi-Factor Authentication (MFA): Implementing MFA adds layers of security to user accounts, making unauthorized access significantly more difficult.

Blockchain for Data Integrity: Exploring blockchain technology can help ensure the integrity and traceability of critical data, enhancing overall security.

09. Collaboration with Experts

Engage Cybersecurity Consultants: Working with external specialists in GenAI can bolster an organization’s security posture by providing expert insights and strategies.

Stay Updated on Trends: Keeping abreast of industry developments related to GenAI and its implications for cybersecurity is crucial for staying one step ahead of potential threats.

Generative AI's continued advancement presents both cybersecurity challenges and opportunities. Organizations must proactively adopt a multi-faceted approach, combining advanced detection, vulnerability management, and continuous learning. Investing in technology, collaboration, and ethical AI will enhance resilience and safeguard digital assets in an interconnected world.

About the Author

Hashini Yuvaraj is a cybersecurity professional with 2.5+ years at GS Lab | GAVS. In her current role, she works with the Security Operations Center (SOC) of the organization. Her prior experience as a Customer Support Specialist equips her to excel in her current security monitoring and incident response role. Hashini's interest in networking further enhances her contributions to the cybersecurity domain.

Hashini Yuvaraj

3 Forward-thinking Practices to Manage IT Risk

In today's rapidly evolving technological landscape, traditional IT risk management practices often fall short in addressing emerging threats and challenges. This article outlines three forward-thinking practices that organizations can adopt to proactively manage IT risk and safeguard their digital assets. These practices emphasize aligning cybersecurity with business goals, fostering collaboration and efficiency, and providing actionable insights to key decision-makers. By embracing these forward-thinking approaches, organizations can enhance their ability to anticipate and mitigate IT risks effectively.

Context & Objectives

Context	IT Risk Management "Old Way"	Forward-Thinking Practices
Increased Cybercrime	One-Time Function	Align cybersecurity with the business goals
Emerging Threats	Siloed Approach	Working faster, smarter, and "win" together
Global Spending on Cybersecurity	Outdated Thinking	Provide actionable insights to board and executives
Spending is up; not much impact on risk reduction	Outdated Thinking	

It is important to establish a strong foundation in risk management principles. Having a basic understanding of risk and steps to manage it effectively is crucial. By grasping these fundamental concepts, organizations can better position themselves to navigate the complexities of IT risk in a proactive and informed manner.

What is Risk?

Threat

Any person or condition that could cause harm, loss, damage, or compromise of an asset.

Vulnerability

Any weakness that exists inside a system.

Asset

Any item that has value to your organization.

Risk

Any Situation that involves exposing something of value to danger.

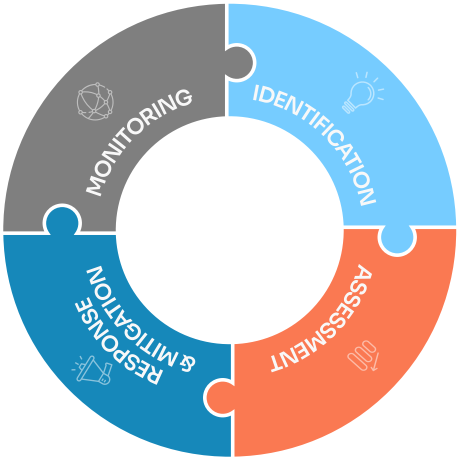
Four Steps to Manage Risk

STEP 01 Risk Identification

STEP 02 Risk Assessment

STEP 03 Risk Treatment

STEP 04 Risk Monitor, Review & Report



Forward Thinking #1: Align CyberSecurity with Business

IDENTIFYING YOUR MOST CRITICAL PARTNERS AND STAKEHOLDERS

- Identify internal teams involved
- Identify key vendors
- Establish clear roles and responsibilities for security along your supply chain

RETHINKING CYBERSECURITY AS A BUSINESS PRIORITY

- Identify and map out your organization's overall revenue goals
- Understand what security means for your specific industry
- Align your strategy

COMPLIANCE CONSIDERATIONS

- Understand your organization's current risk framework
- Understand how cybersecurity factors into this risk framework, considering industry and geography-specific requirements

Forward-Thinking #2: Work Faster, Smarter, and 'Win' Together

Best Practices:

Communicating with Non-Security Personnel

- Standardization
- Grouping/Consolidating
- Single Source of truth
- Helping Hand
- Sharing

Make it a Team Sport!

Leveraging a Solution to Enhance Collaboration

Vendor Risk Managers:
On-Board Third Parties 75% Faster

Sales and Marketing:
Stand-out Due to Security Certifications

Finance:
Optimized the Cost of Cyber Insurance

Corporate Strategy:
Better Assess the Cybersecurity Posture

Executives:
Understand the ROI of Cybersecurity Initiatives

Forward-Thinking #3: Provide Actionable insights that your board can understand

Finding Common Ground

- Report concisely and only on what is relevant to the board
- Use KPI data to make your case in budgetary discussions
- Share data that demonstrates the ROI on cybersecurity investments
- Present security findings in terms of business risk and market trends

Competitive Benchmarking

- Always a top-level board concern
- Improve standing in the marketplace
- Become that security champion

Conclusion

By embracing these forward-thinking practices and establishing a strong foundation in risk management principles, organizations can effectively navigate the evolving landscape of IT risk. Aligning cybersecurity with business goals, fostering collaboration, and providing actionable insights will enable organizations to proactively mitigate risks, safeguard their digital assets, and ensure long-term success in an increasingly complex technological environment.

About the Author

Anitha 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 Rajmohan

Cybersecurity Awareness Month

October 2024

Protect Your **Devices,** Protect Your **Data.**

Keep **Software Updated**
& Be Wary of **Public Wi-Fi**.

#SecureOurWorld

gslab™ | GAVS

www.gavstech.com

Follow us on: