enGAGe

October 2021

"Perfection is not attainable, but if we chase perfection we can catch excellence."

Vince Lombardi

FEATURING

Dileep Mangsuli

Executive Director – India,
Siemens Healthineers
India Pvt Ltd.

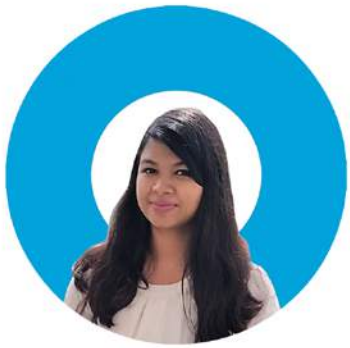
GAVS

When you realize you are mortal
you also realize the
tremendousness of the future.

- Etel Adnan -

Table of Contents

EDITOR'S NOTE



Soumika Das

An organization witnessed a 6-digit drop in its customer base and lost one-third of its value due to a security breach. Another organization lost control of a furnace at its steel mill, preventing a safe shutdown, and causing massive damage. One of the largest petroleum pipelines in the US faced a major cyberattack resulting in disruption in fuel supply for close to a week. Impacts of cyberattacks are not just limited to financial losses; from reputations to even health and safety – a lot is on the line.

Advancements in technology, widespread adoption of technology, and increasingly complex yet fragile supply chains have widened the cyberattack surface. Add to that the accelerated digitization brought on by the pandemic. A large remote workforce means a rise in the number of unsecured devices, networks, and processes. And with so many companies operating in the cloud, one vulnerability can leave millions of customers exposed. Now any equipment, process or dataset that has been digitized is susceptible to attacks.

As per some reports, atleast 66 zero-day attacks have been found this year, a record-breaking number. Zero-day attacks are vulnerabilities that are either unknown to the concerned party or yet unsecured. These exploits can fetch the hackers huge sums of money. Among other factors, the rising cyberattacks can be attributed to a steady proliferation of hacking tools globally and a decline in the cost of such tools.

The U.S. Securities and Exchange Commission (SEC) has made its stance on cybersecurity clear. It now considers cyber vulnerabilities to be an "existential business risk". This was evident in the fines levied against two companies over inadequate disclosures of cybersecurity issues. All this mean one thing - business leaders should look at strengthening their defenses. Cybersecurity should be built into the business strategy and increased risks from emerging tech and behavioral change should also be considered to future-proof businesses.

We have a host of insightful articles in this edition.

We are introducing **Mr. Dileep Mangsuli, Executive Director – India, Siemens Healthineers India Pvt Ltd.** He talks about the lessons he's learnt from traveling, the challenges he has faced, his definition of success and more.

Sundaramoorthy S has written, **'Cybersecurity Risks, Issues & Recommendations in the Healthcare Industry'**.

Maryada Kashyap has written, **'Make Way for Low-Code No-Code'**.

Vishnuraj K has written, **'Breach and Attack Simulation in a World of Growing Cyber Threats'**.

Ganesh Kumar J has written, **'How to Verify the Proper Functioning of DNS Sinkhole?'**

Anjana K has written, **'Identity Theft in the Healthcare Industry'**.

Rama Vani Periasamy and **Karpagam Ramasamy** have written, **'Risk Management – How Not To Do It'**.

GAVS is celebrating **Cybersecurity Awareness month** and the theme for this year is **'Do Your Part. #BeCyberSmart'**, to empower individuals and organizations to own their role in protecting their part of cyberspace.

GAVSians in Spotlight

Badhri Narayan Ramesh

"As a part of the Solutions & Strategy team at GAVS, I work towards delivering Industry leading solutions to clients in AI led Managed Infrastructure Services. I am really grateful to work in a place where there is support & encouragement from the leaders to be pro-active, freedom in decision making along with timely guidance and mentorship. GAVS is truly a great place to grow and a fun place to work, empowering me to grow and contribute more."

Note from Balaji Uppili, Chief Customer Success Officer, GAVS

"From a mechanical background to be able to understand the business imperatives of a healthcare client and his ability to pick up knowledge on Managed Infra Services has been phenomenal. Lot of great contributions in the transition planning in recent times for our biggest client."

Juliana Koshy

"GAVS has been a game-changer for my career. When I look back on the last 10 years here – it has been only learning, learning and learning. I have been blessed with a great manager and supportive team members. My team is emotionally invested and they have been doing wonders. I will continue to contribute towards the growth of GAVS and our customers. All in all – it's the best thing that happened to my career."

Note from Balaji Uppili, Chief Customer Success Officer, GAVS

"Her consistent customer centricity, along with her ability to take ownership end-to-end in key accounts has really helped GAVS lay a strong foundation for growth. She is a real asset for GAVS."

What's new in Tech

AI can write its own computer code

Codex, built by OpenAI, is an AI technology that can that writes its own computer programs. It can generate programs in 12 coding languages and even translates between them. Codex is based on the GPT-3 language model and can solve over 70% of the problems in OpenAI's publicly available HumanEval test dataset.

Robots enlisted to mine lunar resources

A team at University of Arizona College of Engineering has received $500,000 in NASA funding for a new project to advance space-mining methods that use autonomous robots. Mining on the moon's surface could turn up rare earth metals needed for technologies such as smartphones and medical equipment.

Sea slug inspires researchers to mimic its most essential intelligence features

For artificial intelligence to get any smarter, it needs first to be as intelligent as one of the simplest creatures in the animal kingdom: the sea slug. The discovery is a step toward building hardware that could help make AI more efficient and reliable for technology ranging from self-driving cars and surgical robots to social media algorithms.

Human learning can be duplicated in solid matter

Researchers at Rutgers University have found that learning - a universal feature of intelligence in living beings - can be mimicked in synthetic matter, a discovery that in turn could inspire new algorithms for AI. Now, researchers are looking to mimic human cognition in devices that can learn, remember and make decisions the way a human brain does.

Introducing Dileep Mangsuli,
Executive Director - India, Siemens Healthineers

Dileep Mangsuli
Executive Director – India,
Siemens Healthineers India Pvt Ltd.

Dileep is an experienced global technology leader, leading the Global Healthcare Development Center at Siemens Healthineers operating from Bengaluru, India. Over the last four years, Dileep has focused on developing strategy and solutions around affordable, accessible and digital solutions in the Healthcare industry. During his career spanning over three decades, Dileep has worked in a variety of functional areas including business leadership in energy, power and healthcare. Dileep has worked in leadership roles across UK, China and USA for over ten years.

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

My childhood was spent in a small village in Karnataka, India. My father worked in a charitable trust hospital where the hospital's purpose statement was "Here service to patients is service to God". That instilled a strong purpose in life. The hospital and the community living in hospital compound had a culture of punctuality, where sticking to time and commitment and service meant everything. That culture has helped a lot in my career.

2. What have been some of the biggest challenges in your life and how that has shaped you? What's the most important risk you took and why?

There are many challenges that have helped shape my career. At personal and family level we took the risk of going to different locations and taking up challenges in China, UK and US. Those experiences helped in understanding culture and work practices. There was a lot of learning during these assignments. Leadership learnings and market learnings shape your career in a big way.

3. Could you share with us some interesting lessons you've learned while travelling?

Travelling and living in different countries has taught me one great lesson. People everywhere are good by nature. Most of the people are like

mirrors. They reflect your own image. If you do good, good gets returned to you. It is Karma theory. Every country teaches you something unique. China taught punctuality on product delivery, UK taught importance of staying in role to become expert, Germany taught meticulous work practices and quality focus, US taught how to look at scale and dream big for business.

4. How did you discover your passion for STEM?

During high school day there was a lesson on how a door bell works. The concept was so interesting that I started reading and studying a lot of physics concepts. Before I knew STEM subjects became fascinating past-time for me. Mechanics was my favorite subject.

5. How would you define success?

To me success is about an attitude on "never giving up". Success comes after several failures. It is about constant learning and becoming a better version of yourself every day. Whenever I look back on success, I realize that there were several events which were not considered "successful" laid the foundation for future success. Never give up. There is a saying by Edison "***Many of life's failures are people who did not realize how close they were to success when they gave up.***"

6. How do you continue to grow and develop as a leader?

Leadership is a journey. Leadership is about continuing the learning path. They day one stops learning is when leadership is lost. One needs to have child-like enthusiasm to learn and develop. Leadership is about surrounding yourself with people smarter than yourself. Leadership is about seeing things that may be hazy. Leadership is about making people around you successful. Leadership is about bring best out of people. Leadership is about saying "Woh Subaha kabhi toh ayegi" set the vision and lead they way. It is fascinating.

7. In your opinion, what is the ideal way to lead in a crisis?

It is leadership by example. People rally around you. Leadership Positivity rubs on people.

8. 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?

Just enjoy your journey.

Thwart Cyberattacks before they Strike!

Cyber Security Mindset

Engaging awareness programs, routine knowledge testing

Daily reminders with screensavers, desktop alerts, etc.

Cyber Security Framework, Governance

Adopting the right standards, controls: PCI-DSS, ISO, NIST, CIS Controls, etc.

Dedicated SIEM team

Dedicated CPO/DPO for data privacy

Risk Management

AI/Automation led security solutions

Incident response plan, BC/DR plan

Continuity of preparedness

Collaboration with local, international agencies: NCCC,

Routine Risk Assessment

Identification of all digital assets on premise, cloud

Identification of internal/external threats, cyber profiling

Prioritization based on likelihood of occurrence, potential impact

Continuous monitoring, maintenance of digital assets, SIEM integration

Security Safeguards, Policies with Periodic Evaluation

Multi-factor authentication, IAM/PAM, encryption

Application whitelisting, application hardening

Routine patching , software updates, daily backups

Firewalls, mail filtering, host intrusion prevention, data loss prevention, device control

GAVS celebrates **#CybersecurityAwareness** Month.

#BeCyberSmart

Explore GAVS' Cybersecurity Offerings at https://www.gavstech.com/service/security-services/

Cybersecurity Risks, Issues & Recommendations in the Healthcare Industry

Sundaramoorthy S

There has been a marked increase in the number of cyberattacks reported by organizations post-COVID, and the healthcare industry is no exception. Even with security measures and regulations like HIPAA and GDPR to safeguard PII, PHI, EMR, EHR, Healthcare organizations have fallen prey to various cyberattacks. This article focuses on the cybersecurity risks, issues and challenges faced by the Healthcare industry and recommendations on how to avoid them.

The following graph illustrates the number of breaches in Healthcare industry in last 12 months

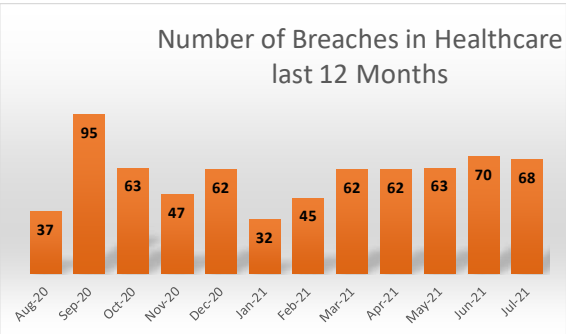
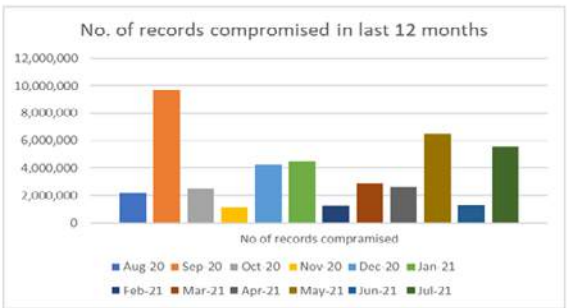
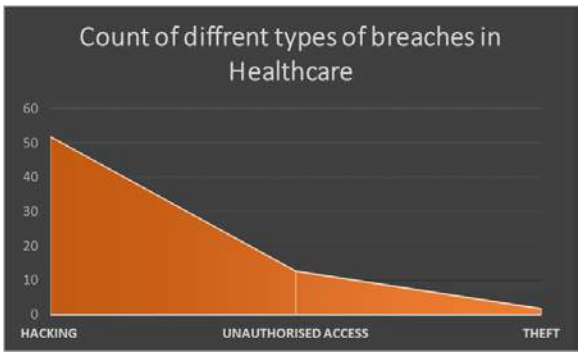


Fig 1.1 Breaches in Healthcare in '20 - '21

The following chart illustrates the of number of records compromised in the last 12 months in Healthcare industry.



The following graph shows the different types of breaches and number of breaches in Healthcare Industry.



Risks, Issues and Challenges in Healthcare

Ransomware Attacks

Ransomware is a malware which attacks the intended target. The target could be files, systems, databases, or other form of data which is mission critical for business. The attacker will demand a ransom from the target owners to restore the business; denial of ransom may lead to the destruction of impacted target, resulting in blocking the critical business operations which could result in loss of millions of dollars.

The rising cases of ransomware attacks on hospitals and other healthcare organizations is a cause for serious concern. When the network is impacted by ransomware, the healthcare organizations are forced to operate offline. Regulatory bodies across the globe are hosting joint trainings to educate on how to defend against ransomware.

3 major ways in which Ransomware attacks -

- Malvertising (Victim clicking the ad link contains Malware)
- Malicious links
- Phishing

Unsecure Virtual Business Operations

In the new normal, a majority of the businesses are operated in remote environments, where the hardware devices like mobiles, tokens, other business critical Healthcare devices, and the identity of the individuals who access the devices are a big question mark. The breach of security might start from here.

Inadequate Access to Clinical Applications

In a sensitive environment like Healthcare, who has access to what applications in the Healthcare network, and duration of the access to clinical and other critical software applications where sensitive data like PHI, PII, EHR and EMR is stored is key to hackers. Inappropriate access to the applications may lead to breach of data and increases the chances of misusing individual roles.

Unsecure Medical devices

Most Healthcare organizations depend on medical equipments connected to the internet. However, a lot of these medical devices are unsecured due to outdated softwares, lack of upgrades, patches, and extended life span. Healthcare organizations using IoT and IoMT devices need to ensure that these devices have the latest threat defenses. Hackers take advantage of these unsecured devices and navigate to the entire network to take control of the critical targets and attack the organization's IT environment.

Lack of Centralized Governance

The pandemic has accelerated the digitization of most businesses including those in healthcare. The Electronic Health Records are business critical data. Lack of an effective way to collect and organize the information may lead to lack of insight and control over the data, thus impeding business processes, and increased chances of compliance failures. In short, lack of effective information management puts the organization's long-term success at risk.

Recommended Precautions for Safe Networks

Data Backup

Have multiple backups of mission critical data, applications, and application service and devices. These backups must be stored offline and password protected. It is a must-have for DR environments and high-availability applications.

Matured Identity & Access Management Solutions

Implementing end-end Identity & Access Management solutions will give the perfect control over corporate systems in terms of Compliance, Governance, Integrations, Provisions, JML, Audits and Reports. For end-end solutions, the following towers of Identity & Access Management should be implemented -

- Identity & Access Management
- Privileged Access Management
- Single Sign On
- Multi-Factor Authentications
- Mobile Device Management

Audit / Penetration Testing

Penetration testing will ensure the networks are secured with the best practices; it is recommended to have the Penetration testing done through third party experts for comprehensive findings on vulnerabilities.

Network Monitoring

Monitoring the IT environment 24/7 for changes to critical files, servers, applications, ports, firewalls, processes and Cron's will help identifying the risks well in advance to have precautionary measures to avoid attacks.

Scheduled Upgrades and Patch Management

Healthcare is an industry where multiple vendor products are utilized to execute the business, the vendor products should be upgraded, patched for latest security updates released by the product vendors.

Before applying the latest upgrades or patches of the vendor, the stability of the latest version or the version which scheduled to be deployed should assessed for the security and performance.

White/Black Listing Enterprise Applications and Websites

Restrict the users of the network from accessing applications and websites by creating a blacklist of applications where access to such apps and URLs will be denied as a precautionary measure.

Security Awareness program

Educate corporate network users about the current risks and issues in cybersecurity, like phishing attacks and how it impacts the networks, business, patients, and providers. Continuous trainings should engage the network users which will reduce the attacks.

Endpoint Protection Solution

Include protection, detection, and response capabilities for laptops, workstations, and mobile devices. This utilizes antivirus (AV) and antimalware (AM) to block cyberattacks. Quickly detect and remediate any malicious activity or infection that has made its way onto the endpoint.

HIPAA compliance

On top of implementing all the security measures to secure the networks, it is must to comply to HIPAA regulations.

Following the mantra **"Security Is A Continuous Improvement"** along with implementing the suggested best practices will help organizations significantly bring down their security risks and issues.

About the Author

Sundar has more than 13 years of experience in IT, IT security, IDAM, PAM and MDM project and products. He is interested in developing innovative mobile applications which saves time and money. He is also a travel enthusiast.

Make Way for Low-code No-code

Maryada Kashyap

We live in unprecedented times and we must constantly come up with new techniques, processes, and systems of doing things efficiently. Low-code platforms coupled with SaaS can accelerate a business innovation journey.

Low-code platforms need coding skills, but it quickens the development process by allowing developers to work with pre-written code components. No-code platforms promise to make software development easier to use for an average business user. With point-and-click or pull-down menu interfaces, such applications help users design and implement their own systems. It reduces the cost of employing an engineering team along with the time and effort put in development. Because of Low-code No-code, the dependency on niche technical skills reduces along with the IT development backlog. Low-code No-code is set to bring about a big change in the application development process.

The expectations are rising for digital experiences on both web and mobile applications. Cloud connected AI-led applications are being used by people daily. Businesses need to make sure that the growing demand of the customers are being met. The annual growth of Low-code No-code platforms is expected to be more than 28% approximately. *"Gartner Forecasts Worldwide Low-Code Development Technologies Market to Grow 23% in 2021 and by 2024, 65% of applications will be low code."* Microsoft has projected that in the next 5 years, over 500 million new applications will be developed. This estimate shows that more applications will be developed in the next 5 years than that were in the last 40 years.

The new applications and improved digital experiences produce an unbelievable amount of data, including a lot of unstructured data. There is a high demand to understand the unstructured data. The tools that we have been using in the last 40 years are not the same tools that will be used in the next 5 years. These tools are unable to keep up with the new application demands.

This fast-growing demand has resulted in companies hiring more professional developers and coders, but are there enough developers to meet these needs? It is projected that in the coming decade the US is going to face a shortage of a million developers. It will be increasingly difficult to find specialists with the required skillsets. Companies need to find more efficient ways to get more out of their current resources and investments. Smaller digital transformation projects with incremental changes that deliver results with better return on investment can benefit from Low-code No-code platforms.

A person who has application experience or the necessary skillset or the standard information can become a Low-code developer and get the job done. This is where citizen developers come into the picture, where a domain expert can leverage easy-to-use tools to build software. This is an easier alternative to allocating or hiring resources solely for such jobs. Smaller businesses can leverage such platforms to digitize, automate and/or develop applications for their business processes, like reservation management for restaurants, order quote creation, etc.

Low-code No-code platforms have many advantages; however, they present a few difficulties as well. Its best practices are still emerging and are not very mature. It also requires a change in the organization's culture. Also, a single platform may not support all the use cases of an organization. Enterprise Low-code No-code platforms, however, are more sophisticated and provide scalability, performance, security, and integration with the organization's apps. Although it

increases productivity and reduces the time taken in the development drastically, becoming an expert in the platform takes time. Even the development teams take time to fully understand the platforms.

Though Low-code No-code has its challenges it is expected to grow significantly. Pretty much every organisation will be adapting to it in the future. It is not a universal remedy, but it can address the issue of resource shortage. In the long run, systems and frameworks will turn out to be considerably simpler to work for common processes, simple programs and use cases. This is the future and going forward even non-technical users will be able to completely customize the apps and frameworks using Low-code No-code.

Gartner's Magic Quadrant for Enterprise Low-code Platforms

References

- https://hbr.org/2021/06/when-low-code-no-code-development-works-and-when-it-doesnt
- https://appdevelopermagazine.com/why-low-code-no-code-will-become-the-mainstay-in-2021/
- https://www.valoremreply.com/post/democratizationofai/
- https://venturebeat.com/2021/02/14/no-code-low-code-why-you-should-be-paying-attention/
- https://www.gartner.com/en/newsroom/press-releases/2021-02-15-gartner-forecasts-worldwide-low-code-development-technologies-market-to-grow-23-percent-in-2021

About the Author

Maryada is part of the ZIF™ product marketing team at GAVS. She is an experienced IT professional with focus on digital technologies and delivering user-centric solutions. She believes that by learning new technological trends and innovations, one can see the big picture and be ready for change.

Outside her professional role, she likes to sketch, dance and travel.

Breach and Attack Simulation in a World of Growing Cyber Threats

Vishnuraj K

"Breach and attack simulations are an advanced computer security testing method. These simulations identify vulnerabilities in security environments by mimicking the likely attack paths and techniques used by malicious actors. In this sense, a breach and attack simulation acts much like a continuous, automated penetration test, and it improves upon the inherent limitations of red and blue team testing."

Why BAS Platform should be a part of our Cybersecurity Arsenal?

- Despite having cybersecurity solutions in place, defending against attacks is becoming more difficult. Organizations are investing heavily in cybersecurity and are expected to invest more in the coming years.
- Selecting security products and services has become complicated, and it is hard to assure their effectiveness. A firewall, anti-malware platform, secure email gateway or other security solutions can be an asset one day and a liability the next.
- This makes it hard for an organization to take informed decisions regarding its cybersecurity investments and risk management. Allocating resources for cybersecurity and ensuring their ROI is a challenge, especially since security products often have overlapping features.

A proactive approach to cyber vulnerabilities consists of deploying a cyber simulation platform. This enables organizations to review their security assumptions, identify possible security gaps, and receive actionable insights to enhance their security postures. Such Breach and Attack Simulation (BAS) platforms -

- Help organizations stay one step ahead of cyberattacks, providing full visibility into the company's security posture 24/7,
- Help monitor the company's cybersecurity on a regular basis to detect the vulnerabilities that could be exploited,
- Provide effectiveness reports of the security programs and thus justify the investments for achieving regulatory compliance, aligning with business objectives, reducing security incidents and breaches, improving the threat profile, tracking improvements in responses, and maintaining the risk profile for optimal cyber insurance rates.

"The ability to test continuously at limited risk is that the key advantage of Breach and Attack Simulation (BAS) technologies, which will alert the IT and business stakeholders about existing gaps within the security posture, or validate that security infrastructure, configuration settings and prevention technologies are operating as intended".

Benefits of a BAS Platform

- Evaluate effectiveness of preventative controls, detection controls and post-breach controls
- Evaluate effectiveness of the monitoring and response workflows
- Evaluate effectiveness of the compare security product
- Automated reporting and metrics

- Prioritize the mitigation efforts
- Ensure defensibility against the latest cyber threats

Leveraging the BAS Platform

By leveraging the automated testing, reporting, and alerting of BAS solutions, you'll continually reduce your attack surface and best position yourself to defend against sophisticated cyberattacks. By proactively challenging and testing controls before the bad guys do, organizations can get a head start and strengthen their defenses. Much like crash testing a car, the way to know the strength of your controls is to check them, then take the corrective measures.

Organization Attack Vectors for Security Posture

A BAS platform attacks an organization's network with real attacks. Some of the attack vectors that test the organization's security posture are as follows:

- **Email attacks testing** – sending emails with malicious link or attachment that would slip through mail filters, and to check if employees would click on it that leads to phishing.
- **Web browser testing** – this is to find out if malware, exploits, malicious scripts, etc. that expose the organization via legitimate browsing of mainstream websites.
- **WAF testing** – to check whether the organization's Web Application Firewall stands up against web payload and the web apps are protected as per best practice.
- **Hopper testing** – this test is to check how easy it is for the hopper to make its way from system to system using different methods to hop and extract data.
- **Data exfiltration (DLP) testing** – this is to validate that the no confidential information goes out of the organization.
- **Endpoint testing** - this is to check if the organization is protected against the latest cyberattack vectors.

Key Features of a BAS Platform

- Administrative console
- Automation software
- Test point agents for production and test environments
- An underlying security framework
- Scenarios for testing which use the framework
- Risk analysis reporting
- SIEM integration
- SOAR integration
- An extensible API or API-1st
- Ticketing system and a case management system
- Direct security technology integration

Automated Breach and Attack Simulation

Automated Breach and Attack Simulation (ABAS) is predicted to be a cyber defense strategy for organizations to continuously identify vulnerabilities and prioritize finding threats and remediation.

Benefits of ABAS

- **Enhanced Insights** - ABAS platforms generate insights and improve the cybersecurity decisions of the organization, from risk to operations and compliance and a rich depth of use cases to improve effectiveness of the security program.
- **Better Business Decisions -**
  - Enables informed decisions about technologies, people, and processes.
  - Maximizes ROI and help future investment decisions.
  - Identifies the vulnerabilities of an organization, so that the security strategy is as planned.

- **Real Security Outcomes** - ABAS verifies security capabilities across the organization, raising productivity, efficiency, and effectiveness by measuring the security program's performance against known cyber threat behaviors.

  Some key benefits realized by end-users:

  - Automation of high-risk manual approaches to the production run environments
  - Low turn-around time to respond to emerging threats
  - Assistance to CISOs to deal with different cyber strategies with 80–100 technologies for an average enterprise
  - Overcoming talent or skill shortage
  - More than 90% accuracy in visualizing attack path and prioritizing results

Conclusion

A BAS solution can optimize an organization's security. Breach and attack simulation technology allows organization to emulate multi-stage, comprehensive adversary campaigns against their complete organization. It was largely focused on running attacks and red team augmentation, it gradually evolved to security control validation. The objective is to maximize the effectiveness of the cybersecurity program.

GAVS recommends leveraging BAS for next gen protection. We have been evaluating BAS as a solution for emerging threats and have identified partners and leaders in this space to partner with.

References

- https://blog.cymulate.com/breach-attack-simulation-platform-integral-part-cybersecurity-arsenal
- https://www.xmcyber.com/what-is-breach-and-attack-simulation/
- https://rthreat.net/wp-content/uploads/2021/04/4_14-attack-simulation-vs-attack-emulation_-whats-the-difference-980x245.png

About the Author

Vishnu Raj is a part of the GAVS Security Practice (Red Team Member). He's passionate about building secure apps as he believes everyone deserves privacy.

How to Verify the Proper Functioning of DNS Sinkhole?

Ganesh Kumar J

Starting with PAN-OS 6.0, DNS sinkhole is an action that can be enabled in Anti-Spyware profiles. A DNS sinkhole can be used to identify infected hosts on a protected network using DNS traffic in environments where the firewall can see the DNS query to a malicious URL.

The DNS sinkhole enables the Palo Alto Networks device to forge a response to a DNS query for a known malicious domain/URL and causes the malicious domain name to resolve to a definable IP address (fake IP) that is given to the client. If the client attempts to access the fake IP address and there is a security rule in place that blocks traffic to this IP, the information is recorded in the logs.

Resolution

This is designed to help verify if the DNS Sinkhole function is working properly through a Palo Alto Networks firewall.

The following 2 scenarios are covered:

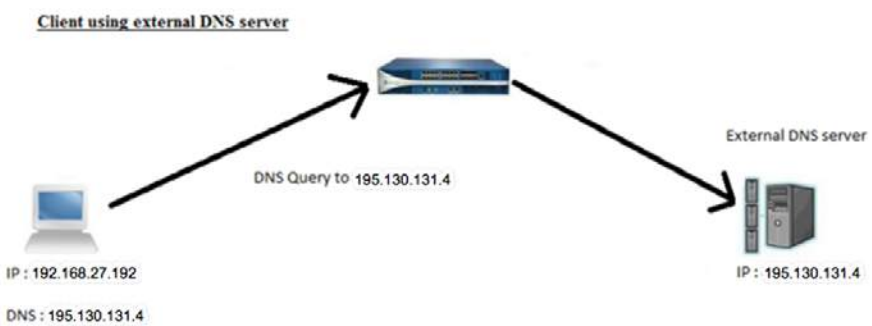
- Client Using External DNS Server
- Client Using Internal DNS Server

Client Using External DNS Server

Note: DNS Sinkhole IP must be in the path of the firewall and the client so you can view the logs from it. For example, the Palo Alto Networks firewall sits between an infected client and the Data Center, but it does not see the internet. In this scenario, if DNS Sinkhole is configured with an internet IP, then the firewall will never see the infected client trying to reach its command & control server.

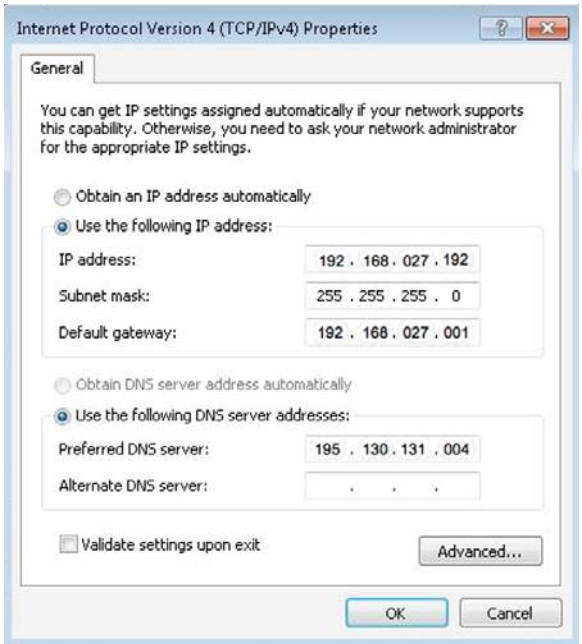
When the DNS sinkhole feature is configured on the Palo Alto Networks firewall and the client system is using an external DNS server, the DNS query from the client will go through the Palo Alto Networks firewall to the external DNS server (client and DNS server are in different subnets). The user should be able to see threat logs with the client IP address as a source.

1. The user is trying to access a malicious website. The client system will send the DNS query to an external DNS server to get the IP address of the malicious website. The firewall will receive the DNS query directly from the client system.
2. The firewall will hijack the DNS query and will give a DNS sinkhole IP address to the client and should be able to see the threat logs with client IP address as a source.



Client TCP/IP Properties Configuration

Review the following config example:



When using an external DNS server, Threat logs show the Client IP address "192.168.27.192" as a source that is trying to access a malicious website:

Client Output When Using External DNS Server

$nslookup	79fe3m5f4nx8c1.pmr.cc
Server:	195.130.131.4
Address:	195.130.131.4#53

Non-authoritative answer:

Name: 79fe3m5f4nx8c1.pmr.cc
Address: 72.5.65.111

The previous screenshot and the above text shows a host machine 192.168.27.192 performing a DNS request for "79fe3m5f4nx8c1.pmr.cc" (a suspicious URL) and the response being 72.5.65.111. Thus, showing that the DNS Sinkhole is working as desired.

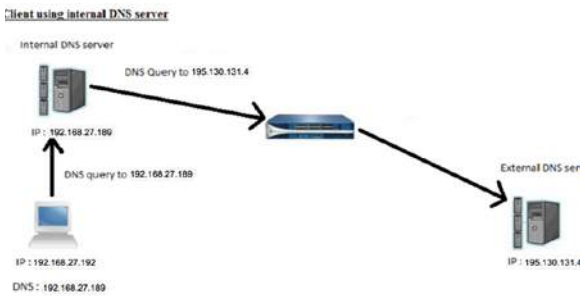
Client Using Internal DNS Server

If a client system is using an internal DNS server (client and DNS server are in the same subnet), the DNS query from the client will go to the internal DNS server. The internal DNS server will forward this query to an external DNS server, and threat logs with the internal DNS server IP address will be seen as a source.

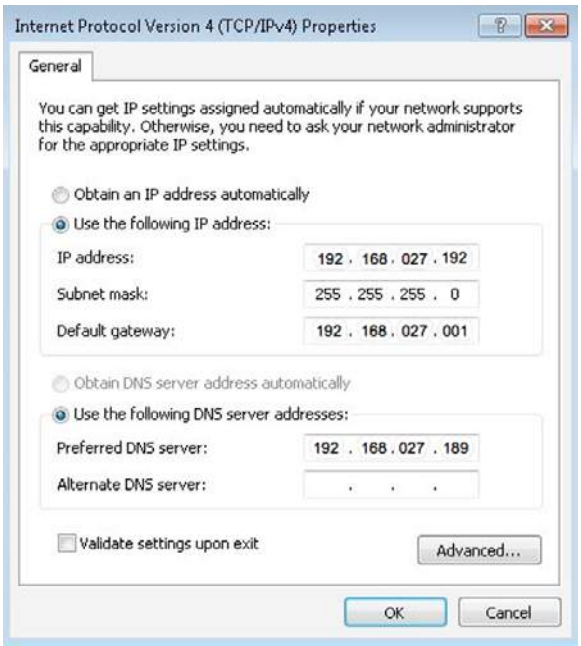
Currently, the Palo Alto Networks firewall cannot identify which end client is trying to access a malicious website with the help of the threat logs, because all threat logs will have the internal DNS server IP address as a source. However, the firewall should be able to determine the end client IP address with the help of traffic logs.

Below is an example where the user is trying to access a malicious website. The client system will send the DNS query to an internal DNS server to acquire the IP address of the malicious website. Here, the internal DNS server will forward the DNS query to an external DNS server. The firewall will receive a DNS query from the internal DNS server.

The firewall will hijack the DNS query and give the DNS sinkhole IP address to the internal DNS server. The internal DNS server will forward the response to the client system and the user should be able to see threat logs with internal DNS server's IP address as a source. However, Palo Alto Networks firewall should be able to see client IP address in the traffic logs because client will try to access that website with DNS sinkhole IP address, as shown in the following screenshot



Client TCP/IP Properties Configuration

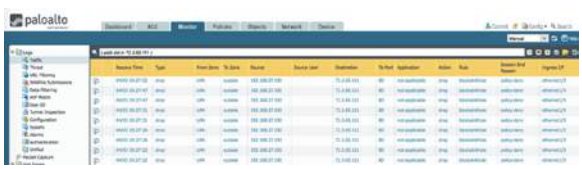


Threat Logs

In threat logs, the firewall shows only the internal DNS server IP address "10.50.240.101" as a source, because the client system is using the internal DNS server IP. Here, the firewall is not able to determine which end client is trying to access that website.

Traffic Logs

However, as soon as client get the IP address from DNS server, it will generate traffic towards the sinkhole IP address (72.5.65.111). Therefore, the firewall will show the end client IP address "192.168.27.192" in traffic logs, as shown below:



Client Output When Using Internal DNS Server

$nslookup	4cdf1kuvlgl5zpb9.pmr.cc
Server:	192.168.27.189
Address:	192.168.27.189#53

Non-authoritative answer

Name: 4cdf1kuvlgl5zpb9.pmr.cc
Address: 72.5.65.111

The previous screenshot and the text above shows a host machine 192.168.27.192 performing a DNS request for 4cdf1kuvlgl5zpb9.pmr.cc (a suspicious URL) with the response of 72.5.65.111. This verifies that the DNS Sinkhole is working as desired.

References

- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0
- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clk2
- https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/use-dns-queries-to-identify-infected-hosts-on-the-network/dns-sinkholing

About the Author

Ganesh is currently managing the Network, Security and Engineering team for a large US-based customer. He has been associated with the Network & Network Security domains for more than 16 years.

Identity Theft in the Healthcare Industry

Anjana K

In addition to the various challenges faced by the healthcare industry, the pandemic has also increased the risk of cyber-security threats. Last year, various healthcare providers all over the world were targeted by a variety of complex and coordinated cyber-attacks.

Targeting the Healthcare Industry

"Medical records are valued at 20 to 50 times more than financial identities on the black market."

DOBs, addresses, emergency contacts, family members' details, and insurance plans are just some of the data that can comprise an individual's medical file. Medical identity theft is when a person illegally uses another person's information to commit fraud, such as getting prescription drugs, submitting insurance claims, charging someone else for medical expenses, etc. This is one of the most expanding criminal activities, with over half a million cases reported across the world.

Industry professionals believe that medical identity theft will proceed to skyrocket in the post-COVID era because healthcare organizations tend to invest inadequately in IT security. In fact, healthcare is the only industry where insiders are a greater threat than external ones — internal employees caused 56% of the breaches, while external caused only 44%. For instance, providers may file fraudulent claims on an individual's insurance to get reimbursement for procedures they never performed. They'll do that to offset the value of treating uninsured clients.

Apart from financial losses, victims of healthcare identity theft may face graver issues like incorrect diagnosis of illnesses due to absence of correct information or refusal of treatment due to restricted access to medical benefits.

"Organizations are far too reliant on firewalls and encryption, neither of which can stop modern-day cyberattacks," says Tom Kellermann, Chief Cybersecurity Officer at VMware Carbon Black.

Social engineering is one of the major enablers of healthcare breaches. Phishing attacks, discarded USB drives, and direct social fabrication help hackers breach a healthcare provider's records.

Consumer complaint data suggests that medical identity theft is at different rates in different regions in the US, creating hotspots. In 2013, the healthcare sector accounted for 43% of all identity theft cases in the US. Around March 2017, Indiana's Medicaid unit discovered that nearly 1.1 million patients' information had been publicly exposed through a hyperlink since February. The report contained patient data including name, Medicaid ID number, name, and address of doctors treating patients, procedure codes, dates of services, and the amount Medicaid paid doctors or providers.

Preventing Medical Identity Theft

The first step is to seek out where it started. Any new websites, response links that come attached with an unusual/unsolicited email, or any registration on e-commerce sites with improper security features can lead to such theft.

Healthcare providers require software patching and vulnerability assessments as a part of the business lifecycle. The best protection against either external or internal theft is constant monitoring through the deployment of honeypots and other security practices. Portable storage devices should be carefully regulated. The management of employees with access to patient data also needs monitoring with the access granting based on the responsibilities of the employee at the workplace.

People should keep their medical information safe and watch their credit reports for unpaid medical bills that enter the records. People who execute medical identity theft usually do so to obtain compensation from an insurance company or others for services they did not provide. To detect this type of fraud, consumers should carefully check through any explanations of the benefit payments they receive from their insurers. The insurance provider should be contacted immediately if the person gets a statement for a procedure they did not receive.

HIPAA – Health Insurance Portability and Accountability Act

The protection of healthcare information starts with educating professionals who handle patients' private data on the greater measures to safeguard patients' details. The covered entities must implement reasonable safeguards to limit incidents, and avoid revelation of PHI, including the disposal of such information. It also gives people the right to copies of their records maintained by covered health plans and medical providers. Patients may request copies of their medical and billing records to help determine the implications of the theft and to examine their records for inaccuracies before requesting further medical attention. There's no central source for medical records, so patients have to contact each provider they are doing business with – including doctors, clinics, hospitals, pharmacies, laboratories, and health plans.

Overall, it is said that the weakest link in cyber security is the human factor. Threats in healthcare continue to evolve in the future. In order to stay one step ahead of these threats, we must increase our awareness about what is happening and share more information about what is going on with our family and colleagues. Healthcare organizations should continue to support cybersecurity professionals as they help to safeguard the patient records. There is no better time than the present to improve our cybersecurity defenses.

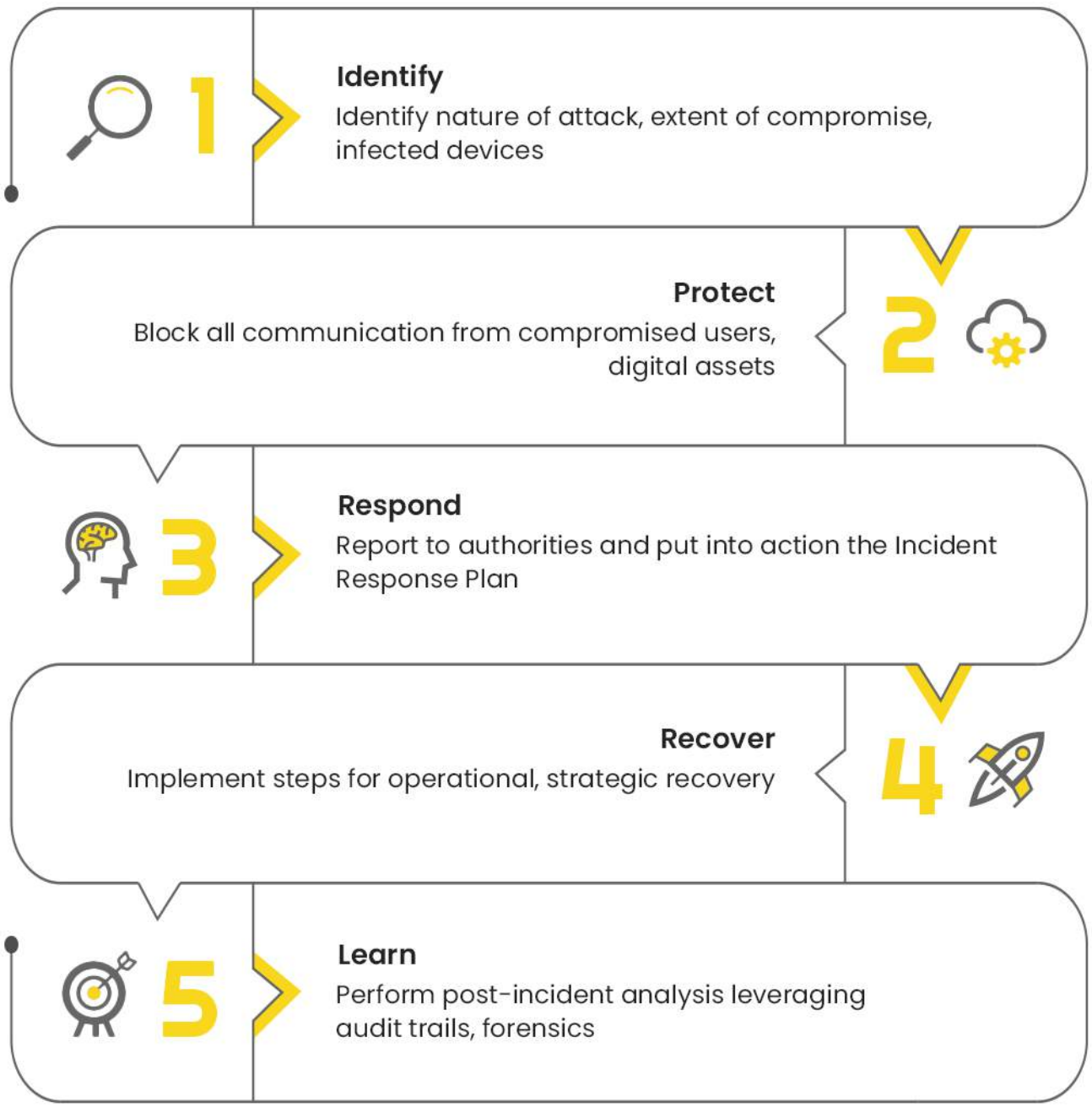
References

- https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare
- https://blog.infoarmor.com/employers/why-healthcare-industry-biggest-victim-of-identity-theft-and-data-breaches
- https://www.healthcareitnews.com/news/intermountain-cio-it-has-never-been-more-relevant-during-covid-19

About the Author

Anjana is part of the security practice. Her interests include mobile application hacking and practices web application penetration testing.

Recovering from a Cyberattack



GAVS celebrates **#CybersecurityAwareness** Month.

#BeCyberSmart

Explore GAVS' Cybersecurity Offerings at https://www.gavstech.com/service/security-services/

Risk Management - How Not To Do It

Rama Vani Periasamy

Karpagam Ramasamy

Risk management has been in most cases an overlooked activity and its potential has never been fully realized. As a member of Quality Assurance team, it is not out of the ordinary to come across risks related to projects/services in an engagement carried out as a tick-box exercise. We have seen risk registers and assessments carried out, but the concerning fact was the risk description and details.

For instance, one risk description just simply said *"There may not be sufficient resources to complete the project"*, another risk statement read *"The project might not deliver the correct quality products"*. It does not concretely convey the degree of risk and the uncertainty associated with the business.

There are umpteen articles on how to do risk management as a practice, but they fail to mention the ways NOT do risk management. Here is a list of not to do actives that might de-rail the risk management benefits and outcomes.

Generic Risk Descriptions

A common mistake that everyone makes in describing a risk is keeping it very generic and vague. The principle of "keeping it short" may not work here. There is a famous saying by Charles Kettering of General Motors, "a problem well stated is half solved". When a risk is well defined and detailed with necessary information (only), it becomes easy to manage.

The primary objective of a good risk statement should be to enable its reviewers understand the degree of uncertainty and its impact on the quality of deliverables, services, products or people.

Take the example of a poorly written risk statement "There may not be sufficient resources to complete the project." It's a generic statement and does not really explain the consequences of not having enough resources to complete the project. Surprisingly this type of statement is far too common in risks registers.

If this statement has to be detailed to bring in the real impact the risk may have on the project , it should be written like this - "There may not be sufficient java developers for the project xyz , to complete the development of the website interface, between October and November 2021." This statement makes it clear on how the risk will impact the deliverable.

Looking beyond 'Negative' Risks

As defined by Oxford dictionary, risk is "A situation involving exposure to danger", or "The possibility that something unpleasant or unwelcome will happen." The dictionary definition is so engrained in our minds, that we fail to look at risks beyond its negative connotations.

Risks may not always be negative, throwing in uncertain events and putting projects at stake. For good reasons when we drop the Oxford definition, risks can also be indicators for opportunity for an organization, which falls under the category of positive risks. Failure to act on opportunities can become a risk.

Using risk management approaches to also identify opportunities can often lead to the creation of value for organizations. For instance, a new product or service is "too successful." It generates drastically more demand than expected and overwhelms the resources. This excess demand compromises the ability to fulfil and meet the demand/requirement in a timely manner. This eventually disappoints and

frustrates the customer, weakens, or destroys brand reputation, increases your cost of doing business and reduces or potentially eliminates profitability.

This risk has a positive impact when analyzed methodologically and can bring in opportunity for the organization to elevate or augment the business.

Lack of Risk Analysis and Prioritization

An elaborate description of a risk gives us only a broad idea of what could happen and we get carried away with the misconception that a risk detailed will be mitigated and eliminated. Without an appropriate analysis and prioritization of the risks, we may be overwhelmed with the number of possible risks and fail to derive at the right risk mitigation/elimination steps.

Assigning priorities to risks is crucial and that is where the RPN (Risk Priority Number) plays a key role. Stakeholders from all parties must be involved in contributing to the Risk Matrix early and regularly, which can be accomplished by following the three simple steps of analysing, prioritizing, and controlling. Risk management should never be carried out as an isolated exercise, but as a collaborative one.

Risk prioritization is important because it also makes it easy for the leadership group to make decisions about where to invest resources to increase the certainty around each risk (whether threat or opportunity).

Passive Risk Management

Risks are commonly associated with some actions, but it can also occur from inaction. In most cases, risks may be identified but they are largely ignored in the planning and execution process until some undesired events occur, at which time solutions are sought.

In order to become active managers of risk there are some important steps to take once a threat or opportunity has been identified, described, analyzed, and prioritized. Analysis and prioritization are key in preventing a risk from becoming a passive one.

The key step is to consider what options are available to us so that we can respond appropriately. There are a range of responses which can be used to alter the cause of the risk, perhaps avoid the event, or possibly reduce the effect.

Lack of Accountability and Responsibility

After the risk has been recorded successfully, we must think of who is going to act on our recorded risk. When a risk is not assigned an owner for action, it is very much a potential candidate of passive risk. Risk accountability and responsibility has an essential role to play in the strengthening of risk management practice. This is a vital information which is ignored in many risk registers.

These are some important roles we can identify to associate with each risk at a project level or engagement level-

- Risk Author – the person who identified the risk, as they will be a key source of information
- Risk Owner – the person responsible for managing the risk, ensuring that its status is monitored
- Risk Actioner – the person who is going to implement one or more responses to a risk.

Risk management and risk registers are used in many projects, but it should not become a mere bureaucratic piece of artefact. Project managers need to ensure that they are managing risks and not simply contributing to a bloated risk register that has detailed risk data and that no one is bothering to manage. Again, the point is not to be a mere chronicler of risks for the project post-mortem, but to take actions and keep the eyes and ears open for opportunities to mitigate risks

It is time that we take fresh look on our organizational practices, change our attitude of looking at risk as “something that might go wrong” and advance towards adopting better approaches to this extremely vital area of project management.

Reference

Risk management – how NOT to do it | AXELOS

About the Authors

Rama is a part of Quality Assurance group , passionate about ITSM. She loves reading and travelling.
To break the monotony of life and to share her interest on books and travel, she blogs and curates at www. kindleandkompass.com

Karpagam is a part of Quality Assurance team at GAVS. She is interested in learning new methods and technologies. Her passions include playing fencing and sketching. She enjoys music and travelling. She believes that, “If you are not willing to learn no one can help you”.

When they say you can't,
they show you their limits,
not yours.

- Kevin Keenoo -

enGAge

GAVS Technologies | www.gavstech.com

Follow us on: