

# TOP CYBER NEWS MAGAZINE

A close-up portrait of a man with a thick, well-groomed reddish-brown beard and mustache. He has light brown hair styled upwards and back. He is looking directly at the camera with a neutral expression. He is wearing a dark, possibly black, jacket or shirt. The background is a soft, out-of-focus blue-grey gradient.

APRIL 2022

**JAY JAY DAVEY**  
SOC TEAM LEAD at CYBERCLAN

Taxonomy of a SOC™

Editorial article by

**Scott D. FOOTE**

CISO, DPO, Managing Director, Founder  
at Phenomenati – Boston, the USA

## THE FUTURE of SECURITY OPERATIONS

HOW JAY JAY DAVEY HELPS ORGANISATIONS PROTECT THEIR VALUE AND DEFEND THEMSELVES FROM CYBER SECURITY  
THREATS BY BUILDING ROBUST AND EFFECTIVE SECURITY OPERATION CENTRES, AND HELPING THEM MATURE



*"Expect the Unexpected  
Envision the Impacts  
Think Solution  
Deliberate Action!"*

~ Stéphane NAPPO, VP & Global CISO  
Groupe SEB





## CREATE A SECURITY OPERATIONS CENTER TARGET MODEL TO DRIVE SUCCESS

The Security Operations Center (SOC) maintains an increasingly complex purview, managing all aspects of the organization's cyber security. Monitoring, evaluating, and driving down risk to the organization is the core job of the Security Operations Centre.

For many organizations, creating and maintaining an effective security operations center can be challenging. Even on a good day, this mission relies upon timely, accurate, and comprehensive knowledge of all aspects of business operations – processes, priorities, people, information and enabling technology.

Complicating this mission, digital transformations continue to expand the complexity of business dependencies upon highly distributed systems and services, increasingly sophisticated devices, and intricately entangled networks, where cybercriminals are seeking to exploit the vulnerabilities inherent in those complex dependencies and cyber threats today are relentless and continuously seeming one step ahead to organization's defenses. To keep pace, every SOC must constantly evolve its capabilities and threat intelligence gathering that informs its decisions and defensive posture.

*“Break down information barriers between physical security and cybersecurity teams. Overcome resistance and drive success using the right Security Operations Center Target Model.”*

Top Cyber News MAGAZINE Team





Digital MAGAZINE

About People

By People

For People



# TAXONOMY OF A SOC™

## THE TOP 20 CAPABILITY AREAS FOR CYBER SECURITY OPERATIONS

### Editorial by Scott D. FOOTE

CISO | CPO/DPO | Managing Director | Founder

At *Phenomenati*, we spend a lot of time working with clients to evolve their Cyber Security Operations efforts.

This can involve process (re)engineering, staffing, technology evaluations, and even system deployments; for teams ranging from a “force of 1” to dozens. But every engagement starts with establishing clarity on two points – 1) *Where are you now?* and 2) *Where do you want to go?*

To facilitate that discussion we have developed a high-level “**Taxonomy of a SOC**”. It’s a reference model, based on the top 20 capability areas that we repeatedly see Cyber Security Operations teams working to address.

That’s a large number of topics to cover, so we have organized them by the 7 major challenges that most Cyber Security Operations teams wrestle with, or will as they grow:

1. Knowledge of one’s own cyber infrastructure (including ICS, IoT, etc.)

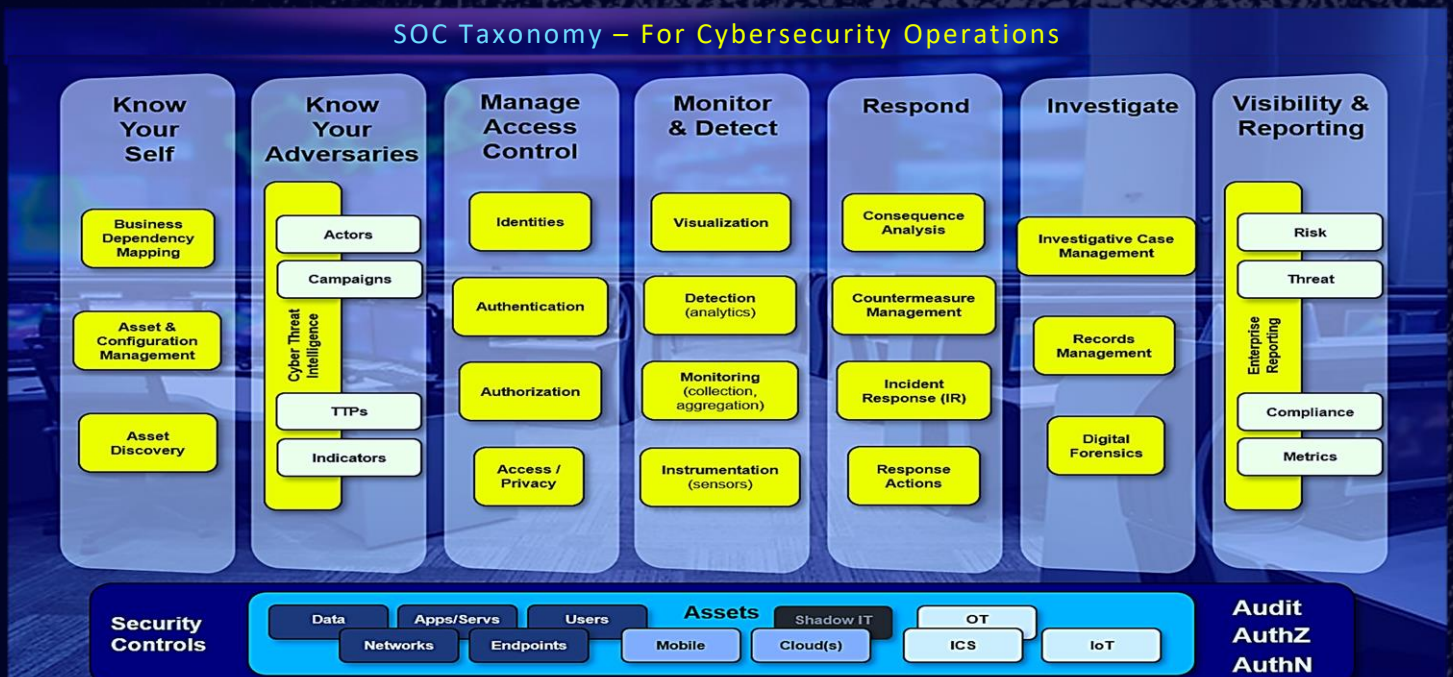
2. Threats emerging in cyberspace
3. Management of Access Controls
4. Monitoring and Detection
5. Informed Incident Response
6. Forensic Investigation, and
7. Visibility through advanced reporting

The list of capability areas is a broad superset, and is intended to be descriptive rather than prescriptive. It’s offered strictly as a reference model to inform Security Operations roadmaps, or simply to help teams manage expectations with their stakeholder and leadership communities. The following is an outline of the taxonomy:

#### Knowledge of one’s own cyber infrastructure

- Capability Area 1) Asset & Configuration Management
- Capability Area 2) Asset Discovery
- Capability Area 3) Business Dependency Mapping (e.g., “Business Impact Analysis”, or “Mission Mapping”)

#### SOC Taxonomy – For Cybersecurity Operations







### Threats emerging in cyberspace

- Capability Area 4) Cyber Threat Intelligence (e.g., "CTI" and Threat Intel Platforms or "TIPs")

### Management of Access Controls

- Capability Area 5) Identity Management
- Capability Area 6) Authentication Management
- Capability Area 7) Authorization Management
- Capability Area 8) Privacy/Confidentiality Management

### Monitoring and Detection

- Capability Area 9) Instrumentation (Sensors & Tuning)
- Capability Area 10) Monitoring (Collection, Aggregation)
- Capability Area 11) Detection Analytics (e.g., "Big Data" security analytics)
- Capability Area 12) Visualization (e.g., Analyst's dashboards, operational pictures)

### Informed Incident Response

- Capability Area 13) Consequence Analysis (e.g., answering the "**So What?**" imperative)
- Capability Area 14) Incident Response (IR) Workflow
- Capability Area 15) Countermeasure Management (e.g., "Playbooks")
- Capability Area 16) Response Action Management (e.g., "Security Automation & Orchestration")

### Forensic Investigation

- Capability Area 17) Digital Forensics (DF) Analysis
- Capability Area 18) Case Management
- Capability Area 19) Digital Evidence Management

### Visibility through advanced reporting

- Capability Area 20) Enterprise Reporting (e.g., KPIs, GRC, and beyond)

Any one of these topic areas on its own, is broad enough to require a more detailed inventory of specific capabilities and requirements. Which may explain why so many mature SOC's employ an average of more than 50 individual tools and technologies.



**Scott D. FOOTE** is an influential leader and communicator and a highly respected experienced cybersecurity executive, designing security and privacy into digital transformation initiatives for his clients.

With more than 30 years of technology leadership experience in cybersecurity and the broader software industry, Scott has an acute ability to understand and map organizational needs to security models, architectures, solutions, and technologies.

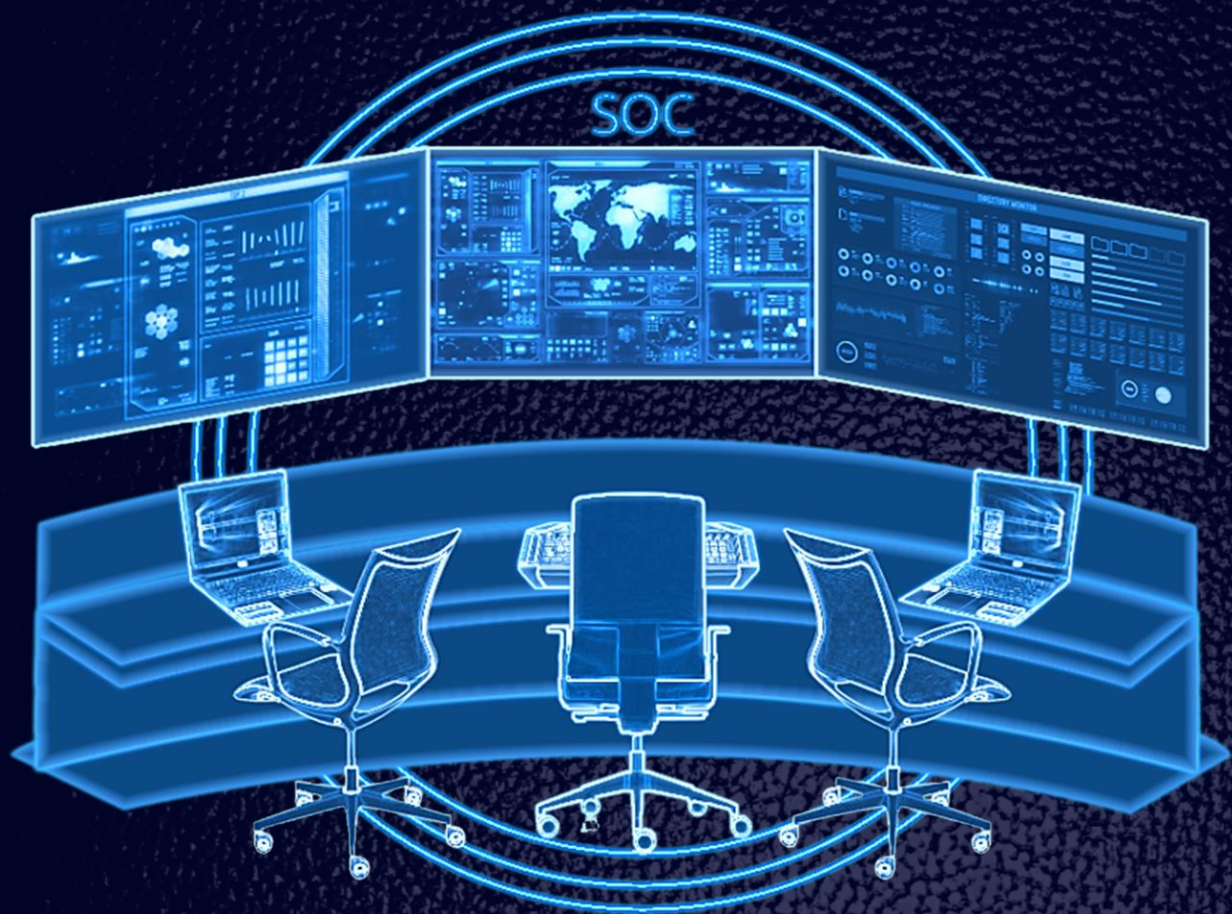
Maximizing return on investment drives every role Scott has played. First as an engineer, then product executive, then analyst, board member, and most recently as a CISO.

Driven to deliver high impact, his leadership experience includes building and leading growth-dominated products and services teams, organizations, and startups leading teams from 10 to 1000.



# Phenomenati

## The Will To Act



Cyber Security Advisory & Consulting Services  
vCISO, CISO-as-a-Service (CaaS)

<https://phenomenati.com/leadership>



A close-up portrait of a man with a full, well-groomed reddish-brown beard and mustache. He has short, light brown hair styled upwards. His eyes are a striking light blue. He is looking directly at the camera with a neutral expression. The background is dark and out of focus, with some faint white curved lines visible in the upper right corner.

## JAY JAY DAVEY, ENGLAND

Respected and cherished by the generation of young cybersecurity professionals worldwide, England born, **Jay Jay DAVEY** is a true representative of the future technology-driven generation. Jay Jay endeavours to help others break into the industry by creating content for people to learn from and building communities to help bring people together.

Jay Jay has been involved in technology and has worked with private, public, and non-profit organisations for over ten years, investing in and developing his strong passion for security operations. A leader in security operations with a mission to help businesses realise the benefits that a defined and aligned security operation centre can bring, Jay Jay is leveraging his experience with a wide range of solutions used by SOC teams. Additionally, he has been involved heavily with implementing processes, playbooks, and the overall strategy of SOCs to address his clients' strategic, operational, training, and business development needs. As a firm believer in better together, Jay Jay is selflessly committed to helping people grow. He has a personal endeavour to bring people together and cultivate a positive community within cyber security by participating in multiple platforms and programs designed to help people. The most recent is CyberMentorDojo, a platform designed to help people mentor others and find mentors.

Looking to the future, Jay Jay strives to become more established in security operations globally and reach the level of a figurehead in security operations with a mission to help SOC teams worldwide grow to be more effective and efficient in building resiliency for the business.



# SECURITY OPERATIONS CENTER MATURITY. TANGIBLE BENEFITS

by Jay Jay DAVEY

*"A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents."*

~ McAfee Enterprise

***"Security Operations Center Maturity Enables a Robust Security Posture."***



Security operations center(s) are an endeavour that many businesses undertake, whether outsourcing or building the capability themselves; this comes with unique challenges around ensuring it is effective and efficient. But what does this mean? It is a vague statement, so I'll clear it up or at least attempt to; security operations need to be aligned to the strategy of the business, meaning it should have the capability to identify and respond to events and incidents that seek to undermine the goals and objectives of the company. Additionally, it can provide good metrics to help security leaders make informed decisions, but those metrics are pain points for most SOC implementations, both outsourced and on-premises.

Before I break down improvement, I want to touch on what I believe to be the most vital part of maturity and growth of a SOC, **and that is the people**, ensuring that they have the skills and development of skills to help bolster the capability of the SOC which ultimately leads to

maturity. Strengths and weaknesses will need to be identified, and with that information, skill development plans can be developed. As the team learns more and gains new skills, it is wise to ask their input on related projects that affect the SOC.

This process should also highlight the team member's ambitions, and it is essential to consider how these ambitions can be harnessed to improve the SOC. For example, an analyst who has the ambition to become a penetration test could assist in the identification of vulnerabilities and validation of controls to help give them the experience and development towards their personal goals; this will lead to better job satisfaction and overall, SOC improvement.

***"Where do we start with maturity? First, you need to measure and understand where you currently are regarding your capabilities, resources, utilisation, and modus operandi."***

To do this, you can perform what we call an in-depth maturity assessment which is an audit of everything from processes, people, and technology to understand what is going on; with this, it pays to be hypercritical to get to the truth of the matter. Once you have completed this assessment, you will be given a score that could be painful for some but a moment of enlightening for others; most importantly, you know where you stand and here is where the fun begins.



You have just completed a gap analysis essentially, you know where you are going wrong, which highlights where you can improve, but now you need to build that strategy to improve. Please don't jump the gun too much here, and we need to make sure this approach is sound from a feasibility perspective. Is it possible?

You have identified these gaps; you now need to select what to improve immediately; people go for the quick wins; however, you should choose the ones that have the highest return regarding increased effectiveness and efficiency while respecting the project's cost. **My advice is to get your processes and playbooks in order, make sense, and communicate with the team before moving on.**

It makes no sense to have a reckless ad-hoc approach to these improvements, and you need to ensure that they are agreed upon and tracked as projects; uncontrolled changes could undermine the mission for maturity. Instead, use project management software or a simple kanban board to help track, communicate and plan these changes and be sure to engage with internal change management for advice and guidance.

Now it is time to start making these changes; before we go any further, it is best to commit to a date for a reassessment to show the positive impact of your maturity mission. Implementing changes into a SOC is not as simple as throwing a process here or changing a rule; the changes need to be meaningful, and the team need to be aware of them. For example, if you implement something like a new incident response process for the SOC, you should make sure this is communicated and tested for effectiveness. Again, you are not looking to score points on the assessment; you are looking to improve.

**How do we prove the improvement?** Again, the reassessment should be a guide only here; we need to get tested to validate our new controls and enhancements to ensure they provide the effectiveness and efficiency we are looking to gain from this endeavour.

There are many ways we can test the SOC, from penetration testing to verify the ability to detect different types of attacks and compare them against a framework such as MITRE ATT&CK. to a tabletop exercise of playbooks against various kinds of attacks. Further to this line of thought, you may need to show senior management how well the SOC is doing; from a time-sensitive view, we need to provide metrics that paint a picture of how well the SOC is doing. Think of metrics like white paint; it is good but not enough to paint an accurate picture; context is like adding colour to the white paint; metrics with context paints a more accurate picture. The SOC's metrics should align with particular business requirements, most importantly, the enterprise risk management function. The metrics may help that team make decisions on a specific risk or add context to identified risk to help remove some uncertainty around risk.

Control validation is a crucial aspect of bolstering not just the SOC capability but also the technical security posture;. At the same time, some think penetration testing and vulnerability assessments are an excellent way to validate our controls, we can take this a step further and perform audits of our controls. The outcome of this should be the assurance we are leveraging these controls to the best of their ability; ask yourself, are you getting the most out of your EDR or SIEM?

Additionally, periodically assessing these controls as they are updated will help ensure that the coverage remains the same while fully utilising the controls. Vendor relationships are meaningful to get the support and documentation required to assist in the control validation.

**Security operations capabilities can be improved in many ways, but the main focus for many SOC's will be the detection and response;** I mentioned earlier about using testing to detect whether the current solutions can detect activity related to the MITRE ATT&CK framework. First, however, it is essential to align your capabilities to the framework to help add context to what



you are deploying, what information you are ingesting, and how you are using that information to detect and respond to the different stages of the attack lifecycle.

Scoping data sources is essential, and it must have context from the MITRE ATT&CK Framework; there is no point ingesting data if you are not going to use it or have future scope to use it. We need to understand what we are looking for and there are complimenting frameworks to ATT&CK that allow us to leverage data sources much better. The DeTT&CT framework, while not produced by MITRE, will give us vital information to enable informed choices when selecting data sources; this should relate to the use cases. Data source life cycle is essential as the SOC evolves because there may be limitations on licensing and bandwidth. Data sources will need assessments to determine their coverage and whether tuning or sunseting data sources are required.

**The SOC of the future should no longer be solely about monitoring and detection; to evolve, it will need to add more capabilities to its arsenal to move beyond the traditional and somewhat broken SOC model.** Proactive improvements of security controls are something the SOC should be helping with using their visibility of the infrastructure to find misconfigurations and help manage them before they become a more significant issue. At the same time, threat hunting is part of this process, and there needs to be a more substantial emphasis on adding context to it with proper threat intelligence. Finally, the lift and shift mentality of the current SOC needs to change; it should be confident enough to handle and respond to incidents if identified instead of treating them as someone else's problem.

If you are starting this journey without metrics, I recommend building a current baseline alongside your assessment; you can create a trend analysis to help show improvement over time; these need to be selected based on the applicability.

For example, you would choose not to use detected threats as this can change as the threat landscape changes but instead a metric like a downtrend in vulnerabilities based on patching efforts; In contrast, this changes often, our actions can have a significant impact on it. **Remember, we can not control the threats, but we can certainly make it harder for them to leverage our vulnerabilities.**

To start this journey, I would recommend you conduct the basic assessment from SOC-CMM alongside this making a conscious effort to build an inventory of skills, technologies and processes, ideally keeping it all in one place for ease of reference. Mapping your efforts to known standards like ISO27001 can be a challenge and reasonably cumbersome; I recommend building a solid relationship with the information security team members to help understand where your function fits into their requirements. The SOC-CMM assessment maps to the NIST Cyber security framework, which translate relatively easily to different standards, good reference for this is the 800-53.

**While a SOC is a valuable function that works towards resiliency for the businesses, it is worth keeping in mind that creating one is iterative and requires lots of work to ensure that it is future-proof and provides a return on security investment. Otherwise, it becomes a cost centre with no actual benefits being realised.**

Overall, assessments can help SOC teams identify gaps in their processes, detection and overall capability; with the completion of an assessment, an improvement plan can be made in line with the desired state and current resources. However, improving a SOC is no easy accomplishment as it is an operational function within the business, and changes to that could negatively impact deliverables and desired outcomes. With that in mind, changes need to be meticulously planned and safely integrated into the current modus operandi to minimise negative impact.





# DOCTORAL VIRTUAL OPEN HOUSE

Attend a free information session to find out more about Capitol Technology University and our online Doctoral Programs taught by world-wide academics and industry experts with a global perspective.

Small cohorts, responsive professors, and dynamic, experienced peer groups allow doctoral students to imagine and test new boundaries and ultimately become a conduit of new knowledge for others.

*Scan the QR code with  
your mobile device's  
camera app to access  
registration page:*



We offer virtual open houses once a month on **Sunday at 3 p.m.** \*

January 9, 2022

July 10, 2022

February 13, 2022

August 14, 2022

March 13, 2022

September 18, 2022

April 10, 2022

October 16, 2022

May 15, 2022

November 13, 2022

June 12, 2022

December 11, 2022

\* Eastern Time (UTC-05:00)

To register, visit [www.captechu.edu/doc-info](http://www.captechu.edu/doc-info)

✉ [doctorate@captechu.edu](mailto:doctorate@captechu.edu)

*It's 2022 - Every job is a technology job!*



# NEXT GENERATION SECURITY OPERATIONS CENTER

by Fatimah ADELODUN

A cyberattack occurs every 39 seconds. organizations are struggling to keep up with the evolution of pervasive attacks. Cybersecurity talent shortages, increases in connected devices, and changing regulations are just some of the challenges facing the information security community.

For most organizations, automated security operations are critical in ensuring protection against cyber-attacks. They monitor and analyze security activities ranging from users' activities on a network to application interactions (APIs), and data exchanges between systems and users, etc. on an ongoing basis.

Before establishing a SOC, organizations need to create a strategy that guides the overall objectives of security across the organization. The National Institute of Standards and Technology (NIST) is the principal standard for many SOC's. These guidelines provide a comprehensive overview of rules and technologies that can be used to safeguard against breaches and streamline incident responses. This also is a major blueprint to help discover your organization's information/ cybersecurity program.

Taking in data from an organization's assets, including infrastructure, networks, cloud services, and devices, the SOC focus on monitoring, analyzing, preventing, and responding to existing and potential threats and ensuring the organization is protected from attacks. The required skill set to run an effective SOC includes an incident responder, security investigator, advanced security analyst, security engineer/ architect, threat intelligence specialist, etc.

## The Importance of a SOC

The criticality of a SOC cannot be overstated. It provides situational awareness of activities on your technology landscape from a security point of view. It gives you round-the-clock visibility of every activity in your enterprise (data applications). It is also vital for organizations that must comply with security standards industry regulations, such as HIPAA, GDPR, PCI DSS, ISO, SOC2, etc. Whether located on-premise, cloud-based, or even outsourced (soc as a service), it may mean the difference between preventing a breach and a successful attack.

## Some Benefits of SOC to a cloud-based environment

A SOC enables you to actively monitor cloud activity and the behavior of users and applications to:

- Protect availability
- Protect data against unauthorized access
- Defend against insider threats
- Manage vulnerabilities and maintain a high-security posture
- Defend against external threats
- Comply with cyber security governance, risk, and compliance mandates

## Forces Shaping the modern SOC

Several factors can be attributed to the increased pressure on how SOC's traditionally function. While in the past, a SOC was restricted to a physical room in which security professionals worked, today, resulting from Covid-19, the adoption of cloud computing and remote work is accelerating and this is driving the adoption of SOC's.



This means that as more organizations are moving their servers, data, and workloads to the cloud, securing and protecting them becomes a major concern. Having dedicated analysts monitor and respond to incidents continuously provides a critical element of effective cloud security.

Today, SOC operations are evolving from exclusive use of logs in SIEM tools to the use of security orchestration, automation, and response, leveraging Machine Learning (ML) and Artificial Intelligence (AI).

**The unique environment of the cloud presents a peculiar and ever-evolving threat landscape. Traditional cyber security best practices are not as effective in the cloud, and processes and tools that work for on-premise data or local data centers will most likely not suffice in the cloud.**

Cloud security works on a shared responsibility model where the cloud services provider takes care of protecting what it owns—the physical infrastructure on which the cloud resides, but organizations are responsible for securing anything they install, run, or store in the cloud.



**Below are some factors to consider to update your SOC to the next level:**

1. Design, implement and automate tested and proven processes: The operation of a good SOC is based on a well-defined process and framework.
2. Capacity Development: It's important that analysts working in the SOC are trained continuously to enable them to hone their skills and help them be more efficient in the protection of your organization against bad actors.

3. Use intelligent tools to enhance decision-making: most companies have too many tools and often these tools are not utilized to their full capability. Some services that traditionally are incorporated with SIEM (e.g., data loss prevention tools and endpoint protection (EDR)) are also moving to the cloud. Increasingly, companies are going to need to supplement or replace on-premises tools with cloud-based products and services
4. Ensure log collection from cloud infrastructure to SIEM: If a cloud service offers an API data feed, then the log data can be pulled into the SIEM so that security analysts will have a single view of all their systems.
5. Consider Managed Soc As A Service (SocAAS): many organizations are already using managed SOC services providers. Managed security analytics and operations services deliver a range of capabilities, including around-the-clock threat monitoring of networks, endpoints, and applications; incident detection and response; SIEM-to-security orchestration, and compliance reporting.
6. Incorporate machine learning to boost threat hunting. As data volumes and security alerts increase, machine-learning (ML) tools are becoming increasingly important in threat detection and response.

***“It should come as no surprise that cloud adoption is accelerating. Utilizing cloud-enabled (SOC) provides a critical element of effective cloud security. SOC's help to focus on the evolving threat landscape and quickly identify and investigate new and emerging threats.”***



# FATIMAH ADELODUN, NIGERIA

A portrait of Fatimah Adelowun, a woman with dark skin, wearing a black turban and a black blazer over a white collared shirt. She is smiling and looking towards the camera. The background is a vibrant red with abstract, flowing white and pink lines.

**Fatimah ADELODUN** is the Information Security Manager at the Nigerian Bulk Electricity Trading Plc, the foremost electricity trading company in Nigeria and one of the largest Energy companies in Sub Saharan Africa.

In that role, Fatimah works to ensure that the security of the infrastructure and data of Nigeria's leading electricity trading organization is protected while leveraging emerging technologies to improve the internal processes that run to produce a financially viable electricity market.

She has a decade of experience in IT & Cybersecurity spearheading highly visible projects that span across Project Management, IT Operations, Security Operations/ Computer Security Incident Response Team (CSIRT) Management, Infrastructure & Asset Security Management, Information Security Standards & Compliance, and execution of the organization's cyber security strategy.

As a strategic cybersecurity leader, Fatimah is leading the charge at encouraging women to pursue careers in the STEM fields, particularly, cybersecurity. She is the founder of SheLovesCyber- an online (Instagram) platform that educates people on practical tips to be safer online and guidance to people that want to pursue careers in Tech & Cybersecurity.

She holds a Bachelor of Science in Computer Science and a Master of Business Administration (MBA) with a specialization in Global Leadership from Edhec Business School, Nice, France. She is a Certified Information Security Auditor (CISA), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH), Project Management Professional (PMP), AWS Solutions Architect, among others.



# CHAMPIONS ARE BRILLIANT AT THE BASICS

by Amit TENGLIKAR

***“Champions are brilliant at the basics.”***

I am sure the veterans of Cybersecurity industry would agree that this simple quote from **John Wooden** makes complete sense in Cybersecurity. **Basics** are not just foundation but takes up much more complex responsibilities in securing the crown jewels (i.e., business critical data) of any organization. It makes perfect sense if you look at it either through the prism of organization's foundational framework i.e., **People, Process and Technology** or through the prism of Information Security CIA Triad (**Confidentiality, Integrity and Availability**).



We have seen from time to time that the cost of data breach is ever increasing, in 2021, as reported by IBM data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the past 17-years. Further, the average cost was USD 1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor. In this chaos of Cyberattacks, we often miss out on the importance of making small basic changes in our Cybersecurity environment, which most of the time, yields significant improvements in the overall security posture and saves our organizations from Cyberattacks.

***“Through the time we have witnessed so many of Cyberattacks which could have been prevented by strengthening basics of cybersecurity and by revisiting and improving from ours / other's experiences.”***

One of the notable examples is of Marriott Hotel Cyberattack, due to which the hotel chain was fined £18.4m for a major data affecting up to 339 million guests. Apart from this its share prices dropped too, and it had to face class action suit. This could have been prevented by having Cybersecurity team overseeing the acquisition of compromised Starwood Hotels, and by conducting a proper Cyber due diligence / Cyber assessment. As we understand, ***“all the shiny Cybersecurity boxes (such as firewalls, Intrusion detection systems (IDS) etc.) in the world won't help if our basics are not setup correctly.”***

For examples, if we don't know what assets (both physical / logical) a company has, and who has access to those, then in most cases the Cybersecurity device won't be able to save you from a breach. Similarly, if there is no effective patch management program in place to patch your assets in a timely manner, then having other security controls / device might not serve the intended purpose. Another factor which adds significantly to the success / failure of Cybersecurity posture of the organization is its Cyber-aware culture amongst its people (Employees, Vendors, Partners etc.). To have the Cyber-aware culture, its essential to have an effective Cybersecurity awareness campaigns and programs, which will create a human firewall which can defend considerable number of attacks posed at them including Phishing. *It should be noted that, according to multiple surveys over 80-90% of all Cyberattacks involves Phishing / Spear Phishing.*



We need to put in conscious efforts to secure our digital environment for securing ourselves, our businesses, our people, our clients, and our partners. This exercise can be initiated with a simple approach with implementation of basic controls addressing each of the 5 functions of Cybersecurity (by NIST) i.e., **Identify, Protect, Detect, Respond, and Recover**.

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

***Once we have the basic framework as per NIST, it's important to further look into gaining quick wins.***

As per Pareto Principle, or 80/20 rule, if we adopt to Cybersecurity, we can surely aim to get 80 percent of positive results with 20 percent of disciplined actions. We must understand that not all cybersecurity risks are created equal. Hence, by using this rule, CISOs and CSOs can tackle practical Cyber risks efficiently with quick wins. So, before tackling the threats with a lower impact on the business, the organization must shift its efforts and resources in the direction of the most formidable threats. The remaining risks still needs to be addressed by management with the appropriate measures, however, with 80 percent results (cybersecurity 80/20 rule) you'll have covered all key bases.

To tackle the rest of the 20 percent of Cyber risks, a consistent sustained effort is needed by the management. CISOs should employ **Defense in Depth** concept to implement multiple layers of security controls (defense) throughout information technology (IT) system which can provide redundancy in the event a security control fails, or a vulnerability is exploited by the threat actor. Thus, protecting your crown jewel. Also, CISOs / CSOs should look at tackling **Advanced Persistent Threat (APT)** by implementing NextGen Security Solutions which works beyond traditional Antivirus landscape and prevents APT attacks through advanced detection and prevention techniques.

Also, moving to cloud for certain Software as a service (SaaS) service such as Office 365, will surely add significantly to the security posture of the organization, since cloud typically has better security and ransomware protection, then on-prem servers providing these services. Further, the vulnerability and patch management is also flawlessly undertaken with minimal disruption for these services, which not only enhance customer experience but also reduces the overall cyber risks.

Lastly, let's remember the famous saying, ***"Cybersecurity is a journey, not a destination"***, and improvements are essential to make this journey pleasant and fulfilling one. To have improvements, it is necessary to revisit our existing cybersecurity environment and see if it can be improved continually by learning our lessons from ours/other's experiences.





# AMIT TENGLIKAR, DUBAI, UAE



**Amit TENGLIKAR** leads BDO UAE's Technology Advisory Services practice with clients served across the Middle East, India, Africa, and Southeast Asia. He is responsible for growing and delivering BDO's technology advisory services including Cybersecurity offerings, Internal Audit, Advisory and consulting Services. He is fortunate to have worked in varied industry sectors such as Government entities, Healthcare, Manufacturing, Education, Insurance, Oil & Gas, Real estate etc. He holds Bachelor of Engineering in Electronics & Communication, and several professional certifications recognized globally including Certified Information Systems Security Professional (CISSP), Certified Data Privacy Solutions Engineer (CDPSE), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM).

He advises clients on best practices for handling information throughout its life cycle, from creation or collection through disposition. He has extensive experience in working with organizations' internal audit teams and audit risk committees, to deliver highly complex cybersecurity audit and assurance engagements to clients across UAE. He also consults clients on various domains including IT risk management, cybersecurity, information governance, data privacy, data security and provides advice which resolves complex technology and cybersecurity challenges.

He is ever curious and proactively keeps tab on current and new age Cyber technologies, and likes to share his experiences and insights through various public speaking events including PrivSec Global and Internal Auditors Association. He has a keen eye on resolving complex cybersecurity challenges faced by businesses in a simple intuitive way; and consults clients on various domains including Cybersecurity, Technology risk management, data privacy & protection and business technology risks.



# WHY BUSINESSES CONTINUE TO FAIL CYBER SECURITY!

by Edward MILLINGTON

Global media headlines continue to demonstrate the Global Cyber War many businesses are confronting in the digital world, where Cyber Attacks from Advanced Persistent Threats (APT's), Phishing Emails, Ransomware, Malware, Exploitation of Vulnerabilities, etc., makes it difficult in having the possibility of winning such war - unachievable, unbelievable and financially prohibiting. Adversaries always seem to be one or more steps ahead, possibly demoralizing Boards and their management infrastructures, inflicting organisational risk - strategic risk, reputational risk, operational risk, transactional risk, and compliance risk.

Adherence to data protection laws, regulations, policies, standards, and nation-state directives should therefore be driving IT and Information Security Governance programs maturity capabilities levels higher, but the continuing loss of data and information (affecting the CIA), including the availability, integrity, and safety of systems through incidents, compromises, and breaches; demonstrates that such governance programs are not being managed and operated well within their lifecycles, which reflects severely at the C-Level - who ultimately holds the full responsibility of the organization.

*"For an organization to manage its cyber-risk - cyber threats and attacks, nation-states attacks, including insider cyber-criminal activities, it is essential that its existing Information Security Governance Program must be continually evaluated, monitored, and updated for its effectiveness and efficiencies."*

The Information Security Governance Program must be RISK-BASED, where all risk management processes and functions that

govern the development and implementation of Security Controls (whether administratively, technically, and or physically) are instituted appropriately - reducing organizational risk and attack surfaces. For the program to be effective, IT Risk Management must also be integrated into the organization's risk management framework, thereby allowing risks to be managed and operated upon by the Enterprise Risk Management System.

The following are possible reasons why cyber-affected businesses' Information Security Program fails in protecting them.

1. The risk management activities were not thoroughly carried out in the development of the program, resulting in **ineffective, inefficient, and insufficient** policy-based security controls.
2. Outdated Security Controls in reducing risks associated with the cyber-defense against adversaries Tactics, Techniques, and Procedures (TTP)
3. Inadequately directing security engineering designs
4. Incorrectly advising on the procurement of security solutions
5. Institute minimum critical monitoring controls that would provide the visibility and awareness needed, where data collected is analysed using Machine Learning, AI, and other techniques to evaluate and highlight potential risks (including safety risks), attacks, compromises, and breaches.
6. Inability to identify, protect, detect, respond and or recover from cyber threats in all areas of the business due to immature and or non-compliant security policies.



While a cyber-attack will occur, the business priority is to make sure that attack surfaces are small and the dwell time (time taken to detect an incident) is in seconds to minutes and not hours, thereby raising the Incident Response Maturity level to the highest.

*“An Information Security Governance Program is a guiding document that strategically aligns the organization, its people, process, and technology to the organization’s vision, goals and objectives; through security frameworks, policies, standards, procedures, and guidelines in securing business assets.”*

While any business information security governance program should contain risk management activities, there is a strong possibility that those activities may not be mature enough or have stopped working, especially if the business is not compliant or does not need to be in complaint to existing standards, laws or regulations. The risk assessments needed to identify threats, vulnerabilities, assets value and the probability and impact of threats occurrence may not be carried out efficiently and accurately, in the determination of the true risk to the asset(s) for **risk treatment**. The end result of ineffective risk management processes can lead to **ineffective, inefficient, and insufficient** security controls, thereby expanding the organization’s attack surfaces to be compromised and breached; exposing assets on a greater scale for exfiltration, unauthorized access and changes, damages, and or unauthorized control. In addition, the Risk Register that is used to track identified risks does not reflect risks in its entirety and risk level. In essence, the risk management life-cycle that is needed to keep risk to an acceptable level is nonfunctional.

**Not understanding the true risk to assets for risk treatment, the implementation of Security Controls** like 1) Antivirus 2) Firewall(s) 3) Configuration & Change Management 4) Identity and Access Management 5) Logging & Auditing 6) Security Methodologies, etc. may not be appropriate in the identification, protection,

detection, response, and recovery from an incident(s) - **can allow a cyber-attacker into the organization affecting its operational risk – as mentioned earlier at the beginning of this article.**

The Information Security Governance Program in operation also implements an Information Security Incident Management Program - in the management of security incidents. The maturity of this program demonstrates how capable the business’ Security Incident Response Plan functions and operates in the handling of a security incident, throughout its lifecycle phases.

A good design Incident Response Plan implies that the incident response to an attacker can be swiftly managed, reducing the dwell-time and attack surfaces coverage. For the incident response to be efficient and effective, the incident response plans much have the following:

1. Resources with the correct skills and tools
2. Assigned personnel with roles
3. Playbooks
4. Testing plans
5. Detection, eradication, and recovery tools
6. Effective communication between all parties and resources

The failure to respond to a security incident accurately and timely can occur by not appreciating the business impact and critical analysis performed in the realization of a threat to the business – again through risk management activities.

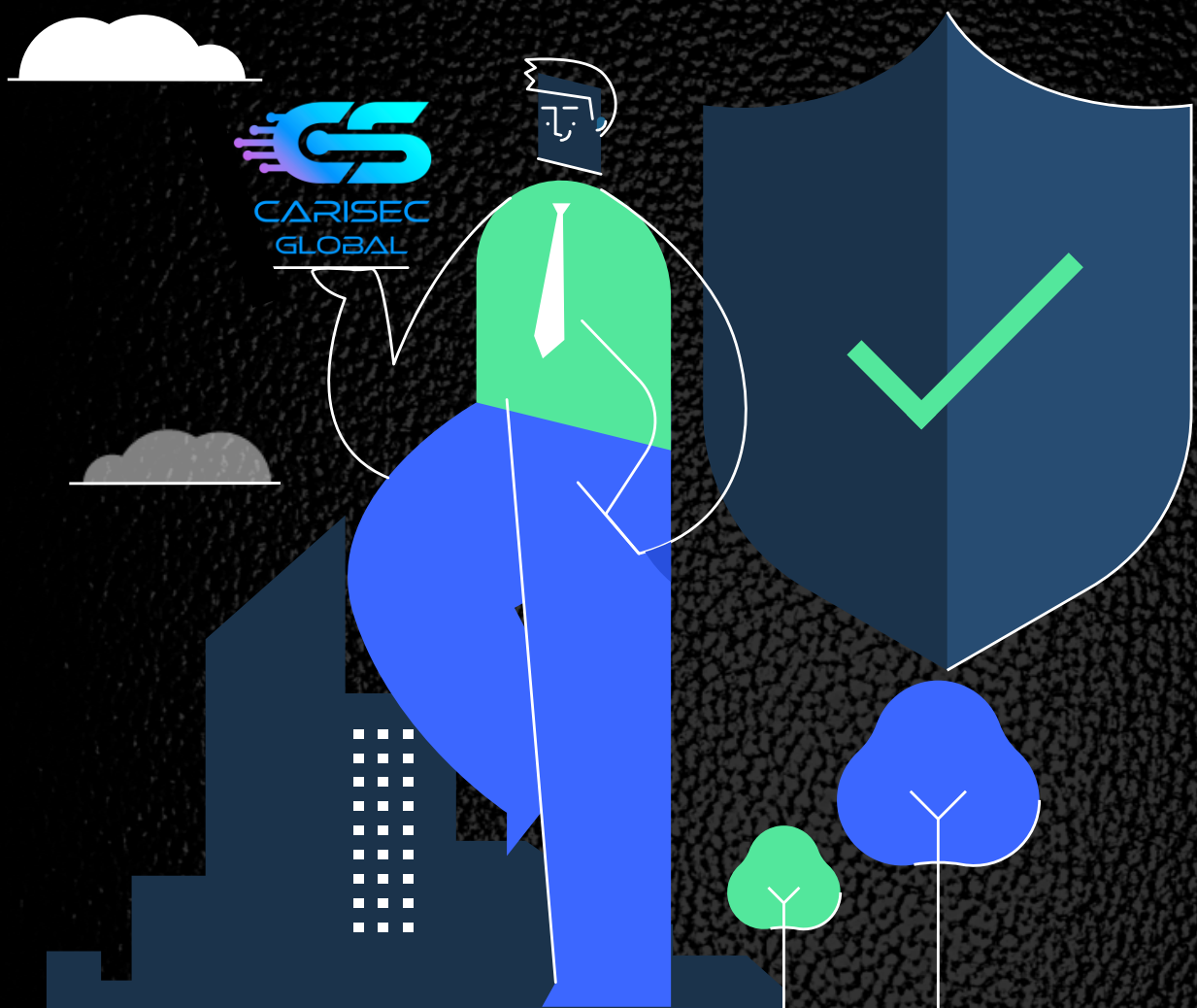
In many instances, the inability to identify, detect, protect, respond, and recover can also imply the inadequacies of the plan, where Threat Intelligence usage may be limited and network visibility is lacking due to insignificant data gathering throughout all aspects of the organization, inefficient threat hunting tools, and unskilled resource teams.

The capability maturity model of the Information Security Governance Program is critical in the operation and defense against an attack and it is therefore very important that the organization keep it alive as new risks arise.



# CariSec Global

Your Partner  
For Cyber Security



CariSec Global Creates Partnerships in the Development of  
Organizations Information Security and ICT Programs.

<https://carisec.global>



# EDWARD MILLINGTON, BARBADOS

A portrait of Edward Millington, a man with short dark hair, a mustache, and glasses, wearing a dark suit, blue shirt, and patterned tie. He is looking directly at the camera with a slight smile. The background is a dark blue with a subtle geometric pattern.

**Edward MILLINGTON**, (BSc, CISSP, ISSA, MCIIS, MIET, PAN-ACE) is the Founder and Managing Director of CariSec Global Inc., a Caribbean (Barbados) based company, strategically focused in providing Security & ICT Governance and Services to organisations operating in the following sectors: financial, government, health, manufacturing, private, retail, and energy and utilities.

He is an Information Systems Security/ICT/Telecommunications Veteran of 21yrs, where he directed organisations, leading them in the achievement of further financial goals through strategic planning, designing, and solutions direction. His specialties are in Policy Development, IT & Security Governance, Information & Cyber Security Risk Management, Enterprise Defense & Security, Cybersecurity Incident Management, Malware & Attack Technologies and Security Operations. His complex skills, knowledge and experience assisted many organisations such as Internet Services Providers, ICT Service Providers, Telcos, Banking, Government, and Governmental Organisations in their development and services evolution. One key highlight of his veteran career was his instrumental service to the Government of Barbados, developing and enhancing its Information and Cyber Security posture.

As a Cybersecurity Awareness Advocate, he has been advocating for True XDR and Zero-trust implementations to organisations since 2018, encouraging them to continue the advancement and development in Security Engineering, thereby enhancing Defense & Security in the identification, detection, protection, responding and recovery from Cyber threats and attacks, and Malicious Insider Activities and in 2021, as an active member and promoter of the Chartered Institute of Information Security (CIISec), led international Masterclasses with Palo Alto Networks on such subject matters. He is also heavily in the promotion of Information Security Governance to organisations with a focus in Governance, Risk & Compliance (GRC).



# “PROTÉGÉ FOR WOMEN IN CYBERSECURITY”

by Pooja SHIMPI

***“Everybody Needs Somebody!”***

## **Global Mentoring for Cybersecurity Program**

Mentoring is one of the most important things a person can do, to enhance their career and professional life. It takes time and commitment, but it is well worth the effort. Whether you are the mentor or the mentee, it's a win-win for both. The opportunity to be both a mentor and a mentee, provides an invaluable retro and forward perspective experience.

The world of cybersecurity is on the move, and with the start of 2022 it's moving faster than ever. Cyber criminals are getting progressively sophisticated in their cyber-attacks, making it imperative for organizations to beef up their defences. Needless to state, there is a supply-demand gap in terms of the need for cybersecurity professionals, to the tune of approximately 2.7 million worldwide.

Many countries and organizations have a roadmap to increase skilled staffing but is it enough? It's been proven that gender diversity in any field results in higher productivity and better profits. While the number of women is gradually increasing in this niche space of Information Security, are we firing up all cylinders to encourage more women to join the cybersecurity work force?

Do you have any self – doubts, such as

***“How can I get into cybersecurity?”***

***“What can I do to make the internet a safer place?”***

***“Why can't I have a career in cybersecurity?”*** ***“When would be the right time to enter cybersecurity?”***

If these thoughts ever crossed your mind, you are not alone!

Many individuals, think of this and are missing a great opportunity to join the cybersecurity field. The **Global Mentorship for Cybersecurity (GMFC)** program is established by Pooja Shimpi in partnership with Cyber Risk Meetup group in February 2022 with the **mission** to bring together highly skilled cybersecurity professionals from diverse background as mentors, along with individual enthusiasts (as mentees) who want to join / grow in the cybersecurity field, from all over the world.

This is a 6 weeks guided program and there is no fee to participate in the program for any participants. The efforts are in place to establish a strong mentor-mentee partnership with a goal to uplift and guide the mentees to meet their cybersecurity related goals. **The overall aim of this program is to help bridge the gap of cybersecurity workforce talent.**

We have received an overwhelming response, and with laser-focused diversity & inclusion approach we have successfully enrolled 39 individuals in our 1st GMFC cohort, The participants are from 9 countries and 19 different cities with a whopping 51% women representation. Out of total 20 women who are participating, 13 are mentees and 7 mentors. Most of the mentees are freshers or experienced professionals with no or few months/years of experience in Cybersecurity field. All the mentors are united by one common goal, i.e., to share knowledge, provide the right guidance & spark passion among the mentees for the ever-changing world of cybersecurity. The mentors come from diverse cybersecurity backgrounds, carrying a balanced combo of cybersecurity knowledge and expertise and required skills to guide the



mentees in correct direction to achieve their goals to break in or grow in cybersecurity industry.

While there is no silver bullet, a good mentorship program & volunteering by leading experts in cybersecurity can be the simple solution that we are looking for. Additionally, it can help address the huge supply-demand gap in cybersecurity workforce. While many organizations are struggling to improve their overall gender diversity, their Human Resources team could start focusing on returning women, as one of the key levers for their hiring. This way they would end up hiring not just a rejuvenated woman who is eager to join the workforce, but also someone who is more motivated, has obtained a fresh perspective, and eager to perform.

Mentorship can also help bust several myths, such as:

- You need to be very technical to join cybersecurity
- Cybersecurity is a very stressful field
- Certification/cybersecurity course will help you secure a high paying job immediately
- Previous experience will be devalued

***“Life’s most persistent and urgent question is “What are you doing for others?”- Dr. Martin Luther King Jr.***

### ***“Protégé for Women in Cybersecurity”***

In Cybersecurity field, the % of women applying for cybersecurity roles is incredibly low and 25% of women representation in Cybersecurity field is not impressive.

***Women need examples of other successful women role models or influencers in “sustained and upward trending” leadership roles to be able to visualize themselves in one.*** Hence, Pooja Shimpi has started an initiative ***“Protégé for Women in Cybersecurity”***, where she publishes Inspirational stories of amazing mentors and mentees across the globe in medium.

Cyber security is an evolving field and limited number of role models and female mentors, but this trend is changing and there is an encouraging sign that women are aspiring for doing higher studies in Cyber security. With this initiative, the young female enthusiast is getting inspiration through the interviews from those talented women role models who are making in the top or on the pathway of breaking the ceiling! In their interview, the mentors provide a great knowledge about Cybersecurity field, their journey, challenges they have faced and guidance to mentees along with best resources to refer to break in Cybersecurity field.

Check her medium.com blogs ***“Protégé for Cybersecurity”*** for the amazing stories from the cybersecurity leaders and young professionals. Participate and share your mentorship in Cybersecurity story through this initiative and it will have an amplifying effect inspiring other.

***It’s time to pay it forward...***





A portrait of Pooja Shimpi, a woman with long, wavy brown hair, smiling at the camera. She is wearing a dark blue top and a small earring. The background is a solid purple color.

## POOJA SHIMPI, SINGAPORE

Based out of Singapore, **Pooja SHIMPI** is a passionate Information & Cybersecurity enthusiast, influencer and advocate. She has 14 years of experience with reputed international banks. She holds Masters in Computer Science degree along with CISSP certification.

Pooja has expertise in driving various initiatives across multiple domains of Information Security and Technology Governance, Risks & Compliance (GRC). Her current focus is on enhancing information security policy & frameworks, management of regulatory requirements, cyber security education and awareness trainings, Application risk assessments and more. She has been featured in various cybersecurity related topics panel discussions, and her articles/interview has been published in magazines and in Cyber Security Observatory – APAC series. She is also actively involved in Global Inclusion & Diversity Programs, mentoring initiatives.

Cybersecurity is rapidly growing field and to keep up with it, is the biggest challenge. However, Pooja believes in challenging herself and participate actively in webinars, various events to gain and share knowledge. She is also involved actively in various global inclusion and diversity initiatives, She is a co-chair of Professional Women's Network in her organization, she is collaborating with ISC2 Singapore chapter to develop and implement ISC2 Singapore mentorship program for cybersecurity 2022.



# VCISO LEVERAGES INFLUENCE TO FILL CYBER SECURITY TALENT GAP

by Mike MILLER

***“Give me someone who has the right attitude, behavior, and communication skills who knows how to learn and wants to learn...”*** ~ Gerald Chertavian, founder and CEO of Year Up

The demand to fill the cyber security gap is stronger than anytime in history. Over the past couple years we have seen spikes in ransomware and breaches in general. Companies are starting to understand the need for 24/7 monitoring of their digital infrastructure. This causes much demand for security analysts. Security analysts are professionals that typically work in a SOC (Security Operations Center). Their job is to look for threats and monitor anomalies that could potentially be an intrusion. They monitor everything that comes in and out of the networks they are protecting. With nearly 50 billion devices connected to the internet, there are many empty seats that aren't being filled. The demand is too high.

There is no blueprint to become a security analyst. They can be trained via bootcamps or college. They can even be self-taught. Much of the demand is specifically in the blue team (defensive security) area.

Cyber Security is a unique field. There is no specific degree needed. Although there are many large certification organizations out there making huge profit on classes and “certifying” students, this field is still very welcoming to those without the certs. It takes communication skills, ambition, self-confidence and the willing to dive in and learn. Fortunately, due to the power of the internet, all the information is out there to learn.

It can certainly be overwhelming. Aspiring Cyber Security enthusiasts just need pointed in the right direction.

At a low level, Security Analysts need to have a good understanding of how network packets travel across the internet. With every piece of communication, such as when a website is visited, there is a network packet that goes across the wire. Inside each packet is a breakdown of what is being communicated. For example, when someone visits a website, packets are created that tell who the source of the traffic is coming from as well as it's destination. Inside the packet it will also have much deeper information such as what is being requested. Much can be determined from analyzing packets.



For example, these packets can be analyzed to generate alerts if something is “out of the ordinary”. An example would be a heavy amount of traffic at an organization at 3am when no one is at the office or working. This could be a possible flag that something is happening that shouldn't be. Network packets tell a story from beginning to end and a good security analyst will be able to read and analyze that story to see if it aligns with the organization.



A clear message needs to be made to HR and Recruiters on hiring for these positions. Candidates are passing over jobs every day because job descriptions are vague. They mention certifications that are “necessary” when the company will knowingly hire candidates without certifications. Entry level job descriptions mention 6 to 8 years of experience. Recruiters and HR need to be very clear and specific about what the requirements are. Many recruiters and HR departments put their “wishlist” in job descriptions. Even though these may be wishlists, candidates think they are requirements and are passing up on the opportunities. In turn companies are paying top dollar to recruiters to help fill positions that could have been filled easier.

Another reason for the gap in Cyber Security is due to companies still not being willing to allow employees to work from home. As we have seen over the past year, employees are refusing to come back to work. We are still seeing the “Great Resignation” and companies are being forced to change their habits. Although many companies have changed their stance, there are still many that are not willing to allow remote work. Unfortunately, this reduces the talent pool for them and makes it hard to fill positions.



Great candidates are willing to work hard to fill positions. In order for the gap to close, companies need to step back and take a 30,000 foot view to realize why they are not able to fill these positions. Are they compensating enough on salary? Are they providing a culture that attracts people to spend 8 hours of their day at? Are they providing opportunities within?

Jobs are out there that need filled.  
Candidates are ready to work. Let's work  
together to fill the gap.



Nearly 7 months ago I decided go “all in” and be proactive to help fill the security gap. With a mere 700 followers on LinkedIn, I put myself out there to give any advice could for people aspiring to be Cyber Security professionals. Not knowing where it would take me, I was shocked on the response that I have received. Since then my following has grown to nearly 15,000 and my posts have reached millions.

For those aspiring to get into defensive security with the goal of working in a SOC, I have laid out some direction. I talk low level and talk about tools and techniques of how one can learn on their own. I have advised them on how to create their own labs. I even have one on one conversations with candidates to help them understand packet analysis and the basics of what they need to know to land their first gig.

Not only should a security analyst be technical, they should also have great soft skills. Communication is key. They must be able to speak in a language to stakeholders in a non-technical language so that it can be understood. They must have drive and ambition.

The end goal is to prepare security analysts with the soft skills and technical skills needed to secure a role to help fill the Cyber Security Gap. Will this happen fast enough? Only time will tell.



A portrait of Mike Miller, a man with short brown hair and a beard, wearing a light blue blazer over a pink shirt. He is looking directly at the camera with a slight smile. The background is dark with glowing blue and white geometric lines, suggesting a tech or cyber theme.

## MIKE MILLER, THE USA

**Mike MILLER** - vCISO, has over 25 years experience in IT/Security. Mike is a rare breed of expert, possessing not only technical skills, but great communication skills and an entrepreneurial mindset that allows him to "think like the business". In addition to being an excellent liaison between technical teams and stakeholders, his skill set has helped him strategize security programs that are perfectly aligned with the business. His experience includes defensive security performing intrusion detection. On the offensive side, he has performed penetration testing for some of the nation's largest retailers. He has also worked in the payment card industry performing PCI audits as well as working with some of the nation's pipeline companies to help conform with compliance.

Mike founded Cyber Protection Group over 12 years ago which was recently acquired by Appalachia Technologies. As an influencer in the Cyber Security space, Mike has a large following on LinkedIn and uses it to mentor people aspiring to get into the security space. Because of the demand in the field of Cyber Security, his posts have reached millions of views.



We provide consultancy-led **Influencer Marketing & Employee Advocacy software** that enables brands to implement and run structured Influencer Relationship Management programs with large Influencer communities to **improve brand awareness, perception and demand generation**. We are the most experienced technology platform & agency having **run 5,000+ social influencer advocacy programs** in B2B for global clients including AWS, Microsoft, Dell, EY, Ericsson, Siemens.

## WHY INFLUENCER MARKETING FOR B2B?

- » **Trust:** 77% of B2B marketers believe that prospective customers rely on advice from industry experts.
- » **Experience:** 74% agree that influencer marketing improves customer & prospect experience with the brand.
- » **Performance:** 63% say their marketing would have better results if it included a B2B influencer marketing program.







*Influencer-Generated Content outperforms Traditional Brand-Generated Content and generates up to **30 x Awareness & Engagement** and up to **5 x Demand Generation**.*

## 5-STEP APPROACH

- 1 DISCOVER** Identify the community of influencers & experts on topics that matter most to your brand, industry and target audiences.
- 2 INSIGHTS** Benchmark your brand's awareness & engagement with the influencer community vs. competitors.
- 3 ACTIVATION** Engage influencer community through organic & paid activation to create Influencer-Generated-Content.
- 4 MANAGEMENT** Continuously interact and develop relationships at scale with your influencer community.
- 5 MEASUREMENT** Measure the impact of your influencer marketing program against business outcomes & track your performance compared to your competitors.

## SOLUTIONS

-  **ENTERPRISE SAAS PLATFORM** We provide a SaaS platform to discover the right influencers, validate, categorise and track them over time to spot engagement opportunities.
-  **DATA** We mine 200 Billion social media posts per year and have a curated database of 1+ Million influencers across 500 topical communities.
-  **ELEARNING** We provide eLearning for Subject Matter Experts to grow their influence online.
-  **PLAYBOOK** Industry-leading frameworks for all use cases to guarantee impactful results.



*Sure, you could try to do influencer marketing on your own, but working with the right partner and technology allows you to access a plethora of data and deeper insight that will help you identify the best influencer for your brand. **Analytica is one of the established leaders in the field.***

**Neal Schaeffer**  
*Author of 'The Age of Influence'*





*Enables brands to tell inspiring stories by activating employees & influencers on social*

analytica 

## USE CASES

### INFLUENCER MARKETING

Leverage influencers to create thought leadership content for campaigns & events as part of a continuous program

Build & develop your Execs' social media presence

### EXEC COMMS

### VIRTUAL EVENTS

Leverage influencers to create content, drive registrations and increase awareness & engagement

Connect your internal Subject Matter Experts with influencers to co-create content on social

### EMPLOYEE ADVOCACY

### CONTENT MARKETING

Create high quality Influencer-Generated-Content that performs better than brand content & reaches the right audiences

Identify which influencers influence government & policy makers, and engage them to influence the key decision-makers

### GOVT / EXTERNAL AFFAIRS

### ABM & SOCIAL SELLING

Enable your marketing & sales team to share Influencer-Generated-Content with target accounts

Track Analysts alongside your social influencers to understand who is influencing the debate and your end customer

### ANALYST RELATIONS

### PUBLIC RELATIONS

Track Journalists to understand who is most influential and how you can best drive earned media attention

## MYONALYTICA

MyAnalytica is the world's **largest B2B influencer marketplace**, designed to make brand and influencer partnerships easy. Brands can easily find topically relevant influencers that are ready to collaborate and the best match to drive successful partnerships.

## KEY BENEFITS

- » Enables brands to easily find relevant Analytica verified influencers that are opted-in, open and ready to collaborate with brands.
- » Provides unique insights on social media performance compared to industry benchmarks.
- » Showcases Influencers' expertise, influence & preference on how they would like to partner with brands – in their own words.
- » Streamlines influencer management with an integrated payments system & contract templates.

*"Achieve your Marketing & Comms objectives through a combination of Analytica's software, professional services and best practice guides, tips and templates."* **Team Analytica**

analytica 



# TOP CYBER NEWS MAGAZINE

BRING TECHNOLOGY TO THE FRONT OF THE BUSINESS

---

Human Centered Communication Of  
Technology, Innovation, and Cybersecurity



*«The individual Cyber Security professionals that the magazine celebrates are all of the Heroes whose Time + Talent + Treasure were brought to bear to bridge the divide between the future-history and today.»*

**Stewart A. SKOMRA**, Chief Executive Officer at OmniQuest



*«Ludmila Morozova-Buss editor in chief Top Cyber News MAGAZINE - a phenomenal bridge builder in the cyber world. Communicating #technology #Innovation & #cybersecurity is no small feat! especially when it is done with class and pizzazz - Ludmila style!»*

**Margo KONIUSZEWSKI**, President at The Bridge Foundation



*«I read your articles and I am first impressed by the sophistication and sense of weightlessness with which you describe some complicated scientific and technical concepts, imparting an understanding of complex ideas with simplicity and clarity. Elegance and artistry is indeed a rare combination in writing on science and technology. You present a balanced view of the issues and competing priorities while elucidating a 360-degree strategic change agenda. Respect!»*

**Scott SCHOBBER**, Chief Executive Officer at Berkeley Varitronics Systems



# TOP CYBER NEWS MAGAZINE

Human Centered Communication Of Technology, Innovation, and Cybersecurity



“MISSION IMPOSSIBLE”: TO WIN YOUR HEARTS!

**Ludmila Morozova-Buss**

Doctoral Student at  
**Capitol Technology University**  
Editor-In-Chief

## TOP CYBER NEWS MAGAZINE