Oracle

FACULTY OF COMPUTING - MONTHLY BULLETIN

NSBM GREEN UNIVERSITY TOWN

MARCH 2026

DIGITAL TRANSFORMATION AND CYBERSECURITY: ARE WE PREPARED?

INSIGHTS FROM GLOBAL CYBERSECURITY LEADER MR. MADU RATHNAYAKE

SCYBERS

MR. MADU RATHNAYAKE

President and Co-Founder *- Scybers, a Global Cybersecurity Firm &*
Former Chief Information Officer *- Virtusa Pvt Ltd*

In a world where cyber threats evolve faster than most of us can keep up, there are a few individuals working quietly behind the scenes: anticipating risks, building defenses, and shaping the very architecture of digital safety on a global scale. Mr. Madu Rathnayake is one such figure. A global cybersecurity leader, and the President and cofounder of Scybers, a prestigious global cybersecurity firm, whose work spans industries, borders, and some of the most complex digital environments in the world, he brings with him not only decades of experience, but also a rare ability to translate complexity into clarity. In this conversation, we step slightly outside the technical comfort zone, asking the questions many of us are quietly thinking, and uncover what cybersecurity really means in today's rapidly shifting, AI-driven world.

Oracle
FACULTY OF COMPUTING - MONTHLY BULLETIN
NSBM GREEN UNIVERSITY TOWN
MARCH 2026

Q1: WE UNDERSTAND THAT YOU ARE QUITE THE GLOBE TROTTER, PROVIDING CYBER SECURITY SOLUTIONS GLOBALLY. WE WOULD LOVE TO HEAR ABOUT YOUR JOURNEY, AND HOW YOU CAME TO BE THIS AMAZING EXPERT IN THE FIELD?

A: I've been in technology from the very beginning of my career. I spent over 25 years at Virtusa, where we grew the company from a small operation into a global organization with around 32,000 employees across 19 countries, generating over a billion dollars in revenue.

During that time, we worked with some of the world's leading enterprises including global banks and telecommunications companies. One thing that became very clear, cybersecurity was never an afterthought. It was central to everything we built.

I led the security practice at Virtusa, where we focused on building secure systems by design. That exposure to global best practices really shaped my understanding of how critical cybersecurity is for modern businesses.

About four and a half years ago, we founded Scybers with a specific purpose: to bring enterprise-grade cybersecurity to mid-market organizations that don't have the resources to build large in-house security teams. Today, we work globally, helping organizations secure their digital environments through an expert led managed service model powered by AI.

Q2: WHAT WOULD YOU SAY WAS YOUR MOST INTERESTING/INNOVATIVE CYBER SECURITY SOLUTION TO DATE?

A: One of the most interesting areas we are currently working on is an AI-assisted security strategy and operations platform called Scyra.

Organizations today face a "perfect storm"; rapid digitalization, increasing cyber threats, stricter regulatory requirements, and a shortage of skilled security professionals. Traditional approaches simply cannot keep up.

Scyra addresses this by combining AI with human expertise. It can analyze threat signals in seconds, perform initial assessments, and present insights to experts for decision-making. This significantly reduces the manual workload and improves speed of security.

This is a fundamentally new paradigm of service delivery "service as software." Instead of customers managing multiple tools, we deliver outcomes; complete cybersecurity services powered by both AI and expertise. This approach simplifies security for our customers while improving speed and effectiveness.

Q3: TODAY, EVERYONE USES THE INTERNET DAILY – FOR THE MOST MUNDANE THINGS, PLEASE TELL US, LAY PEOPLE, WHY SHOULD CYBERSECURITY BE SOMETHING EVERY INDIVIDUAL SHOULD CARE ABOUT?

A: Cybersecurity is no longer just a business concern, it affects everyone.

With the rise of AI, cyberattacks have become more sophisticated, fast and scalable. For example, deepfakes can now convincingly mimic voices or identities, making it easier to deceive individuals.

What's important to understand is that cybercrime operates like a full-fledged industry. Attackers are organized, well-funded, high sophisticated, and constantly evolving.

Even individuals who are not "tech-savvy" are potential targets. That's why awareness is crucial. Being cautious about what you share, verifying requests, and understanding basic risks can make a significant difference.

Q4: IF YOU HAD TO IDENTIFY ONE CYBERSECURITY HABIT THAT EVERY INDIVIDUAL SHOULD ADOPT IMMEDIATELY, WHAT WOULD IT BE?

A: If I had to highlight one thing, it would be protecting your identity.
In a digital world, your identity, your login credentials, personal data, and online presence; essentially unlock everything you own.

Simple practices such as safeguarding passwords, being mindful of what you share online, and verifying communications are fundamental. If your identity is compromised, everything else becomes vulnerable.

Q5: IMAGINE THIS: A MAJOR ORGANIZATION IN SRI LANKA HAS JUST EXPERIENCED A CYBERATTACK OVERNIGHT. SYSTEMS ARE COMPROMISED; DATA MAY BE AT RISK. WHAT ARE THE FIRST FEW STEPS THAT TAKE PLACE BEHIND THE SCENES IN SUCH A SITUATION?

A: The first priority is always damage control.

This involves isolating affected systems, shutting down non-essential components, and preventing the attack from spreading.

Next comes investigation, identifying whether attackers are still present, conducting forensic analysis, and bringing in experts to respond effectively.

Forward thinking organizations today adopt an "assume breach" mindset. Instead of asking if an attack will happen, they prepare for when it will happen. This includes having incident response teams ready in advance, which is critical during high-pressure situations.

Q6: AS SRI LANKA CONTINUES TO DIGITIZE ACROSS SECTORS, WHAT DO YOU SEE AS THE MOST PRESSING CYBERSECURITY VULNERABILITIES OR RISKS FACING THE COUNTRY TODAY?

A: Interestingly, most cyberattacks don't occur due to highly sophisticated techniques—they happen because of poor cyber hygiene.

Basic practices such as strong passwords, two-factor authentication, data encryption, and regular backups are often neglected. Yet these simple measures could prevent the majority of attacks.

Attackers typically look for the easiest target. If systems are well-protected at a basic level, they are more likely to move on to less secure targets.

For Sri Lanka, strengthening these foundational practices across organizations and institutions will be critical as digitalization accelerates.

Oracle
FACULTY OF COMPUTING - MONTHLY BULLETIN
NSBM GREEN UNIVERSITY TOWN
MARCH 2026

Q7: WITH THE RISE OF AI AND AUTOMATION, HOW IS THE NATURE OF CYBER THREATS CHANGING, AND HOW SHOULD ORGANIZATIONS ADAPT THEIR DEFENSE STRATEGIES? PLEASE TAKE US THROUGH THIS EVOLUTION.

A: AI has made both defense and attacks more powerful.

What we are seeing now is the shift towards agentic AI—systems that don't just provide information but can act on behalf of users. This increases efficiency but also introduces new risks.

Cyber attackers are using the same technologies to automate and scale their attacks. As a result, the speed and complexity of threats are increasing rapidly.

We are at a point where change is exponential. New developments emerge almost daily, and keeping up with this pace is one of the biggest challenges in cybersecurity today.

Q8: TO EFFECTIVELY DEFEND SYSTEMS, HOW IMPORTANT IS IT TO THINK LIKE AN ATTACKER/HACKER, AND HOW CAN STUDENTS BEGIN DEVELOPING THIS KIND OF MINDSET?

A: It is absolutely essential.
A key concept in cybersecurity is threat modelling, understanding who might attack you, how they might do it, and what vulnerabilities exist.

Professionals need to anticipate risks and design systems that can prevent, detect, and respond to those threats.
Beyond technical skills, this requires strategic thinking and judgment. While AI can assist with technical tasks, human insight remains critical in understanding risks and making decisions.

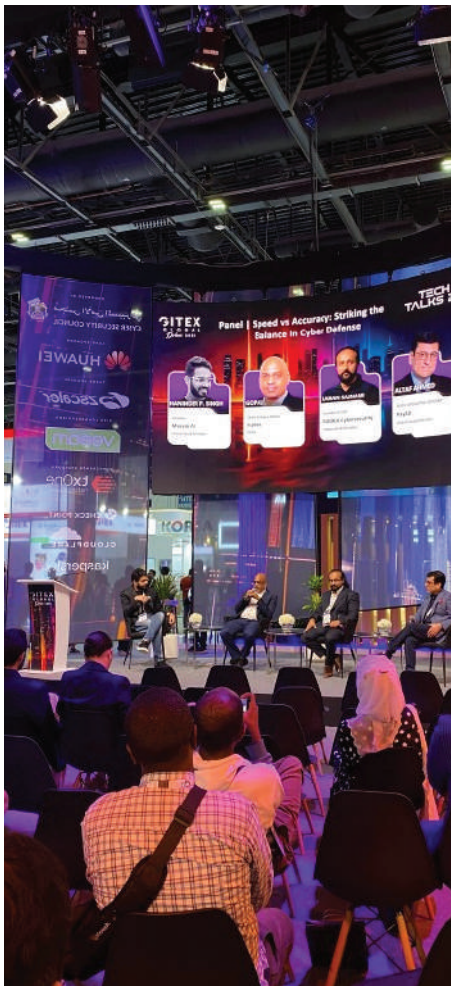
Q9: AS WE LOOK TO THE FUTURE, WHICH EMERGING TRENDS IN CYBERSECURITY DO YOU FIND MOST PROMISING, AND WHAT GUIDANCE WOULD YOU SHARE WITH STUDENTS PREPARING TO PURSUE CAREERS IN THIS FIELD?

A: Cybersecurity is an exciting and rapidly growing field with global demand.

However, students must focus on becoming AI-enabled professionals. Understanding how AI works, experimenting with tools, and staying updated with the latest developments are essential.

At the same time, strong engineering fundamentals are equally important. You need to understand systems, risks, and how technology works at a deeper level.

Ultimately, success in this field comes from combining technical knowledge, curiosity, and the ability to adapt to constant change.



INTERVIEWED AND COMPILED BY:
MS. NATASHYA CHAMBA
(LECTURER AT THE FACULTY OF COMPUTING)

LAYOUT DESIGN BY:
CHARITH LAKPRIYA
(STUDENT - BSC(HONS) COMPUTER SCIENCE, FACULTY OF COMPUTING)