The Daily Swig
Cybersecurity news and views

Simplicity should underpin enterprise security in a Covid-19 world: Magda Chelly surveys the global infosec landscape

Adam Bannister 14 July 2020 at 11:17 UTC
Updated: 14 July 2020 at 14:56 UTC

Coronavirus Vulnerabilities Education

Responsible Cyber co-founder will focus on education, communication, and more at this year's RSA Conference

Infosec recruitment flaws and adapting cybersecurity posture for a global pandemic are two notable topics being discussed at tomorrow's virtual RSA Conference.

These themes will be the focus of three talks from Magda Chelly, head of cyber risk consulting for Marsh Asia.

She is a certified CISO, on the advisory board for the Executive Summit of Black Hat Asia 2020, runs a popular YouTube channel focused on cybersecurity, and has won a string of accolades for being a cybersecurity influencer. Chelly is also the co-founder of Singapore-based security-as-a-service company Responsible Cyber.

Speaking to *The Daily Swig*, Chelly gives the inside track on her RSA presentations and reflects on the global disparities in cybersecurity maturity and the career opportunities open to female infosec professionals.

How did you get into cybersecurity?

I started being interested in cybersecurity when I was doing my PhD in telecoms engineering.

I evolved into an IT/CRM [customer relations management] consultant and even worked in sales and business development roles.

Since then I have had advisory roles [in cybersecurity], which have mostly evolved from governance to more technical cybersecurity – for example, cloud security with AWS, Microsoft Azure, Office 365 – to a more global approach when it comes to being a CISO.

That means building the whole cybersecurity strategy and rolling it out across one to three years, especially with regulated businesses like insurance.

Magda Chelly

Please tell us about your role at Marsh…

Latest Posts

France tops blue-chip cyber maturity index
The nation's largest public compar outperformed their peers

Ledger data breach impacts million users
Hardware wallet funds are 'safe', c reassures

WordPress plugin vulnerabil exposes 80,000 sites to rem takeover
Critical bug in wpDiscuz add-on ha been patched

Marsh Asia provides cyber risk consulting. It focuses on risk quantification, as companies are still facing challenges evaluating and quantifying cyber risks to find out the related financial losses.

Unlike other risks, there is limited historical data about cybercrime, mainly because it is a relatively new risk area, but also due to its constantly changing form.

Cyber risk management has not yet been ‘reduced to practice’ on a wide scale.

This approach enables point estimates of the financial cost – the severity – of cyber events with good accuracy.

YOU MIGHT ALSO LIKE Virtual cybersecurity conferences: An expanding list

Having credible quantitative estimates for both severity and likelihood will allow risk managers to answer the fundamental question: “What is the likelihood that our organization will experience a cyber event causing a loss of greater than, say, $100 million in the next 12 months?”

Most often, it is the likelihood question that derails many attempts at quantifying cyber risk, due to the unpredictable nature of a human-initiated threat.

So we’re talking dollars here – how data loss might happen, how much my business might lose, and how much I can get in terms of investment.

What can RSA Conference attendees expect to hear about ‘Getting the Security and Flexibility Balance Right in a Covid-19 World’?

I’ll be addressing how to be aware of the evolving risks within an uncertain environment.

And I’ll be [urging attendees to make] simplicity [a pillar of their cybersecurity approach] because fundamentals can be applied. You can, for example, apply your NIST compliance checklist every time a risk changes. I will be talking about alternatives.

I will be presenting about use cases and some additional changes that are super interesting.

I believe that cybersecurity professionals tend to be over confident about their capabilities.

We’re talking about an environment with a lot of factors that might impact our security. We’re not talking about traditional corporate security and enterprise boundaries. We cannot take the same approach.

RELATED How to become a CISO – Your guide to climbing to the top of the enterprise security ladder

If you go into an employee’s ecosystem and you understand how they work, you realize that they will find a way to [surmount] technical challenges by using their personal emails, etc, so that of course raises additional risks. And working in a quarantine environment raises risks that were not considered.

And the fact that some [employees] will go back to the office, some will stay working remotely – how do you manage that securely?

Cybersecurity professionals also have a challenge communicating with employees, who [sometimes] do not even know that there is a [security] team.

We tend to make employees feel that we are not reachable. If you’re a CISO of a big company then, obviously, you’re very busy. You have a team and you cannot spare time to talk to everyone, but it’s extremely important to go beyond just sending a newsletter and make sure that employees see cybersecurity as part of the culture.

So don’t talk about only corporate requirements. Talk about how they need to consider cybersecurity in everyday activities – no matter if it’s a corporate requirement or not.

This year's RSA Conference is taking place virtually

And what about your other talk: 'Hacking the Cybersecurity Job Market: A Primer for Students and Grads'?

This is about helping the student understand the different [available] career paths.

We hear about a big skills gap globally. Sometimes [this is exacerbated by] the fact that HR will request everything and anything in the job description. From a hacker to a compliance manager, to a CISO, [all skills and experience] is put in one job description, which is of course impossible. [Or they ask for] someone junior, but already with experience, so it just doesn't make sense.

So [I will talk about] finding the right balance, and how to address the challenges and start the discussions with HR teams.

How does Singapore, or Asia more widely, compare to Europe or North America in terms of its cybersecurity maturity?

I would say it's very different. The Asian market is very fragmented. Every country has different maturity, different initiatives, and different – especially regulatory – requirements.

Singapore is one of the most mature in terms of regulations – we have the PDPA privacy law, the Cybersecurity Act, the MAS TRM guidelines.

In countries where maturity is much lower, companies just do not feel that they need to do anything [to strengthen cybersecurity].

The Asian market compared to Europe or the US is still much, much lower in terms of general maturity, which means, again, there is a greater opportunity to help those companies.

You founded the Singapore chapter of Women of Security, or WoSEC. How would you summarize the chapter's aims?

I'm trying to help female professionals get the right support, to give them a safe environment with talks, workshops, social gatherings where we can talk about challenges, we can give some job opportunities, and recommend mentors.

How much progress are you seeing in terms of achieving parity of opportunity between female and male professionals?

I think there are a lot of unconscious biases, but it is changing.

I've seen a very positive change in the US and Europe. Asia is still trying its best but it's not there yet. There's a lot of work to do.

Companies like Marsh have diversity programs, and they are supporting WoSEC, so the problem is not there as such.

But general feedback from the top of other companies in the region [suggests that] the problem is that the HR process doesn't [encourage] that inclusion or diversity very well. And then unconscious biases don't help female professionals [once they do get roles].

It really depends on the country and the culture.

Finally, you noted that cybersecurity is often seen as exclusively the domain of IT teams. Experts also often feel that cybersecurity's status as a cost center devalues its importance. Are attitudes improving in the boardroom?

Small and medium-sized enterprises are generally focused on increasing sales.

They still lack awareness around cyber risk and do not consider it as a business risk. So they try to get it outsourced. But they are ignorant of the risks that they are exposed to, because the IT or managed service provider [might not be] doing anything about security because it's not in the contract. This is something I have seen in Singapore and abroad.

What mostly drives change is the regulatory requirement. We cannot just assume that a company will raise their understanding of cybersecurity just because then they are aware [of the problem] – unless the business owner is technologically savvy.

It needs a regulatory push. In Singapore, we have the Monetary Authority of Singapore technology guidelines, for example.

READ MORE Strategies for combating increased cyber threats tied to coronavirus

Coronavirus | Vulnerabilities | Education | Secure Development | Privacy | Legal | Singapore | Policy and Legislation | Industry News | Events | Telecommunications | Cloud Security | Compliance | Interviews | Organizations | US | Europe | Asia

Adam Bannister

@Ad_Nauseum74

Related stories

France tops blue-chip cybersecurity maturity index

The nation's largest public companies outperformed their peers

29 July 2020

Ledger data breach impacts one million users

Hardware wallet funds are 'safe', company reassures

29 July 2020

WordPress plugin vulnerability exposes 80,000 sites to remote takeover

29 July 2020

Promo.com data breach impacts 2

content creators

28 July 2020

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes

Vulnerabilities

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Customers

Organizations
Testers
Developers

Company

About
PortSwigger News
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research
The Daily Swig

PortSwig

Follow us