»DO WE NEED HEROES?«

Interview with SAP's Dr. Paul El Khoury on why successful cyber security is not an IT-game alone

FINSBURY

Do we need heroes?

FINSBURY

We discussed with Paul El Khoury why successful cyber security is not just an IT-game. Paul serves as the Head of Agile Secure Development for SAP and is convinced that managing cyber security is first and foremost a matter of having a corporate culture in place that makes teams work with each other, take responsibility and act within their roles. He thinks that when the whole company is 'in' on the topic, it doesn't require individual heroes.

Paul, thank you very much for taking the time for this conversation. Cyber security was once a niche topic in business and is now a mainstream concern – why is this?

We live in an era where cyberspace controls the physical space more than ever before. Everything is interconnected. Assets in cyberspace are not limited to digital assets anymore but are also physical assets that are accessible from cyberspace. If you want to make your assets secure in this interconnected world, you have to look across the whole chain of stakeholders and actors involved in the creation and management of them. This is a huge spectrum.

OK, so how can a company – everyone together – deliver on such a major responsibly?

Peter Drucker once said, "Culture eats strategy for breakfast." From my standpoint as a Security Officer, it is my responsibility to create a culture that protects business data, personal data, networks, etc. The only way to not let things fall through the cracks is to make security a habit, make it part of the value system, bring it into the culture!

Why is the 'together' aspect so important? Why is cyber security not the responsibility of the few, but of the whole organisation in your view?

When you look at the 'attack vector', you understand that basically every employee, every partner, every supplier, every developer – every single person that your organisation is in touch with could be part of the 'kill chain'. That is the series of steps that traces back to the actual exfiltration of data. This means any one of

those people could be a factor in how you might be attacked and how an attack might be contained. Security culture is the effort to mitigate attacks against the human factor.

Furthermore, a threat can come from anywhere and can spread very fast. And to react quickly and manage it properly, the entire chain of players involved in a company has to engage in a responsible and accountable way. The only way to make everyone aware of what needs to be done is to align what they want to achieve with the way they live and work. That's why creating a cyber security culture within a company is the most crucial but challenging part of cyber security.

From our work at Finsbury, we see that cyber security is often perceived as technical and complex – not exactly something that people will voluntarily engage with…

Right. My experience shows that cyber security is a topic that unfortunately triggers negative feelings. An example: I've reached out to people in the past and introduced myself by saying: "Hi I'm Paul and I work in cyber security". Reply: "Are you asking for resources or did I do something wrong?" This shows that the perception needs to change. We have to link security to something positive.

The technical and operational nature of the topic calls for a way to bring them to life. To establish a strong security culture, we need to align it with employees' personal values and needs.

»A threat can come from anywhere and can spread very fast. The only way to make everyone aware of what needs to be done is to align what they want to achieve with the way they live and work.«

In your experience, how is it possible to make a whole organisation 'cyber-ready'?

When I arrived in China in Feb 2017, my position as 'Chief Information Security Officer' was newly created within SAP for a geography. The role usually is tied to a product. The reason was that China was about to implement a CyberSecurity Law (CSL) and we wanted to reinforce the strategic function of security within the company.

How did you generate interest in cyber security within the organisation?

We teamed up with our security education department to create a Lego robot that broke down the topic from something very abstract into something playful that could be displayed in the canteen. It was called Mars Attack.

How did you keep people engaged beyond the initial visit to the canteen, and keep the momentum going?

With Mars Attack and its updates, we attracted talent and built skills. To retain the interest of colleagues, we had to move them further into practise. We trained and educated those colleagues who had expressed an interest in the canteen to become security experts and created the extra roles within the organisation of 'Multipliers' and 'Champions'.*

*'Multipliers' are site managers and managing directors whose awareness we raised and who pass the topic on to the organisation. Their focus is on headlines, so we created a regular compilation for them explaining the top 10 most relevant and interesting news items. **This way we reached people in the company we'd never reached with this topic before.**

'Champions' are developers who spend 80% of their time developing and who showed an interest in cyber security. We trained them on the topic and asked them to pass on what they had learned to the organisation. **We brought them together and created platforms to meet and exchange information like Cyber Month.**

And we used natural communication points to keep momentum. We established a global Cyber Month. In China, this aligned with the Government's cyber security promotion week. During this period, we rolled out events in all of SAP's locations in China, including hackathons, trainings in English and Chinese, mini courses on specific topics, e.g., on home security appliances but also more business related matters.

How was that received?

Very well. Half the company attended voluntarily! We spread it through the culture and through operations and then it spread by word of mouth...

How has top management received your initiative?

Their support has been key – it's prerequisite for a sustainable and comprehensive cyber security culture. By establishing my role as a dedicated Chief Information Security Officer for China, the Top Management showed that they were willing to go above and beyond. I've received an incredible amount of sponsorship and support from management: they recognised that security was a strategic topic for the company.

A programme like this also needs support from other key departments such as HR, Controlling and Finance. It's the actions of those at the top executive level that matter, not just words. And meanwhile the programmes have been implemented globally.

China is so much more digitally savvy than Germany, but then in Europe, people are more concerned about data protection...

China is the most digital country I've ever experienced. That might be why the CyberSecurity Law was implemented there so rigidly. I believe the law brought the subject to the attention of business decision-makers and made it a top priority. I think the COVID-19 outbreak has accelerated China's digital development even more.

Is there a region in the world that is leading the charge in terms of cyber security?

Compared to many countries, China has made a big leap forward, especially through the CyberSecurity Law. However, in terms of preparation, I see Germany leading, but in consistence with Europe as a whole, particularly with GDPR that regulates EU citizen's personal data. The United States is very solid on cyber security for Critical Information Infrastructure. Many of the guidelines on critical information infrastructure that China and Europe are now following have existed before in the US in some different shape or form.

China has a great talent for learning from everything that is out there and improving on it.

Generally speaking, what does a cyber security law regulate?

Let's take a fictitious example: in the 1980s we moved from paper to digital. Imagine a company taking all its records and digitizing them. Then Mr. X, a hacker,

comes and steals all the data documents. The police find Mr. X and accuse him of stealing the data but at the time Mr. X replies, "I didn't steal anything, I copied it. All the data is still there." At the time, due to a lack of cyber security regulations, there were no legal grounds to punish the person, because the copy concept wasn't in existence. In a world where stealing something that ceases to exist in one place and copying something as a criminal act are distinct, the legal system would benefit from an upgrade for the cyber space.

What is the relationship between law and business in implementing cyber security strategies?

In a country without strong regulation, cyber security will be less of a priority. There will be self-regulation between companies and their suppliers and customers on a voluntary or ad hoc basis. But when governments regulate, it goes beyond what individual companies do – there will be an outside compliance aspect that needs to be fulfilled.

Then there's the question of priorities – does compliance come first or security?

Compliance does not mean security. I think, companies will have to aim at being secure and as a result they become compliant. The moment they target compliance as a goal in and of itself, they are likely to focus the wrong way.

Security is deeply intertwined with trust: with reliability, accountability and responsibility. Trust is the ultimate currency, and that's what must be developed through culture.

How secure can a product ever actually be, and how can you ensure you're not behind the curve when it comes to product protection?

It's a very difficult question, but here's the short answer: will you ever be able to be 100% sure that you never have an accident on the road? Even if every driver is extra vigilant, cars are secure by design and default, such as having airbags, intelligent systems, etc. and your driving and handling is trained and skilled...?

I cannot imagine a technology that changes the digital environment and the core issues of security in such a way that will eliminate the need for cyber protection, that is to be prepared and ready to respond to any cyber security situation at all times.

So, you are saying that as long as there's illegal activity, the problem will not be solved?

Correct. And since we cannot mitigate the problem 100%, what can we do? The best practice is to respond professionally. Don't panic and know how to act. Have an incident response plan at hand that is excellent.

The incident response team has to be trained, and all procedures need to be in place. You don't need heroes, you just need people that can run your system in any circumstances. You need a culture that makes teams work with each other by taking responsibility and acting within their roles. The whole company needs to be in. It's the only way to contain the damage.

Is there an example of a company that handled it well?

It's hard to say, because anyone can be the target. And by pointing one company out, they – the hackers – want to prove you wrong.

It's hard for companies to fully recover from incidents and say they are untouched. There's a loss of reputation, even if you handle it well and professionally. It takes a thousand days to earn trust and one day to lose it.

What is a typical mistake in handling a cyber security situation?

To see it as a crisis.

But surely it is?

You have to be so well prepared that even an exceptional case is the norm. You need to treat it like a crisis, yes, but be ready for any situation, which triggers a well-defined and trained process.

You need a 'kill-chain' in place to defend the company's assets.

What's your crystal ball prophesy for the future? For the industry as a whole?

I'm thinking of three aspects here: Firstly, education. When I was studying at university, I was one of a few people who got a cyber security education. Today, I see universities making security a mandatory course. It's becoming a core skill. It's helpful to know a little bit about finance to understand how to deal with money. In today's digital world, you need to know how you deal with passwords.

The second aspect is cyber regulation. Ideally, laws are agreed upon before they are implemented, but this is not always the case, unfortunately. That puts multinational companies in a very challenging position.

The third trend is machine learning. We are going to outsource repetitive tasks in cyber security to machines and will work out what the human aspect of intelligence is and keep within our remit. That will make us better. But we have to consider that the tools are also available to the attackers.

Who's going to win?

I'm an optimistic person. I think with more awareness in organisations, better preparedness and a security culture, it will be more difficult for hackers to attack.

About Dr. Paul El Khoury

Dr. Paul El Khoury serves as the Head of Agile Secure Development for SAP, primarily focused on agility and secure cloud delivery. In this role, Paul drives the global team that reinforces SAP's security culture and leverages and adapts agile development by providing a secure by design software development lifecycle.

Until November of 2019, Paul served as SAP's first Chief Security Information Officer for SAP in China. During his tenure in Asia, Paul led the product security strategy across the different SAP Labs locations in China and also served as the technical advisor for all security topics related to SAP's businesses in the region.

Paul holds a Ph.D. in computer science from Claude Bernard University in Lyon, France. He is a certified information systems security professional and has authored various scientific publications and patents in the field of software security. He is currently based in SAP's Headquarters in Walldorf, Germany.

Cyber reputation: Empathy matters more than technology

How hacked companies can restore trust as well as data.

A DDoS attack cripples servers, hackers steal customers' data or sniff out sensitive corporate information – the scenarios for cyberattacks are menacing. With a strong shift to remote working during the COVID-19 outbreak, opportunities for hackers increased dramatically. Attacks are unfortunately a common part of everyday business life. According to Dell's Global Data Protection Index 2020, the majority of organisations worldwide suffered a disruptive event in the last 12 months (82% in 2019 compared to 76% in 2018). The front line of defense around the clock is IT security. However, it is not only IT systems and company data (the intellectual property) that are at risk, but also stakeholders' trust. They want to be sure the company has cyber risks under control and handles the data entrusted to it responsibly. That is what we call cyber reputation.

But no firewall can protect a company's reputation – communication is needed to defend it. If enterprises leave questions unanswered, take a poorly crafted response or become tangled up in legal pitfalls, even minor incidents could turn into a serious reputation crisis. That means the target of an attack can soon be perceived as a culprit who says nothing, covers up or makes false promises.

The first and foremost priority of the experts in charge is, understandably enough, to address operational issues regarding IT security. Yet good communication is just as important. And it is achieved not through technical explanations, but by focusing on the people affected and their worries, needs and fears – throughout all phases of the crisis.

The lifecycle of a cyber crisis

Recent cyber crises have shown that there are four phases in communications

The discovery phase begins when a company realises it has fallen prey to a cyberattack. In this phase, companies often focus on the incident's technical aspects, such as the question of how an external actor was able to access their systems. The focus is on identifying the vulnerability and closing the security gap as soon as possible. While understandable, this is often to the detriment of a timely communications response. Apart from asking "why did the incident happen and what can we do to prevent it?", the critical question should now be: "How do we protect the interests of our stakeholders in this situation?"

The disclosure phase brings with it the inevitable need to disclose that an incident has occurred and to actively

communicate with the affected parties. The focus now should be on the subjects of the breach, the concerns of employees, business partners and customers. It is crucial to mitigate stakeholders' fears as quickly as possible and to strengthen their confidence in the organisations' ability to effectively navigate the crisis. If that is not the case and stakeholders have the feeling that the company does not care about them, that will increase anxiety amongst those affected and their trust in the company will dwindle. Stakeholders need to understand and, most of all, see how the company is battling on their behalf and will act once the crisis is out of the limelight. Creating a sense of transparency and ability to support those affected should be accompanied by empathetic understanding and appreciation of the situation at hand. Saying too much too soon could cause unnecessary stress, but saying too little too late could be even more damaging. That is all the more important if third-parties engage, whether on-the-record or through social media, by giving their often uninformed, critical and hence reputationally damaging take on events.

In the live handling phase, IT is still working to resolve the problem, while communication has to control how the matter evolves further. Companies need to get ahead of the story and anticipate developments. They have to explain every single step and, in doing so, engage with the interests and wishes of their stakeholders. An unpleasant aspect of cyber crises is that those in charge typically have no relevant past experience to relate to in their decision-making process. Therefore, in order to avoid serious mistakes, the company's various divisions and outside experts must work together closely and in a spirit of trust. The communications team should be already planning for the period after the peak of the cyber crisis and initiate first steps in this phase.

The transition to the fourth and often longest lasting phase, reputation recovery, occurs naturally post any data accident situation. To restore stakeholder trust, the company must remain engaged and provide frequent information and updates to the affected individuals. In order to do this successfully, all stakeholder communication should always clearly outline all the measures that have been taken while reassuring stakeholders that protecting their interests will remain a priority longer term. Once more, the main emphasis here is not on the technology, but on empathy and accountability.

After the cyber crisis is before the cyber crisis

Anyone wishing to take proactive and preventive steps will stage cyber crisis workshops to develop a communications toolbox defining the management and decision-making processes, initial strategies and messages for various scenarios. That not only allows the communications team to prepare for a real-life incident mentally, but also organisationally. Such workshops also give the various corporate functions a controlled environment where they have the chance to test how well they co-operate. As a result, preventive crisis communication is transformed into active cyber reputation management for stormy times.

What makes cyber crises so special?

Compared to other crises, cyber crises have three special features that have a major impact on the communications strategy

The attackers and their objectives are typically only uncovered very late – and sometimes never at all. It may be the case that only the path (vector) used by the attacker to gain access to a system can be identified.

Even after a security gap is discovered, it is often difficult for companies to say reliably how much and which data has been compromised. Moreover, when the data involved is financial or represents sensitive personal information, it may cause major damage to those affected when in the hands of hostile actors – such data could range from medical results, credit card details to information allows for identity theft or social engineering. Needs to be 'allowing'.

Following introduction of the European General Data Protection Regulation, companies have to adapt to a situation where regulatory authorities and data protection officers will closely monitor their activities after cyber incidents. Serious misconduct may be punishable by fines running into the millions.

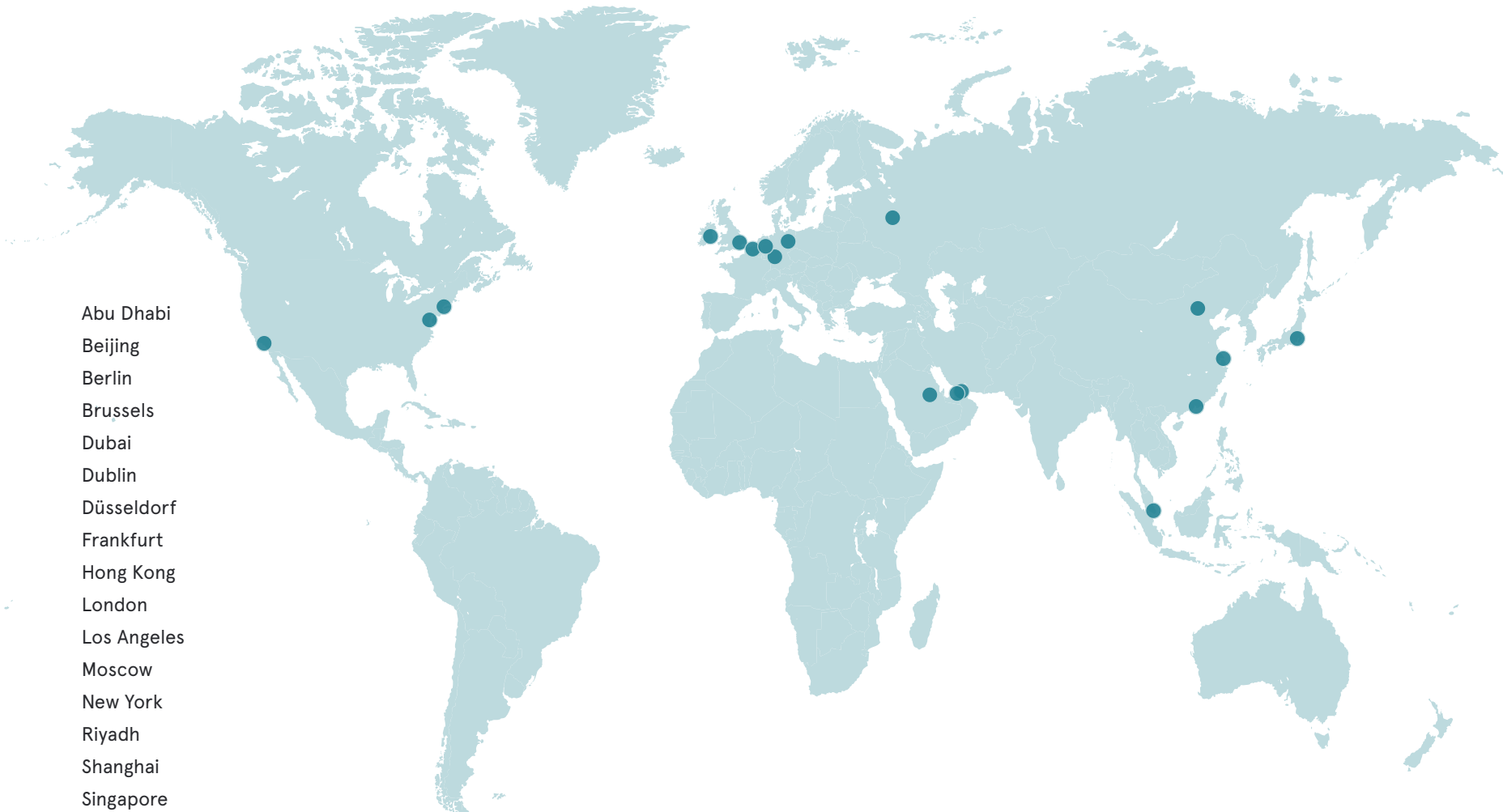
We believe that every crisis can become a test of a company's values, competence and leadership

That's why at Finsbury we take a values-led approach, one that helps ensures you put reputation at the heart of your decision-making, by appropriately leveraging your mission, vision and guiding principles while also considering the commercial, ethical and legal implications of your actions.

Finsbury's multi-disciplinary, global crisis team comprises former senior journalists, veterans of political service, lawyers, employee engagement, investor relations and social media specialists and industry experts with deep sectoral and cross-border expertise.

When a cyber crisis strikes, we will be by your side to help you to manage, lead and recover effectively. We listen to your challenges and have deep experience in anticipating how your stakeholders, the media and the regulatory environment will respond. We project manage, provide extra resources and critical thought to help you think beyond the 'now' and ensure priorities are clear when it matters most.

Global crisis team leads



Abu Dhabi
Beijing
Berlin
Brussels
Dubai
Dublin
Düsseldorf
Frankfurt
Hong Kong
London
Los Angeles
Moscow
New York
Riyadh
Shanghai
Singapore
Tokyo
Washington DC

Global cyber security team leads

Asia

Ben Richardson,
Partner, Hong Kong, Head of Asia
Ben.Richardson@Finsbury.com

Claudia Kosser,
Managing Director, Head of Shanghai
Claudia.Kosser@Finsbury.com

Germany

Dirk von Manikowsky,
Partner, Dusseldorf
dvonmanikowsky@heringschuppener.com

Tina Kunath,
Managing Director, Dusseldorf
tkunath@heringschuppener.com

United Kingdom

Jenny Davey,
Partner, London
Jenny.Davey@Finsbury.com

Meglena Petkova,
Managing Director, London
Meglena.Petkova@Finsbury.com

United States of America

Jeff McAndrews,
Partner, Los Angeles
Jeff.McAndrews@Finsbury.com

Michael Dolan,
Managing Director, New York
Michael.Dolan@Finsbury.com