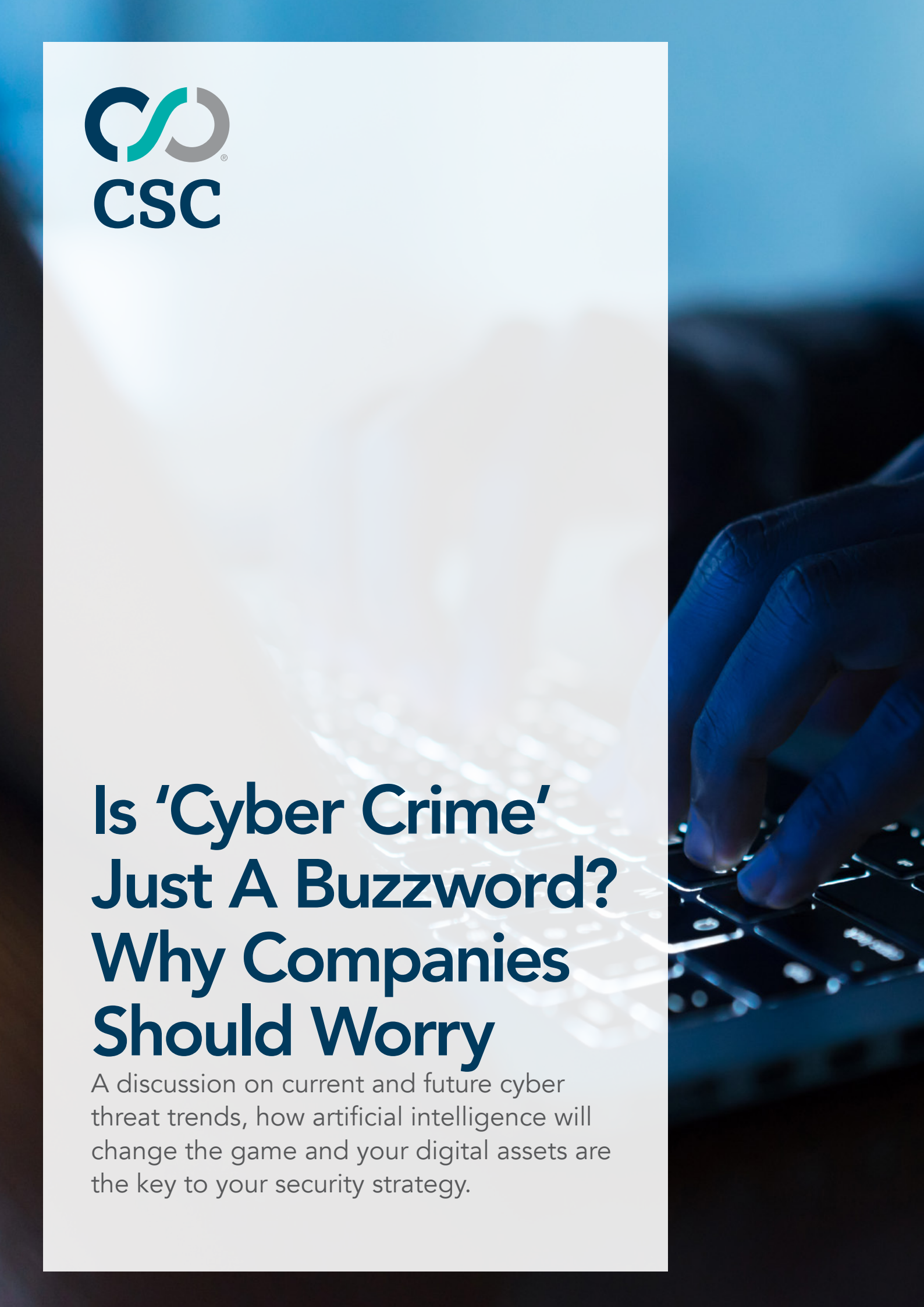

Is 'Cyber Crime' Just A Buzzword? Why Companies Should Worry

A discussion on current and future cyber threat trends, how artificial intelligence will change the game and your digital assets are the key to your security strategy.

Meet our Roundtable Panel

MARK FLEGG

Global Product Director, Domains and Security

At CSC®, Mark Flegg is responsible for advising a global client base on digital risk and the preventative measures brands can take to safeguard their digital assets. During his 16 year career, Mark has acquired a wealth of experience in cyber security technology focusing on domain management systems, domain name systems, secure sockets layer, and distributed denial of service protection software and mitigation.

SØREN BRANDBYGE

Infrastructure Engineer, Security Engineering at LEGO Group

Søren manages DNS cryptography systems for LEGO, and is part of a team building security solutions. His previous and concurrent experience includes being the appointed GTS representative for all DK research institutions, tasked with participation in building the research network; contributing to the DK-related OECD report on spam; co-authoring a PhD thesis, writing articles, lecturing, and building tools he releases to the public. He also writes articles about economics, math, physics, IT security, social politics, third-world development, ethics, and humor.

Søren has a variety of degrees, including an international master's degree in food engineering . He also holds a master's in information technology, with a specialty in multimedia production, from the University of Southern Denmark (SDU-Odense). He's currently working on his third master's in math.

Executive summary

Over the past few years, we've seen an uptick in articles, alerts, recommendations, and solutions for cyber crime. In the beginning of 2019, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the UK National Cyber Security Centre, and other leading security organizations issued an alert about domain name system (DNS) infrastructure hijacking campaigns. The Internet Corporation for Assigned Names and Numbers (ICANN) followed suit by alerting particular registries, registrars, and organisations of the heightened risk, and promoted domain name system security extensions (DNSSEC) as a way of mitigating the threat.

It only took a few days for the media around the world to pick it up. Other government agencies in Sweden, France, the United Kingdom, and more—as well as registries—issued notifications to their partners and clients, CSC included. The Danish Centre for Cybersecurity—a government agency—recently published their annual report threat assessment: The cyber threat to Denmark 2019. It looks at the current known forms of attacks, provides specific examples, and discusses the current level of risk, as well as future trends.

With all that happening in the first six months of 2019, we have to ask—what's really behind it? Is cyber crime just another buzzword, or should organizations around the world, and the public, really be worried?

Søren Brandbyge, infrastructure engineer for LEGO System A/S, expert, and thought leader in security, cryptography, and DNS joins CSC's Mark Flegg, global director for Security Services, to give us insight into these current events, what actions companies can take to secure their brands, and their views on current and future threat trends.

Index

In recent months, we've seen an increase in alerts from government agencies as well as the press all over the world regarding DNS hijacking threats. Can you give us a quick overview of what's going on?

Mark Flegg (MF): DNS hijacking isn't new. This form of attack has been ongoing for years. However, this form of cyber attack was previously predominantly used by hacktivists for political reasons. Now, that's changed. Over the past four years, DNS hijacking has been increasing and cyber criminals—rather than hacktivist—are becoming more and more active.

In January 2019, FireEye®, a security vendor, released its report on DNS hijacking campaigns. Around the same time, the U.S. Department of Homeland Security issued an emergency directive ordering all U.S. federal civilian agencies to secure the login credentials for their internet domain records. KrebsonSecurity, run by American investigative journalist, Brian Krebs, then reviewed all DNS hijacking findings on his blog—and coupled with the ICANN alert to its members of the domain name industry, registries, registrars, and resellers—global media outlets picked up the news.

In most countries, the media reinforced the alerts. In some cases, in particular in France, the alerts were misconstrued as a cyber attack on ICANN. Our French office received many calls in regards to that mistake, but thankfully Le Monde and other media outlets were quick to correct the misinformation.

Søren Brandbyge (SB): There is really no simple answer to what's going on. But the long answer is that the general public is catching up—knowledge wise—to the current state of the IT world. The reality is like the Wild West online, so blatant that a layperson can no longer ignore it. This embattled environment has given way for opportunists, criminals, and a wide range of

diverse actors to exploit technology for their own gain. On the surface, it looks like an immense uptick in hostile activity—an offspring of the building tensions around the globe—with IT as the new weapon of choice, enabling the various actors to use the lack of common regulation and enforcement to their benefit.

But people are probably thinking we've passed the tipping point now, relying on IT as an integral part of almost every society's infrastructure. The reality has dawned that disruptions have catastrophic impact—not just globally, but also to individuals directly. I think recent cases make it impossible to ignore this fact, thus the increase in warnings and alerts.

Likewise, for the criminal actors who long ago saw the vast opportunities to (almost) risk free exploits and earnings, the extent of that economy has grown over the years to a level that dwarfs most other crimes and even the gross domestic product of many states. This kind of unregulated economy could destabilize countries and certainly be a threat towards even the largest companies. Again, it is something that cannot be ignored anymore.

> "The internet is a fast moving space. New technology is being adapted by customers at a very quick rate. I think we are in very exciting times, however you will always have people trying to exploit new technology for either political or monetary reasons."

Adding to the mix is the emergence of artificial intelligence (AI) and the expected quantum computing. Lessons learned from the last several decades is that such technology will be used to the full extent by both state actors and organized crime. These additions will most probably accelerate the gap between the capabilities of the general public (and small states, most companies, etc.) and the select few having (almost) unlimited funding and technological capability. It looks like it is history repeating itself. We are putting all our eggs into one basket (and we keep adding more)—because we have gone from real life activities and economics in a transparent and regulated realm to a boarder-free, and unregulated realm with ample room for actors to hide and leach information. This conversion is almost one-to-one, yet we seldom have a "plan B."

Cyber espionage, also known as cyber spying, has been a known threat to governments, typically aimed at political gain or destabilizing governments. Do you consider cyber espionage a threat or form of attack for companies and brands?

SB: Cyber espionage is a broad term. It covers many bad actors, agendas, methods, and most importantly, many different timeframes.

Most would associate the term with state actors having specific political and economic intents, but that would only cover a fraction of the activities taking place. A more full definition encompasses all covert actions to gain control of vital data that another entity depends on to achieve a specific goal. Another aspect is that cyber espionage is just a set of tools in a much larger tool chest, so the possible drivers for the activity have to be assessed to determine long-term impact. When figuring out the reasons for espionage, companies have to think like the criminal does—in terms of "what's in it for me?" That could include gaining control, knowledge, power, or profit.

The motives that top the list for companies are direct economic gain (i.e., learning secrets that can be used to siphon finances) and exfiltration of trade secrets (e.g., specifications for IP or products). The common denominator is that the threat actor stands to gain something, as long as they're not spotted or hindered.

How the criminal gets a foothold is another story, using all the tricks and techniques available at any given time, hence my point that cyber espionage is just a fraction of the whole picture.

The recently published threat assessment talks about the high levels of cyber crime and cyber hactivism threats. Can you explain the difference between the two types of crime?

SB: The terms are easily defined. Cyber crime is any activity that is deemed illegal in the context of the victim; cyber hactivism is a small subset of cyber crime PLUS a range of activities (that are either legal or not yet regulated by law) using the electronic platforms available.

The devil is in the details. If you look up the most costly, most disruptive, and most often seen and reported types of cyber activities, cyber hactivism is almost last on the scale of most used. The reason we hear about it a lot is because cyber hactivism sells newspapers, so it always makes the headlines. A very good source to gain an overview of the different types of cyber crime is the National Institute of Standards and Technology lists of crime types. Lumping several activities together ɹnder the term cyber hactivism still accounts for less than 0.1% of cyber crime (both in number of reported activities and financial impact).

Digging back through the last 20 years, hactivism has steadily declined in the overall picture. There are many reasons for that, including that governments acknowledged early the damage these activities can cause and focused on both controlling it and possibility using hactivism as a method. My worry is that it's becoming easier for the early the damage these activities can cause and focused on both controlling it and possibility using hactivism as a method. My worry is that it's becoming easier for the bad actors to get tools, exchange knowledge, hide in the masses, and form sub groups under the radar. What we have seen over the years is a steady recruitment and an increasing

diversity in tool chains (sub-contractors) in business models resilient to legal measures and our defence. That trend seems to also migrate into hactivism as well, blurring the boundaries.

Can you give us some insight into the most common forms of attacks companies experience today?

SB: There are two major classes mostly seen: zero day exploits and tailored attacks.

The attacks shift over time, both in response to the security posture one has and to the ongoing arms race between the good and bad actors. Attackers are very fast at picking up on what a company's security posture is, adjusting their methods accordingly, and ramping up their efforts. What we also see is that threat activities are very obviously driven by simple economy calculations. If the expected gain is less than the needed effort, they move on to another target.

MF: In our industry, the most common attacks we see are phishing, domain name system (DNS) hijacking, man in the middle attacks, structured query language (SQL) injection, and distributed denial of service (DDoS), to name a few. We find that these types of attacks are becoming more and more sophisticated and vicious, and this is of great concern to us.

Most organisations are focusing on protecting their assets inside the firewall, which you can also call a gateway. However, since 2018, we've refocused our concern more on what's happening outside of the firewall—the pathways where a company's online presence links to their internal systems and data. Domain name security is the key element to securing a company's online brand. When your domain is being attacked—be it from phishing, DNS hijacking, DDoS, etc.—a business is being attacked. Since these connections are outside the usual, rigorous IT infrastructure, a higher degree of risk needs to be accounted for to ensure the whole system stays secure.

> "Personal data is under attack, which is whythe European Union's implementation of the General Data Protection Regulation (GDPR) is so important."

Websites, email, cloud-based authentication, virtual private networks (VPN), voice over IP, file transfer protocol, and apps all depend on domains being functional and secure. With new technologies constantly introduced into the marketplace, networks will increasingly grow more complex. Internet of Things (IoT) devices come to mind, and companies will embrace those opportunities, yet they MUST also secure them.

Have you seen any new form of attacks recently that worry you?

SB: Every day, a new variant or a new concoction of techniques show up. It is not as much the steady evolution and broadening of attack vectors and their increasing impact that is worrying, it's that the focus seems to be shifting more and more into a massive harvest of personal data and profiles. If you combine that with the fact that more of our personal lives and identities are kept electronically, we've got a recipe for problems of epic proportions. So personal data tops my list.

MF: I agree with Søren. Personal data is under attack, which is why the European Union's implementation of the General Data Protection Regulation (GDPR) is so important. Fines for companies found to have customer data breaches was not enough, so it has been equally as important that GDPR also gives power back to European consumers to control personal data collected and stored. Just reading the daily news headlines underscores why this provision is important to consumers, and in turn, companies. It costs far less to get domains secured ahead of time than it does to clean up a data breach, restore customer confidence, and catch up on annual revenue.

How do those attacks affect a company and their vital functions?

MF: Depending on the form of attack, the worst case scenario is a complete take down of an entire system. That does not just include websites customers might depend on, but entire email, VPN, and telephone systems that employees depend on to conduct business. A full-blown, successful DDoS attack can paralyze an entire business for hours or even days.

Data breach or data leak will have a severe impact on a company, especially with the implementation of GDPR. A data breach via malware on IoT, phishing, or even by DDoS attack is very common and should be avoided by implementing all proper security and training.

Whatever attack we're looking at, it will cost a company dearly, it will damage a brand's reputation, and therefore account for a loss of their customer base.

What would you recommend to companies to stay protected against those types of attacks?

MF: Take action! And remove any conditional statements when reviewing security strategy—it's not if, but when an attack will happen.

I always recommend a three-step approach.

Step 1: Audit all digital assets. What domains, digital security certificates, apps, social media handles, etc. do you own? What security measures are in place? Are you using registry and registrar locks? Are two-factor authentication and DNSSEC in place? What DDoS protection has been applied? How secure is your DNS vendor? Are you using email fraud protection? The list seems long, but it's actually pretty straight forward.

Step 2: Train and retrain employees on security. This is the most vital element as the enemy is within (even

if it's often accidental). Human error is the biggest risk to security. Training should be repeated regularly, and employees should be tested for compliance.

Step 3: Educate your customers. Your customers need to understand how to differentiate between a phishing email, phone call, or otherwise. Make sure they know that security is one of your top customer priorities. Tell them what they can expect from you, and especially what they won't get from you, e.g., that you'll never ask them for their password.

What are the primary security measures that you see global companies neglecting today? Are there any typical blind spots companies tend to miss when securing their business online?

SB: Globally, I think we're being subverted into thinking that advanced persistent threats and sophisticated attacks are the biggest threats—threats that call for high-tech counter measures and specialized tools. But most of these threats rely on some rather simple techniques and attack vectors. I would argue that our biggest global—and growing—blind spots are the basics. We tend to focus on the end goal while not paying enough attention to the chain of events and methods, meaning we miss the issues that are indeed under our control and can easily be handled without the need for elaborate technology.

In short, any type of attack relies on a reconnaissance stage, access, more intel gathering, then escalation, and gaining control. From the very beginning of this chain of events, basic security should be governing counter actions, like making sure security is up to date, using best practices, and so on. It also calls for a thorough look into one's capability of monitoring, and what you own that's of value to criminals. Think about redoing some processes and solutions instead of just adding band aids. Blind spots like DNS, email, and data storage are the most overlooked supportive systems for the infrastructure.

MF: Here again, I fully agree with Søren. As previously mentioned, domain names aren't understood enough. And it doesn't get more basic then that. We've seen domain security being passed around like a hot potato, yet this is a crucial element when talking about securing blind spots outside the firewall.

Over the years, we've produced several cyber security reports focusing on different industries and are still shocked by how many companies are using their own DNS, for example, and not switching on registry and registrar locks. Secure sockets layer certificates are also an interesting topic; we are seeing many companies not using the correct certificates and, even worse, not managing those already in place in a central repository. Multiple people in a company could be buying certificates, using their personal email address to register them, then letting it lapse when they change departments or leave the company—so certificates are not being reissued when they should, leaving websites unsecured.

It's our job to educate our clients. It's not always easy, as many stakeholders from various departments are involved, but we feel this is our responsibility.

With IoT, artificial intelligence, and 5G being introduced slowly but surely into all our lives, are threats growing or changing? If so, how and why?

SB: Whenever you add complexity to your operation, you add risk. Whether or not that also equates to a growing threat depends on how you go about implementing new technology, the security required, and especially how much you depend on the new components.

In addition, all industries tend to focus on the potential gain of new tech, downplaying the hidden cost of additional blind spots. We need to understand how new technologies transform our infrastructure and what a normal baseline should look like. Issues mostly arise in the boundaries between systems and functions.

Expecting the provider of a new technology to deliver 360 degrees of security coverage is probably not realistic.

Lastly, industry as a whole quite often doesn't understand new security technologies fully before implementing and using them. Take artificial intelligence (AI), for instance. AI has been heralded as a silver bullet that can be fed almost anything, making sense out of incoherent data. But AI is not capable of deducing anything that is not in the data. Mathematically speaking, AI can only be used meaningfully for a very confined set of problems. AI is probably the most misunderstood new technology, opening us up to risk. What we need is industry cooperation to find a secure way forward with AI.

> "Companies have to think about how to protect the customer before protecting themselves. It's basic: build it, build what supports it, safeguard it, andhave alternatives ready."

How has the rapid evolution of the internet, which includes major opportunities and risks, shaped how global brands conduct their business?

SB: A broad historical question demands a broad encompassing answer. As I am not an expert on business models, I have to describe the evolution from a technical view. The emergence of IT as a business tool back in the 70s through the 90s created new ways of modifying internal procedures and services, mostly a one-to-one conversion from manual to IT-based labour.

As such, the internet was a new extension in the IT toolbox, not yet recognized as a new method for reaching out to customers. The challenges with the new internet were rooted in catering to customers by delivering solutions that are tailored, not just reused mock ups.

Risks arise when services that support our secure services

fail, opening up exponential avenues of exploitation and risks. We are forced to adapt to the customer through a simple architecture, and risk. If we can do this right, the future doesn't look bad. For starters, we should acknowledge that controls are good, but are at best just a band aid if we do not build the services correctly from the start. Companies have to think about how to protect the customer before protecting themselves. It's basic: build it, build what supports it, safeguard it, and have alternatives ready.

> "New technology is being adapted by customers at a very quick rate. I think we are in very exciting times, however you will always have people trying to exploit new technology for either political or monetary reasons."

Sharing knowledge is also paramount. We see the bad guys thriving in a dynamic, dark economic business evolution, building very mature systems by sharing knowledge. If we really have the aspiration to get ahead of this game, we need to act as one entity, sharing best practises, sightings, failures, and learnings. We also need to embrace our customers and value their feedback. Some of this is already happening, but is far from the level matching the adversaries. Even though the dark economy is working at their highest capacity, the legitimate world is still capable of gaining the upper hand.

At CSC, what do you think your clients will need to stay secure in the future? Any insight on your plans?

MF: The internet is a fast moving space. New technology is being adapted by customers at a very quick rate. I think we are in very exciting times, however you will always have people trying to exploit new technology for either political or monetary reasons.

Our top priority at CSC is to protect and secure our clients' online presence. For that, we always try to look ahead. How are connecting devices going to change the security levels of our clients? How will 5G affect HTTPS and DNS, and what does that mean for our clients? Can blockchain be an alternative to the current DNS or online IP?

In our industry, you can't stand still. That makes it the most exciting industry to be in right now, yet never forget to focus on your clients and their needs.

So, is cyber security just the buzzword of the year or decade?

MF: I sometimes wish it was. We do see companies using the term cyber security when they actually have nothing to do with it. So I would advise everyone to research, and when talking to those companies, dig deep. As Warren Buffet once said, "You only find out who is swimming naked when the tide goes out."

Securing your company's business from the inside out must be the priority, therefore ensuring you get the appropriate solution with a trusted vendor in place.

SB: If by buzzword you mean a word used to the extent of becoming diluted and almost meaningless, then yes. Cyber security is used and referenced in so many contexts that it is as precise as saying "life can be hard." But, it's a really good catchphrase. It sells papers.