Supply-side Liability: Cybersecurity as a USP – The Most Secure Supplier Takes the Lead

Written by Joshua Bucheli, Talent Community Manager at cyberunity, in Collaboration with Tolga Ergin, cybersecurity specialist in digital and mobility solutions at Mercedes-Benz Mobility AG, and Peter Kosel, Founder of cyberunity

Earlier this year, the US software firm Kaseya fell victim to a $70 million ransomware attack. Factoring in all the direct and indirect customers of Kaseya's products, this single attack compromised over 1,500 companies worldwide, even forcing hundreds of Swedish supermarkets to close down operations when their tills stopped working.

Businesses are increasingly recognizing that awareness forms a considerable part of the cybersecurity game. But this awareness is often directed inwards, addressing the vulnerabilities that arise within a company and overlooking the indirect threats associated with third party business relationships. Everyone knows that cutting corners exposes a business to the threats of the digital world. What is less often talked about are the impacts that a company's cybersecurity maturity has on those it interacts with.

Business is not conducted in a vacuum. It is, by its very nature, an interactive endeavour. More often than not, it involves a chain of collaborative efforts between clients, customers, suppliers, vendors, contractors, original equipment manufacturers (OEMs), distributors, external service providers, and so on. While businesses are paying more attention to how secure their own processes are, they still often neglect to consider how secure their partners' processes are.

However, as Tolga Ergin, cybersecurity specialist in digital and mobility solutions at Mercedes-Benz Mobility AG, points out, with a little cunning, suppliers can turn this Achilles heel into a valuable USP with which to build more steadfast, secure, and sustainable business relationships with their clients.

Supply-side security – A chink in the cyber-armour

As with every proverbial chain, the digital supply chain is only as strong (or secure) as its weakest link. Increasingly, this weak link manifests as suppliers who have access to client data but whose security protocols do not measure up to those of said clients.

Cybercriminals are after data. They don't care where this data comes from. If they can access a company's data more easily by going through a supplier with less robust security protocols, they will. If this supplier happens to have access to the data of several clients at once, as in the Kaseya incident, then this just sweetens the pot for any bad-actors.

According to ENISA, the EU's agency for cybersecurity, cybercriminals are catching on to the fact that many businesses are no longer the easy targets they once were. Instead, they are increasingly targeting their victims indirectly, taking advantage of the still oft overlooked and highly scalable vulnerabilities in digital supply chains. As of 2021, over 60% of all cyberattacks rely on the trust that customers place in their suppliers, with as many as 66% going through the code of suppliers in order to access the data of targets.

The narrow scope that many businesses still afford to their cybersecurity runs to the heart of the issue. As Tolga notes, "currently the importance of holistic approaches to cybersecurity is severely underexposed, especially in SMEs. Such security considerations should really be the responsibility of directors and management, but on the ground, this is seldom the case."

Instead, cybersecurity is often approached in a piecemeal, reactionary fashion, largely being left up to individual security specialists within a business. This inevitably leads to unforeseen vulnerabilities – chinks in a company's digital armour – which threaten not only them, but also their clients, and even end users.

The solution to this problem? – more conversation about the importance of third-party security, says Tolga:

"Businesses are going to need to devote resources towards the threats that third parties bring to the equation. Vulnerabilities related to phishing attacks, identity and access management protocols, and social engineering threats need to become a priority. For this to happen it's vital that both suppliers and their clients begin assessing the risks brought about by their interactions. Open communication regarding these additional entry points and how to go about plugging them is key. Talking more about the mutual security risks posed by client-supplier relationships may bring about the external pressure needed for businesses across the board to embrace a broader perspective."

Cost, Quality, *and* Security

IT-security is often framed as a question of 'security for its own sake' – of identifying and filling gaps in awareness. But security can be much more than a burden that companies bear dutifully. Increasingly, some companies are recognizing that security can just as well be a marketable and potentially lucrative USP.

What if, instead of pursuing security purely for protection, both suppliers and their clients instilled a corporate culture in which security was recognised as a competitive advantage to be capitalised on? A transparent approach to supply-side cybersecurity doesn't just make things safer, it's an opportunity for businesses to set themselves apart from the competition.

Traditionally, quality and price have been the two major factors that companies consider when deciding who to do business with. As corporate awareness of the threats of the digital world increases, *security* is becoming the third factor in this equation.

"At the end of the day, in a world where the importance of cybersecurity and Integral Corporate Security (ICS) is gaining recognition, clients are going to choose the *most secure* supplier, all other things being equal. Inevitably, companies will become more inclined to do business with partners whose processes and culture of security match or surpass their own.", says Tolga.

Future-conscious suppliers would therefore be well advised to foster a sense of partnership and trust by involving their clients in the planning of their security strategies.

"Security is an enabler for success, it's something that companies can use to differentiate themselves from the competition. As they realise this, questions like 'what do you need from our end as your supplier/client in terms of security?' will become increasingly important for future-facing approaches to cybersecurity", emphasises Tolga.

Seizing the silver lining: Using 'Security Inside' as a business enabling USP

"It's not rocket science, and with the right people at the helm and on the ground it's entirely achievable," says Tolga.

Businesses need both leaders and employees who recognise and appreciate the value and importance of interactive security. Only then will they be able to proactively encourage and drive this mindset throughout their companies.

One good resource with which SMEs and their employees can start building a reputation for supply-side security is the BSI, which supports businesses in establishing robust IT protection procedures via its myriad publications. The ICS Security Compendium Test and the IT-Grundschutz Compendium stand out as prime examples.

Alternatively, OT manufacturers may want to take advantage of the ICBC's dedicated OT Security Demonstrator and Courses or VINCI Energies' international security operations center for ICT and OT.

Another avenue to explore is cybersecurity insurance. Ultimately, security breaches cannot be avoided entirely, and clients are going to feel much safer entrusting businesses with their data if it is properly insured as well as being protected. In addition to the financial protection offered, such insurance often requires an audit of a company's internal security,

adding an extra layer of awareness to the mix. Well known insurance companies have, for example, recently added broader coverage to their Security and Privacy Liability Policies and even offer prevention services to help end users and clients use digital products safely.

Supply-side security awareness specialists – hard skills and qualifications:

As Tolga emphasises, "employees are a company's most valuable asset, not its weakest link as is often said, and they should be empowered accordingly." Indeed, if businesses want to turn their security into a USP, they are going to need dedicated supply-side specialists who can establish and supplement a mature culture of cybersecurity.

In terms of formal training, individuals interested in pursuing a career in this field would be well advised to start with basic cybersecurity certifications like the BSI's IT-Grundschutz (basic security) course. From there, building out their skillset with the help of trainings like the ISC2's CISSP course will let them stand out from the candidate pool.

Businesses should be on the lookout for individuals who can tailor industry standards in supply-side cybersecurity to their particular needs. As such, these individuals should have an understanding of both international and local legal and regulatory foundations around IT security and data protection, like the EU's GDPR, NIST's cybersecurity framework, and Switzerland's FADP.

While legal professionals may fit this bill, ideal candidates will also bring supply-chain know-how to the table – for example, procurement specialists or technicians with strong backgrounds in governance and compliance. Risk management professionals who can bring a holistic approach to security, classify potential risks, and apply methodologies like data protection impact assessments will also be especially valuable. Ultimately, it is pragmatism and big-picture thinking that will make the difference rather than a reactive, ad hoc attitude to incident mitigation.

Personality – beyond technical know-how:

Supply-side cybersecurity awareness specialists need more than just technical skills. Beyond proactively identifying risks and opportunities, they also need to be able to effectively communicate next steps that are in the best interest of the company to management. In this respect, the ability to communicate effectively and to approach complex issues from a broad perspective – to see how the technology-, legal-, and business-worlds interface with one another – is absolutely key.

Perseverance is also vital. While the issue of cybersecurity is increasingly making it onto the radar of employers, it is often still not afforded the priority it deserves. Professionals who can handle dismissive attitudes to cybersecurity and who can convince management that it is worth their time will be paramount.

Finally, tenacity and a natural flair for presenting ideas convincingly will round off an ideal candidate's profile. Businesses are still coming to terms with the threats that their digital supply chains introduce, and they may need some help recognising the hidden USP that this

presents. The ability to persistently communicate both the necessity of supply-side cybersecurity, and the reputational opportunity it presents will be vital tools in the arsenal of tomorrow's cybersecurity awareness specialists.

At the end of the day, the digitisation of corporate supply chains is unavoidable. Insurance companies entrusted with the sensitive personal data of millions of people are migrating this information to the cloud. The automotive and fleet management industries, where the stakes go well beyond data and cross over into life and death, are increasingly relying on digital systems to coordinate and automate their products. OEMs are interfacing their control panels with the IoT.

The trajectory of these developments is set, and the associated risks to businesses and the public alike are far from trivial, sums up Peter Kosel, Founder of cyberunity AG. Cybersecurity is no child's play, and the best we can hope for is that the right individuals step up to the plate and that companies get to know them at an early stage – here, too, it's a question of gaining that decisive edge over the competition. Those who start looking for top performers today, because they would like to win them over tomorrow or the day after, are already too late. Those who can help develop and implement robust SOPs for supplier-client interactions – professionals who are equipped to boost industry awareness about the devastating risks and the potentially lucrative USPs that digital supply chains are introducing – are in exceptionally high demand. They are not on the street-corner waiting for someone to offer them a job.