*Media release*

# Cyber Incident Hub – a powerful response to cyber attacks

**Zurich, 25 August 2021 – The three leading consulting firms MLL MeyerLustenberger Lachenal Froriep (MLL), Farner Consulting, Oneconsult and the start-up CYBERA launched the first inter-disciplinary "Cyber Incident Response Hub" for Switzerland on 25 August 2021 to coincide with the trade association's XBorder event entitled "Trends in E-Commerce". The range of services provided covers highly relevant support against cyber attacks. This is offered by the four companies around the clock (24 hours per day, 7 days per week) if attacks occur. The services cover specialist legal advice relating to cyber affairs (MLL), incident response and digital forensics (reacting to and investigating cyber attacks) (Oneconsult), crisis communication and reputation management (Farner), as well as the international response to money stolen through acts of fraud (CYBERA). This unique proposition to Swiss business counters the steeply rising threat to companies from cyber attacks, data corruption, fraud and extortion at a time of digital transformation. Alongside cyber insurers, it is aimed at every type of business potentially exposed to this threat.**

Spectacular cyber attacks, such as the ones carried out recently on the tech giant Microsoft and the American company Kaseya, "enjoy" a huge amount of international attention - normally to the benefit of the attackers: their criminal business models appear to be indirectly endorsed and worthy of emulation, because these attacks all too often end up with the criminals getting away with a lot of money and no punishment. This is why the number of cybercrime incidents, and the amount of losses sustained, is rising steeply and markedly.

**Smaller businesses get caught out too**

But it is not just the big corporations that are being hit by the rising number of cyber attacks. That has been proven by the Stadler Rail and Comparis cases. A ZHAW study has also revealed that about one-third of all Swiss SMEs have already fallen victim to cyber attacks; and some 4 % of them have also been blackmailed. This means that already around 200,000 SMEs have been the victim of a cyber attack. That is a significant number, especially when considering that in various surveys, some 56 % of managing directors judge their IT security standards to be "good" or even "very good".

These findings reflect the scale of the threat facing businesses in this digital age. Thanks to their lack of awareness they may easily fall victim to cyber criminals. ICT Switzerland put out this warning in one of its studies: *"The risk of falling victim to a cyber attack is not rated highly enough. The possibility of being unable to operate for a whole day or even to have their very livelihoods put at risk was viewed as a significant or major danger by only 10 % and 4 % of respondents respectively."* But at the same time, only 60 % of respondents confirmed that they had deployed in full such basic protection measures as malware protection, firewalls, patch management and backups. Systems to identify cyber incidents had only been fully implemented by one in every five businesses. Only 18 % of the businesses surveyed said they had procedures in place to deal with cyber incidents; a mere 15 % said they ran training for employees on the safe use of IT.

**Sound advice is needed if it happens**

If a business falls victim to a cyber attack, it needs sound advice from a knowledgeable partner. A ransomware attack, for example, will be swiftly followed by a demand for ransom money, usually in a cryptocurrency so as to cover up tracks. Victims often remain uncertain, even after making the payment, whether they have indeed regained full access to the data that was encrypted by the attackers. They are left potentially with law suits, reputational damage, financial losses and uncertainty. Prevention, intervention and aftercare, along with sound advice, are called for here.

**360° package offers a promising solution**

This is the starting point for the services being offered by the four companies. Successful prevention together with the appropriate response to cyber security risks calls for interdisciplinary and cross-border collaboration. The skills of legal, technical, forensic and communications experts are all needed if companies are to be optimally prepared for attacks, able to ward them off successfully and deal with, or at least minimise, their consequences. The law firm MLL has built up a network of first-class, experienced partners, allowing it to offer a coordinated response to all types of cyber security problem. Their round-the-clock service ranges from drawing up a cyber security response plan and analysing a company's ability to deal with cyber risk, to dealing with security breaches, data loss and the investigation of cyber attacks in a legally correct manner. Good communication in the event of an attack helps to restore any reputational damage quickly.

When all is said and done, being able at all times to ensure cyber and data security is essential for companies today if they are to meet their legal obligations in respect of compliance and good governance.

---

Lukas Bühlmann, a partner at MLL: *"Any loss of data, and the response to it, immediately gives rise to liability and accountability risk. Responding in the right way, even under the pressure of events, helps to reduce the risk of legal consequences."*

Tobias Ellenberger, COO of Oneconsult: *"The sooner professional assistance is given, the smaller the risk that an organisation will sustain heavy losses because of a cyber attack. That is why it is important, if you are attacked, that you can call quickly on the services of an experienced, reliable and professional partner."*

Daniel Heller, partner at Farner Consulting: *"Damage to, or theft of, sensitive customer data can lead very quickly to a public scandal. For the organisation involved, this can cause serious reputational damage. With the help of a good and experienced team providing professional crisis communication, reputational damage can be minimised."*

Nicola Staub, founder and CEO of CYBERA: *"In order to block sums of money that have been fraudulently obtained by providing the information relevant under criminal law, and to secure those sums before they get laundered and are irrevocably lost, you need new solutions - and we offer them."*

The four partners together provide the optimal bundle of expertise to deal with cyber attacks, no matter what form they take. They offer: cyber-centred legal advice and data protection, cyber security, reaction to and defence against attacks, as well as digital forensics, reputation protection and crisis communication, protection against cyber fraud and 24/7 incident response.

## Further information from:

**MLL MeyerLustenberger Lachenal Froriep AG**: Lukas Bühlmann, +41 79 205 00 94 / Nicola Benz, +41 76 518 81 85

**Farner Consulting AG:** Dr Daniel Heller, +41 79 434 23 85

**Oneconsult AG:** Tobias Ellenberger, +41 79 538 38 71

**CYBERA:** Nicola Staub, +41 78 761 80 31