COVER AGAINST FRAUD AND CYBERCRIME

THE SOLUTION FOR:
Every company with its own employees that uses digital data systems and the Internet.

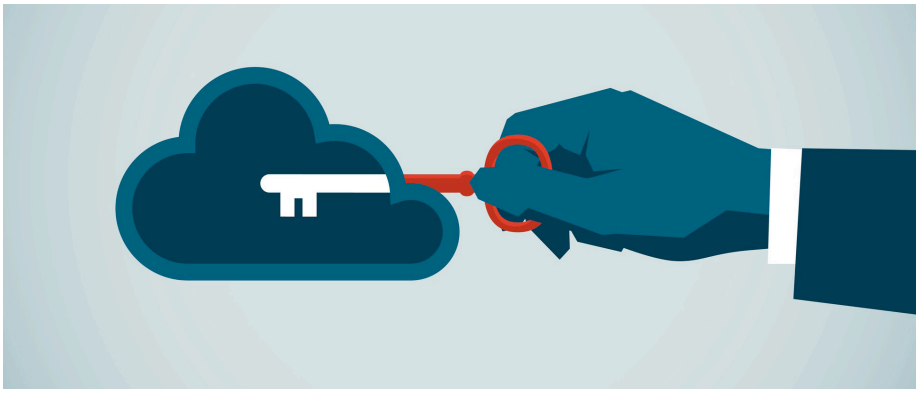
REASONS TO TAKE OUT FIDELITY INSURANCE:

- **Minimisation of personal liability risk** for members of the Executive Board and the Board of Directors.
- **Optimal addition to cyber insurance** for extra cover against computer crime and social engineering.
- **Financial protection against hacking** and data misuse.
- **Cover against fraud** by employees or third parties (external IT providers, auditors, cleaners).
- **Cover against social engineering attacks** involving phishing, pharming and spyware.
- **Lasting minimisation of your business risk.**

More and more companies in Switzerland are at risk of falling victim to cybercrime and hacking. Anyone who trusts blindly in the security of their IT systems and antivirus software may be in for a nasty surprise. From spying on internal company matters to data theft, deliberate sabotage and targeted malware attacks, the consequences can quickly become expensive. Social engineering in particular, i.e. identity misuse by employees and business partners in order to give instructions for the execution of financial transactions, for example, is becoming increasingly prevalent. A company's trust in its own employees can sometimes be abused, too. Time and time again, black sheep among the workforce or external staff can harm their employer or customer through fraud, embezzlement or data manipulation.

THE COMPELLING BENEFITS FOR YOU

- **Cover against losses due to social engineering** (fraud committed by assuming a false identity, such as fake president fraud).
- **Cover against losses caused by your own employees,** external staff, temporary workers and lawyers, tax advisors and auditors working for your company.
- **Insurance against losses caused by hacking** as a result of intrusions into your IT systems.
- **Cover against losses caused by third parties** through acts of robbery, theft and fraud.



INSURED RISKS:

- **Financial losses** that you incur as a result of criminal activities by persons of trust, e.g. through theft, embezzlement, fraud, misappropriation or property damage – collectively known as fidelity losses.
- **Losses from fraud involving the use of false identities,** such as fake president fraud or payment diversion by third parties pretending to be one of your business partners.
- **Losses caused by third parties** committing acts of robbery, theft or fraud.
- **Losses resulting from the betrayal of secrets** and contractual penalties.
- Assumption of costs for measures to **minimise reputational damage.**
- **Cover for contractual penalties.**
- Assumption of internal and external loss **investigation and legal costs.**
- Cover against losses resulting from intentional, illegal and targeted intrusions by third parties into your IT system with or without financial gain (hacking losses).
- Cover against losses caused by illegal and unauthorised acquisition and misuse of passwords or login details by means of phishing, pharming, spyware, keylogging or other criminal methods.

ANY QUESTIONS? HERE ARE SOME FAQS:

- **I will not accept any criticism of my employees. Why should I mistrust them?**
  Many entrepreneurs trust their staff without hesitation, and usually they are right in doing so. The figures paint a different picture, however. Every year, crimes like embezzlement and fraud cause millions of francs' worth of losses. In many cases, employees commit these crimes because they have got into financial difficulties, for example because they need to fund an expensive lifestyle or pay off existing debts. Gambling addiction can also be a factor. And sometimes opportunity makes a thief, as the saying goes.

- **Our IT system has state-of-the-art security. Who is going to hack into it?**
  Digital gangsters are good at staying ahead of the game and will always find new ways to hack into companies' systems. One particularly popular method is the use of targeted phishing e-mails. A link integrated into the e-mail tricks employees into revealing their user data, giving the fraudsters unhindered access to their computer system. Even an IT system with the very highest security standards can do little in such cases.

- **Even if somebody steals something, it won't break the bank, will it?**
  The problem is not the smaller offences such as theft of office equipment; it is cases of embezzlement that run into the millions and often go on for years – as is frequently reported in the media. Once the perpetrator is convicted, it is usually impossible to get anything out of him or her – the money is gone! Incidentally, if there is already an undiscovered case of this kind at your company, the unlimited retroactive cover which comes with Euler Hermes fraud insurance will also cover this.

Euler Hermes Switzerland Richtiplatz 1 8304 Wallisellen T +41 44 283 65 65 info.ch@eulerhermes.com www.eulerhermes.ch
Office Lausanne Avenue Gratta-Paille 2 1018 Lausanne T +41 21 643 74 20
Office Lugano Via Antonio Adamini 10A 6900 Lugano T +41 91 922 73 64