

## “The threat is very real”

Mark Greisiger is CEO of NetDiligence, a company that helps businesses manage cyber risks. Topics asked him how these risks can best be minimised.



### Topics: In your opinion, what are the greatest cyber liability risks?

Mark Greisiger: I would say in the USA it is the risk of a data breach involving non-public sensitive information on customers (privacy violation) that leads to a massive class-action lawsuit. The type of data most at risk would include both financial and medical information. Much of this is attributed to the lack of encryption still in place for data “at rest”. The legal negligence can be underscored and demonstrated by non-compliance with a growing list of privacy and government regulations that govern the security of certain data. I also feel that for certain business models business interruption (first-party loss) can be their key concern, such as business that requires 24/7 availability of their systems. The threat of extortion or a denial of service (ddos) attack against their corporate network to degrade performance or shut down their operations altogether for several hours or days would be catastrophic to their bottom line and reputation. This seems to be the main risk concern for our European clients.

### Have technical security systems improved significantly in the last ten years?

I would definitely say yes. There are so many good technologies these days to prevent “bad guys” from breaking into networks or to mitigate the accidental mistake by an employee that leads to a leak of private information. Moreover, whole disc encryption of laptops is now a baseline standard and there is software to prevent the release of certain data types from being allowed to traverse a corporate network. Another example is preventing “SQL injection” through regu-

lar scanning of your applications and installing a firewall at the application layer (in addition to the network) to defeat the SQL exploit, which is the main cause of many of the large public breach events to date. Having said that, the e-risks still exist and grow because the threats continue to morph and appear to stay one step ahead of the security safeguards.

### Have companies become more aware of risks that result from all-embracing internet connections?

Yes, I would say that is a key contributor. Many risk managers quickly became aware of their own reliance on the internet (i.e. the inherent security risks of a public network), their growing reliance on many third-party dependencies (business partners, contractors, ISPs), and the unknown quality of the security practices in those trusted partners. Awareness has also increased because at least 80% of companies have suffered one or more attacks and/or network breach incidents at first hand, so they know the threat is very real.

### What are the critical issues companies have to bear in mind in order to identify such risks?

For example, it is vital to undertake an annual enterprise-wide assessment of security and privacy practices that includes a review of people, processes, policies and technology safeguards. It is important to establish whether your organisation measures up to industry-accepted standards, compliance with regulations, and is in line with your competitors. Especially important is an inventory of network and data assets. There needs to be open internal communication in place between key management so as to better understand the business activities that might create risk. There needs to be regular network penetration testing (e.g. monthly) so organisations can understand if their public-facing network can truly deflect the some 6,000 known hacker exploits.

**What are your thoughts on technical trends in the next few years and what could they mean for the insurance industry?**

Right now in the USA, the coverage sought most often is third-party privacy liability due to emerging lawsuits, but I feel over the next few years, as risk managers and their corporate board members/directors gain a better understanding of their overall cyber risk, that their appetite will expand to include first-party (business interruption) coverage. And we are paying attention to the recent lawsuit case – against eBay – where certain site users with a disability (sight or hearing impaired) sued because they could not access the site to buy services. This trend is called “universal access”. Claims for discrimination against the disabled are common in the physical world, requiring businesses to have, for example, easy access to buildings such as wheelchair ramps; now it seems virtual wheelchair ramps might be needed. And there have been more discussions and concerns with our customers and broker alliance partners about insuring against energy-grid failure, which can be attacked by cyber terrorists or degraded due to an act of God.

**MARK GREISIGER** is head of NetDiligence, a cyber risk management company. For more than nine years, NetDiligence has been supporting companies in all sectors with cyber risk assessment, due diligence for risk management and compliance. Its services are specially tailored to the needs of US and UK insurers offering network liability coverage.