UNDER ATTACK

Threats from cyberspace aren't just a problem for governments. Companies should worry about them, too, says Ian Searle

There is lots of talk about cyber risks and, increasingly, the topic is creeping into newspaper headlines – if only reaching the inside pages. So what do cyber risks mean for treasurers? As one treasurer puts it: "There's a lot of hype around the topic, but it does seem to be limited to politically motivated attacks." Another adds: "I suspect many of us are quiet on the subject as we simply don't have the time, resources or knowledge to do anything about it."

Well, if you believe Fang Fenghui, the chief of staff of the Chinese People's Liberation Army, cyber risks can be likened to an atom bomb. He thinks they will cause widespread infrastructure damage and loss of life, and warns that cyberterrorists could also manipulate systems that control nuclear facilities and even weapons. This impassioned view is particularly interesting since it comes from a dignitary whose country is responsible for 96% of all intellectual property cybercrimes, according to a report by US telecoms company Verizon.

What is alarming is that cyber risk events are happening all the time, but many corporations simply don't know that they have been targeted. Those that have been attacked often don't know how it was caused or what to do about it – and they have made no contingency plans to deal with such situations.

"A large number of organisations lack the understanding to deal with sophisticated attacks and their growing volume," says Alex Fidgen, director at information security consultancy MWR InfoSecurity. "Complex networks involving suppliers and partners are a challenge to security and were not built to defend against the attacks that are now being witnessed on a weekly basis."

Where a cyber event has taken place, a veil of secrecy usually falls. This is because most businesses fear the reputational risk that publicity around a cyberattack would create. Certainly, it is difficult to find treasury functions that will publicly share their own action plans.

An examination of the cyber events that surfaced in 2013 shows that they cover many and varied activities. In June, Gmail accounts in Iran were hacked in an apparent attempt to influence the country's national election while weapons systems in the US were targeted in May (fortunately unsuccessfully). US banks have also seen their trading and customer accounting sites intercepted and disrupted. But this year the highest-profile and largest cyber disruption on record plagued Spamhaus, a not-for-profit organisation based in Geneva and London that specialises in identifying and filtering unwanted spam messages. It was overloaded with messages that were intended to force its servers to crash and massive volumes of data were sent maliciously to its account – the work of organised and IT-savvy cyberterrorists.

Why do these IT geeks initiate a cyberattack? It seems that the existence of so-called 'big data' (large and complex data sets) makes the malicious, deliberate and mass release of information attractive to hackers. Motives vary and there are suspicions that some cyber incidents are carried out by governments as a means of political interference. Most hackers simply enjoy the thrill of the attack and the trail of destruction they cause – Wikileaks is perhaps the best example of a coordinated plan to publicise sensitive data aimed at maximising embarrassment and humiliation.

The threat to treasury

Treasurers should not wait for a cyber event to disrupt their businesses. But the actual steps they need to take to address cyber risks will vary from company to company and depend on the sectors they trade in. They will also be affected by their company's relationships with governments, political affiliations and, of course, the extent to which it stores and maintains sensitive data. Hackers often target businesses on the basis of flimsy information gathering and may be haphazard in their selection of targets.

So to prepare for a cyber event, the starting point must be a full risk assessment, which identifies critical data, the sensitivity of that data and what could happen if it got into 'the wrong hands'.

Paul Bramwell, senior vice president, treasury from SunGard's corporate liquidity business, says: "Cyber risks are a serious consideration for corporates when deciding to implement a treasury solution, whether they are installing it in-house or using an outsourced hosting environment. The reality is that nothing is bulletproof. A company can be hacked when a system is installed on-site, as well as when it is hosted in the cloud."

Which neatly brings us on to cloud technology, an increasingly core component of information storage and distribution. But is it safe? Reassuringly, Bob Stark, Kyriba's vice president of strategy, explains there are two key security considerations when it comes to the cloud. "The first is security of the data at rest. The second is protecting the information exchange between external systems – for example, from treasury system to bank. Protecting the information exchange is exactly the same whether the corporate solution is on premise or in the cloud. The only difference is whether the data, while at rest, is hosted within the corporate's IT server rooms or whether it is in a state-of-the-art hosting facility. It is well known that cloud providers have more resources to invest in security than corporate IT teams, meaning that these hosting facilities will offer more protection."

Companies that are targeted by cyberattackers may find that the perpetrators can come from the left field, including internally. They may be disgruntled staff or individuals who disagree with company policy. Externally, factions can choose to target a particular business for no apparent reason by a simple random attack. It is also the case that hackers scour for ever-greater challenges, often based on inaccurate or poorly researched information, particularly where there is political or environmental motivation.

For those who fear for their company's defences in the event of cyberattack, it is worth mentioning the availability of insurance cover. It has taken many months to gain traction, but there are products out there, covering both first-party and third-party exposures. Brokers maintain that there is plenty of capacity, which has brought the cost of insurance down.

However you choose to prepare for them, one thing is for sure – cyber risks are not going to go away. There is plenty of information available on the current cyberthreats and issues so treasurers should ensure that they are plugged into this information feed. It is valuable source material for monitoring and managing exposures within your own business.

A TREASURER'S CHECKLIST FOR TACKLING POTENTIAL CYBERCRIME

Secure board-level awareness and support, and empower the risk committee to research and implement preventative measures.

◆

Undertake a full risk analysis, involving all stakeholders in treasury data transactions. Don't forget the IT team.

◆

Identify and prioritise the key treasury risks facing the business.

◆

Identify the existing protections that can address or mitigate the risks and prepare a gap analysis. Determine what needs to be done to plug these gaps.

◆

Create a business continuity plan to cope with any outages. Ensure a risk log is maintained to record and assess new exposures and change the plan to reflect them.

◆

Keep up with what's happening in the world of cyberterrorism and discuss the potential implications to the treasury function.

◆

Remember, the risks may be with your stakeholders – consider what would happen in the event of a bank's outage.

KEY QUESTIONS FOR CEOs AND BOARDS

In its document *Cyber Risk Management – A Board Level Responsibility*, the Department for Business Innovation & Skills outlines some key questions for boards to consider when reviewing cyber risk. See http://tinyurl.com/atgghnc

Ian Searle is an independent risk management consultant, specialising in communicating risk issues