Deloitte.

# What you don't know could hurt you

To assess exposure to cyber threats, companies need to go beyond generalities and focus on specific questions about security practices...

Could it happen to us? Alarmed by an uptick in cyber attacks on high-profile businesses, many boards of directors are asking their CIOs and CISOs just that question. Unfortunately, at most companies the short answer may well be that it's already happening. As an example, 50 businesses participating in a 2011 study on cyber crime experienced an average of more than one successful cyber attack per company per week – a 44 percent increase over the 2010 rate.[1] In light of statistics like these, it's reasonable to assume that most companies either have been or are at risk of being compromised by cyber crime.

## What's at stake?

Although most cyber attacks don't make national headlines, they can hurt a business in any number of ways, from simply vandalizing its website to shutting down networks, perpetrating fraud, and stealing intellectual property. The financial impact can be significant: one 2011 study reported a median annualized cyber crime-related cost of $5.9 million among participating businesses, a 56 percent increase over the previous year.[2] Cyber attacks can also deal a serious blow to a company's brand and reputation, with potentially significant consequences. Concerns about data security may prompt current and prospective future customers to take their business elsewhere, and negative reactions among investors may even drive losses in market value.

What's more, because cyber threats are both a relatively new and constantly evolving source of risk, many organizations may not be as effective at managing the cyber threat risk as they are at managing risk in other areas. Indeed, many data breaches are discovered not by the victimized organization itself, but by external parties such as law enforcement or third-party fraud detection programs.

## Ask the right questions

Given the high risk of cyber threats – and intensifying regulatory scrutiny – boards of directors have good reason to ask CIOs and CISOs questions beyond "Could it happen to us?" to "How likely is it to happen to us, and what are we doing about it?" More formally, the central issues to consider are exposure and effectiveness: "What is our company's level of exposure to the cyber threat risk? And how effective are we at keeping that exposure to within acceptable limits?"

The frequent challenge, however, is that couching the questions in these high-level terms may not always elicit useful answers. That's because, unless a company is already quite sophisticated in its cyber threat risk management practices, it may not yet have the risk management infrastructure and/or governance elements in place to support a meaningful conversation. For instance, leaders may not have agreed on risk definitions, risk tolerances, or metrics specific to cyber threat risk. Or the company might lack the technology tools to effectively collect and report cyber threat-related information.

If an organization isn't yet in a position to discuss exposure and effectiveness as such, we recommend, as a first step, that CIOs and CISOs be prepared to answer four questions about specific information security practices that we believe are essential to effective cyber threat risk management:

- How do we track what digital information is leaving our organization and where that information is going?
- How do we know who's really logging into our network, and from where?

**IT risks and security challenges, a Deloitte perspective as published in the WSJ, CIO Journal**

- How do we control what software is running on our devices?

- How do we limit the information we voluntarily make available to a cyber adversary?

### What's next?

In the next two installments in this series, we'll explore these questions. The measures reflected in these questions aren't the only ones to address relating to cyber threats, but they do represent core elements of an effective cyber defense. This, in turn, makes your organization's practices in these areas a reasonable proxy for the effectiveness of its cyber threat risk management practices overall.

In the fourth and final installment in the series, we'll discuss applying a risk management maturity perspective to address cyber attack issues. Applying such a perspective enables an organization to gain valuable insights into its cyber risk management strengths and weaknesses – as well as into how it might be able to improve its practices.

April 4, 2012, Rich Baich and Henry Ristuccia
Center for Security & Privacy Solutions

1 "Second annual cost of cyber crime study: Benchmark study of U.S. companies," Ponemon Institute, August 2011, p. 1. Available online

2 Ibid

### Contacts

**James Nunn-Price**
+44 20 7303 8708
jnunnprice@deloitte.co.uk

**Vijay Samtani**
+44 20 7303 0132
vsamtani@deloitte.co.uk



Designed and produced by The Creative Studio at Deloitte, London. 24346A