Assurances et gestion des risques
Insurance and Risk Management

Staying safe on your virtual voyage: How to assess your organization's exposure to cyber risk

Barb Szychta

Volume 72, numéro 4, 2005

URI : https://id.erudit.org/iderudit/1106848ar
DOI : https://doi.org/10.7202/1106848ar

Aller au sommaire du numéro

Éditeur(s)

Faculté des sciences de l'administration, Université Laval

ISSN

1705-7299 (imprimé)
2371-4913 (numérique)

Découvrir la revue

Citer ce document

Szychta, B. (2005). Staying safe on your virtual voyage: How to assess your organization's exposure to cyber risk. *Assurances et gestion des risques / Insurance and Risk Management*, *72*(4), 696–698. https://doi.org/10.7202/1106848ar

B. STAYING SAFE ON YOUR VIRTUAL VOYAGE: HOW TO ASSESS YOUR ORGANIZATION'S EXPOSURE TO CYBER RISK

by Barb Szychta

1. Introduction

Part of being competitive in today's business world means having a stake in the ever-expanding cyber universe. But as the virtual world grows, so do the potential sources of risk. We all have a pretty clear idea of the damage a fire or a flood can do. But it can be harder to conceptualize the scope of damages or liabilities that can arise from the technological innovations we count on every day, and often take for granted.

The term *cyber risk* has come to encapsulate a wide variety of potential threats that stem from our transition to an information-based economy. But what do you really need to know about cyber risk? Because sources of cyber risk are continually growing and coming to our attention, it's important not to get caught up in fear-mongering and misinformation. Instead, you can empower your organization through increased awareness about your unique needs and exposures. A realistic awareness of cyber risk is paramount to protecting your network, your clients and your business.

2. Continually evolving risks

CIO Canada magazine has teamed with Athabasca University for the past four years to survey Canadian companies on a variety of IT issues, including security. The survey found that 37 per cent of respondents' companies had at least one serious breach of security in that year; with seven per cent saying they had a serious breach of customer privacy. Even so, only 44 per cent said their organization had a disaster recovery plan.

Most of us are familiar with the potentially devastating effects of viruses and worms, which are growing increasingly powerful. In early May 2004, the Sasser worm shut down the computer system of the North Wales Coast Guard, leaving staff unable to access emergency service contacts stored in its database, while a major bank in Finland was forced to close 120 of its offices to update anti-virus

The author:

Barb Szychta is National Leader, Technology Risk Group, Aon Reed Stenhouse.

software against Sasser. The impact of Sasser spread worldwide, affecting businesses, governments and banking operations in North America, Asia and Australia. Having operations grind to a halt is bad enough, but keep in mind that companies can also be held liable for transmitting a virus.

Since many of us have had personal experiences with viruses we've learned to prepare and to prevent them as best we can. However, emerging threats like cyber extortion and cyber terrorism often go unheeded and might seem a little too "sci-fi" to some. "Distributed denial of service (DDoS)" attacks have run rampant in the online gambling industry, with blackmailers threatening to crash operations if they're not paid. But this kind of cyber-crime has also made its way to the mainstream. Perhaps the most well known case of cyber-extortion occurred in August 2000, when Michael Bloomberg, now mayor of New York City, addressed threats from two hackers who claimed they could compromise his company's global financial information network. The two men had demanded $200,000 in "consultancy fees" for the information, which, like many cyber-extortion demands, is comparatively not an exorbitant sum. It's this reason, as well as the risk to corporate reputation, that many cases of cyber-extortion go unreported. Bloomberg, on the other hand, called in police and was able to thwart the attempts of the hackers.

Hackers can demand money for a variety of threatened actions, including theft of confidential client information and threats to make that information public. As well as client information, confidential corporate information and funds are also vulnerable. Many organizations are now realizing that they have to take stronger steps toward protecting their networks. Like viruses, new forms and methods of cyber-crime are being developed at an increasing rate.

In addition to cyber extortion there are a number of other threats and sources of cyber risk. Even if your company's web site is strictly informative, with no e-commerce operations, its content can be subject to cyber risk. Copyright infringement and libel are just two of the legal implications of web site content that is not strictly monitored. That means that if an outside user posts defamatory material on a web site's bulletin board, the company maintaining the web site can be found responsible.

If a company is found to have an insecure network or becomes the victim of a cyber-crime it can also suffer damage to its reputation and be perceived negatively by the public. Indeed, 51 per cent of the *CIO Canada*/Athabasca University study respondents said they do not report security breeches to authorities. And in many ways it's understandable that companies are hesitant to show their vulnerability.

Just as you wouldn't feel safe entering a building that had fire damage, you'd be cautious entering a virtual structure that had been violated in some way. In addition to losing current customers, companies must invest in winning back the confidence they have lost. However, this common corporate silence can create a false sense of security.

3. What you need to know

Think back five or even two years and consider how our daily lives have changed with technology. It's important to be aware that cyber risk evolves at the same pace as other innovations, possibly even faster. Ahead of each new breakthrough is a way to break it down. That's why balancing risk and reward is so important.

Just as global business operations have been enhanced by technology, perpetrators of cyber-crimes do not fit a single mould and can operate from anywhere in the world. A German teenager was arrested for authoring the Sasser worm, while the cyber-extortionists in the Bloomberg case hailed from Kazakhstan and operated out of the U.K. But attacks don't always come from far a field; disgruntled employees are another likely source of attack.

How then, in such a large and ever-changing playing field, can organizations protect themselves from the numerous threats to their networks? The answer lies in comprehensive cyber risk management that begins with an initial assessment that identifies corporate assets and the risks those assets face. This means examining assets and critical functions within networks, web sites and general computer applications.

How are you prepared, both financially and in terms of capability to deal with any interruptions, losses or attacks? With traditional commercial policies rarely extending into cyberspace, an assessment of coverage is an important step toward security. New specialized policies are emerging that provide coverage for third-party liability (such as damage to third parties from a virus/inadvertent release of confidential information) and for first-party losses (data reconstruction costs because of theft, corruption, deletion, business interruption because of a virus, DDos or cyber extortion demands by hackers).

Identifying the various exposures your company has to cyber risks, as well as assessing your insurance needs, will give your organization the knowledge necessary to separate fiction from reality. Most importantly, your business will be able to move ahead with exciting technological innovations carrying the confidence that comes with sound and realistic preparation.