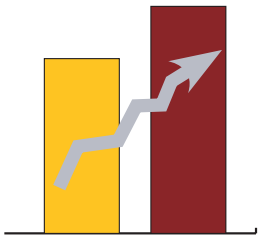
CYBER RISK:
WHAT YOU NEED TO KNOW

The Institutes®

CYBER RISK FAST FACTS

312
data breaches in 2014

23% increase from 2013



The average data breach comprises **1.1** million identities[1]

Average loss per cyber attack:

United States: **$5.85** million[2]

Globally (not including the U.S.): **$3.5** million[3]

Most frequently targeted industries:

- Banking
- Retail
- IT
- Hospitality[4]

---

1 2015 Symantec Internet Security Threat Report, http://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

2 2014 Ponemon Institute Cost of Data Breach Study: United States, http://www.accudatasystems.com/assets/2014-cost-of-a-data-breach-study.pdf

3 2014 Ponemon Institute Cost of Data Breach Study: Global Analysis, http://www.accudatasystems.com/assets/2014-cost-of-a-data-breach-study.pdf

4 Experts Exchange, http://i.imgur.com/7RkfSIP.jpg

CYBER SECURITY TERMS DEFINED

Cyber risk	*Any risk of financial loss, disruption, or damage to the reputation of an organization from some sort of failure of its information technology systems*
Hacktivism	*The practice of gaining unauthorized access to a computer system and carrying out various disruptive actions as a means of achieving political or social goals*
Phishing	*A digital form of social engineering to deceive individuals into providing sensitive information*
Ransomware	*A type of malicious software designed to block access to a computer system until a sum of money is paid*
Data breach	*The intentional or unintentional release of secure information to an untrusted environment*
Cyber security	*Measures taken to protect a computer or computer system connected to the Internet against unauthorized access or attack*
Enterprise risk management	*An approach to managing all of an organization's key business risks and opportunities with the intent of maximizing shareholder value*

A Bit of Background

The conversation around cyber risk is not new. For as long as computers have existed, certain individuals and groups have made it their mission to take advantage of computer users. But as technology has advanced, so too have the capabilities of those wishing to exploit it. Expensive data breaches are on the rise, and some of the world's largest corporations have fallen victim to attacks. Despite their presumably sizeable resources for defense, giants such as Sony, Target, and Home Depot have recently been exposed as vulnerable, seeming to signal that no organization is truly safe from the threat.

The typical media coverage of these attacks focuses on issues around consumer privacy, specific technologies, or legal analyses of the repercussions. This overshadows the crux of the issue. For any organization, attention to cyber risk should not be exclusive to the IT and legal departments. Everyone—from consumers to corporate stakeholders to government officials—should be aware of and prepared for cyber threats.

Cyber Risk and Enterprise Risk Management

Successful organizations have strategies to manage risk. Cyber threats are, primarily, an enterprise risk management (ERM) issue. Although cyber risk is not yet well understood, this constantly evolving risk can be handled through the same disciplined approach as fire, theft, or traditional liability.

ERM involves a six-step, cyclical process:

1. Identify loss exposures
2. Analyze loss exposures
3. Examine feasibility of risk management techniques
4. Select the appropriate risk management techniques
5. Implement selected risk management techniques
6. Monitor results and revise the risk management program

Identifying and Analyzing Exposures

Loss exposures generally fall into two categories: first party and third party. First-party exposures relate to the entity that has been directly attacked, as this party faces reputational damage and revenue loss, post-breach repair costs and costs associated with business interruption, responsibility for notifying customers or other parties affected by the attack, and post-breach repairs.

Third-party exposure relates to liability to those who may suffer damages as a result of the data breach or other type of cyber attack. This can include, for example, liability for loss of privacy regarding customer data, or charges of slander and libel when false information is published during a malicious website hack. Directors and officers may face liability for failing to prepare the organization against a cyber attack; insurance producers can face errors and omissions liability for failing to advise clients about adequate cyber risk coverage.

Choosing Risk Management Techniques

Frequently, risk is inevitable, which is why ERM addresses techniques to help an organization manage its risks. Most risk management approaches can be categorized as risk control or risk financing.

Risk Control

Avoidance—Avoidance means removing the threat in its entirety: you can avoid an auto accident by never getting in a car. While most effective, it is also the most difficult technique to realistically implement. It is not feasible to participate in modern commerce without a connection to the Internet, for example.

Prevention—Instead of attempting to fully eliminate the potential for loss, prevention aims to reduce the frequency of loss. For instance, the use of a password for computers or mobile devices should reduce the number of breaches.

Reduction—Much like prevention, this technique accepts the inevitability of loss and attempts to mitigate it. But instead of targeting loss frequency, reduction targets loss severity. A fire extinguisher, for example, can reduce damage from a fire. If an organization has cyber breach experts on speed dial and a "what if" plan of how to respond to the public in the wake of a data breach, it will recover more quickly than an organization without such a plan.

Separation,Duplication, and Diversification—These related techniques have a common goal of minimizing single points of failure. For instance, keep a duplicate and off-site copy of essential data so that if a cyber breach destroys information, it can be quickly restored.

Risk Financing

Retention—How do you pay for cyber losses? The retention technique recognizes that losses may occur and requires an organization to understand how much exposure it can retain without jeopardizing the ongoing business.

Transfer—As with other types of risk, organizations can manage the potential financial impact of cyber risk by the purchase of cyber insurance policies. As cyber risk evolves, so do cyber insurance policies, and the types of cyber risk coverages expand regularly.

In Closing

Alarm bells go off when decision makers talk about cyber attack but this new threat can be managed in the same way that best-in-class organizations assess and mitigate risk. Managing cyber risk does, however, require a change in organizational thinking, as it cannot be handled effectively by merely delegating responsibility for it to IT or legal units. More useful is a mindset that cyber risk should be managed with an ERM approach, and that it is a company-wide issue requiring cross-functional stakeholder buy-in.

www.TheInstitutes.org