

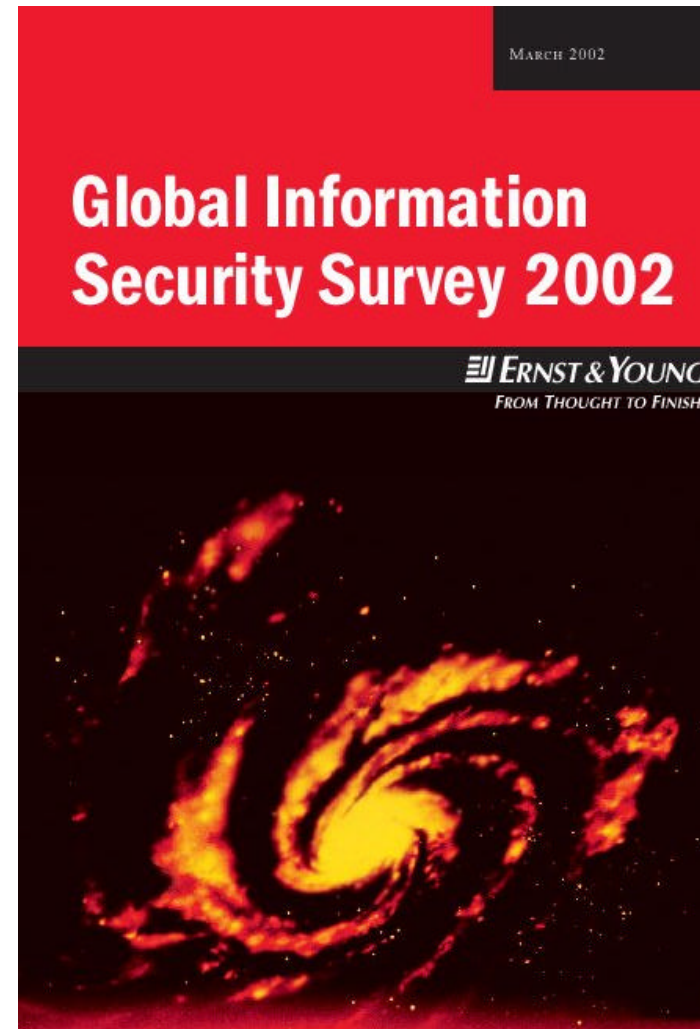
Technology and Security Risk Service

Business Continuity Plan



Perché abbiamo scelto di parlare di BCP

Annualmente E&Y effettua uno studio internazionale presso i propri clienti finalizzato alla rilevazione dello stato della Sicurezza Informatica



Perché abbiamo scelto di parlare di BCP

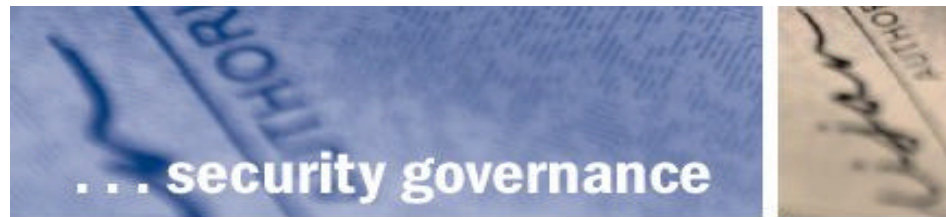
Dall'indagine effettuata tra ottobre e dicembre 2001 è emerso che il BCP esiste soltanto nel 53% delle aziende

Issues at a glance

- Only 40% of organisations are confident they would detect a systems attack
- 40% of organisations do not investigate information security incidents
- Critical business systems are increasingly interrupted - over 75% of organisations experienced unexpected unavailability
- **Business continuity plans exist at only 53% of organisations**
- Only 41% of organisations are concerned about internal attacks on systems, despite overwhelming evidence of the high number of attacks from within organisations
- Less than 50% of organisations have information security training and awareness programmes

There are some **alarming gaps** and some organisations could be judged **irresponsible** in their approach to information security, the management of which is now critical to **business survival** and **competitive advantage**

Perché abbiamo scelto di parlare di BCP



è emerso inoltre che il 70% delle aziende prevede di implementare il BCP e l'IT disaster recovery.

Come seconda problematica con il 61% segue quella di razionalizzare i progetti IT

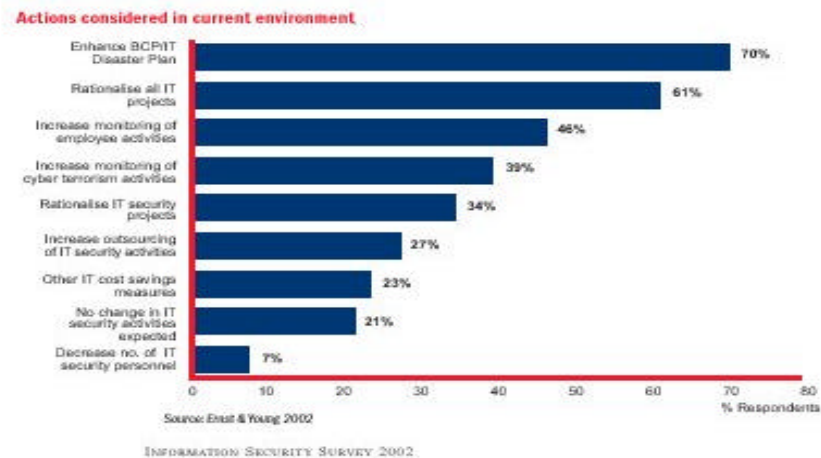
culture. It must be a living document which drives tactical and operational decisions in all business areas. Components often overlooked are training and awareness, sourcing strategy, and performance and assurance measures.

Wherever the budget sits, it must be communicated and monitored if proper control and return on investment is to be achieved. If this is not the case, there may be a lack of visibility of the overall commitment and spending priorities and spend may be duplicated unnecessarily. In addition, it can result in unexpected additional expenditure during the year. For example, implementation speed may be in the business unit budget, but support and maintenance is expected to come from the IT budget, yet neither include security related elements.

If budgets are perceived to be sufficient for the short term, the questions to ask are:

- 1) whether this view is based on an informed and objective business-based assessment of threats and vulnerabilities; and
- 2) whether there is true visibility of the spend and its relevance to business needs.

70%
of organisations
plan to enhance
business continuity
and IT disaster
recovery plans



Le principali cause di indisponibilità dei sistemi:

Dall'indagine effettuata è emerso che :

56% Hardware/Software Failure

49% Telecommunications Failure

26% Problemi di terze parti

è emerso inoltre che

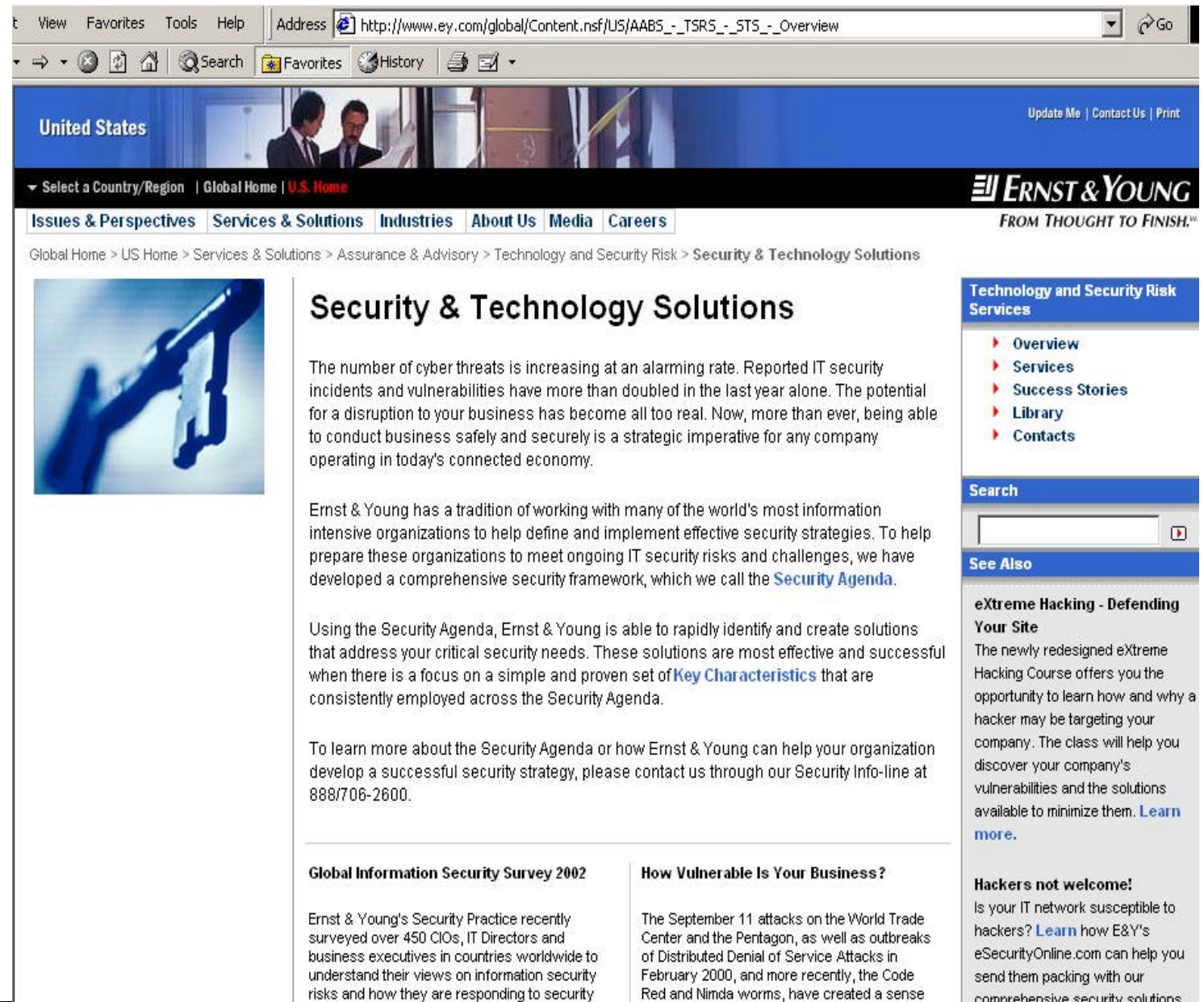
il 40% delle aziende che ha un BCP non ha effettuato la Business Impact Analysis e il 21% non lo ha testato.

Le aziende che hanno un Disaster Recovery Plan sono il 71% e di queste il 16% non lo ha testato.

e dopo aver deciso di esporre la nostra conoscenza delle problematiche di BCP è pervenuto a molti Istituti di Credito il questionario di Banca d'Italia in cui vengono chieste informazioni circa i piani in essere

e questo ha reso ancora più attuale la problematica.....

Sul nostro sito
www.ey.com
effettuando la
ricerca di
"Security Survey"
è possibile fare il
download del file
in formato acrobat
con tutte le
informazioni che
Vi ho esposto sino
ad ora



United States Update Me | Contact Us | Print

Select a Country/Region | Global Home | **U.S. Home**

Issues & Perspectives | Services & Solutions | Industries | About Us | Media | Careers **ERNST & YOUNG**
FROM THOUGHT TO FINISH.™

Global Home > US Home > Services & Solutions > Assurance & Advisory > Technology and Security Risk > Security & Technology Solutions

Security & Technology Solutions

The number of cyber threats is increasing at an alarming rate. Reported IT security incidents and vulnerabilities have more than doubled in the last year alone. The potential for a disruption to your business has become all too real. Now, more than ever, being able to conduct business safely and securely is a strategic imperative for any company operating in today's connected economy.

Ernst & Young has a tradition of working with many of the world's most information intensive organizations to help define and implement effective security strategies. To help prepare these organizations to meet ongoing IT security risks and challenges, we have developed a comprehensive security framework, which we call the **Security Agenda**.

Using the Security Agenda, Ernst & Young is able to rapidly identify and create solutions that address your critical security needs. These solutions are most effective and successful when there is a focus on a simple and proven set of **Key Characteristics** that are consistently employed across the Security Agenda.

To learn more about the Security Agenda or how Ernst & Young can help your organization develop a successful security strategy, please contact us through our Security Info-line at 888/706-2600.

Global Information Security Survey 2002

Ernst & Young's Security Practice recently surveyed over 450 CIOs, IT Directors and business executives in countries worldwide to understand their views on information security risks and how they are responding to security

How Vulnerable Is Your Business?

The September 11 attacks on the World Trade Center and the Pentagon, as well as outbreaks of Distributed Denial of Service Attacks in February 2000, and more recently, the Code Red and Nimda worms, have created a sense

Technology and Security Risk Services

- ▶ Overview
- ▶ Services
- ▶ Success Stories
- ▶ Library
- ▶ Contacts

Search

See Also

eXtreme Hacking - Defending Your Site

The newly redesigned eXtreme Hacking Course offers you the opportunity to learn how and why a hacker may be targeting your company. The class will help you discover your company's vulnerabilities and the solutions available to minimize them. [Learn more.](#)

Hackers not welcome!

Is your IT network susceptible to hackers? [Learn](#) how E&Y's eSecurityOnline.com can help you send them packing with our comprehensive security solutions



andrea.berna@ernst-young.fr
francesco.blanco@it.eyi.com
tsrs.ey@it.eyi.com