Key facts about risk

Risk statistics

Citicus ONE risk and compliance management software implements a research-based approach to measuring and managing information risk, and applies the same principles to other areas of operational risk. The research is conducted via face-to-face case studies, evaluation of incidents, work group meetings and statistical analysis of data about controls applied to – and incidents suffered by – information resources of various types.
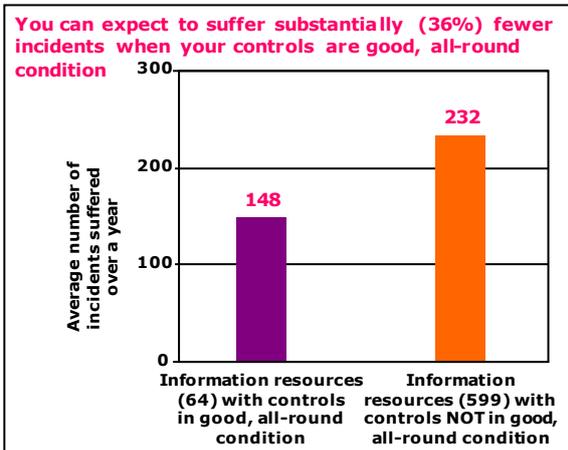
In the main these information resources are, or support, mission-critical business applications.

Rigorous analysis, using techniques pioneered by Citicus staff, reveals that the secret of success in driving down information risk is achieving a 'good, all-round level of protection'.
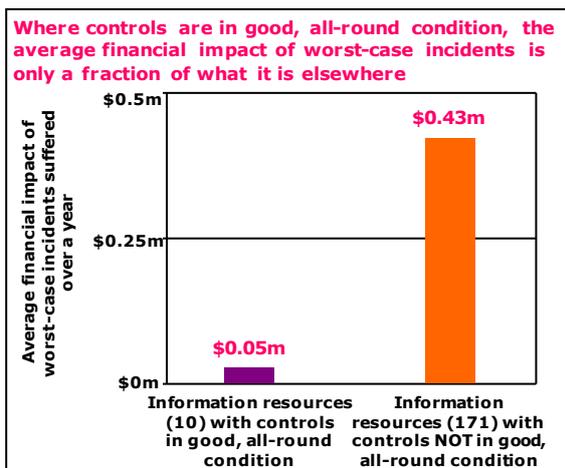
The advantages of achieving such protection are shown by the top three charts on this page

This desirable state is surprisingly achieved by only about 1-in-12 surveyed information resources – hence the drive for better risk management.
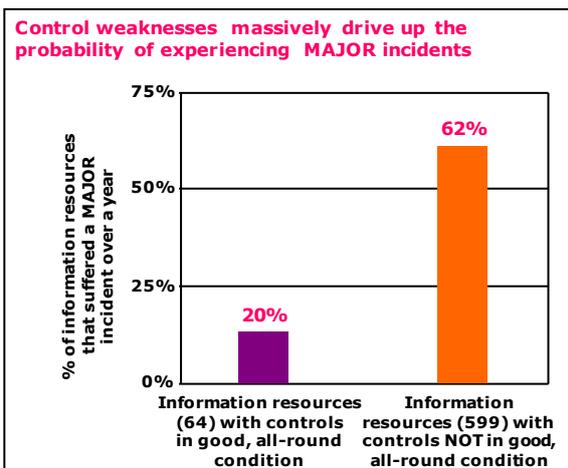
The charts at the foot of the page illustrate key facts about incidents (ie events that compromise the confidentiality, integrity or availability of data) and their relationship with the status of controls.

You can expect to suffer substantially (36%) fewer incidents when your controls are good, all-round condition

Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's information security status survey.

Where controls are in good, all-round condition, the average financial impact of worst-case incidents is only a fraction of what it is elsewhere

Source: Citicus analysis of 181 worst-case incidents affecting 181 information sources 'on the ground' covered by the Information Security Forum's information security status survey.

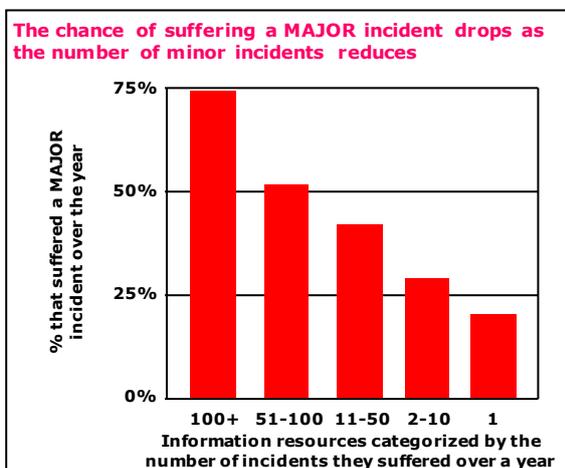**Control weaknesses massively drive up the probability of experiencing MAJOR incidents**

Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's information security status survey.

The chance of suffering a MAJOR incident drops as the number of minor incidents reduces

Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's information security status survey.

Accidents are by far the most common type of information incident suffered over a year
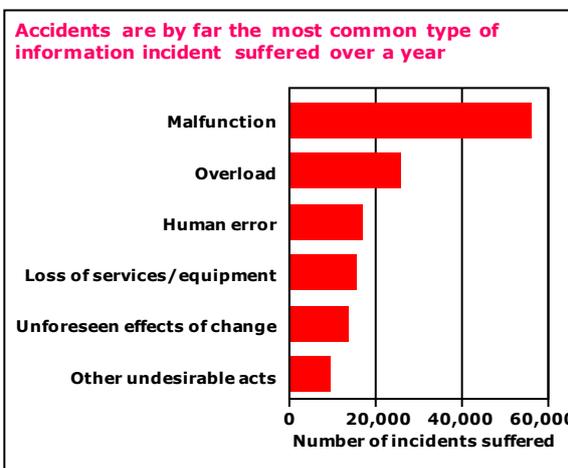
Source: Citicus analysis of 139,000 incidents affecting 558 'live' information resources 'on the ground' covered by the Information Security Forum's information security status survey.

What the statistics show

The figures presented on the previous page emerged from rigorous analysis of the world's largest source of hard fact on the chances of business critical systems 'going wrong' - the Information Security Forum's biennial information security status survey.

They show that incidents are disturbingly common and, while most have minor impact, some can have very serious consequences; and the cumulative effect of such incidents significantly erodes profits and makes enterprises underperform.

The research evidence shows that by getting controls in good shape, your organization can not only reduce the information risk it faces: it can save substantially - since as well as reducing the chance of suffering major incidents, good controls cut the number of minor incidents suffered day-to-day, and the inefficiencies that go with them.

Thus the benefits of driving risk down are substantial.

Key success factors for risk management

As well as looking at the statistical evidence, the research behind the Citicus methodology examined factors that had caused risk management initiatives both to fail and to succeed in a wide variety of case-study organizations. These factors are outlined in the following two tables.

The causes of failure	
Over-complex approaches to risk assessment	✗
Inability to measure risk objectively	✗
Turf wars between departments	✗
Lack of tools to automate the process in a reproducible way	✗
Lack of co-operation on the ground	✗
Lack of resources to drive and run the risk management initiative	✗
Immature processes and reporting structures	✗

The secrets of success	
Keep risk fact-gathering simple	✓
Ensure your risk management process is constructive rather than blame-oriented	✓
Produce meaningful results that capture the attention of busy decision-makers	✓
Show that incidents are not an inescapable feature of business life	✓
Introduce an element of competition across the enterprise	✓
Make risk management a personal responsibility	✓
Cause pressure to filter down so it motivates others to act	✓
Get the organizational arrangements right	✓
Highlight where to focus scarce resources	✓
Gain top management commitment	✓

So in essence, the key to effective risk management is **behaviour**: to drive risk down you've got to **motivate and equip people** to do it.

This objective is manifested in the **two-phase constructive risk management process** supported by our web-based risk and compliance management software, **Citicus ONE**.

Citicus ONE is specifically designed to help our customers put these core principles into effect.

For further information

If you are interested in learning more about Citicus Limited or our flagship risk and compliance management software, you are welcome to contact us as follows:
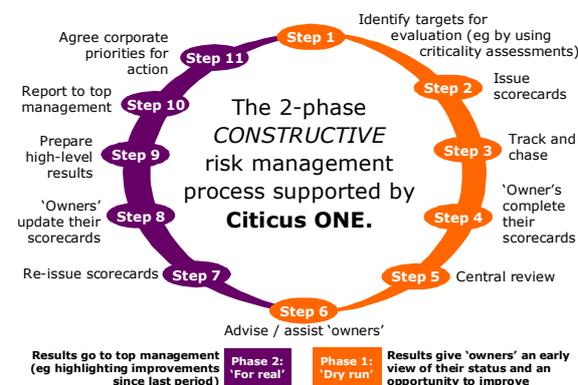
Direct contact

Simon Oxley, Managing director
E-mail: simon.oxley@citicus.com
Tel: +44 (0)1729 825 555

Sian Alcock, Director
E-mail: sian.alcock@citicus.com
Tel: +44 (0)20 7866 8116.

Head office

Citicus Limited
71-75 Shelton Street
Covent Garden
London WC2H 9JQ
United Kingdom.
E-mail: info@citicus.com
Web: www.citicus.com
Tel: +44 (0)20 3126 4999