To err is human

Paul Brettle explains how intelligently deployed technology can help minimise the risk of human error to business

People make mistakes. That is a fact. Fortunately, reliable and automated IT systems will increasingly continue to take on some of our responsibility in circumstances where managing error is critical. That human element, however, still goes into the design and management of business critical systems, which means inevitably that problems can be built into our most vital IT infrastructure. So how do we manage this inherent risk to ultimately secure information flow?

An important initial consideration is that as an organisation’s dependence on technology increases, the potential impact of error grows. April’s four-day Blackberry network outage, for example, hit global business heavily both financially and in terms of reputation, despite the parent company RIM’s best efforts to keep the network intact. RIM spends millions of dollars a year to avoid downtime, yet someone somewhere, probably at a Network Operations Centre, made simple, human mistakes that caused a non-essential system routine to withhold network access to over five million enterprise users. Up to 80 per cent of Blackberry users polled online reported disruption to their operations.

Hackers who stole 45 million customer records, including credit card details from TJX, the parent company of TK Maxx, had benefited from the fact that an individual had made the decision that Wired Equivalent Privacy, one of the weakest wireless LAN security technologies available, would be sufficient to protect that section of the network. It was estimated at the time that the blunder may cost the company more than $8 billion.

The importance of reducing and eliminating business and financial repercussions of human error is obvious. Unfortunately, the truth is we cannot eliminate human error entirely, so the answer is to take reasonable steps to ensure that errors are less common and that their impact is reduced.

One way of minimising the error of risk is to simplify controls. Vendors and businesses tend to build increasingly complex bespoke management systems into IT systems. But increasing complexity – by raising the number of options available or including multiple control points – also increases the chance of error.

The simplest method of reducing the opportunity for a human mistake is to cut down two factors: the time it takes to react to a mistake should one occur; and the opportunity to make a mistake in the first place.

The requirement for continuity also means that we need a form of management system powerful enough to carry out issue resolutions across multiple devices. This enables administrators to work quickly through a single device in a single location. To minimise the likelihood of human error, we must also ensure these systems support some form of workflow process to steer administrators, prompting and advising on status and progress.

Taking the example of a distributed organisation with multiple locations and a requirement for high-availability (a typical medium to large business), a centralised management console can provide an overview over a whole network, provide advance warning of problems, a centralised problem resolution capability and manage bandwidth across the business, taking into account high-risk areas outside the perimeter of the business and internal networks too.

The diagram to the right shows how secured, optimised, and resilient connectivity can be established across internal and external networks, providing secure information flow to business VPNs, including mobile devices and remote locations. It also shows the areas centralised management can control.

However, a small mistake by a novice user could potentially affect many systems across a wide territory, causing big problems. So an effective common platform needs to provide, at least:

• tiered access to rule-bases to ensure that not all abilities are available to all users, enforcing hierarchical authorisation and access rights;
• a fully transparent audit trail of all users and actions carried out within the system allowing any mistakes to be tracked, stored and easily rectified; and
• rigorous checks and blocks of actions that could impact critical systems and be detrimental to overall service, with visual prompts for administrators.

Accepting a certain level of risk to IT systems is unavoidable. So intelligent management technology and people is just as important than prevention in managing the impact of human error.

Paul Brettle is UK & Ireland technical manager for Stonesoft