

SECURITY ROUNDTABLE:

The price of a smooth run

IT executives at an *MIS Asia* roundtable on security agreed that formulating a comprehensive programme to keep the enterprise running and make a quick recovery in the event of a disaster is everyone's business. By **Jonathan Hopfner**.

An unfortunate side effect of technology playing an ever more vital role in most businesses is that increasingly all eyes turn to the IT department when something goes wrong. Whether external threats such as natural disasters, identity theft and hacking attacks, or poor user practices that create internal vulnerabilities, rarely have IT executives been called on to fend off so much.

And when disasters do occur, enterprises expect everything to be back up and running at lightning speed, conscious of the damage that downtime can inflict on their brands and reputations. The chief problem, noted many of the delegates to a recent *MIS Asia* roundtable on security held at New Delhi's Oberoi Hotel, is that business leaders often want this responsiveness at minimal cost.

"We are a 24 by 7 industry, and business continuity is of prime importance to us, because we are a luxury brand and would never want to be faced with a situation where I have to tell my customers, 'Sorry, my system is down,'" says Indrani Ghose, vice-president of IT at EIH, a member of the Oberoi Group. "More than the internal customers I serve, it's my external customers who are really important."

With over four plants, some 120 sales offices and a presence throughout Asia, tyre manufacturer JK Industries must be on call to interact with its clients 365 days a year, says SS Sharma, the firm's general manager of IT.

"You can imagine what kind of impact the loss of

information services would have on our business. We can't afford for IT to be non-operational for even one hour," he adds.

How much is too much?

The importance of constructing a secure IT architecture that minimises instances of downtime and supports business processes even in times of crisis seems to be clear. Unfortunately, some delegates noted, many business heads are reluctant to allocate the investment that comprehensive business continuity and disaster recovery strategies require.

"We're right in the thick of building a disaster recovery plan and find we're continually having to outweigh the cost," notes Manish Gupta, general manager of IT at appliance maker Whirlpool India. "Disaster recovery and business continuity plans are

always regarded as a cost; there's an investment involved for backup and storage that may never be used. Some business owners don't want to buy into that, and there are expenses that will always be resisted by user departments."

"There are places where (IT) reports to finance, and it hampers the process, you have to do a lot of convincing that spending on security is necessary," adds SK Dey Biswas, a deputy director-general responsible for IT at the Indian Council of Medical Research. "This costs valuable time, and sometimes the decisions get diluted."

His experiences have led Biswas to believe that ideally, when it comes to security, IT should be accountable to nobody.

"I'm of the view that the (IT) department should be stand-alone," he says. "If it's a centralised IT setup,

"Five to seven years ago, a lot of Indian companies didn't have this mindset, that you need disaster recovery and business continuity."

—Indrani Ghose, vice-president, IT, EIH, a member of the Oberoi Group



Manish Gupta



Indrani Ghose

then everybody else is a user and you're providing a service. So in that sense, the department should be able to make its own decisions rather than depend on a user, which is just another level of bureaucracy. Since I have to find solutions to my problems myself, what's the use of reporting to somebody? We report to non-IT people and after we explain a problem we have to convince them that investment is necessary, and then they try to cut the costs involved."

According to John Mulligan, director, planning and engineering at AT&T Asia Pacific Group, such experiences highlight the need to phrase business continuity and disaster recovery investments in stark financial terms.

"You're saying you'll go down for a day and have to work manually, the business is saying 'No, don't,' so you say OK, it'll cost this many dollars not to, now what's the value," he explains. "This is part of designing an overall business plan; if my IT processes take a certain percentage of revenue, that's what business continuity is. You have to look at how much (downtime) is going to cost. (The investment) is a joint business decision, site by site, throughout the company."

SS Sharma adds that business buy-in can only really be secured if IT has a proven, integral role within the enterprise.

"Where information security is concerned, the involvement of the management is of prime importance. Without this, it will be very difficult to implement throughout the entire organisation," he says. "If IT is totally woven into the business processes, then the management will put prime importance on

security and business continuity. If business processes are going to stop (without IT) then the value will be there in the mind of the management."

IT managers such as Gupta have tried to address the costs associated with security by implementing shared services programs under which user departments are charged for the disaster recovery services they need. But this, he admits, leads to the problem of deciding "what (costs) should be shared and what should be charged back."

Another option, notes Ghose, is engaging an outside service provider to provide backup or storage facilities.


"You can look at data centre services, because today the option is there, and you can pay on an annual basis," she says. "In a lot of cases people are not willing to make that initial capital expenditure, so you can consider leasing hardware if you are unable to make your own investments."

Appreciate what you have

Regardless of the shape a company's security and disaster recovery plans take, delegates were virtually unanimous in their agreement that the first and most difficult step is prioritisation. As no organisation can hope to plug all the loopholes in its defences, any security or business continuity programme must target those areas most vital to the survival of the business.

"It's very important that you look at all your assets, people, software, licences, and have a formal evaluation of them," says Vivek Jain, information security officer at software developer HCL Technologies.

In HCL's case, this involved all the executives



"The first thing to do is decide for your organisation what is mission critical, what your customer needs to have 24 by 7."

—John Mulligan, director, planning and engineering, AT&T Asia/Pacific Group



“There are places where (IT) reports to finance, and it hampers the process, you have to do a lot of convincing that spending on security is necessary. This costs valuable time, and sometimes the decisions get diluted.”

—SK Dey Biswas, a deputy director-general responsible for IT at the Indian Council of Medical Research

heading the company’s various business units and even some external customers, allowing the company to place a value on virtually all its IT assets and services, though this value is not necessarily financial.

“The values we have are availability, whether something needs to be available at all times, and integrity, whether integrity is of critical importance,” he explains.

SK Sharma, vice-president, systems at Engineering Projects India, says security-related spending must be proportionate to the “needs and value of the data” that a user has. VK Paliwal, general manager of IT at transportation infrastructure firm Ircon International, agrees that IT should support security “on a needs basis”.

“We have to identify what information will have an impact on our business and what information is not going to harm the company if it’s being shared,” SS Sharma adds. “Any information which is to be secured has to be cost-evaluated, and any information system should set out the confidentiality of the information, its integrity, availability, and last and most important, accountability.”

AT&T’s Mulligan notes that the difficulty of measuring the value of different sets of data or services is compounded by the fact that enterprises’ concerns are constantly shifting.

“The first thing to do is decide for your organisation what is mission critical, what your customer needs to have 24 by 7,” he says. “Some



SK Dey Biswas

Senior IT executives at the security roundtable

- **INDRANI GHOSE**, vice-president, IT, EIH, a member of the Oberoi Group, a hotel chain
- **SK SHARMA**, vice-president (systems), Engineering Projects (India), an integrated engineering firm
- **VIVEK JAIN**, information security officer, HCL Technologies, a software developer
- **SK DEY BISWAS**, deputy director-general (senior grade), Indian Council of Medical Research
- **VK PALIWAL**, general manager (IT), Ircon International, a transportation infrastructure firm
- **SS SHARMA**, general manager, IT, JK Industries, a tyre manufacturer
- **MANISH GUPTA**, general manager, IT, Whirlpool of India, an appliance manufacturer
- **JOHN MULLIGAN**, director, planning and engineering, AT&T Asia/Pacific Group, a networking and communications solutions provider

Moderator: John Lui, editor, *MIS Asia*

departments in the company may think what they're doing is mission critical and they may want it 24 by 7, but it may not really be a mission critical item when you look at the whole organisation. It's a living process that moves quarter on quarter, year on year. You can't do a business continuity process that encompasses the entire lifeblood of your organisation, put it on the shelf and not look at it for five years, because the next year you're a different organisation with different priorities."

EIH's Ghose points out that a company's most precious information assets are often impossible to secure as they rest with the firm's employees.

"What's of prime importance to us is our customer data; the history that we have collected over these many years on our various customers and the different market segments we serve," she says. "How do we prevent our existing employees from walking out with all that data? This is something we're looking at now as turnover in the (hotel) industry is very high and competition is very stiff. External security threats are of course there for everybody but I think internal security is a greater concern. I honestly don't have a good answer to this problem."

Security is everyone's job

Ultimately, says Gupta, companies must realise that the responsibility for business continuity in times of crises extends far beyond the IT department.

"Disaster recovery is really completely separate from business continuity," he notes. "User departments should just continue with the business even when the systems are down, use manual forms or



SS Sharma

other backup devices, just get on with it. They should not be pointing fingers at the IT department."

"But disaster recovery is something that should ultimately be with the IT department," Gupta adds. "After the system is back up, there should be a procedure in place to put (manual data) back into the system. You should have a system of instant backup in place to save your assets."

Other delegates agreed that security and business continuity must be viewed as enterprise-wide processes rather than the tasks of a single department, and that these practices depend more on people and corporate culture than technological solutions.

"I'm constantly trying to convince authorities that security is not something that you read about in a book and implement," notes Biswas. "Every organisation has different security needs."

"Internally for us, business continuity is a philosophy. It permeates everything we do, from when we're assigning services, to opening new offices. We have it built in to the culture of the company," Mulligan says. "The most important thing with business continuity is engaging your whole organisation ... the enabler of business continuity is technology, but it's an overall business issue, in terms of the end goal of continuing to seamlessly provide services to our customers."

Though the path to a more secure, disaster-ready enterprise is a challenging one, expanding regulatory requirements and an increasingly competitive business environment means organisations ignore it at their peril.

"We have to re-look at our complacency," says Ghose. "Five to seven years ago, a lot of Indian companies didn't have this mindset, that you need disaster recovery and business continuity. It's basically another form of insurance, especially with the competition coming in, business needs, and the timelines for getting products to market shortening so much." ■



Vivek Jain

This roundtable was kindly sponsored by AT&T.