Holistic risk management: perspectives from IT professionals

An Economist Intelligence Unit research program commissioned by IBM

Meet the experts

Nicko van Someren is chief techology officer of Good Technology, a provider of secure mobile solutions.

Joseph Robinson is global business continuity manager of Navistar, a global manufacturer of commercial and military trucks, diesel engines, parts and other vehicles.

Chris Gibson is the chair of Forum of Incident Response and Security Teams (FIRST), an international confederation of trusted computer incident response teams.

Introduction

Global organizations are increasingly emphasizing business resilience, that is, the ability to adapt rapidly to a continuously changing business environment. This movement has led to important changes in the roles of IT professionals as they become progressively more engaged in managing all types of risk confronting the organization.

That was the conclusion of *Key trends driving global business resilience and risk*, a report written in September 2011 by the Economist Intelligence Unit for IBM ¬based on an EIU survey of nearly 400 executives worldwide. That study also found that traditional business continuity plans—typically with a strong IT focus – remain critical, even as they become part of a bigger picture and senior executives strengthen their oversight of enterprise-wide risk management.

Nearly two-thirds of respondents polled in the survey agreed that senior IT executives are expected to play a stronger role in developing their organization's business resilience strategy. This perception was even more pronounced among CIOs and technology directors, with only 12% disagreeing. *Holistic risk management: perspectives from IT professionals*, a follow-on study, takes a closer look at these findings through an IT prism. This report examines how the drive toward more holistic risk management is affecting the day-to-day work of business continuity planners, IT risk managers and security executives.

This report was written by the Economist Intelligence Unit (EIU) on behalf of IBM. The EIU also conducted the interviews. The report is based on the findings of *Key trends driving global business resilience and risk*, an IBM study conducted by the Economist Intelligence Unit in 2011 to investigate how organizations are increasingly adopting integrated business resilience strategies in an uncertain environment.

Economist Intelligence Unit

Business continuity in a world of interrelated threats

In *Key trends driving global business resilience and risk*, survey respondents were split nearly evenly on the following question: "Is business continuity primarily an IT issue?" Surprisingly, the views of senior IT executives mirrored this dichotomy, with 47% agreeing with the above proposition. Risk management specialists interviewed for our current report suggest that the dichotomy reflects the fact that a single external event can result in multiple aftereffects that ripple across the business infrastructure. This blurs the distinctions between IT security and other operational threats.

Nicko van Someren, chief technology officer at Good Technology, a provider of secure mobile solutions, explains, "If you view all these risks [IT security and other operational threats] in a set of silos, then it is hard to work out which ones are priorities for risk mitigation investments because [in reality] they are interrelated." He notes, for example, that a flu pandemic would cause many employees to work from home, which would put stress on IT systems while simultaneously making it harder for customers to conduct business. Similarly, if Canary Wharf, a major UK business district, were to be evacuated because of a bomb scare, traffic chaos could disrupt businesses in London's financial sector in multiple ways. "People are viewing IT security and other threats in a more holistic way," Dr. van Someren says, "because this gives them a better picture of the whole risk curve."

These risk interrelationships are magnified by the impact of globalization. Joseph Robinson, global business continuity manager for Navistar Inc, says that as a company's global footprint grows, "executives recognize not only that their risk profile is expanding but also that they are being affected in new ways." While this obviously includes IT security, he says, business continuity practitioners need to integrate other types of risk such as those related to supply chains, facilities, personnel and logistics. "As a manufacturer, logistics is especially important to us," he says. "We have particular

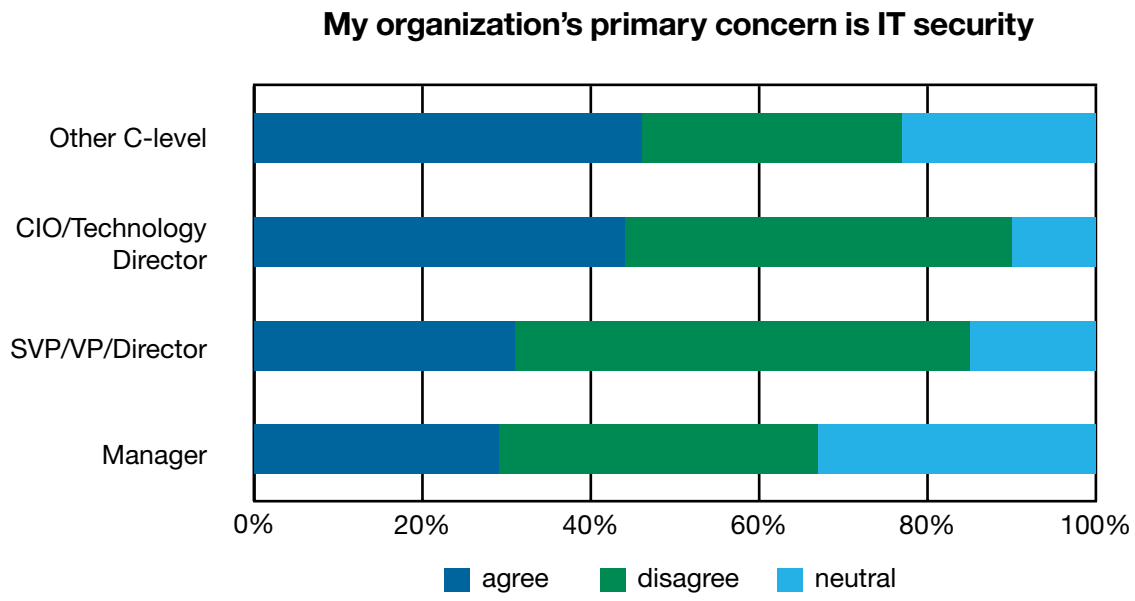

Figure 1. C-level executives are more inclined to equate risk management with IT security.

routes that we take for supplies, we use particular ports and border crossings and they have just as much impact on our business as an IT system would. This is causing a long-term shift away from different risk management functions operating in relative isolation toward a much stronger focus on simultaneously managing a larger number of risks."

A broader role for IT

IT security and business continuity specialists agree that their expanding engagement in all forms of risk management is changing the way in which they do their jobs (Figure 1). They face an array of challenges ranging from broad trends in the risks confronting the enterprise to developments within their own specialties. And they must find solutions in a setting where senior management is increasing its oversight of the risk management process.

A new collaboration style

The trend toward more holistic risk management requires not only an increase in day-to-day collaboration among all types of risk managers, but also a different style of collaboration. Mr. Robinson says that this is especially true in large organizations, which are more profoundly affected by globalization. They require greater interconnectedness among different parts of the organization and business lines than do smaller firms. "As business continuity practitioners, we go in and say, 'we are here to help you, so show us how we can best do that,' says Mr. Robinson. "This represents a shift away from the traditional policy-driven approach where executives would buy into something and say, 'yes, yes, do this – everyone is going to comply with this.' It is a cultural change to get people to see the reward of business continuity and overall risk management."

"Given the complexity of IT security, we have produced some fairly substantial processes around risk management and now we are taking them to other parts of the business."

-Chris Gibson, Chair, Forum of Incident Response and Security Teams

This new collaborative style applies just as strongly to IT security specialists (Figure 2). Traditionally, the IT function was inclined to service business functions the way it believed they needed to be serviced, with ready-made solutions, according to Mr. Robinson. "Now they [IT security

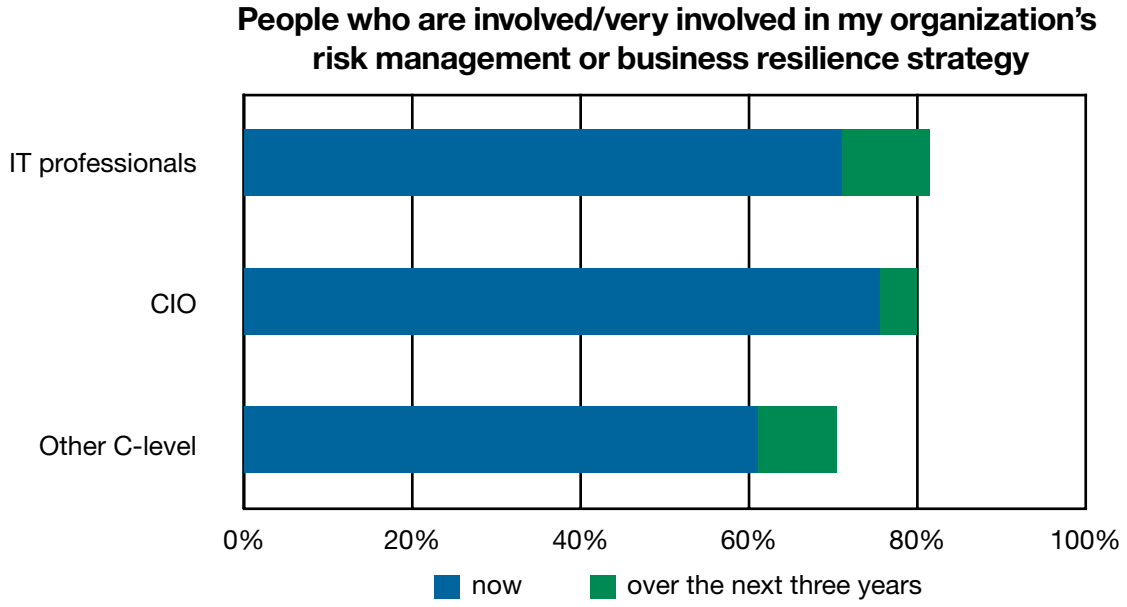

Figure 2. The new collaborative style of addressing risk and resilience strategies extends from the C-suite to IT.

specialists] are coming to the table as partners more often than they have in the past," he says, so there is a greater need to interact with business managers to understand where IT can have the greatest impact. "In the end it is all about the business; if IT cannot speak the language of the business and create plans that make sense to the business, then IT is not going to have a seat at the table," says Mr. Robinson.

Track important trends in organizations' integrated resilience and risk strategies, including the place of security and cloud, by downloading the 2011 IBM Global Business Resilience and Risk study.

Dr. van Someren of Good Technology adds that this is becoming an even bigger challenge as risk assessment methods become more quantitative: "An IT person might tell you, 'we must put our cryptographic keys in a hardware security module,' and maybe they will get some budget for that. But the broader questions for the enterprise are: What are the threats if we don't do that? What are the chances of those threats occurring? What are the costs if those threats are realized? And unless IT can talk about those things in the same terms as everybody else in the risk management room, it is very hard for them to make their case."

The voice of IT professionals in driving risk management strategies is strengthened by their ability to contribute powerful risk management tools. "I see value in bringing those people into broader discussions and getting them involved in areas that traditionally they may not have been," says Chris Gibson, chair of the Forum of Incident Response and Security Teams (FIRST). "Given the complexity of IT security, we have produced some fairly substantial processes around risk management and now we are taking them to other parts of the business. We are helping managers to look at their risks in a process-driven way, not just holding up a finger in the air to try to sense where the threats are."

The compliance challenge

Another consequence of globalization is a sharp rise in the number of regulations constraining business operations. Compliance issues mostly highlight problems that would need to be addressed anyway, as they affect revenue, profits and corporate reputations. "Compliance is always an issue and can force change where businesses didn't necessarily see the risks before," Mr. Robinson says. "But compliance for the sake of compliance does not change the way we look at risks. Non-compliance is the risk that is being managed, and committed risk management occurs most often when executives have lived through the impact of a poorly managed risk." This view may explain the Economist Intelligence Unit's survey results in which a relatively low 60% of CIOs and technology directors said that compliance management was part of their organization's formal risk management strategy.

"Compliance is always an issue and can force change where businesses didn't necessarily see the risks before."

-Joseph Robinson, Global Business Continuity Manager, Navistar, Inc

Mr. Gibson cites the 2011 Avian influenza scare as an example of how the actions of regulatory authorities sometimes prompt companies to look at risk in different ways. "We went

through a number of exercises with government regulators in the UK," he says. "They came in and said to the banking community, 'if 10% of your staff weren't here, what would happen?' We went through a whole process of how we would cope and developed contingency plans, and an awful lot of that was impacting IT."

Yet regulatory compliance can hinder responses to IT security incidents. Mr. Gibson points to laws governing the privacy of individuals' personal information as a particular challenge. "About 90% of all the IT security incidents we see involve the Internet Protocol," he says. "Hackers will break into systems all around the world, naturally with little concern for regulations. However, in terms of any subsequent investigation, if the information involved could identify an individual, in many countries due to privacy laws we are unable to log in remotely and forensically review the affected systems. That fragments the investigation." According to Mr. Gibson, while privacy is a high priority for IT security personnel, policy could affect global companies that are looking to reduce the number of data centers they operate.

Tracking emerging threats

The impact of globalization isn't the only thing "keeping IT security specialists awake at night." Several other trends are affecting their jobs. IT systems are becoming increasingly complex, especially Internet-based systems that are expected to feature ever-new functionality. "Data security is a huge issue for FIRST members," says Mr. Gibson. "Everybody wants the latest whiz-bang web features, but they can jeopardize security. We want our staff to be able to work with the latest technologies in the safest way possible.

This challenge has become more daunting as would-be miscreants are increasingly sophisticated. "A number of years ago all they wanted to do was deface your website," Mr. Gibson says. "But now they want [to get] inside and we see financially driven intrusions much more frequently." He adds that even a minor attack on a website can create reputational risk. IT security experts also have to consider that it may actually be a smokescreen for something more nefarious. "They have taken all the lessons we have learned about encryption, so even if we find their software, it will be harder to discover exactly what they have ex-filtrated," he says.

"Everybody wants the latest whiz-bang web features, but they can jeopardize security."

-Chris Gibson, Chair, Forum of Incident Response and Security Teams

---

Awareness of threats to supply chain logistics has also grown, especially for manufacturers. Mr. Robinson of Navistar points to the tsunami in Japan in 2011 as an example of how a localized event can affect supply chains worldwide. "Now everyone is asking whether we have been doing the right thing with supply chains and that is causing a lot of re-evaluation," he says.

Mr. Gibson offers another example of how companies are trying to better anticipate and plan for emerging threats. The 2012 Olympics will be held near London's financial district. "Travelling to and from central London will be challenging," he says. "We are looking into flexible-working measures and we expect many companies to adopt these in the run-up to the games." He notes that the solution involves more than just asking people to work from home, since that often requires an increase in network capacity and remote access may introduce new security risks.

Dr. van Someren sees another emerging security challenge as the nature of IT organizations changes. "There is less ownership of hardware and more use of virtualized services," he says. "So server hardware management can be almost completely delegated, while at the client end, there is a move toward getting users to bring their own devices." This opens up new opportunities, he says, but also brings a host of new threats. "We need to build solutions that are more tightly wrapped around the enterprise data and separate enterprise applications from personal applications," he says. "If you do that, you can achieve the productivity and usability gains you were after while still maintaining a high level of control over the enterprise data."

"We need to build [bring your own device] solutions that are more tightly wrapped around the enterprise data and separate enterprise applications from personal applications."

- Nicko van Someren, Chief Techology Officer, Good Technology

---

Selling solutions internally

Silos within the organization are the most important single barrier to implementing a holistic approach to business resilience planning, according to 28% of survey respondents. But breaking down those silos through improved collaboration is only part of the answer. In an environment where resource constraints go hand-in-hand with expanding risks, selling solutions to senior management is an even bigger challenge. More than half of survey respondents noted three related obstacles: budget limitations (20%), inability to predict accurately return on investment (ROI) from improvements (17%), and lack of C-level vision and commitment (14%). Financial limitations are an ongoing reality, but a perceived lack of commitment from the C-suite may boil down to failure to present effective proposals.

"If individual risk management units are going up to the executives and competing for limited resources, then we are not going to get the things covered that are really the most important to the business."

-Joseph Robinson, Global Business Continuity Manager, Navistar, Inc

---

In his role as global business continuity manager at Navistar, Mr. Robinson consults with the company's enterprise risk manager to place operational threats in context with financial and other risks. He also interacts with business line managers in collaboration with the company's experts in the areas of IT security, business intelligence, physical security, safety, environment and health, among other specialties, to address operational risks. The goal is not just to share information and avoid duplication but also to establish priorities. "If individual risk management units are going up to the executives and competing for limited resources," he says, "then we are not going to get the things covered that are really the most important to the business. So we need to come together and prioritize the risks that we are dealing with and create a united front when we ask for those resources. Otherwise pushback from decision-makers could derail even the best thought-out proposal."

Conclusion

Business continuity planning and IT security management are becoming an integral part of enterprise-wide risk management and business resilience frameworks at a growing number of organizations. This creates both challenges and opportunities for business continuity practitioners, IT security specialists and risk management executives. These professionals can adopt a number of strategies to leverage their knowledge when they are invited to participate in broader discussions:

- Focus on business goals. Interact with operational managers to understand risks to key business processes from their perspective and think beyond IT challenges.
- Seek out common ground. Collaborate with the risk management community within the organization to understand other specialists' priorities and look for areas where risks could interact and affect different parts of the organization.
- Speak the language of the business. Assess problems and present ideas in terms that make sense to both business line managers and other risk managers.
- Bring something new to the table. Consider how tools developed for IT security management, especially quantitative methods and process-driven approaches, can be adapted to mitigate other types of risk.

"Business continuity practitioners need to integrate other types of risk such as those related to supply chains, facilities, personnel and logistics."

- Joseph Robinson, Global Business Continuity Manager, Navistar, Inc

---

These strategies will become increasingly powerful as senior executives ramp up their oversight of enterprise-wide risk management strategies. Designing solutions that make sense to both risk managers and operational managers builds support for proposed solutions. And the ability to present compelling risk-mitigation proposals to senior decision-makers has never been more important.

For more information

To learn more about a holistic approach to business resilience and risk management—and how IBM can help you put it into practices—you can contact your IBM representative, request a call from an IBM representative, or visit the following websites:

ibm.com/services/continuity

ibm.com/services/security

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10589

Produced in the United States of America
April 2012

Please Recycle

RLL12346-USEN-00