IT@Intel White Paper

Intel IT
IT Best Practices
IT Continuity
March 2012

Intel IT: Keeping the Business Running in a Crisis

By applying Business Continuity plans in real disasters, we have identified several practices that are highly effective, including use of mobile business PCs and duplicate factories and data centers.

Virgil Fleming
IT Business Continuity Program Manager, Intel Information Risk and Security, Intel IT

Naoyuki Tomizawa
Japan Site Manager, Customer Capability, Intel IT

Executive Overview

Intel IT's Response and Recovery Management (ITRRM) program keeps the Intel core business processes running when a disaster occurs and helps with recovery after the disaster subsides. A recent example of exercising our business continuity (BC) plans was the 9.0 magnitude Great East Japan Earthquake. The earthquake occurred Friday afternoon, yet Intel employees at the damaged Tsukuba facility were able to work remotely Monday morning.

As part of Intel's Crisis Management program, the ITRRM program shares the underlying goal of first protecting employees and their families. It does this by aligning BC capabilities for response and recovery with risks and business requirements. Our program is based on industry standards, regulations, and best practices. We use this information in a cycle of continuous improvement that includes:

- Developing and maintaining program policies and infrastructure
- Helping BC plan owners develop, maintain, and test their plans
- Improving our program and plans based on multiple factors including plan audits, learnings from real disasters, and industry-wide best known methods.

Our program provides BC plan owners with the support and resources they need to develop plans that align with corporate BC strategies and address each stage of an event—preparedness, response, recovery, and restoration. Having applied BC plans to real disasters, we have identified several practices that are highly effective, including use of mobile business PCs and duplicate factories and data centers.

Although disasters, such as earthquakes, floods, power outages, widespread illness, and cybercrime, threaten to interrupt business, our ITRRM program helps Intel IT and the Intel groups we support be safe and productive after a disaster.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Images of the recent Great East Japan Earthquake and the subsequent tsunami that caused extensive flooding, loss of life, and destruction are etched in the minds of many. Yet, the more than 300 Intel employees at Intel's Tsukuba site in Japan were able to work remotely Monday morning just two days after the earthquake on Friday afternoon.

Intel has over 91,500 employees at 164 sites in 62 countries, and its factories and IT data centers operate 24/7. The nature of Intel's business has always dictated robust emergency management practices and recovery plans. The company has a responsibility to its employees, customers, and shareholders to maintain safety and productivity during and immediately following a disaster, such as the earthquake in Japan, and to recover quickly with minimal impact after an emergency event subsides.

A comprehensive approach to planning for business continuity (BC) seeks to mitigate all major interruptions of business systems. To this end, Intel has long emphasized the importance of a BC strategy and requires each Intel business group, including IT, to have a BC management program in place.

Intel's BC program started in the 1970s with the founding of the Corporate Risk Management program. After the terrorist attacks in New York on September 11, 2001, business continuity management became a corporate mandate for all business groups. Since then, threats appear to be on the rise, highlighting the need for all business groups, including Intel IT, to have a robust BC strategy.

Intel's success depends on the ongoing operation of its offices, and more importantly, its factories—both of which increasingly rely on IT. Our IT Response and Recovery Management program is a critical part of Intel's ability to maintain operations during emergency situations.

SOLUTION

Intel IT's Response and Recovery Management (ITRRM) program is part of the Intel Crisis Management (ICM) program, which strives to keep employees and their families safe and the business running after a crisis. ICM drives overall recovery efforts and mandates that each business group, including Intel IT, have an active continuity plan for its core mission and business critical functions and processes. These BC plans are tested at least annually as part of a continuous maintenance and improvement process.

The four key characteristics of the ICM program success are:

- A good foundation of emergency response and emergency management functions organization-wide
- Executive-level support and sponsorship for BC
- Ownership of BC programs by each business group
- Demonstrated results from response and recovery of real events

As Figure 1 shows, the ICM program oversees and supports focused management programs developed by the business groups, one being the IT Response and Recovery Management program.

IT Response and Recovery Management Program

IT Response and Recovery Management (ITRRM) program encompasses IT's response and recovery efforts for all unplanned events. The goal of ITRRM is to align recovery capabilities and resources with risks and business requirements. This approach involves:

- Proactively assessing emerging threats and risks and taking actions to avoid or reduce their impact through partnering with privacy and threat intelligence teams
- Developing emergency response and recovery capabilities that return Intel to business as usual as soon as possible
- Exercising effective leadership and communications during crisis events

The ITRRM program is composed of two teams: the IT Emergency Response Process (ITERP) team, which responds to unplanned events to mitigate business impact, and the IT BC Management (ITBCM) team, which provides the BC planning tools, training, assessments, and compliance enforcement to maintain IT operational resiliency and preparedness.

The teams coordinate activities and processes by maintaining a close working partnership and cross-functional team members. Each team is further described below.

IT EMERGENCY RESPONSE PROCESS (ITERP) TEAM

The ITERP team is the focal point for implementing IT emergency efforts. This team ensures that IT can respond to any unplanned event by providing rapid containment, mitigation, and recovery, while minimizing business impact. The team developed its strategies using incident management principles based on the U.S. Federal Emergency Management Agency's response to disaster events (see Figure 2).

As shown in Figure 3, the ITERP team is composed of representatives from every discipline in IT. The Incident Commander (IC) directs all response and recovery operations and pulls in the appropriate resources from the various sections, branches, and groups based on the need. The IC is responsible for providing leadership and ownership of the event, as well as communicating up

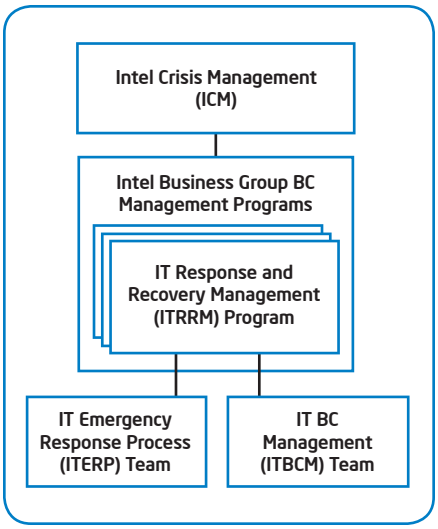

Figure 1. As part of the Intel Crisis Management program, the Intel IT Response and Recovery Management program is composed of two teams.

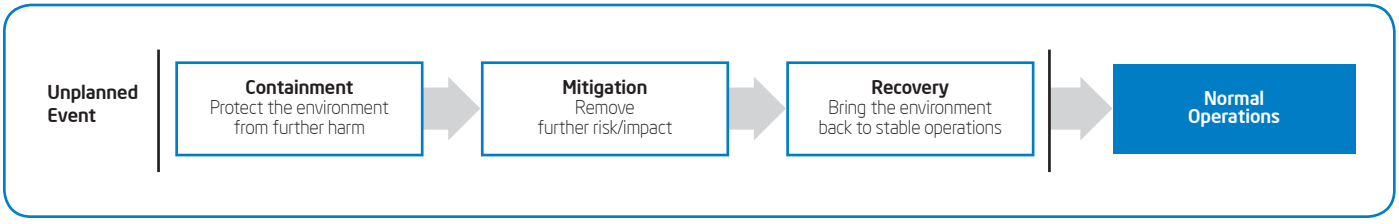

Figure 2. The IT Emergency Response Process Team responds to unplanned events using incident management principles based on the U.S. Federal Emergency Management Agency's response to disaster events.

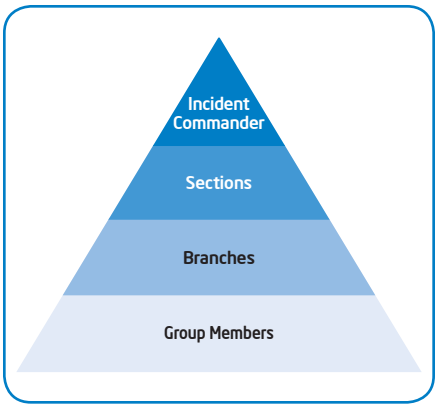

Figure 3. Pyramid structure used for event management, modeled after the U.S. Federal Emergency Management Agency's Incident Commander Structure. Resources are activated only as needed.

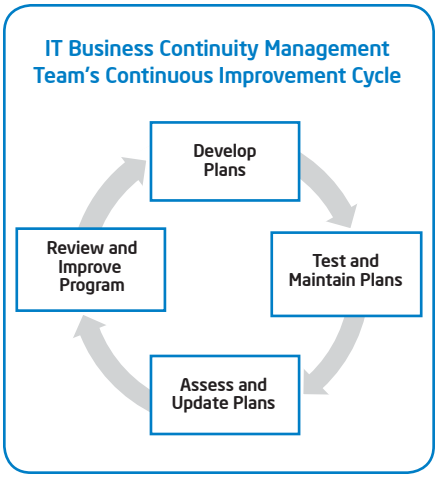

Figure 4. The IT Business Continuity Management team's process and methods are implemented as part of a cycle of continuous improvement.

and down the chain of command. When an unplanned event occurs, all team members perform their response roles instead of their normal duties until all issues are resolved. This team has proved to be an essential component of the successful resolution of every crisis management, coordination, control, and communication activity in IT for the past 11 years.

IT BUSINESS CONTINUITY MANAGEMENT TEAM

The IT BC management (ITBCM) team provides the tools, processes, training, assessments, and compliance enforcement necessary to maintain business continuity and recovery plans that enable IT operational resiliency and keep Intel legal and secure. The ITBCM team supports and reviews more than 600 active BC plans for IT infrastructure, applications, and services classified as Critical.

While ICM drives the overall effort, the ITBCM team establishes the program's more detailed guidelines and requirements by outlining performance objectives, program administration, and records management. In addition to providing the tools that enable IT BC plan creation, the team coordinates large cross-function integrated drills, tests, and exercises and conducts audits of critical plans.

The ITBCM team's process and methods are implemented as part of a cycle of continuous improvement as shown in Figure 4 and detailed below.

Develop Plans

With tools and training provided by the ITBCM team, individual plan owners develop plans based on program guidelines and requirements. Our program relies on a standard planning methodology for the industry that evaluates the impact of a disaster as opposed to evaluating the threat itself. For example, the plan would evaluate the impact of a power outage rather than the cause of the outage, which could be a snowstorm, earthquake, fallen tree, or any number of other causes.

In this approach, plan owners evaluate risks and identify controls for each risk, assess the business impacts, develop strategies that address the impacts, and develop emergency preparedness and response capabilities.

A BC plan includes how communications and warnings will be issued, how resources will be managed, how crisis information will be communicated to key responders, and who are the members of the emergency response teams and how they are organized and trained.

Test and Maintain Plans

To ensure continuous quality and validity of our plans and procedures, we develop training and establish the frequency and evaluation criteria for plan maintenance and testing, which include:

- Reviewing BC plans
- Developing plan tests and exercises
- Defining plan maintenance requirements
- Defining roles and responsibilities for maintaining and testing plans
- Ensuring individuals with roles and responsibilities are well-trained and have access to all plan documentation

Each year, the ITBCM team ensures all critical plans are drilled against a set of maintenance and validation requirements. Our IT plans have been 100 percent compliant with these requirements for the last three years.

Assess Performance and Update Plans

The plan owners update and improve the plans according to how effectively they helped with response and recovery during tests and to real events. To do this, plan

owners measure performance with metrics, examine any corrective and preventive actions taken, and update the plans based on any identified gaps and areas for improvement.

The ITBCM team conducts internal audits to verify that the plans meet requirements. These audits include validating the quality of the plans, ensuring inclusion of required elements, completing annual drills to manage required improvements and track the actions needed to fix any issues.

Review and Improve the Program

The ITBCM team reviews all IT BC plans and provides feedback to corporate and IT upper management. This feedback includes audits of individual plans, results from our response to real disasters, gaps and areas for improvement detected through tests and drills, and tracking overall program metrics. The ITBCM team also identifies other factors that could impact the program, including changes that occur over time such as new technologies, shifts in business priorities, evolving risks, and new standards and regulations. These sources of feedback and new information help influence the ongoing development and improvement of our BC program and plans.

Best Practices for Effective Business Continuity

Over the last decade or more, several natural and human-caused disasters have occurred that have tested the ITRRM strategy. These disasters include the 9/11 attacks, the Great East Japan Earthquake, the outbreak of severe acute respiratory syndrome, Hurricane Katrina, the Cheng Du earthquake in China, numerous cyber attacks, and even small, localized events such as a travel restriction due to poor weather, a burst pipe, and power outages. Each disaster event has tested our BC plans allowing us to identify the approaches to BC that are most effective for us.

USE OF MOBILE BUSINESS PCS AND OTHER TECHNOLOGIES

Intel IT has found that mobile business PCs are crucial for keeping the business running during a variety of disaster situations (see Table 1). By standardizing on a mobile business PC platform for Intel's highly mobile workforce, employees can work from almost any location, with robust, secure computing capabilities.

We support this mobile work environment with several additional technologies.

Table 1. How mobile business PCs provided business continuity in disaster situations

Event	How Mobile Business PCs Helped
Earthquake damaged an Intel site in Japan	More than 300 employees at Intel's Tsukuba site telecommuted from their homes, worked from alternate workspaces, or worked from other locations with Internet access for 8 months while a new Intel facility was prepared for occupancy.
Flooding from a burst water pipe rendered an Intel facility unusable	450 employees worked from on-site locations such as travelers' workstations, conference rooms, and cafeterias or telecommuted effectively for up to 2 months during renovations.
Snowstorm caused dangerous road conditions, preventing access to multiple Intel facilities	5,000 employees telecommuted for 3 days.
Outbreak of severe acute respiratory syndrome forced closure of an Intel office and interrupted travel to some Asian countries	Employees telecommuted, and stranded employees were able to work from any location.
Frequent, brief power outages affected an Intel facility in India	Employees remained productive because mobile PCs switched to battery power during brief outages.

Intel Crisis Management

Whatever the crisis, Intel's highest priority is the safety of its employees and their families. At the earliest indication of a problem, Intel Crisis Management (ICM) assesses the situation, evacuates the building if necessary, and contains the damage as fast as possible. Much depends on the situation as to what procedures are followed. At the first, safe opportunity, Intel IT assesses damage to the data centers and brings them back online or ensures they stay online.

The success of our program has required long-term commitment and support from Intel corporate and IT upper management. This support includes defining the program scope, developing and reviewing program policy, and developing the program's organizational leadership and team. Since the terrorist attacks in New York on September 11, 2001, business groups are now expected to follow a greater number of standards and regulations and have much stronger BC programs.

Our BC program's current guidelines incorporate external guidance from new and pending regulations, industry standards, and best practices. For example, we incorporate guidelines from the Disaster Recovery Institute International and ISO standards.

Actions Intel IT Has Taken in Response to Disasters

When disasters have occurred, Intel IT has kept the business running, sometimes with as little as 60 percent of its workforce, by responding with a number of actions, some of which are standard for any IT organization. These actions include enabling contact with employees to verify their safety and well-being, providing alternative workspaces and the ability to work from home or at other safe location with essential IT communication capabilities, relocating core IT business support capabilities, and restoring systems using backups, alternative IT data centers, and remote data access.

Other less typical actions Intel IT has taken include:

- Supporting humanitarian aid to regional disasters by providing networks and computers to relief agencies
- Communicating disaster-related information, including posts to internal and external web and social media sites, and recorded messages on emergency toll-free telephone numbers for our employees and their families.
- Securing second-source suppliers to alleviate supply chain issues

Our goal is for employees to continue to work productively despite disruptions.

Employees can use videoconferencing to meet and collaborate without being in the same location. Unified messaging lets employees use their PCs for all messaging, including voicemail. The Enterprise Portal and the Intel Virtual Private Network provide employees secure access to enterprise applications, Voice over IP (VoIP), and services wherever they have network access. Whole Disk Encryption is installed as part of our standard build, so information is stored securely in case the laptop is lost or stolen. We remotely manage and maintain business PCs with Intel® Core™2 processors with vPro™ technology, which helps us keep employees productive not only during disasters, but also during normal operations.

In addition, we used Wi-Fi* technology to assist with communications in disaster situations. For example, after Hurricane Katrina, fixed communications systems in the New Orleans area were destroyed. We helped with disaster recovery efforts by building wireless networks and connecting laptop computers using satellite feeds to set up communications centers for humanitarian groups and relief agencies. We can apply this same approach if a disaster destroys an Intel site's fixed communications.

STRETCHING MISSION CRITICAL SYSTEMS BETWEEN DATA CENTERS

We are responsible for keeping Intel's assembly and test manufacturing automation systems running 24/7. To address the possible occurrence of a crisis in one data center, we have developed a cost-effective approach that stretches mission-critical systems, including applications, the storage area network (SAN), and network-attached storage systems between two data centers located at the same site.

Without this approach, it would have taken us more than 24 hours to recover the SAN; however, we were able to do it in one hour.

USING A LOW-COST DISASTER RECOVERY SITE AS A DATA CENTER

Disaster recovery (DR) sites are often viewed as an expensive insurance policy against a disaster event. We developed a low-cost DR strategy for data centers that maximizes the use of compute servers, uses a tiered storage system on low-cost serial advanced technology attachment disks, and offloads backup services from the main data center to the DR site.

In a disaster drill, we simulated the main site being down by eliminating network connectivity between the DR site and the main data center for about 24 hours. At the DR site, a team of IT staff and microprocessor design engineers were able to bring up the DR environment and restore 95 percent of services. And when not in a disaster scenario, we maximize the DR computing resources through high utilization rates.

REDUNDANT FACTORIES

Since the 1980s, Intel has used the concepts of flexibility and redundancy when building factories around the globe, making them virtually identical from a process and product standpoint. IT provides the services that support these widely distributed, redundant manufacturing facilities. This approach to safeguarding factories against the impacts of a disaster helps keep Intel manufacturing operating if an event occurs in one part of the world.

COPY EXACTLY DATA CENTERS

Because Intel's manufacturing environment relies on IT systems 24/7, we use dedicated data centers for factories. To keep factories running if a data center failure occurs, we have invested heavily over the last few

years in a copy exactly approach when deploying new solutions.

In the copy exactly approach, we deploy the data center solution in a single factory. Once successfully deployed, we copy that implementation across other factory environments. If a factory data center suffers a catastrophic failure, the IT systems that support manufacturing can quickly shift to another factory data center. This enables us to immediately resume manufacturing using the replicated data center solution. As a result of these efforts, since 2009, we have experienced no factory downtime related to data center facilities.

CRITICAL CAPABILITIES HOSTED IN THE CLOUD

We have engineered and implemented an enterprise private cloud and about 60 percent of our Office and Enterprise environment is virtualized. These capabilities increase production capabilities, but they also support our BC efforts by increasing security and redundancy of data access.

IT Response and Recovery Management in Action: The Great East Japan Earthquake

The recent Japan earthquake and tsunami tested our BC plan at Intel IT in Japan. The key lessons we learned are:

- Our mobile business PC strategy was highly effective. Employees in Japan are 100 percent mobile, so they were immediately and easily able to work from home after the event.
- Working from home was effective for one to two weeks. After that time, challenges such as interruptions and distractions from family members and pets began to hinder productivity. Consequently, we built two temporary offices to give employees a place outside of their home to work.
- WiMAX*, deployed widely to our mobile workers, proved to be extremely useful as a means to provide network connectivity right after the earthquake when the 3G data network was congested. However, when users were more concentrated in a given location, as was the case of the temporary offices we created, a bottleneck at the base station impacted performance. In general, WiMAX is more effective in urban areas where local providers are prepared to handle a greater number of users.
- Many of our critical capabilities, such as e-mail, enterprise resource planning (ERP), and other critical business tools were hosted in our enterprise private cloud. As a result, the earthquake did not impact our access to these capabilities.
- We found that two new technologies were extremely helpful in improving communications. We replaced desk phones with VoIP softphones, and employees relied on social media forums for needed support and communications. For example, information from Intel was made available via an online forum that employees could access.
- When recovering from the disaster, we learned that it is important to have a prioritized list of services that need to be restored to ensure that the most critical services are restored first.

During this disaster, we kept the business running with no downtime. Employees worked at home, then in temporary offices, and moved into permanent, fully renovated offices within eight months. Throughout that time period, we experienced no impact on the delivery of large IT projects such as re-platforming the ERP system. In spite of the challenges that Intel Japan faced as a result of the earthquake, they recorded increases in revenue after the disaster, putting them on track for a record year.

CONCLUSION

We developed our IT Response and Recovery program to align with the Intel Crisis Management's overall goal, which is to protect Intel's employees, their families, and the business in the event of a disaster. It incorporates industry best practices and standards and is built on a cycle of continuous improvement.

Although we can never predict exactly when and what type of disaster will occur, we have learned through experiences with numerous disasters which aspects of our program and plans are effective. These practices include equipping the workforce with mobile business PCs, building duplicate factories, and hosting critical services in Intel's enterprise private cloud. As we build our BC plans, we focus on the business impact rather than the disaster event that causes the impact.

Implementing these practices has made a difference to Intel in many disaster situations, including the Great East Japan Earthquake. Instead of being shut down as a result of the earthquake, Intel Japan recovered quickly, recording increased revenues in the third and fourth quarters of 2011. Our ITRRM program reduces risk to Intel's business and helps maintain business as usual.

FOR MORE INFORMATION

Find additional IT@Intel white papers at www.intel.com/IT.

- "Business Recovery and Disaster Recovery with Mobile Business PCs"
- "Establishing a Low-cost Disaster Recovery Site"
- "A Cost-effective Disaster Recovery Solution for Intel's Factories"

For more information on Intel IT best practices, visit www.intel.com/it.

CONTRIBUTORS

Lisa Oppedahl
IT Emergency Response Program Manager, Intel Information Risk and Security, Intel IT

Jim Holko
Intel Emergency Management Program Manager Intel Corporate Security

ACRONYMS

BC	business continuity
DR	disaster recovery
ERP	enterprise resource planning
IC	Incident Commander
ICM	Intel's Crisis Management program
ITBCM	IT Business Continuity Management team
ITERP	IT Emergency Response Process team
ITRRM	IT Response and Recovery Management program
SAN	storage area network
VoIP	voice over Internet protocol

0312/WWES/KC/PDF 326721-001US