

COMPUTERWORLD STRATEGY GUIDE

Best Practice Business Continuity Management

Best practice business continuity management starts by preparing for disasters before they happen, rather than simply trying to clean up during and after they have occurred.

This guide will outline how to best create an incident response plan, as well as the best way to protect your computers from risk. Learn from those who have already experienced disasters in our case studies, and discover for yourself why tomorrow is too late to think about business continuity.

Contents

- 2 The New Business Continuity
- 3 Why Tomorrow Is Too Late to Think About Business Continuity
- 4 Five Tips for Building an Incident Response Plan
- 5 Case Study: Crash
- 8 Best Practice Case Study: Business, Gov't Systems Keep Running Despite Wildfires

The New Business Continuity

GONE ARE THE DAYS when a comprehensive business-continuity plan meant mailing backup tapes to a hot site a few miles away. Today, businesses are always on, running at break-neck speed 24/7. And their business-continuity plans need to reflect that reality.

"If we're not getting data from our customers, we can't run our business," says Jeff Flanigan, director of IT infrastructure at E-gatematrix, an Atlanta company that tracks and stocks meals, headsets, blankets and other service items for major airlines around the world. "There are airplanes in the sky 24/7, and we're always either loading aircraft or getting ready for aircraft to come in. It's a nonstop process. We can't be down, and our disaster-recovery plans have to take that into account."

Fortunately, new data centre technologies, such as business process monitoring, continuous data protection and virtualization are emerging to make recovering such environments easier and more cost-effective. Experts and users who have built successful business-continuity plans offer the following best practices for business continuity in the era of the new data centre.

Tier applications by criticality

Today's organizations are becoming increasingly data-intensive and, as a result, the amount of data they potentially need to recover quickly can become overwhelming. "Up until now, many companies aimed to recover absolutely everything in one fell swoop," says Michael Croy, director of business-continuity solutions at Forsythe Technology, an IT consultancy. "But that's just not feasible anymore because most organizations have too much data, too many applications and too many interdependent processes."

The solution is to take a holistic view of the business and bring back only the most critical applications right away. "It is not always feasible to bring everything back straightaway," says Penny Turnbull, senior director for crisis management and business-continuity planning at Marriott International, in Washington, D.C. "If you don't need certain things immediately, you can be wasting time, effort and money planning for their recovery. And that's what business-continuity planning is all about: Knowing the must-haves, because you can't recover everything."

Marriott has built an enterprise business-continuity framework that guides users through the process of deciding business process and application criticality and tailoring continuity plans accordingly. "You need to put applications into context because this isn't business as usual," Turnbull says.

Weigh criticality against overall cost

In some cases, business-continuity planners need to weigh even the most critical applications against the overall cost of recovering them after an incident.

"You can create any solution if you have enough money," E-gatematrix's Flanigan says. "But in a lot of situations, you don't have to."

Instead of instantaneous recovery, E-gatematrix realized it could get by on a four-hour window for getting its most critical applications up and running after a disaster, he says. "Just because the technology is available to get everything back right away doesn't mean my business can afford it. I try to craft the solution that best fits the needs of the business and go from there," he says.

Buy with an eye toward business continuity, Savvy organizations virtually never purchase technology for disaster recovery alone. Today, companies can leverage most new data centre technologies in building robust, just-in-time business-continuity plans.

The Chicago Tribune, for example, has consolidated its critical applications onto two Sun Fire 15K servers, located on opposite sides of town, says Pete Mashek, director of production systems at the newspaper. It links those servers via AT&T fibre and Nortel metropolitan Ethernet switches. The whole point was to build more reliability into the production systems, but the company also made huge strides in business continuity.

"We needed to upgrade anyway, so it made sense for us to take disaster recovery into account while we were at it," Mashek says. "From a purely financial point of view, disaster recovery is a cost. But when you're buying new equipment and putting in new architectures to support the business anyway, you can mitigate the disaster-recovery costs at the same time."

For the Tribune, the result is an active-active clustering solution that supports day-to-day business and offers less than a second of down-

time when a disaster affects one centre.

Emphasize the "business" in business continuity

"Business continuity can't be a one-off anymore," Forsythe's Croy says. "It should be an integral part of day-to-day business."

This means evangelizing continuity across the business so that not only is it taken into account each time a new system or application is brought online, but also so that business expectations and actual systems availability align appropriately. "There can be an awful lot of assumptions made about what's backed up, what's protected, what's recoverable, how quickly and who's going to do it," Marriott's Turnbull says. "It's only when you sit down and talk it through that you find the gaps."

Ensuring ongoing discussions between the business units and Information Resources (Marriott's technology department) is a core part of her job, Turnbull says. The goal is making sure assumptions are correct and everyone is clear on their roles and responsibilities.

"The business-continuity planning discipline has changed so much in the last few years. It used to be much more technology-focused. Now it needs to be far more comprehensive," she says. "You need to go beyond technology to look at the whole business – the people, facilities, assets, reputation and brand image, and so on. It has to become part of everyday operations."

Don't get enamoured with technology

Sometimes a company can support critical business processes with plans that involve simple paper-based procedures or focus on more important assets, such as people. "Bottom line, it is important to recognize which business processes can go manual," Turnbull says.

At Marriott, this emphasis on the bigger picture of business continuity, as opposed to simply a technology-centric view, was underscored during the Sept. 11 terrorist attacks, Turnbull says. Sept. 11 "highlighted the importance of people," she says. "You can recover all the systems you want in the world, but if you don't have people to operate and utilize them, then why are you recovering? Business continuity is more than that." ●

By Joanne Cummings

Why Tomorrow Is Too Late to Think About Business Continuity

WALK AWAY FROM THIS GUIDE with two pieces of data in your mind: 1. The University of Texas estimates that more than half of small and midsize businesses (SMB) that lose data in a disaster go out of business within two years 2. Gartner estimates that less than half of all midsize businesses and only 25% of small businesses have disaster recovery plans in place. If there is any bright spot in the legacy of Hurricane Katrina, it is that business, government and education institutions seem to have a better understanding of the requirement for business continuity and disaster recovery. Yet, as the Gartner numbers testify, there is still a chasm between understanding the requirements and generating the organizational commitment to meeting them.

Like all business leaders with priorities, SMB owners and executives must juggle a number of things that compete for time and resources. As a result, they tend to put business continuity into the “solve tomorrow” pile until right before (or right after) an incident. This is a critical, sometimes disastrous mistake. Like all business-essential Information Technology (IT) programs, designing and implementing a functional continuity plan is a multimonth process. Here is why:

Business continuity is a business process:

A functional business-continuity plan is more about understanding and protecting key business process than it is about managing IT assets. As such, it will require input from key business leaders and will necessitate in-depth planning and preparation so that every person in the organization knows what to do in the event of an emergency.

Assessment and design:

Developing the core business-continuity plan is not a one-person job; it requires input from a cross-functional team that includes sales, communications, finance, back office, human resources and IT leaders. Without that input, it is impossible to correctly prioritize and tier support systems to meet demands during a disaster incident

Back order of critical elements:

The back order log for business-sized power generators from reliable manufacturers is often 30 weeks. That means if you order today, your generator will be available in seven months. If you try to substitute this essential element with a generator from your local Home Depot, you'll find that the power from household gen-

erators is too unstable for use by IT equipment without some type of power cleaning device. In some cases, the power simply won't turn on, while in others you risk permanent damage to your assets.

Entering the telecommunications queue:

It usually takes a long time to get telecommunications providers to install backup lines to SMBs, because: 1) the backup service provider is (we would hope) different from your primary provider; you will have to initiate a new business relationship, including all of the associated legal and administrative hurdles; and 2) as the backup line will not represent a sizeable business opportunity, you will have to wait in line behind more profitable opportunities – including some that enter the queue after you do.

Implementation:

Once all of the pieces of the continuity solution are in place, building the system, connecting it to ongoing IT programs and aligning it with the corresponding business processes takes time. Assuming that the IT staff (or person) will also have to focus on their regular job at the same time they implement the new system, view this commitment in days or weeks as opposed to hours.

Temporary relocation:

In many disaster scenarios, resuming operations at the same location will no longer be possible. It will be necessary to have plans and agreements in place for a backup location and logistics for resuming operations in the new facility. This also involves having an IT layout pre-planned for the backup location to ensure that all of your critical systems will function at the secondary facility.

Testing:

Your business-continuity system is only as good as its last test. Like flashlight batteries, smoke detectors or brakes, you don't want to find out about shortfalls during an emergency. Regular and systematic testing in a number of different situations will consume time and effort, but it is really the only way to know if systems are functioning properly. Plan to extend tests over weeks and months to make sure that the system aligns fully with business operations.

In the end, you can beat the odds, but not the percentages. Though Gartner and the University of Texas did not correlate the relationship between business continuity and disaster survivability, experience across thousands of customers leads us to believe that the link between the two is significant. If you are

inclined to agree, we would recommend that you get started today with the following steps:

1. Conduct a business-impact assessment:

As mentioned above, convene a cross-functional team to evaluate the business requirements and tier data based on its importance to operations.

2. Take steps to protect data:

Organizations should back up data frequently to ensure records are kept, and consider upgrading the backup equipment to a faster version to reduce the time it takes to complete a backup cycle.

3. Review power options:

Organizations should add uninterrupted power supplies (UPS) for critical servers, network connections and selected personal computers to keep the most essential applications running.

4. Document, test and update the disaster preparedness plan:

Documentation should include updated configuration diagrams of the hardware, software and network components to be used in the recovery. The plan should also include logistical details, including travel to backup sites, and even who has spending authority for emergency needs.

5. Consider telecommunications alternatives:

Telecommunications backup must involve both redundancy and alternatives. In the case of spot outages, redundancy may be enough. For larger outages, alternatives such as wireless phones, wireless data cards and satellite phones should be considered.

6. Form tight relationships with vendors:

A strong relationship with hardware, software, network and service vendors can help expedite recovery, as these vendor contacts often can work to ensure priority replacement of critical telecommunications equipment, personal computers, servers and network hardware in the event of a disaster. This is especially important for small and midsize organizations, which may lack the resources that larger companies can tap in an emergency.

In the end, there is no guarantee against a natural or man-made disaster, only a very high probability that you will fail without a detailed business-continuity plan. Though the time and resources required will conflict with other organizational priorities, executives need to dedicate the time to ensure business survivability. Tomorrow is already too late. ●

By Firooz Ghanbarzadeh

Five Tips for Building an Incident Response Plan

LIKE ALL IT PROFESSIONALS, Darryl Lemecha worries about viruses and hackers, data centre problems and technology meltdowns. But what separates his worried mind from many others is a detailed incident response plan that will guide him, his IT staff and his company through whatever problems may arise.

“The more you get that down on paper, the better you’re going to be in a real crisis,” says Lemecha, CIO and senior vice president of shared services for ChoicePoint, a data aggregator based in Atlanta.

An incident response plan takes its place beside business continuity and disaster-recovery plans as a key corporate document that helps guarantee companies will survive whatever glitch, emergency or calamity comes their way.

“A lot of companies have that mentality – ‘We have some really good people in our organization, things are running well, the chances of something happening are small, and if something does happen, we’ll be able to deal with it.’ But in the event of a real crisis, people won’t know what to do,” says George McBride, director of IT risk consulting with Aon Consulting Worldwide in the US.

The typical response to trouble – the deer-caught-in-the-headlights look – is exactly why companies need such a plan, McBride says. And while a business continuity plan aims to preserve operations in the face of adversity and a disaster recovery plan details what to do in case of a disaster, McBride says an incident response plan is broader, laying out how to respond to scenarios as diverse as data security breaches and network crashes.

Given their breadth and specificity, these documents are usually lengthy and in need of regular upkeep. They will vary from company to company and even among departments within the same corporation, but here are five points that all IT-specific plans should contain.

1. A sense of what can happen

You can’t possibly anticipate what will happen in a crisis or during the aftermath – that’s the nature of the beast. But that doesn’t mean you can’t plan for one, says Ian I. Mitroff, a senior investigator at the US Centre for Catastrophic Risk Management at University of California, as well as a professor emeritus at the US-based Marshall School of Business and the Annenberg School for Communication at the University of Southern California, an adjunct

professor in the School of Public Health at St. Louis University, a professor at Alliant International University in San Francisco, and the author of *Crisis Leadership: Planning for the Unthinkable* (John Wiley & Sons, 2003).

Well-prepared companies pick potential incidents representative of the various crises that could occur and then devise strategies to handle them, Mitroff explains.

2. A well-chosen team

CIOs need to name names, says Janice Malaszenko, an IT executive who has held the CIO position at several US Fortune 1000 companies. They need to identify which departments have roles to play when something happens.

Think broadly, she says, lining up people from the human resources, public relations, legal and purchasing departments to pitch in during an incident. Go outside the company, too, and identify the key suppliers and service groups most likely to play a part during a crisis. “Identify secondary or backup people, too, in case [the first-tier] people are unavailable,” she adds.

3. A communication plan

Bridge lines, conference call numbers and Intranet sites will be crucial for getting team members together when they’re trying to fix problems that might have them working in diverse geographical locations, Malaszenko says.

The plan should also include the individual contact information for team members that goes well beyond office e-mail addresses and phone extensions, she says. The document needs to contain home phone numbers and e-mails along with mobile phone numbers. Finally, Malaszenko adds, the plan needs to say which team member owns communications, so when the time comes, there’s no delay in getting everyone talking.

4. A list of who does what (and when)

Good incident response plans don’t just name the members of the response team; rather, they lay out who will have which responsibilities and authority so they can get right to work, says Joe Brennan, who, as Ohio University’s executive director of communication and marketing, played a key role in the aftermath of data security breaches that hit the college in 2006. “In a crisis, a CIO can’t run around and say, ‘Hey, do I have permission to do this?’ A

public relations person can’t run around and say, ‘Who’s going to approve my release?’” he explains. The plan must give them the power to make those decisions quickly. But the plan should also give them guidelines to help them make the best decisions. “It should spell out the values and principles that will guide the response and the communications,” he says. A hospital CIO might establish in his incident response plan that patient safety is the top priority, so that the response team knows that its actions must first align with that goal. Or a university CIO might state that communicating promptly and honestly with students and faculty is a top concern, thereby establishing for team members that they need to put that above other priorities.

It’s important, too, to assign key roles to specific team members in advance, says Mike Tainter, the IT service management practice director at the US-based Forsythe Solutions Group. Determine who will handle communications with the public, internal business colleague and external partners. Pick a particular person to track spending. And assign someone to document the team’s response to an incident – those notes will be valuable when it comes time to update the incident response plan. “Nothing works better than to have a go-to team that’s trained and ready to resolve the problem,” Tainter says.

5. A safe, accessible home

Good incident response plans will have detailed often proprietary, corporate information along with personal contact information for team members. That kind of document should be kept under lock and key, or at least secured deep in the corporate computer system. On the other hand, if your IT system goes down and the plan is inaccessible, then it doesn’t do any good. The best approach is to thoroughly think out how and where the information is stored to guarantee access during all sorts of scenarios. Lemecha, for example, has copies of his company’s incident response plan in three spots. Everything is on ChoicePoint’s Intranet, a second copy is on an encrypted CD that’s given to all the team leaders, and a third copy is kept off-site at one of the company’s locations (the exact location is undisclosed).

Plan to revisit and revise

An incident response plan is never really done. Rather, it needs to be revisited and revised as

an organization grows, new threats develop, and team members change, Malaszenko says.

Start by putting someone in charge of managing the document. According to Malaszenko, IT security executives are often in charge of incident-response plans in larger organizations. Whatever the title, the plan's manager should update the document not only with everyday items, such as the names of new team members as employees come and go, but also with revisions to policies and procedures as incidents happen. The manager should also train new team members as they come on board and

organize regularly scheduled drills, tests and simulations.

Testing requirements

You don't want to find holes and glitches in your incident response plan when you're dealing with a denial-of-service attack or a downed server. That's why it's so important to test it ahead of time. Start with a desktop-type test, just walking through and acting out the plan; that will help identify any glaring problems with the document before going through the time and expense of a simulation, Malaszenko

says. Then move to the next level by simulating an actual event.

Brennan worked at one university that tested its plan by simulating a hostage situation in which a gunman barricaded himself in a fraternity house. Among other things, simulations like that can test how fast the IT response team can set up a bank of toll-free telephone numbers and put together a new Web site for communications. Brennan says that test took a half day, with debriefing taking the remainder of the day. ●

By Mary K. Pratt

Case Study: Crash

THIS PAST FEBRUARY 2, at 5.15pm, Alan Boehme, 47, VP and CIO of Juniper Networks, left his office and climbed into his black 2004 Infiniti G-35. He pulled out of the company parking lot and began the 90-minute drive to his home in Half Moon Bay, a coastal town in Northern California's San Mateo County. Boehme's work had been going well. In December, he had completed an ambitious restructuring of the \$US2.5 billion networking company's IT infrastructure, globalizing its operations and laying the foundation for its future growth.

Boehme took California Highway 280 to Highway 92, a two-lane road about 10 minutes from his house. A few seconds later, a drunk driver in Boehme's lane hit him head-on.

"The person in front of me swerved off the road because he saw the guy coming," Boehme recalls. "The next thing you know, these headlights were coming straight at me. We hit headlight to headlight. I remember thinking, my wife and son are going to lose their husband and father."

They didn't. But the aftermath was ugly.

"I felt blood just gushing down my face and I was in a state of panic and shock," says Boehme. "Somehow, I was able to get the seat belt off, kick the door open. I got out of the car and just started yelling: 'Help me, help me.'"

A person who witnessed the crash helped Boehme to the side of the road. An artery in his nose had been severed and he was bleeding profusely. "I had broken bones in my face, and my nose was turned sideways and crushed," he says. "I ended up with a contusion of the skull and a fracture at the base of the skull, along with, we found out later, a series of injuries to the left side of my body, including my knee, where there were torn ligaments and a crushed kneecap, as well as a broken finger and torn muscles in the shoulder from the seatbelt."

Boehme lay on the side of the road as

EMTs attended to the drunk driver, believing his stomach wound was more life-threatening than Boehme's injuries. "I was very upset that here's this person who for all I knew had ended my life, and at minimum had dramatically impacted my life, and they're rushing to save him," he recalls. Feeling cold and abandoned, Boehme asked the man who had stopped to grab his BlackBerry. He called his wife, Alisa, who arrived 20 minutes later with their 11-year-old son, David. They found Boehme lying on the roadside, still waiting to be taken to the hospital.

Later that night, at Stanford Medical Centre, doctors monitored what they believed was a fluid leak in Boehme's brain. They stitched up his face and put IVs in both arms. Boehme drifted off as the painkillers did their work. He awoke on Saturday morning to find his BlackBerry by his side.

"I don't know if my wife picked it up or if they put it on my person," says Boehme, "but I e-mailed Danny Moquin [his VP of IT operations and infrastructure]: 'Been in a car accident. You need to take over.'"

The importance of succession planning

What happens when a key player in a company goes down? Who takes over? What effect will replacing an individual have on operations? While most businesses have org charts that map out what to do after disruptions – whether they're caused by resignation, firing, retirement, sickness, injury or death – these are often crude in format and live in dusty filing cabinets in HR. And because succession planning often falls under the categories of disaster recovery and business continuity, it frequently receives less attention than does preparing for sexier events such as hurricanes, bushfires and terrorist attacks, even though these are far less likely to occur than, for example, a car accident.

Planning for major catastrophes also

emphasizes information systems and the proprietary data within them and all too often gives short shrift to the people who manage it all. "The old question is: 'What if someone gets hit by a bus?' Well, we know the answer to that now," says Moquin, who took over for Boehme during his two-and-a-half-month convalescence.

Companies often lack succession plans that reach beyond their C-level officers and their direct reports. In a report by Aberdeen Research, 82 percent of the companies surveyed claimed to have a succession plan for their executives, while only 17 percent did for lower-level workers and just 12 percent for their IT staff. This leaves less-visible (and often younger) employees stepping into managerial roles after a disturbance in the head ranks, often without sufficient training or preparation.

"Ideally, it starts with the C-level and the direct reports, but it can't just stop at the management level," says Sam Bright, an analyst at Forrester Research. "There are key people on the technical side that if the company were to lose them, it would have a huge impact on performance."

Today, after the collision on Highway 92, Boehme and his staff know that no matter an organization's size or how solid and well thought out its processes, individuals matter.

"Obviously, a well-run corporation isn't about a single leader," says Boehme. "But still, what are those unsaid things that a person does or that a person contributes to that are not in the process? Those are the hard things to measure, and those are the hard things to plan for."

The pre-crash plan

In the year leading up to his crash, succession planning had come up in conversations Boehme had had with his direct reports. They had a plan laid out on spreadsheets. The document, which resembled a standard org chart,

lived in HR. It covered Juniper's C-level officers, IT executive team, and their direct reports – and not much else. This type of succession plan is typical in the majority of America's top companies, 62 percent of which use the same method, according to the Aberdeen survey. While Juniper's HR stored resumes on its system as well, Boehme says "you couldn't just press a button to get what you need".

The reason Juniper's plan went no farther was not laziness; it was, says Boehme, time pressure. During his first year and a half as CIO, Boehme restructured Juniper's operations and infrastructures in Asia, Europe and the US – each with its own networks and systems – and put them all under one umbrella. This was not just about technology for Boehme; it was a managerial challenge. The direct reports he inherited after he came on board in 2005 were, he says, lukewarm about the integration.

"Change is difficult," Boehme says. "Some people self-selected themselves out of the organization. I literally replaced the entire leadership team of the IT organization, all of my direct reports, with the exception of one."

As Boehme's some 300 IT employees and contractors adapted to a lot of change, it was hard for him to focus on a formal succession plan, at least until he conceptualized their new roles and established a new chain of command. "Because we'd just got through the restructuring, we'd just started to move to standardizing the job ladders," he says. "We'd done some of the work, but [at the time of the car crash] it was basically a work in progress."

Since his return, Boehme has made installing Oracle's PeopleSoft software, which logs employee data for succession planning, a high priority. However, he says he won't implement it until Juniper has collected sufficient information about his employees' skill sets and work histories. Experts say that's wise. An automated solution of this type is only as good as the information put into it. A lot of companies don't have enough information about the skill sets, leadership skills and experience levels of their employees to warrant spending on an automated system, notes Kevin Martin, research director of human capital management and analyst at Aberdeen. "The primary reason that companies are still paper-based is that they don't have the succession planning process nailed down yet," he says.

The ripple effect

In Moquin, Boehme had the benefit of a fairly obvious replacement while he was recovering. As a friend and colleague (they worked together at GE Energy, a \$US20 billion division of the company that Boehme worked for from 1999 to 2003), Moquin was put in charge of Juniper's IT operations and infrastructure when he was hired by Boehme in June 2006. "It was pretty clear that Danny was going to be the person we went to," says Bill Skeet, director of IT communications and Web technology, one of Boehme's direct reports. "Sometimes, it's just enough to know that when someone is absent, there is a 'Number One' that fills in, taking the Star Trek analogy."

Approval processes were shifted to Moquin, who began sitting in on the senior leadership meetings that Boehme normally attended. Almost immediately, however, Moquin noticed something obvious but inescapable: His old work didn't suddenly go away.

"The eye opener was that as I started taking on Alan's responsibilities, especially his strategic ones, I had to look to my team and start delegating both some of Alan's work and some of my own," he says.

The consequences rippled through the entire IT department. And as work was passed down the chain of command, it became clear that simple delegation had its difficulties. For instance, one IT lieutenant, Brian Nichols, senior director of business program management, was charged with overseeing an upgrade to a business process management software project that had hit some snags in Boehme's absence. But because some of Boehme's responsibilities had trickled down to him, Nichols found himself with an overflowing plate. Although it would have been desirable for him to pass the BPM project on to one of his reports, he didn't feel that any of them had sufficient management expertise to handle it on their own. "I had to step in when I would have liked to have delegated," Nichols recalled.

Nichols now says he recognizes the importance of giving his direct reports the same type of leadership training that he, Moquin and other director-level reports have received. Analysts say this is especially vital in a field like IT, where technical workers usually have the requisite skills to do the job but often lack the necessary managerial expertise. "You need

to encourage employee development beneath the managerial ranks," says Forrester's Bright. "When attrition occurs, you can't take the time to catch people up when you have a gaping hole to fill."

Boehme says that before the accident, Moquin was in the process of laying out a training program for managers and people who aspired to be managers, but "we had been somewhere between the beginning and mid-stages of laying it out". He adds they plan to continue with the program in the future to develop a deeper bench. "You need it from the bottom up as well," he says.

Clout that's hard to replace

Moquin says the momentum Boehme had established kept things moving forward after the crash. "Having everyone within the organization focused on the same goal made it easier to carry on," he says. "There weren't a bunch of different agendas."

That may have been true, but after Boehme's crash, Juniper's IT projects didn't all move forward with the same momentum they had in the past. Juniper employees say this wasn't due to a lack of leadership at the top; everyone contacted for this article lauded Moquin's leadership. But they say Boehme's C-level pull across the organization just couldn't be replaced, particularly with senior executives. "[Boehme] has relationships and understands the needs of business partners at the senior VP level," says Nichols. With Boehme out of commission, communication at that level was compromised, Nichols adds.

For example, Juniper was in the process of implementing a new document management system. The decision to begin the project had been made at an executive steering committee meeting that Boehme had attended. After the decision was made to do the upgrade, Boehme placed Nichols in charge of implementing it. Nichols found a company that had the appropriate software and bought the licences. However, when he began implementing it during Boehme's absence, a problem arose. One of the user groups didn't want it, preferring a home-grown system. "We had some pushback," says Nichols. "I had to fight that battle without Alan and without knowing the context within which the decision was made. Normally, Alan would have taken care of it."

Without Boehme – and without a subordinate with Boehme’s full authority and knowledge of the situation – a conflict that normally could have been resolved in a few hours took much longer and absorbed more energy than it needed to.

Back to normal?

Boehme takes the train to work now. His days of driving fast, sporty cars are over. He recently bought a BMW X5, which is “probably the heaviest SUV I could find short of getting a [Chevy] Suburban”, he says. He attends physical therapy sessions two to four days a week. Doctors tell him that his brain injury will take up to 18 months to fully heal. Since the crash, his blood pressure has risen and he now takes medicine for it. He still hurts. He gets tired earlier in the day. “I come home from work and the first thing I do is sit down and rest for 20, 30 minutes before I can continue with my evening,” he says.

Boehme’s injuries kept him out of the office for two and a half months. He admits that when someone misses that much time, it’s not like coming back after a vacation. It’s disorienting. In fact, he spent a lot of time planning his re-entry with Moquin, COO Stephen Elop (to whom Boehme reports) and with Juniper’s HR department. Boehme says he couldn’t pick up where he had left off. “It wasn’t like all of a sudden, I’m back,” he says.

Succession planning, however, has risen on the list of Boehme’s business continuity priorities. He says he has nearly 45 people working on the new PeopleSoft HR system. It will include areas that log employee history to help Juniper executives and managers make a more comprehensive succession plan, from top to

3 Key Succession Planning Tips

Expert advice on how to leave your business in a position to move forward when the predictably unpredictable occurs

Extend succession plans as far down the chain as possible. When a disruption occurs, “it cascades through the entire organization”, says Kevin Martin, an analyst with Aberdeen Group. “You should be prepared at every level, two to three people deep.”

Encourage people to step in for others during vacations. This builds expertise. “It’s like trying to tell if someone can ride a bicycle when you’ve never seen them ride,” says William J. Rothwell, a consultant who deals with HR management and succession planning. “An excellent way to find out is to let them ride the bicycle for short distances.”

Assess employee skill sets. This could prevent you from having to go into the market and overpay for talent you might already have in-house. “There are so many skills in demand,” says Sam Bright, an analyst at Forrester Research. “If you have to go outside, you’re going to pay a premium. You need to know what you have in-house.”

By C.G. Lynch

bottom and across the whole company.

Other companies seem to be moving in that direction as well. According to Aberdeen, 39 percent of companies report now having a fully or partially automated solution for succession planning. “Although [Juniper’s] was paper-based and it worked, the accident wakes you up to realize that it can be much more efficient if it is systematized,” Boehme says.

Boehme reiterates that Juniper will continue to train workers at all levels in leadership and managerial skills to create a deeper, more agile bench. Analysts on succession planning and human capital suggest mentoring programs that have lower-level technical workers shadow their bosses from time to time and make connections with other leaders in the business. “Establishing political relationships helps grease the wheel,” says Forrester’s Bright. “They’ll have established credibility.” And perhaps that will help avoid situations like the one Nichols found himself in with the engineering

group on the document management project.

For now, Boehme is working on regaining his energy while adjusting his schedule. He works at home more. He’s set up a special router in his house that will ensure a secure connection to Juniper’s network. He uses videoconferencing to help communicate with other Juniper sites across the globe. But more time working at home doesn’t mean taking it easy; he says he’s now as busy as ever.

The crash has given Boehme a new understanding of and appreciation for the human side of business continuity planning. “When you think of business continuity and disaster recovery, you tend to think of earthquake and tornadoes and events,” he says. Today, Boehme thinks about what most people don’t want to think about: what can happen to a person in a bad moment.

“We don’t personalize these things,” he says, “because you don’t want to wish what happened to me on anybody.” ●

Business, Gov't Systems Keep Running Despite Wildfires

IN OCTOBER THIS YEAR, Qualcomm CIO Norm Fjeldheim became one of the more than 250,000 San Diego area residents driven from their homes by the fiercest set of wildfires to ravage Southern California since 2003.

"I became concerned on Sunday night," says Fjeldheim. "I was watching the news closely and monitoring e-mail. I was scheduled to fly to San Francisco yesterday, which I cancelled. My neighbourhood was evacuated at about 10:00 [on Monday]."

Fjeldheim and his family – four people and two dogs – are now camped out in a downtown San Diego hotel, watching the news and following the latest developments in the fire, which has been burning for three days and has destroyed at least 1,000 homes and 100 businesses, according to news reports.

Yet despite the fire, Fjeldheim and Qualcomm were both on the job Tuesday. The CIO says all systems are up and running at the San Diego-based maker of wireless communications devices and software. "There have been some intermittent power issues because of the fires, but so far none of our systems have been impacted due to the backup systems we have in place," he says.

In part, that's because Qualcomm has an "Operations Readiness" team in place to respond to emergencies and IT is a part of that, says Fjeldheim. The team has been in place for many years: it was originally formed to deal with Y2K in the mid-1990s. Its scope was later expanded to handle all disaster preparedness and responses for Qualcomm. While Qualcomm's main IT facilities were not threatened by the fires as of Tuesday morning, Fjeldheim said a number of outlying buildings in the evacuation zones were being closed down as a precaution. All Qualcomm's systems and buildings can be monitored remotely, which Fjeldheim and his team have been doing for the past 36 hours. But with media outlets putting the number of area evacuations to as many as 500,000, the ability

to communicate with employees is critical, especially when it comes to keeping workers alerted to office closings in potential danger zones. To deal with such an event, Qualcomm has multiple communications systems in place to notify its employees. "We have extensive Remote Access Systems (RAS) in place," says Fjeldheim, "enough for up to 10,000 employees." And with staff needing to work remotely due to the blazes, "we can also support a very large number of conference calls for employees," he adds.

Four years earlier another conflagration swept over the region, and Fjeldheim says the company learned from that experience. "This is the second time we have had to deal with San Diego wildfires," he says. "After the last fires, we increased our RAS capacity, along with our conference call capacity."

And while Qualcomm Stadium is housing those displaced by the fire, the company is also helping fight the fire on another front: Fjeldheim says its cell phones are being used by some emergency personnel.

San Diego County CIO William Crowell says he was sitting on Torrey Pines Beach when the first fires broke out on Sunday morning. He says he smelled the smoke when he got home but "I thought it was the neighbor burning something." However, by late Sunday night, he says, "we knew we had a major issue on our hands".

At that point Crowell, who had been monitoring the fires on the news, instituted his continuity of operations plan for the IT department as the county activated its Emergency Operations Centre. For Crowell and San Diego officials, the good news is that the county's two data centres are far from the flames: one is in Tulsa and the other is in Plano, Texas, both outsourced to Northrop Grumman.

Still, Crowell has been working 12-hour shifts with other IT team members ever since Monday to support and enhance the county's Web site and its 211 emergency hotline system.

While the fires and ensuing evacuations have meant some of his staff have been unable to report to work, "We've been OK. I have a core team of key people who are coordinating various activities."

From Crowell's perspective, "our two biggest issues are to support the dissemination of information to the public through our Web and 211 services".

The County's Web site, which got about 400 visitors a day before the fires, saw its volume swell to more than 500,000 visits on Monday as residents sought emergency information about the spreading blazes. To support the increase in visitors and to speed performance, Crowell's team made technical changes on the fly to separate the emergency part of the county's Web site and put it on a separate server. IT had originally planned to re-architect the site in December to improve its ability to deal with dramatic volume increases; Crowell says it he may just do it now. "When you outsource, you can marshal the resources to get something like this done," he says.

Demand also initially overwhelmed the county's "2-1-1" service, an emergency hotline for fire and related information, says Crowell. However, Crowell's team was able to quickly scale the system up from handling 24 concurrent callers to taking 237 simultaneous calls. "Wait times are becoming reasonable again," he says, noting that they had been as long as 15 to 20 minutes during the recent peak.

"The principal issue for IT is the ability to leverage up your capacities. You test your assumptions and you see what works and what didn't. And we have done a fairly good job," says Crowell, who notes that others, including AT&T and some ISPs, have also been initially overwhelmed by the public's use of their infrastructure in the wake of the fires.

In a disaster, "everything gets overwhelmed", he says. "So everyone is facing the same issues." ●

By Steff Gelston