ITM Whitepaper

ILLINOIS INSTITUTE OF TECHNOLOGY | *School of Applied Technology*

...because knowledge is power.

Selling the Boss: Convincing Senior Management of the Need for Contingency Planning

Dave Wallenberg, Mario Russo and Batchum Mataruke
Edited by Ray Trygstad

5/22/07

www.itm.iit.edu

An Information Technology and Management Whitepaper from
Illinois Institute of Technology's School of Applied Technology

ITM Whitepaper: ***Convincing Senior Management of the Need for Contingency Planning***

The Problem: Despite more than adequate evidence that planning for business continuity in the face of disruptions and disasters is critical in today's unsettled world, many firms resist making the necessary investment in contingency planning. In our graduate curriculum in Information Technology & Management, we posed this question to graduate students:

If you were working in an organization that had no contingency plans (incident response plan, disaster recovery plan, business continuity plan, crisis management plan), what argument might you as an information security professional make to higher management as to why these plans are necessary?

The Solutions: The three responses presented here represent three very different but equally valid approaches to making the necessary arguments to senior management as to why an investment in contingency planning is essential to the health and well-being of the firm. They are also representative of the type of thought process that Illinois Institute of Technology's Information Technology & Management degree programs are designed to build in our students.

A Quick Business Contingency Planning Vocabulary:

Before we look at why we need to invest in contingency planning, we need to establish some commonly used vocabulary.

Contingency Planning: prior planning for an appropriate response to any event that could disrupt or disable business operations; most often scenario-based and normally includes incident response, disaster recovery, business continuity and crisis management

IR > Incident Response: in the Information Technology area, a response to any clearly identified attack on assets; in a broader business context, a planned response to any abnormal event that has the potential to disrupt business operations

IRP > Incident Response Plan: discusses incident identification, classification, response, and recovery, detailing specific steps to be taken when responding to a specific type of incident

DR > Disaster Recovery: the process of regaining access to the data, hardware, software, facilities and resources necessary to resume critical business processes after a natural or human-caused disaster

DRP > Disaster Recovery Plan: the contingency plan in place to facilitate disaster recovery; may include strategies to limit losses before and during the disaster BC > Business Continuity: a progression of disaster recovery, aimed at allowing an organization to continue functioning after — and ideally, during— a disaster, rather than simply being able to recover afterwards; often differentiated from disaster recovery by an assumption that it takes place at a site other than the normal place of business

BCP > Business Continuity Plan: a plan for recovery and restoration of partially or completely interrupted critical business processes within a predetermined time after a disaster or extended disruption

BRP > Business Resumption Plan: a structure which merges DRP and BCP into a single plan.

BIA > Business Impact Analysis: evaluation and assessment of potential impact of events, incidents or disasters on the organization.

SLA > Service Level Agreement: a negotiated agreement between two parties which formally defines expected and/or required levels of service to be delivered by one party to the other.

Crisis Management: actions taken by an organization in response to a an emergency situation in an effort to minimize injury or loss of life; may also serve in support of IR/DR/BC.

Argument One: Dave Wallenberg

Contingency planning is actually quite easy to justify to senior management once one has identified the business implications, the risk potentials (likelihood of occurrence), and especially the potential cost to the business of NOT having contingency plans in place.

- Often, there are regulatory requirements which demand implementing contingency planning such as HIPAA. In this case, the justification is nonnegotiable and the scope is defined by regulatory requirements and therefore becomes the minimum requirements to satisfy.
- Business Continuity is VERY different than Business System Continuity whereas the later has the scope and responsibility of the technologies to support business processes.

To build the case for contingency planning, one must perform a Business Impact Analysis (BIA). The BIA results help management prioritize contingency planning needs based on cost analysis as listed in the BIA. A form of risk management, the BIA is the most critical piece of the process because it captures and inventories the critical business processes (BP), the systems and technologies to support these processes, dependencies of the BPs such as logistics and people, Service Level Agreements (SLA) expected for each BP to be available during a DR cut-over, and costs. BIA costs break-out into 2 needs:

1. Identify the cost to the business for each business process if it were NOT included in a contingency planning. An example is a BP which generates revenue for the business. It's critical that the real cost of the loss of revenue be determined. Management decision must focus on these costs. I like to refer to this as the "Cost of Loss".
2. Identify the cost of provide a contingency planning to support each business process. This is the cost to stand-up the contingency plan operation for just one BP. These costs include technologies, facilities, logistical challenges, and more. The cost from item #1 is then compared with this cost.

One must also capture the perceived need of SLAs for each business process to be supported in a DR/BC cut-over. Sometimes referred to as Recovery Time Objectives (RTO), the SLA needs also drive the cost to support the DR solution – especially for DRP which involve technologies. An example of this might be a live database application whereas the application and the data must remain accessible during a DR cut-over making the transition transparent. Such a scenario would very costly to implement for both normal production and DR faculties operations.

A risk assessment considers the likelihood of a disaster occurring or an event which threatens business continuity. These risks can be natural disasters, fire, power failure, terrorist attacks, organized or deliberate disruptions, theft, system and/or equipment failures, human error , computer viruses , legal issues , worker strikes , testing.

The results of the BIA are summarized in presentation form for senior management review. Once justified, it is the decision of senior leadership to accept the risk and responsibility for those vulnerabilities that are remediated. These conditions become business risks accepted by senior management.

- Sometimes the decision NOT to remediate is cost and time related
- Sometimes the decision NOT to remediate is due to pending business plans which shed a different perspective on business needs. These future-state business needs should be considered.

Justifying contingency planning needs to management must focus on needs of the business which are critical, have a likelihood of occurring, and "Cost of Loss". Together, these three components define the Risk to the business.

Argument Two: Mario Russo

September 11 has awoken America and businesses throughout the world to their vulnerability to attack. Many Americans never would have imagined something like this could have ever happened, yet it did. Believing, thinking, or imagining something is not a prerequisite to making it real. W e cannot let ourselves be mislead to think that we are impenetrable or to have a "It cannot happen to us" mentality. W e need to operate under the premise that something will happen and it's a matter of if rather than when.

As upper management, you are aware that the decisions you make will either improve our corporate image, or tarnish it. W e spend vast amounts of money determining the market demands for our products, the best branding for our products and so on— but what about the sustainability of our company? How can we justify that we invest so much in ensuring we can provide the market the products customers demand, and yet not have cared enough about our needs to ensure we are able to effectively continue and recover from an incident or a disaster? I cannot stress the urgency that we need to place on contingency planning. W e need to take our heads out of the sand and look at the world around us. September 11 was not a culmination but rather a beginning. Based on reports which indicate that over 80% of businesses that underwent major incidents were never able to reopen their doors or went out of business within 18 months, how can we possibly justify not having solid contingency plans in place?

How can our firm recover from an incident when we do not have a plan to succeed? W ords of wisdom dictate 'If you fail to plan, you plan to fail'. Let this not be our destiny. Rather, let's take the lessons we have learned from the unfortunate incidents on 9/11 and use them to strengthen our ability to protect our assets.

Just as we need the servers within our server farm to facilitate day-to-day operations, we NEED to have a fully detailed and regularly updated contingency plan. W e need an incident response plan as this will help us to identify any incidents as well as respond to them in a well thought out and pre-arranged manner. How much better would it be to be ready and able to identify and handle an incident rather than wait for it to explode into something more disastrous? An incident response plan will help us be more proactive in these efforts. If an incident then escalates to a point that cannot be controlled or contained by our incident response plan and if we had a team in place to over see our contingency efforts, we would then be able to activate the disaster recovery portion of the plan. This part of the contingency planning phase could help us to reduce and minimize the time needed to recover from a disaster. Just think of the impact to our bottom line if we are able to recover from a disaster within a few minutes or hours as opposed to days!A disaster recovery plan will definitely allow us to recover in a more expedient manner since we would have already thought through multiple scenarios and already have a planned acti on plan.

Now what would we do if the disaster was just too large? W ould we just let the business shutdown and close our doors? If we had a contingency plan we could continue our process through the business continuity plan to determine how we could continue our business operations at an alternate site. Since we currently do not have such a plan this would mean we would need to attempt to come up with a solution for a major disaster in the mist of the storm, and as we all know, decisions made in the heat of battle are not always the most appropriate. If the disaster is so serious that many employees loose their lives are we prepared to address their families? W hat about their family's attorneys? If we cannot demonstrate that we have exercised due care and due diligence to prevent injury and/or loss of life we could be held liable. Having a good crisis management plan can go a long way to showing that due care was taken and that our corporation has the best interests of our employees at heart.

In the end having a contingency plan will not only prepare us to protect our assets but allows

us to continue to have something to protect. A disaster will be disastrous to our bottom line if we have no idea how to recover. Just as we need our CEO/President and all of you to guide our corporation and lead us into more profitable markets, explore new products and take new risks, we need a contingency strategy to be able to guide us and see us through incidents and disasters.

Argument Three: Batchum Mataruke

Tornadoes, hurricanes, war, fire, earthquake, floods, war, terrorist attacks, power outages: every business and organization can experience a serious incident that can prevent it from continuing normal operations. Given this fact, management has a responsibility to recover from such incidents in the minimum amount of time, with minimum disruption and at minimum cost. This requires careful preparation and planning, which is why every organization needs contingency planning.

Contingency planning is like purchasing insurance before an accident, disaster or sickness comes our way. It is a plan of action for solving unexpected problems which ease worries about the future of the organization should disaster strike. It provides plan X should plan Y fail to work for any reason. It provides assurance as to what should be done during the disaster and after disaster to minimize or eliminate the business risk. In the business world, it is critical for every company to have contingency plans in place to minimize risk to the business should a disaster occur.

Management should be warned of possible repercussions if the company were to ignore the need for contingency planning. Some of these consequences could even include going out of business if a disaster occurs or any unexpected events of a similar nature. Not having a plan will needlessly jeopardize the livelihood of all those employed by the firm. Also, by NOT having a plan, it would be far more expensive to recover company resources if disaster occurs. In addition, it would clearly increase the time it would take to recover key business processes during a disaster, which very likely would result in loss of revenue and customer dissatisfaction due to poor service which might be provided during and after a disaster. Last but not least, investors may not be interested in investing in a firm which does NOT have contingency plan in a place.

Finally we should emphasize to management that contingency planning helps a firm place themselves in a better position to cope with anyunexpected developments. W ith plans in place, a firm will not get shocked if anything unexpected happens. Contingency planning reduces indecision, uncertainty and delays when an out-of-the-ordinary event occurs. W hile a firm with contingency plans is more likely to respond rationally to an unplanned situation than a firm without plans, it also leads managers to think in terms of possible outcomes, rather than just the most likely outcome. Management should recognize that contingency planning is NOT only useful for the worst of times. It can be used in other areas by looking for smart ways to maintain more peripheral functions, or in strategies for moving quickly when new business opportunities present themselves. This can make a substantial contribution to the organization's resilience for change.

ABOUT THE AUTHORS

Dave Wallenberg, Mario Russo and Batchum Mataruke are graduate students in the Information Technology and Management degree program at Illinois Institute of Technology.

Ray Trygstad is the Director of Information Technology for Illinois Institute of Technology's School of Applied Technology and the Associate Director of IIT's Degree Programs in Information Technology and Management. He teaches courses in open-source operating systems; operating system virtualization; multimedia; information systems security management; and incident response, disaster recover and business continuity. He also teaches in the Master of Public Administration program at IIT's Stuart School of Business.

ABOUT ILLINOIS INSTITUTE OF TECHNOLOGY'S SCHOOL OF APPLIED TECHNOLOGY

Illinois Institute of Technology's School of Applied Technology offers hands-on, project-based technology-oriented education and training for both full-time students and working professionals. Courses are taught by IIT professors and industry professionals with significant working, teaching and research experience in their fields. The School of Applied Technology offers degree, non-degree, certificate, credit, non-credit programs, corporate training, short courses and seminars ranging from a few hours to several days in length. Both Bachelors and Masters Degrees are offered in Information Technology & Management and Industrial Technology & Management, as well as Undergraduate Certificates in Industrial Technology & Management, Graduate Certificates in Information Technology & Management topics and adult education/CEU courses in all fields. Our Information Technology & Management curriculum is supported by extensive dedicated laboratory facilities. We offer an comprehensive range of courses in information security and business continuity.

For more information on our education and training programs in information technology, please see http://www.iit.edu/cpd/

Illinois Institute of Technology (IIT) is a private, Ph.D. granting university founded in Chicago in 1890, offering programs in engineering, science, technology, architecture, design, psychology, public administration, technical communication, business and law.