2009

Managing Risk of IT Disruptions in Healthcare Settings: A Continuity of Operations Planning Process

Scott Dynes
Tuck School of Business, sdynes@dartmouth.edu

Stephen Pixley
Dartmouth College, stephen.c.pixley@hitchcock.org

Douglas Madory
Dartmouth College, douglas.c.madory@hitchcock.org

Managing Risk of IT Disruptions in Healthcare Settings: A Continuity of Operations Planning Process

Scott Dynes
Tuck School of Business
sdynes@dartmouth.edu

Stephen Pixley
Dartmouth Hitchcock Hospital
Stephen.C.Pixley@Hitchcock.ORG

Douglas Madory
Dartmouth Hitchcock Hospital
Douglas.C.Madory@Hitchcock.ORG

ABSTRACT

Over the last few decades, a rapid adoption of information technologies in nearly every facet of patient care in healthcare settings has taken place; the recent U.S. government emphasis on the utilization of IT in healthcare will only serve to increase the dependency of care providers on IT. As IT becomes increasingly central to clinical and business practice, health care institutions must become increasingly vigilant about preparations for continuity of operations when normal IT functions are disrupted. In this paper we describe the development and use of a process designed to manage the risk to patient safety and clinical operations due to IT and communications failures; this process includes identifying critical applications and formulating plans for organizational and departmental responses in cases of IT and communication failures. Lessons learned will be discussed in the context of enabling other healthcare organizations to use this process.

Keywords

Information risk management, health IT, business continuity planning, emergency management

INTRODUCTION

Information technology has a long history of success, and of failure. While most end-users now think of servers and networks as being fairly robust (with episodes of 'crankiness' every now and then), this has not always been the case. At the birth of electronic calculating machines in the 1940's, the expected time between failures was a few hours; even as recently as ten years ago, contracts for certain classes of internet-based services were written with an up-time requirement of 95% - meaning a service unavailability of over an hour a day was acceptable.

As the sophistication and dependability of the information infrastructure (computers, networks, software, etc.) has increased over time, nearly all business sectors increasingly rely on this information infrastructure to run the most critical elements of their business. Examples range from the financial sector, whose business is completely dependent on technology (literally, data is money), through oil refineries, which are dependent on digital process control systems to measure pressures and temperatures and to control

pumps, heaters and valves. These industries have thought about the consequences of the loss of their information infrastructure, and taken steps to assure the safety and resiliency of their operations. This contingency planning is in addition to having redundant systems that serve to make the primary systems highly reliable.

Another sector that has become extremely reliant on the information infrastructure for core operations is the health care sector. The use of information technologies such as computers and networks in health care started in earnest in the 1970s, with the development of the first electronic medical record applications (MediTech). Driven by the promise of increased productivity, increased quality of care and reduced cost (Austin 1995, Tan 1994), the use of technology has grown to the point that many hospitals are using digital systems for all major care-related activities: scheduling, medical records, imaging (X-rays, CT, MRI), communication of lab results, prescriptions, and patient monitoring as well as critical facilities operations such as HVAC and security operations such as infant abduction alert and staff access systems. A recent study on the unintended adverse consequences of healthcare IT adoption revealed the "largest theme clustered around the problem of practice disruption and loss of patient safety during system unavailability" (Campbell 2007). Given the recent emphasis on further adoption and coordination of electronic medical systems (Halakma, Leavitt and Tooker 2009), this dependency will only grow.

As hospitals become increasingly dependent on the information infrastructure, how are they managing the risks associated with IT disruptions? Results from our own research and from recent events indicate that hospitals are less than resilient to IT and communication failures.

A field study (Dynes 2006) assessed the impact of a Zotob worm infection on the ability of one middle-sized hospital to function. The results indicate that there were moderate to major disruptions to the normal routine of both clinical and business units[1] at the hospital over a period of three days. Other examples include a system failure at Beth Israel Deaconess hospital in Boston during which the delivery of care continued (Kilbridge 2003) and the recent Mytob infection of computers in hospitals in London (Leyden 2008), which caused the shut down the computer network in at least one of the hospitals, resulting in some disruption in the provision of care to patients.

At the field study hospital, localized, short duration IT failures of occur regularly; as a result many staff have come to assume that all IT failures will be of short duration. For some units, especially off-site clinical areas, staff members had developed site-specific work-arounds; none of these work-arounds have been centralized or communicated widely.

Given that IT and communication disruptions are almost certain to happen, the question becomes one of how to prepare the organization and its staff for these events. How

[1] In this paper we use 'unit' as a generic term for any organizational entity; these might be known by 'unit', 'department', 'clinic, 'division' in various organizations.

should health care organizations approach the management of the risks they face from dependency on their information infrastructure?

This paper reports on the development and use of an information risk management process at a medium-size academic hospital; we will describe the genesis of the process, the organizational incentives that led to its use, and our experience with the process. A desired result of this work is the packaging and dissemination of this process for use by other institutions; we discuss issues other hospitals might face in the use of this process.

THE CHALLENGE: MANAGING INFORMATION RISK

All firms that depend on information infrastructure for core business processes adopt some approach to managing the inherent risk; these approaches range from accepting the risk (doing nothing) to taking a very aggressive approach to information risk management (IRM) (for examples see Dynes 2005, Dynes, Goetz and Freeman 2007 and Johnson and Goetz 2007). There are major challenges facing IRM efforts in firms including attainment of institutional support and development of an appropriate process.

While it seems obvious that firms should adopt some level of information risk management practices, the incentives and drivers that cause widespread action appear limited, and include government regulation (e.g. Sarbanes-Oxley, financial sector regulations, HIPAA), and embarrassment – no firm wants their name on the front page of the Wall Street Journal in connection with an IT failure (Dynes et. al. 2007).[2] In our study case, the primary driver of the information risk management effort was The Joint Commission (TJC) [3]. TJC requires an annual hazard vulnerability analysis, and a quality improvement process to address the highest risks. At the field study hospital a routine hazard vulnerability analysis identified IT outage as a primary risk[4]. A hospital-wide exercise was then held to understand impact, and subsequently a workgroup was formed to develop a response plan and to mitigate adverse consequences wherever possible. The resulting business continuity workgroup, co-headed by representatives from Emergency Management and Information Systems was formed and has met for over a year, gathering and analyzing data, and continues to meet formulating plans.

Note that the workgroup was not focusing on the information systems (IS) unit's processes for responding to an outage; the field study hospital already had in place an existing process to develop plans for recovering from such outages, usually referred to 'Disaster Recovery' plans. IS disaster recovery plans are developed for the IS

[2] There are examples of altruistic behavior; large pharmaceutical firms and specialist oil refiners will maintain a sufficient stock of certain finished goods to assure that customers will not suffer irreparable harm should production be disrupted. There is also an element of professionalism; there are baseline IRM efforts a CISO will do just to be professional, such as deploy antivirus suites.

[3] In the U.S. The Joint Commission reviews and accredits hospitals every three years; the 'Joint' issues a set of standards against which hospitals are judged. Without the accreditation hospitals will not be reimbursed by health insurers (specifically Medicare) for services performed; successful reaccredidation is a top priority for all hospitals.

[4] The HIPAA Security Rule also requires the development and testing of both Disaster Recovery and Emergency Mode Operation Plans.

department and focus on the resumption of IT service following a major disruption. In contrast the focus of the group was on developing a plan enabling the institution to continue clinical and business processes during IT failures lasting 72 hours or less, usually referred to as 'Business Continuity' plans or Emergency Mode Operation Plans under HIPAA. The workgroup recognizes that the plans developed for these short to mid-term outages are not sufficient to address longer-term outages, but agreed upon a need to get some plan in place which could then be augmented and improved; following the completion of work on the sort-term plans (i.e. plan is written, accepted, and exercised) the planning group expects to move on to address longer term outages in a complete business continuity plan.

The challenge for this workgroup was to oversee the development of operational continuity plans by unit staff members (as subject matter experts) for use by individual units in the hospital and by the hospital's Incident Command System[5] (ICS) in the event of an IT or communications failure. The primary vision was to develop clear and simple plans that could be used effectively whether late at night or during stressful crisis conditions by 1) ICS staff to lead the organization through the outage while maintaining patient safety and continuity of clinical operations, and 2) by operational (clinical, support, and business) units in their unit-level responses during the outage (1-2 page 'cheat sheets'). This would involve determining which applications and/or devices were critical to which departments over different outage durations, and what IT downtime plans needed to be created or integrated into an overall continuity of operations plan. An additional objective was to identify and coordinate enterprise-level actions that could be taken now that would lead to greater resiliency during outages such as having Information Systems technicians develop alternative mechanisms by which patient information (e.g. electronic medical history, allergies, current medications) could be securely accessed and read if the standard suite of clinical applications were unavailable.

The set of 'cheat sheets' for the units would be concise references to assist the clinical user community. For each core software application, each 'cheat sheet' would answer three fundamental questions in terms a non-technical user could understand:

1. How do I know if this application is down and I should revert to emergency mode procedures?
2. Having confirmed the application is down, how do I request services provided by this application during emergency mode?
3. Having confirmed the application is down, how do I receive services provided by this application during emergency mode?

[5] The hospital's Incident Command is a pre-designated group of senior personnel representing core functions which is tasked with managing incidents of any type that are substantially disruptive to hospital operations.

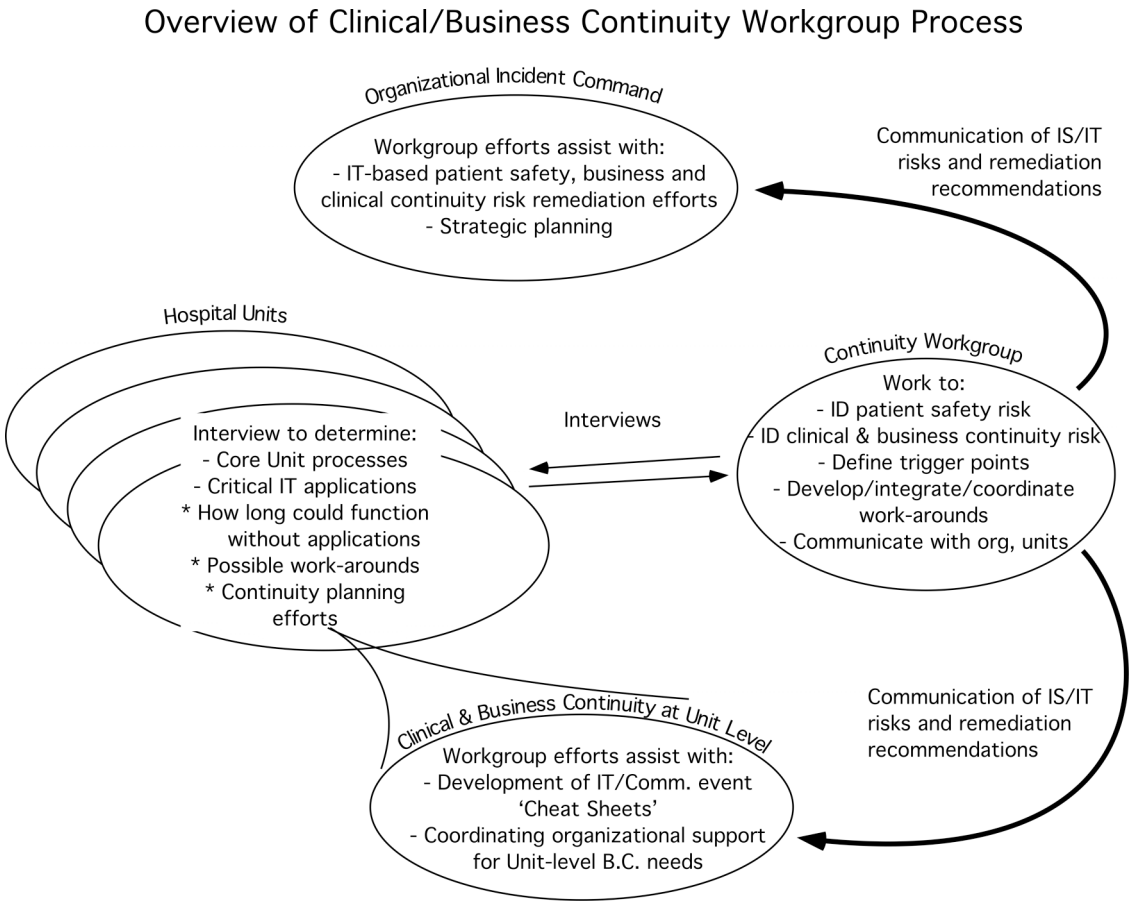

Figure 1. An overview of the efforts of the Clinical/Business Continuity Workgroup.

For example, a 'cheat sheet' for the laboratory information system (LIS) would detail how to confirm the LIS was down, how lab tests would be ordered using paper forms, which labs would be given priority during an outage, and how results would be communicated back to the clinician ordering the test.

Figure 1 shows schematically the interactions between the work group and other hospital entities. Another initiative was to discover and share work-around processes already established by individual units, and also to estimate the impact of outages by understanding which processes could be worked around, and which systems would just be out of service/unavailable.

Accomplishing this goal required the development of an appropriate methodology. While members of the IS organization believed they knew the list of critical applications, would the clinical and business units agree? Did a list of unit downtime procedures exist? While there were examples of downtime plans found in individual units, there was no higher-level integration until the creation of this workgroup. At a high level, an appropriate process would need to define the mission of the hospital, how that mission was supported by the various clinical and business units, and how technology (applications and devices, and their enabling networks/servers/etc.) supported the efforts of these units. The

workgroup examined one such process (RiskMAP, Watters 2006); this process was deemed too resource intensive for use in hospital settings. The challenge is to take general business continuity principles and develop a process that is usable in hospital environments by taking into account the complexity of hospital environments, resource and time constraints, and other realities that distinguish hospitals from businesses in other sectors. Standard business impact analysis (BIA) is a substantial undertaking which attempts to identify *de novo* the high-impact business processes which depend on IT systems. While large amounts of variation exist in the organization and operation of one hospital to another, the high-impact processes that a hospital BCP effort would ultimately discover typically consist of a standard set of information flows described later in this paper. By starting with this set of information flows, the BIA can be greatly streamlined making the process discovery stage a far more efficient and less-intensive step in the process. A streamlined BIA increases the likelihood that a resource-constrained hospital could develop an effective BCP, which would greatly mitigate patient safety issues resulting from an extended IT outage.

A CONTINUITY PLANNING PROCESS FOR USE IN A MEDIUM-SIZED HOSPITAL: DEVELOPMENT

As noted above, developing a continuity plan requires an assessment of which units, applications and devices are critical to the safety and operation of the hospital, and also when units are significantly impacted by the outages (e.g. after an outage of a minute, an hour, etc.). Contingency plans for outages of varying duration and for various types of units need to be discovered, created, and integrated to fulfill the goals of the workgroup. To aid in defining a workable problem, the workgroup decided that in the initial planning phase only outages of 72 hours or less and only those departments core to the functioning of the hospital would be considered.

The core applications and IT-dependent devices needed to be prioritized. Ranking applications can be a complex undertaking, as applications will have varying levels of importance to different units. For example, the electronic medical records (EMR) system will be highly critical to a hospitalist caring for a sick patient, but not critical to payroll – even though both are ultimately critical to the functioning of the hospital. There are additional complications, an example of which is the loss of one application that might have a major impact on one unit after 15 minutes whereas another unit could go for 24 hours before a significant impact.

Another complication is that some ‘applications’ are essentially a synthesized view constructed from the output of many separate applications. An example is the electronic medical record system, which is a unified user interface to a collection of underlying applications and databases. An outage of one component of the system can affect access to medical record information but not ability to order medications. The field study hospital has multiple such ‘applications’.

While every hospital has a unique organization and suite of clinical software applications, from the user’s perspective these applications typically enable a standard set of bi-directional information flows unique to a healthcare setting that would be acutely impacted by in IT outage:

Table 1. Tier I Applications

Common enterprise communication

- Intranet websites
- Internet access
- Radio Paging Systems (Includes Web/e-mail paging interface)
- Central File Storage
- Microsoft Exchange

Healthcare-specific functions

Accessing and editing the electronic medical record
- Electronic Medical Records (EMR) system

Ordering laboratory tests and reviewing results
- Laboratory information system (LIS)

Ordering imagery exams and reviewing results
- Radiology information system (RIS)
- Picture archiving and communication system (PACS)

Ordering medications and viewing patient medication profiles
- Pharmacy application

Registering and tracking the status and location of patients
- Patient registration application

Scheduling patients and resources such as operating rooms
- Scheduling application

Processing claims for reimbursement
- Charge capture and coding
- Automated billing application

Patient care systems which are dependent on IT services
- Patient monitoring application
- Radiation treatment system

- Accessing and editing the electronic medical record
- Ordering laboratory tests and reviewing results
- Ordering imagery exams and reviewing results
- Ordering medications and viewing patient medication profiles
- Registering and tracking the status and location of patients
- Scheduling patients and resources such as operating rooms
- Processing claims for reimbursement
- Patient care systems which are dependent on IT services

In order to prioritize applications and IT-dependent devices, three tiers were established, and the workgroup members placed applications/devices into the tiers. Tier I contained applications and devices where an extended outage of one or more of these applications would cause widespread and/or immediate impact to patient care and/or hospital

operations[6]. Tier II includes applications where an extended outage of one or more of these applications would cause limited impact within 24 hours to patient care and/or hospital operations. Tier III applications were those where an extended outage of one or more of these applications would cause minimal impact within 72 hours to patient care and/or hospital operations. The Tier 1 applications listed below represent a common set of software applications that a business continuity effort in any healthcare setting would need to address.

In order to develop a shared understanding around continuity of operations between the workgroup and the administrative and clinical managers, it was decided to conduct a series of interviews to (1 test the assumption that all application in Tier I were critical to business and clinical continuity, (2 obtain input as to additional systems perceived as critical and existing work-arounds, and (3 gather additional context around the criticality of these applications. This was accomplished through semi-structured interviews with approximately 40 individuals representing 19 clinical and administrative units. The interviews were designed to elicit at a high level the processes core to that particular unit, and the applications used in support of those processes. As an example, interviewees at outpatient clinics described all interactions with a patient, beginning with initial contact or with scheduling the appointment, and ending with discharge. Applications were noted at each step, and critical steps and applications were identified. For example, scheduling an appointment is normally done using the scheduling application; this application is noted for later discussion. Patient visits could end with another appointment, going to the lab for tests or the pharmacy for a prescription; each of these activities was supported by an application that was also noted.

Following the outlining of core processes, the noted applications were quickly binned into those that would have a significant impact on life safety or unit operations, and those that were 'nice to have'. The interviewee was then asked to fill in a chart that would depict the impact an application outage would have on a process over time; an example is shown in Figure 2. These 'Time-To-Pain' charts plot, as a function of application or device outage duration, the impact on the unit's ability to function (on the left Y-axis) and the possible impact on patient safety (right Y-axis). There are two Y-axes in order to capture the relative difficulty the unit would experience as well as the absolute risk to the hospital's core mission – providing care for the patients.

Originally, the left Y-axis breaks out the impact into 'low', 'minor disruption with a work-around', 'major disruption with a work-around' and 'can't do task'. During pilot interviews it was made clear by clinical interviewees that in some circumstances 'can't do task' is not an option however difficult it is to complete the task; the left Y-axis was modified by adding 'really hard' to incorporate this learning.

[6] Hospital operations are defined as those processes within the hospital outside of direct patient care. This includes, but is not limited to, financial and administrative functions. An extended outage is defined as a period of unavailability or degraded operation of an application for more than 1 hour. Impact is defined as a negative effect that profoundly hinders workflow.

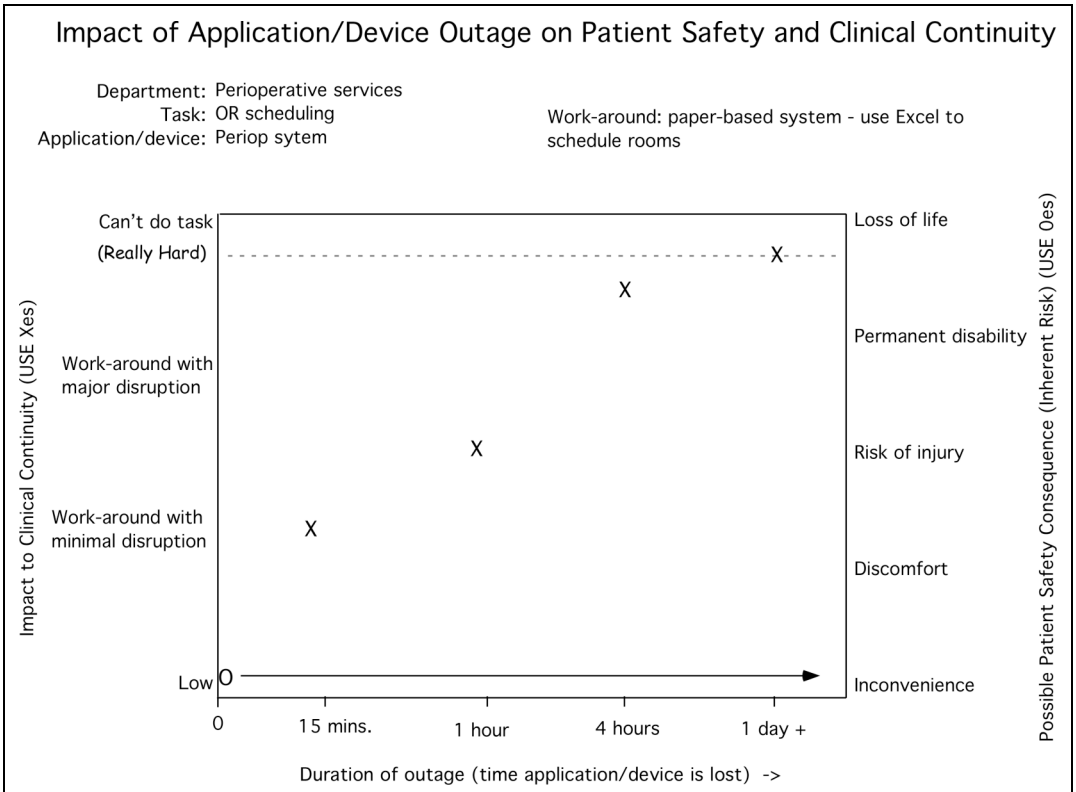

Figure 2. A 'Time-To-Pain' chart filled out by the perioperative services unit. Xes correspond to the impact an outage of the custom perioperative support application would have on the unit's ability to accomplish scheduling operating rooms for patient cases and the Oes correspond to the possible patient safety consequences as a function of the outage duration.

The right Y-axis records the potential impact to patient safety, ranging from patient inconvenience to loss of life, as a function of outage duration. When filling out the right Y-axis, interviewees are asked to think of the most serious reasonable consequence to patient safety. This measure allows comparison of TTP charts across different departments: for example, if the outage of a certain application would very quickly leave the revenue management division unable to perform a core task; on the TTP chart an 'X' would be entered at the 'cannot do task' level. For most critical patient-facing units even the loss of the most critical application would be scored at the 'really hard' level, which would make it appear that revenue management would be worse off because it could not conduct a core billing task than the emergency department, which would adapt and overcome to care for the patient. Collecting data related to the possible consequences to patient safety makes it considerably easier to distinguish between the case of revenue management, where there are no patient safety issues, and the emergency department case, where there are.

The value obtained from the interviews was manifold. First, the interactions with administrative and clinical staff were very informative as to which applications belonged in Tier I; no application that was present prior to the interviews was removed; two additional applications were added. The discussions also uncovered existing workaround plans that had been developed by individual units; this provided insight into the pending

difficulties of coordinating individual plans at an enterprise level, although several innovative options were noted.

The interviews also contributed fundamentally to the workgroup's understanding of the timeline of the impact of an application's outage on the units of the hospital. The data from the TTP charts was used to create views for use by the incident command system; during outage of the electronic medical record system, the ICS could note which units would be affected immediately, after 15 minutes, an hour, etc. Additional views will be created for use by individual departments so they will be able to develop continuity plans for the most critical applications as identified during the interviews. An overview of the process is depicted in Figure 3.

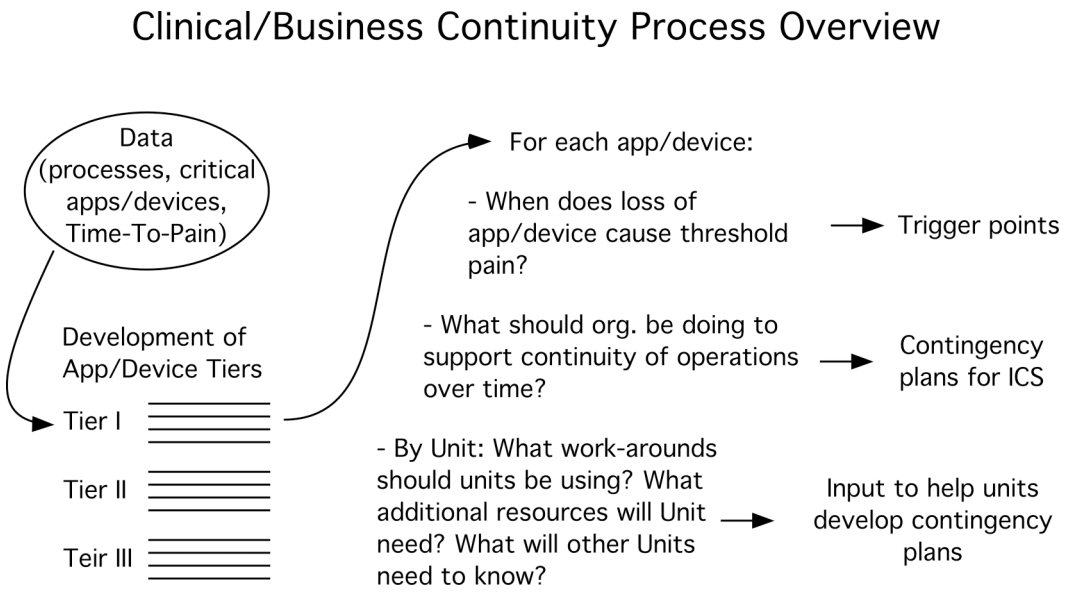

Figure 3. An overview of the clinical/business continuity process used.

One of the most important outcomes of the interview process was the development of an organization-wide view of the clinical and business continuity efforts undertaken by individual units, and the opportunities to build continuity-planning bridges between units that need to be (and in normal times are) tightly integrated from an information sharing standpoint. The interviews showed that there were a few key units that had already developed and documented application downtime/ contingency procedures; almost none of these units had spoken with partner units to develop inter-unit contingency plans. As an hypothetical example, the lab may have developed a contingency plan for obtaining samples and reporting results in case the pneumatic tube system was out that involved being called by a patient floor and dispatching a runner to get the sample. If that plan was not shared with the nursing station on the floor, it would be of little practical use should the tube system fail.

At this stage of developing a hospital-wide business continuity effort, one of the foremost challenges appears to be coordinating the actions of individual units during outages, primarily by developing alternate methods for the communication of information when

normal channels are unavailable. This effort clearly has to happen at an integrative level that has an enterprise-wide view.

At an organizational level, the second challenge is defining "triggers," the point in time at which a hospital-wide response to an outage should be implemented. In the past there was no formal process, which resulted in some outages continuing for a significant period before hospital administrators (or clinical staff) became aware of the larger situation. Triggers are designed to make clear at what point in an outage administration should be informed, and at what point the incident command system should be activated. Centralizing and standardizing this trigger process is an organizational opportunity to more clearly define and delineate unit responsibilities, both internally and externally, and to obviate the need for a subjective decision during the stress of an outage.

At the individual unit level, members of the workgroup will serve as consultants to assist units in developing their internal contingency plans. This would include using the TTP chart data to assess what steps should be taken at what time, and to make connections between units that need to coordinate their contingency plans. Through the integrative efforts of the workgroup, the result should be a hospital more robust to information disruptions at all levels.

DISCUSSION

There were multiple goals for this clinical/business continuity planning effort: the hospital expected an effective clinical and business continuity plan and the research hoped to develop an IT-to-business risk mapping process that could be used by hospitals with a reasonable amount of effort to produce useful, effective results. Although the process has not been completely implemented, enough has been completed that some judgments can be made with respect to achieving these goals.

Usability of the Process

From a usability standpoint, the major challenge was to find a process that could be used in the resource and time-constrained hospital environment. In most business environments, getting buy-in at the executive level assures that there will be cooperation in the rest of the organization. For example, when the RiskMAP process was done at an oil refinery, many refinery personnel spent multiple days working to develop the information needed for the process. This included the development of a complete network diagram for almost all network devices (e.g. routers, firewalls) and computers, which was a very significant effort.

Hospitals are not typical business organizations. Their primary incentives are humanitarian, and a sense of life and death importance is often present among clinical providers. While interviews with administrative and support staff were easy to arrange once senior leadership was convinced of the value of this data, clinical providers are not as easy to access. This demands that interactions with staff be very focused and limited; the interviews were designed to take no more than 20-30 minutes. The actual interview experience showed that interviews with administrative staff took closer to an hour, as

interviewees were quite willing to expand on points and relate stories. Physician interviewees were quite focused and succinct, but still did not find the interview protocol length objectionable. It seems that the process can realistically be used in hospital settings.

Even with access to both administrative and clinical staff, the workgroup was unable to interview all units deemed 'critical' because of finite interviewer/interviewee time availability. This will likely be a challenge in any similar hospital continuity planning effort. One approach to deal with this issue is to interview one example of each 'class' of units: interview at least one patient floor, at least one critical care unit, at least one outpatient clinic, and units that are unique, such as radiology and the pharmacy. In addition we recommend interview of supportive areas such as registration, record-keeping, and finance, as well as infrastructure areas such as security and engineering.

Can this process be successfully used by other hospitals? Conceptually, yes. The process is based on a general risk-to-mission process that can be applied in a variety of health care settings. The process described above assumes that the local IS unit knows which applications are associated with which machines, so that if an organizational decision is made to increase the resiliency of an application through redundancy that may be accomplished. This may require modification of this process if used exclusively at one site of a group of hospitals where IT infrastructure exists both locally at the hospital site as well as at the umbrella organization's headquarters; challenges may also be present in coordinating IS efforts to provide support for units during unplanned application downtime in this context.

One issue other hospitals might also consider is whether this process is best done by internal staff or by an external moderator or consultant. The challenge with internal staff is the tendency to over-utilize their understanding (e.g. of application criticality or unit resiliency to application downtime) rather than interviewing the potentially affected parties; this tendency was present in the early stages of our own study workgroup. An outside resource is unfamiliar with hospital staff and processes, and feels free to ask the 'simple' questions that internal staff may hesitate to ask, and is also unencumbered by preconceived conclusions. On the other hand we do suggest that hospital staff needs to be involved, and we support the idea that staff participation in the planning process itself is critically important. (Dwight Eisenhower said, "Plans are nothing; planning is everything."). This maxim is often quoted by our Emergency Management team, who build plans for high-risk contingencies. The planning process itself adds significantly to preparation for the event whereas a copied or outside-built plan may sit on a shelf and never be understood or trialed.

Effectiveness of the Result

It was the goal of this hospital to develop a contingency plan for IS failure. This process was used effectively to identify critical systems, and to identify existing work-arounds. This led to a gap analysis, and also to the identification of systems that will plainly be unavailable. Consequently a far more accurate assessment of impact is now possible, as well as temporizing measures to mitigate the impact. There is more work to do with this

planning process in this institution, but further focus areas are now identified and "buy-in" is significantly higher among staff and administration. Territorial boundaries are softened, and are appropriate boundaries are clearer. Was this process successful? Absolutely, although the real benefits are more than the plan itself, as discussed above.

Finally, the true complexity of clinical and business continuity planning in a hospital setting must be acknowledged. The hospital has about 130 units, and a similar number of software applications, and provides IT services and IS support to many remote clinics. A true business impact analysis would be a huge undertaking; the results complex to implement and use. This exposes the difference between planning for failure (i.e. business continuity planning) and planning for resiliency (i.e. developing a responsible, proactive corporate culture): while planning works well for failures that have happened, and can work well for foreseeable failures, it is not as effective as having people who are committed and empowered to do what it takes to make things work. This is particularly true in health care organizations, as demonstrated in other work (Dynes 2006) and in this work, where 'can't do task' was noted on the TTP charts as not an option.

ACKNOWLEDGMENTS

We would like to thank the many individuals that selflessly contributed their time, ideas and energy to this work. This work is supported in part by the U.S. Department of Homeland Security under grant award #2006-CS-001-000001 and the U.S. Department of Commerce, National Institute of Standards and Technology, under grant award #60NANB1D0127, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program which is managed by Dartmouth College. The views and conclusions contained in this document are solely those of the authors.

REFERENCES

1. Austin, C., Trimm, J., Sobczak, M. (1995) Information systems and strategic management. Health Care Management Review, Vol. 20 No. 3, pp. 26-33.
2. Campbell EM. Sittig DF. Guappone KP. Dykstra RH. Ash JS. (2007) Overdependence on technology: an unintended adverse consequence of computerized provider order entry. Annual Symposium Proceedings/AMIA Symposium. :94-8.
3. Dynes, S. (2006) Information Security and Health Care – A Field Study of a Hospital After A Worm Event http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoSecHealthCare.pdf Accessed 19-Feb-2009
4. Dynes, S. (2005) Information Security Investment Case Study: The Manufacturing Sector, http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoSecManufacturing.pdf Accessed 19-Feb-2009.
5. Dynes, S., Goetz, E. and M. Freeman (2007) Cyber Security: Are Economic Incentives Adequate? in Critical Infrastructure Protection, E. Goetz and S. Shenoi, eds. Springer, New York
6. Halakma, J., Leavitt, M. and Tooker, J. A Shared Roadmap and Vision for Health IT *http://ehrdecisions.com/papers/a-shared-roadmap-and-vision-for-health-it/* , Accessed 19-Feb-2009

7. Johnson, M.E. and Goetz, E. (2007) Embedding Information Security into the Organization, IEEE Security and Privacy, vol. 5, no. 3, pp. 16-24
8. Kilbridge, P. Computer Crash – Lessons from a System Failure, The New England Journal of Medicine, 348, 10, 881-882.
9. Leyden, John. (2008) Computer virus quarantines London Hospital for second day. http://www.theregister.co.uk/2008/11/19/hospital_computer_virus_shutdown_update/ . Accessed 13 Feb 2009.
10. MediTech http://www.meditech.com/CorporateTimeline/homepage.htm Accessed 19-Feb-2009
11. Tan, J., Hanna, J., (1994), "Integrating health care with information technology: knitting patient information through networking", Heath Care Management Review, Vol. 19 No. 2, pp. 72-80.
12. Watters, Charlton J., Analyzing Corporate Risks with RiskMAP, 2nd I3P Process Control Systems Workshop, Torrey Pines, CA., June 8, 2006. http://www.thei3p.org/docs/publications/riskmap-2009-02-26-1323.pdf (accessed 28-Feb-09)