Information Security and Health Care – A Field Study of a Hospital After A Worm Event

Scott Dynes
Center for Digital Strategies
The Tuck School of Business

22 August 2006

Introduction

Businesses are increasingly relying on technology to improve their productivity. The increasing reliance of business on the information infrastructure (i.e. networked computers, the internet) raises the issue of how resilient businesses are to cyber-events such as internet outages and computer viruses. Consequences of such events can range from minor inconvenience to major societal disruptions. This range of potential impacts reflects not just the severity of an event but also the criticality of different business sectors. The societal implications of having the bubble-gum industry affected by a information infrastructure hiccup would be very different than the implications if the same hiccup were to occur in the financial sector.

As part of exploring how technology-enabled processes can and do support the increasingly decentralized, partnered business environment, the Center for Digital Strategies has been studying how organizations are assessing and managing the risks associated with their increased reliance on technology. A core part of our current research efforts is understanding how firms think about and act to secure their business processes from technical interruptions. To do this we conduct field studies at companies and their supply chain partners in which we talk to InfoSec and supply chain managers and directors about how they approach InfoSe, and estimate what impact certain types of interruptions would have on the ability of each firm and the extended enterprise to operate. Prior to the field study detailed herein, none of the companies that we've spoken with had any experience to provide more than guesses as to what impact an event would have on their ability to operate; as such their responses were based on experience and conjecture.

In the fall of 2005 we became aware of a health care organization that had been affected by the Zotob worm in August 2005. We contacted this organization, and were able to establish a relationship that allowed us to in to conduct a field study. This field study would enable us to explore the actual impact of a cyber event on a heavily tech-dependent organization, as well as the organizational precursors and responses to this event.

We were particularly interested in this opportunity because with our field studies we are trying to sample a breadth of critical infrastructures. Our first two field studies were in

the manufacturing and oil/gas sectors, which are two of the critical infrastructures; health care is a third (the remaining sectors are: financial, communications, emergency services, government, transportation).

In this field study our research questions were:

- How the loss of the information infrastructure affected their ability to function
- What adjustments they made to offset the loss of the information infrastructure
- At what percentage of normal capacity was the unit able to function
- Whether the loss compromised the quality of care they were able to provide

Background

Methods

The field study consisted of a set of interviews with security and supply chain executives and managers at each participating firm. The interviews were designed to elicit the knowledge and beliefs of the interviewed individuals; security audits of the interviewed firms were not a part of this study. At the start of each interview, we made it clear to the interviewees that the interview was anonymous; during the interview every effort was made to build a high degree of trust with the interviewee. Interviewees at the host firm included top-level managers of information security, administration, clinical units and supply chain management. By asking the same questions of different interviewees in the same organization, we were able to look at the internal consistency of information provided in interviews and triangulated between the different data sources to arrive at a robust conclusion (Gubrium and Holstein 2002). Additionally, this approach exposed both strategic as well as tactical issues regarding information security and its role in maintaining the funcitonal ability of the organization.

Questions asked during the interviews were centered on the identification and management of information security risks, and of particular interest for this work, business continuity risk the organization faced as a result of using select technologies to enable their services and supply chains. These were open-ended questions eliciting the impact that cyber event had on the ability of their division to continue to operate. Another focus was determining the risk management culture within their division and at the hospital overall. Topics explored included their perceived reliance on technology, who was responsible for managing that risk, and the development of contingency plans for cyber events. The results of these conversations were documented, and serve as the basis for the determinations presented in this paper.

12 individuals representing six clinical divisions, three administrative divisions and three IS divisions were interviewed from October 2005 to Feb 2006 as part of this study.

Description of the organization

The health care organization consists of a main campus where the main hospital, multiple clinic and most administrative functions are located at this location. Multiple hospitals and clinics are located throughout the geographic region are owned and operated by the

organization. The Main campus acts as the ISP for these owned/operated hospitals and clinics.

The organization has both physicians on staff as well as independent but affiliated physicians that have admitting privileges. Staff physicians have access to organizational digital assets such as digital patient records, lab results and the scheduling system through the internal network; affiliated physicians have access through internet-mediated (web-based) interfaces to this information. There are also web-based interfaces for patients to access a via the internet a limited set of patient-specific information.

Internet access itself is fairly unimpeded; prior to this event inbound internet traffic was filtered by a firewall (which blocked external Zotob worm attacks) while outbound traffic was not filtered at all; the network was set up to enable easy access of the internal network by laptops.

Every division interviewed is dependent to a greater or lesser extent on information technology; this will be discussed below. As a whole, the organization is currently in the process of adopting an electronic medical records system; this system's servers are located on the main campus. Access to the included records is available via the internet for those external tot he main campus.

Across the entire organization there are several thousand Windows Pcs running primarily Win 2000; there are a much smaller number of Macs, and a handful of large Unix servers running core administrative applications.

Nature of event

As noted above, prior to our interviews this organization had suffered an infection by the Zotob worm (http://en.wikipedia.org/wiki/Zotob). The Zotob worm infects Windows 2000 machines, and then tries to replicate by looking for other vulnerable machines on the network. Zotob was developed in response to a Microsoft patch release on the Tuesday of the previous week; Zotob was present on the internet the following weekend. The Zotob worm replicated using a vulnerability in Microsoft Window's plug-n-play software; the installed worm would check for internet connectivity, and if connected, log into and IRC chat channel to listen for commands.

The Zotob worm was introduced to the hospital through a laptop that was infected external to the hospital and then attached to the internal network on the afternoon of Tuesday August 16, 2005. The worm started infecting the organization's Windows 2000 machines; the actions of the worm caused noticeable effects on the network within minutes. These effects included machines rebooting themselves, and a slow-down of the internal network due to the volume of traffic from machines testing for internet connectivity and logging into the IRC chat channel. Within 30 minutes of the first identifiable infection to the organization's network (the laptop), the issues had progressed to the point that the organization's connection to the internet was closed by IS as a defensive measure against the attacks they were seeing against their systems. This caused the volume of traffic on the internal network to greatly decrease, as the virus knew it was

not connected to the internet and thus did not try to connect and stay connected to the IRC channel. At this point the major impact of the worm was twofold: a denial of internet service, and the unavailability of many machines that had to be disinfected before they could be allowed access to the intranet (and potentially infect other machines again). Of the several thousand machines present on the organization's internal network, it is believed that at a minimum a sixth of them were infected, though that fraction could have been much higher.

The steps that were taken by the IS organization to disinfect the machines include the development in-house of a patch to clean individual machines and the largely manual application of that patch; the partitioning of their internal network into subnets; an abortive effort to reconnect to the internet (which resulted in a network flood), and a sustained effort by the organization's IS department from Tuesday afternoon to Friday morning at which time the organization's machines were disinfected and the internal network reconnected to the internet.

Description of Event Impact

Overall, while the effects of the worm had a substantial impact on the customary business processes of the hospital, there was very little to no impact on the ability of the hospital to provide health care to its patients. The administrative and clinical units of the hospital were able to provide a customary level of service for the volume of patients received, with the exception of the radiology unit, which could take images but not deliver them to physicians except in emergency situation, and the radiation oncology unit, which was not operational. While it was universally agreed that the quality of care actually delivered was not affected by the event, it was also generally felt that the event significantly increased the chances for substandard care. This will be clear from the details of each unit.

Each unit will be discussed in turn; we will start with the CTO interview, as the impression of the event impact given during this interview is rather different than the impression of the impact given in interviews with different units. We will end with the other IS units, as they will address some issues raised in the intervening interviews.

It should be noted that most all these interviews took place with the presence of a representative of the IS organization. This representative at times was an active participant in the discussions.

CTO perspective

As part of the initiation of the study the CIO of the health care organization was interviewed a little less that two months after the August worm event. As part of this interview we spoke about the organizational and IT structure of the organization, the organizational response to the event, and his perspective of the impact of the event on the organization. The structural parts of the discussion are reflected in the description of the hospital above.

One of the first point he made was that hospitals as organizations are different from organization in other business sectors – because of the nature of their business, they need to go through lots of planning for disasters/events as the hospitals need to be responsive during such events. As will be seen, this statement is at odds with the reality of this organization for this event certainly, and very probably for most cyber events.

The CTO recounted how the IS group had first become aware of the event, from calls to the help desk about machines rebooting themselves and a general slowness of the network. His group was quickly focused on this emergent event; within minutes of the surge of calls to the help desk early Tuesday afternoon, IS had the probable cause of the event as a worm exploiting a recently announced MS Windows vulnerability, and within 15 minutes of the surge of calls to the help desk IS had disconnected the organization from the internet, and began to segment its internal network in an attempt to prevent the further spread of the worm. An emergency email message was sent to senior IS personnel to convene a conference call; this conference call would continue until Friday morning, when the active response to the event by IS was considered complete.

The CTO described how the IS organization worked throughout the event to develop a script to clean infected machines (anti-virus vendors and Microsoft were not producing a disinfecting solution in a timely fashion), and how IS personnel would go around the main campus and remote locations, disinfecting infected machines, passing out notes to incoming employees giving them updates on the progress and asking them to reboot their machines. IS personnel worked diligently throughout the days and nights, very focused on eradicating the infection of their machines.

When asked about the impact of the event on the organization's ability to function, the CTO's response was that the impact was primarily to the IS organization; if I were to go talk to the clinical or administrative units, they would say that the event had no or very little impact on their unit's ability to function; the major disruption would have been the requirement to reboot their machines a few times. His reasoning focused on the fact that the core applications (digital medical records, financial, scheduling applications) continued to be available throughout the event, as these applications were running on platforms other than Windows.

The CTO saw the predominant impact to the organization as including:

- The inability of affiliated physicians to access medical records from outside the hospital (as the organization's internet connectivity was cut off).; they would have to call the hospital for patient information.

- The lack of email, an important communication channel between physician and patient.

- Clinical machines that were controlled by Windows 2000-based applications but were classified as "medical devices"; FDA regulations required that these

machines had to be maintained by the vendors, and the vendors were not very responsive in a timely manner.

As a result of this event, the CTO said that there would be changes in procedures at the hospital. Prior to this event, the hospital spent a week testing patches before applying them; now patches would be 'tested' for a few hours in a live pilot group before being rolled out to the rest of the organization.

Administrative perspective
As art of this field study directors of the revenue management and materials acquisition (the ordering of supplies) were interviewed.

The revenue management division (RMD) is responsible for generating all the claims and processing all the remittances for the organization and for coding patient claims and handling patient relations concerning billing.

The impact to the RMD was very significant, since internet-based communications are at the core of their operations. They used the internet for:

- Making insurance claims - claims are process daily; any delay causes blips in cash flow. The outage happened during mid-month, which was the best time for an outage. If it had happened at the end of month the impact would have been greater.
- Remittance processing – RMD needs to access to records of payments from insurance plans; during the outage RMD couldn't post payments to accounts because they could not reconcile payments and deposits.
- External communications (email) to vendors - email stayed up internally after an initial outage
- Web access – RMD workers access external web sites for information such as eligibility, prior authorization, precertification, etc. None of this happened during the outage.

Thus, the internet outage that resulted from the event impacted RMDs operations; the director noted that during the first day they were operating at 30-40% of capacity from the perspective of keeping people busy (e.g. filing paperwork), but 0% from a mission standpoint. Gthe use of phone or fax was not a possibility considered during this event; all communications with business partners (e.g. insurance companies) are EDI transmissions.

On the first day of the outage (Wednesday), the director had discussed with the IS department the possibility of getting access to the internet for their needs; the response was that getting access for RMD "was not a priority". As the outage lasted into Wednesday and Thursday the director of RMD started to develop work-arounds, primarily working with employees and business partners and clearing houses to enable the sending and reception of EDI transmissions from the homes of workers, whose cable internet access was available, and working with IS to open the firewall to allow certain machines access to certain web sites. As a result of these work-arounds, by the end of the event (Friday) RMD was able to effectively function at 100% of capacity, handling the

normal load of claims and remittances. The director of RMD felt that they would have been able to maintain that level of performance indefinitely. After the organization's IT systems had been disinfected, the manager estimated that it took about a week before all functional consequences of the event (i.e. unanswered email, progress on non-critical projects) had been cleaned up.

When asked about how RMD assessed and managed the risk due to their reliance on the information infrastructure, the manager said that no thought had been put into being so IT dependent, and that there had been no contingency planning for cyber events; the sense is that there will be no formal contingency planning in the wake of this event.. The manager felt that it was the IS department's responsibility to manage the risks associated with being IT dependent. When asked about the relationship between RMD and IS with respect to InfoSec, the manager said that RMD had no input into the IS InfoSec agenda. The manager thought that while the worm event had been disruptive, the loss of internal applications would have been worse.

The materials acquisition department (MAD) is not located on the main campus, but a couple of miles away at the supplies warehouse. The materials ordering and stocking process at the main campus is based on an enterprise resource planning (ERP) system which runs on a non-Windows machine on the main campus; because of organizational history MAD houses a separate IT staff devoted to the maintenance of the ERP application.

At the main campus hospitals and clinics, while the supplies may be located on carts or in closets or elsewhere, these locations are generically referred to by MAD staff as "PAR carts". In each clinical unit are individuals (e.g. nurses or technicians) who are responsible for ordering additional stock as needed. The typical way this is done is by using a computer-based interface to the ERP system to order what is needed. The ERP application maintains an internal database of the state of all supplies in the warehouse; if there are sufficient supplies in the warehouse to cover the request to restock the PAR cart, the ERP application will generate a pick list that MAD staff will use to pick the proper items for transport to the PAR cart.

If there is not sufficient stock in the warehouse, the ERP application will add an order to the appropriate vendor(s) for restocking the warehouse to a list of vendor orders. This list is processed a few times a day by creating a single order for each vendor that is then sent via the internet to the vendor.

As the department was formed, it was realized by the director that there would be risks from using technology to enable their business processes, that there would come a day when the technology will not work. As a result contingency plans had been developed in the case of an IT/cyber event. These contingency plans consisted of developing for every requester a paper "favorites" list that contains the most commonly ordered items; the requester can copy this list and enter restocking orders and deliver or fax the order to the MAD. At the MAD level, there were paper POs for each vendor that the MAD staff could fill out and fax to vendors. This contingency plan is very labor-intensive; for this reason it

would not be implemented if an event would likely be shorter than six hours. From the buffer of supplies maintained on the PARs and in the warehouse MAD staff determined that this contingency plan was sustainable for roughly 48 hours; if an event went longer than that then the MAD would enter "all hell has broken loose" phase and bring in temporary help to help with paperwork. MAD had discussions with other directors to discuss this issue; plans are to bring in 2-3 temps to do data entry.

MAD staff first became aware of the worm event because the ERP application could not access any internet sites. At this point the primary question within MAD was figuring out how long the event would be; as noted above, if it were going to less than 6 hours MAD would rather wait for the ERP system to come back on line. Around noon on TuesdayQQQ the MAD director, having seen reports that CNN and NBC had been struck by Zotob, determined that this was a major event and kicked off the contingency plan. Even though this resulted in a much more manual process for reordering supplies, there were no outages of supplies, either at the warehouse or in the hospital or clinics on the main campus. After the event was over, the director of MAD estimated that it took MAD staff 1.5 days to enter the paper-based orders into the ERP system, and to run the ordering system to restock the warehouse for the draw-down that occurred during the event.

For the director of MAD, the division of risk and the management of risk is pretty clear. MAD assumes the risk for the use of and the management of the ERP application itself; IS assumes the risk for the hardware that the ERP application runs on and internet connectivity.

Clinical perspectives

Six clinical units were interviewed: the radiology unit, the perioperative unit (which handles pre, trans, and post operative care), the emergency department, orthopedic surgery unit, internal medicine, and the pharmacy. All of the clinical units depend on software applications to run their units to some extent; units were affected because the workstations that are used to run or access the applications were unavailable.

For all practical purposes, the radiology department is completely digital: scheduling is handled via a computer application, and the machines that take X-rays, CT or MRI scans produce digital images (exception: mammography is half film, half digital). These digital images are moved to a PACS (Picture Archiving and Communication System), where they are broadly available to physicians accessing the organization's intranet via the electronic medical records system.

Because of its great dependence on technology, the radiology department maintains an in-house IT capability devoted to the maintenance of its machines.

The radiology department first became aware of the event due to the slowness of the internal network, which slowed to the point that it was not possible to use the patient scheduling application or upload images to the PACS. Radiology would be unable to upload images to PACS for the next 24 hours; this meant that physicians were not able to

read new images. In addition to the slowness of the network, several of the machines that radiology uses to take or hold images were infected with the worm.

As a work-around for the unavailability of images, an attempt was made to print out the images to a laser printer. The volume of patients being seen made this impractical, and this work-around was discontinued. Patients would come to have an image taken, and be told that the doctor would read it later, and to expect the results in a few days. One work-around that was effective was to bring physicians to read images on the machine used to take them – the X-ray, CT scanner, etc.

The operations manager noted that since Microsoft seemed to be taking a while developing a patch, radiology used the patch developed by the organization's IS department. With respect to the machines that are used to take and store images, the operations manager said that some machines had sufficient anti-virus protection, and some did not. The operations manager said that the vendors were hands-off with respect to anti-virus software: "they don't want to deal with it". As a result, the radiology IS team deals with antivirus and worm issues.

The overall result was that although the worm "was a huge disruption" for the normal operations of the radiology department, no patients were turned away: scheduled patients were seen, pictures were taken (although not read immediately); emergency images were taken and read in a timely manner by having the emergency department clinicians walk to the machine's location. According to the operations manager, all the images stored on the acquiring machines (i.e. the X-ray, CRT, etc. machines) were transferred to the PACS and available to physicians 2.5 hours after the 24 hour outage ended (this would be sometime Wednesday). He went on o say that he is pretty sure (but not certain) that all the images were read and notes dictated over the next 15 hours.

The operations manager said that from the start, their reliance on technology was a concern and over time developed plans in case technology failed. The basis of these plans was the belief that they were dependent on the PACS or scheduling system manager or IS to resolve any technical issues; the plans themselves consisted of who to call if a particular technology was experiencing problems. As for who is responsible for managing risks, the operations manager thought that it was a shared responsibility between the radiology department and the IS department to manage the risks.

The orthopedic surgery clinic (which is separate from the surgical department) is a consumer of images from the radiology department. Orthopedic surgery is part of the orthopedics department; patients come in to the clinic for evaluations, surgical procedures, and follow-up. Technology is used primarily in scheduling, imaging and the organization's electronic patient records system. According to the practice manager, the initial difficulty experienced by the clinic Tuesday afternoon was the inability to schedule patients. Workers could see the schedule, but could not make changes. The work-around was to write the patient's name down and call back when a time could be arranged. The practice manager stated that the unavailability of the scheduling system was the major impact of the virus.

Wednesday morning the radiology image server was down (PACS); this was a big problem, because if clinicians can't view an image, they could not make a diagnosis. The work-around was to tell the patient that the clinic would call later when the image had been read. The practice manager said that radiology was able to figure out a way that images could be viewed fairly quickly on the internal network, if not through the normal mechanism. This is in agreement with radiology's assertion that images were available 24 hours after the start of the event.

One point the practice manager made repeatedly was that the electronic medical records system "came back pretty quickly". This individual's recollection is that the electronic medical records system was unavailable for some period of time. The practice manager's opinion was that of the electronic medical records system were unavailable that would be a huge deal because without medical records there would be very little or no care. This assessment was shared by other clinical units.

The orthopedic surgical unit did not seem to have a contingency plan; when asked about whose job it was to assess and manage the risk due to reliance on IT, the manager said that his gut feeling was that it was the IS department's responsibility. The clinic had talked about having a liaison with the IS department, but the resulting arrangement was not collaborative enough to be beneficial.

The emergency department (E.D.) also relies on technology, specifically for patient management, dispensing medicine and information retrieval and other needs. The workflow in the E.D. is reflected by a software application that makes visible where patients are, how long they've been in various phases of treatment, the members of their treatment team, etc. The E.D. staff depends on this view to enable the efficient operation of their clinic. During treatment, a physician might want to consult some information; the physicians will commonly use external web sites to access that information. If a physician fills out a prescription, that prescription will be entered in to the hospital's pharmacy management system, which will enable the dispensing of the medications from drug cabinets located in the E.D.

The director of nursing, also the practice manager for of the E.D.'s physician group said that overall, the impact of the worm on the operations of the E.D. was "moderate". In the E.D. the impact of the worm was first felt because the E.D. staff was having difficulties entering patient names into the pharmacy management system; as a result they had difficulties in getting medications out of the drug cabinets in the E.D. The patient management system stayed up, although most of the workstations the staff used to access the system were down. As a result, the normal flow of movement was interrupted, because particular machines that were heavily used were unavailable, and staff would have to look elsewhere for one of the few functioning machines that became crowded and a bottleneck. Because the organization's connection to the internet was cut, E.D. staff could not access web sites and information sources they would usually use.

Despite these difficulties, the director said that “nothing stopped happening”, that the worm did not impact their ability to treat patients. He felt that they could have continued “almost indefinitely” given the volume of patients being seen by the E.D. at the time of the worm event. He did say that the volume of patients seen by the E.D. can vary greatly; the volume during the worm event was not demanding.

During the event steps taken to mitigate the effects of the worm included treating the workstations very carefully so they would not crash and require a reboot, and setting up a whiteboard in case the patient tracking system failed. The director said that while they are dependent on technology they are not as dependent as they should be. He thinks that processes are not adequately automated. From a risk management and contingency standpoint, the E.D. department did not have a contingency plan for technical failures; the director thinks that the IS department is responsible for risk management regarding the use of IT in the E.D.

The pharmacy is more dependent on technology than the E.D. The pharmacy controls the dispensing of medications to patients; this process is largely automated. There are a few software and hardware components to how a written prescription from a physician results in the delivery of medications to a patient. The main instances of hardware and software divide along the lines of medication ordering and fulfillment. A pharmacy supervisory application handles the patient accounts and the prescriptions each patient has as well as the billing for medications received. This supervisory application ran under DOS at the time of the event and was functional throughout. The supervisory application interfaces with the organization’s financial system for billing information, and with a different set of software/hardware systems for prescription fulfillment.

The first class of these are drug cabinets, two of which are present on each patient floor, and which were referred to in the discussion of the emergency department. These cabinets hold medications commonly prescribed on each floor; nursing staff can use these machines to fill preplanned medicine regimens, or to get an additional pain killer. The drug cabinets keeps track of which patient receives what medications for billing purposes as well as keeping track of its internal stock of drugs.

Each remote drug cabinet communicates with a server application via the internal network; the software resident within each cabinet runs on Windows 2000, and thus was vulnerable to the Zotob worm. The supplier of these devices does not install anti-virus software on these drug cabinets; while software maintenance (patching of the OS in the cabinets) can only happen from the central server, it was the experience of the pharmacy IS team that trying reboot the cabinets from the central server is works as often as not, and that to complete the patching requires someone to physically visit the cabinet and reboot it.

The second class is a robot that fills prescriptions of less-common medicines by automatically picking and placing in envelopes bar-coded plastic baggies of individual doses of medications. This machine did not have antivirus software either. Both classes of prescription fulfillment software/hardware are maintained by the vendor and local IS

teams; patches are released by the vendor with installation instructions; it is up to local IS teams to download these patches and install them.

The pharmacy department first became aware of the worm when the organization's IS department told them that they were going to remove the drug cabinets from the network unless they were patched. If the drug cabinets are isolated from the network then new patients cannot be uploaded and thus nurses will not be able to get the prescribed meds for new patients. Accounts differ as to whether for some period of time the cabinets were isolated from the network until a patch was applied. If they were, there was a back-up procedure in which all prescriptions would be manually filled in the pharmacy in the basement of the hospital. In this process, physician's prescriptions would still be written by hand ot the pharmacy, but instead of being entered into the supervisory application and communicated to the drug dispensing systems, the medications would be picked by hand and hand delivered to each patient. This backup process is requires much manual effort and cannot support the pharmaceutical needs of the hospital; the drug cabinets would be set to an "inventory" mode where all the individual drug drawers would be accessible. Again, the interviewee was not certain whether this manual back-up process was used during the worm event.

One unique aspect of the pharmacy is the relationship between the drug cabinet vendor and the organization. The pharmacy systems coordinator said that while the vendor retains authority over the drug cabinets and robot, they are not active participants in the management of these machines – the sense was that the local IS team has the responsibility to maintain the machines, but not the authority to do anything with the machines. It was only through working directly with the vendor that the local IS teams were able to get permission to install the patches in the machines.

Perioperative services in the main hospital is very dependent on technology – the result of starting to automate its processes over twenty years ago. As of the time of the event, the homegrown system had been built to the point where anyone associated with perioperative patient care (scheduling, pre-operative admission, prep, transoperation, post-operative care) depended on the application to get at necessary information; displays throughout the surgical floor would display the status of patients, OR suites, etc. This system was integrated with the lab IT system so that surgical staff could order lab analyses of blood or tissue and receive results; documentation was entered into the patient's record at the point of care.

The operating room (OR) staff became aware of the worm event when they received an electronic message from the organization's IS department saying, in effect, 'the worm is here (present in perioperative dept. machines) and to shut all machines down. This came when there were more than a dozen patients in OR suites. The perioperative experience with the worm was that over the next 3-4 days machines would be disinfected and then reinfected; as a result nobody was certain if a machine was usable or not.

The administrative director of the surgery department described the experience of trying to run perioperative services without the supporting application as "a living hell". When

the application was not available everyone had to revert to paper documentation. Lab slips, etc., a situation very few were familiar with due to the length of time the supporting application had been in use. This manual work-around resulted in much uncertainty but no change in productivity; the surgical department still worked at 100% of capacity. Unlike the situation in the pharmacy and materials acquisition department, the consequences of the event lasted significantly beyond the event itself. All the paper documentation and notes generated had to be entered into the system, and 3-4 days after the event ended the perioperative staff was still finding missing documentation.

When assessing the risk to perioperative services as a result of being so dependent of technology, the director said that he had never even considered what would happen if machines were infected with a virus or worm. When asked who is IT risk identification and management he said, “We all are”.

The general medicine department is the primary care provider for patients and their health care needs in the hospital. The administrative supervisor was interviewed as part of this field study; the top three challenges that his staff faced were scheduling, the patient experience, and insurance/billing processing, which occurs when a patient first arrives at the clinic.

The scheduling activity is supported by a software application that runs on a mainframe in the IS department. While the application itself was available during the event (because it ran on an OS other than Windows 2000), access to it from the Windows workstations that workers use was not. As a result, the current schedule could not be seen (unlike the orthopedic surgery clinic case) and new appointments could not be made. Work-arounds included getting IS to do a dump of the scheduling system database, and much manual scheduling by taking possible appointment times from callers and walking around to see what physician’s schedules looked like. The scheduling application would automatically weekly print out a list of the upcoming week’s appointments; the internal medicine staff would automatically immediately toss these in the recycle bin. An effort was made to find this printout.

The administrative director spoke of the impact that the event had on the patient experience. In the internal medicine clinic patients are used to having physicians take notes on laptop computers; during the event notes were taken on paper. Patients were told that the clinic “was experiencing technical difficulties”. Physicians at times also had difficulty getting information they wished to provide to patients as well as getting medications for patients. The director also spoke at some length about the frustration experienced by her staff and clinic physicians; “you would have thought this was the end of the world”, he said. Staff had difficulties adapting to the paper-based scheduling; clinicians were upset about double-bookings and having to write, rather than dictate, notes. According to the administrator, patients got to see the internal stress "up close and personal"; this did not affect patient trust as long as they got to see a physician.

According to the administrator, there had been no contingency planning in the internal medicine department; while this event was disruptive, losing access to email and the

electronic medical records system would have been worse. As for risk identification and management he thought that it was split between his department and IS: IS should stick with what they know, and his department was responsible for developing contingency plans for their own processes.

Further IS Interviews

After the interviews detailed above it was clear that there was a very different message coming from the CIO and the department representatives. During the CIO interview, the CIO was clear that he thought that the worm event had little to no impact on the operation of administrative and clinical departments; the interviews demonstrated that this was not the case. This and the stated dependence on the electronic medical records system led us to conduct interviews in the IS organization with managers of application development.

The first interviewed manages the development and support of the application used to support the perioperative unit as well as the scheduling application used by some departments of the hospital. During the worm event, his team of programmers did not develop any code for two main reasons: their development workstations were locked down to prevent the spread of the worm, and they were busy helping running the "fire drill" to locate and disinfect the organization's infected machines. This manager said that the organization's major applications run on non-Windows machines and remained available throughout the (event even if the Windows-based workstations used to access then were unavailable); his view is that the primary mission-critical uses of the internet are to send dictated examination notes to be transcribed, and receiving the transcriptions. The manager said that recently commercial off-the-shelf applications running on Windows servers had been purchased for use by certain departments but managed his group; some of these may have been affected by the event.

His group develops software using an application development and server environment descended from MUMPS and used primarily in the health care sector. The manager said that all of IS is aware of HIPPA and the security and privacy requirements HIPPA imposes on the applications they design and develop. His group has not paid a lot of attention to assuring the reliability or availability of their applications in the face of cyber events. The manager said that "because we run VMS [an uncommon operating system], we don't get involved with the OS level of stuff". They have taken no actions relating to possible virus attacks on VMS; they rely on the vendor of the application development and server environment they use to assure that the environment is secure from cyber threats.

At a higher level, the manager did relate cases of weighing the risk of making certain business processes dependent on the internet. As an example, he talked about the decision to move the transmission of dictated examination notes to transcribers from phone lines to the internet. The concern was that if the internet was unavailable, there would be no transcription of notes. This risk was discussed within the IS organization at the level of IS managers, the CIO and the director of data communications, who was "quite vocal" about the need to have a contingency plan in this case; the discussion weighed the risk of interruption against benefit from cost and other factors.

The second interview was with the director of the electronic medical records application. The electronic medical record (EMR) system is envisioned to be the repository for all clinical information; at the time of the event it was the authoritative repository for clinical information and provided mechanisms for clinicians to enter information. The EMR system was used by thousands of clinicians at the main campus and the organization's other hospitals and clinics. The EMR was a 'view' created from information present on IS and other servers; the EMR interfaced with well over a hundred other applications that provided information, including applications from business, financial and clinical departments. Examples include radiology's PACS system, other departmental systems, documents such as living wills that are scanned in, and information living on third-party servers.

During the event the director's team also stopped normal development to assist with the "fire drill". According to the director, even though the application itself was not affected (because it ran on a non-Windows server), because of network congestion and the effect the worm had on workstations used to access the application the EMR system was effectively unavailable for the first couple of hours of the event. During this period people might write a paper note, or try to work through the slowness – people stuck with it. He said that the EMR system has never failed.

The director was well aware that workers are very dependent on the EMR system. The team had taken steps to create redundant ways of doing certain things, such as prescription writing. They were looking at what the critical information elements (e.g. medical records) were so that they could develop redundant ways of getting at all the critical information.

While the director did not talk specifically about actions relating to the management of risk associated with the organization's dependence on the EMR system, he did talk more broadly about how the worm event was changing the perception of risk identification and management within the organization. In his view, the Zotob worm event was the first real troublesome event that the organization had experienced; as a result clinical departments were starting to have formal discussions about what else could happen. There would be presentations to department leaders and directors at which questions such as "what are your backup plans?" and "what are your sources of risk?" were asked. These presentation were given by the CIO, the IS departmental liaison group and organization-level steering committees. According to the director, at the time of the interview it was not clear who within the organization would be developing backup plans: IS, the clinical departments, or someone else. As part of the response to the worm event, the organization had hired external consultants that were assisting with the identification of risk; the director thought that this was not just IT risk, but business risk as well.

Emergent Themes/Discussion

The will to succeed

Throughout the interviews it was clear that the main focus of everyone throughout this event was the continuity of patient care. The attitude of the clinical department managers was, “we can’t stop, we just have to do what it takes to keep on going”. The result was that even though some departments experienced major disruptions, patient care delivery remained at normal levels.

This is not to say that the worm event did not affect the delivered care. Interviewees in clinical departments felt that while the actual care delivered was not compromised, the risk of sub-standard care was increased. The administrator of the perioperative unit was clear on this, saying “if we have to go backwards and do it [record notes, document procedures, phone for labs results] by hand, it sets us up for failure." His concern was both around the execution of operative procedures – worrying about waiting 2-3 times as long for lab results, wondering if nurses are going to pay attention to the computer screen to make sure an order for blood went through - as well as to rigorously documenting what happened during the procedure, where not documenting the serial number of an implanted device could be very costly. He was also concerned about the lack of experience his staff had with using paper forms.

The inability of the radiology department to share images was also a concern. While in acute cases images could be read by clinicians at the point of imaging, the reading of other images was delayed by up to two days. Nobody felt that this had in fact adversely impacted care. While it is unknown if a 40-hour delay in reading images would impact care, it could very conceivably adversely impact the perceived quality of care.

The radiation oncology department faced this issue more directly. The machines that deliver radiation treatment to patients is based on a Windows 2000 platform; these machines were infected with the worm and were unavailable for treatment. These devices could not be disinfected and patched by local IS resources; it was necessary for the vendor to take those actions. As a result, these machines were unavailable for three days, and none of the patients scheduled for treatment during those days received any treatment. This was the only example of a clinical department that was unable to deliver care as a result of the worm.

Risk management

One very prominent theme was the level of consideration the organization gave to the risks it faced as a result of being so dependent on the information infrastructure. At the departmental level, none of the clinical departments had thought about or developed contingency plans for the time when technology failed. The perioperative department which had spent years developing applications to support its business operations, had never considered the consequences of their systems being infected by a virus. The radiology department, which acknowledges being very dependent on technology, has developed contingency plans to the extent of knowing who to call if something needs fixing.

Only the materials acquisition department had considered the consequences of their technology failing; they had explicitly recognized that at some point this would happen and had worked through a contingency plan. The results of this planning were the development and distribution of 'favorites' lists for re-ordering supplies to consumers as well as developing paper-based backups and staffing plans for their department.

The director of the electronic medical record (EMR) system had put some thought into contingency planning for a case where the EMR system would not be available; the results of these considerations was the development of redundant methods for doing certain tasks; his department is currently starting to identify all critical processes in a systematic manner.

The disconnect between IS and business

Another clear result of the interviews is the chasm between the perceptions of the IS department and the business departments regarding the impact of the virus. Following the initial interview with the CIO we were questioning the utility of even conducting interviews with other departments because of the CIO's certainty that the worm event had so little impact on the operations of those departments. As detailed above, the worm event had a moderate to major impact on the operations of departments. A representative of the IS department was present during the great majority of interviews; in response to interviewee comments about the difficulties faced by their division this individual would note that IS had done a good job. When an earlier version of this report was presented to the organization's information security steering committee, which included the CIO, the CIO more than once would interrupt to say that the EMR system or a scheduling system were available when interviewee statements to the contrary were quoted.

These behaviors indicate that the IS department takes a very parochial view of its job. In fact, the EMR and scheduling applications were available because the non-Windows machines on which they ran were not affected. The challenge was at the departmental level, where the workstations used to access that applications were unusable, or the network was so congested that the applications were not responsive. While IS certainly put much effort into disinfecting these machines during the event, during the interviews and presentation IS acted as if the health of these machines was not their concern.

The extent of this very local view of responsibility for information security is all the more striking when compared to that of other firms. During the course of this field research, we have interviewed over a dozen companies from different business sectors. This health care organization is the only firm where business directors are pushing for the IS organization to adopt greater levels of information security: in every other case it is the IS organization that is trying to get the business units to invest in and adopt greater levels of information security. In other organizations, the path to greater information security is not technical, but social; here the greatest challenge is likely organizational.

References

Gurium, J.F. and J.A. Holstein (2002). **Handbook of Interview Research**, Sage Publications, London.

Yin, R. K. (1994). **Case Study Research: Design and Methods**, 2nd edn. Thousand Oaks, CA: Sage