IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4604

Identifying Security Threats and Mitigating their Impact: Lessons from Y2K and 9/11

Laura Lally
BCIS/QM Department, Hofstra University
Hempstead, NY 11549-134
516 463-5351
acslhl@hofstra

ABSTRACT

In the Post 9/11 environment, there has been an increasing awareness of the need for information security. This paper presents an analysis of the Y2K problem and 9/11 disaster from the perspective of Lally's extension of Perrow's Normal Accident Theory and the Theory of High Reliability Organizations. Insights into: 1) how characteristics of the current IT infrastructures make disasters more likely and 2) how IT can be used to identify future threats and mitigate their impact in the future, emerge from the analysis.

INTRODUCTION

In the post 9/11 environment, Information Technology managers have become more aware of the importance of security. Throughout the 1990s, IT security faced a wide range of new challenges. Yourdon (2002) places these challenges in three categories:

1) More organizations are dependent on the Internet for day-to-day operations.
2) An increasing number of computer systems, networks and databases make up a global IT infrastructure. Individuals, organizations and nations are "increasingly "wired," increasingly automated, and increasingly dependent on highly reliable computer systems" (Yourdon, 2002, p. 96).
3) IT managers faced more sophisticated and malevolent forms of attacks on these systems. Unlike the Y2K, problem, which was the result of an innocent bad judgement, "the disruptive shocks to our organizations are no longer accidental, benign, or acts of nature; now they are deliberate and malevolent." (Yourdon, 2002, p. 205).

This research will present an analysis of the sources, propagation and potential impacts of IT related threats. The Y2K problem and the information technology implications of 9/11 will be used to illustrate the analysis. The analysis will focus on both: 1) how the current IT infrastructure allows for the propagation of IT based threats, and 2) ways in which available IT tools can help identify potential threats and to mitigate their impact.

EXTENDING PERROW'S NORMAL ACCIDENT THEORY AND THE THEORY OF HIGH RELIABILITY ORGANIZATIONS

This analysis will draw on Lally's (2002) extension of Perrow's Normal Accident Theory (1984, 1999), as well as the Theory of High Reliability Organizations. Perrow developed his theory studying complex systems such as nuclear power plants. He distinguished characteristics of systems that would permit single failures, called "incidents" such as an operator error, to propagate into major accidents such as meltdowns. Systems that had these characteristics were likely to be subject to accidents in the normal course of their operation. Perrow concluded that accident prone systems are more:

1) **Complex**—with multiple versus linear interactions, and invisible interactions with only the "Tip of the Iceberg" visible, leading to the problem of "unknowability,"
2) Tightly coupled—with no slack time to allow incidents to be intercepted, and
3) Poorly controlled—with less opportunity for human intervention before problems spread.

Lally argued that Normal Accident Theory is a sound theoretical perspective for understanding the risks of Information Technology, because IT is:

1) **Complex**—The hardware that makes up IT infrastructures of most organizations is complex, containing a wide range of technologies. Software often contains thousands of lines of code written by dozens of programmers. Incidents such as bugs can, therefore, propagate in unexpected ways.
2) **Tightly coupled**—Both hardware and software are designed to increase the speed and efficiency of operations. Incidents such as operator errors can quickly have real world impacts.
3) **Poorly controlled**—Security features are often not built into systems. Testing of software is often inadequate in the rush to meet release deadlines.

Researchers in the Theory of High Reliability Organizations have examined organizations in which complex, tightly coupled, technologically based systems appeared to be coping successfully with the potential for disaster. Their studies of the Federal Aviation Administration's air traffic control system, the Pacific Gas and Electric's electric power system, including the Diablo Canyon nuclear power plant, and the peacetime flight operations of three United States Navy aircraft carriers indicate that organizations can achieve nearly error free operation (La Porte & Consolini, 1991; Perrow, 1994; Sagan, 1993).

High reliability organization theorists identify four critical causal factors for achieving reliability:

* Political elites and organizational leaders put safety and reliability first as a goal.
* High levels of redundancy in personnel and technical safety measures.
* The development of a "high reliability culture" in decentralized and continually practiced operations, and
* Sophisticated forms of trial and error organizational learning.

The two theories have been contrasted as "pessimistic" — Perrow's contention that disaster is inevitable in badly designed systems, versus "optimistic" — La Porte's pragmatic approach to achieving greater reliability. The theories, however, are in agreement as to which characteristics of systems make them more or less accident prone.

Lally applied these theories to various aspects of Information Technology including reengineering (Lally, 1996, 1997), the Y2K problem (Lally, 1999), and privacy in the hiring processes (Lally, 2000), (Lally and Garbushian, 2001). Lally concluded (Lally, 2002) that the rapid pace of **change** in Information Technology is a further exacerbating factor increasing the likelihood of disasters.

1) **Changes in Hardware**—According to Moore's Law, hardware doubles in power every 18 months. As a result, hardware continues to evolve rapidly. Furthermore, entirely new kinds of hardware appear and must be

integrated into existing systems.

2) **Changes in Software**—New software releases fuel revenue streams in the software industry, resulting in mandatory "upgrades" every two years. The changes create an additional learning burden on users. Programmers are again under time pressure that can result in poor testing and de-bugging (Halfhill, 1998), (Westland, 2000), (Austin, 2001).

In addition to these first order effect, Lally also argues that changes in IT create second order effects by enabling changes in organizational processes. These processes can also become more complex, tightly coupled, and poorly controlled, further increasing the problem of serious accidents. As a result, IT managers and users are faced with complex, tightly coupled, poorly controlled systems that undergo radical changes on a regular basis, making these systems more prone to "Normal Accidents".

LESSONS FROM Y2K

By the late 1990s, a significant number of researchers and IT professionals were highly concerned about catastrophic IT failures. They believed that the design flaw of representing years with only two significant digits would propagate throughout the global infrastructure causing widespread failures. Perrow (1999, p. 392) argued that "Y2K has the potential for making a linear, loosely coupled system more complex and tightly coupled than anyone had reason to anticipate". Perrow emphasized that Y2K made him more keenly aware of the problem of "unknowability":

> One of the key themes of the theory, but not one formalized as much as it could have been, was the notion of incomprehensibility—What has happened? How could such a thing have happened? And What will happen next? This indicated that observers did not know what was going on and did not know what would happen next. The system was in an unknowable state (Perrow, 1999, p.293).

Not only were managers and users unaware, programmers were unlikely to know the real world impacts of the programs they wrote. One programmer who worked for the Federal Reserve System only became aware of what the Federal Reserve actually did during the Y2K crisis, "I read an article about how the Federal Reserve would crash everything if it went bad…I discovered we were kind of important" (Ullman, 1999, p. 4).

Lally (1999) also argued that the radical changes that IT programming, hardware and telecommunications had undergone in 40 years made the global infrastructure even more unknowable, and Y2K incidents even harder to isolate and their impacts harder to trace. Date representation errors were found in 40 year old COBOL code whose programmers had long since moved on to other careers and who, even if they could be located would be unlikely to still be able to read and de-bug the code.

By the late 1990s, computer systems were increasingly integrated and spanned organizational, and even global boundaries. Y2K failures in one organization, therefore, were likely to propagate to other organizations and to the economy as a whole. Y2K practitioners referred to this as the "ripple effect" (Kirsner, 1997).

> One patched together, wrapped up system exchanges data with another patched together wrapped up system—layer upon layer of software involved in a single transaction until the possibility of failure increases exponentially (Ullman, 1999, p. 7).

On a global level, the lack of compliance by many countries lead airlines to consider practicing a form of fault isolation, establishing "no-fly zones" over non-compliant countries (Anson, 1999). Concern was also been expressed about potential cross border damage between countries that were Y2K compliant and those that were not. As a result of many countries' non-compliance, Ed Yardeni, Chief Economist at Deutsche Morgan Grenfell predicted that there was a 60% chance that Y2K will lead to a global recession (Golter & Hawry, 1998).

Isenberg (1999) argued that only "social coherence," the ability for individuals to pool their knowledge and work together for the common good, could minimize the impact of Y2K disasters. Having redundancy, in terms of backup systems, and slack, in terms of time and personnel needed to contain incidents and keep damaged systems running, is another key to survivability suggested by the Theory of High Reliability Organizations. Lally (1997), however, argued that organizations which have eliminated human labor during reengineering efforts in favor of computers would have fewer resources to keep the critical systems running manually, should computers fail. Other Y2K researchers agreed:

> The "slack time" that could have been devoted to addressing the year 2000 issue before it became urgent has been deliberately cut out of the system in the search for leaner and meaner business processes. Furthermore, because they now lack the internal resources to handle the year 2000 problem, companies who have been through BPR downsizing will be forced to outsource the Year 2000 problem. Ironically, this contract could end up in the hands of the very consultants who advocated their BPR process in the first place (Gerner, 1998, p 144).

Y2K, therefore, was also characterized as a problem where poor control —the absence of redundancy, slack or the potential for social coherence— could exacerbate the damage.

Y2K came and went with a number of local failures but no major catastrophes. Failures happened within individual systems, but the "ripple effect" did not materialize as a serious threat. Y2K did succeed in raising the level of awareness on the part of managers regarding IT security. However, a number of managers who spent thousands of dollars preparing for Y2K only to have it be a minor problem, accused Y2K practitioner of "crying wolf," claiming catastrophic disasters were unlikely to happen.

9/11/01-WHAT HAS HAPPENED? HOW COULD SUCH A THING HAPPEN? WHAT WILL HAPPEN NEXT?

On September 11, 2001, a surprise terrorist attack left the world wondering,"What has happened? How could such a thing Happen? What will Happen Next?" The damage caused by the initial impact of the planes quickly spread destroying the World Trade Center and causing massive destruction and loss of life in lower Manhattan.

The Y2K problem was an innocent error, recognized ahead of time, and prevented from causing catastrophic failures. 9/11 was a deliberate, well organized, surprise attack that caused catastrophic damage before the military, the police, or the thousands of individuals who lost their lives could do anything to circumvent it. The prediction of the Y2K bug causing a worldwide recession did not come true. 9/11, however, will have serious global economic ramifications for years to come.

Responding to terrorism will be a more complex task,"…as John Koskinen, former head of the government's Y2K effort, remarked recently, "Unlike the Y2K Phenomenon, today's terrorist threat to IT is undefined, the response is difficult, and there is no known time frame," (Yourdon, 2002, p. 29).

A number of parallels, however, do emerge between the two events that can provide insight for preventing and/or mitigating the impacts of future terrorist attacks. Both emphasized the importance of planning for catastrophic failures. Some organizations indicated that their Y2K planning helped them mitigate the damage caused by 9/11 (Merian, 2001). Pressure is on from the business community to re-create the U.S. government effort in combating the Y2K problem as a means of combating terrorism (Thibodeau, 2001). This paper will argue that Y2K, therefore, provides a useful starting point in analyzing the 9/11 disaster.

RECOGNIZING AN INCIDENT AND UNDERSTANDING ITS POTENTIAL IMPACT

From a Normal Accident Theory perspective, a number of critical issues emerge regarding 9/11. First, what was the "incident" that needed to be recognized? Was it:

1) The first plane hitting the North Tower—at which point a serious problem became "knowable"?
2) The second plane hitting the South Tower—at which point a terrorist attack could be identified as occurring?

At this point there was no need to convince anyone that a serious problem existed. Here we can clearly distinguish between the "intellectual" threat of Y2K, which required large numbers of technical experts to convince the public of its seriousness and the "visceral" threat experienced by anyone viewing the 9/11 disaster. This paper will argue that although the plane crashes

propagated into even greater destruction, the first plane crash was already an "accident" leading to massive destruction and loss of life. Incidents preceding this event, if intercepted, could have prevented its occurrence. Examples of such incidents include:

1) Terrorists boarding the planes.
2) Discovering the existence of the 9/11 plot.
3) Hearing a young man say he wishes to learn how to steer an airliner, but not how to take off and land.

However, recognizing a potential terrorist and uncovering a terrorist plot is a challenging intelligence task, which is likely to result in many "false positives" with serious implications for individual privacy. Individuals detecting these incidents will be in a much more difficult position in terms of convincing others that a serious problem exists. One approach is to adopt suggestions from High Reliability Theory to create a decentralized High Reliability culture where individuals are encouraged to report information they consider threatening. "..we need to make it easier for front line observers to communicate their warnings quickly and effectively, without worrying about being criticized as alarmists," (Yourdon, 2002, p. 199). More sophisticated IT based methods are also available (Verton, 2002). Customer Relationship Management software, such as that used by Amazon books to detect patterns in buyer behavior, can also be used to detect patterns of suspicious behavior. If initial fears are confirmed, collaborative projects can help make early warnings more widely available. Isenberg's theory of social coherence where individuals and organizations co-operate in sharing information also supports this approach.

MODELING THE UNTHINKABLE: MITIGATING THE IMPACT OF TERRORIST ATTACKS

On 9/11, many lives were lost after the initial impact of the two planes because bad judgements based on incomplete information were made by individuals working in the towers, as well as by firemen and police. This was particularly true in the North Tower. Individuals remained in the upper portion of the North Tower hoping to be rescued despite the fact that they were unreachable and that one stairway was still passable. Firemen continued climbing up into the lower portion of the North Tower despite the fact that the South Tower had collapsed and they were in imminent danger. Incompatible communication devices prevented critical information from reaching the firefighters (Dwyer, 2002). However, wireless communication devices, emails and other Internet communication did increase social coherence during the disaster. Victims said goodbye to loved ones, and the passengers on Flight 93 were able to mitigate the impact of the disaster they had become a part of. Regular business communication took place over employee cell phones and personal Internet accounts (Disabatino, 2002), (Kontzer, 2002).

Simulation models of the building, such as those designed afterward (see Nova's "Why the Towers Fell"), could be used to minimize the problem of "unknowability" that resulted in so many deaths. Office workers in all large complex buildings could use these models to develop optimal evacuation plans during an emergency. Firemen could train by simulating rescue missions in all large complex buildings in their area. Finally, in terms of social coherence, good communication between structural engineers, who are best able to determine the condition of the building, and the workers and firemen inside could also save hundreds of lives.

CONCLUSION AND IMPLICATIONS FOR FURTHER RESEARCH

IT based communication tools for improved Incident Detection and increased Social Coherence appear to have significant potential for preventing malicious attacks. Simulation models that would reduce Unknowability and further increase Social Coherence would help mitigate the impacts of attacks that have already occurred. Further research is needed as to how best to design and implement these technologies in a manner that is, technically and economically feasible, as well as being sensitive to individual privacy rights.

Finally, this analysis needs to be extended to other kinds of malicious acts. 9/11 was remarkable because of the relatively low degree of technological sophistication needed to make it happen. A second kind of terrorist attack, E-terrorism, in which terrorists exploit their knowledge of the complex, tightly coupled, poorly controlled and continually changing global infrastructure to create disasters will be the focus of future research.

REFERENCES

Anson, R.S. (1999). 12.31.99. Vanity Fair, January, 80-84.

Austin, R. (2001). "The Effects of Time Pressure on Quality in Software Development" Information Systems Research, June, pp. 195-207.

Disabatino, J. (2001). "Internet Messaging Keeps Businesses, Employees, in Touch," Computerworld, September 17.

Dwyer, J. (2002) "Radio Problem Could Last Years", *New York Times*, September, 18.

Gerner, M. (1998). Five More Reasons Many Delayed From Year 2000: Best Practices for Y2K Millenium Computing. D. Lefkon, Editor. Upper Saddle River, New Jersey, Prentice Hall Publishers.

Golter, J. & Hawry, P. (1998). Circles of Risk. http://year2000.com/archive/circlesrisk.html.

Halfhill, T. (1998) Crash-Proof Computing. BYTE www.byte.com/art/9804/sec5/art1.html.

Isenberg, D. (1999). "SMART Letter $16." www.isen.com, February 1.

Kirsner, S. (1998). The Ripple Effect. http://www.cio.archive/y2k_ripple_content.html.

Kontzer, T. (2001). "With Phone Lines Bottlenecked, Internet Messaging Became Lifeline," *Information Week*, September, 12.

Lally. L. (1996). "Enumerating the Risks of Reengineered Processes," *Proceedings of 1996 ACM Computer Science Conference*, 18-23.

Lally, L. (1997). "Are Reengineered Organizations Disaster Prone?" *Proceedings of the National Decision Sciences Conference*, pp. 178-182.

Lally, L. (1999). "The Y2K Problem: Normal Accident Theory and High Reliability Organization Theory Perspectives," *Proceedings of the 1999 National Decision Sciences Conference*, pp. 234-237.

Lally, L. (2000). "Pre-Employment Screening for Reengineered Jobs: Issues in Information Access and Information Privacy," *Proceedings of the National Decision Science Conference*, 2000, pp. 371-373.

Lally, L. and Garbushian, B. (2001). "Hiring in the Post-Reengineering Environment:A Study Using Situationally Conditioned Belief," *Proceedings of the International Information Resources Management Conference*, pp. 234-237.

Lally, L. (2002). "Complexity, Coupling, Control and Change: An IT Based Extension to Normal Accident Theory," *Proceedings of the International Information Resources Management Conference*, upcoming.

LaPorte, T. R. & Consolini. P. (1991). "Working in Practice But Not in Theory: Theoretical Challenges of High Reliability Organizations" *Journal of Public Administration*, 1, 19-47.

Merian, L. (2001). "Y2K Plans Aided in Recovery, But More Planning Needed," Computerworld, September, 19.

Perrow, Charles. (1984) *Normal Accidents: Living with High Risk Technologies*, New York: Basic Books.

Perrow, Charles. (1999) *Normal Accidents: Living with High Risk Technologies 2nd Edition*, New York, Basic Books.

Sagan, Scott. (1993). The Limits of Safety. Princeton New Jersey: Princeton University Press.

Ullman, E. (1999). The Myth of Order Wired. http://wired.com/archive/7.04/y2k_pr.html.

Thibodeau, P. (2001). "Businesses Eye Y2K Effort as Model for Terrorism Fight," Computerworld, October 2.

Verton, D. (2002). IT Key to Antiterror Defenses at Nation's Sea Ports,"Computerworld, January 12.

Westland, J. C. (2000). "Modeling the Incidence of Postrelease Errors in Software" Information Systems Research, September, pp. 320-324.

Yourdon, E. (2002). *Byte Wars: The Impact of September 11 on Information Technology*, New Jersey: Pre ntice Hall.