Computer Attack:
The Role of Modelling in Developing an Integrated Security Policy

Stephen Sturges and Graham Winch
University of Plymouth
Plymouth Business School
Plymouth PL4 8AA
England

Stephen Sturges 100307.1542@compuserve.com
Graham Winch graham.winch@pbs.plym.ac.uk

Abstract

Many trends in computing - distributed processing, telecoms, reliance on computing for key business processes - combine to increase greatly the risks and vulnerability of firms to computer attack. The form of attack is also diversifying - mischief-making by "hackers" or virus writers, sabotage by disgruntled employees, fraudulent activity, or simple random hardware or software failure. The threats and potential costs to firms of breakdowns in security can be very large, involving the need to replace or re-engineer systems, to recover or reconstruct key information and data, and maybe even to try to re-establish goodwill with customers who may have been affected. The literature reflects that while the general issues here are appreciated, few firms understand fully the potential threats to their business, nor have explicit policies and procedures to guard against them.

This paper describes a system dynamics model that integrates the direct impacts of computer threats on IT systems with the potential damage to production and paperwork processes and to customer relations. The model is calibrated to capture the operations of a manufacturing firm. In particular the model uses the authoring facilities of iThink to present a user with easy interface, and the ability to quickly and dynamically change run parameters. The model thereby provides support to the first critical phase in developing a comprehensive computer security policy which is to identify the nature and extent of a firm's vulnerability. The 'gaming' use of the system then offers the IT manager a means of communicating and exploring the threats with their functional colleagues in the firm.

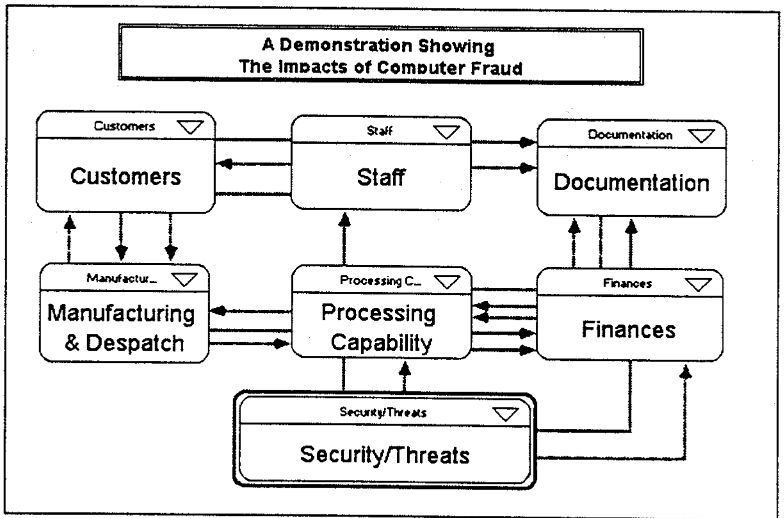
The Costs of Computer Crime

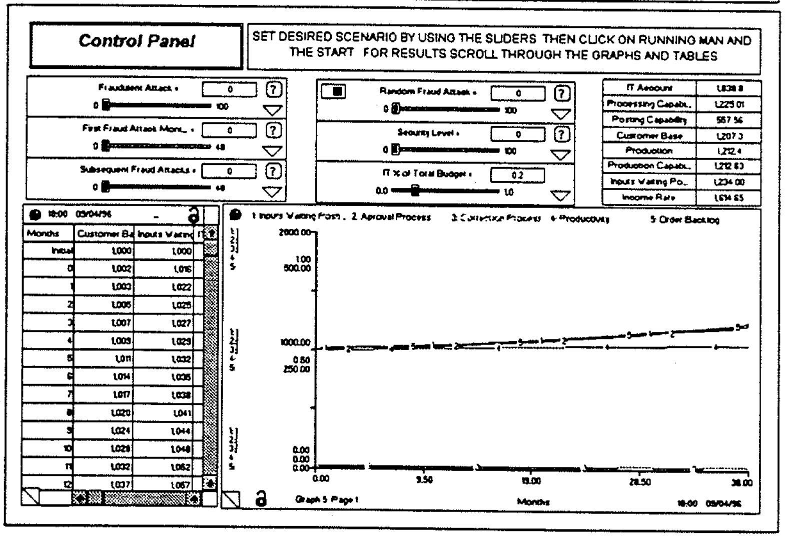
Computer crime is a booming industry with each reported case seemingly more spectacular than the last. Why is this? Is it that the systems employed are so easy to penetrate that teenagers with a home PC and modem are able to seriously disrupt business processes, to redirect funds, to alter account balances, amend college grades and generally cause havoc amongst the business community? Or, is it that the perpetrators are becoming more sophisticated, applying even more devious techniques, with potentially disastrous consequences? A recent report "Opportunity makes a thief" by the National Audit Commission (1995), who surveyed 1073 UK organisations, estimated that security lapses have cost UK organisations £1.2 b. since 1992. Some 36% of respondents reported incidents involving 'logic' security - software viruses or hacking - compared with 12% in 1992. The total value of reported incidents has risen by 183% from 1991 to 1994, with the average financial loss per incident at £28,170. The single most costly reported incident was a £1.2 m. fraud in an insurance company.

Supporting this another survey, carried out by Gallup (Lindsay 1991) and involving 101 UK companies, concluded by observing that three out of ten UK security managers do not have an explicit policy on security. Further, they are apparently oblivious to threats of fraud, vandalism, technical failure, and espionage. What perhaps is more damaging is that 60% of the polled managers do not have a risk assessment programme for their computer equipment. The survey highlighted that medium-sized manufacturing firms seem to be especially complacent, as 60% of those polled claim to have no protection against computer hackers, while 40% have no contingency plan for coping with a technical failure in the system. Ironically, the great majority of MIS managers believe their firms could become the targets of hackers.

Computers are now integral to all aspects of operations within organisations, which have embraced distributed processing and encouraged the spread of computing power to individual employees via personal computers, and have built large local and wide area networks, with global connections not knowing all the end and entry points into these systems. The impact of this has drastically changed the way they are managed and information resources controlled. Yet even with this dependence on computer systems, computer security is seen by many as at best a necessary evil. With today's firms focused on competitive advantage, becoming world class, with the drive for profits, security is seen as a cost contributor, a direct drain on the bottom line. But is it, and are the damaging impacts from fraudulent activity fully understood?

Modelling Computer Crime





Control Panel

SET DESIRED SCENARIO BY USING THE SLIDERS THEN CLICK ON RUNNING MAN AND THE START FOR RESULTS SCROLL THROUGH THE GRAPHS AND TABLES

Fraudulent Attack • 0 (0–100)
First Fraud Attack Mon... • 0 (0–48)
Subsequent Fraud Attacks • 0 (0–48)
Random Fraud Attack • 0 (0–100)
Security Level • 0 (0–100)
IT % of Total Budget • 0.2 (0.0–1.0)

IT Account	1,838.8
Processing Capab...	1,225.01
Porting Capability	557.56
Customer Base	1,207.3
Production	1,212.4
Production Capab...	1,212.83
Inputs Waiting Po...	1,234.00
Income Rate	1,634.65

18:00 09/04/96

Months	Customer Ba	Inputs Waiting
Initial	1,000	1,000
0	1,002	1,016
1	1,003	1,022
2	1,005	1,025
3	1,007	1,027
4	1,009	1,029
5	1,011	1,032
6	1,014	1,035
7	1,017	1,038
8	1,020	1,041
9	1,024	1,044
10	1,028	1,048
11	1,032	1,052
12	1,037	1,057

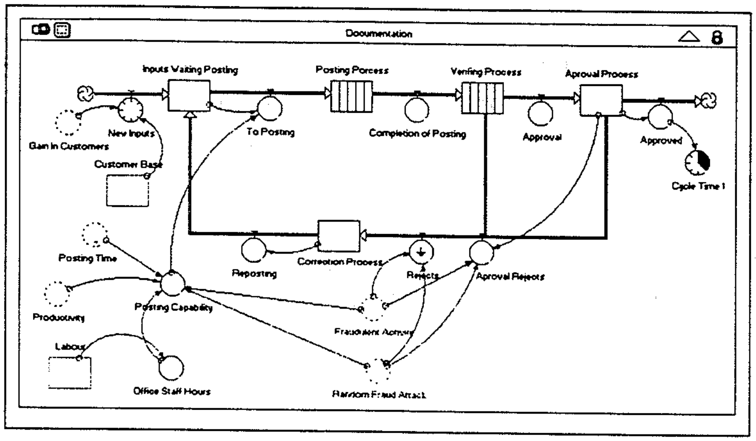
This paper describes the early work with a model developed to take a holistic view of a company's operations and its vulnerability to computer 'attack'. The model has been constructed with a 'gaming' interface for user interaction using iThink, utilising the authoring facilities of this software.

What seems clear from the press is that management and those in positions of responsibility often only consider computer security as an 'after the fact' issue. Traditional solutions have been based on a financial analysis basis, quantifying the trade off between costs of security vs. direct costs involved in system recovery. Although this approach has its merits, it is still at best an approach focused on a simple view of the cost of business functions. The underlying 'knock on' effects are all but ignored. It is because of this, that quantifying the cost trade off has proved to be notoriously difficult. What is important is that management fully understand the costs versus risk balance, and understand the degree of risk and potential for knock on impacts and costs remaining after security controls are implemented.

The model, which is typically representative of a small manufacturing company, reflects the relationships between the processes of a company, including the feedbacks resulting from a fraudulent attack. Sub-sector models have been created for these processes including documentation & administration, manufacturing & despatch, customers, staff, finances, information technology, and for the levels of security/threats. The interface is set up with 'sliders' allowing users to decide for themselves the level of attack, the frequency and duration, along with the level of security measures. The modelled system may be subject to interventions representing totally random attacks, of any volume and duration, but the model is calibrated and balanced to produce stable conditions when run without any interventions.

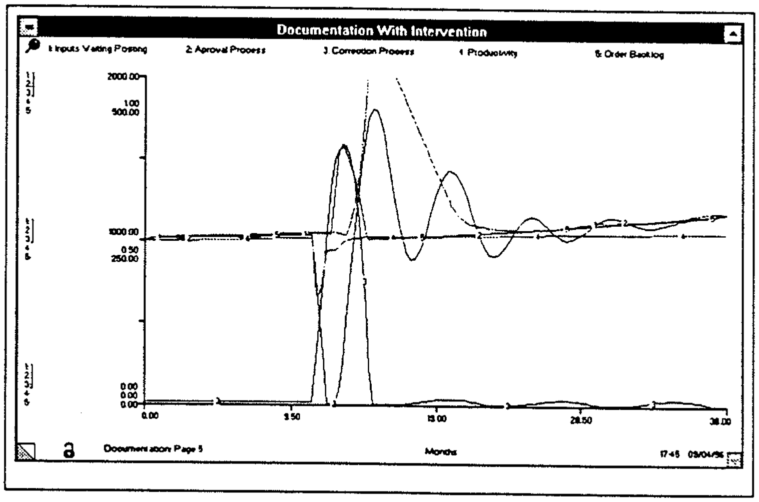
Example of Impacts on Documentation Subsection

Taking the documentation sub-section as an example, the full impacts of an intervention can be traced. The output rate of flow from inputs awaiting posting in the documentation sub-section is determined by the posting capability, derived from a level of labour, the average hours worked, a productivity factor and the average posting time per document.

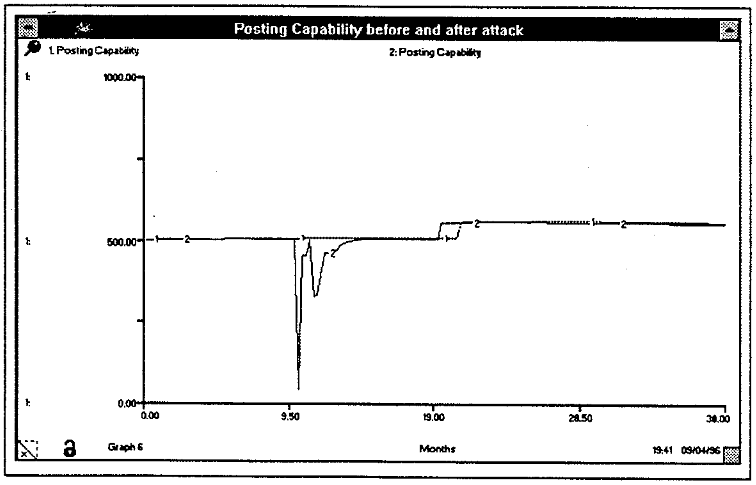


Should a fraudulent activity take place that is below the set security level then no impact occurs, however should this activity exceed the security level, the impacts in the documentation subsection are felt simultaneously at two points, (1) the flows into the rework section and (2) the available posting capability.

As posting time increases and productivity decreases due to the attack the effect is that posting capability is reduced (see the "Documentation With Interventions" graph). This allows the level of inputs waiting posting to build up creating a backlog in the system. The attack also impacts upon the number of rejects and the correction processes in the system, again increasing the amount of inputs waiting posting. This feeds back through changes in staff motivation to productivity, thereby affecting posting capability again, setting up a negative feedback loop. Once the attack is over, the sub section oscillates as it tries to regain its equilibrium position, depending upon the severity of the attack this oscillation can occur over a number of months. This dynamically demonstrates the knock on effects of the attack over time.



The posting capability of the system demonstrates vividly how the first and second order impacts of an attack must be taken into account (see the "Posting Capability before and after attack" graph). The system is initially able to recover quickly from the original computer attack which occurs at month 10, and within a short period - only a month - posting capability has returned to its base level. However a second dip in capability occurs as staff moral reacts adversely to the experience of the attack. Unlike the computer systems themselves which can be recovered quickly from an attack, staff moral returns to normal much slower. Consequently, capability is depressed following the attack for a total period of 4 to 5 months. A further secondary impact occurs later when the company is forced to bring forward a system upgrade in response to the lost productivity during the extended period of reduced posting capability following the attack.



Envisaged Role For The Computer Attack Simulator.

The model described here adopts a view of computer attack which considers the impacts not only to the equipment but to the processes of the whole organisation. By showing the knock on costs and effects, it can provide IT managers and security professionals with an analysis and communication tool that enables them to:

- Clarify the comprehensiveness of their own thinking in evaluating costs of attack.
- Give fellow executives a moving picture of the dynamic consequences of possible attacks.
- Reinforce the system dynamics message that "cause and effect are not close in time and space".

The model is a tool that can help decision makers take actions and emphasise points that they may already have identified in their own minds, but have failed to communicate adequately to others. It can be used as a vehicle for risk free experimentation, facilitating the rapid review of many scenarios, strategies or policies. It provides a trial-and-error way to investigate the likely effects of interventions and evaluate different options for the level of computer security the organisation needs to establish.

References

Lindsay, Nicolle, 1991, "No longer secure in the knowledge", (Gallup survey) Computer Weekly; Feb. 7, n1248, p26(2)

National Audit Commission, 1995, "Opportunity Makes a Thief", HMSO National Report