A SIMULATION MODEL OF INFOSEC DEFENSE AGAINST NATURAL DISASTERS

Norman Pendegraft, College of Business and Economics, University of Idaho, Moscow ID 83844, 208-885-7157, norman@uidaho.edu

ABSTRACT

A simulation infosec model is extended to include natural disasters. Results suggest that system value is sensitive to backup interval and restoration lag. In a costless world, it appears that value is sensitive to both the interval between backups and the delay in restoring after a disaster. It appears that value is more sensitive to restore lag than to backup interval. It also appears that in extreme cases of restore lag and backup cost that infrequent backups are preferable.

Keywords: infosec, disaster, simulation

OBJECTIVE

The reported work is part of a program of research examining the behavior of information systems under attack, the attackers, and the users of those systems. It seems that disasters differ from attacks in two fundamental ways: they are random, discrete events as opposed to purposeful ongoing continuous events. Both of these differences will add new facets to our model.

BACKGROUND

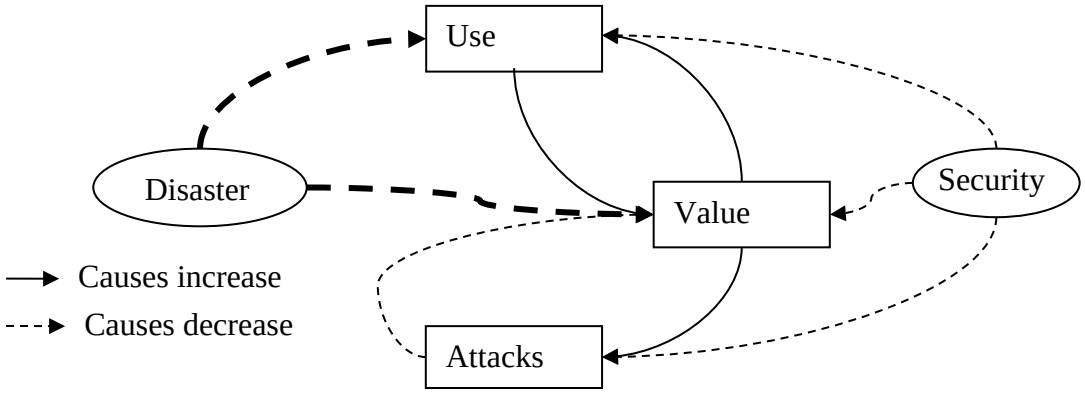
The problem of information system security (infosec) has been widely studied. Some of that work has looked at the human and dynamic aspects of the problem. As long ago as 1975, Saltzer and Schroeder [3] noted the importance of human behavior in the computer security problem. Recently, there has been considerable work using systems dynamics models to study infosec [1].

The model is based on that of the model of [2]. The paper extends the basic model by noting that disasters directly affect use: if a system is down, there can be no use. This is different from attacks which do not directly interact with users.

METHODOLOGY

The simulation was conducted using IThink which facilitates continuous event simulation using a stock and flow graphical modeling language. This extension seemingly requires a fundamental change in our current models (see Figure 1) in that they are continuous and deterministic, and modeling of natural disaster would seem best done as a discrete stochastic process.

FIGURE 1: BASIC MODEL



Model Outline

The model assumes that both users and attackers are motivated by data volume as a proxy for value. Periodically, the system is backed up. Disaster arrivals are modeled as a Bernoulli Process. This is implemented by assuming that disasters occur with some probability in each time period. If a disaster occurs then the system is not available for use nor for attack during the restoration period (assumed constant) at the end of which, the system is restored to the value in the current backup and operation (and attacks) begin again. The interval between backups and the time required to restore the system are the primary variables of interest in this paper. We used as a base case a situation in which value increased over time and in general security was efficacious at the margin for low levels of security.

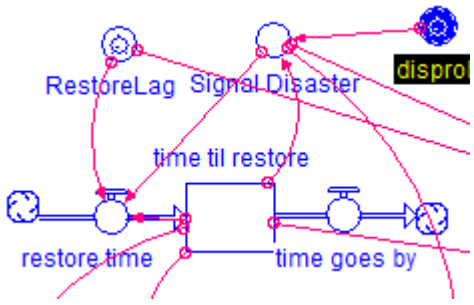
Disasters as Discrete Events

In order to treat disasters as discrete events, it was necessary to be able to remember when a restoration would be complete. Similarly, it was necessary to remember when backups were to occur, to ensure that backups did not occur during as restoration, and that if a disaster occurred during a backup, that the previous backup value was used. While these are not difficult problems in a procedural language they present challenges in IThink. To illustrate the method, we consider here the problem of remembering the time when a restoration is complete.
Figure 2 illustrates a small part of the model which calculates the time until restoration. That reservoir is constrained to be non-negative and drains at a rate of 1 per time period. It is "pulse loaded" when the disaster signal = 1 so that it goes to its full value in a single fractional time step.

Validation

To test that these issues were adequately modeled, a detailed analysis of intermediate values was considered. It is shown in Figure 3. In this example, DT (the interval used in the numerical integration) was .25, and backups are scheduled with interval 3 starting at time 0. Thus, there should be backups at 2(end), 5(end), 8(end), and 11(end). Note that the excerpt shows only times 2(end) and 11(end). There are backups at 2(end) but not at 11(end) because there was a disaster at time 11.75 which is still in restoration, so the model does not schedule a backup until after the restoration is complete at time 16(end).

FIGURE 2: LAG CALCULATION



RestoreTime = if (time_til_restore>0)
then 0
else if (Signal_Disaster=1)
then pulse(RestoreLag)
else 0

TimeGoesBy = 1

FIGURE 3: TEST OUTPUT

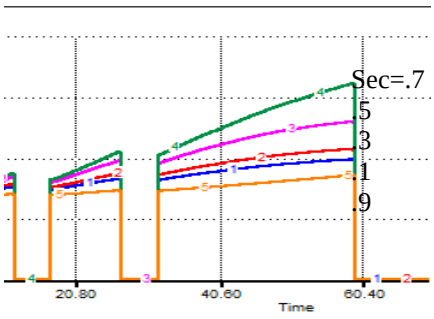
Time	Data	DataBU	TimeTilRestore	SignalBU	Signal Disaster	TimeOf NextBU	SignalRestore
Initial	100.00	100.00	0.00	0	0	3	0
1: .25	100.60	100.00	0.00	0	0	3	0
1: .50	101.21	100.00	0.00	0	0	3	0
1: .75	101.83	100.00	0.00	0	0	3	0
1: end	102.45	100.00	0.00	0	0	3	0
2: .25	103.09	100.00	0.00	0	0	3	0
2: .50	103.73	100.00	0.00	0	0	3	0
2: .75	104.37	100.00	0.00	0	0	3	0
2: end	105.03	100.00	0.00	1	0	3	0
3: .25	96.69	105.03	0.00	0	0	6	0
3: .50	97.25	105.03	0.00	0	0	6	0
3: .75	97.82	105.03	0.00	0	0	6	0
3: end	98.40	105.03	0.00	0	0	6	0
10: end	96.62	101.24	0.00	0	0	12	0
11: .25	97.18	101.24	0.00	0	0	12	0
11: .50	97.75	101.24	0.00	0	0	12	0
11: .75	98.33	101.24	0.00	0	1	12	0
11: end	0.58	101.24	4.75	0	0	17	0
12: .25	0.58	101.24	4.50	0	0	17	0
12: .50	0.58	101.24	4.25	0	0	17	0
16: .50	0.58	101.24	0.25	0	0	17	0
16: .75	0.58	101.24	0.00	0	0	17	1
16: end	101.82	101.24	0.00	1	0	17	0
17: .25	93.45	101.82	0.00	0	0	20	0
17: .50	93.97	101.82	0.00	0	0	20	0

RESULTS

Base Case

The base case is illustrated in Figure 4. Parameters were chosen so that the system would illustrate "nominal" behavior. That is: values increase over time and increased security increases value until it gets too high (.9). The graph illustrates sensitivity to security for backup interval (BI) and restore lag (RL) both equal to 5. That is an arbitrary choice, but the result held over a wide range of values for BI and RL. Now we turn to the sensitivity analysis.

FIGURE 4: BASE CASE



Sensitivity to Backup Interval and Restore Lag

First we varied BI over the range 3-7 in steps of 1 with RL held at 5 and security set to the best value from the base case (.7). Results are shown in Figure 5a with a close up in Figure 5b. It is clear that increasing BI has a negative impact on the time trajectory of value. Figures 6a and 6b show similar results for variation in RL with BI held at 5 and security at .7 The close ups (5b and 6b) use the same scale and it is clear that more variation occurs with changes in RL.

Sensitivity to Costly Backup

We conducted a third experiment by accounting for costly backups. Figure 7 illustrates the results for a backup cost of 2. We conducted one final "extreme case" experiment with RL = 10 and BU cost = 10. In that case, the best of the 5 tested backup intervals is the longest.

DISCUSSION

It is apparent from the results that the model is more sensitive to changes in RL than to changes in BI. Operationally this makes sense in that when a system is unavailable due to disaster, no business can take place, and thus growth opportunities are lost. When the costs of backups are considered the results are not so clear. It is clear that backup cost can have a profound effect on system value. In the illustrated case with cost = 2, it is clear that shorter backup intervals do not necessarily lead to better performance. In this case the an interval of 5 is better than the alternatives (3..7).

The results lead us to two conclusions. First including discrete events in the simulation allows us to model a broader range of issues at the cost of considerable programming difficulty. Second, it is clear that optimal backup strategies are highly dependent on the cost and performance of the available technology. This is best illustrated with the extreme case in which costs were so high and performance so poor that a very long backup interval was indicated. In the "more normal" cases, it appears that restore lag is the more important variable which makes sense since the system is unavailable during the restoration.

This work extends our program of research by considering the impact of natural disasters on defensive strategies. Doing so required adding a discrete event component to the model. thus introducing a fundamental change in the model.

The work reported here aims to advance a program for developing a more complete model to allow for policy experimentation. The paper admits of several obvious extensions. Most obvious seems to be combination of this model with the attacker choice model. Empirical validation of the assumptions of this line of research continues to be an important extension.

FIGURE 5 A, B: SENSITIVITY TO BACKUP INTERVAL =3..7 (CLOSE UP ON RIGHT)

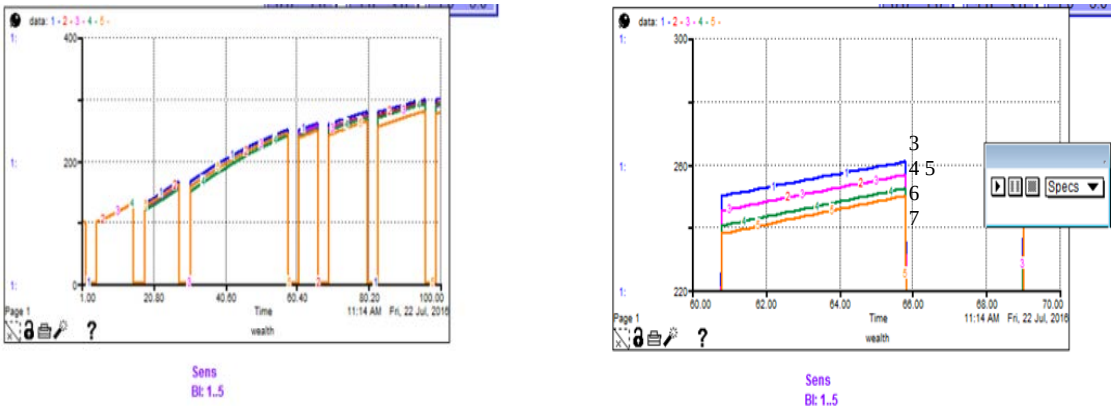


FIGURE 6:A,B SENSITIVITY TO RESTORE LAG =3..7 (CLOSE UP ON RIGHT)

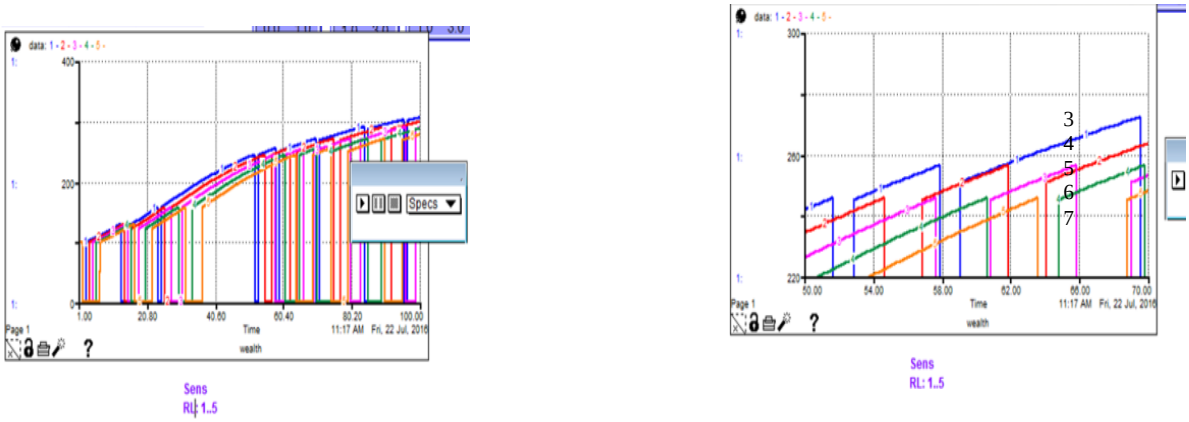
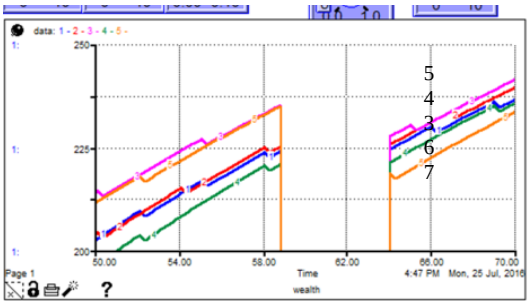


FIGURE 7:SENSITIVITY TO BACKUP INTERVAL (3..7) WITH BACKUP COST = 2



ACKNOWLEDGEMENT

The author acknowledges the support of the College of Business and Economics in completing this work.

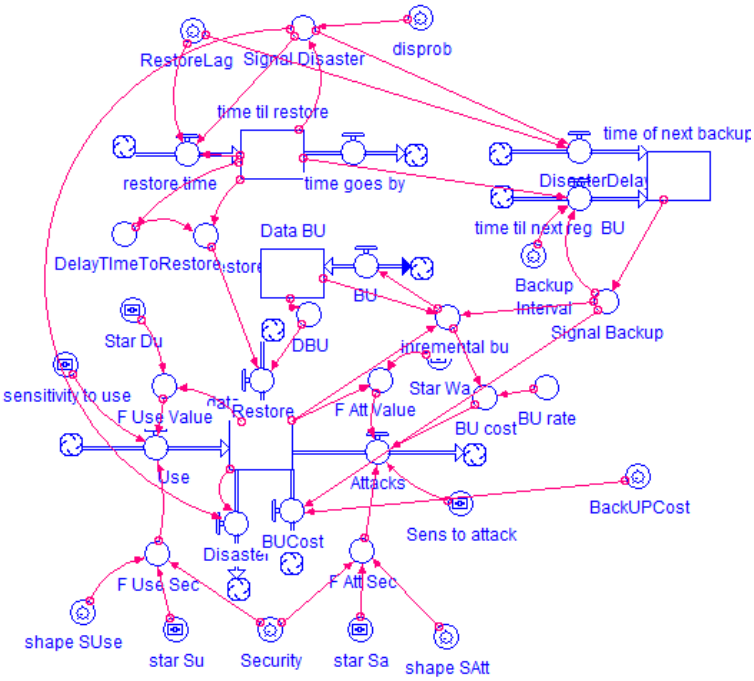
BIBLIOGRAPHY

[1] Dutta, A. & Roy, R., 2008. Dynamics of Organizational Information Security, System Dynamics Review 24#3, 349-375.

[2] Pendegraft, N. & Rounds, M. A. 2007. Simulation Model of Information Systems Security. *International journal of information security and privacy* 1 #4 (62-74).

[3] Saltzer, J.H. & Schroeder, M.D. 1975. The protection of information in computer systems. *Proceedings of the IEEE. 63#* 9 (1278-1308).

APPENDIX A: ITHINK MODEL AND CODE



IThink Model Layer

Think Equation Layer: Available on Request