

ALERT

THE NEWSLETTER FOR INFORMATION PROTECTION PROFESSIONALS

Number 199
October 1999

COMPUTER
SECURITY
INSTITUTE
600 HARRISON STREET
SAN FRANCISCO
CALIFORNIA 94107
TEL: (415) 905-2626

INSIDE INFORMATION

-  **Authentication** 2
What to know to prepare for SSO
-  **Industry Update** 7
ActiveX flaws revealed at USENIX symposium
-  **Job Listings** 7
Career opportunities
-  **Tools & Techniques** 7
Consider Tripwire 2.0
-  **In Case You Missed It** 8
Horror stories from the dark side of cyberspace
-  **Tools & Techniques** 10
"Provable" security?
-  **Telecom Security** 11
More help in dealing with rogue modems
-  **Calendar of Events** 11
Register now for the 26th annual conference and exhibition
-  **Bonus Item** 13
Second jobs must not impact objectivity or help competition
-  **Y2K Update** 14
Some Y2K threats you should consider

CSI special report: How to quantify financial losses from infosec breaches?

By Richard Power

There simply isn't a clear-cut way to tabulate the bill for information security breaches—yet. To help the process of developing such a methodology along, I included some insights from Dr. Eugene Schultz, CISSP, of Global Integrity/SAIC, Prof. Eugene Spafford, CISSP, of CERIAS/COAST at Purdue University and Dan Erwin, CISSP, of Dow Chemical in the 1998 CSI/FBI Computer Crime and Security Survey (*Computer Security Journal*, Vol. XIV, No. 3, Summer 1998). To give another push forward, I recently elicited some remarks from several more knowledgeable individuals.

You can't fully quantify the loss if you haven't valued the resource

Chris Grillo of Minnesota Power and Light (Duluth, MN), and also a CSI Advisory Council member, lays the foundation.

"Before we can quantify costs, we first must identify what the value of any given computer resource and the value of the information/data itself. Much of this value may have been identified during company disaster recovery projects or Y2K efforts.

"Unfortunately, many companies have not allocated resources to identify and quantify total cost of ownership at this level. Some may think that certain IT resources cannot be measured, but I believe that if it is observable, then it is countable, and if it is countable, then it is measurable.

"The question of quantifying financial losses due to security breaches involves any loss to a computer resource that either affects the revenues or expenses of a company, including even loss from lost operating efficiencies causing increased costs or from lost opportunities to place resources elsewhere (i.e., opportunity cost).

"You can even extend this to cover the intangibles such as customer service and corporate image (for example, if customers can't perform some form of communication or electronic commerce, etc. or a Web page is defaced). Such events affect revenues and/or expenses in some way.

"To estimate the costs, I would look at the total cost of ownership of my resources. We do this for accounting purposes, so why not build a total cost of ownership (TCO) chart of accounts. The costs could be categorized many ways."

Grillo suggests putting various costs into the following categories:

- Capital costs such as hardware, software, networks, servers, switches, etc.
- Administration costs such as management of the assets, security monitoring and follow-up, legal assistance, audit department, etc.
- Technical support costs when all the people call the help desk, documentation of the calls, end-user training, etc.
- End user operational costs such as the management of user data of resources breached, awareness training of users, etc.

continued on page 12

continued from page 1

"While there are many ways to look at the costs for quantification you can also use some more obvious methods to determine costs, such as just asking your customer or including the concept of risk in the equation.

"For example, you may ask the owner of the asset what you would need to pay them for the asset. This would at least give you a starting point for the 'negotiation' of what you should be insuring the item for. (For example, if you own a piece of art, you might not insure it for the total replacement value. Rather, you might pick a lower number to at least cover most of the costs if it were stolen—at least you wouldn't feel so bad about losing everything.) Also, you can evaluate the likelihood of that happening and then determine what you should pay to protect the asset.

For example, Grillo suggests, consider a trade secret.

"How much would you accept to sell this trade secret to someone right now?" \$1 billion.

"What is the likelihood that the trade secret would be used to develop a marketable product?" 75%.

"You would end-up having a market value (adjusted) to about \$750 million."

Grillo also offers an example using a more tangible asset.

"How much would it cost to replace the server and data stored on the server? \$150,000.

"What are the odds that there will be a security breach that will completely compromise this secret? 10%.

"What should I pay to secure or insure it? 10% x \$150,000= \$15,000. Okay, let's estimate and insure it for \$15,000 and use this cost as part of the loss.

"If opportunities are lost or delays due to a computer resource loss occur causing financial loss, I would consider using an impact of delay analysis. In this analysis I would 'bracket' estimates of delay into ranges with their associated costs based on the above methods. For example, what would the cost be if our Electronic Commerce site were down for one day? One week? One month?"

Don't over simplify the problem

William Hugh Murray, CISSP, of Deloitte and Touche (Wilton, CT) issues a warning.

"Be careful not to over-simplify."

He deals with the problem of quantifying financial losses due to information security breaches in the following terms:

- Kind of target
- Cost of attack
- Value of success

Cost to the victim

"There are two kinds of targets: targets of opportunity and targets of choice. A target of opportunity is one of a large population of similar targets, with a similar cost of attack and value of success. One need only raise one's defenses high enough (i.e. raise the cost of attack) to get out of the population. A target of choice is one where the attacker believes the value of success exceeds the cost of attack.

"Cost of attack is measured in term of work, access,

indifference to detection, special knowledge, and time to corrective action. There are enough of these elements in the world to break any system but not enough to break every system. These costs are fungible; an abundance of any one can reduce the requirement for all of the others.

"The value of success can be measured in terms of computer time, data, information, knowledge, application value; access to other networks; identity, anonymity, trust or confidence; and other(e.g., vengeance, power)

"The cost to the victim can be measured in terms of loss of confidentiality (often not easily

repairable), loss of integrity, loss of reliability and trust, loss of use, liability to third parties, loss of resources for restoration

"Keep in mind that cost of losses is a function of the frequency as well as the consequences of the event and that consequence of events is inversely proportional to their frequency."

Let's look at some scenarios.

System penetration from the outside

A hacker crawls all over your networks for days or weeks, deploying sniffers, using network resources for storage, computational power, or access to other organizations, etc. How do you begin to quantify the financial losses involved?

Marcus Ranum of Network Flight Recorder (www.nfr.com) takes a stab at it.

"First, I would itemize into categories of sub-loss:

- Downtime / lost opportunity/business
- Staff time (their salaries)
- Consultants (if used)
- Legal time (hourly)

"It might be a reasonable approach to break it up in terms of phases of the clean-up:

- Detection
- Response
- Repair

continued on page 4

continued from page 12

□ Prosecution

"You would say, 'We spent \$1,120 on consultants detecting what the hacker did. Following that, we spent \$2,200 on consultants helping our staff respond and backtrack the hacker. We spent \$3,000 on re-installing the O/S on our firewall. We spent \$2,929 on consultants assisting our legal counsel in preparing to prosecute the hacker.' For each type of expense you could break it into those phases, 'We had no legal expenses during detection, no legal expenses during response, we notified and briefed legal counsel of the situation during repair at a cost of \$39,393 for their hourly services, and we had costs of \$81,238 preparing to prosecute the hacker.'

"The expenses here are going to break down pretty evenly between figuring out what they did and fixing what they did. One might want to argue that some of the expenses during the repair phase would belong to the victim, since they might be valuable for the infrastructure in the absence of the attack (i.e., 'I should have done it anyway'). So you would also end up saying 'We bought a new tape silo for backups at a cost of \$331,311.'

Murray adds that in incidents of system penetration from the outside, the time to corrective action is inversely proportional to the size of the breach.

Ernest Hernandez, CISSP, of Sprint Paranet (like Grillo, a member of the CSI advisory council) offers some insights.

"Factor in the cost of computing resources used. In some internal recharge systems, the use of CPU cycles is recharged at approximately \$100 per CPU minute. Days or weeks of using CPU cycles could accumulate very quickly.

"Likewise, costs for disk storage is also recharged to recover costs. Again, if a hacker is inside the internal network, there is a possibility of significant amount of disk space being consumed, translating to costs not only for disk space that is now not available to company personnel, but perhaps even purchases of additional disk space due to the hacker's consumption.

"Investigation of the incident can consume countless hours of several people's time. Typically, an investigation involves several people from an organization, starting with Information Security personnel, System Administrators, Management, Legal, and external security or police forces (including the FBI).

"The cleanup effort can be just as costly as the investigation. Penetration analysis has to be done to identify weaknesses. Then the weaknesses have to be fixed. The penetration analysis can vary in the amount of time it takes to do based on the number of firewalls, routers, and hosts on the internal network. The internal network has to be evaluated for host-based security weaknesses to determine

how the hacker gained access to the host machine or machines. Fixing all of the weaknesses in the firewalls, routers, and internal hosts can be a significant dollar amount.

"Litigation of such a penetration and intrusion can run into the hundreds of thousands of dollars. There may also be employees, customers, or stockholders who file law suits against a firm who was hacked into, especially if personal or confidential information was compromised or could have been compromised."

Unauthorized access from the inside

An insider, maybe an employee, maybe a contractor on-site, accesses sensitive information (for example, trade secrets, sales data, marketing plans, R&D) over the network, downloads it and then sells it to your competitor. How to do quantify the losses incurred?

Ranum comments.

"Same paradigm. Discover that the situation occurred (detection), figure out what happened (response), figure out the business impact of the access and put things in place to prevent it again (repair), and perhaps prosecute, which is lots of work.

"The bulk of the expense in an unauthorized access by an

insider is going to be determined by what they did. Fixing insider attacks is not as big a deal, because they don't need to do as much damage to get the information they need. They're also less likely to put Trojan horses and all that kind of stuff all over the network."

Murray notes that while we normally think of insiders in terms of loss of confidentiality via unauthorized access, data is usually compromised by those who are authorized to access it. He also observes that insiders are usually after money, i.e., 'application value,' and that "the time to corrective action is often very high."

As Hernandez remarks, the damages can be devastating.

"If the information stolen and sold to a competitor was, for example, the formula for a new product (for example, a drug) the costs can be disastrous. The costs incurred would include all the Research and Development costs that went into development of the product, all the R&D personnel costs involved (salaries & benefits), all the projected sales that will be potentially lost, all litigation costs if legal action is pursued, possible lawsuits from stockholders."

Sabotage of data and/or network operations

A critical server or network is trashed whether from the inside or the outside. What kind of costs would be involved?

Murray comments that most publicized incidents of sabotage, although large-scale, have been against targets of

"The cleanup effort can be just as costly as the investigation. Penetration analysis has to be done to identify weaknesses. The weaknesses have to be fixed...Fixing all of the weaknesses in the firewalls, routers, and internal hosts can be a significant dollar amount."

Ernest Hernandez

opportunity, and their cost has been a function of the number of targets. Therefore, these incidents, while costly, do not represent a threat to the health of the business.

However, he adds that "sabotage against targets of choice is a threat to the health of the business."

Ranum comments.

"Downtime is the main factor in sabotage. Determining who did it, how/when, are the secondary factors. If there are no backups then I guess you'd need to somehow try to establish the value of the system and re-creating the data on it. (Though if the victim tried to claim the system was critical but they had not been keeping backups, I'd be amazed if they didn't get laughed at in court).

Hernandez comments.

"Sabotage of data on a critical server could be disastrous without adequate backup. The business could possibly be lost without it. If the sabotage was perpetrated from the inside, there will more than likely also be costs associated with an investigation, litigation, and the costs associated with restoring or recreating the data. If the origin of the attack was external, there could be huge costs associated with public image notwithstanding the costs to recover, restore, or recreating the data."

Malicious code

How do you begin to quantify a serious hit from "Melissa"? How would you calculate damage?

Ranum answers.

"Again, it's how do you detect what systems it's been on, how do you repair it, and how do you prevent it afterwards? Obviously, the cost of prevention shouldn't be part of the damages. For a viral outbreak, the costs to consider are the cost of restoring the data and downtime. Of course, if there is lost data that can be much more costly."

But Ranum finds little sympathy for anyone suffers significant loss of data.

"It's always the victim's fault if they lose data! If the data is important, you should have enough copies of it that you would only lose a very small increment of work."

Hernandez comments.

"Costs incurred due to virus outbreaks are not exorbitant, but are a waste of resources. With the network capabilities the problem is a double-edged sword. On one hand, it is easier to manage the cleanup, but on the other hand, it is easier for the viruses to spread. In a large employee organization (40,000), costs ran into the \$100,000 range for the Melissa virus. The costs were only calculated on the

'cleanup' effort."

Murray adds that the cost of a virus incident will vary significantly depending upon the particular virus involved.

"This a function of how quickly and successfully the program spreads, i.e., scope, and the damage caused by each copy. Melissa spread very quickly and successfully, but did not do much damage per copy. Chernobyl did spread successfully, but not quickly. Most businesses were prepared for Chernobyl and did not suffer. However, the damage per copy for the unprepared was very high"

"Downtime is the main factor in sabotage...If there are no backups, you'd need to somehow try to establish the value of the system and re-creating the data on it. (Though if the victim tried to claim the system was critical but they had not been keeping backups, I'd be amazed if they didn't get laughed at in court)."

Marcus Ranum

and you have to rebuild it. Simple enough. Ten staffers work one day to bring the site back up (1 X 10 = 10 staff days). Of the 10 staff, you had one manager, one systems administrator, one Web administrator, one network engineer, two content specialists, and four other staff members. Figure their billing rates or cost rates and do the math. When you get your final number, you have the direct personnel costs of bringing that single site back up from that particular breach. The complexity here is figuring out who exactly was involved for how long—for example, were the staff all local or were there headquarters staff as well?

"There is a lot that is not covered by this calculation.

"In all of your scenarios—outsider, insider, sabotage, malicious code—there will be some level of investigation. The cost of investigation is based on how much energy you expend to investigate and whether the people and resources that are applied to the investigation are yours or someone else's. Again, this becomes a somewhat straightforward equation. How many people? For how long? At what cost?

"But this cost is only clear if you are talking about resources that are only used for this single event. If the resources you use to investigate are part of a permanent security team, then you have to factor in the personnel costs of having an information security team. Now you're factoring

Don't underestimate "soft costs"

Keith Allan Rhodes of the U.S. General Accounting Office stresses the importance of not underestimating "soft costs."

"You have asked *the* profound question, because this analysis of cost is what forms the basis for deciding whether the security effort is worth the effort. One can generate a baseline personnel cost estimate for any of the cases you've mentioned. On the surface, this seems fairly easy, but it is also a very incomplete estimate of the costs. For example, let's say you have a Web site, and it gets hacked,

continued on page 6

continued from page 5

in the administrative overhead associated with a permanent security cadre.

"There is also the hidden cost of outside law enforcement that cannot be ignored. For example, the Melissa case included local, state and federal law enforcement resources.

"The U.S. Justice Department's 'Cost of Crime' Web page shows statistics. For example, in 1997, \$0.5 billion was lost in robberies, \$7 billion was lost in arson, etc. These quantifiable costs are clearly understood. They correspond to our discussion of the costs to bring a site back up.

"But it is the 'softer' costs that really break the bank. For example, personal crime loss estimates of \$105 billion annually in medical costs, lost earnings and public program costs related to victim assistance. When pain, suffering, and the reduced quality of life are assessed, the costs increase to an estimated \$450 billion annually.

(See <http://www.ojp.usdoj.gov/ovc/ncvrw/1999/cost.htm>)

"This may seem trivial. But they're not. Violent crime results in lost wages equivalent to one percent of American earnings, three percent of U.S. medical spending and 14 percent of injury-related medical spending.

"You should also add in insurers' losses of \$45 billion annually due to crime (roughly \$265 per American adult).

"The U.S. government pays \$8 billion annually for restorative and emergency services to victims, plus perhaps one-fourth of the \$11 billion in health insurance payments.

"The statistics on computer-related crime have got to include these kinds of "soft" costs, which means that corporations or organizations that are hit need to understand their value as well.

"For example, let's say you and I are corporate officers in P&R, Inc. One of our 'trusted' business planners is on the road and at a payphone, speaking with her/his spouse about a change in schedule. S/he turns around to see the void that was once her/his laptop. So we begin a reconstruction period. Let's say s/he has written up in a five-year corporate business plan. The plan and its backup data are all on her/his laptop. How do you quantify the cost of recreating that lost business plan? How do you quantify the loss if it falls into the hands of your competitors?

"Furthermore, if in any of the scenarios you've mentioned the organization is trying to prosecute the perpetrator, the litigation will probably be time-consuming and very

costly—especially if the litigation is part of a corporate abuse scenario.

"Let's say a person uses the corporate intranet for sexual harassment or child pornography. Now you're talking about litigation against your corporation or you personally as the head of the corporation. Remember, if you are a corporate officer, and your corporation does something illegal, you can be held both criminally and civilly liable personally."

If we can quantify losses, we can calculate ROI

Rhodes points out another benefit of being able to put a price tag on financial losses due to such security breaches.

"What we are trying to figure out is the return on investment (ROI) on a security team or any security apparatus that one chooses. Is any of this worth it if no one goes to

jail? Is any of this worth it if my site still gets hacked? Is this just the price of doing business—a risk to be factored into any and all business decisions? This is one aspect of business decisions that most organizations do not face.

"Security is the price of doing business. How secure you are is a function of the business risk you are willing to take. For example, we all know that wireless service is rife with fraud. (If you can't highjack a cell phone, you better get out of the highjacking business.) But the wireless services are booming—at a rate that far outstrips the risk. Partly because the wireless service providers

pass their losses directly on to the great unwashed who do not make the connection between higher access fees and phone fraud. Just because the phone company was 'nice' enough to remove the unauthorized use from your bill does not mean you're not going to have to pay."

"It is the 'softer' costs that really break the bank. Personal crime loss is estimated at \$105 billion annually in medical costs, lost earnings and public program costs related to victim assistance. When pain, suffering, and the reduced quality of life are assessed, the costs increase to an estimated \$450 billion annually.

Keith Rhodes

Plan now to join a Working Peer Group in Y2K

CSI Working Peer Groups were established at the request of member organizations and have proven to be extremely valuable to members. Groups meet three times a year to discuss in confidentiality specific issues facing them on the job. Each meeting is moderated by CSI Director of Education, John O'Leary. Membership in a Working Peer Group is US\$6,000 annually (and includes CSI membership). We are also planning to establish a Working Peer Group to address the needs of those working in government jobs.

For details about CSI Working Peer Groups, contact Pam Salaway at 516-878-2205 for details.