Hacker's Insurance: When All Else Fails

Heather Eikenberry
January 9, 2000

WHAT IF…

What would your company do if someone hacked into your database and copied a list of all your company's client's personal information? What would your company do if a virus were introduced that wiped out your data records? How costly would it be if your company had an attack which caused a "denial of service" resulting in no business for several days?

Is your company prepared to handle the financial loss due to the situations just described? Standard insurance does not cover the above events yet millions can be lost if any of them happen. If something does go wrong, there is a relatively new service being offered by insurer's that can help ease the pain. This paper describes this new product called "hacker's insurance".

COMPUTER CRIME ON THE RISE

In March 2000, Computer Security Institute (CSI) released the results of their Fifth Annual "Computer Crime and Security Survey. With the assistance of the FBI, CSI reported responses from 643 companies and government agencies, suggesting an increase of computer crime.

Highlights of the CSI survey include the following:

- 9 out of 10 organizations reported computer security breaches.
- Viruses, stolen laptop computers, and employees abusing their Internet privileges are still the most common forms of unauthorized computer intrusions.
- 70% of the respondents report serious computer security problems such as theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks, and sabotage of data or networks.
- 42% of the companies quantified their financial losses to a total loss of $265 million dollars, more than double the average for the previous three years.
- The most serious financial losses occurred through theft of proprietary information ($66 million) and financial fraud ($55 million).

In July 2000, Reality Research reported their findings from a study of financial costs of viruses and computer hackers. Reality Research assisted Information Week Research to survey 4,900 information technology professionals in 30 nations. They estimate that 1.6 trillion dollars will be spent globally on information security issues this year. Their study indicates a lot more damage than most believe if the loss of productivity due to downtime and the loss of sale opportunities is taken into account.

With such damage occurring at an increasing rate, organizations must implement good information security practices to protect their assets. However, no system is foolproof and attacks will get through. A company will always hope that damage is kept at a minimum. However, if there is significant damage, “hacker’s insurance” can provide coverage.

VIRTUAL VALUE

Today, information constitutes a significant portion of a company's wealth, which is stored predominately in an electronic form and shared over networks. This information includes accounting information, intellectual property (such as trade secrets), patent information, design data, source code, customer information, competitive information, and supplier information.

Traditional insurance policies are inadequate to handle most aspects of property and crime damage due to computer based causes.

The following is a list of the common problems found with traditional insurance:

- Exclusions and definitions in traditional policies limit cyber-risk coverage.
- Many companies do not have errors and omission coverage, but if they do, such coverage contains exclusions for breaches in security.
- Coverage does not completely address intellectual property infringement, content, and advertising offenses over the Internet.
- Losses are based on physical assets and physical perils, not information assets and electronic risk.
- Intellectual property is not recognized to have a quantitative value.
- There are exclusions and limitations with respect to employee dishonesty and computer fraud.
- Policy coverage is not global.
- Non-recognition of monetary loss to a company if their business is reduced or shut down because of computer crime.

A PARTNERSHIP

A new trend in the last couple of years is for security firms to team up with insurance brokers to offer policies that protect against loss of revenue and information arising from security breaches. For example, MIS Corporate Defence announced a collaboration with insurers J S Wurzler to provide companies with loss of revenue and virus attack insurance. In these cases, a risk assessment is done by the security company and forwarded to the insurers. A policy is written and a premium is determined based on the integrity of the company’s information security infrastructure.

Another trend is for security companies to seek insurance for themselves to provide guarantees on their services and products. International Computer Security Association (ICS), an Internet security company, announced in 1998 that it would pay corporations up to $250,000 if ICS’ system gets cracked.

WHO PROVIDES HACKER'S INSURANCE

Providing insurance for cyber loss is a new industry. Most insurance carriers do not have the necessary expertise or tools to adequately assess the needed coverage. As a result, there are currently only a few companies offering hacker's insurance. However, with the financial losses continuing to escalate, the demand for this protection will also increase.

Lloyd's of London has created an insurance product that incorporates elements of crime coverage and property coverage, addressing specific exposures faced in our computer age.

The product, Computer Information & Data Security Insurance (CIDSI), combines theft and malicious damage protection coupled with business interruption coverage. CIDSI further provides expert computer security surveying and loss control services to mitigate exposures and losses. The product is a comprehensive program that can help address significant exposures.

Other vendors of computer crime insurance include:

- Internet Security Systems (www.iss.net)
- Counterpane (www.counterpane.com)
- J.S. Wurzler Website Insurance & Security (www.jswum.com)
- Axent Technologies (www.axent.com)
- Insuretrust.com LLC (www.insuretrust.com)
- Ace Ltd. (www.acelimited.com)

COST

Liability is still difficult to calculate. An example of one method for calculations is to average a Web site's revenue over several months and divide for an estimate of the hourly cost of downtime. However, this calculation doesn't consider account traffic and potential customers lost as the result of service interruption.

Insurers typically determine policy costs according to the company's size, the volume of business a company conducts on the Web, and the effectiveness of company's security policy. Some insurers offer a discount if you have an affiliation with certified information security experts.

Policies can carry premiums starting at $7,000 all the way to $3 million dollars. Lloyd's of London has recently announced a policy to cover up to $100 million dollars but the price of the premium has to be negotiated specifically with Lloyd's.

CONCLUSION

There is no information security system that is infallible. Everyone will face an attack. What distinguishes the victims is how much damage is done. If good security principals were implemented, the loss will hopefully be limited. However, with technology growing at an exponential rate, creative computer attacks will also rise. The potential for extreme damage even in the most secure facility needs to be considered.

Information security professionals need to consider what to do if failure occurs. Along with repairing the damage, they should consider reimbursement for those damages. Hacker's insurance is an added step of protection that security professionals need to investigate and present to management as part of the corporate security plan.

REFERENCES

Computer Security Institute. " Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey." CSI Press Release. 22 March 2000. URL: http://www.gocsi.com/prelea_000321.htm (3 Jan. 2001)

Edwards, Cliff. "Protection Money: Firms Offer Insurance Against Hack Attacks."10 July, 2000. URL: http://www.abcnews.go.com/sections/tech/DailyNews/hackinsurance000710.html (5 Jan. 2001).

Meinel, Carolyn. "The ABCs of IDSs (Intrusion Detection Systems)." 10 Oct. 2000. URL: http://www.messageq.com/security/meinel_2.html (4 Jan. 2001).

Net Secure and Marsh, Inc. "The Problems With Traditional Insurance." 7 Dec. 1998. URL: http://www.netsecuresite.com/ns/nssite.nsf/Frameset?OpenForm&Query=Main:Home (5 Jan. 2001).

Reality Research. "Study Finds Computer Viruses and Hacking Take $1.6 trillion Toll on Worldwide Economy." 7 July, 2000. URL: http://128.11.101.21/pressrel_7_7_00.asp (24 Jan. 2001).

Symantec. "Playing it Safe with Online Insurance." 13 June, 2000. URL: http://www.symantec.com/region/uk/enterprisesecurity/es000613a_uk.html (5 Jan. 2000).

Tri-City Brokerage, Inc. "Computer Security Fundamentals and Risk Management." URL: http://www.tricityins.com/cc_security.htm (4 Jan. 2001).