



Impairment of Computer Services Malicious Programming

The Risks Are Real

Information and network technology has become the lifeblood of almost every business operation today. Through the Internet, even the smallest businesses can engage in commerce in parts of the world previously beyond their reach. Unfortunately, technology brings with it complex new threats to the financial vitality of businesses large and small. Chubb, a leader in developing global insurance solutions for today's businesses, has developed a new approach to address these emerging threats. *Customarq Classic's* Impairment of Computer Services/Malicious Programming insurance addresses the emerging first-party exposures presented by the Internet and companies' increasing reliance on electronic information in their business activities.

Customarq Classic offers cutting-edge insurance protection for the risks stemming from computer virus, distributed denial of service and other acts of malicious programming. Separate automatic limits are provided for acts of malicious programming committed by those authorized to access information technology systems (insiders) and those who are not (outsiders). This insurance responds to the electronic data recovery costs, business income loss and extra expense incurred because of malicious programming, without requiring evidence of physical loss or damage to covered property.

A company can incur substantial expenses when its network or electronic data have been compromised. Costs to copy, re-create, replace or retrieve electronic data and restore system functionality can mount. The time it takes to restore business operations to pre-loss levels is often underestimated. In addition, there is likelihood that extra expenses will be incurred to continue operations.

Take a look at these loss scenarios and then consider whether you have adequate insurance protection.

Malicious Programming by "Insiders"

Systems Administrator Cripples Organization

A system administrator for a manufacturing firm was given unlimited access to all internal computer systems. Following a poor performance review, the administrator ran an online application with incorrect data in order to cause multiple erroneous product shipments. When the incident was discovered, it was not known if other applications or systems had also been impacted.

A Cover-up

A retail employee conspired with a third party to share customer credit card numbers issued by his employer. This crime involved the random selection and distribution of customer data by printing off customer information from the billing system. Becoming increasingly paranoid, the employee entered the system and deleted the records in an effort to cover up his activity. In addition, the employee erased several other credit card databases in an effort to divert attention from the actual crime.



Delayed Attack by Terminated Employee

Fearing termination due to a recent merger, an employee programmed the company's computer to delete a variety of important data files but delayed program execution until after a scheduled reduction in force (RIF). Four months later, the application started randomly deleting files. Management placed a six-month freeze on any further data migration until all systems were evaluated.

System Integration Leads to Disaster

A law firm hired a computer consulting firm to integrate its local computers with the firm's corporate network. Employees of the consulting firm were authorized to access the corporate network. The integration suffered numerous delays, and an investigation ensued to determine the cause of the delays. The investigation discovered that the law firm's data had been tampered with. Several weeks later, confidential information related to several high-profile cases was made available to the public via the Internet.

Supply Chain Is Interrupted

A manufacturer of automotive transmissions utilizes a computer ordering system that supports its just-in-time inventory-delivery strategy. Delivery logistics were subcontracted to a freight company, and several freight company employees were authorized to access the manufacturer's network. A freight company employee maliciously programmed the system, compromising the ability of the manufacturer and its component suppliers to deliver its products. Without prior notice, gearbox housings were not delivered to the manufacturer as scheduled. The manufacturer determined that it will be three months before it receives a supply of gearbox housings.

Backup Data Is Contaminated

Following the passage of Sarbanes-Oxley, a manufacturer of office supplies reviewed and updated internal procedures to ensure transparency and timely reporting of financial data. The procedure called for daily data backups to be stored both on premises and remotely and archived for a period not less than one year.

An employee committed an act of malicious programming, compromising the integrity of both the general ledger and the backup files. The act was discovered when the manufacturer used backup files to restore a financial operation.

Malicious Programming by "Outsiders"

Employees Install Wireless LAN Access Points

A newly hired creative director observed that the lack of a wireless network was limiting productivity of the "creative" employees of a video game publisher. One weekend, the creative director used personal funds to install a wireless LAN access point to boost morale and productivity. By Monday morning, the creative staff found their new productivity tool to be most helpful.

Unfortunately, the company's system administrator reacted too late. A competitor, using a handheld antenna, intercepted communications and gained access to the computer systems. In an act of industrial sabotage, all the files related to an upcoming game were altered.

A Shared Network for Universities

Several universities share a common computer network for the purposes of exchanging scientific research among the faculty and students of each institution. A student commits an act of malicious programming on his university's computer system which then spreads to all other computers on the shared network. The net result is an impairment of all computers connected to the network.

Get the protection you need now. Talk to your agent or broker today about Chubb's *Customarq Classic* Impairment of Computer Services/Malicious Programming insurance protection.



Chubb Group of Insurance Companies
Whitehouse Station, New Jersey 08889
www.chubb.com

Chubb refers to the insurers of the Chubb Group of Insurance Companies: Federal Insurance Company, Vigilant Insurance Company, Great Northern Insurance Company, Pacific Indemnity Company, Northwestern Pacific Indemnity Company, Texas Pacific Indemnity Company, Executive Risk Indemnity, Inc., Executive Risk Specialty Insurance Company, Quadrant Indemnity Company, Chubb Custom Insurance Company, Chubb Indemnity Insurance Company, Chubb Insurance Company of New Jersey, Chubb National Insurance Company, Chubb Lloyds Insurance Company of Texas. Not all insurers do business in all jurisdictions.

This literature is descriptive only. Actual coverage is subject to the language of the policies as issued.

Form 61-01-0005 (Rev. 3/05)