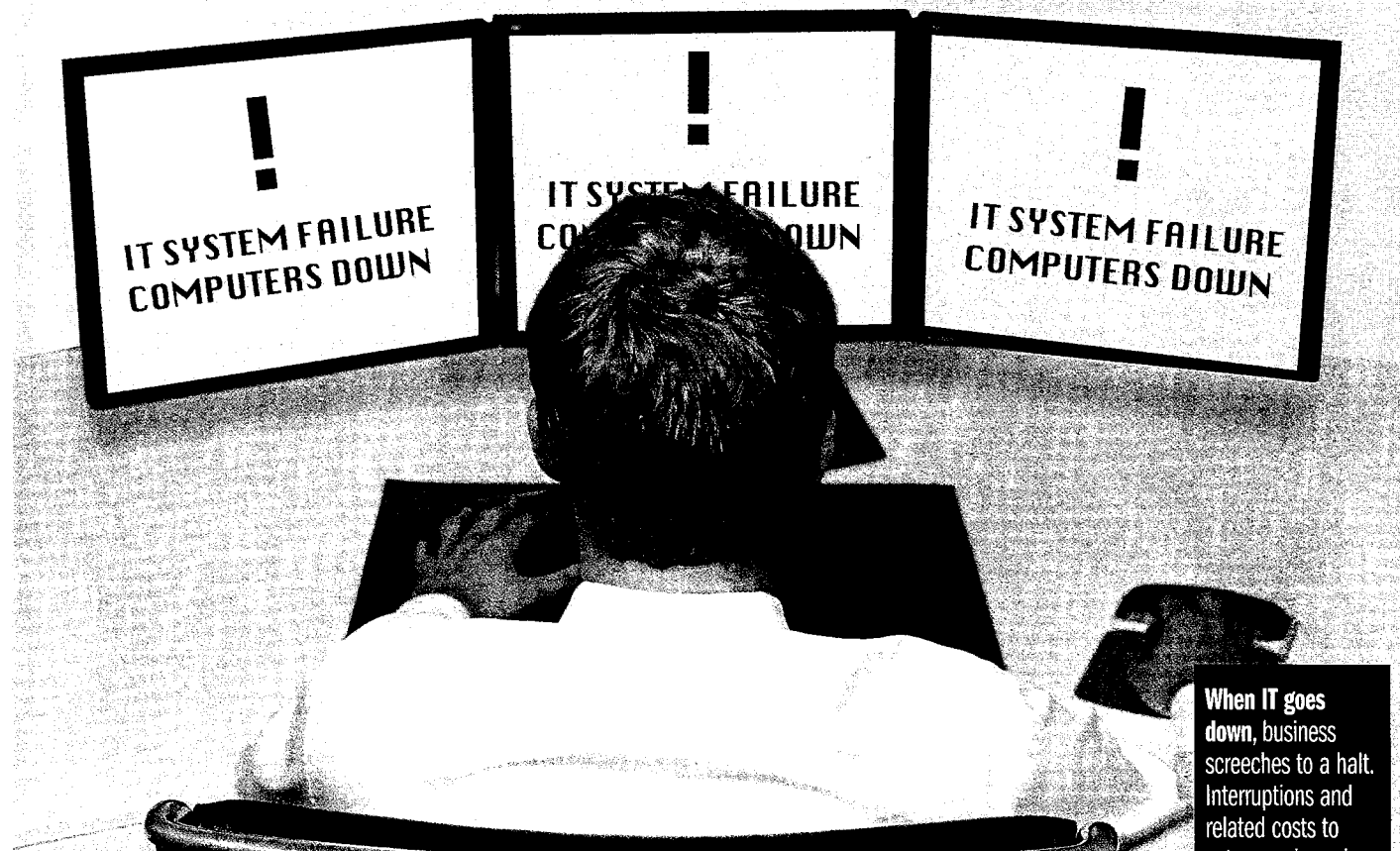


■ THREATS INCREASE

Cyber Coverage: The New 'Must-Have' In The Property & Casualty Portfolio?

Businesses from the local doctor's office to Fortune 1000 rely on IT



When IT goes down, business screeches to a halt. Interruptions and related costs to get up and running aren't covered by standard p&c insurance policies

BY RICK GRIMES AND KAREN KUTGER

IF CURRENT TRENDS CONTINUE, cyber insurance coverage just may take its place alongside workers' compensation, general liability, fire and auto insurance in the core commercial property and casualty package, meaning a business would be foolish to open its doors without it.

The reason is simple. Virtually every modern enterprise—from the local doctor's office or supermarket to Fortune 100 corporations—lives and breathes on its information technology applications, databases and computer systems.

When IT goes down, business

screeches to a halt.

Indeed, for businesses such as online retailers, brokerages and some financial firms, the IT and data assets are the entire business—every bit as critical as the factory and warehouse are to the hard-goods manufacturer, or the vehicle fleet to a trucking company.

Imagine Amazon.com or a regional bank trying to do business without their databases and computer systems.

As more and more companies—and their insurers—are realizing, this reliance on IT creates a hornet's nest of risks that can result in crippling losses that conventional, turn-of-the-century P&C insurance coverages won't respond to. These new issues call for a new category of coverage.

THE NEW RISKS

On the one hand is the issue of first-party losses. These might include business inter-

ruption, which could be caused by a flood or fire in a data center, or malicious hacking by a disgruntled employee or even a cyber-crook half a world away.

Traditional p&c insurance might help replace some of the lost hardware or compensate for physical damage to the data center. Yet there is no coverage for the onerous costs of restoring data, re-installing software, or for lost revenue, since standard p&c packages typically exclude such losses completely.

It means a company could be out of business for days or weeks, while also being responsible for costs of restoring the IT functionality.

Perhaps even more ominous are the all-new liability exposures inherent in IT operations. A raft of relatively new regulations and legislation makes companies responsible for safeguarding personal and confidential data they collect as part of everyday e-commerce operations.

Companies are liable for customer credit card numbers, financial transactions, medical history, credit information and other sensitive data.

Regulations ranging from HIPAA (the Health Insurance Portability and Accountability Act) for health care information to Sarbanes-Oxley and an array of state laws provide stiff penalties for companies that mishandle data, permit leaks or unauthorized access, or otherwise fail to safeguard sensitive information, which conventional insurance will not cover.

There is also the risk of being sued by third parties for somehow allowing—or failing to prevent—unauthorized access to sensitive information.

An example of this would be an overseas hacker who infiltrates an online shopping Web site and steals hundreds of thousands of customer credit card numbers. The Web site now faces claims from angry customers for unauthorized charges made on their credit cards, as well as claims from banks that issued the cards for costs incurred in

canceling and reissuing them.

Traditional insurance simply will not apply here.

The new reality is that criminals, terrorists and insiders are beginning to recognize that the real Achilles heel of today's companies and organizations is the IT side of their businesses. Secrets, sensitive data and inside information have now become their prime targets.

LOSS SCENARIOS

WHAT ARE THE LIABILITY RISKS?

The third-party side of Network Security and Privacy Liability insurance policies usually addresses liability arising from network and information security, privacy liability and electronic media. The following loss scenarios illustrate the need for coverage in these areas:

NETWORK SECURITY BREACHES

▶ **A company inadvertently transmits a malicious virus** that damages computer systems of hundreds of customers, causing widespread loss of data and other damages.

The company is sued by the receiving firms for failing to detect and prevent this transmission.

PRIVACY VIOLATIONS

▶ **A flaw in the IT system of a large medical group** allows hackers to access the medical records of several prominent political and entertainment personalities and sell them to journalists and bloggers.

The affected parties sue the medical group for negligence and failing to safeguard confidential information.

MEDIA AND CONTENT PRACTICES

▶ **A company uses a price comparison feature** on its Web site.

A competitor sues, alleging that the company used deceptive and misleading prices for competing products, as well as inaccurate specifications in an effort to make its own products more attractive.

▶ **Customers sue a well-known specialty store**, claiming that the store's online shopping Web site is deceptive and confusing about shipping costs, and that the site's "shopping cart" feature frequently charges customers for rush shipping without their approval.

The suit requires the company to issue refunds of overcharges to customers.

THE INSURANCE OPTIONS

Since common p&c insurance coverage doesn't respond to most IT and privacy-related losses—and are in fact specifically excluded in most forms—major carriers and specialty insurers are now offering an array of cyber products designed to address the critical gaps.

These cyber products—usually called "Network Security and Privacy Liability" policies—tend to vary significantly from carrier to carrier, as the markets try to discern what provisions and terms prove most attractive to enterprise customers at different levels of risk. The situation is similar to where employment practices liability insurance was just a few years ago.

The Network Security and Privacy Liability policies are generally designed to address first-party risks and third-party liability—sometimes in the same policies,

sometimes separately.

First-party coverage typically includes:

- Business Interruption
 - Data Restoration
 - Cyber Extortion Payments
 - Crisis Management Expenses
 - Media/Intellectual Property
 - Regulatory Actions
 - Expenses to Notify Affected Parties
 - Expenses to provide credit monitoring
 - Forensic costs to determine how the breach occurred
 - Transmission of a virus/worm
 - Loss or damage to an organization's own network, or e-theft
- The third-party side usually addresses liability arising from network and information security, privacy liability and electronic media. (See related infographic, "Loss Scenarios.")
- Depending on the nature of a company's operations and IT structure, insureds can negotiate a number of coverage enhancements that address situations not covered in the core policy.
- Coverage could be extended to cover the actions of "rogue" employees, authorized staff acting in an unauthorized manner, or to independent contractors or outsourcers.
 - Coverage could also be extended to cover off-line or non-electronic data that contains sensitive or private data, and is somehow breached or released.

■ First-party expenses might also be negotiated for the costs of restoring a network after a breach, investigations of the breach, costs of workarounds, or short-term services to restore functionality.

■ Defense costs, civil penalties and fines due to regulatory actions, as well as amounts that must be deposited into redress or settlement funds.

UNDERWRITING CYBER

Thanks in part to an overall soft market, capacity for cyber coverage is abundant at this point; however, one sector that is facing increased underwriting scrutiny is the financial institutions segment.

In addition to evaluating basics like rev-

▶ continued on page 22

CYBER COVERAGE

continued from page 13

enue, employee count and the nature of the business, underwriters take into account the technical safeguards a company has in place, its overall privacy and security policies—and occasionally, the recommendations of an outside consultant or security auditor.

Underwriters may also require certain upgrades to procedures or technology as a condition of the insurance.

In designing insurance coverage for an enterprise, agents and insureds should start with a thorough assessment of potential risks and vulnerabilities of the existing systems, perhaps with the help of a security specialist, and then secure the appropriate insurance coverage.

Network Security and Privacy Liability insurance is just another important component of a risk management strategy in today's business environment. The more businesses rely on information technology as an engine for operations and communication, the more crucial it becomes to protect IT assets with the right coverage. ■

INSURER SCRUTINY

WHAT DO CYBER INSURANCE UNDERWRITERS LOOK AT?

Typically, providers of Network Security and Privacy Liability insurance consider:

- ▶ **Business revenue:**
- ▶ **Employee count:**
- ▶ **Nature of the business:**
- ▶ **Technical safeguards:** a company has in place for cyber events
- ▶ **Overall privacy and security policies:**

Occasionally, they consider recommendations from consultants or security auditors.

In some situations, underwriters may require certain upgrades to procedures or technology as a condition of the insurance.

▶ **Rick Grimes** is an executive vice president for Professional Risk Solutions, a wholesale insurance broker that places directors and officers, errors and omissions and cyber security and liability coverages headquartered in Somerset, N.J. Mr. Grimes may be reached at rick@prsbrokers.com.

▶ **Karen Kutger**, vice president and branch manager for the Philadelphia branch of Professional Risk Solutions, may be reached at Karen@prsbrokers.com.