

Delivering essential employee benefit and commercial insurance information to customers and our members

DATA BREACHES

Coverage Gap Concerns as Cyber Threat Grows

Small and mid-sized firms are increasingly bearing the burden of cyber threats, as criminals are betting these companies don't have the resources in place to mount a strong defense.

A severe attack on a small company can incapacitate its ability to do business, and the expenses of getting operations back on track — coupled with loss of goodwill — can easily force a firm into bankruptcy.

That's why it's important to not only have safeguards in place to avoid being compromised in the first place, but to also secure cyber insurance.

CYBER INSURANCE

Your commercial property and liability policies will not cover cyber-related losses. Fortunately there is cyber insurance.

Coverage varies among insurers. We can help you weigh your choices so that you get the coverage you need to protect your firm.

Generally, cyber insurance is designed to protect your company in five areas:

1. NETWORK SECURITY

This covers your firm in the event of network security failure; such as a data breach, malware infection, cyber extortion demand, ransomware or business e-mail compromise.

Network security coverage will reimburse for expenses that you incur as a result of the cyber incident, including legal expenses, negotiations and payment of ransomware demands, data restoration, breach notification costs and more.

2. PRIVACY LIABILITY

Privacy liability coverage protects your company from liabilities that stem from a cyber incident or privacy law violation.

This usually arises when a third party's personally identifiable information that your company stores has been compromised.

3. NETWORK BUSINESS INTERRUPTION

If your network goes down due to a cyber event, the insurance will pay for your lost profits, expenses and extra costs incurred during the time your business was interrupted.

For example, if your network goes down due to a cyber event, the insurance will pay for your lost profits, expenses and extra costs incurred during the time your business was interrupted.

See 'Refine' on page 3

TOP REASONS FOR LOSSES

- Malicious breaches resulting in data losses: 52%
- Unintentional data disclosure: 16%
- Physical loss or theft of data: 13%
- Network or website disruptions: 5%
- Phishing, spoofing, and social engineering: 5%

Source: Advisen and Nationwide Insurance Co.



VMA MEANS VALUE-ADDED

For a quote or review on workers' comp insurance, business insurance, professional liability (E&O), employment practices liability (EPL), cyber liability, health insurance, or other products, please contact David Katz.

CONTACT US

David Katz
CA License #0712961
415-489-7614 ext. 703
david@vma.bz



INTELLECTUAL PROPERTY

Companies Bleed Data as Workers Move It Offsite

The more employees are working from home, the greater the risk that their employers' sensitive data is also being stored on their poorly secured devices and laptops.

A new study by Symantec Corp. found many workers are sharing, moving and exposing sensitive company data as part of carrying out the requirements of their jobs, and they may not realize they could be compromising the information or that what they are doing is wrong.

More worrisome, the study found that half of all employees surveyed who left or lost their jobs in the prior 12 months had kept confidential company data. When that happens, the departing worker, your company and the new employer are all put at risk.



HOW DATA LEAKS FROM YOUR FIRM

- Workers move it to their personal devices, both mobile and at home
- Employees transfer the data or save it on cloud services or personal hard drives
- Employees take data with them to their new jobs

Worse still, the majority of employees put these files at further risk because they don't take steps to delete the data after transferring it.

"In most cases, the employee is not a malicious insider," writes Symantec, "but merely negligent or careless about securing IP. But, the consequences remain. The IP theft occurs when an employee takes any confidential information from a former employer."

WHAT YOU CAN DO

Symantec suggests attacking the problem from multiple angles:

- **Educate employees** — Take steps to ensure that IP migration and theft awareness is a regular part of security-awareness training. Create and enforce policies dictating how they can and cannot use company data in the workplace and when working remotely.

WHY DATA LEAKS FROM YOUR BUSINESS

- 47% of employees say their organization doesn't take action when employees take sensitive information offsite
- 68% say their employer does not take steps to ensure staff do not use confidential competitive information from third parties
- 56% do not believe it is a crime to use a competitor's trade secrets

Help employees understand that sensitive information should remain on corporate-owned devices and databases. Also, new employees must be told that they are not to bring data from a former employer to your company.

- **Enforce non-disclosure agreements** — If you have not done so already, you need to craft new employment agreements to ensure they include specific language on company data.

They should include language that the employee is responsible for safeguarding sensitive and confidential information (and define what that is).

- **Conduct exit interviews** — For employees that are leaving your employ, conduct focused conversations during exit interviews and make sure they review the original IP agreement. Include and describe, in checklist form, descriptions of data that may and may not transfer with a departing employee.

- **Track your data** — You need to know where your data is going and how you can find out by using monitoring technology. One option is to install data-loss-prevention software that notifies managers and employees in real time when sensitive information is inappropriately sent, copied, or otherwise improperly exposed.

Also introduce a data-protection policy that monitors inappropriate access or use of company data and notifies the employee and you of violations.

This increases security awareness and deters theft. When you know how data is leaving your company, you can then take steps to prevent it from seeping out.

EMPLOYEE THEFT INSURANCE CAN HELP

Contact David Katz today for a quote:

 415-489-7614 ext. 703  david@vma.bz

Visual Media Alliance | Insurance Services | Get a Quote and Get Your Questions Answered | insurance.vma.bz | 800-659-3363



INSURE YOUR BUSINESS

Full Service Commercial Brokerage serving printing, graphic arts, and the broader communication industries



INSURE YOUR STAFF

Medical, dental, vision, life, disability, supplemental benefits, and more



WHY VMA INSURANCE

VMA Insurance Services offers preferential group rates and other cost-saving benefits

WORKERS' COMPENSATION

Reporting Claims Late Can Increase Your Premiums

One of the keys to keeping the costs of a workers' compensation claim from spiraling out of control is prompt claims reporting.

Claims are routinely filed late, either by the injured worker who fails to report it, or the employer dawdling and not reporting the claim to its insurer. Either way, this can result in delays in treatment, which can exacerbate the injury, leading to additional medical care and higher overall claims costs.

In fact, a 2015 study by the National Council on Compensation Insurance (NCCI) found that claims reported four weeks after an incident ended up costing nearly 45% more than claims reported in the first week after injury. Waiting to file claims three to four weeks after the injury ended up costing 29% more.

Those added claims costs can come back to haunt you in the form of higher premiums during your next policy renewal.

The NCCI found that claims that were reported more than two weeks after an incident were characterized by more attorney involvement, and more use of lump-sum settlement payments.

THE FALLOUT

Many employers delay reporting workers' comp claims, particularly if they seem minor at first. A worker may be injured but does not require medical treatment, so the employer thinks "It's a small injury and they'll heal up in the next few days. No big deal."

Not reporting even minor injuries can cost you. Here's why:

- **Delaying reporting makes an investigator's job harder.** Delayed reporting leaves the potential for inaccuracies, misstatements and even destroyed evidence.
- **The chances of litigation increase with delayed reporting.** Claims reported on the same day they occur involve an attorney only 13% of the time, compared to 32% for claims reported four weeks or more after injury.
- **Delayed treatment can cause more problems.** Delays in medical treatment can end up making injuries worse, resulting in more treatment. It also is likely to extend the life of the claim as the injuries may take longer to heal and they could be unable to work.

- **Longer closure rates.** Claims that stay open longer have a lower closure rate at 18 months after injury, according to the NCCI.
- **It hurts workers.** By delaying reporting, employers shortchange their workers, which can affect employee morale.

THE TAKEAWAY

Start the reporting process as soon as you become aware of a workplace injury.

The longer you wait, the costlier the claim likely will be and the more chance your worker will hire an attorney.

Establish a claims reporting protocol for all employees to follow. They should be required to immediately report any work-related injury, no matter how small. That includes first aid claims.

Put in place protocols to ensure that any injury report gets to your office's point person so the next step can be determined.

Let employees know that it's in their best interest to report any work injuries and that you won't retaliate for filing a claim.

If all employees are responsible for reporting injuries to their supervisor, every supervisor needs to know what their own responsibilities are, as well.



Continued from page 1

Insurance Will Cover Claims for Failing to Perform Your Services

4. MEDIA LIABILITY

This coverage pays for costs related to intellectual property infringement, other than patent infringement, resulting from the advertising of your services.

It often applies to both your online advertising, including social media posts, as well as printed advertising.

This could be the result of using copyright holders assets without their permission.

5. ERRORS AND OMISSIONS

An attack can result in your firm not being able to fulfill its contractual obligations and deliver services to your customers.

The errors and omissions portion of a cyber policy will cover claims arising from failure to perform your services.

This can include technology services, like software and consulting, or more traditional professional services like graphic design, lawyers, doctors, architects, and engineers.



VISUAL MEDIA
ALLIANCE | INSURANCE SERVICES

665 Third Street, Suite 500
San Francisco, CA 94107

For more information on VMA's workers' comp, health, or voluntary benefits programs, please contact VMA Insurance Services.

INSURANCE.VMA.BZ | 800-659-3363 | INFO@VMA.BZ

RiskReport

JUNE – AUGUST 2022



VISUAL MEDIA
ALLIANCE | INSURANCE SERVICES

ABOUT US

Visual Media Alliance Insurance Services (VMAIS) provides a full suite of insurance programs including property and liability, commercial auto, management liability, professional liability (errors & omissions), and group health programs to over 550 firms since 1985.

VICE PRESIDENT

David Katz

COMMERCIAL INSURANCE CSRs

Mary Fernandez and Renee Prescott

HEALTH INSURANCE CSRs

Sue Benavente, Diedra Lovan, Deirdre Ross, and Shannon Wolford

INSURANCE.VMA.BZ

800-659-3363

INFO@VMA.BZ

The Small Business Insurance Checklist

Running a business is full of risks, and you'll want to make sure that you are properly covered and you offer a strong suite of employee benefits to your staff. Review this handy checklist to make sure your business is protected.



PROPERTY/CASUALTY INSURANCE

- Property and general liability
- Workers' compensation
- Commercial auto and umbrella
- Cyber liability
- Management liability
- Professional liability

EMPLOYEE BENEFITS

- Group medical
- Dental and vision
- Group life
- Short-term and long-term disability
- Supplementary employee benefits

Ensure your business is covered, contact:

David Katz

david@vma.bz • 415-489-7614 ext. 703