Ridgemark Insurance Services

OCTOBER 2023 | VOLUME 4 | ISSUE 9

NEWSALERT

Coverage Issues

Pay Attention to Exclusions in Cyber Policies

WHILE CYBER threats grow and the cyber insurance market evolves, insurers are regularly adjusting their policy terms and conditions in response to new threats and exposure.

Carriers have amassed nearly a decade's worth of data and are getting more stringent about underwriting and demanding that policyholders do their share by implementing best practices aimed at preventing cyber attacks and reducing their impacts.

They have also been adding more exclusions to policies, according to a new report by Delinea. The report is a sobering reminder that business owners need to carefully read their policies. The access-management software firm notes that:

- All respondents to its survey had at least one exclusion in their policy that would void coverage.
- All respondents had at least one attack-related expense that wouldn't be paid for by cyber insurance.
- Businesses should create a "rainy day" fund to pay for situations that won't be covered by their cyber insurance. The report notes that the average cost of a data breach in 2023 exceeds $4 million.

Exclusions to watch out for

Obviously, the crucial question is: What are the most common exclusions in cyber insurance policies?

Missing security protocols – Insurers require businesses to have certain security protocols in place, such as keeping software and systems updated as well as security patches and regularly training staff on cyber security.

Internal threats – Acts by employees, like hacking, cyber extortion, data theft and other illegal or unauthorized activities, are typically excluded.

Human error – If an incident is caused or worsened by a mistake, like misconfiguring or failing to address known vulnerabilities, a cyber claim may be denied as the insurer could argue that the event could have been prevented or mitigated.

Act of war or terrorism – While many cyber insurance policies have these exclusions, courts have increasingly pushed back on them as a pretext for denying a claim after a cyber attack. Often it's difficult for the carrier to prove it was an act of terrorism or war.

Out of compliance – Misrepresentations or nondisclosure of material information on a cyber insurance application may cause the insurer to deny coverage.

Failure to report an event in a timely fashion – If you fail to inform your cyber insurer of an event within the timeframe specified in the policy, or if you provide incomplete information, the company may deny the claim.

See 'Protocols' on page 2

Ridgemark Insurance Services

Ridgemark Insurance Services

2130 Professional Drive, Ste 225,
Roseville, CA 95661

Phone: 916-306-1550
www.ridgemarkinsurance.com

If you would like to receive this newsletter electronically, e-mail us at:
info@ridgemarkinsurance.com

Transportation Hiring Alert

Always Check New Drivers' Clearinghouse Records

FLEET OPERATORS face an increased risk of potential liability if they are not diligent about checking their drivers' moving violation records with the state Department of Motor Vehicles, in addition to the Federal Motor Carrier Safety Administration's Drug and Alcohol Clearinghouse.

To ensure the safety of our roadways, as of 2020, it became mandatory that all registered motor carriers sign up their drivers in the Clearinghouse and run their driver rosters through the system to clear them for duty. But many companies are skipping this step and only checking their drivers' records with the DMV, which may not reflect any suspensions issued by the Clearinghouse.

Clearinghouse rules require that drivers be tested for drugs prior to being hired and randomly throughout the year. This helps employers weed out drivers who may be at higher risk of both moving violations and accidents.

The Clearinghouse

The Clearinghouse was created to keep commercial drivers who have violated federal drug and alcohol rules from lying about those results and getting a job with another motor carrier.

This electronic database tracks commercial drivers' license holders who have tested positive for prohibited drug or alcohol use, as well as refusals to take required drug tests, and other drug and alcohol violations.

The Clearinghouse tracks a driver's drug and alcohol tests and bars them from operating commercial vehicles after they fail a test. If they want to return to driving, they must successfully pass a return-to-duty process that includes substance abuse treatment and a test to evaluate their readiness.

The Clearinghouse restriction can be lifted should the driver sign up for a Clearinghouse program that will test them 14 times in two years, with the first 12 tests having to occur in the first year. This cost all comes out of the driver's pocket.

This system is an important check on drivers and helps employers reduce their exposure.

State Departments of Motor Vehicles are required to check the Clearinghouse before issuing a new or renewing a commercial driver's license.

The takeaway

While it is the law that employers follow Clearinghouse procedures, because it's a new system, many companies are failing to follow the rules, and are possibly allowing suspended drivers to operate their vehicles.

If you are relying only on pulling a driver's moving violation record and not the Clearinghouse, you are in breach of regulations and you could leave your organization exposed.

If you employ a driver who is under suspension from driving by the Clearinghouse and they are involved in an accident, the victims could build a case that your organization was negligent in letting the individual drive and not checking the Clearinghouse first.

If they can prove negligence on a fleet operator's part, the business could be in for a hefty court judgment. ❖

Continued from page 1

Have Protocols to Reduce Chances of an Excluded Event

The takeaway

If your firm is hit by a cyber attack, you'll be doing most of the heavy lifting and you'll be dealt many expenses to get back to normal.

Respondents to the Delinea poll said that their cyber insurance policies were most likely to cover expenses related to data recovery, although insurers' definitions of that term vary depending on the circumstances.

"For example, say an attacker is holding your data for ransom. Some insurance companies may say they want to make the decision whether to pay the ransom to recover your data (regardless of your preference)," the report states.

The key is to understand your policy's coverage and have protocols in place to reduce the chances of an excluded event taking place. ❖

Theft and Vandalism on the Rise, Protect Your Business

THEFT AND vandalism against business has been growing rapidly, with 28% of businesses reporting an increase from 2021 to 2022, according to a new report.

Only 3% of organizations polled in "The State of Physical Security Entering 2023" survey by Pro-Vigil reported a decrease in such crimes, while 59% said it had stayed the same.

Burglaries, robberies and vandalism can be devastating to small businesses in terms of money, customers and employee safety. Mitigating this risk can be difficult since gaps in insurance may leave firms unprotected.

Here are some considerations to safeguard your firm:

Burglary prevention

Establish clear policies about employee theft, crime reporting, opening and closing, and other security procedures. Provide training for all employees on these procedures.

Use good locks, safes and alarm systems, keep detailed inventories and banking records and have back-up copies off-premises. Engrave your company name on valuable office equipment and tools.

Fit outside entrances and security doors with deadbolt locks. Security doors should be metal lined; secure them with metal crossbars and install security hinges or peen hinge pins.

Remove expensive items from window displays. Light the outside, especially around doors and windows, and keep lights covered or high to prevent tampering.

If you have a safe, leave it open when empty, as well as the cash register. Change the combinations and keys when an employee that has had access leaves the business.

Robbery prevention

If confronted by a robber, your employees should cooperate with them. To minimize risk, employees should greet every person who enters in a friendly manner, as personal contact can discourage a would-be criminal.

Keep windows clear of displays and signs and make sure the business is well-lit. Eliminate any blind spots that may hide a robbery in progress. Instruct employees to report any suspicious activity or person, and write down any information, like car license plate, for future reference.

Make your bank deposits often, and during business hours. Do not establish a pattern; take different routes and times.

Vandalism prevention

Annual damage in the United States due to vandalism is in the billions.

Use landscape designs, building materials, lighting or fences to discourage vandals. Clean up any vandalism after it happens, and work with local law enforcement to report vandalism.

Consider organizing a "business watch" that is modeled after the neighborhood watch. Be alert and report suspicious behavior to law enforcement immediately, even if it means taking a chance on being wrong.

The takeaway

Crime and theft prevention are key to keeping your premises, inventory and machinery safe. You should have in place procedures for all of the above to ensure the safety of your property and your employees. ❖

Worker Stress, Burnout May Compromise Safety

AMERICANS ARE working longer hours and facing more demands for productivity, leading to stress and burnout, which in turn can affect workplace safety, according to risk management experts. Understaffing plays a part in this, they found.

When workers are stressed or required to work quickly, they are more prone to making mistakes that can injure themselves or co-workers. On top of that, there's been an increase in mental health issues, while outside factors like household finances can also add to an employee's stress, making them less mindful at work.

In May 2023, Fed-OSHA launched a web portal for employers to understand and recognize the workplace safety implications of stressed workers and what they can do to help.

THE NEGATIVE EFFECTS

A recent poll of 2,515 workers by the American Psychological Association (APA) found that 77% of respondents said they had experienced work-related stress in the last month and 57% said they were experiencing negative effects of work-related stress driven by burnout, including:

- 31% reported feeling emotionally exhausted,
- 26% said they don't feel motivated to do their best,
- 25% had a desire to keep to themselves,
- 23% wanted to quit,
- 20% reported lower productivity,
- 19% said they felt irritability or anger with co-workers or customers, and
- 18% said they felt ineffective.

Stress is prevalent in production environments, liike construction, manufacturing, warehousing, health care and transportation.

Workplace stressors

Workplace stress is caused by a multitude of factors, including:

- Toxic workplaces.
- Verbally abusive superiors, co-workers or customers.
- Difficult-to-meet deadlines or quotas.
- Too much or too little work.
- Poor work relationships.
- Poor communication from management,.
- Insufficient compensation.
- Uncomfortable workplace environment.

What employers can do

OSHA and the APA recommend that employers:

- Be aware and acknowledge that people can carry an emotional load that is unique to their lives. They may be experiencing heightened levels of loneliness, isolation, uncertainty, grief and stress; and some may face additional demands, such as parents caring for children or elderly household members.
- Identify factors making it harder for workers to get their jobs done and determine if adjustments can be made.
- Show empathy. Employers can reassure employees they are open and receptive to discussions about their work stress by creating a safe and trustworthy space.
- Offer health insurance with coverage for mental health and substance use disorders.
- Encourage workers to take their breaks.
- Offer an employee assistance program.
- Offer paid time off and sick leave.
- Offer paid mental health days off.
- Train supervisors and managers to avoid being verbally abusive and to treat employees with respect. ❖