



WEISER
INSURANCE SERVICES

FIRST QUARTER 2025

THE REPORT

BEST PRACTICES

Why It Is Important to Review Your Insurance Annually

BUSINESS E-MAIL compromise scams are now the most common type of cyberattack businesses face, and all types of these attacks are showing no signs of letting up, according to a new report.

Nearly three out of every four businesses were targets of these attacks and 29% of those firms became victims of successful attacks, according to the report by Arctic Wolf, a cyber-security firm.

While this has become the most common type of attack, a number of other schemes like ransomware attacks and data breaches continue growing in number.

Any of these attacks can drain a company's finances and result in tricky legal and possibly reputational issues that take time and money to resolve.

The trends

The main threats businesses face, according to the report, are:

Business e-mail compromise (BEC) – Seven in 10 organizations surveyed said they had been targeted by these types of scams.

Some examples of BEC attacks include impersonating company executives to request wire transfers, falsifying invoice payment details, and tricking employees into revealing sensitive information. These scams can result in significant financial losses for businesses.

CAUTION: For businesses that use cloud-based e-mail services like Office365, these attacks are hard to detect since they don't reside on company servers.

With many organizations moving to cloud-based e-mail services, these types of attacks can be difficult to identify with traditional security tools and may go undetected until they have successfully executed their objectives.

Data breaches – Nearly half (48%) of organizations surveyed reported that they'd found evidence of a breach in their systems. The authors said that does not mean that the other 52% didn't suffer a breach; it means they failed to find evidence of one.

Ransomware – Some 45% of organizations surveyed admitted to being the victim of a ransomware attack within the last 12 months. These attacks usually involve criminals gaining access to a company's systems by getting an employee to click on a malicious link, after which they lock down the system and demand a ransom to unlock it.

Increasingly, perpetrators are also stealing data and demanding a second ransom to give it back and not release the data to others.

See 'Coverage' on page 2

WEISER INSURANCE SERVICES

WISHES YOU A

Happy New Year!

2025

Welcome to the Weiser Insurance Newsletter!

Weiser Insurance is pleased to present you with the first edition of our newsletter. We hope the articles in this and future editions will provide insight into an array of insurance matters, and we urge you to contact us with questions and comments.

Our goal is to provide excellent service, competitive pricing, and products tailored to meet the special needs of each client.



WEISER
INSURANCE SERVICES

Weiser Insurance Services

201 S 9th
Adel, IA 50003

Phone: 515-993-1829
E-mail: info@weiserins.com
weiserins.com



Twelve Months of Safety Meeting Topics

JAN **Workplace hazards** — Cover common types of hazards found in the construction industry, how to assess their severity and the different control methods employed to prevent incidents from occurring.

FEB **Managing worksite conditions, equipment** — The dangers change depending on the job and the weather. Focus on general tool safety guidelines, including rotating machinery, air, electric and power tools. Also focus on potential slips, trips and falls.

MAR **Fall protection** — Focus on fall-protection equipment, how to safely work on heights, and common fall-protection inspection points.

APR **Ladder and scaffold safety** — Focus on the types of ladders and scaffolds that will be used in a job, correct set-up, usage and contraction, along with a description of scaffold tags.

MAY **Defensive driving** — Focus on state driving laws, defensive driving, proper operations of equipment on worksites and roads, and typical causes of accidents.

JUN **Powered mobile equipment** — Cover all powered mobile equipment you'll have on site, conducting pre-job walk-arounds of a machine and how to work safely around the various pieces of equipment.

JUL **Personal protective equipment** — Focus on which PPE should be used for different types of work and circumstances that call for specialized PPE.

AUG **Excavating and trenching** — Training should explain hazards like engulfment, different soil types and their properties, and proper safety precautions.

SEP **Personal physical care and conduct** — Work in construction requires health and stamina. Concentrate training on ways to care for your body to prevent injuries and the impacts of drugs and alcohol on your ability to work safely. Also cover expected professional behavior and conduct on the worksite.

OCT **Hazard communications** — Focus on the Globally Harmonized System of hazardous materials labeling and the function of safety data sheets.

NOV **Environmental safety** — Focus on the types of pollutants found in the industry, what to do in case of an accidental release of hazardous materials — and on the safe transportation of dangerous goods.

DEC **Emergency response** — Train on emergency response. Cover whom they should call, including emergency services, evacuation, locating first aid supplies and basic fire-fighting techniques.

Continued from page 1

Coverage Reviews with Are Ideal for Identifying Coverage Gaps

How to Protect Against BECs

- Register all domain names that are similar to the business's legitimate website and can be used for spoofing attacks.
- Create rules that flag e-mails received from unknown domains.
- Monitor and/or restrict the creation of new e-mail rules on your servers.
- Enable multi-factor authentication.
- Conduct BEC drills, similar to anti-phishing exercises.
- Companies that use Office 365 or other cloud-based e-mail services, should employ detection tools or services specifically designed to monitor for threats related to BEC scams.

Ransomware defence

Train your staff on how to detect or flag suspicious or potentially malicious e-mails and not to click on links in e-mails from unknown senders.

Regularly back up system so you can restore functions if hit by ransomware.

Store backups separate devices that cannot be accessed from a network or the web, such as on an external hard drive. ❖

CONSTRUCTION THEFT

How to Protect Your Tools, Equipment

ONE OF the biggest headaches for contractors is equipment and tool theft, as thieves regularly raid worksites after hours or steal tools from parked vehicles. They can make away with tens of thousands of dollars worth of equipment, and in serious cases it can result in project delays and workers unable to do their jobs.

Also, if the theft occurs away from the contractor's own facilities and instead at a worksite or while the equipment is in transit, the company's commercial property insurance policy won't cover the theft.

Enter tool and equipment insurance

Typically, commercial property insurance only covers your equipment when kept within your premises and not on a worksite. Tool and equipment insurance covers movable equipment and tools wherever you've stored them.

It typically covers theft, vandalism, accidental damage, and loss of tools and equipment while they are on-site, in transit or stored at a designated location.

Some policies may offer coverage for the cost of renting replacement tools or equipment to minimize project disruptions. Others include provisions that compensate you for lost income and costs incurred due to project delay if these are caused by a covered incident.

Policies typically cover tools and equipment worth up to \$10,000. If the value of everything is more than \$5,000, the insurer will often require that all of the items are inventoried and scheduled on the policy.

If you have extremely high-value tools and equipment, you would likely need to get a separate specialized policy.

Prevention tips

The best approach is to avoid having your tools and equipment stolen in the first place. Fortunately, there are steps you can take to reduce the chances of theft.

Secure equipment and tools – If you store your equipment on-site, set aside a section of your site where you can store the gear in locked, secure storage containers when not in use. Use well-constructed and tamper-proof containers that cannot be moved.

Install security cameras and alarms – Security cameras and alarms, along with signs announcing their presence, can help deter thieves. Cameras also can provide evidence of theft and alarms can alert your workers of intrusions.

Asset marking and tracking – Adopt asset-management solutions with telematics to discourage theft and aid in recovery if equipment is stolen. Implement tracking devices on high-value assets to enable real-time location monitoring. Decals on equipment stating that it is tracked and monitored can deter theft.

Create a reporting system for missing tools – Implement a system so that employees can report missing tools. A well-designed reporting system can help track any misplaced tools, while addressing issues like theft or inaccuracies with inventory.

Train your staff – Devote an afternoon to discuss best practices in van and tool safety and security with your team. Additionally, ensure that new staff members are informed about these measures to maintain a vigilant and secure work environment.

Conduct employee background checks – Conducting background checks during the hiring process can help combat theft on your construction site. Background checks not only verify the qualifications and past work history of potential employees, but detect any known criminal activity as well. ❖

EXPENSIVE HEISTS

- In September 2023, thieves stole more than \$50,000 worth of tools and landscaping equipment from a worksite run by Ground Builders Landscaping in Douglas County, Nebraska.
- A Columbus, Ohio man who committed countless thefts of tools and construction equipment across a 10-county area was sentenced to more than a decade in prison in October 2023. It is estimated that upward of around \$100,000 worth of construction equipment and tools were stolen by the thief.
- In November 2022, thieves stole \$100,000 worth of tools and equipment from a construction site run by SolTerra Capital Inc., a Portland, Oregon, developer.



A Hacker's Tips on Keeping Your Personal Data Safe



ONE BIG concern for all of us these days is online safety and protecting our personally identifiable information and credit card information.

Not only that, but clicking on a nefarious link on a website or in an e-mail can unleash a cyber attack on your computer with bots rifling through all of your files.

In addition to online scams, criminals are also calling people and asking for personal information.

Recently, an anonymous hacker who now writes a cyber security blog had these recommendations for individuals who want to protect themselves and their files when online.

Here's the techie's advice:

- **Check senders carefully.** Cyber criminals will try to get you to click on a link in an e-mail by making it seem like it comes from an official source, like "auditor@irs.gov." If in doubt, don't click on any links and call the agency using information from 411 or other legitimate sources.
- **Don't believe every caller.** If you get a call from someone claiming to be from the IRS who tells you that you owe back taxes or from your bank asking you to log into your account it's likely a scammer. Tell the caller that you'll call them back. Conversely look up the number and call.
- **Don't follow links to a site that's going to ask for secure information, such as a password.** Scammers will send official-looking e-mails asking you to log into your bank account by clicking on a link. But, the link is to a spoof site that will ask them to input their username and password, which the scammer then steals to raid your bank account.
- **Verify that the visual link and the actual link match.** For instance, let's say the link is "PETA. org." But if you move your cursor over the link without clicking, most

browsers will then show you the real link, either near the cursor, or at the lower-left corner of the window. If you see something like "PETA.smurfit.org" or "PETA.ru," or anything else that doesn't exactly match, it's likely they're trying to dupe you.

- **Don't automatically grant access for all programs.** If you download a new game online and it asks you to enter the system manager password, you may be right to be suspicious as a game would not need system-level access.
- **Use unique passwords.** Employ passwords that have a combination of numbers, letters, capitals letters and unique characters. Don't use the same password on multiple sites.
- **When a website asks security questions, give ridiculous answers.** For instance, if a site asks which high school you went to, don't use the name of your real school. A dedicated hacker can find out where you went to high school. Instead, you might want to write something like "cuddly panda" or "fuchsia."
- **Ignore spam e-mail.** You can often tell that e-mail is spam before opening it. Look at the "From" address. Do you know anybody named "Special Offer?" If the subject is odd, like "Donald Trump says he has a big brain, here's why," it's likely spam and should be avoided.
- **Set your e-mail reader so that it does not load images or follow links automatically.** For instance, if a scammer includes an image, allowing it to load can send the image ID to another server that then gains access to your system. Before you allow the browser to load images, check that every image name is generic. ❖