



BEST PRACTICES

Risk Management Pitfalls Your Firm Must Avoid

HAVING A solid risk management program in place can help your company avoid significant disruptive events, or enable it to respond.

However, even the best-laid plans can go awry. This can happen if management fails to fully buy into the efforts or if implementation of a risk management regime is done without careful forethought or appreciation of all the potential exposures that the organization faces.

Risk management covers workplace safety, business interruption, catastrophe response and liability issues that could harm the organization, third parties, vendors or customers.

Unfortunately, many firms make mistakes when implementing a risk management plan. You'll want to avoid the following crucial mistakes that could cause it to fail.

Failure to identify potential risks

It's important that organizations assemble a team to identify risks. This should involve staff members from different departments, supervisors and management.

- Workplace walkarounds,
- Talking to industry experts,
- Evaluating past incidents and near-miss reports, and
- Conducting job safety analyses or a similar method.

Not analyzing the risks

You can't stop at identifying risks the organization faces.

Failing to perform an analysis of the risks will make it more difficult to understand them, and to develop plans for managing and mitigating them.

For example, your team can analyze workplace injury records and near misses to develop or improve safety policies and procedures to prevent future incidents.

Also, a thorough analysis of external risks can help them develop procedures to avoid legal or regulatory entanglements that can result in fines, penalties and jury awards.

See 'Risk' on page 4

Areas where committee should identify risks

- Business processes.
- Personnel management, policies and hiring procedures.
- Company data security.
- External environment, including vendors, catastrophes, supply chain, etc.
- Market competition
- Other unique factors to the firm.

To expand on the process and ensure they don't miss anything, your team should use different methods to identify exposures, including:

- Checklists,
- Employee interviews,



Welcome to the Latest Edition of our Newsletter!

We've packed this issue with exciting insights and fresh content to keep you informed and inspired. Whether you're looking for new trends, helpful tips, or exclusive news, we've got something for you. Read on for everything you need to know this month — and as always, feel free to share your thoughts with us. We hope you find some time to enjoy the rest of your summer!



Weiser Insurance Services

201 S 9th
Adel, IA 50003

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

As Mobile Threat Booms Revisit Your BYOD Policies



AS NEW malware and ransomware that specifically targets mobile devices grows exponentially, if you have not set rules for employees who use their own smartphones for company business, you should do so now.

While implementing a bring your own device (BYOD) program can save your company money by not buying new phones for staff, there are other benefits like increased productivity, greater flexibility and higher employee satisfaction.

However, if your staff are not protecting their devices and following rules aimed at thwarting hackers, their smartphones can become backdoor gateways for malicious cyberattacks.

Threats to your organization include:

- **Data leakage.** Data can be lost or exposed when devices are misplaced or stolen, or if a personally owned device has malware on it.
- **Unauthorized access.** Attackers can gain access to a compromised device or network credentials stored on it, potentially leading to unauthorized access to sensitive company information.
- **Malware infections.** Malware can easily spread from personal devices to company networks, enabling attackers to steal data.

- **Legal issues.** Using personal devices for work can raise legal issues, especially if data is not properly secured or if employees are not adequately trained on security protocols.

Strategies for protecting your firm

Take care when downloading apps – A July 2024 report by Human Security found more than 250 “evil twin” applications on the Google Play Store. These apps are built to look authentic and often contain malicious code that launches upon download.

Urge caution – Inform your staff that they need to be cognizant of their online behavior. You won’t be able to control if they shop online at compromised websites or lose a device.

Keep a register of connected devices – Maintain a detailed register of users and devices. Audit your network regularly to detect unauthorized connections and resource usage.

Enforce on-device security – Smartphones and tablets come with passcode controls that restrict access. As part of an employer’s default BYOD agreement, staff should have the passcode enabled before they are granted access to corporate resources. Also consider implementing multi-factor authentication for an additional layer of security.

Require VPN use – To ensure that data transfers are secure in transit, require that your staff devices be set up with VPN access.

Implement a mobile device management platform – This allows you to enroll devices, specify and enforce network access rights and even apply content filtering.

Segregate apps – Creating a barrier between personal and private use of the device can prevent accidental access to work data. This can be achieved through techniques like containerization and work profiles, which isolate corporate data and apps within a specific part of the device, preventing them from being accessed by personal apps or data.

Have protocols for when employees leave – If an employee is terminated or begins exhibiting questionable behaviors, immediately revoke their access to sensitive data before it’s leaked.

Insurance

Some cyber insurance policies limit coverage to devices owned or leased by an organization. If you allow BYOD in your workplace, you’ll want to make sure that your policy covers these devices.

Some insurance providers offer enhanced or specialized coverage for BYOD-related incidents, acknowledging the unique challenges and risks involved. ❖

BEST PRACTICES

Filing Late and Other Ways to Have a Claim Rejected

ONE MISTAKE you want to avoid if you incur property damage to your business is to wait too long before filing the claim.

The owners of Dallas Plaza Hotel learned this the hard way when a U.S. Circuit Court of Appeals held that the business had waited too long to file a claim with its insurer after suffering hail damage.

The court ruled that because the hotel had waited nearly two years to file the claim, it was impossible for the insurer, American Insurance Co., to ascertain exactly when the damage had occurred.

The hotel's property policy required that the insured make "prompt notice" of any claims.

The insurer rejected the claim when it received it 19 months after the initial damage.

It reasoned that there had been so many hailstorms in the area that it could not determine what caused the damage or when the damage occurred and, specifically, whether it had occurred within the policy period.

The lesson: waiting too long to file an insurance claim can be costly and businesses risk seeing their insurer deny the claim as most policies require that claims are filed in a timely manner. But that's just one way to have your claim denied.

The following are other sure-fire ways to risk having your claim denied or disputed by your insurance company.

Not reading your policy

Understand exactly what your policy covers. Typically, commercial property policies will not cover flooding or earthquake damage. That kind of coverage will often require a separate policy or rider.

Not being prepared

If your business has suffered damage, you'll be better off if you know what to do in advance. You can minimize any hassles by planning ahead before you suffer any damage.

Advance steps you can take

- Create an emergency action plan.
- Review your policy to make sure you have adequate coverage.
- Know where your insurance policy is kept.
- Keep electronic or physical copies offsite.
- Have your insurer's claims phone and e-mail information in the contacts on your phone, so you can call them immediately if you have to file a claim.

Not keeping damaged goods

If your business cleanup includes removal of items such as water-damaged merchandise, flooring or insulation, keep it all, even if it has to pile up in the parking lot. The damaged materials are all evidence of the impact of the disaster on your business.

Take photos and itemize everything that was damaged. You may have to make repairs immediately to prevent further damage, or move machinery to a new location. However, you should check with your insurer about any repairs that may go beyond just trying to minimize damage.

If so, photograph the original scene to document how it was before you started your cleanup. Also take photos of any repairs you make. ❖





WEISER
INSURANCE SERVICES

Weiser Insurance Services

201 S 9th
Adel, IA 50003

Continued from page 1

Your Risk Management Plan Must be Robust as Risks Rise

Failure to control risk

Knowing the risks is only part of the equation. Your team also needs to establish policies and procedures for controlling those risks and create plans to react if an incident occurs.

By controlling risks, you can reduce legal, operational and regulatory exposures, ensure business continuity and reduce work injuries.

Failure to secure proper coverage

Ensure that the organization has insurance coverage that meets its risks. After your team has conducted its risk analysis, you may want to schedule time with us to review your policies to see if you have any coverage gaps that could turn out to be costly.

A policy review should be an annual event, and you should note any new equipment or property purchases and additions to your staff.

Insurance issues to keep in mind

- Make sure you have an accurate assessment of your business assets' value.
- If you have risks not covered by your current policies, you may need specialized coverage. Look for insurance gaps like lack of employment practices liability insurance or professional liability coverage if you provide services.

Failure to follow up, monitor results

Your risk management plan must be robust and adaptable as new risks arise. The committee should meet every quarter to discuss new risks that members have identified since the last meeting.

The meetings should also be used to monitor results and progress. For example, if you instituted new safety protocols in one department, you should evaluate its effectiveness and take steps to improve it if needed.

By monitoring risk management, you can expose gaps in your plan and better evaluate its effectiveness. ❖

