CHILD WELFARE
Specialty Insurance Program

Emergency Response Safety for Schools

Most school districts and individual schools have emergency management plans in place. However, they are not always practiced regularly, coordinated with community resources, updated regularly or based on factual data and circumstances. As a result, when schools and districts find themselves in situations that merit an emergency response, they are often left unprepared.

Having a solid emergency response plan in place is essential, as emergencies of all shapes and sizes occur in schools on a daily basis, and these incidents can have lasting physical, emotional and educational ramifications.

According to the U.S. Department of Education Office of Safe and Drug-Free Schools, there are several phases involved in planning an effective emergency management program.

Phase 1: Mitigation and Prevention

Mitigation is the actions schools and districts can take to eliminate or reduce the loss of life and property damage related to an event that cannot be prevented. On the other hand, prevention is the actions schools and districts can take to decrease the likelihood that an event or crisis will occur.

Some examples of mitigation include taking the following steps:

- Bolting bookshelves to the wall
- Fencing off hazardous areas
- Some examples of prevention include taking the following steps:
- Forming policies related to food preparation, mail handling and building access
- Making assessments related to threats, physical infrastructure, and culture and climate of the school
- Current school efforts such as anti-bullying policies and wellness activities

To put this phase into action, school officials should be encouraged to take the following steps:

- Know the school building thoroughly and the community at large.
- Become acquainted with local first responders, community partners and the state emergency management agency.
- Bring together regional, local and school leaders.
- Make regular school safety and security efforts part of larger mitigation and prevention efforts.
- Establish clear lines of communication.
- Conduct safety and security need assessments.
- Incorporate lessons learned from previous emergencies and drills to update emergency plans.

Phase 2: Preparedness

The preparedness phase is designed to get the school community ready for potential emergencies by coordinating efforts with community partners. This involves developing protocols and policies, creating incident command systems and conducting formal training and exercises:

- Identify and involve stakeholders in the planning process.
- Determine what crises the plan will address.
- Define roles and responsibilities.
- Develop methods for communicating with staff, students, families and the media.
- Obtain necessary equipment and supplies.
- Prepare for immediate responses.
- Create maps and facility information.
- Develop accountability and student release procedures.
- Predetermine policies for locating staff and teachers following an emergency.
- Establish systems off-site for storing registration information and for conducting payroll services.
- Practice your program with all those affected by a potential emergency.
- Address liability issues.

Marshall & Sterling Insurance
Child Welfare Specialty Insurance Program
www.marshallsterling.com/monticello/child-welfare

Marshall & Sterling INSURANCE

Irene Jones, Program Manager
800-782-2926, x2603
ijones@marshallsterling.com

Phase 3: Response

The response phase encompasses taking action to effectively contain and resolve an emergency through the implementation of the school's or district's emergency management plan:

- Expect the unexpected.
- Assess the situation and choose the appropriate response.
- Notify appropriate emergency personnel and the school crisis response team.
- Evacuate or lock down the premises, as appropriate.
- Triage injuries and provide emergency first aid to those who need it.
- Keep supplies nearby and organized at all times.
- Identify primary and alternative evacuation sites in case the primary sites are not available during an emergency.
- Move district resources (buses, etc.) out of the disaster area.
- Trust leadership to know how to handle the situation.
- Communicate accurate and appropriate information.
- Activate the student release system.
- If it is a large-scale disaster and the buildings were evacuated for an extended period of time, establish a system for distributing or disposing of food stored in school facilities,
- Allow for flexibility in implementing the emergency management plan.
- Document the process and how successful the emergency management plan was.

Phase 4: Recovery

The recovery phase is designed to assist students, staff and their families in the healing process and to restore the educational operations of the school. This includes repairing the physical/structural aspects of the school, attending to business or fiscal needs, getting back to academics and healing psychological or emotional wounds.

Planning for recovery involves establishing community partnerships, developing policies, providing training and developing memorandums of understanding:

- Assemble a crisis intervention team.

Having a solid emergency response plan in place is essential, as emergencies of all shapes and sizes can occur in schools on a daily basis.

- Return to the "business of learning" as quickly as possible.
- Keep students, families and the media well-informed.
- Provide assessments of the emotional needs of the staff, students, families and responders.
- Provide stress management after class resumes.
- Conduct daily debriefings with staff, responders and others assisting in the recovery efforts.
- Take as much time as needed for the recovery.
- Pre-negotiate contracts for transportation, food, construction and other district needs.
- Implement a system to manage the receipt of any donations.
- Goal of Emergency Response Systems
- If an emergency response system is created and executed correctly, it should hopefully achieve the following objectives:
- Address all four phases of emergency management, as listed above.
- Take an "all hazards" approach. This means that the plan addresses the following perils:
- Natural disasters–earthquakes, tornadoes, floods and other natural disasters.
- Technological, such as power outages
- Infrastructure, such as roads, bridges and utilities
- Nonstructural, such as portable room dividers, bookshelves, suspended ceilings and light fixtures
- Man-made, such as hazardous materials release or acts of terrorism
- Biological, such as flu pandemic or contaminated food
- Physical well-being, such as broken bones from playing too rough or student suicide
- Student culture and climate, such as bullying, drugs or violent behavior on the premises

By engaging the local government, law enforcement, the students and their families and the school district in these emergency response efforts, you are taking the appropriate measures to make your school and district a safer place to learn and work.

Marshall & Sterling Child Welfare Specialty Insurance Program Newsletter – MARCH 2016

Pollution & Your Organization: Control Hazards to Control Risks

Your organization should provide a safe and healthy environment, but there is a significant hazard to children and young adults that many educational facilities overlook—pollution. Young people are much more susceptible to illness from pollutants than adults, and with countless sources of pollution, you should recognize the gravity of the risk.

A pollution incident or contaminant release at your location could cause large-scale injury, illness or even death. In addition to potentially massive bodily harm lawsuits, the organization would also be responsible for other legal fees and cleanup costs. Plus, a large enough incident could cause a closing or gain a bad reputation in the local community. Identify sources of pollution and take steps to mitigate these risks to avoid costly and preventable mistakes.

Potential Pollution Sources

The following are examples of common pollutants in educational environments:

- Fumes from fresh paint, new carpeting, cleaning chemicals or pesticides
- Drinking water
- Mold conditions
- HVAC systems
- Caulk containing harmful particles
- Poor ventilation
- Chemicals that have been improperly disposed of
- Chemicals from art and science classrooms
- Older buildings that deteriorate or malfunction, causing air or water contamination
- Elevated lead levels in drinking water
- Water contaminated by sidewalk salt, pesticides or other chemicals
- Polluted air from nearby building or car emissions

Buses are also a source of pollution, as dangerous fumes can enter the enclosed space; however, educational facilities are generally only liable for this risk if they own and operate their own buses, though you should check your insurance coverage to be sure.

Pro Tip: *In the event of a pollution incident, you could be responsible for everything from legal fees to cleanup costs, and it could leave your school with a poor reputation in the community. Call us with concerns!*

Risk Management Techniques

Be aware of possible pollutants and then work to mitigate or eliminate the hazard if possible. Here are some tips to get started:

- Develop, maintain and train staff on standard procedures for storing, handling and disposing of chemicals, pesticides and other hazardous materials.
- Have your buildings regularly inspected and repaired, including HVAC systems, ventilation, faucets and pipes.
- Use minimal amounts of fertilizer when possible.
- Keep lockers and buildings clean and dry to avoid attracting pests.
- Use sand on slippery surfaces instead of salt.
- Keep the ground free of litter.
- Use safer alternatives to hazardous materials when possible.
- Ensure that bus companies under contract with your facility install appropriate filtering devices on tailpipes to avoid fume leaks into the interior of the bus.
- When planning new construction, take distance from industrial buildings and highways into consideration.

Marshall & Sterling Insurance
Child Welfare Specialty Insurance Program
www.marshallsterling.com/monticello/child-welfare

Marshall & Sterling INSURANCE

Irene Jones, Program Manager
800-782-2926, x2603
ijones@marshallsterling.com

Marshall & Sterling Child Welfare Specialty Insurance Program Newsletter – MARCH 2016

Cyber Risks - Responding to a Data Breach

No company, big or small, is immune to a data breach. Many small employers falsely believe they can elude the attention of a hacker, yet studies have shown the opposite is true—a growing number of companies with fewer than 100 employees are reporting data breaches every year.

Data breach response policies are essential for organizations of any size. A response policy should outline how your company will respond in the event of a data breach, and lay out an action plan that will be used to investigate potential breaches to mitigate damage should a breach occur.

Defining a Data Breach

A data breach is an incident where Personal Identifying Information (PII) is accessed and/or stolen by an unauthorized individual. Examples of PII include:

- Social Security numbers
- Credit card information (credit card numbers—whole or part; credit card expiration dates; cardholder names; cardholder addresses)
- Tax identification information numbers (Social Security numbers; business identification numbers; employer identification numbers)
  - Biometric records (fingerprints; DNA; or retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information (paychecks; paystubs)
- Medical information for any employee or customer (doctor names and claims; insurance claims; prescriptions; any related personal medical information)
- Other personal information of a customer, employee or contractor (dates of birth; addresses; phone numbers; maiden names; names; customer numbers)

"…a growing number of companies with fewer than 100 employees are reporting data breaches every year."

Internal Responsibilities Upon Learning of a Breach

A breach or a suspected breach of PII must be immediately investigated. Since all PII is of a highly confidential nature, only personnel necessary for the data breach investigation should be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?
- How did the breach happen?
- What types of PII were possibly compromised? (Detailed as possible: name; name and social security; name, account and password; etc.)
- How many customers may be affected?

Once basic information about the breach has been established, management should make a record of events and people involved, as well as any discoveries made over the course of the investigation to determine whether or not a breach has occurred.

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the PII lost (customer contact information alone may present much less of a threat than financial information)
- Amount of PII lost and number of individuals affected
- Likelihood PII is usable or may cause harm
- Likelihood the PII was intentionally targeted (increases chance for fraudulent use)
- Strength and effectiveness of security technologies protecting PII (e.g. encrypted PII on a stolen laptop, which is technically stolen PII, will be much more difficult for a criminal to access.)
- Ability of your company to mitigate the risk of harm

Government Regulation

There aren't many federal regulations regarding cybersecurity, and the few that exist largely cover specific industries. The 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley (GLB) Act and the 2002 Homeland Security Act, which includes the Federal Information Security Management Act (FISMA) mandate that health care organizations, financial institutions and federal agencies, respectively, protect their computer systems and information. The language is generally vague, so

individual states have attempted to create more targeted laws regarding cybersecurity.

California led the way in 2003 by mandating that any company that suffers a data breach must notify its customers of the details of the breach. Today, 46 states and the District of Columbia have data breach notification laws in place. Only Alabama, Kentucky, New Mexico and South Dakota have yet to enact such a law.

While notification laws vary from state to state, all include four basic provisions:

1. All notification laws put a number on how long companies have to notify customers of a data breach and by what medium the notice will be given (written, email, press release, etc.).
2. Laws set forth a penalty system (that differs from state-to-state) for failure to notify customers in a timely manner.
3. Depending on the specifics of the breach, customers can sue the company for its part in the data breach.
4. All notification laws have exceptions in a range of situations.

Your Notification Responsibilities

Responsibility to notify is based both on the number of individuals affected and the nature of the PII that was accessed. Any information found in the initial risk assessment should be turned over to the legal counsel of your company who will review the situation to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification should be made in a timely manner, but make sure the facts of the breach are well established before proceeding.

In the case that notification must be made:

- Only those that are legally required to be notified should be informed of the breach. Notifying a broad base when it is not required could raise unnecessary concern in those who have not been affected.
- A physical copy should always be mailed to the affected parties no matter what other notification methods are used (e.g. phone or email).

- A help line should be established as a resource for those who have additional questions about how the breach will affect them.

The notification letter should include:

- A brief description of the incident, the nature of the breach and the approximate date it occurred.
- A description of the type(s) of PII that were involved in the breach (the general types of PII, not an individual's specific information).
- Explanation of what your company is doing to investigate the breach, mitigate its negative effects and prevent future incidents.
- Steps the individual can take to mitigate any potential side effects from the breach.
- Contact information for a representative from your company who can answer additional questions.

We Can Help You Recover from a Data Breach

At Marshall & Sterling, we understand the negative effects a data breach can have at your organization. Contact us today so we can show you how to recover from a breach and get your company back on its feet.

Learn More: *Is cyber insurance right for your organization? Watch as Irene Jones briefly shares the importance of cyber liability insurance for your child welfare organization.* ***Click here to watch the video!***

Irene Jones, Program Manager
800-782-2926, x2603
ijones@marshallsterling.com

Marshall & Sterling Child Welfare Specialty Insurance Program Newsletter – MARCH 2016

CWLA 2016 NATIONAL ADVOCACY SUMMIT

Investing In What It Takes: A Full Continuum of Care

Advocate on Capitol Hill for America's Children! On **April 18-20, 2016** the Child Welfare League of America (CWLA) will hold their National Advocacy Summit, *Investing in What it Takes: A Full Continuum of Care*, in Washington, D.C.

This Summit is your opportunity to tell Congress that we need new investments in children - starting with preventing child abuse, preventing foster care when possible and providing the best care when necessary, and above all, ensuring permanency and safety for all children through reunification, kinship care and adoption.

The CWLA plans to have speakers addressing some of the hot topics being considered on Capitol Hill, including the Administration's latest initiatives, proposals and pending guidance from Commissioner Rafael Lopez the head of the Administration on Children, Youth and Families (ACYF).

Click here to learn more and to register!

Just Press Play!

View our Child Welfare Risk Management video collection from Marshall & Sterling

Have you had funding changes at your Child Welfare organization recently? In this month's video Irene Jones, Program Development Manager for Marshall & Sterling's Child Welfare Specialty Insurance Program, shares how those funding changes may affect your insurance, and what you can do about it. Click to watch!

Featured Link of the Month:

How can Nature Play influence the well being of children? Find out at Green Hearts Institute for Nature in Childhood: http://www.greenheartsinc.org

LEFT: *Marshall & Sterling plays an active role in advocacy efforts for the child welfare industry. Irene M. Jones, our Child Welfare Program Manager, has previously joined others from across the nation for the Child Welfare League of America's national conference in Washington, D.C.*

Marshall & Sterling Insurance
Child Welfare Specialty Insurance Program
www.marshallsterling.com/monticello/child-welfare

Marshall & Sterling INSURANCE

Irene Jones, Program Manager
800-782-2926, x2603
ijones@marshallsterling.com