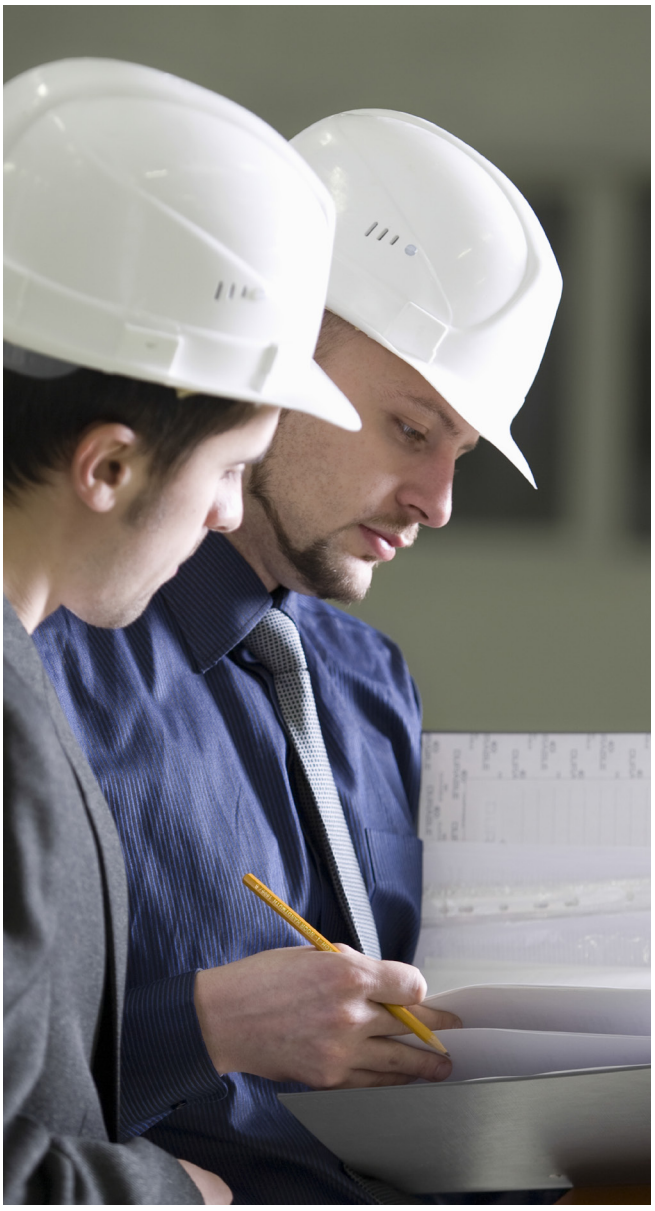
How to Build an Actionable Incident Response & Recovery Strategy

Over the past few decades, the world's economic and political infrastructures have been tested by physical and virtual terrorist attacks. If a business is targeted, transnational criminal organizations can destroy years of success and profitability in a matter of minutes.

These criminal networks are expanding and diversifying their activities, which increases the difficulty for businesses that are preparing response strategies that include potential terrorist threats. In the wake of the recent terrorist attacks in Paris and San Bernardino, companies are reassessing their own disaster response and recovery plans to make sure they account for potential terrorist threats to day-to-day operations.



Preparing for internal and external risks can help protect your business, but it is impossible to predict exactly how or when disaster will strike. Focusing too narrowly on specific incidents when designing your incident response strategy could hinder your company's ability to train your staff and react when faced with a threatening situation.

When creating your strategy, it is crucial to establish a framework that allows you to respond quickly in any situation. Regardless of the cause of the business disruption, the following four components will help you create a simple, yet holistic incident response and recovery strategy that is easy to implement.

Loss of Facilities

Immediately following the deadly shootings and explosions in Paris, French authorities closed major landmarks and cultural facilities, such as the Bataclan Theatre, the Eiffel Tower and the Louvre Museum. When an incident renders a facility unavailable for normal business operations, it can lead to devastating financial and functional consequences for the company. Regardless what causes the loss of facility, your strategy

needs to include how your business will continue its operations without disruption. This might include allowing your employees to continue their work from home or identifying a temporary alternative location for your staff, such as a client facility or community collaborative workspace.

Loss of People

Even if your facility remains intact after an incident occurs, your staff could be divided. Personal tragedy, illness or injury can render key employees unavailable or incapable of making critical decisions necessary to get your business back on track. Part of your overall strategy should include the cross-training of your staff so that each member is prepared to step in to perform critical functions should another employee be unavailable. Documenting your processes and procedures can ease the burden of training and provides employees with reference materials if necessary. It may also be valuable to identify an outside third party that could assist your team with critical functions in situations that would cause large members of your staff to be unavailable.

Loss of Technology

Not every incident will be physical. In 2014, JP Morgan experienced a data breach that compromised an estimated 83 million customer records. As today's business environment increases its dependency on information technology, companies need to have a plan in place that helps them recognize when a cyber-attack is occurring, react quickly to stop the breach and recover in a way that addresses both the short- and long-term problems from unauthorized access. Identifying potential system workarounds can keep your operations functioning should you lose the use of a system during an attack. Knowing exactly how long your company can continue to deliver client service without a particular system can help you create a recovery timeline once an outage or breach is contained.

Loss of Vendors

Even if you take loss of facility, people and technology into consideration, your incident response strategy is only as strong as the third party vendors you rely on to deliver goods or services. These vendors should be prepared to step in and assist should an incident happen to your company. Additionally, companies should expect that a vendor's disaster recovery plan offers protection for their company, as clients expect that you are protected if the disaster strikes on the vendor's end. For example, in 2013 hackers were able to access 40 million Target customer debit and credit card accounts by intruding into their systems through credentials stolen from a refrigeration, heating and air conditioning subcontractor. Your company should have a few alternative vendors identified that you could rely on should your primary vendor be compromised.

Your primary objective when designing an incident response and business continuity strategy is to create something that is actionable. Writing a plan that includes recovery steps for every possible scenario will most likely result in a complex document that isn't practical when employees need to act quickly. The key to a strong response and recovery plan is not to over-complicate the context. Your strategy should account for places, people and procedures, and it should be able to work in multiple situations. Over time, you can and should adjust or build upon your strategy as your company grows and evolves.

If you have any specific questions, comments or concerns about your organization's business continuity planning, please contact:

Mark Madar
CBIZ Risk & Advisory Services
RASinfo@cbiz.com | 866.956.1983

CBIZ®

Our business is growing yours

Learn how our business continuity planning services can protect your company at www.cbiz.com/ras