Booz | Allen | Hamilton

3 KEYS TO EFFECTIVE INCIDENT RESPONSE

Cyber incidents impact business operations and manifest themselves in various forms and levels of severity. They can touch every facet of your business, which can have a tremendous effect on your reputation and the trust you've established. An effective cyber incident response plan considers and involves the whole enterprise. A business, in its entirety, can be ready to respond more diligently if it takes into account the following tips.

Create a Holistic Plan

Create an incident response plan to prepare your company for two distinct, but interconnected, incident response purposes: Technical containment and resolution of the issue, and broader corporate risk mitigation. Effective cyber incident management extends beyond incidents. Your steady state—planning/preparing and post-incident improvement activities—are equally important. The response plan should reflect enterprise-wide roles and may address specific scenarios and how to mitigate their impact to the business. Drafting an initial plan requires effort to determine how people, processes, and technology work together across business functions. Consider both technical and corporate response roles. Once the plan is created, disseminate it to relevant stakeholders to ensure awareness and familiarity. The C-suite should communicate consistent support and encourage working relationships between business units and the IT department. This way, IT is empowered to share and enforce basic cyber security measures among staff, and staff will turn to the IT department when suspicion arises.

Test the Plan and Know the Roles

The most effective way to know how prepared you are for a cyber incident is to simulate one through an exercise to gauge your response. Testing not only gives you an assessment, but it can also help in keeping your plan updated to evolve with changes in threats, tools, and resources. These practice scenarios, often called "wargaming", can provide clarity on strengths and gaps within the organization, help you identify sufficient tools and resources, establish and clarify lines of authority, and designate response roles. This testing entails more than just making sure employees are trained on tools and procedures; they must be able to detect and remediate an incident—real or fictional. Wargaming serves to manage realistic situations and bring together the diverse set of groups that need to work collaboratively to respond.

Increase Awareness

Once the plans have been written and tested, keep up momentum and continued awareness about cyber risks. Engage your corporate communications or training department to help staff learn about cyber security in a way that is meaningful to their roles. In addition to internal messaging, make sure cyber incidents are incorporated into your organization's crisis communications capability. Organizations can benefit from having a crisis communications plan for a cyber incident, as well as designated spokespersons who are media-trained prior to an incident. You can also prepare in non-crisis times by setting up a responsible disclosure portal or by incorporating cyber information into your marketing materials.

KEY TAKEAWAY:

Have a cyber incident response plan that is enterprise-wide and uses a tested, all-staff approach to help resolve cyber incidents quicker and more transparently. Given that cyber threats are omnipresent, an incident may be all but inevitable. Fortunately, smart and proactive incident response planning can minimize the impact to your business.

For more information, contact:

Bill Stewart
Executive Vice President
stewart_william@bah.com
Tel +1 410 684 6473

www.BoozAllen.com/cyber-solutions

About Booz Allen Hamilton

Booz Allen Hamilton has been at the forefront of strategy, technology, and engineering for more than 100 years. Booz Allen partners with public and private sector clients across the globe to solve their most difficult c hallenges. To learn more, visit www.boozallen.com. (NYSE: BAH)