BEST PRACTICES: INTEGRATING INCIDENT RESPONSE AND BUSINESS CONTINUITY PROGRAMS

Cybersecurity incident response and business continuity, or disaster recovery, are still considered as separate functions and distinct disciplines in most organizations. This is clearly a missed opportunity to maximize resources since they are two sides of the same coin. These disciplines share the common goals of protecting the organization's reputation and ensuring continuity of operations. Therefore, it makes sense to integrate them so you can respond to attacks and data breaches faster, efficiently and effectively.

Here are some best practices to follow.

CONDUCT REGULAR JOINT PLAN REVIEWS

Business continuity plans and cybersecurity incident response plans should be linked and reviewed jointly with a similar process approach. It's important to establish a hierarchy of your organization's emergency plans so that everyone, including key stakeholders and decision-makers, clearly understands how these plans fit together. That context will enable smoother joint review processes. For example, if a critical system needs to be taken offline in an emergency and won't be available for an extended period, the potential business impacts should be addressed upfront during a joint review.

COLLABORATE ON DEFINING A COMMON LANGUAGE

Too often, business continuity and disaster recovery plans remain separate from incident response plans because team members have not collaboratively explored incident classification and response thresholds. Many business continuity and disaster recovery events are linked to technology and cybersecurity threats. By working together, teams can identify some of the most likely scenarios and test their plans and collaborate accordingly. In addition, by coming to a consensus on a common language, teams can prioritize the highest likelihood of incidents (through an impact and likelihood rating) and focus on those incidents first.

MERGE EXERCISE PROGRAM COORDINATION EFFORTS

Business continuity and disaster recovery teams pioneered the process of conducting simulations and drills to test their plans for situations like hurricanes and natural disasters. Cybersecurity incident response plans need testing, too. Everyone can benefit from practice drills to prepare for cybersecurity attacks. Business continuity and disaster recovery exercise planners may shy away from exercise scenarios involving technology if they do not have a technology background, and most technology people don't know how to properly develop exercise activities. These groups need to partner. Since people often need a motivational push to work outside of their silos, management teams should provide strategic direction to require the business continuity, disaster recovery and incident response teams to work together for the greater good of the organization.

USE A STANDARDIZED COMMUNICATION PROCESS AND TOOLS

We still see many instances in which the business continuity team has one set of communication tools, and the IT or information security teams have another. However, the processes around communicating critical information to key stakeholders in an emergency are not unique to the different disciplines. Since the different groups don't usually collaborate on defining requirements or allocating budget, they use different tools and operate in silos. Removing those silos and standardizing communication processes and tools helps to establish a common language, reduce redundancies and limit the confusion of responsibilities.

FIVE QUESTIONS TO ASK ABOUT INCIDENT RESPONSE AND BUSINESS CONTINUITY INTEGRATION

1. Do our incident response and business continuity or disaster recovery plans apply industry best practices?
2. Will combining teams and management processes provide equal focus to both disciplines? For example, if we have more dedicated resources and a bigger business continuity and disaster recovery team compared to our incident response team, will incident response get the same level of attention?
3. Are these teams reporting to a single person, and if so, is that person able to balance and coordinate responsibilities?
4. How can we balance the incident response team's focus on controls with business continuity and disaster recovery needs for meeting business goals?
5. Can we implement a high-level executive report that incorporates both sets of issues and communicates the business impact to key stakeholders?

MOTOROLA SOLUTIONS - YOUR TRUSTED PARTNER

As a leading provider of mission-critical solutions, we understand your mission can only be as secure as your partners enable you to be. Our goal is to provide you with transparency, accountability and security that's built-in from the start.

We believe that our set of highly knowledgeable people with industry certifications, best-in-class organizational policies and procedures and state-of-the-art automation and analytics tools enables us to uniquely deliver enhanced cybersecurity solutions that address your needs today and in the future.

For more information on our incident response and disaster recovery services, contact your Motorola Solutions representative or visit us at **www.motorolasolutions.com/cybersecurity**

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**