MARSH

INSIGHTS | NOVEMBER 2018

Cyber Incident and Breach Response Planning: Is It Optional Any Longer?

Cyber-crime has become a reality that businesses must become accustomed to. According to the *2018 Global Risks Report*, the number of cyber breaches that the average business recorded annually almost doubled from 68 in 2012 to 130 in 2017.

This reality is compounded by the reliance of companies on internet and connected technologies, which have become an integral part of their revenue-generating operations. A breach or attack could, therefore, be catastrophic, with costs potentially running into the hundreds of millions of dollars.

In view of the current threats, organizations have no choice but to take action to protect their business. Among the steps that organizations should be taking is the creation of a well-developed Cyber Incident and Breach Response (CIBR) plan, which is critical to business resilience and functions as an important risk mitigation tool.

Is Your Company Cyber-Ready?

The first question that businesses leaders must ask themselves should be: *Is our company ready to respond to a cyber incident or breach event?*

To be truly resilient, an honest and realistic answer is required. If the answer is "no," your company could face significant financial strains in the wake of an attack. According to the Ponemon Institute, in 2018 the average cost of a data breach was up 6.4% over the previous year's, to $3.86 million, with the average size of a breach increasing by 2.2%.

The financial benefits of effective incident response readiness are significant. As discussed in the Online Trust Alliance's 2017 *Cyber Incident & Breach Response Guide*, effective planning requires anticipating decision points. Evaluating scenarios in advance and running tabletop exercises help organizations align decision-making with their strategic goals and objectives. Not only does completing this process offer the benefit of improved preparation and potentially lower costs in the event of a real incident, but exercises also help refine and improve incident response plans that can dramatically reduce operational impacts. Having demonstrable incident response processes can also work to an organization's advantage by potentially making it a more desirable risk for cyber insurers. These include establishing relationships — whether formal or informal — with vendor partners before a crisis and making them part of exercises and training.

Three Paths to CIBR Plan Development

Organizations can develop CIBR plans by following one of three basic paths:

The do it yourself (DIY) method: The least costly — in theory — the DIY method involves all of the steps required if an organization was acting on its own. This includes researching best practices, evaluating available references, surveying stakeholders, and more. However, unless the team members involved have some CIBR experience, this method can take the longest amount of time and could be the most costly if there are false starts.

The subject matter expert (SME) method: Engaging a cybersecurity SME with experience in CIBR plan development can be the most costly method, but will likely take the least amount of time for the organization since such experts have the right experience.

Leveraging Best Practices for a CIBR

A good CIBR plan will apply guidance from NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, which outlines a firm foundation for planning that should be tailored to an organization's unique needs. Consistent with SP800-61, other NIST references, and other applicable resources, you should:

- **Develop a tailored, efficient, and effective plan:** This needs to fit with other organization plans and policies, including business continuity, IT disaster recovery, and crisis management and communication plans. They should reference each other where applicable and be consistent.
- **Use external rather than internal counsel:** In many cases, internal organizational counsel may not have the requisite experience. When a cyber incident occurs, make sure your first call is to external cyber-experienced legal counsel. Resulting decision-making and actions may be covered by attorney-client privilege.
- **Understand exact policy wording:** If your insurance policies include cyber perils, make sure you know exactly how they are defined and the resources your policies may require you to use in any cyber incident response or recovery activities. It is good practice to contact your insurance broker or insurer early to advise whether you're following the policy stipulations when a claim will follow the recovery process.
- **Identify your cyber vendors before an incident:** If you're not using vendors required by your cyber insurance policy, make sure you identify external cyber incident support vendors and have a list with updated points of contact as part of your CIBR plan. You may want to consider keeping some of these external vendors — especially legal counsel, forensic, call-center support, and IT engineering resources — on retainer so they will prioritize your response needs ahead of others.
- **Practice, practice, practice:** Once you have a plan in place, hold cyber incident exercises with technical support staff and senior leadership at least once a year. Companies that experience more frequent cyber-attacks might need to carry out quarterly exercises. All senior leadership and technical staff that are members of the CIBR team, or have supporting roles, must understand their responsibilities and can develop "muscle memory" to support a real-world cyber incident.
- **Conduct an after-action review:** Whether you've just carried out a CIBR exercise or dealt with a real event, you should complete a post-incident review that includes all key participants. Document what went well and any activities that need improvement and use these insights to improve your CIBR plan. Any actions from the review should be assigned to an action owner who is responsible for identifying corrective action until completed.

The hybrid method: This process offers the benefit of outside experience and time efficiencies along with internal skill-building and cost-saving benefits.

An organization's specific operating environment and resources, including available funds and cybersecurity staff, will dictate the path it chooses. Once a decision has been made, the organization needs to develop its CIBR plan strategy, goals, objectives, and governance, reinforcing that the CIBR plan is a policy document and has the approval of senior leadership.

Building a CIBR Team

Who sits on the CIBR team is an important decision that business leaders shouldn't take lightly. Team members have a crucial role since they will be the ones overseeing the responses and actions during a cyber incident or breach event. They do not necessarily need technical expertise, nor are they generally members of the senior executive leadership team. Instead, they tend to be midlevel managers with experience in IT, IT security, operations, logistics, finance, legal, communications and media relations, and human resources, with some knowledge of how IT systems directly support the business. They will need to work with technical experts to answer several questions, including:

- What is the financial impact of the loss of a specific business system, application, or database?
- How can we run the business if we lose a specific business system, application, or database?
- How can personnel do their jobs without access to a specific business system, application, or database?
- What is the quickest way to bring affected business systems, applications, or databases back online, even if only in a limited capacity?
- For how long will affected business systems, applications, or databases be unavailable?
- What externally facing business systems or web applications are no longer available to the business? How long will these systems be unavailable?

Once a cyber incident or breach is detected, the primary focus for the CIBR team's IT and IT security members is to identify what happened and what devices — such as servers, laptops/desktop workstations, and mobile devices — were affected through computer forensics and investigation. This will enable the CIBR team to document clear causes, develop appropriate responses, and implement necessary repairs. The team can then develop and approve a recovery and restoration plan that can be quickly refined and actioned. If no internal computer forensics capability exists, an external resource should be identified and notified in a timely manner. The CIBR team will also need to identify resources that can support plan execution and event-driven responses.

Three Phases of Planning

Creating a CIBR plan can be accomplished in three phases.

In Phase I, an organization should develop its CIBR preparedness strategy, identify key CIBR stakeholders and team members, and outline team roles, external resources, and response guidelines.

Phase II adds the requisite details to the plan: the procedures, processes, CIBR team member roles and responsibilities, event tracking, and key decisions required of senior leadership as related to various types of cyber incidents and breach events. As organizations and teams become more skilled in handling cyber incidents and events, they can add more details to expedite response processes. The final result will be a set of standard operating procedures for dealing with specific types or groupings of cyber events that the CIBR team must respond to.

Phase II also helps establish key activity tracking for the CIBR team. The team will need to develop various forms and templates to support event information tracking. These include, for example, detailed contact lists of external partners and vendors that will provide support during a cyber incident or breach event.

Additionally, the team should identify what information related to a cyber incident or breach event would be of value to leadership and what response actions would require approvals before an incident or at the time it occurs. At the end of Phase II, the CIBR team should execute a cyber incident or breach event "dry run" to test whether the plan is complete, is effective, and meets the organization's needs.

Phase III culminates in the finalized CIBR plan. A key component of this phase is the execution of a detailed tabletop exercise with the participation of the CIBR team and senior leadership team to validate the plan. This exercise usually includes a technical component to help validate certain aspects of the CIBR plan. Further, it will expose senior leaders to the types of decisions they are likely to face during a real cyber incident or breach event.

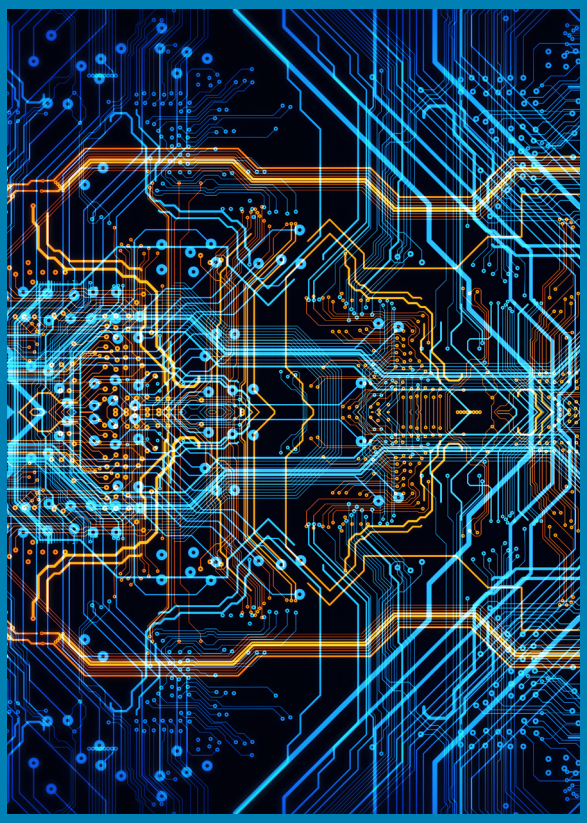
Following the tabletop exercise, organizations should conduct a formal review, during which all participants can discuss what happened, what went well, and what requires further improvement. This information should be captured in a lessons learned document that is used to refine and complete the CIBR plan for formal distribution.

Once completed, the CIBR team and senior leadership can engage in periodic exercises to remain proficient in handling cyber events. Scheduling a series of exercises, such as three in an 18-month period, allows the organization to develop exercises of increasing complexity or difficulty while also improving its ability to handle cyber incident and breach events.

Supporting Resources

In addition to the plan itself, CIBR team members can expedite their responses through supporting resources that should be made available or identified in advance. Examples of valuable supporting resources include:

- Experienced outside cyber legal counsel.
- Administrative support to help track CIBR event activities and key decisions for senior leadership.
- Cybersecurity technical, forensic, and analytical experts.
- Business operations experts who understand the organization's dependence on IT resources.
- IT recovery plan technical experts.
- Risk management and/or insurance experts who understand their policies and how to leverage them to support a crisis event when required.
- External vendor contracting/procurement experts to support onboarding of CIBR external support and/or materials procurement.
- Communications and media relations experts to develop cyber incident/breach event messaging.



With the threat of cyber-attacks constantly looming, it is imperative for organizations to develop an effective and efficient CIBR plan, which should become a key part of their enterprise cybersecurity programs. But the CIBR team's work doesn't stop there. A CIBR plan needs to be constantly reviewed and updated, with regular exercises held to continually refine and hone the plan through lessons learned. And in order to be effective, a CIBR plan must be part of an overall cyber resilience strategy and integrated with other crisis event plans to help companies be as prepared as possible when the next cyber incident or breach occurs.

The question that organizations should be asking themselves at this point is: When our next cyber incident or breach occurs, will we be ready?

For more information, visit marsh.com, contact your Marsh representative, or contact:

JIM HOLTZCLAW
Marsh Risk Consulting
+1 202 297 9351
james.holtzclaw@marsh.com