Business continuity management, security can work together to safeguard data

An interdisciplinary approach helps protect against and mitigate data breaches

Highlights

- Organizations that involve business continuity management teams in data breach planning and response can reduce the likelihood of data breach.
- Such involvement also reduces breach costs by an average of US$14 per compromised record.
- Business can also see a reduction in the mean time to detect a breach—from 234 to 178 days—and the mean time to contain a data breach, from 83 to 55 days.
- You can take five specific steps to help your organization begin coordinating business continuity management and security operations' breach response.

Organizations that involve their business continuity management teams in data breach planning and response can reduce the likelihood of data breach and lessen the cost and impact of any breach that should occur.[1] These and other compelling findings were uncovered in the 2015 Cost of Data Breach Study: Impact of Business Continuity Management, sponsored by IBM and conducted by the Ponemon Institute.

Ponemon has been charting the cost of data breaches for the last 10 years. In 2014, at IBM's request, Ponemon began examining the correlation between the cost of data breaches and business continuity management's (BCM's) involvement with cyber security teams in responding to them. This year, the study found that such involvement reduces breach costs by an average of US$14 per compromised record, from US$161 to US$147 (see Figure 1). Because data breaches can affect thousands of records, overall savings can be significant: BCM involvement can reduce the total cost of each data breach from US$3.8 million to US$3.5 million.

Identifying and containing a data breach quickly is instrumental to limiting its impact. The Ponemon study—which surveyed 350 companies operating in 16 industries across 12 countries—found BCM to be extremely helpful in this effort. In fact, for the first time this year, the study found that business continuity involvement can reduce the mean time to identify and contain a data breach. BCM involvement reduces the mean time to detect a breach from 234 to 178 days, and the mean time to contain a data breach from 83 to 55 days.

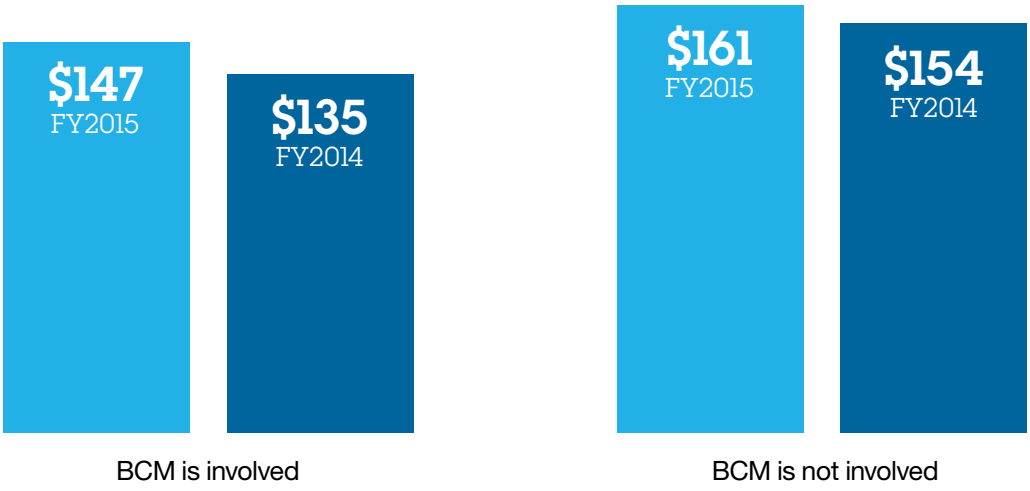

Figure 1. BCM involvement in data breach response can reduce the costs associated with each affected record to US$147 from US$161.

Perhaps most important, the study found that BCM involvement with security operations can actually reduce the likelihood of data breach. According to the Ponemon study, the likelihood of a data breach involving 10,000 or more records striking a company that involves BCM in security operations is 21.1 percent, compared to 27.9 percent for organizations that have no BCM involvement with security. And if a breach does occur, it will negatively affect the business operations of only 55 percent of organizations that involve BCM with security, compared to 80 percent of organizations with no such involvement.

Integrating security, BCM for breach prevention and mitigation

Clearly, BCM involvement with security operations can help limit the instances of data breach and mitigate the damage caused if a breach does occur. Organizations now understand this, and are finding ways to coordinate security and BCM response to breach. According to the Ponemon study, roughly 50 percent of the companies polled now have BCM involvement in data breach response planning and execution, up from 45 percent in 2014.

So how can your organization begin coordinating BCM and security operations' response to breach? IBM suggests the following five approaches.

1. Confirm your organization has a robust BCM program in place. As discussed earlier in this paper, the establishment and maintenance of a robust BCM program can help prevent a data breach, and mitigate the damage caused if a breach does occur. If your organization is unsure of the quality of your current BCM program, consider contacting IBM. The IBM Resiliency Services Framework model can help your organization examine BCM operations across seven zones of interdependent IT and business operations: business strategy and vision, organizations and people, processes, applications, data, and IT infrastructure and facilities. IBM Resiliency Services consultants use the framework to help your organization uncover weaknesses in BCM operations and chart a path to moving from your existing BCM state to your desired state.

2. Establish cross representation on business continuity and cyber security teams. Designated business continuity and cyber security specialists should work as members of each other's teams. Business continuity personnel, for example, should attend cyber security staff meetings and planning sessions, sharing business continuity information, processes and procedures as pertinent, and sitting on cyber security advisory councils as applicable. Business continuity professionals should also be part of data breach response teams. In some instances, organizations may even want to hire a staff Chief Information Security Officer to bridge the gap between continuity and security.

3. Conduct joint recovery testing. In disaster recovery testing, business continuity and cyber security should work together to identify actions that must be taken after a data breach, aligning their processes and procedures as closely as possible. Disaster simulations and preparedness exercises may prove particularly useful in helping cyber security determine which business continuity processes and information it can access in the wake of a data breach.

4. Appoint crisis management representatives to coordinate business continuity and cyber security efforts after a breach. Designate a single member of the business continuity team and a single member of the cyber recovery team to communicate during a data breach, to share information, make sure that appropriate remediation steps are being taken and coordinated, and to share information between disciplines, and, as appropriate, with the organization at large.

5. Identify needs and allocate budget. Continuity and security divisions should begin identifying what they need to more closely align procedures in the event of a data breach: databases may need to be reconfigured, as one example, or new procedures implemented for the re-routing of network traffic. These activities cost money. In addition, in implementing the approaches listed above, organizations may find that they need to hire additional continuity or security personnel, and find the cash to pay their salaries. IT budgets are always tight. However, organizations can use the Cost of Data Breach Study to begin building a persuasive business case for these additional funds.

While these approaches are helpful, to most effectively coordinate interdepartmental response, some organizations may want to work with a trusted technology provider—one with extensive experience melding business continuity and security operations in support of data protection and data breach-incident response. This is especially true for organizations at particular risk for breach or those with widely-dispersed operations

Why IBM?

IBM is an acknowledged market leader and innovator in the fields of data protection, data resiliency, and overall business resiliency. Our more than 6,600 IBM Resiliency Services professionals serve more than 10,500 clients. You can find our more than 300 Cloud Resiliency Centers in 68 countries around the globe. Specific services to help more closely integrate BCM and security include IBM Business Continuity Consulting, and IBM Business Continuity Management.

IBM Business Continuity Consulting services help organizations assess their risk postures, including their vulnerability to data breach, and determine how to improve data protection and breach response as part of an overall resiliency plan. Expert IBM consultants examine your organization's data protection and resiliency environment against industry best practices, governmental regulations and the environment's ability to meet overall corporate goals for security, continuity, availability and recovery. Additional consulting offerings help organizations design, plan, implement and test business resilience programs.

For organizations that would prefer IBM to manage their resiliency and security programs, IBM offers **Business Continuity Management** services. With these services, IBM acts as an extension of the customer organization's BCM department, managing resiliency and data protection solutions in whole or in part—depending on customer requirements—at either an IBM resiliency center or at site determined by the customer.

BCM involvement with data breach response can help organizations reduce the cost of the incident. IBM Business Continuity Consulting and IBM Business Continuity Management services can help your organization align continuity and security efforts to minimize or avoid data breaches, and to recover more quickly and effectively should they occur.

For more information

For more information on how IBM consulting and business continuity management services can help you protect your organization from data breach, visit the following web site: **ibm.com**/services/resiliency

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10504

Produced in the United States of America
July 2015

[1] All statistics are from the 2015 Cost of Data Breach Study: Impact of Business Continuity Management, Ponemon Institute LLC, 2015

Please Recycle

BUW03049-USEN-00