Business continuity helps reduce cost of data breach

Highlights

Data breaches are expensive and damaging to business reputation. The 2014 Cost of Data Breach Study, sponsored by IBM and conducted by Ponemon Institute, shows that risks and costs can be mitigated when business continuity and cyber security teams work in tandem to help an organization recover from a data breach. Approaches can include:

• Establishing cross-representation on business continuity and cyber security teams
• Conducting joint recovery testing
• Appointing crisis management representatives to coordinate business continuity and cyber security efforts after a breach

Business continuity and cyber security can work in tandem to limit damage

Attacks against data are becoming more prevalent, with hackers finding new ways to exploit networks, mobile devices and other technologies. Concurrently, the cost of data breaches is increasing. But there is some good news for those who want to limit the cost of these incidents: involving business continuity specialists in data breach response can help. This is the finding of the 2014 Cost of Data Breach Study: Impact of Business Continuity Management, sponsored by IBM and conducted by Ponemon Institute.

Ponemon Institute has been charting the cost of data breaches for the last nine years. This year, at IBM’s request, Ponemon began examining the correlation between the cost of data breaches and the involvement of business continuity organizations with cyber security teams in responding to them. The study found that such involvement can reduce costs by an average of $9 per compromised record, from $145 to $136. Because data breaches often affect thousands of records, the savings can be significant.

In addition, the Ponemon benchmark research—which studied 314 companies operating in 16 industries and 10 countries—found that business continuity involvement can actually help prevent breaches from occurring. Organizations that involve business continuity operations with cyber security activities are about five percent less likely to suffer a data breach than those organizations with no business continuity involvement (see Figure 1).
Likelihood of a material data breach for companies with or without business continuity involvement

<table>
<thead>
<tr>
<th>BCM is involved</th>
<th>BCM is not involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.3%</td>
<td>24.7%</td>
</tr>
</tbody>
</table>

Figure 1. Likelihood of a data breach drops when business continuity management (BCM) divisions are involved in cyber security operations.

Business continuity involvement can also help reduce interruption to business and IT processes and help protect organizational reputation. According to the study, 75 percent of companies that do not involve business continuity in data breach response suffer a disruption to business processes as a result of the breach, compared to 63 percent that do involve business continuity. Sixty-seven percent of companies that do not involve business continuity in incident response experience a disruption of IT operations, compared to 57 percent of companies that do involve business continuity. Finally, in the all-important arena of business reputation, only 49 percent of companies that involve business continuity in data breach response reported damage to business reputation as a result of the breach, compared to 58 percent without business continuity involvement (see Figure 2).

To limit the costs of data breaches and to protect organizations against the harm they can inflict, organizations should involve business continuity professionals in their cyber security incident response. However, that involvement occurs too infrequently: 55 percent of the organizations studied said that business continuity management is either not involved or only informally involved in data breach response.

Rates of negative impact to business reputation for companies with or without business continuity involvement

<table>
<thead>
<tr>
<th>BCM is involved</th>
<th>BCM is not involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>49%</td>
<td>58%</td>
</tr>
</tbody>
</table>

Figure 2. Business continuity involvement with security breaches can help reduce damage to business reputation.

Why does business continuity involvement help?

The 2014 Cost of Data Breach Study does not address why business continuity involvement in the remediation of data breaches helps limit their severity. However, based on our experience aiding organizations throughout the world with their continuity and security needs, IBM has seen that continuity operations’ maturity, reach and traditional role in data protection can be useful to cyber security divisions.

Business continuity operations almost always predate cyber security. As the more mature organization, business continuity divisions have often proactively developed rigorous processes for preventing and mitigating events likely to cause business disruption. These can include, for example, processes to protect data from loss or contamination, shift business-critical workloads to backup facilities should equipment fail, and quickly restore data once the recovered resources
come online. As a newer organization, cyber security may not have tested processes in place, but can leverage business continuity's processes in times of data breach.

Business continuity organizations typically have a broader reach than cyber security, working with many corporate divisions to plan for and recover from business disruptions as quickly as possible. Cyber security operations are often siloed: outsiders cannot be allowed to know the nature of the corporation's IT vulnerabilities. However, this isolation can stymie recovery from a data breach, which often requires cross-organizational involvement. Suppose network traffic has to be rerouted as the result of a breach. Often, the cyber security specialists responsible for containing the breach are not the same people who can reroute network traffic. Worse, they may not even know who to call to have the traffic rerouted.

Alternatively, business continuity involvement with cyber security often helps enable a faster and more complete recovery from data breaches because business continuity has historically taken charge of protecting, backing up and restoring data. In a business environment where mobility and cloud computing have fostered the expectation of 24x7 data access, containing and remediating a data breach is only half the battle: data must then be made usable again as quickly as is safely possible. Since business continuity is charged with this task, its involvement with cyber security can help speed the resumption of normal data access and the business processes that depend on it.

How to involve business continuity with cyber security
What's the best way to get business continuity and cyber security teams working together to mitigate the damage caused by data breaches? IBM suggests the following four approaches.

1. 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.

2. 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.

3. 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, make sure that appropriate remediation steps are being taken and coordinated, and share information between disciplines as well as with the organization at large.

4. Identify needs and push for a bigger 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 rerouting 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 funding to pay their salaries. IT budgets are always tight. However, organizations can use the 2014 Cost of Data Breach Study to begin building a persuasive business case for these additional funds.
Why IBM?
Data breaches are expensive and damaging to business reputation. These risks can be mitigated when business continuity and cyber security professionals work in tandem to help an organization recover from data breach. IBM offers services to help bridge the gap between continuity and security. IBM Business Continuity and Resiliency Services is an acknowledged market leader and innovator in the field. We have more than 1,800 continuity and resiliency professionals supporting 9,000 clients worldwide. Our portfolio of continuity and resiliency services combines consulting and management expertise with cutting-edge technological innovation. IBM Security Services offers a host of services to protect data, systems and applications. Our continuity and security services can be combined to help your organization align efforts to minimize or avoid data breaches and to recover more quickly and effectively should they occur.

For more information
For more information on IBM Business Continuity and Resiliency Services and IBM Security Services, visit the following websites:

ibm.com/services/continuity
ibm.com/services/security

Sources