IBM Global Technology Services

Resiliency
Services

Business continuity management can help your organization improve cyber resiliency

Resiliency orchestration, automation help fight against cyber attacks

IBM

The average data breach now affects about 24,000 records and costs more than USD 3.6 million to remediate.[1] This is according to the *2017 Cost of Data Breach Study: Impact of Business Continuity Management*. The study, independently conducted by the Ponemon Institute and sponsored by IBM, examined companies that have experienced a data breach affecting between 2,600 and 100,000 records. Hackers and criminals—both inside and outside the organization—cause 47 percent of all data breaches worldwide. In the United States that figure jumps to 52 percent.[2] System glitches and human error account for the rest (see Figure 1).

"Instances of malicious data breach will only increase," said Dr. Larry Ponemon, chairman of Ponemon Institute. Complex IT systems, the Internet of Things, and mobile access to corporate data and apps present hackers with new attack pathways. In addition, the need to store ever-increasing amounts of information leads to imprecise data-classification schema. Companies can't appropriately secure sensitive information if they don't know where to find it.

About the study

Who? The *2017 Cost of Data Breach Study: Impact of Business Continuity Management* examined 419 companies that had previously experienced a data breach affecting between 2,600 and 100,000 records.

Where? The companies are located in 13 countries and regions across North America, South America, Europe, Africa and Asia.

What industries? These companies operate in 17 industries—from financial services and transportation to hospitality and entertainment

Ponemon

2017 Cost of Data Breach Study

Impact of Business Continuity Management

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
June 2017

Ponemon Institute© Research Report

IBM

To learn more about the companies surveyed, download the study.

Malicious data breaches have already proven more expensive to resolve than system glitches or human error, and upcoming regulations are expected to increase that cost. According to the study, malicious data breaches around the globe cost an average of USD 156 per record to correct. This is roughly 22 percent more than the USD 128 per-record cost associated with data breaches caused by system glitches, and 24 percent higher than the USD 126 cost per record incurred in data breaches caused by human error. (Throughout this paper, the costs of data breach have been converted from local currencies to US dollars.) Concurrently, new data protection regulations worldwide levy increasingly severe fines. The European Union General Data Protection Regulation is an example. The law, slated to go into effect in 2018, calls for data breach fines of up to EUR 20 million.

At this critical juncture, IBM believes it is vitally important for business continuity management (BCM) to work closely with cybersecurity teams to form *cyber-resilient* organizations. IBM defines these as organizations that combine business continuity, information security and organizational resilience efforts to help prepare for, protect against, detect, respond to, and recover from cyber attacks. Effective cyber resilience programs also help companies more quickly return to normal operations after a disruptive event.

BCM involvement with data breach planning and response leads to

16.2% reduction in the total cost of data breach

"Our recent study on the financial consequences of a data breach found that companies that deploy resiliency orchestration and automation realize a significant economic savings when compared to organizations that rely primarily on manual procedures," Ponemon said. "The results of this study and our earlier studies consistently demonstrate the cost of data breaches and security exploits can be moderated by applying resiliency orchestration and automation in the business continuity management ecosystem."

The rest of this paper will discuss study findings. It will also examine the benefits of BCM teaming with cybersecurity in data breach response and discuss how to build a cyber-resilient enterprise.

Root causes of data breach

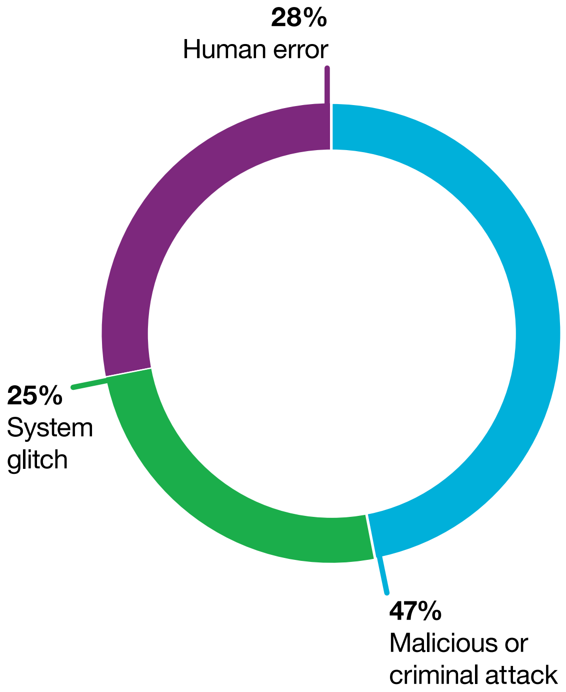

Figure 1: Malicious and criminal attacks are the single largest cause of data breach.

Reducing the impact of data breach

The study demonstrates how involving BCM with cybersecurity in data breach response planning, and in the response itself, reduces the mean time to identify and contain a data breach, and the likelihood of suffering an additional data breach in the next two years. In doing so, such involvement decreases the cost of data breach.

Organizations recognize the value of this teamwork. In 54 percent of the companies surveyed, BCM professionals work with cybersecurity, enterprise risk management and crisis management teams to prevent and resolve data breaches. Of those companies that team BCM and cybersecurity, 95 percent rate BCM involvement as either "significant" or "very significant." BCM professionals may advise the data breach incident management team, serve as a member of the team, or even lead it.

The Ponemon study demonstrates the value BCM professionals bring to the incident response team: data breaches cost less to remediate when BCM is involved. According to the study, companies that involve BCM teams in data breach planning and response spend an average of USD 3.35 million to remediate the data breach, a nearly 15 percent decrease from the USD 3.94 million spent by those organizations that do not involve BCM. Business continuity management involvement also reduces the costs associated with each compromised record from USD 152 to USD 130. BCM involvement also helps reduce the time needed to detect and contain a data breach (see Figure 2).

Saving time with BCM involvement

How long does it take to detect and contain a data breach?

With BCM involvement:

Identify: 171 days	Contain: Additional 50 days	Total: 221 Days

Without BCM involvement:

Identify: 214 days	Contain: Additional 65 days	Total: 299 Days

Figure 2: Organizations that involve BCM in data breach planning and response take 78 days less to identify and contain a data breach than companies without BCM involvement.

In the always-on era, companies must avoid business disruption caused by data breaches and other events. Here again, BCM involvement can help. Only 55 percent of companies that involved BCM in data breach response suffered a material disruption to business operations because of the data breach, compared to 76 percent of companies without BCM involvement.

Of course, one way to minimize business disruption caused by data breach is to implement plans that reduce the risk of your data being breached. Companies with BCM involvement in data breach planning and response have only a 23.9 percent likelihood of suffering another data breach in the next two years, compared to 31.8 percent for those companies without BCM involvement.

BCM involvement with data breach planning and response leads to

USD 10.90 reduction in per-record cost of data breach

The value of cyber resiliency

Because hacking and insider criminal activity constitute the single most significant source of data breach, it is imperative that BCM work with cybersecurity divisions to help the entire organization grow more cyber resilient—or better able to prepare for, protect against, detect, respond to, and recover from cyber attacks. BCM can help accomplish this by:

- Establishing a structure that reduces the complexity of incident response processes
- Creating an orientation toward rigorous planning and testing
- Enabling upstream and downstream communications during times of data breach or other crisis
- Advancing a culture that embraces monitoring and vigilance

Make no mistake: most organizations will need this help to grow more cyber resilient. In the *Second Annual Study on the Cyber Resilient Organization*, a 2016 report independently conducted by the Ponemon Institute and sponsored by IBM® Resilient®, only 32 percent of the 2,000 IT and security professionals surveyed said their organizations had a high level of cyber resilience—down from 35 percent in 2015. Nearly two-thirds reported that their organizations felt unprepared to recover from cyber attacks. This at a time when emerging and disruptive technologies provide hackers with new attack points through which to exploit system vulnerabilities.

So how can BCM organizations work with cybersecurity to improve an organization's cyber resilience? From its more than 50 years' experience in business continuity, IBM suggests the following tactics.

BCM involvement with data breach planning and response leads to

43-day reduction in the mean time to identify a data breach

Implement resiliency orchestration and automation tools to improve data breach response.

According to the study, DR automation and resiliency orchestration reduce the daily cost of data breach by roughly 33 percent, from USD 5,015 for those companies that use only manual DR processes to USD 3,360 for organizations that have implemented DR automation and resiliency orchestration techniques (see Figure 3). Pre-packaged software tools can help automate workflows in the data- and application-recovery process. Automated workflows help limit human error and reduce the need for human expertise. Resiliency orchestration and automation capabilities should cover apps and data stored in on-premises data centers, public clouds and private clouds.

Deploy communications technologies that enable a faster response to data breaches and other disruptive events.

Implement technologies that can help automate and streamline communications during a data breach or other crisis. These technologies can engage the right people to manage a specific disruptive event. They can also improve and automate mission-critical communications through multiple internal and external channels. The best of these technologies provides real-time incident status reports and automated activity tracking.

Resiliency orchestration demo

Want to learn more about how resiliency orchestration and automation can help improve DR?

[Watch the demo.]

Streamlining communications

Streamlined, automated communications flows are more important during times of crisis than at any other.

Learn more about automating communications with this demo.

Automating and orchestrating DR significantly reduces the cost of data breach

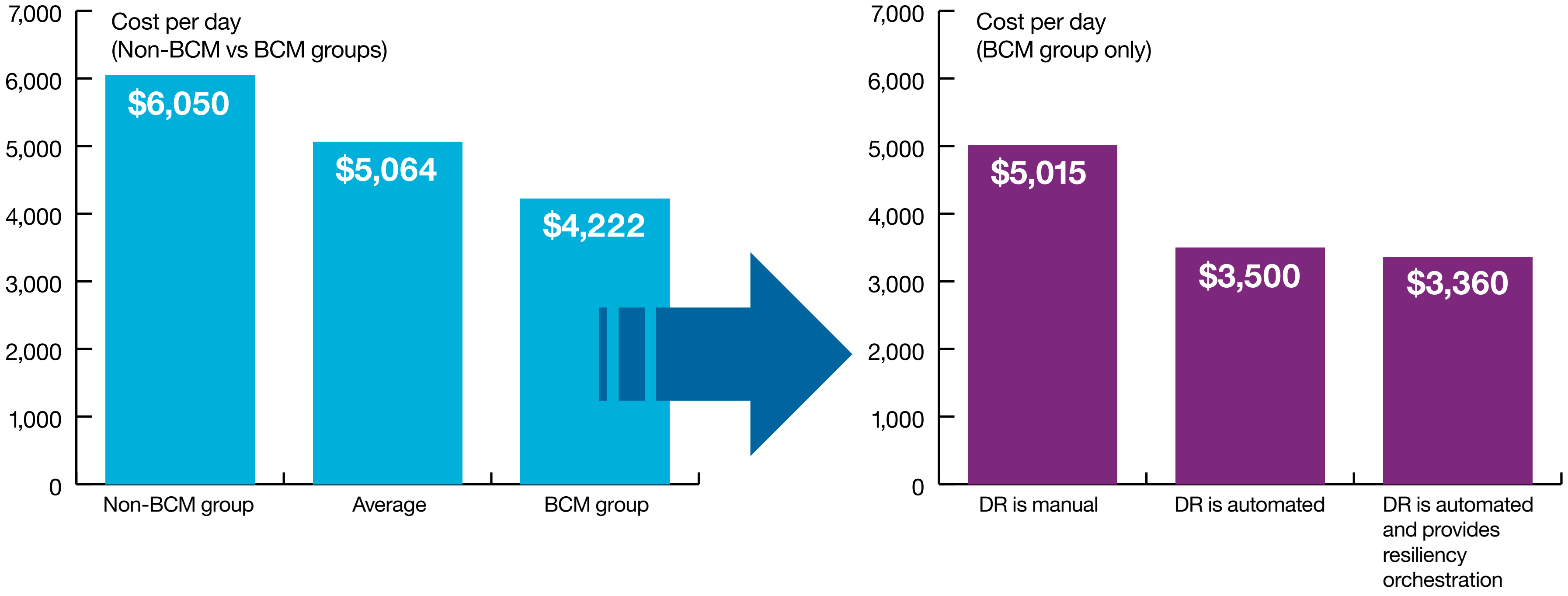

Figure 3: Companies that utilize DR automation and resiliency orchestration can significantly reduce the daily cost of data breach compared to companies with no BCM involvement in DR.

Protect critical data.

Retain secured copies of mission-critical data that can replace breached or corrupted information. This can be accomplished through security-rich, scalable cloud backup tailored to the needs of your organization. Organizations may also consider additional tape- and disk-based backup as necessary.

Evaluate your backup capabilities

Unsure of the efficacy of your current backup?

Evaluate it with the IBM Resiliency Backup as a Service evaluation tool.

BCM involvement with data breach planning and response leads to

28.4% decrease in the likelihood of a data breach over the next two years

Why IBM?

Through thousands of resiliency and security engagements worldwide, IBM Resiliency Services™ has developed repeatable methodologies and cutting-edge technologies to help keep data safe and mitigate the effects of any data breach that does occur. Specific services to help organizations more closely integrate BCM and cyber resiliency with cybersecurity include:

- IBM Cloud Resiliency Orchestration
- IBM Resiliency Communications as a Service
- IBM Resiliency Backup as a Service

IBM Cloud Resiliency Orchestration is an orchestrated disaster recovery solution that helps organizations automate response to data breaches or other disruptive events. This solution has been developed for hybrid IT environments and addresses the security and resiliency needs and interdependencies of those environments. The solution offers a single dashboard through which IT professionals can conduct a number of DR tasks. The dashboard allows DR professionals to monitor application and recovery groups, test and execute switchover and switchback, generate reports, monitor metrics and otherwise simplify recovery. The dashboard also provides users with a real-time snapshot of applications, noting which are DR ready and which are actively providing services from a DR site. Recovery point objective and data lag meters show which are meeting, or failing to meet, recovery goals. Delivery models include IBM BlueMix® and Amazon Web Services cloud offerings.

Data breach costs by industry

Data breach costs vary by industry. The average cost of data breach per compromised record is USD 380 in the healthcare industry and USD 245 in financial services. At the other end of the spectrum, per-record costs in the media industry run only USD 119, in the public sector, USD 71.

IBM Resiliency Communications as a Service is a high-availability, cloud-enabled incident management service. It streamlines crisis communications by helping organizations automatically engage the right person at the right time for the right recovery job. The solution's capabilities include rapid-response prompts, real-time incident status reporting, advanced one-on-one and team communications capabilities and automated activity tracking.

IBM Resiliency Communications as a Service offers multiple incident form types that organizations can use to capture data about a breach or other disruption. This data is used to automatically trigger other communications workflows. Templates can even help companies generate press releases and other communications with the general public. This solution also incorporates events from The Weather Company to provide organizations with accurate early warning of developing weather events, then help companies proactively respond to those events.

IBM Resiliency Backup as a Service is a cloud solution providing security-rich, scalable backup of critical data. It allows organizations to choose from a menu of cloud backup options, leveraging a mix of public, private and hybrid cloud delivery models to meet specific business needs. Delivery models include IBM Bluemix and Amazon Web Services cloud offerings.

BCM and cybersecurity must work together to help make their organizations more cyber resilient. In doing so, they can help mitigate the risk of data breach and reduce the duration and cost of any incursions. IBM offers cutting-edge solutions to help organizations with this process.

Learn more

For more information on how IBM Resiliency Services can help you protect your organization from data breach, visit our website: ibm.com/services/resiliency

IBM Corporation
IBM Global Technology Services
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
August 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♻ Please Recycle

[1] Unless otherwise noted, all statistics are from the 2017 Cost of Data Breach Study: Impact of Business Continuity Management, Ponemon Institute LLC, 2017.

[2] Second Annual Study on the Cyber Resilient Organization, Ponemon Institute LLC, 2016