A SINGLE SECURITY BREACH can cause shareholders to scurry, IT teams to scramble, and systems to crash. But no greater is the disruption than to customer trust.

According to an IDG Research study, 64% of survey respondents cite loss of customer confidence as their biggest concern in the event of a security breach.

The reasons are clear: Companies count on customers to feel comfortable sharing their personal information, from credit card numbers to email addresses. For shoppers, disclosing personal details is an opportunity to make online purchases, participate in loyalty programs, and schedule home deliveries. But for organizations, these bits and bytes are a competitive advantage – pieces of the puzzle that help shape customer service, product development, and growth. When a data breach occurs, consumer confidence plummets. And any loss of consumer confidence can equal a loss of revenue.

Consumers aren’t the only ones driving greater attention to data security. Thanks to social media channels, reports of cyberattacks now spread like wildfire, providing organizations with little time for damage control. At the same time, regulators and auditing bodies are upping the ante on how financial services, healthcare and legal companies store and secure their confidential data.

Prevention isn’t enough
Confronted with this perfect storm of pressures, many organizations have preventative measures in place to safeguard against security breaches. Sixty-five percent of survey respondents count reinforcing identity and access management controls as one of their top five data protection priorities over the next 12 months. And 62% say they conduct regular cybersecurity maintenance.

Yet there’s a disconnect between threat perception and threat preparedness. More than half (59%) of respondents say their approach to data protection and minimizing risk is focused on proactive/preventative measures, whereas 41% of respondents expressed a focus on reactive measures.

Despite the importance of a proactive stance, a two-pronged approach that includes both preventative and restorative measures is the secret to a truly secure organization. Reactive and resolution-oriented security measures must be part of a complete security strategy.

Consider, for example, ransomware. Ransomware works by preventing companies from accessing their data unless a ransom is paid. Often large amounts of money are demanded to restore these critical files. But not if a company has already taken restorative measures. By creating redundant versions of data, and backing up applications offsite securely, organizations can effectively manage a ransomware scenario and even prevent the need to pay out any ransom at all.

IT teams and senior-level executives alike are waking up to the value of this two-pronged approach to data security. In today’s digital age, the connection between data security and business

SPONSORED BY:

bluelock.
continuity deepens. Service disruptions caused by a malware attack are not only an IT nuisance, but a precursor to a tarnished brand and legal liabilities.

Recognizing the business imperative of security, senior-level executives are focused on recovery in the event of a security breach and recognize the need to get back to a steady state quickly and efficiently. In fact, nearly half (44%) of VPs say the inability to recover data and systems in less than a day is one of their biggest concerns in the event of a security event.

The time is now
Fortunately, it’s not too late to make disaster recovery a key component of your security strategy. Currently, 41% of survey respondents say their approach to data protection and minimizing risk is focused on reactive/restorative measures. And the majority – 64% of respondents – say they believe that disaster recovery should be incorporated into an IT security strategy.

One way of emboldening a security stance and adopting a two-pronged approach, is by implementing Disaster-Recovery-as-a-Service (DRaaS). This modern technology tool replicates systems and data to an offsite secure disaster recovery site. Regardless of an IT environment’s complexity, DRaaS matches an organization’s systems and data to recovery solutions based on recovery objective tiers and technical platform types.

Key features include regular testing capabilities to ensure systems stay in sync to support a successful recovery. Although self-service solutions are available, managed DRaaS allows companies to tap into the expertise and methodology of teams that tackle restorative challenges on a daily basis. And because no two IT teams are built the same, managed service options can be aligned with the level of a company’s in-house expertise and capacity.

Access to these varying levels of support across the lifecycle of DR management – from implementation and steady state to testing and recovery event management – is ideal for overburdened IT teams. In the past, DR initiatives often entailed replicating data to depreciated assets that may – or may not – fully recover in the event of a security breach. Other past obstacles included the time-consuming task of managing a second site or multiple sites.

However, with replication into the cloud, DRaaS eliminates the need to manage capacity and infrastructure at a second production site, thereby freeing IT teams to focus on more business-critical tasks.

Getting started
It’s easy to embark on a two-pronged approach to data security. Before deploying DRaaS, perform an analysis of the business to identify vulnerabilities and prioritize assets requiring the greatest degree of protection.

Also, keep an open dialogue between IT teams and other business units. This is critical to examining which security and recovery options make the most sense for an organization’s unique characteristics.

Following this, companies can begin taking the necessary steps to predictably restore and run services from their backups and replicated data in the cloud.

A win-win result
Security breaches are multiplying, posing a serious threat to customer confidence and business continuity. Proactive measures are a must, but the time is ripe for organizations to pay more heed to restorative and results-oriented security solutions.

DRaaS can salvage customer confidence in the event of a security breach by quickly getting systems back up and running. With a strong, responsive stance in place, organizations can minimize risk exposure and eliminate the headaches of capacity management, all while taking advantage of the economies of the cloud.