CrashPlan™

How to build data resiliency that works for (and with) real people

Introduction

When it comes to business resiliency and data protection, prevention can only go so far. Despite the greatest security efforts, businesses still need technology tools that accommodate humans and provide a solid backup plan to get back up as swiftly as possible when compromised. Even with essential tools in place – like EDR (Endpoint Detection & Response) — preventative measures cannot 100% account for natural human behavior.

In this guide, we'll define and discuss what business resiliency means for data, how to balance data loss prevention with human unpredictability, and practical steps to achieving holistic resiliency. We'll also outline some reasonable steps to take immediately and provide fuel for thought as you embark on your resiliency and backup security journey.

Reimagining Resiliency

Resiliency is a word often heard lately in a business context, but it's also something we have all experienced directly in our personal lives. Throughout our lives, people have figured out how to keep moving through adverse situations. We've learned that there's usually an easy way to do things and a complicated way to do things. The same reality applies to businesses. Companies must think about protecting themselves while also embracing the easy ways of doing things – particularly when critical data is at stake. The resiliency of a business hinges on the intersection of technological tools and human behavior. And one key step in understanding where these two forces overlap is understanding how data gets lost in the first place.

© Copyright CrashPlan 2023 | crashplan.com

The Different Reasons Behind Data Loss

It's not *if* data loss will happen, but when it inevitably happens. While technological measures and security systems are essential, human and natural factors still contribute significantly to data loss incidents.

Human Error

Human error is one of the primary causes of data loss. It occurs when end-users accidentally delete or overwrite data, mishandle storage devices, or make mistakes during data transfers or backups. In addition, factors such as fatigue, distraction, lack of awareness, or inadequate training can be key contributors. Researchers from Stanford University found that approximately 88% of all data breaches are caused by human mistakes.

Lack of Security Awareness

Many data breaches occur due to a need for more security awareness among employees. Some examples include falling victim to social engineering attacks such as phishing scams, using weak passwords, sharing sensitive information without proper encryption, and neglecting security protocols.

Natural Disasters

Natural disasters such as fires, floods, earthquakes, or storms physically damage infrastructure and storage devices, which leads to data loss. The destruction of data centers or the loss of physical storage media can permanently lose critical data if offsite backups or disaster recovery plans are inadequate or not implemented.

Data loss incidents have far-reaching consequences for humans and organizations, impacting their finances, operations, reputation, legal standing, and overall well-being. Some critical repercussions include:

Financial Loss

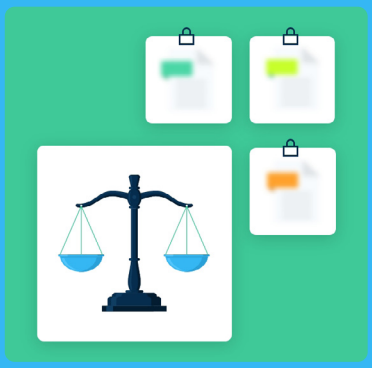
Data loss can result in financial ramifications for individuals and companies. For businesses, the cost of recovering or recreating lost data, restoring systems, and addressing the aftermath of an incident can be substantial. The average cost of a single ransomware attack is $4.54 million. Additionally, there can be legal consequences, fines, or penalties for non-compliance with data protection regulations. For individuals, data loss leads to financial identity theft, loss of personal assets, or fraudulent activities, resulting in financial hardship.

Operational Disruption

Data loss throws normal business operations into chaos, leading to downtime and reduced productivity. Companies may experience temporary or prolonged service interruptions, inability to access critical information, delays in decision-making processes, and loss of customer trust. Operational disruptions have cascading effects on various departments, partners, and stakeholders, impacting revenue generation, customer satisfaction, and overall business performance.

Legal Consequences

Data loss can also lead to legal and regulatory consequences. Organizations may face lawsuits from affected individuals or regulatory bodies for failing to protect sensitive information or comply with data protection regulations. Legal battles can result in costly settlements, damage to the company's image, and potential long-term legal implications.



These consequences underscore the critical importance of implementing robust data protection measures, disaster recovery plans, and comprehensive data resiliency strategies to minimize the risks and mitigate the impacts of data loss incidents.

Rethinking Compliance

Only 10% of IT users conduct daily backups. Integrating a data backup policy into day-to-day practices is vital for data protection, business resilience, regulatory compliance, and risk mitigation. But when backup policies are designed to put the burden of compliance too much on the end user, organizations set themselves up to fail. That's because no matter how well-intentioned employees are, their primary goal at work is to get their job done. When shortcuts, misunderstandings of policy, or simple thoughtlessness occur, data is vulnerable to loss. The business can point the finger at non-compliant employees, but the end result is still data loss and all the ramifications that accompany it.

It's time to make it as easy as possible for employees to comply with policies. That means setting up tools and processes that don't rely too much on the end user. Automation and centralized administration of tools are great strategies for human-proofing your organizational data. Use tech as a complement to your workforce rather than a barrier.

There's more data at the endpoint than you think

The endpoint is where work happens. Yes, that will often entail interacting with a CRM or other structured data storage solution however, invariably, work is stored locally. Whether it's a designer using an illustration program, a copywriter interacting with a text document or just good old-fashioned local software development, users store data on their endpoints without thinking about it twice. Regardless of the business you find yourself in, there are users in your organization (likely most of them) who do not religiously follow established data storage practices and policies because they would rather be doing their jobs than worrying about data governance.

Not backing up endpoint data will have serious consequences. When hardware fails, a cyber-attack lands, or accidental deletions occur the data that your users innocently or unknowingly stored on their devices will be lost. This will either lead to lost productivity due to a need for the user(s) impacted to recreate everything which was lost, or in the case of a larger incident could be an unrecoverable loss for the business. Establishing regular and secure endpoint data backups is vital for maintaining smooth operations, safeguarding user productivity and contributing to the corporate bottom line.

© Copyright CrashPlan 2023 | crashplan.com

Humanizing Technology

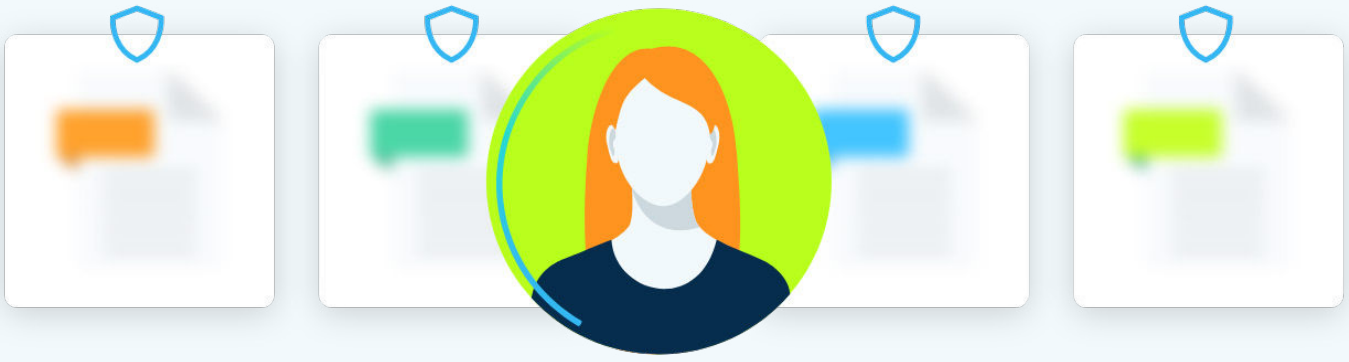
By considering the human context and taking a user-centric approach, organizations can successfully implement technical solutions that close many of the gaps where user error or neglect can occur, greatly reducing the chance of data loss. Aligning with users' needs and seamlessly integrating into their existing workflows increases user acceptance, productivity, and the overall effectiveness of the technology implementation.

Case Study

One of the world's largest independently owned advertising agencies needed to strengthen its ransomware and proprietary data protection processes. Their on-prem process relied on third-party solutions that were slow to respond and provided inaccurate data that was out-of-sync with their needs — resulting in a higher potential for end-user data gaps and non-compliant processes.

By working with a cloud-based end-user backup and recovery solution, they created a more efficient way to automatically collect and preserve user-created data in a centralized and secure location.

Through having a dedicated enterprise solution that supported legal hold backup, recovery, and device migration, the agency's workflow was optimized with an automated backup system that worked as a conduit for the agency's IT team to quickly and easily restore people's data, upgrade their machines, and work remotely in a fully decentralized setting.



10 Essential Steps to Establishing Data Resiliency

Let's walk through an overview of the essential steps to achieving a more resilient organization.

1	**Conduct a data resiliency assessment**	Start by assessing your current data infrastructure, systems, and processes to identify vulnerabilities and potential points of failure. Next, evaluate your existing data protection and recovery mechanisms, security measures, and disaster recovery plans.
2	**Define data resiliency requirements**	Clearly define your data resiliency requirements based on what is critical to your business operations. Next, determine the desired data availability, integrity, and recoverability level, considering data criticality, compliance requirements, and business impact.
3	**Develop a data resiliency strategy**	Create a comprehensive strategy that outlines the specific actions and measures needed to achieve your data resiliency goals. This strategy should address data backup and recovery, security, disaster recovery planning, and cloud or hybrid solutions.
4	**Implement robust data backup and recovery mechanisms**	Establish regular and automated data backup processes, ensuring backups are performed consistently and stored securely. Consider adopting a combination of on-site and offsite backups, leveraging technologies such as snapshots, replication, and incremental backups.
5	**Enhance data security measures**	Implement robust data security measures, including access controls, encryption, data classification, and monitoring systems. Regularly update security software and patches to protect against evolving threats. Train employees on best data security practices and establish incident response and breach management protocols.

© Copyright CrashPlan 2023 | crashplan.com

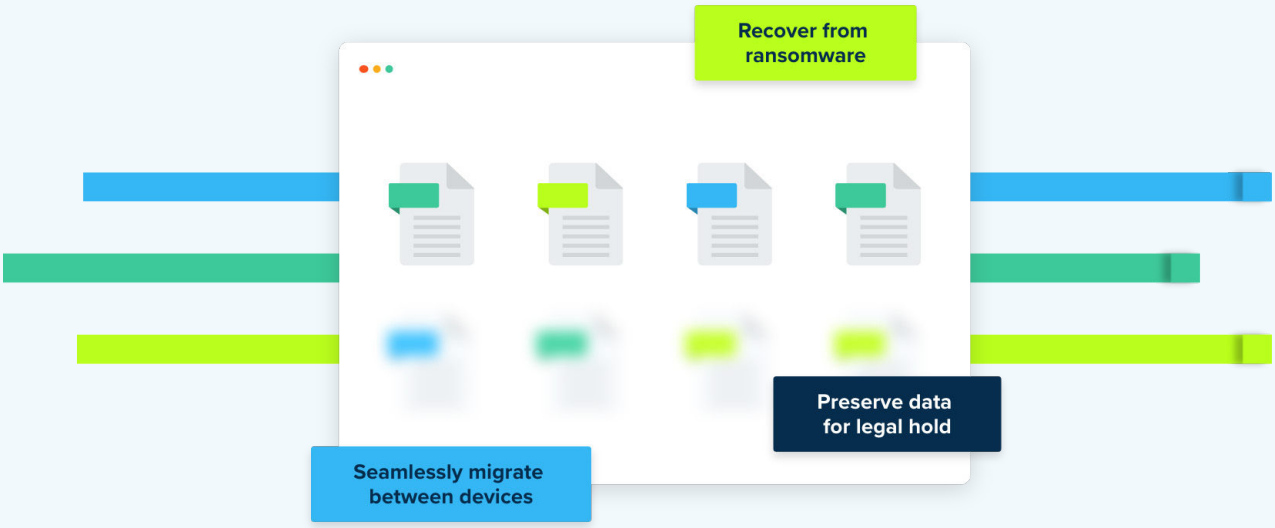
6	**Develop a disaster recovery plan**	Create a well-defined and tested disaster recovery plan that outlines the steps to prevent data loss or system failure in the event of a disaster. This plan should include roles, responsibilities, communication protocols, backup restoration procedures, and alternative infrastructure options. Organizations that have plans in place and regularly test them save an average of $2.66 million.
7	**Leverage cloud and hybrid solutions**	Explore using cloud-based or hybrid data storage, backup, and computing solutions to enhance data resiliency. Cloud platforms often offer built-in redundancy, scalability, and automated backup and recovery capabilities. Evaluate the suitability of cloud providers based on their security measures, compliance certifications, and data availability guarantees.
8	**Establish data resiliency policies and procedures**	Develop and communicate clear policies and procedures for data resiliency throughout the organization. This includes data handling, retention, disposal, and incident reporting guidelines. Regularly review and update these policies to reflect changing technology landscapes and compliance requirements.
9	**Train employees and foster a resilient data culture**	Provide comprehensive training to employees regarding data resiliency best practices, security protocols, and their roles in maintaining data integrity. Foster a culture of data resiliency by promoting awareness, accountability, and continuous improvement. Encourage employees to report vulnerabilities, incidents, and near-misses.
10	**Regularly test and audit data resiliency measures**	Conduct regular testing, simulation exercises, and audits to validate the effectiveness of your data resiliency measures. Test backup restoration processes, disaster recovery plans, and security controls to identify and address weaknesses promptly.

© Copyright CrashPlan 2023 | crashplan.com

Conclusion

When it comes to organizational data resiliency, policies alone cannot out-engineer a human – so the best way to set yourself up for success is to set up systems that accommodate and account for natural human behavior. There are an abundance of tools geared toward prevention of data loss, and it makes sense to utilize them, but ultimately there will be situations where adversaries or disasters break through your defenses. When that happens, will you be ready with a recovery plan that gets you back up and running without losing critical data?

With CrashPlan's automatic, end-to-end encrypted cloud endpoint backup, you don't have to rely on fallible but well-intentioned end users to follow backup policies. So when prevention efforts aren't quite enough, you'll be able to recover your data quickly and easily. Learn more at crashplan.com



CrashPlan™

crashplan.com

CrashPlan® enables organizational resilience through secure, scalable, and straightforward endpoint data backup. With automatic backup and customizable file version retention, you can bounce back from any data calamity. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds. So you can work fearlessly and grow confidently.

For more information, visit **crashplan.com**.

© 2023 CrashPlan Group LLC. All rights reserved. Crash Plan, and the CrashPlan logo are registered trademarks or trademarks of CrashPlan Group LLC. in the United States and/or other countries. All other marks are properties of their respective owners.