

THE CASE FOR MODERNIZING YOUR DATA PROTECTION STRATEGY IN 2014

Cyberattacks are on the rise—and so are temperatures, which can increase the risk of natural disasters. Get the scoop on these and other challenges to your data protection strategies.

CONTENTS:

- Increased cybercrime
 - Increased impact from natural, accidental and man-made disasters
 - Malicious attacks
 - Increased infrastructure complexity
 - Increased BYOD
 - Increased security and privacy regulations:
- The modern era is a time of constant change and challenge for IT professionals:
- Everyone expects uninterrupted access to data, no matter what.
 - E-commerce and social media create landslides of new data that must be housed, analyzed and, in some cases, protected.
 - Storage requirements are doubling at regular intervals.
 - Virtualization technologies help streamline management and cut costs, but they also put an organization's technological assets all in one place so they're more vulnerable to disaster and outage.
 - Ever-increasing compliance regulations require organizations to constantly ratchet up privacy and security parameters or face stiff fines.

There's never been a more compelling case to modernize your data protection strategy. Read on to learn more about the biggest threats to data in 2014, and consider how your current data protection strategy addresses them.

Increased cybercrime: According to the 2013 US State of Cybercrime Survey, "cyberattacks are now a routine part of doing business in today's uncertain world, and they likely will be a part of doing business going forward."¹ This report, as well as statements

¹ "Key findings from the 2013 US State of Cybercrime Survey," PricewaterhouseCoopers LLP, June 2013



from thought leaders who specialize in studying cybercrime, suggests that most organizations don't fully comprehend the nature of whom and what they're up against. In fact, this survey and others show that most companies are severely underprepared for the sophisticated nature of modern cyberthreats. The good news is, most cyberattacks target weaknesses in an organization's internal infrastructure. With education, monitoring and a well-maintained infrastructure, security experts agree that 80% of cybercrime can be thwarted.²

Increased impact from natural, accidental and man-made disasters: Statistically, natural disasters aren't on the rise. However, Earth Observatory, a part of NASA, states that higher global temperatures are likely to increase the intensity of storms.³ A recent study from Tulane University suggests that the impacts of natural disasters are increasing because more people and businesses are moving to geographic areas with higher disaster risks. Additionally, some formerly stable geographic areas are becoming less stable due to development and deforestation. Threats from accidental disasters include pandemic, blackouts and nuclear leaks. Though accidental and natural disasters aren't increasing, denser populations, proximity to coastal areas and increased dependence on technologies and supply chains mean human and business vulnerability to disaster are on the rise.

Malicious attacks: The Federal Emergency Management Agency states that "recent technological advances and ongoing political unrest are components of the increased risk to national security."⁴ The terrorism landscape is complex, and businesses must be ready to persevere in the face of increasing unrest.

Whether man-made, accidental or natural, disasters don't have to destroy your business. A solid data protection strategy will protect your digital assets and keep staff productive.

Increased infrastructure complexity: Though virtualized technologies streamline management and reduce costs, consolidating servers into virtual machines can mean that critical data is concentrated in fewer places. The impact of downtime and damaged or destroyed hardware and data centers is greater. Most organizations are still recovering from a global recession and are struggling to integrate or replace legacy systems that are far past their prime. It's critical that virtual servers have appropriate redundant backup and can be recovered quickly. And if your legacy servers are showing their age, protecting critical data while you make a migration plan is key to eliminating unplanned downtime and data loss.

Merger and acquisition (M&A) activity broke record after record in the past couple of years, compelling IT organizations all over the globe to consolidate servers and data centers into mega warehouses of final business intelligence. Thomson Reuters Deals Intelligence reports that more than \$158 billion in deals were announced in 2013, which is more than twice the activity in 2012—and the trend shows no sign of slowing down.⁵ M&A transitions are precarious times for blended organizations—a modern data protection strategy can ensure that no time or data is lost while infrastructure is merged.

Increased BYOD: The bring-your-own-device (BYOD) phenomenon has certainly added to infrastructure complexity headaches—BYOD is here to stay, however. Wired magazine reported on the many benefits of

² Ibid

³ "The Rising Cost of Natural Hazards," NASA, March 28, 2005

⁴ "Terrorist Hazards," Federal Emergency Management Agency

⁵ "M&A deals lift Wall Street shares nearer a record high," Reuters, Feb. 19, 2013

BYOD, including increased productivity, more options for interactive learning, environmental benefits, reduced costs and increased agility and innovation.⁶ BYOD comes with some increased security risks, however. Experienced IT professionals will tell you that the biggest mistake an organization can make is to assume it can skirt the issue by banning personal devices. For most organizations, the best BYOD policy is to analyze how to keep mobile devices and the data on them secure.

Increased security and privacy regulations: The Ponemon Institute reports that 75 out of 80 polled healthcare organizations experienced at least one data breach incident in the last two years, and 36 out of 80 healthcare organizations had more than five data breach incidents. According to Ponemon, data security breaches cost the healthcare industry alone almost \$7 billion per year. Though healthcare providers are in the spotlight these days, regulations regarding increased security and privacy are growing across almost every industry. In fact, any business of any size that accepts credit cards must comply with PCI data security standards, which means few organization are unaffected by increased governance.

Compliance regulations are also becoming more stringent. In the realm of healthcare, previous HIPAA requirements stated that a provider had to provide notification of a data breach only if more than 500 patients were affected. The new HIPAA Omnibus rule states that, “regulators will assume risk to patients anytime information is inappropriately accessed.” Data breaches are expensive, but they’re also public incidents that weaken consumer confidence, damage the practice’s brand and erode the organization’s competitive advantage. A modern data protection strategy can help keep the organization compliant, and help you avoid fines and brand damage.

CONCLUSION

Sophisticated cybercrime, increased vulnerability to disasters, BYOD adoption, complex new technologies and increased regulations are sure to make 2014 another interesting year for technology professionals. While some organizations will fail to appreciate how important it is to re-evaluate and modernize their current data protection strategy, competitive businesses will take time to put best-in-class solutions and technologies to work for them.

**TO LEARN MORE VISIT-
[HTTP://DATTOBACKUP.COM/](http://DATTOBACKUP.COM/)**

Datto is the preferred provider of hybrid cloud-based backup, disaster recovery and business continuity solutions for MSPs and VARs worldwide. With solutions ranging in size from 150GB to 100TB, Datto helps its Channel Partners provide solutions for businesses of every size, with the opportunity for significant recurring revenue. Datto leverages image-based backup, instant local and off-site virtualization and its proprietary technologies such as Screenshot Backup Verification™, Backup Insights™ and Inverse Chain Technology™, combined with high-end hardware and its secure Cloud. The Datto product line includes Datto SIRIS 2, Datto ALTO XL, Datto ALTO 2, and Datto NAS. Learn more at www.dattobackup.com, partners@dattobackup.com or 888-294-6312.

datto

⁶ “BYOD All About Benefits and Risks,” Wired Innovation Insights, Sept. 20, 2013