Acronis

Transitioning from Reactive to Proactive: **The Evolution of Disaster Recovery**

An increase in threats and risks, the broad use of data, and the 'instant-on' mentality of users, has led to a dramatic disaster recovery transformation.

1970s

Paper Mountains

- Backup evolves from punch cards to magnetic tape
- Paper backup is susceptible to fire and flood
- Batch-oriented mainframes exist
- Computer systems become linked
- Disaster recovery means:
  - Cold storage – Duplicate documents in boxes, not immediate recovery ($)
  - Hot storage – Copy of organization's entire infrastructure for speedy recovery ($$$)

1971 – 'Creeper System,' the first computer virus created by BBN Technologies, fills storage drives

1978 – Sungard, the first disaster recovery company, is founded

1980s

Tape Rotations

- Massive mainframes take up storage space
- Realization that data, systems, and applications are critical to business operations
- Advent of open systems and real-time processing
- Business impact analysis starts
- Business continuity is a more formalized discipline
- Disaster recovery necessitates storage of tapes in an external data center

1983 – U.S. federal government mandates backup and recovery plan for banks

1984 – Floppy disk storage is brought to consumers

1986 – 'Brain,' the first MS-DOS virus affects boot files

1988 – 'Morris Worm' impacts 6,000 computers and causes an estimated $10-100 million in repair costs
– Disaster Recovery Institute is founded

1990s

Digitization and Outsourcing Begins

- Tiered architecture makes its appearance:
  - Colocation
  - Dedicated servers
  - Virtual private servers
  - Redundant power connections
  - Redundant internet connections
  - Multiple onsite backup generators
- 99.999% availability objectives are established
- CD-R, DVDs, and flash drives create opportunities for digital backup and disaster recovery

1990 – Microsoft Office release increases the volume of files

1994 – Business Continuity Institute is founded

1996 – Health Insurance Portability and Accountability Act (HIPAA) is signed
– ISACA develops Control Objectives for Information and Related Technolog (COBiT) framework

1998 – 'Solar Sunrise' seizes control of over 500 government and private computer systems, highlights how a coordinated effort could affect an entire country's IT infrastructure

1999 – 'Melissa' virus infects Word documents and causes $80 million in damages.

2000s

Internet-Driven Diversity of Approaches

- Server virtualization makes recovery much faster
- Storage Area Networks offer speedy, immediate, and programmable backup solutions
- Rise of cloud computing provides faster recovery time and lower costs
- Organizations deal with massive amounts of data with the emergence of big data, cloud, mobile, and social media
- DR plans are more complex to account for larger amounts of data storage from a myriad of devices

2000 – MafiaBoy causes $1 billion in damages

2001 – 9/11 World Trade Center attack places greater emphasis on fast disaster recovery
– Tropical Storm Alison hits twice, impacts 2 million people and causes $5 billion in damages

2002 – DDoS attack aimed at 13 domain name systems, shuts down internet for an hour – the largest and most complex cyberattack to that point
– Federal Information Security Management Act (FISMA) is enacted

2006 – Amazon Web Services is founded, offers first cloud storage
– Two Iron Mountain data storage facilities hit by fire

2007 – Financial Industry Regulatory Authority (FINRA) is founded

2008 – 'Anonymous' DDoS attack cripples Church of Scientology for days
– Hurricane Ike causes $28 billion in damages

2009 – Tens of millions of debit and credit card numbers stolen from 7-Eleven pay

2010s

Cloud Replications

- Complexity of IT infrastructure ensures high-available scalability
- Outsourcing of disaster recovery as a service (DRaaS) begins

2012 – Superstorm Sandy causes NYSE to close for two consecutive days

2013 – 'CryptoLocker', a new form of ransomware, appears
– Yahoo falls victim to the largest data breach in history with 3 billion user accounts compromised

2016 – Man accidentally deletes his entire company's information on all backup servers

2017 – Equifax suffers data breach exposes 147.9 million consumers
– Junior software developer accidentally destroys production database on first day of new job
– 'WannaCry' virus infects 230,000 computers across 150 countries in just three days
– 'Hurricane Harvey' causes the worst flooding and second-most costly natural disaster in U.S. history

2018 – Power and gas-owned electrical lines spark 'Camp Fire', destroy 18,000 structures and cause $16.5 billion damages in California

2019 – Capital One admits 106 million were affected when social security numbers, banking transactions, balances, credit scores, and addresses were stolen

2020s

High Expectations

- Data protection (traditional DR and backup) will be completely inter twined with security. Having one without the other will fail to deliver holistic data protection.
- Protecting data will become an enterprise- and supply chain-wide endeavor as more data is propagated throughout the organization, more workers permanently work remotely, and SaaS offerings continue to grow.
- Artificial intelligence will play a bigger role in the future of data protec tion to stop issues before they happen or make data protection deci sions without human interaction.

2020 – 2020 – End of May - 603 confirmed tornadoes and 209 unconfirmed across the U.S.

Sources

https://www.engadget.com/2015-11-23-the-history-of-disaster-recovery.html
https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/IBM
https://www.jdfoxexec.com/resource-center/articles/history-of-disaster-recovery/
https://www.worldvision.org/disaster-relief-news-stories/2017-hurricane-harvey-facts
https://frii.com/tips/natural-disasters-strike-importance-disaster-recovery-preparation/
https://www.globalsecurity.org/military/ops/solar-sunrise.htm
https://www.csis.org/programs/technology-policy-program/significant-cyber-incidentsForbes
https://www.computerworld.com/article/2546131/two-iron-mountain-facilities-hit-by-fire.html
https://disasterphilanthropy.org/disaster/missouri-kentucky-tennessee-and-alabama-tornado-outbreak/
https://thenewstack.io/junior-dev-deleted-production-database/https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/
https://www.comparethecloud.net/articles/a-brief-history-of-disaster-recovery/
https://www.forbes.com/sites/stephenmcbride1/2020/05/14/why-the-largest-cyberattack-in-history-will-happen-within-six-months/#3eae1d01577c
https://www.independent.co.uk/life-style/gadgets-and-tech/news/man-accidentally-deletes-his-entire-company-with-one-line-of-bad-code-a6984256.html
https://www.npr.org/2019/11/09/777801169/the-camp-fire-destroyed-11-000-homes-a-year-later-only-11-have-been-rebuilt
https://www.foxbusiness.com/lifestyle/the-worst-cyber-attacks-of-the-past-10-years
https://searchdisasterrecovery.techtarget.com/podcast/IT-business-continuity-and-disaster-recovery-Past-to-future