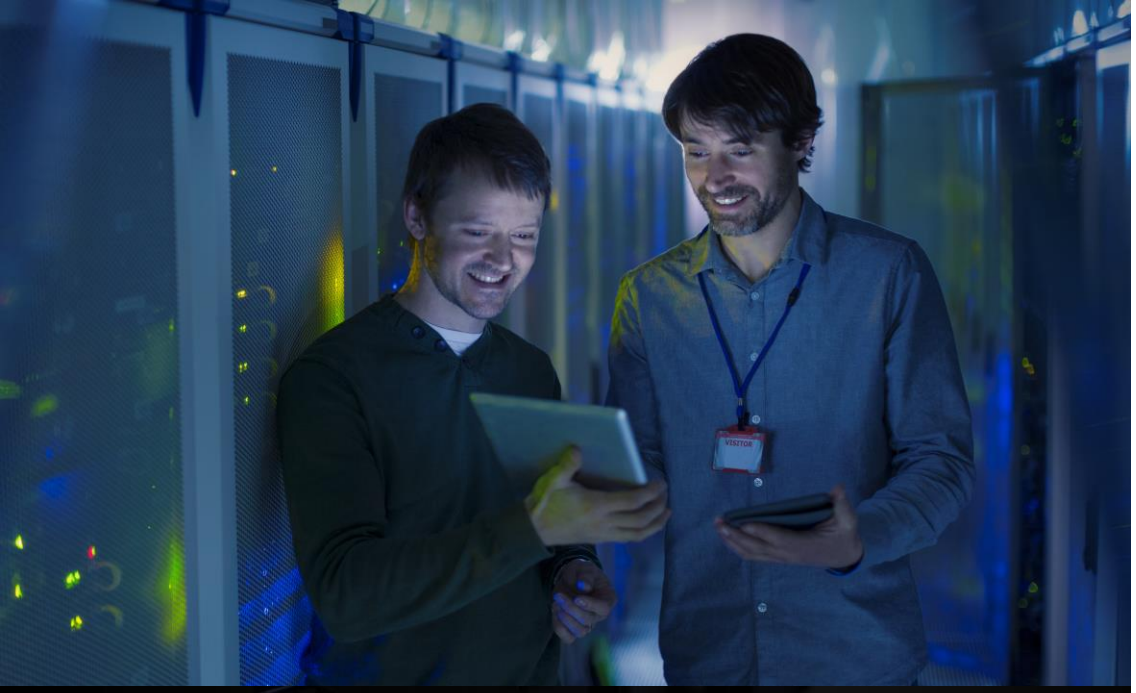
IBM Storage:

An effective line of defense against cyber attacks



CONTENTS:

01 | The latent threat to global business

Whether they are caused by human error, system glitches, or malicious criminal acts, data breaches are among the gravest and most expensive threats to today's businesses. The annual Cost of a Data Breach Report, conducted by the Ponemon Institute found that the average cost worldwide of a data breach in the preceding 12 months was $3.92 million.[1] Organizations affected by a breach also run the risk of having their normal business operations disrupted, as well as losing valuable data, customers and reputation within their industry.

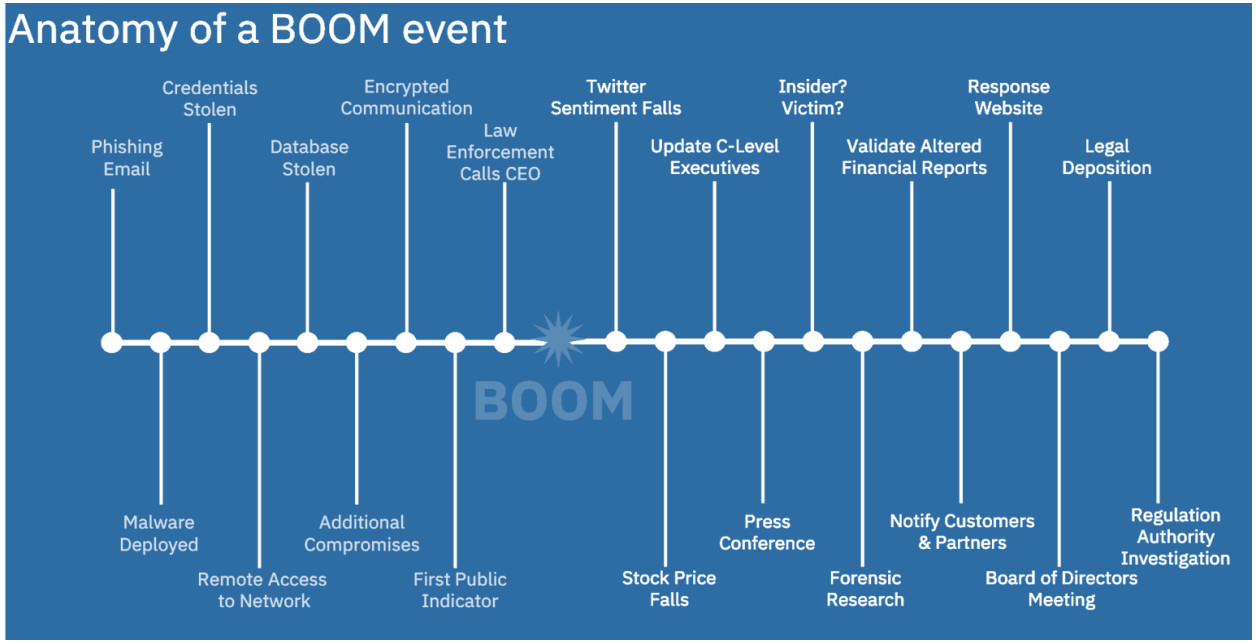
There is also a corresponding human toll. The World Economic Forum's (WEF) 2020 Global Risks Report rated cyberattacks as one of the top risks to human welfare. 75% of those surveyed by the WEF said they expect the risk of theft of data or money from cyberattacks to increase, while 76.1% also saw an increased risk of disruption of operations and infrastructure. [2]

IT organizations require a systematic approach to security today to meet the new challenges posed by pervasive security threats. Leading enterprises are adopting innovative storage technologies such as safeguarded copies. They're also leveraging existing, highly effective physical air gap methods to thwart threats and deliver on their business expectations. The key to executing on such approaches lies in successful risk management.

Timeline of a security breach

During the lifecycle of a security breach, several critical events happen. The first event is the point when a breach occurs. The second is when data has been taken or destroyed. The third is when the breach is discovered (either by external or internal parties). And the fourth is when the breach is made public. When it comes to incident response, each of these points in the timeline are colloquially called “boom” events.

Although the news media often focuses on the event itself, breaches often span many months. Before the breach is disclosed or discovered is termed the “left of boom.” During this time, cyber thieves are taking credentials, gaining deeper access, stealing data to be monetized, targeting key intellectual property, or preparing a destructive attack. Everything to the “right of boom” is about responding and dealing with the fact that a security breach is now known.



During a boom event, organizations have the opportunity to respond well, fumble or completely lose control of their response. They require a systematic approach to security today to meet the new challenges posed by pervasive security threats. Leading enterprises are adopting innovative storage technologies such as Safeguarded Copy, Pervasive Encryption or Air Gap data protection.

02 | Cybersecurity and risk management

Cyber Security VS Cyber Resiliency: An ideal environment should be both cyber secure and cyber resilient. You want both!

- **Security:** “Lock the doors! Prevent intruders!”
- **Prevention**: It’s about trying to keep the bad actors out of your environment in the first place.
- **Resiliency:** “My locks are broken! How do I replace my property?”
- **Recovery:** once the bad actors are in, does the organization have the means to recover quickly and continue business operations

There are already several methods available for organizations to protect themselves from disruption or to help minimize their costs. The Ponemon Institute suggests the following steps to help minimize financial consequences of a data breach:

- Have an incident response team and put incident response plans to the test.
- Implement programs that preserve customer trust to help reduce the unexpected loss of customers following a data breach.
- Discover, classify, and encrypt sensitive data and identify database misconfigurations.
- Invest in technologies that help improve the ability to rapidly detect and contain a data breach.
- Invest in governance, risk management and compliance programs.
- Minimize complexity of IT and security environments.

To establish and maintain a robust cybersecurity strategy, a procedural approach should be employed to understand what data and system assets you have, what their value is, and what risks apply to them. Adopting the principles of risk management to profile the current and desired security state of your organization enables you to consider a range of possible tiers of implementation.

A strong framework is critical for assessing and implementing cyber resilience strategies.

03 | The foundation for the IBM cyber resilience lifecycle

In 2018, the National Institute of Standards and Technology (NIST) published the Framework for Improving Critical Infrastructure Cybersecurity. The framework features three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles.[3]
Within the Framework Core, a series of cybersecurity functions exist. Every organization can take these necessary and achievable steps, if it hasn't already:

- **Identify**: Foster an organizational understanding of the risks cybersecurity threats posed to systems, people, assets, data and capabilities.
- **Protect**: Ensure delivery of critical services with appropriate safeguards.
- **Detect**: Identify a cybersecurity event as it occurs.
- **Respond**: Take action on a cybersecurity incident.
- **Recover**: Restore any capabilities or services impaired by a cybersecurity incident.

Working together, these functions provide greater visibility into an organization's management of cybersecurity risk. With a clearer understanding, the organization can zero in on appropriate storage solutions.

04 | The role of storage infrastructure

Storage has long played the role of “data custodian” in enterprise operations. In addition to providing containers where data goes when not in main memory, the system storage layer has traditionally provided protection functions that help organizations recover from unusual events. Over time, the range of these functions has grown:

- **Backup**: From the 1960s on, storage has allowed application users to save a version of data on separate media to protect it from accidental deletion, corruption, or primary device failure.
- **High availability**: For roughly two decades, storage has provided designs to create multi-path access, multi-server access, and duplication of online copies of data within a machine room.
- **Disaster recovery**: Since the late 1990s, storage has provided designs to create replicated copies of active data at distances sufficient to protect from power outages or natural disasters.
- **Fast online data recovery**: Beginning in the 2010s, storage has provided protected snapshot copies of data for rapid recovery from accidental deletion or data corruption.

In each of these cases, the new function was introduced in storage systems, management software and operational processes to address the specifics of the risk

Shifting from general storage functions to cyber resilience-related ones specifically, there are four key capabilities that deliver across block, file, object, tape, software-defined storage, and cloud:

- **Isolation** is the degree of separation of snapshot or backup data from the rest of the network. Isolation can be achieved though logical means by utilizing safeguarded copies, cloud object storage, or through a physical air gap.
- **Immutability**, or tamper-proof storage, prevents any attacker, external or internal, from changing or deleting data.
- **Performance** is an important capability of the cyber resilience framework. How fast can your organization recover from a cyberattack? While tape excels at isolation and immutability of your backup data, it can take several hours for recovery.
- **Ease of reuse**, or the ease of access to your backup data, is important for testing recovery procedures, validating backups, and restoring data into a sandbox environment to find a valid recovery point in the event of a ransomware incident.

The threat of logical data corruption (LDC) through a cyberattack — specifically a ransomware or wiper attack — presents a new set of protection considerations. To provide the needed level of resilience, solution providers can borrow some of the storage tools already in place for backup and disaster recovery, but some new storage functions are also needed to address the new threats. A mechanism is needed that combines storage functions and operational processes to preserve current recovery copies of data — even in the face of a sophisticated malware attack. Once the attack has been detected and a response mounted, these preserved copies can be used to restart applications and resume normal service.

IBM® Safeguarded Copy prevents data from being modified or deleted due to user errors, malicious destruction, malware, or ransomware attacks with immutable point-in-time copies of production data and dual control security.
The IBM RedPaper™ DS8000® Safeguarded Copy identifies three new capabilities needed to create preserved copies:

- **Granularity**: Organizations must be able to create multiple protection copies in order to minimize data loss in case of a corruption incident.
- **Isolation**: The protection copies must be isolated from the active production data so that they cannot be corrupted by a compromised host system. (This is also known as an "air gap.")
- **Immutability**: The copies must be protected against unauthorized manipulation.

In Five Key Technologies for Enabling a Cyber-Resilience Framework, IDC added two additional considerations: automation and orchestration, and regulatory reporting and assurances.[3] While not unique to LDC attack resilience, they are good for a best practice list.

05 | Storage infrastructure solutions

A successful storage solution delivers a broad spectrum of features for building IT operations that are resilient in the face of LDC attacks or accidental disruption. Comprehensive solutions combine storage functionality, network configuration, administrative controls, and physical security.

Let's take a look at some of the key cyber resilience solutions and technologies currently available, including snapshots, protected backups with WORM (write once, read many) media, tape air gap protection and cloud object storage.

Traditional snapshot-based backup and recovery

Snapshots have become one of the best performing and most cost-efficient methods to address the requirements of traditional backup. Space-efficient, read-only data copies provide cost-effective recovery points that can be used for quick restores of prior versions of data. Using snapshots to recover from accidental deletion or corruption has become a widespread practice.

Protected snapshots

What is the best way to protect snapshots? One approach is to replicate storage volumes from the production system to a secondary storage system of the same type. Periodic snapshots can then be used as recovery copies on the secondary array. The replication and snapshot function should be automated through software. The non-production storage system should not be connected directly to any application servers, and the only storage data connection active should be the port or ports through which backup copies arrive.

Protected backups with WORM media

A functional backup and archive software system can move full copies of data into a managed storage space and maintain backup versions by storing changed data. For the purposes of protecting recovery copies, WORM media can be useful. Tape cartridges can be identified as WORM and used to write recovery copies that are protected from overwrite by the tape drive. Once committed to a WORM cartridge, no type of malware in application or management servers can destroy the backup copy.

Unlike space-efficient snapshots, full copies written to tape require time to move data. Restores are also much slower than what can be achieved with snapshots. Designs should be customized to the needs of each business, but it may be desirable to create a full defense with a snapshot-based recovery augmented by a backup that places data on offline media.

Powerful tape air gap protection

The term “air gap” refers to physical or virtual isolation of systems or networks to avoid widespread corruption of data due to malware infection, system failures, or human error. The basic concept around an air gap is to bring secondary storage systems online periodically to incorporate the latest changes and then take them back offline. Approaches that use snapshot functions to create copies can be quickly mounted to recover damaged applications.

Full protection of the copied data does have some limitations, however. The most complete protection approach, which provides no network or software access to protected copies, can be implemented using a tape library. The “offline by design” nature of tape offers a true physical air gap and provides one of the most secure protections to confront cybercrime.

For more details on data protection with tape, including the use of air gap techniques, WORM, and other security capabilities, please refer to the IBM tape solutions provide modern and powerful data protection solution brief.

Protecting data with cloud object storage

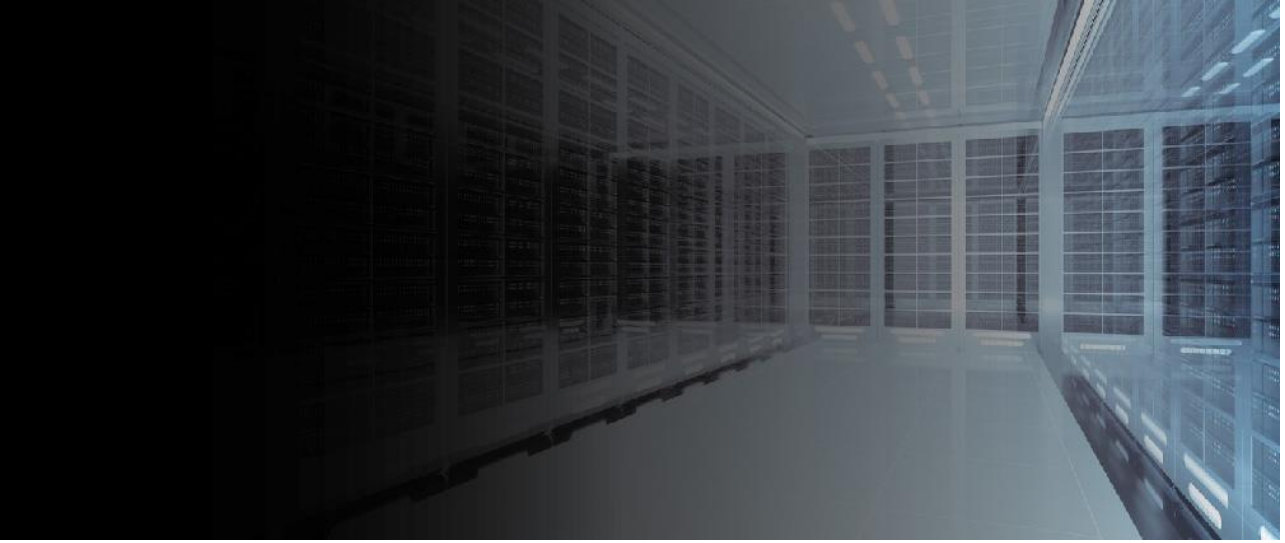
Cloud object storage is a durable, secure, and cost-effective means of archiving and protecting data. Defining policies grants the flexibility to specify the default, minimum, and maximum retention periods. These retention periods and additional legal holds can be applied to a single object or multiple objects as data is fed into the cloud. This means that objects cannot be deleted until the retention period has expired, and all legal holds are removed.

06 | Achieving the optimal security balance

Cyberattacks that deny access to data, or destroy it, are not going anywhere. In fact, they are growing more sophisticated. That is why striking the right balance between the technology your organization uses and the philosophy it takes to data protection is essential for building an effective security strategy. Measures to recover from successful attacks will also be an important part of a well- designed security posture.

In both cases, a number of storage solutions with key security capabilities play a primary role in safeguarding your organization's systems from the array of threats designed to do harm. But without a solid understanding of today's threat landscape — and the information you are tasked with protecting — striking that balance can feel like an uphill climb.

Modern businesses can leverage approaches such as the NIST Framework and the discipline of risk management to help build a comprehensive storage strategy. Technologies like snapshots, tape air gap protection and cloud object storage can be used to create and implement cyber resilience solutions that will help organizations like yours remain secure in the face of mounting threats.



07 | Cyber Resilience Storage Solutions

Only IBM is in the position to offer end to end certified cyber resilience solutions as the result of the deep integration between innovative technology and a comprehensive portfolio of proven software, hardware and solution offerings.

Build cyber resilience solutions with IBM Spectrum Scale and IBM Qradar

IBM Spectrum Scale is a state-of-the-art software-defined storage (SDS) solution that offers a long list of leading-edge data protection and security features.

Artificial intelligence (AI) is a powerful new technology being used to enhance cyber resilience. IBM has developed cyber resilience solutions that utilize the wide-ranging data management features of IBM Spectrum Scale, leverage other IBM Spectrum Storage solutions as needed to bolster specific capabilities, and add powerful AI capabilities through a new solution called IBM QRadar.

When combined, this suite of IBM SDS solutions with IBM Spectrum Scale as the foundational component offers great flexibility to address the full range of cyber resilience requirements using proven enterprise-grade components and powerful AI-driven capabilities.

To learn more about this solution, please visit:
https://www.ibm.com/downloads/cas/VOJ907RG

IBM FlashSystem drives high performance cyber resilience solutions

IBM FlashSystem has earned a reputation for being one of the fastest, most feature-rich storage families in the marketplace. Its capabilities go from Non-Volatile Memory Express (NVMe)-accelerated architecture and IBM Spectrum Virtualize-driven data management capabilities.

IBM FlashSystem data storage solutions can serve as the foundation of a flexible, high-performance, cost-efficient cyber resilience approach to significantly reduce the risk of disruption and financial losses due to user errors, malicious destruction or ransomware attacks. The storage arrays offer many data protection and high-availability features through their use of IBM FlashCore technologies but the real key to building powerful cyber resilience solutions stems from the capabilities of the IBM Spectrum Virtualize.

To learn more about this solution, please visit:
https://www.ibm.com/downloads/cas/EM2XWBEJ

WHY IBM?

IBM Storage for cyber resilience provides end-to-end solutions that can efficiently prevent, detect, and respond to cyberattacks as a result of a deep integration between innovative technology and a comprehensive portfolio of software and hardware offerings. By providing multi-layered security and high resilient functionality, this portfolio can maximize the data protection capabilities to help organizations significantly reduce the risk of business disruption and financial losses due to user errors, malicious destruction, or ransomware attacks.

Don’t let your organization be caught unprepared. IBM Storage Lab Services have the expertise and technical consultants to help you turn your business into a cyber resilient organization by providing:

i. Cyber resilience storage assessments
ii. Implementation services
iii. Post deployment health checks

Talk to your local IBM Business Partner or IBM Representative to learn more

Resources

[1] “2019 Cost of a Data Breach Study: Global Overview.” Ponemon Institute, July 2019

[2] “Global Risks Report 2020.” World Economic Forum, Geneva, Switzerland, January 2020

[3] Framework for Improving Critical Infrastructure Cybersecurity, version 1.1. National Institute of Standards and Technology