Are you ready to recover from a cyber attack corrupting your data, network or systems?

IBM **Services**

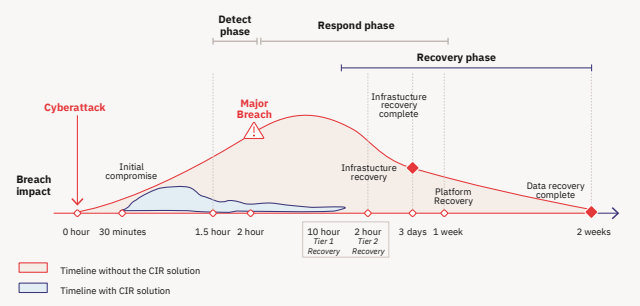
Failure to recover from a cyber-attack will put you out of business

Cyber-attacks and data breaches are on the rise. The odds of a data breach being 1 in 4, breaches are a matter of 'when' and not 'if'. Cyber disruptions have significant impact on your business, resulting in loss of revenues, regulatory penalties and damaged reputation.
Today you are confronted with these 3 key facts:

1. Compliance with evolving data protection and availability regulations is not optional

The European Central Bank Guidance on Cyber Resiliency report specifies resumption within two hours (i.e. two-hour Recovery Time Objective). Financial market infrastructures – for example payment and settlement systems – should design and test its systems and processes to enable a safe resumption of critical operations within two hours of a disruption, even in the case of extreme but plausible scenarios.

2. Managing an outage caused by a cyber-attack takes too long[1]



Average number of days an organization needs to contain a cyber-attack
69 days

Average number of days hackers spend inside IT environments before being discovery
197 days

Today, real clients experience a cost that runs into tens and hundreds of millions following a data breach they were not able to recover.

3. The frequency of cyber-attacks and the attack landscape is continuously expanding

Some of the commonly known cyber-attacks of 2017 were WannaCry, Petya, and NotPetya. The outbreaks were quick, devastating and inflicted maximum impact on businesses giving Chief Information Security Officer (CISO) hardly any time to respond. The WannaCry ransomware attack struck over 100 countries within 48 hours, and the Petya cyber-attack spread rapidly and impacted systems in 65 countries. These, along with common phishing, malware, and denial of service attacks continue to expose critical data and disrupt businesses.

Effective cyber incident recovery solution relies on five key components

Recovery automation, air-gapped protection, multiple data copies on immutable, storage are essential for rapid recovery of applications and data.

Key Components for Cyber Incident Recovery

- Air-gapped Protection
- Immutable storage (WORM)
- Orchestration/Automation
- Data Verification
- Reporting

[1] *Reference*

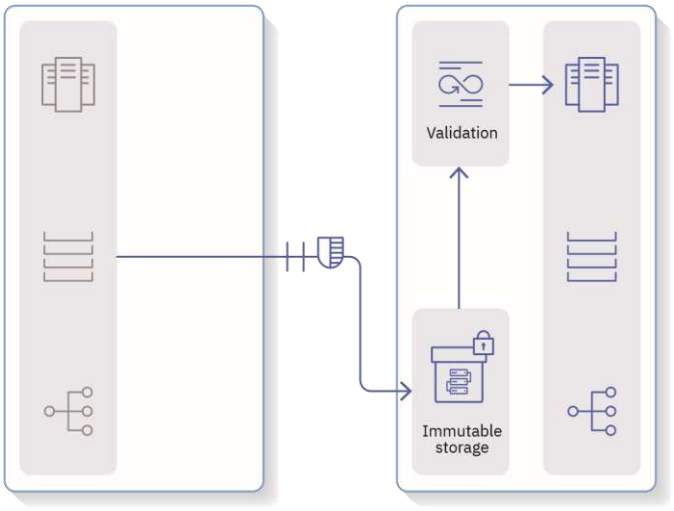
How can IBM help you ensure a minimum viable bank following a cyber-attack?

The IBM cyber incident recovery solution consists of a dedicated backup infrastructure and specialized orchestration tools

1. The dedicated backup infrastructure guarantees quick access to clean backups

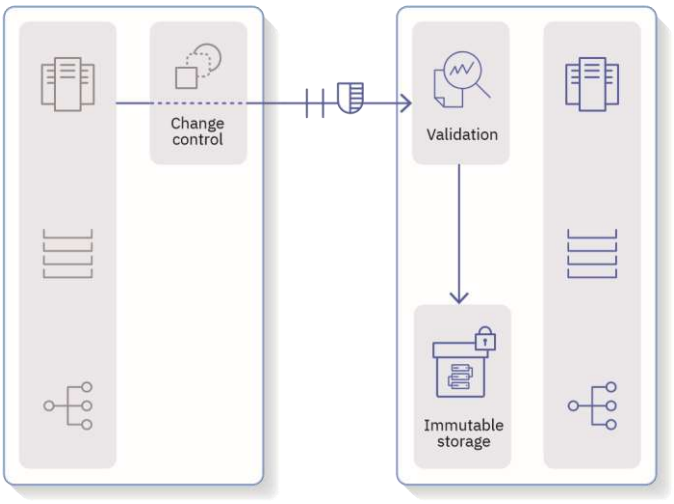
Critical data is copied to an air-gapped location on immutable storage. The copies are verified and tagged as clean for fast retrieval. When an infection is detected, a clean copy is restored.

Cyber Incident Recovery for data



Data is copied to imputable storage in an air-gapped location. The point-in-time copy is mounted on the DR infrastructure and verified. When no infection is found, the copy is tagged as clean and is readily identifiable for a fast restore.

Cyber Incident Recovery for platform configuration



Configuration files are copied to imputable storage in an air-gapped location. The files are compared against the golden copy. If a change is detected, the system cross-checks in the change control system whether the change is legitimate. If the change is legitimate, the backup becomes the new golden copy.

2. The specialized automation tool called 'IBM cyber recovery orchestrator' allows you to automate and orchestrate'

Don't try to manage this manually... Orchestration and automation is necessary to deliver a consistent and predictable Cyber Incident Recovery experience.

- Automation and orchestration maintains the air-gap tight and **speeds up the verification and validation**.
- The automation **reduces the average recovery time** by 50% **and labour cost** associated with testing the solution by up to 75%.
- The dashboard provides a **quick view of incidents** impacting business data and platform configurations. The reporting feature generates the input to **demonstrate compliance** with regulatory requirements.

Resiliency Orchestration provides early warnings for cyber events and provides near-immediate response, reducing the impact of an attack.

Is IBM the right partner to help with this?

IBM's experience and expertise is unparalleled in this space

1. **Proven orchestration & automation solution**

A banking client had a need to enable an automated Cyber Recovery capability AWS. The co-created solution between IBM, the client, and AWS led to realizing compliance to Global Banking regulatory guidance, automated recovery capabilities from cyber events for all attack vectors and accelerated the client's drive to enable a rapidly variable multi-cloud capacity model.

HDFC BANK

HDFC, India's largest private bank, has a need to perform a DR switchover within 2 hours, run live in the DR situation and switchback – and this four times a year – to adhere to the Indian banking regulations. The DR flows are fully integrated with the start-of-day and end-of-day business processes and are managed from a single panel. Through the resiliency orchestration, HDFC has improved its success rate of DR drills from **less than 65% to over 95%**.

2. **Unique end to end integrated capabilities managed from a centralized dashboard**

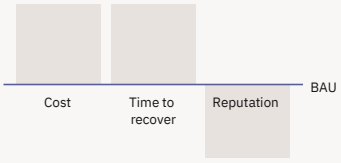
IBM is one of the first few technology companies offering a DR solution with Cyber Incident Recovery capability for multi-cloud environments from a centralized dashboard. The state-of-the-art data protection technologies, Recovery Automation Library based workflows, dashboard monitoring and integration with Resiliency Orchestration make the Cyber Incident Recovery capabilities unique amongst the cyber resilience solutions available in the market today.

3. **Almost 60 years of cyber resiliency experience**

IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and has been granted more than 8,000 security patents worldwide.

- Leading data protection provider: 3.5+ exabytes of data backed up annually and under management
- 388 IBM Resiliency Centers in 68 countries around the globe providing managed disaster recovery and data protection
- Only IBM can deliver Cyber Recovery as a Service (CRaaS), as part of a holistic approach using the Cyber Resiliency framework based on the National Institute of Standards and Technology (NIST) protocol

4. **IBM's cloud recovery orchestration (cro) solution with cyber incident recovery (cir) turns recovering from a cyber-attack into business-as-usual**



Impact of cyber-attack without the CRO-CIR solution

Impact of a cyber-attack mitigated with the CRO-CIR solution

Let us help you transform Cyber Recovery into BAU