CLIENT CASE

Travel and transport

Client challenge
Faced with the imminent risk of bankruptcy due to a restore that took too long to restart business operations after a cyber attack, the client was looking for a significant reduction of restore time for critical data in the IT environment in case of future cyber attacks and downtime events.

Results
IBM delivered a commitment of 7 Days SLA to restore the client's systems and data in 7 days, significantly down from the prior restore time of 30+ days, which reduces client's risk in prolonged disruption in case of future cyber security attack events. Proposed solution includes a 7 Days SLA governance that is responsible for reporting, regular updates of documentations (runbooks etc.) and coordination of needed resources.

CLIENT CASE

Oil and Gas

Client challenge
The client's overall goal was for IBM to provide integrated resiliency and security recommendations including a 3-year recommended plan to achieve the selected disaster recovery alternative.

Results
IBM prepared three disaster recovery alternatives with relative costs, along with strengths and weaknesses of each, to provide the client with direction and planning for the next three years. The team also provided detailed recovery direction, and the specific size/effort/cost of the disaster recovery alternatives. With this information, and the security assessment recommendations, we jointly prepared an executive presentation and 3-year roadmap for the client.

4000+
Professionals dedicated to business continuity

3500+
security patents

2,5
exabytes of customer data managed

#1
in enterprise security software and services

IBM protects
80%
of Fortune 100 companies

7500+
Security professionals

100%
Success in meeting commitments to clients who declared incidents

ARE YOU REALLY READY FOR A CYBER ATTACK?

Organizations need a unified cyber resiliency lifecycle approach, encompassing information security, business continuity, agile network, and organizational resilience, to be able to mitigate emerging cyber risks.

THREE KEY TAKEAWAYS

SECURITY

Clients are ill-prepared on how to respond if their email, active directory, VoIP and laptop/ desktop infrastructure are wiped out in a matter of few hours around the world.

RESILIENCY

Most companies have business continuity and disaster recovery plans, but they are not suited to handle cyberattacks.

NETWORK

Networks that are 5+ years old are seldom resilient. Clients will not be able to segment their critical workloads from other workloads.

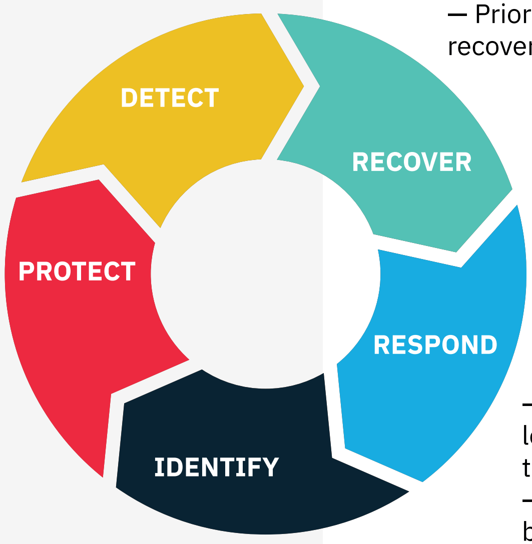
IBM CYBER RESILIENCY LIFE CYCLE

Detect unknown threats with advanced analytics

— See attacks across the enterprise
— Investigate active threats hiding inside the enterprise
— Detect attacks coming from outside the enterprise

Recover access to critical data and applications

— Rebuild mission-critical business applications
— Restore data from back up
— Prioritize network resources to speed recovery



Protect against attacks

— Disrupt malware and exploits
— Discover and patch systems
— Automatically fix vulnerabilities
— Zero Trust as a guiding principle of your network policy

Respond to cyber outbreaks

— Engage cyber incident responders leveraging threat intelligence to repel the attackers
— Remediate the attack damage by restoring systems and closing vulnerabilities
— Utilize network resource to defend against outside threats

Identify your cyber resiliency plan

— Assess your cyber resiliency readiness, process and posture
— Define a roadmap and action plan to improve

FOR MORE INFORMATION PLEASE GO TO:
www-935.ibm.com/services/business-continuity/cyber-resilience