11:11 SYSTEMS

Cyber Incident Recovery Program

Compromised Data / Cyber Incident – Risk Level (High / Very High)

Inherent Risk Level: High / Very High

Threat: Malicious security attack / cyberattack (externally or internally)

Threat Likelihood (High): Multiple attack vectors

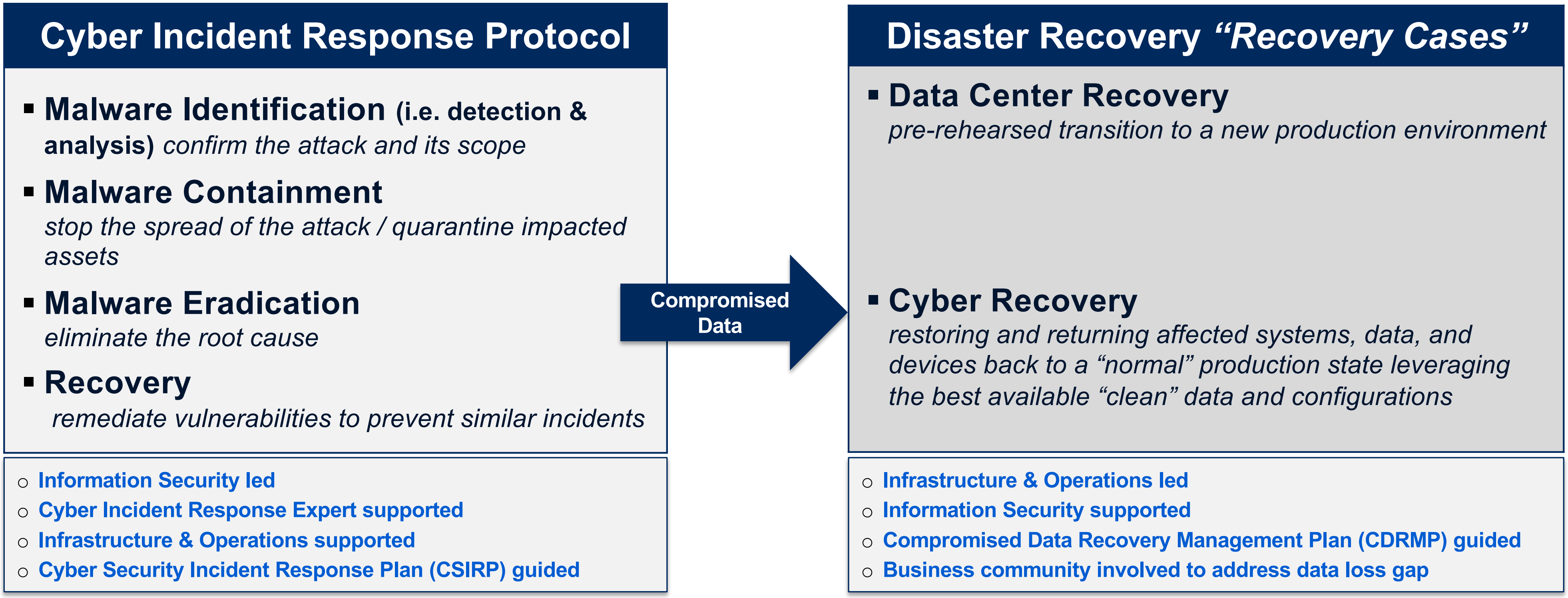
- Internal / Insider (rogue employee / contractor, privileged access, etc.)
  Network connected, understands current defenses, IT environment awareness, etc.
- External / Threat Actor (black hat hacker, bad actor, etc.)
  Highly intelligent, undetected intruder / dwell time, plan a targeted attack, etc.
- External / Malware (ransomware, data-wiping, keylogging, trojan horse, worm, etc.)
  Ever-changing malware (detection tools lagging-behind), zero-day attack, etc.

Threat Impact (V. High): Compromised vital data (both, production & backup data)

Disaster Recovery vs Cyber Compromised Data Recovery

	Disaster Recovery	Compromised Data Recovery
Triggering Event:	Datacenter compromising event e.g., fire, flood, power loss	Data compromising event e.g., ransomware, wiper malware, rogue employee
Production Impact:	Production shift to a “new place” Production shift to a pre-determined Disaster Recovery site	Data recovery ”in place” Malware-free data is re-patriated back to the production environment
Data Currency:	Most current replica or backup data available at the Disaster Recovery site	Most currently available “**clean**” backup data
Recovery Objectives:	✓ RTOs ✓ RPOs Assumes successful prior test experiences with a proven technology	X RTOs Recovery time is predicated on duration of malware clearing activities; potentially a week or more ? RPOs Data loss can be days, weeks, or more depending on backup compromising actions of perpetrators

There are multiple workstreams within a Cyber Incident Response protocol … … and a linkage to DR is essential



Cyber Incident Response Protocol

- **Malware Identification (i.e. detection & analysis)** *confirm the attack and its scope*
- **Malware Containment**
  stop the spread of the attack / quarantine impacted assets
- **Malware Eradication**
  eliminate the root cause
- **Recovery**
  remediate vulnerabilities to prevent similar incidents

- ○ **Information Security led**
- ○ **Cyber Incident Response Expert supported**
- ○ **Infrastructure & Operations supported**
- ○ **Cyber Security Incident Response Plan (CSIRP) guided**

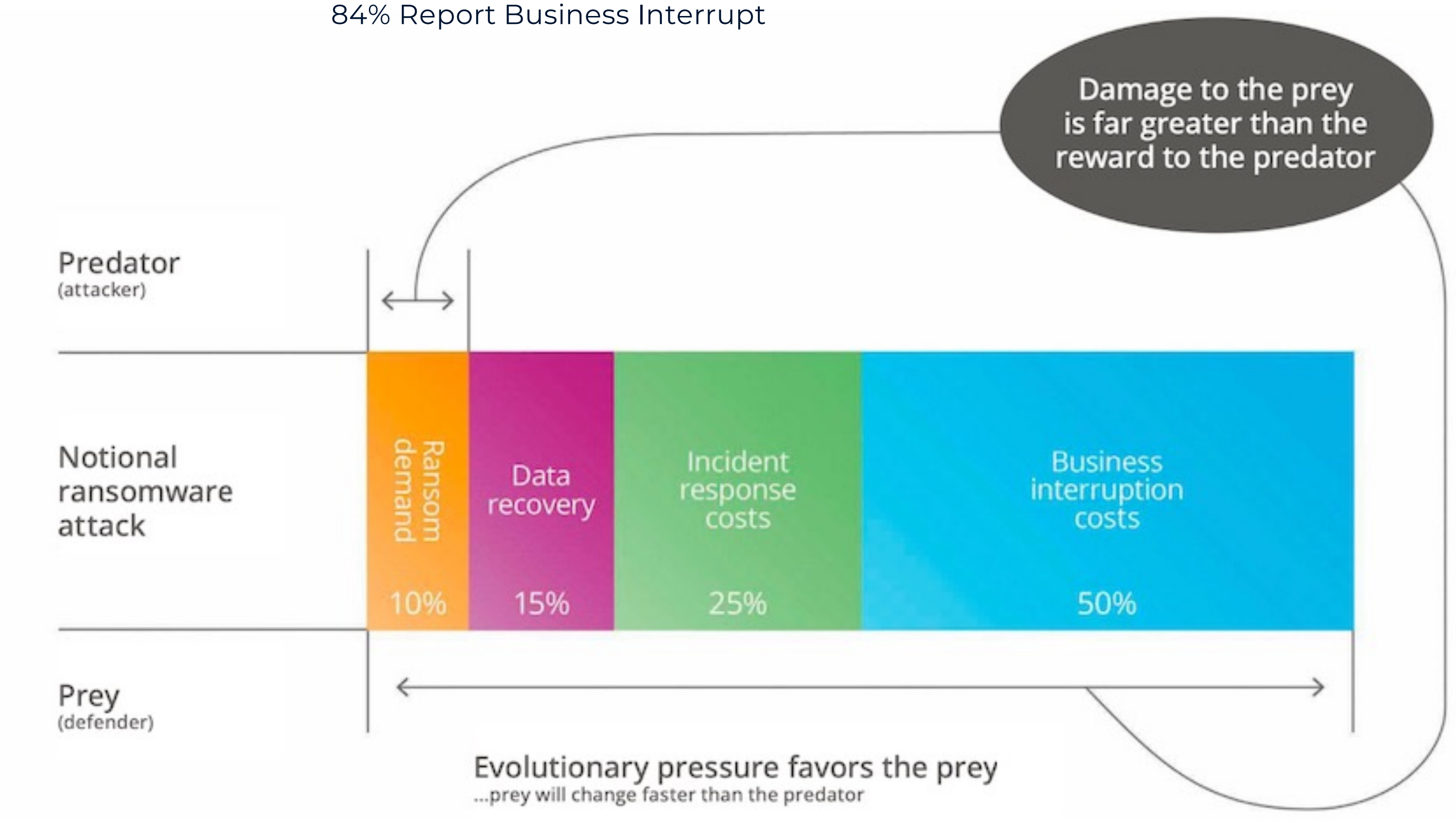
Disaster Recovery *"Recovery Cases"*

- **Data Center Recovery**
  pre-rehearsed transition to a new production environment
- **Cyber Recovery**
  restoring and returning affected systems, data, and devices back to a "normal" production state leveraging the best available "clean" data and configurations

- ○ **Infrastructure & Operations led**
- ○ **Information Security supported**
- ○ **Compromised Data Recovery Management Plan (CDRMP) guided**
- ○ **Business community involved to address data loss gap**

True Cost of a Compromised Data Event

84% Report Business Interrupt


Damage to the prey is far greater than the reward to the predator
Predator
(attacker)
Notional ransomware attack
Prey
(defender)
Ransom demand
10%
Data recovery
15%
Incident response costs
25%
Business interruption costs
50%
Evolutionary pressure favors the prey
...prey will change faster than the predator

AXIS 2024 NetDiligence Cyber Risk Summit.

Industry Analysts Perspective

All industries must consider recovery from cyber events as part of a risk management strategy. If they are not, they should be".

Gartner, Inc. Innovation Insight for Leveraging Isolated Recovery Env and Immutable Data Vaults to Protect and Recover From Ransomware. ID G00748659

While isolated recovery can protect the entire environment, it is intended to protect the most critical applications and data.

Gartner, Inc. Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware. ID G00748659

Creating an immutable copy of backup data in an air-gapped network location is now a must for any data protection strategy.

Gartner, Inc. How to Recover From a Ransomware Attack Using Modern Backup Infrastructure. ID G00738061

Following an established plan during a ransomware attack will limit confusion and reduce the impact by reacting in an efficient manner.

Gartner, Inc. *How to Recover From a Ransomware Attack Using Modern Backup Infrastructure. ID G00738061*

There is a lack of dedicated DR Plans to implement, manage and create an optimal response and recovery process for such a complex solution.

Gartner, Inc. *How to Recover From a Ransomware Attack Using Modern Backup Infrastructure. ID G00738061*

DR program owners need to develop recovery options, runbooks, workflows, and plans for the inevitable ransomware attacks, as the recovery runbooks will differ significantly from those in more commonly addressed disaster incidents.

The State of Disaster Recovery Preparedness In 2020 by Naveen Chhabra

Don't treat ransomware, DDoS, or other cyberattacks as the exclusive domain of the security team.

The State of Disaster Recovery Preparedness In 2020 by Naveen Chhabra

Only 13% of organizations were able to fully recover without paying a ransom

Future Enterprise Resiliency & Spending Survey, Wave 6, July 2021

27% reported not paying the ransom, but also not being able to fully recover their data from backup

Future Enterprise Resiliency & Spending Survey, Wave 6, July 2021

Gartner Isolated Immutable Vaults

Gartner Recover from Ransomware

Forrester Report DR Preparedness

* Cost of a Data Breach Report – IBM Security

11:11 SYSTEMS

11:11 Systems' Compromised Data Recovery Good Practice Framework

Identify ***Vital Data Asset Requirements***	**Protect** ***Data Protection / Backup Methods***	**Respond** ***Compromised Data Incident Response***	**Recover** ***Compromised Data Recovery Execution***
VDA Identification *Assessment Criteria and Process*	**Unchangeable Data** *Immutability*	**Response Scope** *Compromised Data Recovery Requirements*	**Clean Room Enablement** *Isolated Recovery Environment*
VDA Interdependencies *Workflow Requirements*	**Unreadable Data** *Encryption*	**Response Plan** *Compromised Data Incident Response & Data Recovery Management Plans*	**Clean Data Identification** *Immutable Backups Forensics Analysis*
VDA Requirements *Approved Scope*	**Inaccessible Data** *Authentication Controls*	**Business Continuity Plans** *Manual Workaround Procedures for extended Durations*	**Clean Data Recovery** *Compromised Data Recovery Execution*
VDA Technical Profile *Technical Recovery Requirements*	**Unreachable Data** *Air Gapped Cyber Data Vault*	**Response Advisors/Break Glass** ATOD Expertise to Leverage for Incident Response, Coaching & DFIR	**Cyber Recovery Readiness** *Recovery Lifecycle Management*
VDA Data Profile *Data Protection Requirements*	**Uncompromised Data** *Anomaly Detection*	**Response Exercises** *Response Plan, Tracks, and Options*	**Cyber Recovery Tests** *Recovery Capabilities Verification*

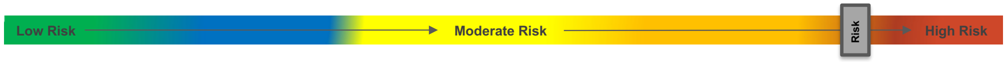
Vital Data Assets (VDAs) are an organization's "must-have" / "mission-enabling" data requiring advanced levels of protection and recovery preparedness

What is Your Organization's Confidence Level You Can
Manage Through and Recover From a Ransomware Event?

11:11 SYSTEMS

Where you are in the journey requires awareness of the essential controls needed for compromised data recovery readiness…

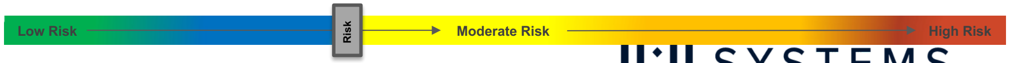
Identify *Vital Data Asset Requirements*	**Protect** *Data Protection / Backup Methods*	**Respond** *Compromised Data Incident Response*	**Recover** *Compromised Data Recovery Execution*
🟥 **VDA Identification** *Assessment Criteria and Process*	🟥 **Unchangeable Data** *Immutability*	🟧 **Response Scope** *Compromised Data Recovery Requirements*	🟧 **Clean Room Enablement** *Isolated Recovery Environment*
🟥 **VDA Interdependencies** *Workflow Requirements*	🟧 **Unreadable Data** *Encryption*	🟧 **Response Plan** *Compromised Data Recovery Management Plan*	🟥 **Clean Data Identification** *Immutable Backups Forensics Analysis*
🟥 **VDA Requirements** *Approved Scope*	🟧 **Inaccessible Data** *Authentication Controls*	🟥 **Response Tracks** *Compromised Data Recovery Options*	🟥 **Clean Data Recovery** *Compromised Data Recovery Execution*
🟥 **VDA Technical Profile** *Technical Recovery Requirements*	🟥 **Unreachable Data** *Air Gapped Cyber Data Vault*	🟥 **Response Advisors** SMEs with proven cyber recovery experience	🟥 **Cyber Recovery Readiness** *Recovery Lifecycle Management*
🟥 **VDA Data Profile** *Data Protection Requirements*	🟧 **Uncompromised Data** *Anomaly Detection*	🟥 **Response Exercises** *Response Plan, Tracks, and Options*	🟥 **Cyber Recovery Tests** *Recovery Capabilities Verification*



- Governance
- People
- Process
- Technology
- Validation

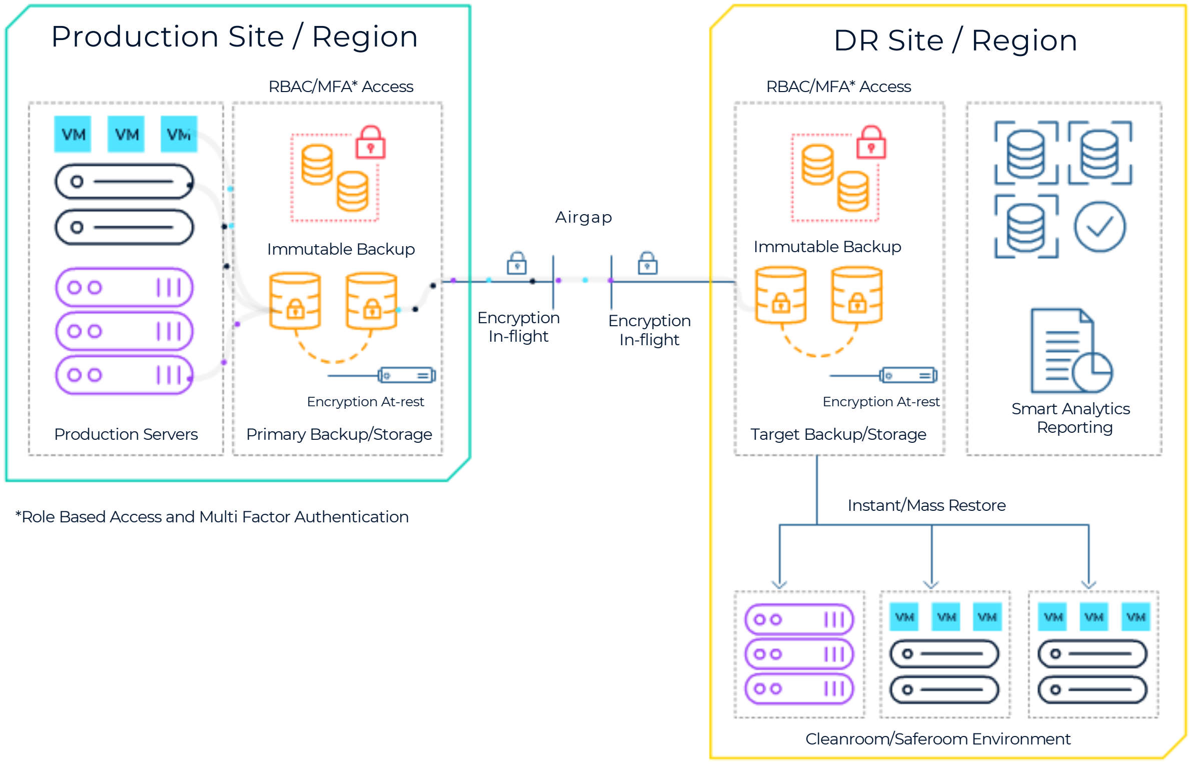
Remediation

Identify *Vital Data Asset Requirements*	**Protect** *Data Protection / Backup Methods*	**Respond** *Compromised Data Incident Response*	**Recover** *Compromised Data Recovery Execution*
🟩 **VDA Identification** *Assessment Criteria and Process*	🟩 **Unchangeable Data** *Immutability*	🟩 **Response Scope** *Compromised Data Recovery Requirements*	🟩 **Clean Room Enablement** *Isolated Recovery Environment*
🟩 **VDA Interdependencies** *Workflow Requirements*	🟩 **Unreadable Data** *Encryption*	🟨 **Response Plan** *Compromised Data Recovery Management Plan*	🟩 **Clean Data Identification** *Immutable Backups Forensics Analysis*
🟩 **VDA Requirements** *Approved Scope*	🟩 **Inaccessible Data** *Authentication Controls*	🟦 **Response Tracks** *Compromised Data Recovery Options*	🟩 **Clean Data Recovery** *Compromised Data Recovery Execution*
🟨 **VDA Technical Profile** *Technical Recovery Requirements*	🟩 **Unreachable Data** *Air Gapped Cyber Data Vault*	🟨 **Response Advisors** SMEs with proven cyber recovery experience	🟦 **Cyber Recovery Readiness** *Recovery Lifecycle Management*
🟨 **VDA Data Profile** *Data Protection Requirements*	🟩 **Uncompromised Data** *Anomaly Detection*	🟨 **Response Exercises** *Response Plan, Tracks, and Options*	🟨 **Cyber Recovery Tests** *Recovery Capabilities Verification*



II:II SYSTEMS

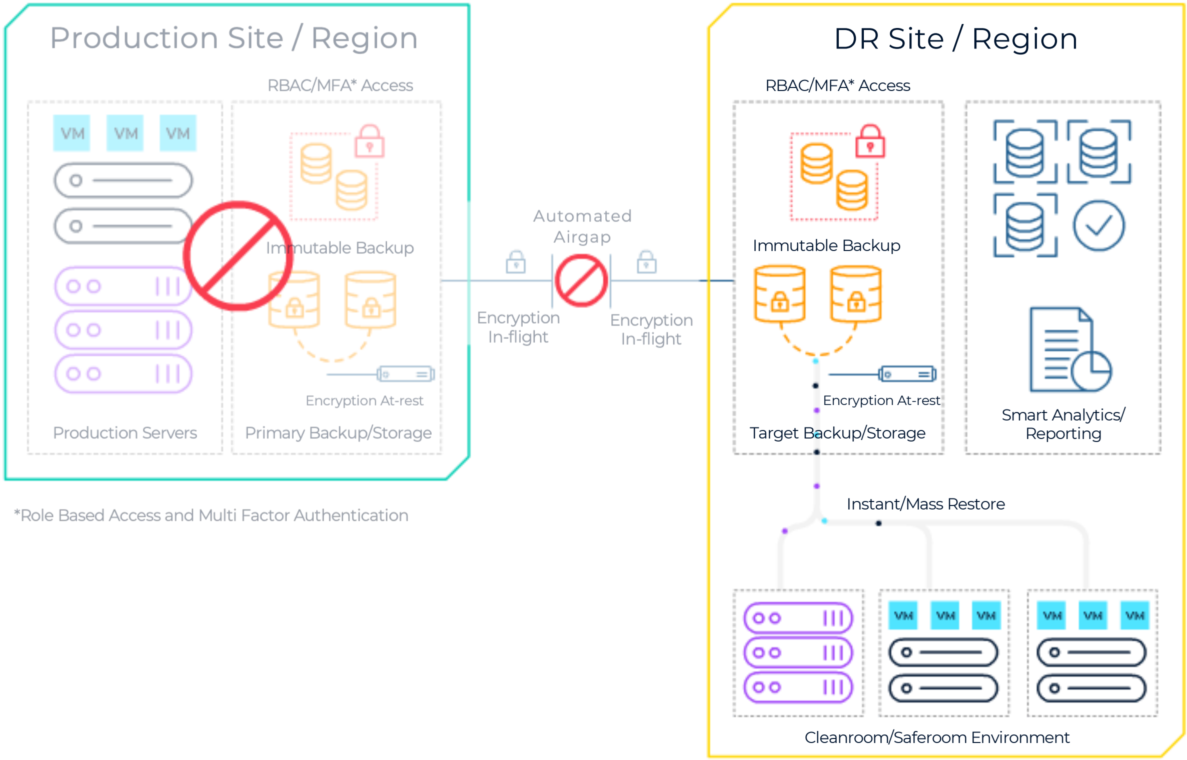
Cyber Incident Recovery – Reference Architecture



*Role Based Access and Multi Factor Authentication

- Immutable Backup
- Airgap
- Encryption
- RBAC and MFA
- Backup/Data Integrity

Cyber Incident Recovery Simulation



*Role Based Access and Multi Factor Authentication

Historic Credentials

System Configuration and Runbook Snapshot

Backup Retention

Cyber Recovery Simulations

Forensic Analysis and Data Validation**

Isolated Data and Application Recovery

Post DR Clean-up

II:II SYSTEMS

Managed Recovery & Managed Cyber Recovery

Disaster Recovery + Compromised Data Recovery

DISCOVER

DISCOVER

Discover Production

- Infrastructure and Application Discovery
- Populate CMDB
- Baseline Scope for Recovery
- Understand Change Management Process

DESIGN

ASSESS & DEFINE

Assess & Design Recovery Strategy

- Analyze Discovered Information
- Apply Recovery Best Practices
- Design Recovery Solution Architecture

Define Recovery Plans & Procedures

- Define Core Recovery Configuration
- Define Application Recovery Configuration
- Generate Application Recovery Plans and Procedures
- Backup and Credential Retention Policy
- Meta-data and Runbook Snapshot Policy

RUN

IMPLEMENT & TEST

Recovery Implementation and Execution

- Build Recovery Solution
- Test Execution
- Forensic Analysis*
- Data Validation*
- Clean Room Restores
- Post-DR Clean-up
- Cyber Recovery Simulations
- Test Management and Reporting

MANAGE

RECOVERY LIFECYCLE

Recovery Lifecycle Management

- Analyze Production Changes for Impact on Recovery
- Update Recovery Design, Plans and Procedures
- Ongoing Recovery Optimization
- Meta-data and Runbook Snapshot
- Backup Retention
- Credential Retention

Confidential- For internal purposes only, not for external distribution.

Successful Track Record

- Successfully recovered customers from various business verticals:
  - Healthcare
  - Insurance
  - Finance
  - Retail
  - Automobile
  - Manufacturing
  - IT service

- Average time customer stayed in 11:11 Systems post cyber incident – 14 Weeks

CASE STUDY

Recovery from Ransomware

CHALLENGE

- Global pharmaceutical and life sciences company
- On top of handling operations during the global COVID-19 pandemic they suffered a ransomware attack that took down their production servers
- Limited IT staff and access to the production datacenter restricted in-house response

11:11 SYSTEMS SOLUTION

- 11:11 Systems Managed Recovery Solution
- Utilization of back-dated backup sets for “pre-infection state” recovery

RESULT: Production services restored within stipulated timeframe

Business process continued despite disaster

Point-in-time recovery achieved within hours

Zero reputational impact and no need to concede to attacker’s demands

Business continued uninterrupted with no financial impact

> “11:11 Systems helped us to recover all our servers with great urgency. Since then, we are running our business /production environment from their DR POD.”
>
> “We have never encountered such a great coordinated support and service from any vendor yet, this is exactly the kind of benchmark we wanted”
>
> **General Manager-IT**

11:11 SYSTEMS

Thank You