THE MORE LIKELY DISASTER RECOVERY EVENT

Ransomware is a persistent threat to business viability requiring multiple pre-defined and pre-enabled data recovery strategy options

Unlike traditional Disaster Recovery (DR), there is no single or guaranteed approach to recovering maliciously compromised data. Pre-planned and flexible compromised-data recovery options will make the difference between success and failure.

COMPROMISED DATA RECOVERY STRATEGY OPTIONS

Where to Focus Data Protection Investments

Investments in data recovery readiness need to reflect the importance of data to the viability and survival of the organization – the focus must be on the data that matters – the Vital Digital Assets (VDAs)!

Compromised Data Recovery

Minimizing IT downtime and data loss requires a flexible suite of recovery strategies and capabilities that can be individually or concurrently leveraged to address the particulars of a data-compromising cyber intrusion.

What is a Vital Data Asset (VDA)?

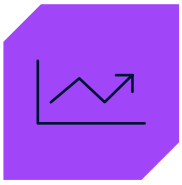
VDAs are an organization's "mission-enabling" / "must have" data needed to support the Minimally Viable Enterprise.

Identify vital data assets (VDAs).

Most organizations can't afford to follow the 3-2-1-1-0 rule for all of the data in the IT environment. So you need to figure out what assets are absolutely vital. This includes data that could threaten business viability if the information becomes:

- Exposed
- Compromised
- Unavailable

SENSITIVE OR REGULATED INFORMATION



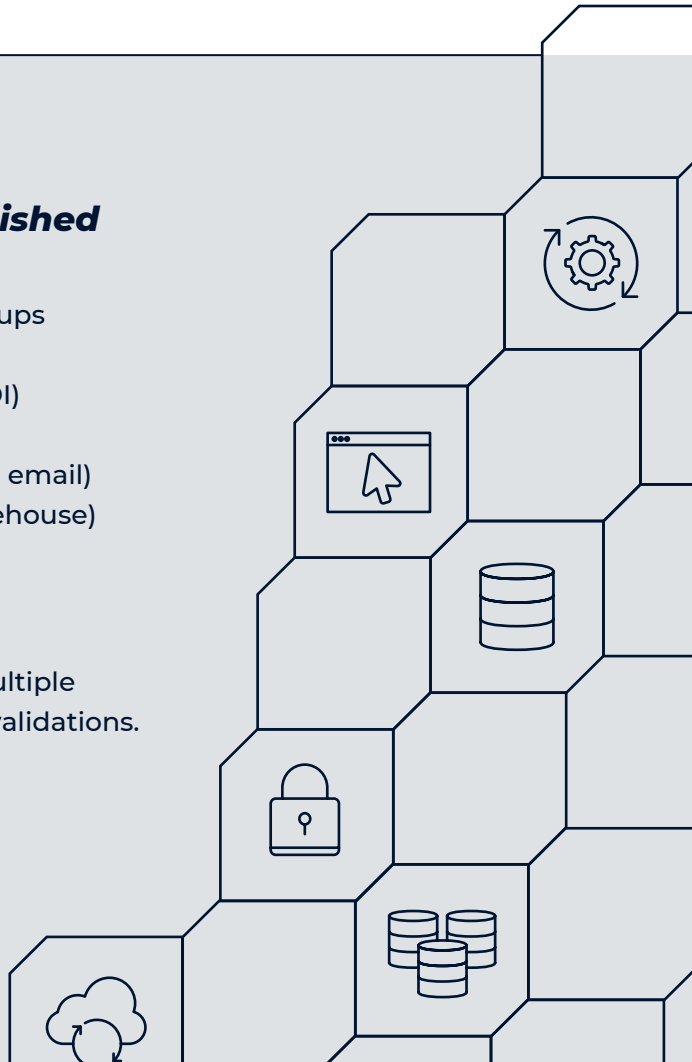
ANYTHING THAT GENERATES REVENUE

DATA RELATED TO YOUR ORGANIZATION'S MISSION

Recovery Options and Plans Must Be Established And Validated For Each VDA

- Restore to a point in time from extended retention backups
- Decrypt data via acquired decryption key
- Reprocess transactions from source repositories (e.g., EDI)
- Rebuild data from other systems (e.g., data warehouse)
- Reenter transactions directly from source materials (e.g., email)
- Recreate transactions manually (e.g., re-inventory a warehouse)

Reducing the risk of a failed data recovery effort requires multiple strategies and accompanying plans, capabilities, skills, and validations.



II:II SYSTEMS

THE ROAD TO DATA RECOVERY READINESS

Identify Vital Data Assets

Identify the business and infrastructure data that justifiably requires additional levels of protection beyond what is in place for traditional disaster recovery.

Define and develop Alternative Recovery Strategies for Each Vital Data Asset

Recovery from backups may simply not be possible in a ransomware situation. It is therefore imperative to work in concert with the business community to pre-determine feasible data recovery options.

Validate Effectiveness

To understand if it all works and to be able to convey the overall stats of readiness to executive leadership requires tests, exercises, and rigorous reviews.

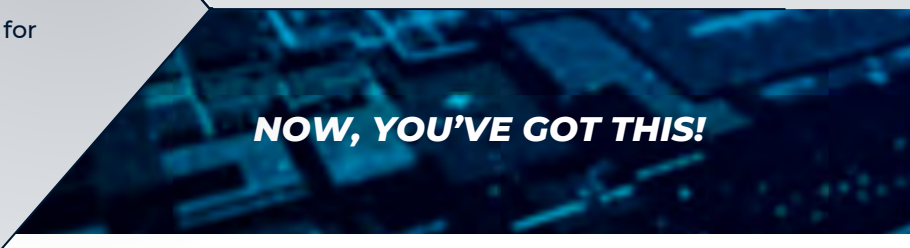
"Modern" Backup of Vital Data Assets

Implement a backup solution exhibiting the specialized characteristics essential to protecting data and enabling cyber-compromised data recovery:

- Immutability
- Air-gapping
- Anomaly detection
- and more ...

Prepare Plans and Establish Enabling Capabilities

- Plans for each recovery strategy option should be developed
- Teams with the right skills and experience levels need to be defined for each plan recognizing that recovery efforts may run in parallel
- Some strategies will require an off-network technology space to undertake recovery efforts



HOW 11:11 SYSTEMS CAN HELP

Our Compromised Data Risk Management (CDRM) framework helps identify data recovery risks and needed mitigations.

The first step in the journey is to understand the controls and proven practices essential to an effective recovery effort. From there, we'll create a prioritized roadmap of actions to address your gaps. Over time, this will reduce the risks of a failed data recovery effort.

Our CDRM Framework is quite comprehensive, featuring over 100 controls and established practices that are key to understanding the risk associated with recovering compromised data. To make it easier to grasp, we've included a color-coded sample below that illustrates how we assess a client's situation.

COMPROMISED DATA RISK MANAGEMENT (CDRM) - FRAMEWORK

Identify *Vital Data Requirements*	Protect *Data Protection / Backup Methods*	Respond *Compromised Data Incident Response*	Recover *Compromised Data Recovery Execution*
VDAs Identification *Assessment Criteria & Process*	**Unchangeable Data** *Immutable Data*	**Response Scope** *Compromised Data Recovery Req.*	**Clean Room Enablement** *Isolated Recovery Env. for Forensics*
VDAs Interdependencies *Workflow Requirements*	**Unreadable Data** *Encrypted Data*	**Response Plan** *Compromised Data Recovery Mgmt. Plan*	**Clean Data Identification** *Immutable Backups Forensics Analysis*
VDAs Requirements *Approved Scope*	**Inaccessible Data** *Authentication Controls*	**Response Tracks** *Compromised Data Recovery Options*	**Clean Data Recovery** *Compromised Data Recovery Execution*
VDAs Technical Profile *Technical Recovery Requirements*	**Unreachable Data** *Secured Data Vault*	**Response Advisor(s)** *SME's / Incident Experience*	**Cyber Recovery Readiness** *Recovery Lifecycle Management*
VDAs Data Profile *Data Protection Requirements*	**Uncompromised Data** *Anomalies Detection Scanning*	**Response Exercises** *Response Plan, Tracks, Options, etc.*	**Cyber Recovery Tests** *Recovery Capabilities Verification*
Risk Level: High	*Risk Level: High*	*Risk Level: Low*	*Risk Level: Very Low*

Sample - Assessment Results

Integrating the operational resilience pillars

Readiness for compromised data recovery requires well-orchestrated integration across multiple operational resilience disciplines including disaster recovery, backup and data retention, business continuity, crisis management, cyber incident management, and digital forensics

Our Compromised Data Risk Management Services

Risk Identification

- Compromised Data Risk Management Assessment

Exercise & Test

- Ransomware Challenge Exercises with various focus:
  - Executive Decision • Technical Recovery • Business Readiness
- Compromised Data Recovery Exercise and Test Program Design

Data Protection

- Vital Data Asset Identification and Data Protection Requirements
- Backup strategy and solutioning

Response & Recovery Planning

- Compromised Data Recovery Management Plan (CDRMP) Development
- Business Continuity Plan Development to include response to extended loss of application availability (>>> RTO) and data (>>> RPO)

BEING CYBER RECOVERY READY REQUIRES AN ONGOING PROGRAM, AND 11:11 SYSTEMS HAS THE EXPERTS AND THE TECHNOLOGY TO HELP.

We bring together more than 40 years of history providing tactical expertise and customer success in disaster recovery and cyber recovery. We will work with you to build a cyber readiness program that will ensure that your team is ready when cyber criminals strike.

11:11 SYSTEMS

RETHINK CONNECTED

1111systems.com