SUNGARD AVAILABILITY SERVICES®

RECOVERING CYBER-COMPROMISED DATA

In the ever-evolving world of cybercrime it is now, more than ever, essential to properly protect your critical data from malicious data cyberattacks that corrupt or hold your organization's "crown jewels" hostage. And despite your best protection efforts, it is imperative to be ready and fully enabled to recover that data when a cyberattack is successful.

It's a different recovery case

Recovering data in the aftermath of a successful cyberattack is a very different "recovery case" from physically focused data center disaster scenarios. Cyber-compromised data recovery simply happens differently and rarely are traditional disaster recovery plans and capabilities sufficient for this purpose.

Here are the key differences:

	DISASTER RECOVERY	DATA RECOVERY
Triggering Event:	Recovering infrastructure, applications, and network services following a **datacenter compromising** event	Recovering data following a **data compromising** event (e.g., ransomware, wiper malware, rogue employee)
Production Impact:	Transition to a temporary production /DR environment with the possibility of a second transition to a revitalized or new production environment	Repatriation of data back to the production environment where it was originally compromised; typically on hardware rebuilt from bare metal
Data Focus:	Recovering the most current data from replicas or backups	Recovering the most current "clean" data from backups taken prior to the date and time of initial compromise
Likely RTO/ RPO Success:	RTOs and RPOs should be met assuming successful test experience	RTOs and RPOs will rarely/not be met with significant data loss often occurring

Some data has extraordinary value

Disaster recovery focuses on critical application recovery and the data associated with it, but there are a few key points of reality to keep in mind:

1. **It rarely makes sense to invoke DR** for cyber-compromised data recovery purposes.
2. **It typically takes 5 days or much longer** to recover data after its integrity has been compromised; RTOs and RPOs will rarely be met.
3. **It is possible that the latest clean data** suitable for repatriating back into the production environment **is weeks or more old** which may be well beyond its useful shelf life.
4. **Your attackers may have encrypted** all of your on-network backups.
5. **Critical does not mean vital.** So it's important not to assume that your Business Impact Analysis has identified what data absolutely CAN'T be lost and the data that could impact the viability, mission, or compliance regulations of your organization. Vital data may be out of scope of your DR program.

The Sungard AS Good Practice Model for Cyber-compromised Data Recovery

There's a lot to consider in order to gain confidence that your organization is ready to effectively and efficiently recover data, both vital and non-vital. It requires a defined program and a well-rehearsed multi-disciplinary team. Sungard AS has pioneered a comprehensive good practice program model addressing this increasingly serious and impactful threat.

Program Level Good Practices for Effective Cyber-compromised Data Recovery

IDENTIFY Vital Data Assets (VDAs)	PROTECT VDA recovery architecture	DETECT VDA vulnerabilities	RESPOND Plans and capabilities	RECOVER Recovery rehearsals
VDA Identification Criteria	3 Areas of Resource Separation (People-Process-Technology)	Ethical Hacking of VDA Environment	Compromised Data Recovery Management Plan	Plan Reviews and Walkthroughs
VDA Identification Process	2 Different Recovery Strategies	Ransomware Attack Simulation on VDAs	Business Continuity Strategies for Data Loss	Tabletop Exercises
VDA Risk Ranking	1 Off-network Immutable Copy	Dark Web Assessment of Potential VDA Compromise	Technology Strategies for Data Loss	Data Recovery Tests
VDA Approval	1 Off-network Secured Environment		Ransomware/Cyberattack Response Advisor	Technology Recovery Tests

CONTINUAL IMPROVEMENT

Who is responsible? Who is involved?

Mistakenly, many organizations see this as a CISO-led responsibility, but that is rarely practical. Information Security is involved, but when it comes to recovering data from backups, your disaster recovery team will typically lead the rescue effort. The CISO would certainly lead the undertaking when it is believed that the quickest and lowest cost data recovery approach is to negotiate with your attackers; at least those to be known as reputable. Often these two data recovery tracks happen concurrently, so you do need Information Security to assess whether the data you plan to bring back into the production environment is clean (malware-free).

Sungard AS recommends the following considerations when creating your Cyber-Compromised Data Recovery program:

Data optimized for traditional disaster recovery and database restores is likely to be ineffective for a cyber-compromised data recovery effort.

Extra-duty-of-care is essential for your most vital of data assets.

An off-network safe room is essential for analyzing data before it gets restored back into your production environment.

Testing to assure plan, team, and archive effectiveness is essential.

Together, these best practices will enable you to create a program that reduces risk and allow your organization to enjoy a high degree of confidence that it can rapidly recover critical data after a successful cyberattack.

With our proven Good Practices model, Sungard AS can help you mitigate the risk of prolonged down time and increase your chances of quickly and effectively recovering your vital data from a successful cyberattack. Visit sungardas.com to learn more.

North America:
www.sungardas.com
or call us at +1 (866) 714-7209

EMEA:
www.sungardas.co.uk
or call us at +44 (0) 800 143 413

SUNGARD AVAILABILITY SERVICES®