Sun Tzu's Core Principle for Attacks and How It Can Be Used to Develop a Ransomware Resilience Strategy

Wayne Hankins

Sun Tzu:

Strategy without tactics is the slowest route to victory.

Tactics without strategy is the noise before defeat.

Gartner's Resilience and Innovation in Infrastructure Survey

73% of the group was missing the three basic elements of a DR program:

- Formalized scope
- Business impact analysis
- Detailed recovery procedures

Ransomware Attack Victim

What is the probability of an infected system contaminating others?

What data/workloads are critical to the business?

Who owns the assignment of crown jewels?

What are our containment capabilities?

When should I engage incident response service provider?

What is the current health of the business being supported by cybersecurity and IT? Before, during and after a ransomware attack?

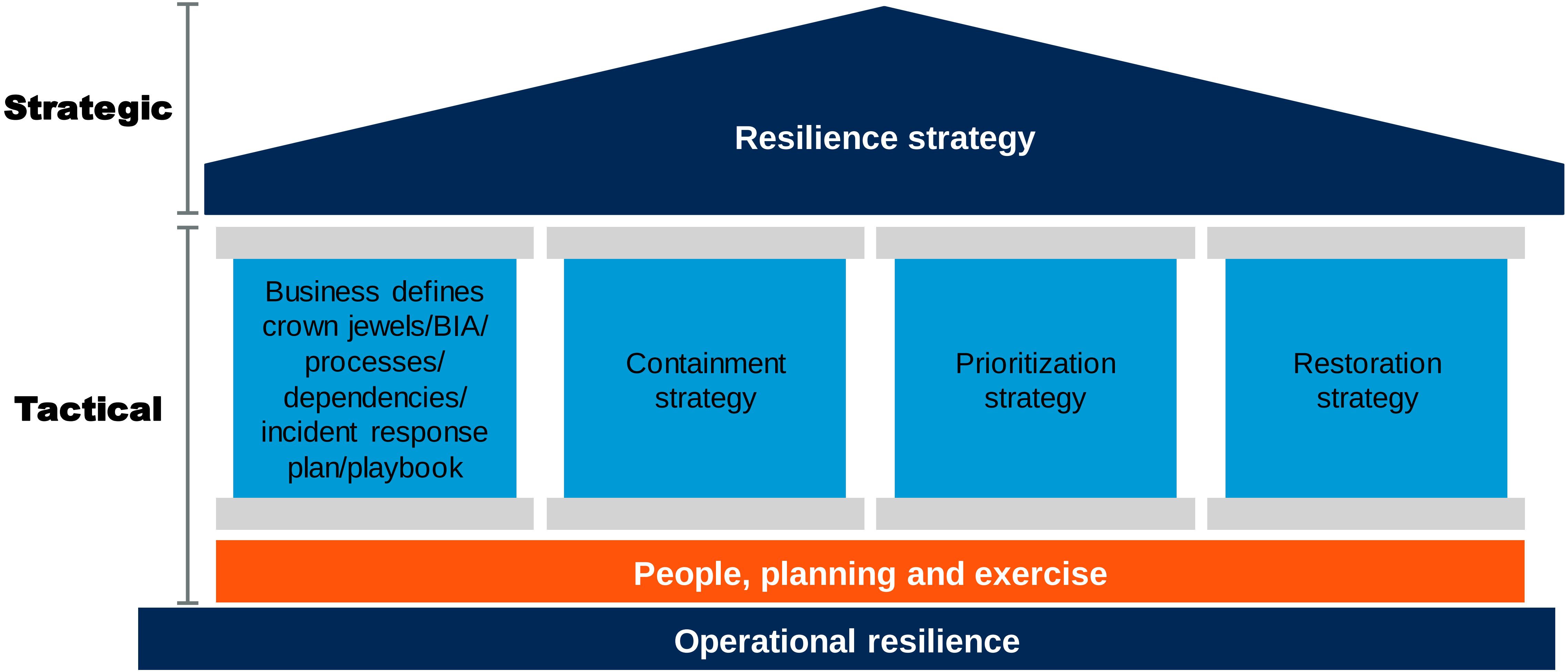
Do we pay or not pay?

Which systems should be brought online first and the sequence?

Can we recover from backup, or have they been tested? Last know good copies? Immutable vaults? Isolated recovery environment?

Resilience strategy ransomware framework

Resilience Strategy for Malware and Ransomware



Strategic

Tactical

Resilience strategy

Business defines crown jewels/BIA/ processes/ dependencies/ incident response plan/playbook

Containment strategy

Prioritization strategy

Restoration strategy

People, planning and exercise

Operational resilience

Resilience strategy ransomware framework

Ransomware Resilience Strategy

Vision: The business will continue to function during a ransomware attack

Top cyber risks

- **Ransomware/malware** attack on critical systems/data

…

…

Business priorities

- Reduce the cost of operations
- Protect business processes linked to revenue
- Reduce unplanned costs (e.g., legal and consulting)

…

…

Tactical strategies

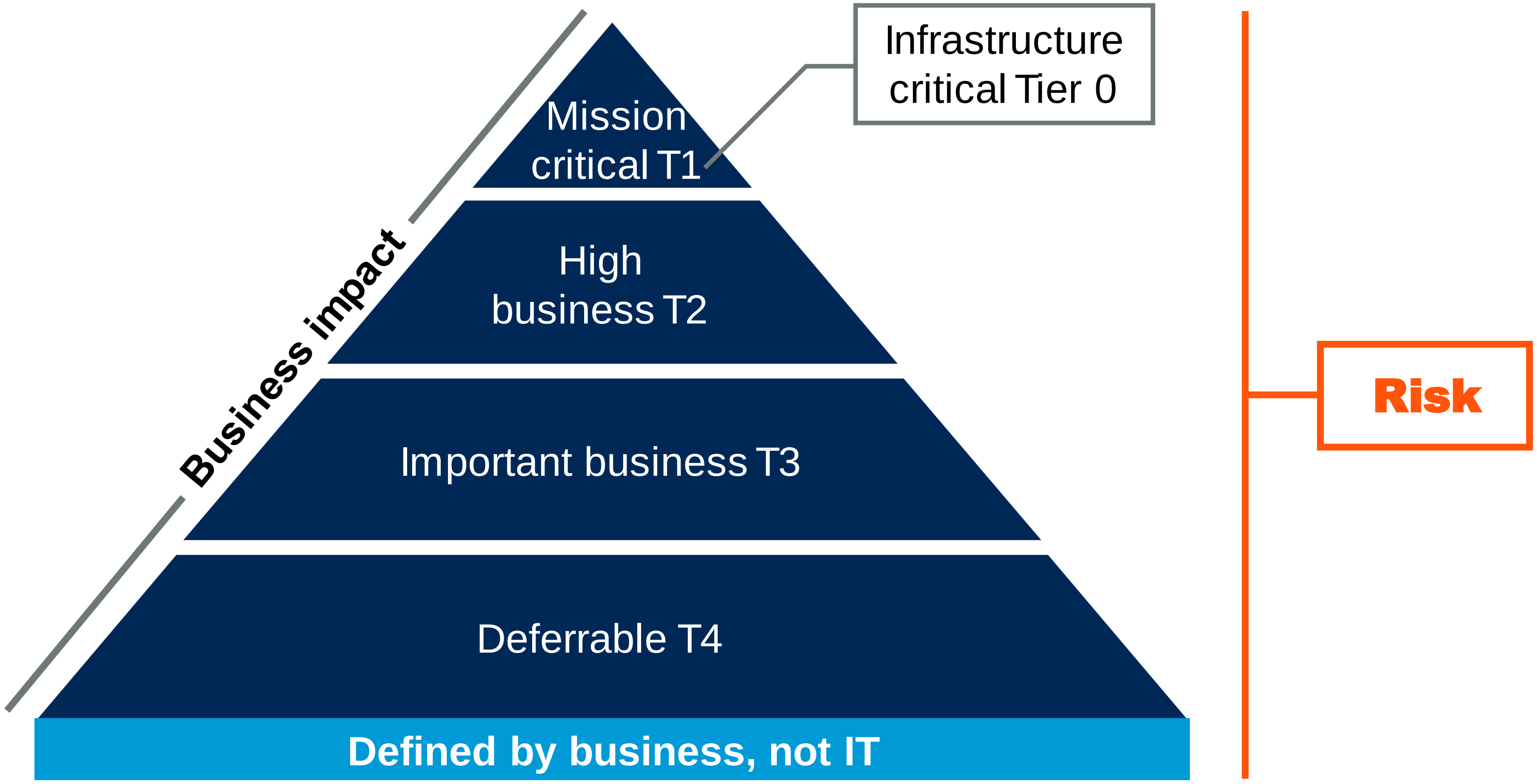
- Crown jewels strategy
- Containment strategy
- Prioritization strategy
- Restoration strategy

First: Resilience Is an All of Enterprise Initiative

Resilience component	Typical organizational role
Resilience program, framework, metrics	CRO; COO; CFO; resilience leader
Cyber resilience	CISO; business continuity leader
Supply chain resilience	Supply chain leader; procurement
IT resilience	CIO
Cloud resilience	CIO
Data resilience	CIO
Infrastructure resilience	CIO
Operational resilience	CRO; COO; resilience leader; BCM leader; CISO
Workforce resilience	HR leader

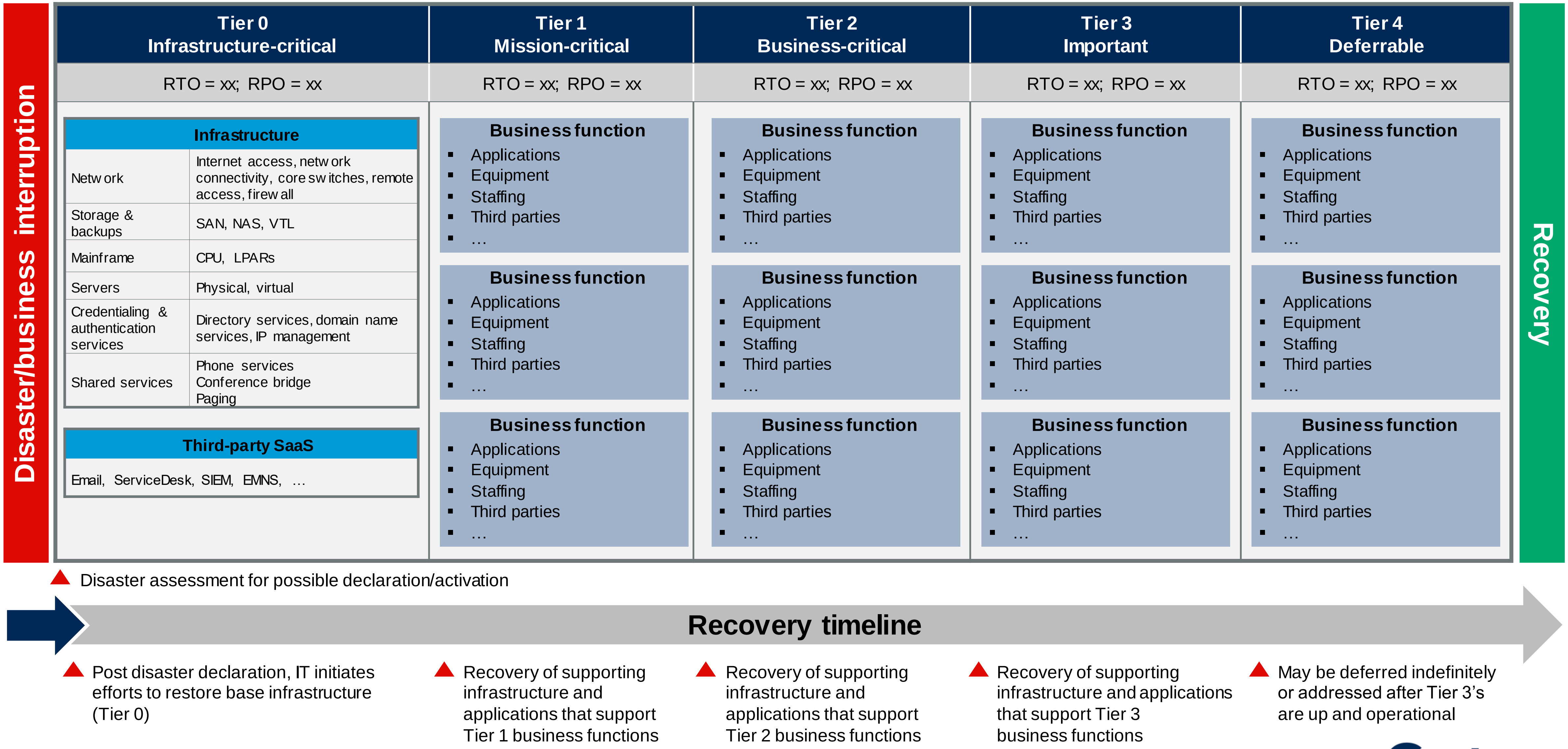
Tactical strategies: crown jewels and supporting processes

Crown Jewels (Business Functions)



IT and cybersecurity: chartered to protect crown jewels

Business Impact Analysis Enables a Sound Strategy



Disaster/business interruption

Tier 0 Infrastructure-critical	Tier 1 Mission-critical	Tier 2 Business-critical	Tier 3 Important	Tier 4 Deferrable
RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx

Tier 0

Infrastructure	
Network	Internet access, network connectivity, core switches, remote access, firewall
Storage & backups	SAN, NAS, VTL
Mainframe	CPU, LPARs
Servers	Physical, virtual
Credentialing & authentication services	Directory services, domain name services, IP management
Shared services	Phone services Conference bridge Paging

Third-party SaaS
Email, ServiceDesk, SIEM, EMNS, …

Tiers 1–4

Tier 1	Tier 2	Tier 3	Tier 4
Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …

Recovery

▲ Disaster assessment for possible declaration/activation

Recovery timeline

▲ Post disaster declaration, IT initiates efforts to restore base infrastructure (Tier 0)

▲ Recovery of supporting infrastructure and applications that support Tier 1 business functions

▲ Recovery of supporting infrastructure and applications that support Tier 2 business functions

▲ Recovery of supporting infrastructure and applications that support Tier 3 business functions

▲ May be deferred indefinitely or addressed after Tier 3's are up and operational

Business Impact Analysis Enables a Sound Strategy

<table>
<tr><th>Tier 0
Infrastructure-critical</th><th>Tier 1
Mission-critical</th><th>Tier 2
Business-critical</th><th>Tier 3
Important</th><th>Tier 4
Deferrable</th></tr>
<tr><td>RTO = xx; RPO = xx</td><td>RTO = xx; RPO = xx</td><td>RTO = xx; RPO = xx</td><td>RTO = xx; RPO = xx</td><td>RTO = xx; RPO = xx</td></tr>
<tr><td rowspan="3">
<table>
<tr><th colspan="2">Infrastructure</th></tr>
<tr><td>Network</td><td>Internet access, network connectivity, core switches, remote access, firewall</td></tr>
<tr><td>Storage & backups</td><td>SAN, NAS, VTL</td></tr>
<tr><td>Mainframe</td><td>CPU, LPARs</td></tr>
<tr><td>Servers</td><td>Physical, virtual</td></tr>
<tr><td>Credentialing & authentication services</td><td>Directory services, domain name services, IP management</td></tr>
<tr><td>Shared services</td><td>Phone services
Conference bridge
Paging</td></tr>
</table>
<table>
<tr><th>Thirs-party SaaS</th></tr>
<tr><td>Email, ServiceDesk, SIEM, EMNS, …</td></tr>
</table>
</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td></tr>
<tr>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td></tr>
<tr>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td>
<td><b>Business function</b>
▪ Applications
▪ Equipment
▪ Staffing
▪ Third parties
▪ …</td></tr>
</table>

Tactical strategies containment strategy

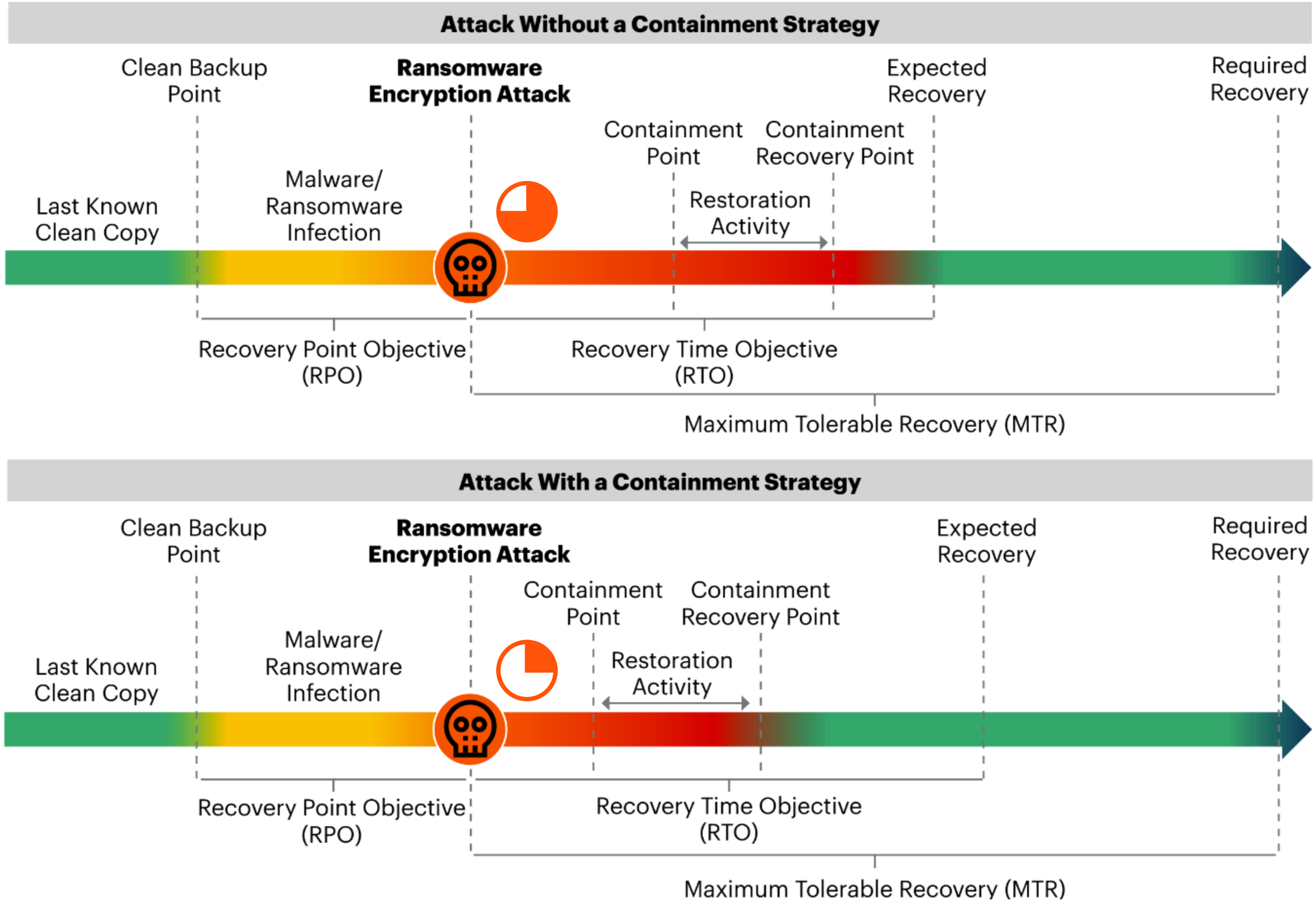
Containment Strategy

🟥 Cyber crisis 🟧 High 🟨 Medium 🟩 Low

From BIA, IRP or independent report		Restoration	Containment decision		Defined in BCP	
System	Business impact	Restoration priority	Containment risk level	Containment method	RTO	MTD
CRM	2	2	1	Isolation VLAN	24	48
Email services	4	3	3	Isolation VLAN	12	24
Directory services	4	4	4	Isolation VLAN	12	24
ERP	3	3	4	Isolation VLAN	24	48
User endpoints	1	1	1	Taken off network	None	None
Fax server	1	1	1	Physical layer isolation	None	None

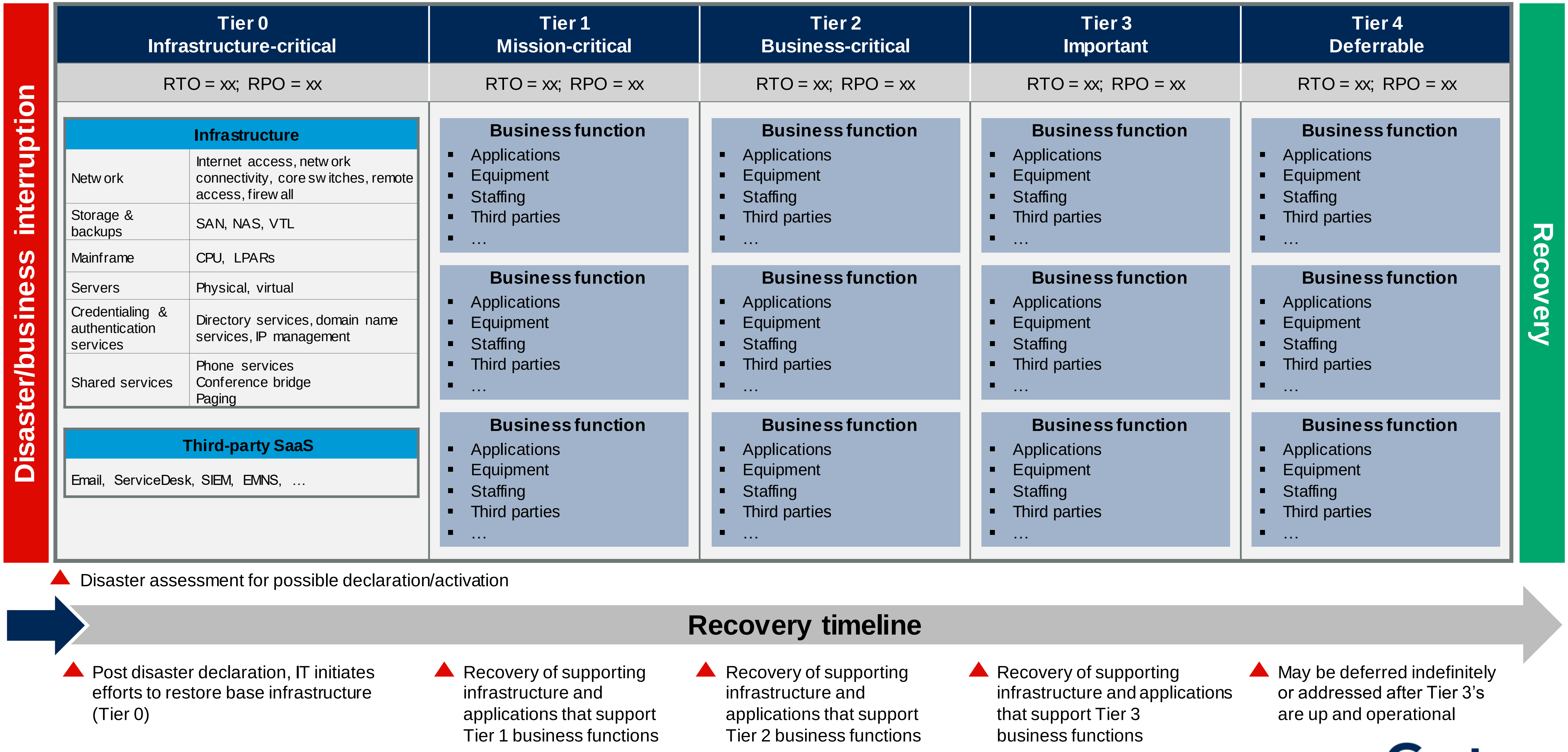
MTD = maximum tolerable downtime; IRP = incident response plan; BIA = business impact analysis

Execute Your Containment Strategy


Attack Without a Containment Strategy
Clean Backup Point
Ransomware Encryption Attack
Expected Recovery
Required Recovery
Containment Point
Containment Recovery Point
Last Known Clean Copy
Malware/ Ransomware Infection
Restoration Activity
Recovery Point Objective (RPO)
Recovery Time Objective (RTO)
Maximum Tolerable Recovery (MTR)
Attack With a Containment Strategy
Clean Backup Point
Ransomware Encryption Attack
Expected Recovery
Required Recovery
Containment Point
Containment Recovery Point
Last Known Clean Copy
Malware/ Ransomware Infection
Restoration Activity
Recovery Point Objective (RPO)
Recovery Time Objective (RTO)
Maximum Tolerable Recovery (MTR)

Tactical strategies prioritization strategy

Business Impact Analysis Enables a Sound Strategy



Disaster/business interruption

Tier 0 Infrastructure-critical	Tier 1 Mission-critical	Tier 2 Business-critical	Tier 3 Important	Tier 4 Deferrable
RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx
	Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
	Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
	Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …

Infrastructure	
Netw ork	Internet access, netw ork connectivity, core sw itches, remote access, firew all
Storage & backups	SAN, NAS, VTL
Mainframe	CPU, LPARs
Servers	Physical, virtual
Credentialing & authentication services	Directory services, domain name services, IP management
Shared services	Phone services Conference bridge Paging

Third-party SaaS
Email, ServiceDesk, SIEM, EMNS, …

Recovery

▲ Disaster assessment for possible declaration/activation

Recovery timeline

▲ Post disaster declaration, IT initiates efforts to restore base infrastructure (Tier 0)

▲ Recovery of supporting infrastructure and applications that support Tier 1 business functions

▲ Recovery of supporting infrastructure and applications that support Tier 2 business functions

▲ Recovery of supporting infrastructure and applications that support Tier 3 business functions

▲ May be deferred indefinitely or addressed after Tier 3's are up and operational

Gartner

Business Impact Analysis:
Key to Prioritization Strategy

Disaster/business interruption

Tier 0 Infrastructure-critical	Tier 1 Mission-critical	Tier 2 Business-critical	Tier 3 Important	Tier 4 Deferrable
RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx
	Business function Score 98 ▪ Active Directory ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
	Business function Score 97 ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function Score 85** ▪ SAP ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
	Business function Score 96 ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function Score 5** ▪ Fax Server ▪ Equipment ▪ Staffing ▪ Third parties ▪ …

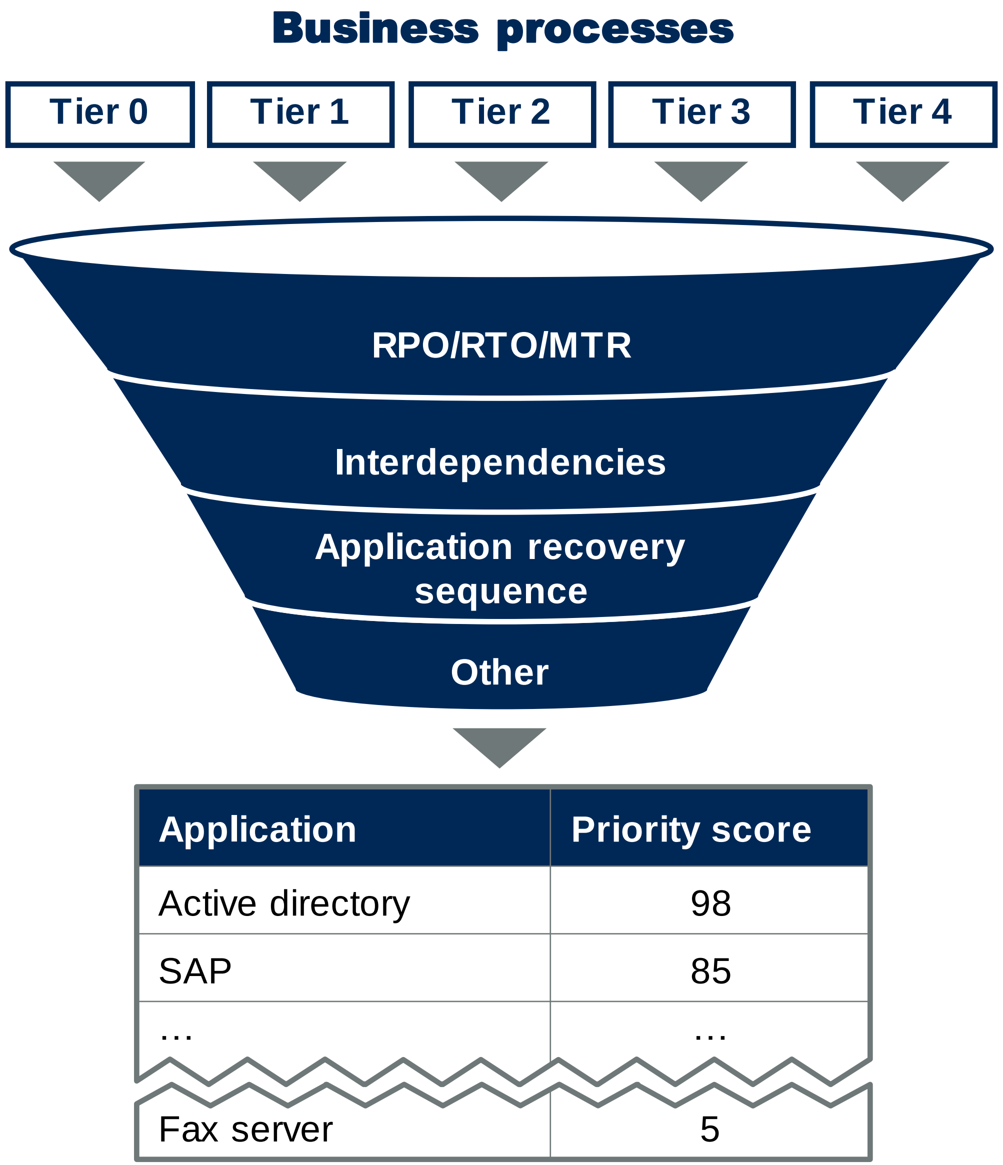
Infrastructure	
Network	Internet access, network connectivity, core switches, remote access, firewall
Storage & backups	SAN, NAS, VTL
Mainframe	CPU, LPARs
Servers	Physical, virtual
Credentialing & authentication services	Directory services, domain name services, IP management
Shared services	Phone services Conference bridge Paging

Third-party SaaS
Email, ServiceDesk, SIEM, EMNS, …

Recovery

Tactical Strategies: Prioritization Strategy

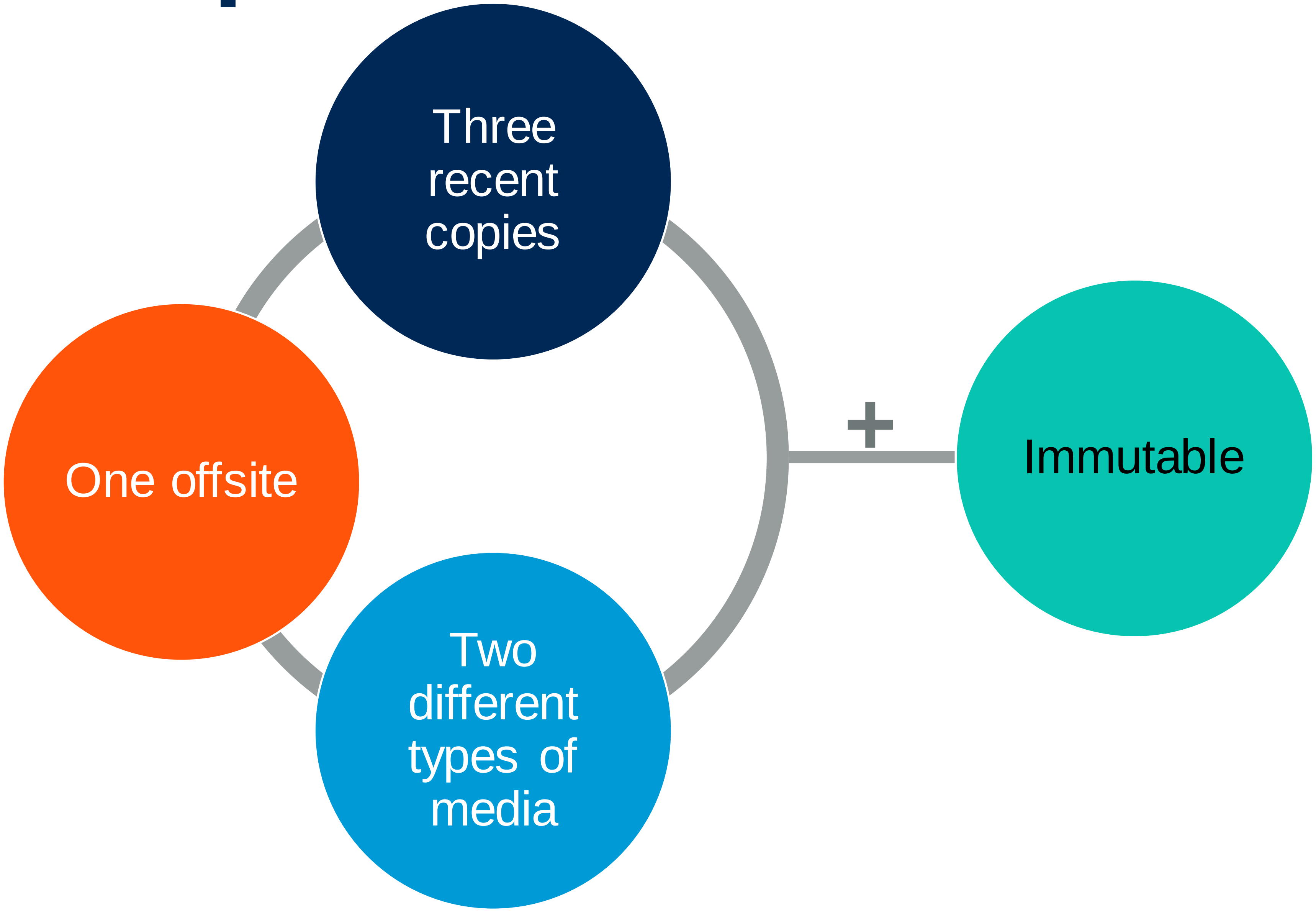
- Utilize BIA to assign business functions to tier groups.
- Associate applications with their interdependencies.
  - — Threat models
  - — Bayesian network
- Create a priority score for each system to assist in the sequence they will need to be recovered.



Application	Priority score
Active directory	98
SAP	85
…	…
Fax server	5

Tactical Strategies Restoration Strategy

Protect Backup



Business Impact Analysis Enables a Sound Strategy

Disaster/business interruption

Tier 0 Infrastructure-critical	Tier 1 Mission-critical	Tier 2 Business-critical	Tier 3 Important	Tier 4 Deferrable
RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx

Tier 0:

Infrastructure	
Network	Internet access, network connectivity, core switches, remote access, firewall
Storage & backups	SAN, NAS, VTL
Mainframe	CPU, LPARs
Servers	Physical, virtual
Credentialing & authentication services	Directory services, domain name services, IP management
Shared services	Phone services Conference bridge Paging

Third-party SaaS
Email, ServiceDesk, SIEM, EMNS, …

Tiers 1–4:

Tier 1	Tier 2	Tier 3	Tier 4
Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …
Business function ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …	**Business function** ▪ Applications ▪ Equipment ▪ Staffing ▪ Third parties ▪ …

Recovery

▲ Disaster assessment for possible declaration/activation

Recovery timeline

▲ Post disaster declaration, IT initiates efforts to restore base infrastructure (Tier 0)

▲ Recovery of supporting infrastructure and applications that support Tier 1 business functions

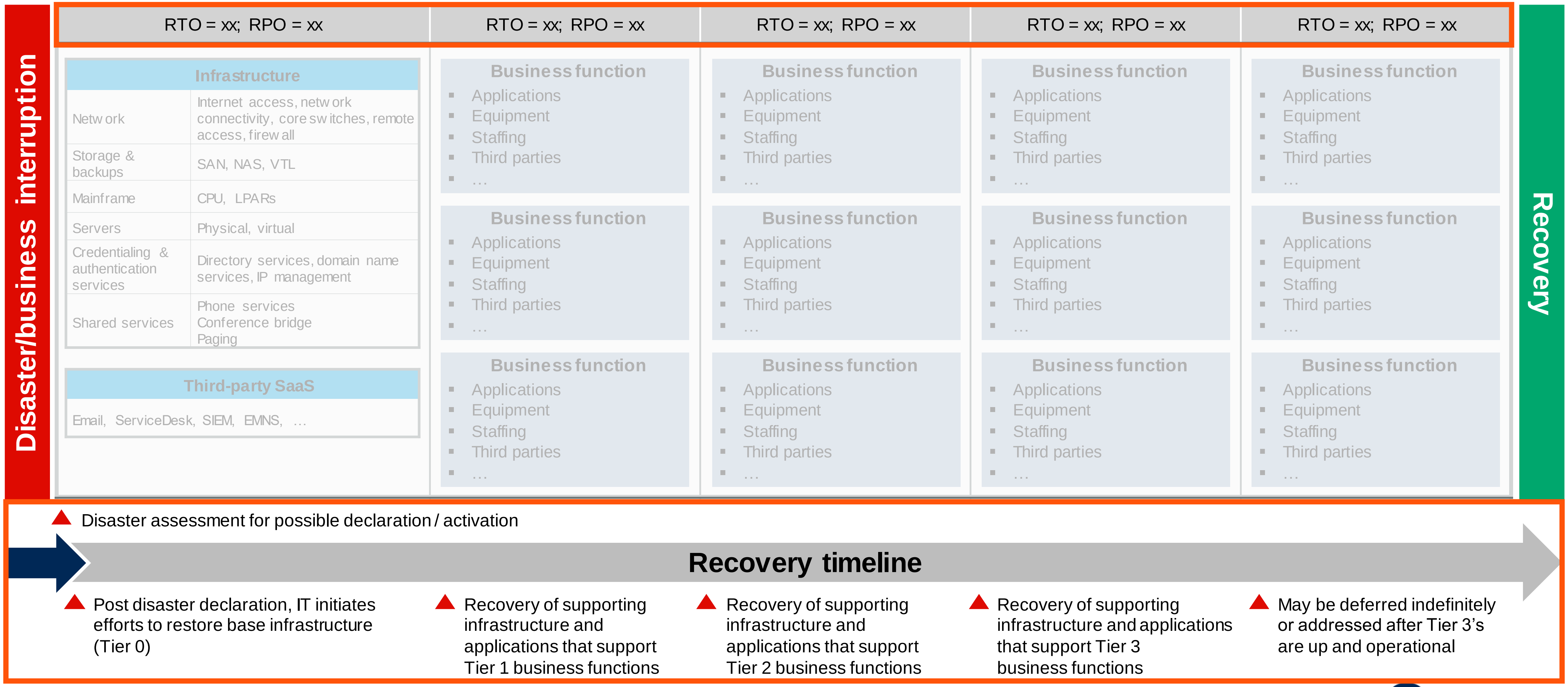
▲ Recovery of supporting infrastructure and applications that support Tier 2 business functions

▲ Recovery of supporting infrastructure and applications that support Tier 3 business functions

▲ May be deferred indefinitely or addressed after Tier 3's are up and operational

Gartner

Business Impact Analysis:
Identifies Recovery Sequence



Disaster/business interruption

RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx	RTO = xx; RPO = xx

Infrastructure

Netw ork	Internet access, netw ork connectivity, core sw itches, remote access, firew all
Storage & backups	SAN, NAS, VTL
Mainframe	CPU, LPARs
Servers	Physical, virtual
Credentialing & authentication services	Directory services, domain name services, IP management
Shared services	Phone services Conference bridge Paging

Third-party SaaS

Email, ServiceDesk, SIEM, EMNS, …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Business function
- Applications
- Equipment
- Staffing
- Third parties
- …

Recovery

▲ Disaster assessment for possible declaration / activation

Recovery timeline

▲ Post disaster declaration, IT initiates efforts to restore base infrastructure (Tier 0)

▲ Recovery of supporting infrastructure and applications that support Tier 1 business functions

▲ Recovery of supporting infrastructure and applications that support Tier 2 business functions

▲ Recovery of supporting infrastructure and applications that support Tier 3 business functions

▲ May be deferred indefinitely or addressed after Tier 3's are up and operational

Backup Strategy Is Critical, but Different With Ransomware

Differences between traditional DR and ransomware recovery

Typical differences	Traditional DR	Ransomware recovery
Recovery approach	Failover	Restore + scan or rebuild + reconstitute
Recovery location	Alternative DC	Isolated recovery environment first, production or alternative DC location second
Data loss	Per RPO	?
Recovery time	Per RTO	?
Back to business as usual	Hours/days	Weeks/months

Additional steps

- Stop attack
- Forensics
- Evidence collection
- Ransomware/negotiation decisions
- Secure/repair foundational infrastructure
- Analyze/clean backups in IRA
- Establish minimum viable environment

All hands on deck

Source: Quick Answer: Can My Disaster Recovery Plan Also Address Ransomware Recovery?

Backup Strategy Is Critical, but Different With Ransomware

Differences between traditional DR and ransomware recovery

Typical differences	Traditional DR	Ransomware recovery
Recovery approach	Failover	Restore + scan or rebuild + reconstitute
Recovery location	Alternative DC	Isolated recovery environment first, production or alternative DC location second
Data loss	Per RPO	?
Recovery time	Per RTO	?
Back to BAU	Hours/days	Weeks/months

Additional steps

- Stop attack
- Forensics
- Evidence collection
- Ransomware/negotiation decisions
- Secure/repair foundational infrastructure
- Analyze/clean backups in IRA
- Establish minimum viable environment

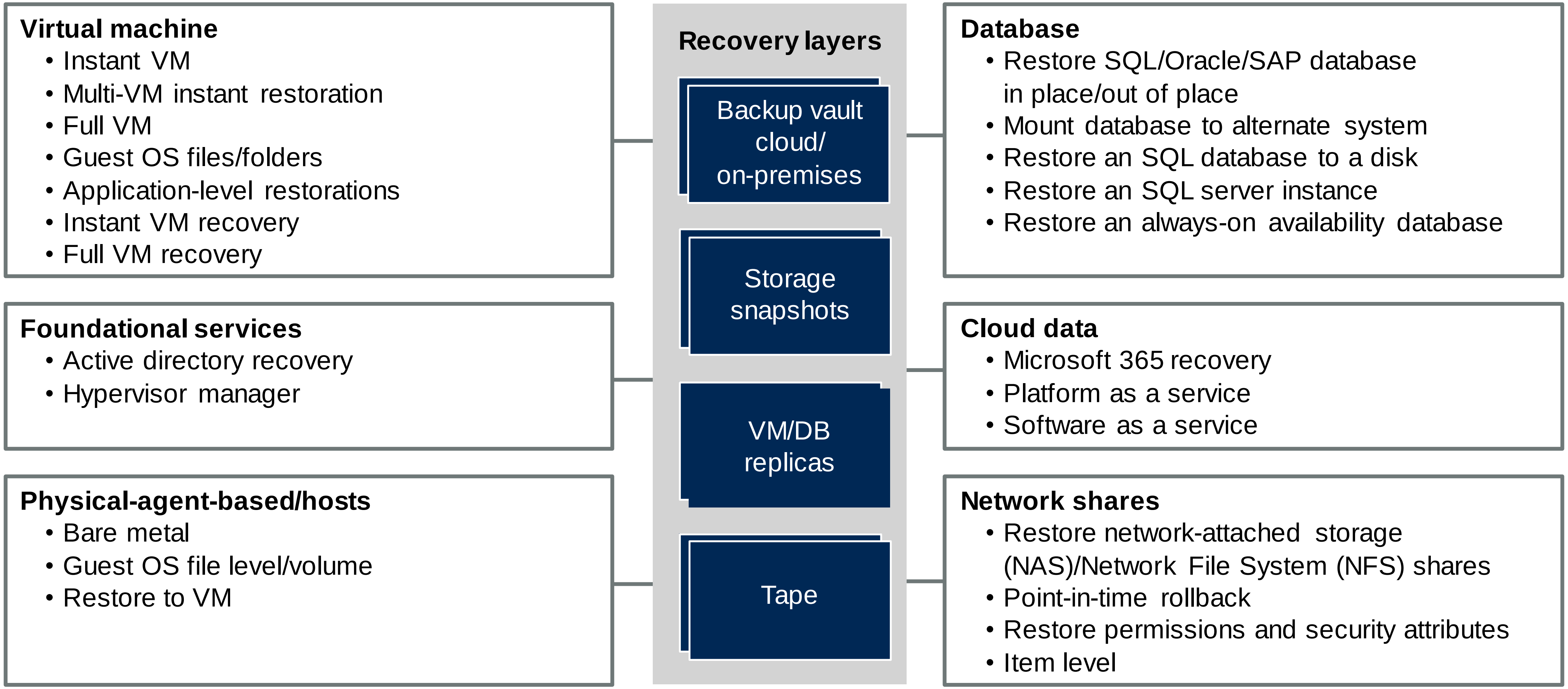
All hands on deck

Four critical elements

- Identification of critical datasets
- Protect directory services
- Establish backup target hierarchy to optimize recovery
- Align critical datasets to fast storage media

Source: Quick Answer: Can My Disaster Recovery Plan Also Address Ransomware Recovery?

Recovery Layers and Restoration Options



Virtual machine

- Instant VM
- Multi-VM instant restoration
- Full VM
- Guest OS files/folders
- Application-level restorations
- Instant VM recovery
- Full VM recovery

Foundational services

- Active directory recovery
- Hypervisor manager

Physical-agent-based/hosts

- Bare metal
- Guest OS file level/volume
- Restore to VM

Recovery layers

- Backup vault cloud/ on-premises
- Storage snapshots
- VM/DB replicas
- Tape

Database

- Restore SQL/Oracle/SAP database in place/out of place
- Mount database to alternate system
- Restore an SQL database to a disk
- Restore an SQL server instance
- Restore an always-on availability database

Cloud data

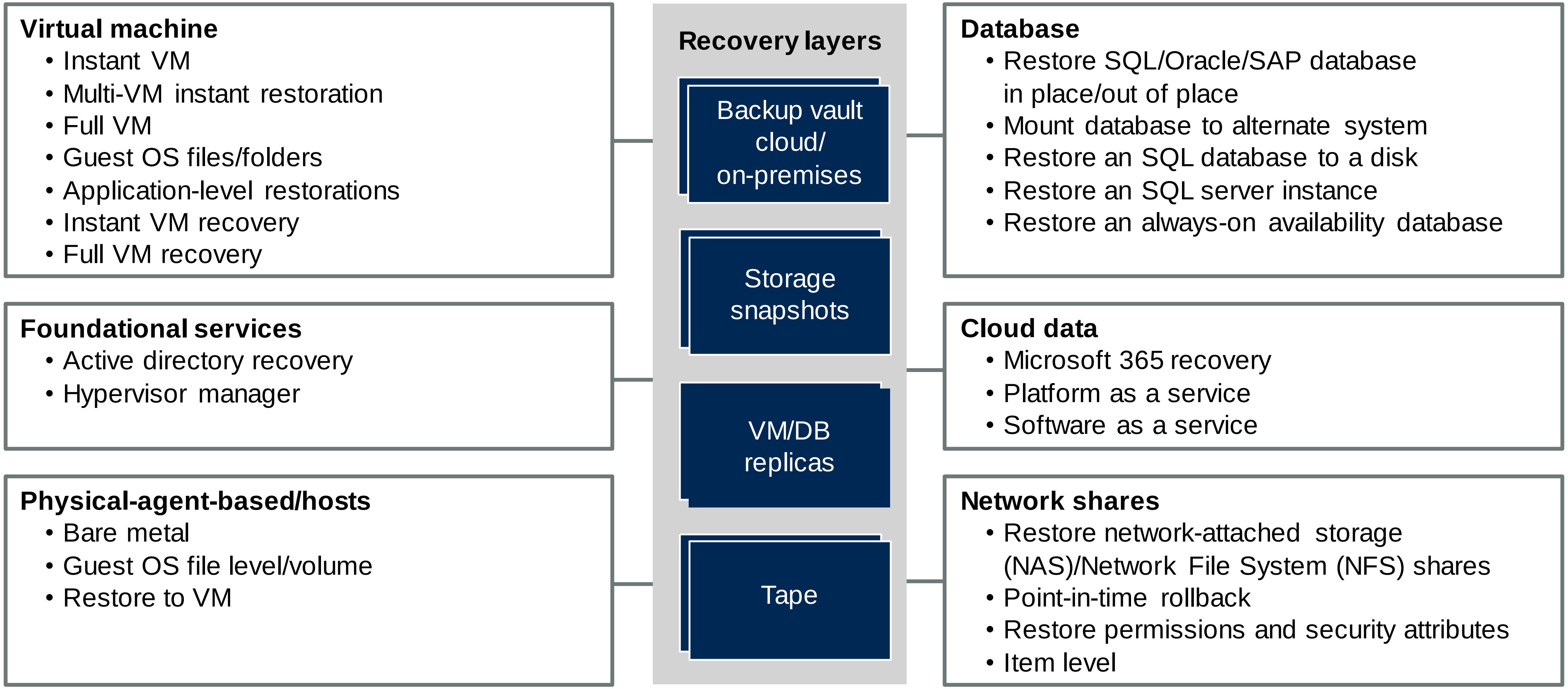
- Microsoft 365 recovery
- Platform as a service
- Software as a service

Network shares

- Restore network-attached storage (NAS)/Network File System (NFS) shares
- Point-in-time rollback
- Restore permissions and security attributes
- Item level

Source: The Gartner Framework for Ransomware Recovery

Recovery Layers and Restoration Options



Virtual machine
- Instant VM
- Multi-VM instant restoration
- Full VM
- Guest OS files/folders
- Application-level restorations
- Instant VM recovery
- Full VM recovery

Foundational services
- Active directory recovery
- Hypervisor manager

Physical-agent-based/hosts
- Bare metal
- Guest OS file level/volume
- Restore to VM

Recovery layers

Backup vault cloud/ on-premises

Storage snapshots

VM/DB replicas

Tape

Database
- Restore SQL/Oracle/SAP database in place/out of place
- Mount database to alternate system
- Restore an SQL database to a disk
- Restore an SQL server instance
- Restore an always-on availability database

Cloud data
- Microsoft 365 recovery
- Platform as a service
- Software as a service

Network shares
- Restore network-attached storage (NAS)/Network File System (NFS) shares
- Point-in-time rollback
- Restore permissions and security attributes
- Item level

Keep data transfer rates in mind

Source: The Gartner Framework for Ransomware Recovery

Additional Recommended Items to Check

- ✓ Include cyber-physical systems (OT, IoT, IIoT, Smart X) in the resilience strategy.
- ✓ Invest in stress management for your team members to increase performance.
- ✓ If there is no business continuity program, develop a cross-functional committee and ensure business owners invest in this committee.
- ✓ Again, resilience is a business initiative. Therefore, challenge business owners to develop their own playbooks to manage through a major cybersecurity incident when critical systems are unavailable.
- ✓ If there is pushback, develop a charter for a business resilience program with SR leadership signoff.
- ✓ Practice your incident response plan. The more the better.

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **Ransomware Recovery Requires a Layered Recovery Response**
  Paul Furtado and Fintan Quinn
- **Quick Answer: How Can CISOs Reduce Downtime During a Ransomware Attack?**
  Wayne Hankins and Craig Porter
- **Critical Capabilities for Enterprise Backup and Recovery Software Solutions**
  Jason Donham, Jerry Rozeman and Others
- **Toolkit: Cybersecurity Incident Response Plan**
  William Candrick, Wam Voster and Others
- **Market Guide for Enterprise Backup Storage Appliances**
  Chandra Mukhyala

Access to Gartner research is subject to individual subscription type and product entitlements.

Appendix

How to improve the base for the pillars?

People, planning and exercise

People

Your SOC and CSIRT Teams Are Stressed

67%	81%	73%	65%
Daily stress and anxiety	Ransomware has increased job pressure	Experienced burnout	Sought mental health assistance due to work

Source: 2022 IBM Security Incident Responder Study

Actively Manage Team Welfare

✓ Monitor hours and workflows to ensure individuals get rest.

Actively Manage Team Welfare

✓ Monitor hours and workflows to ensure individuals get rest.

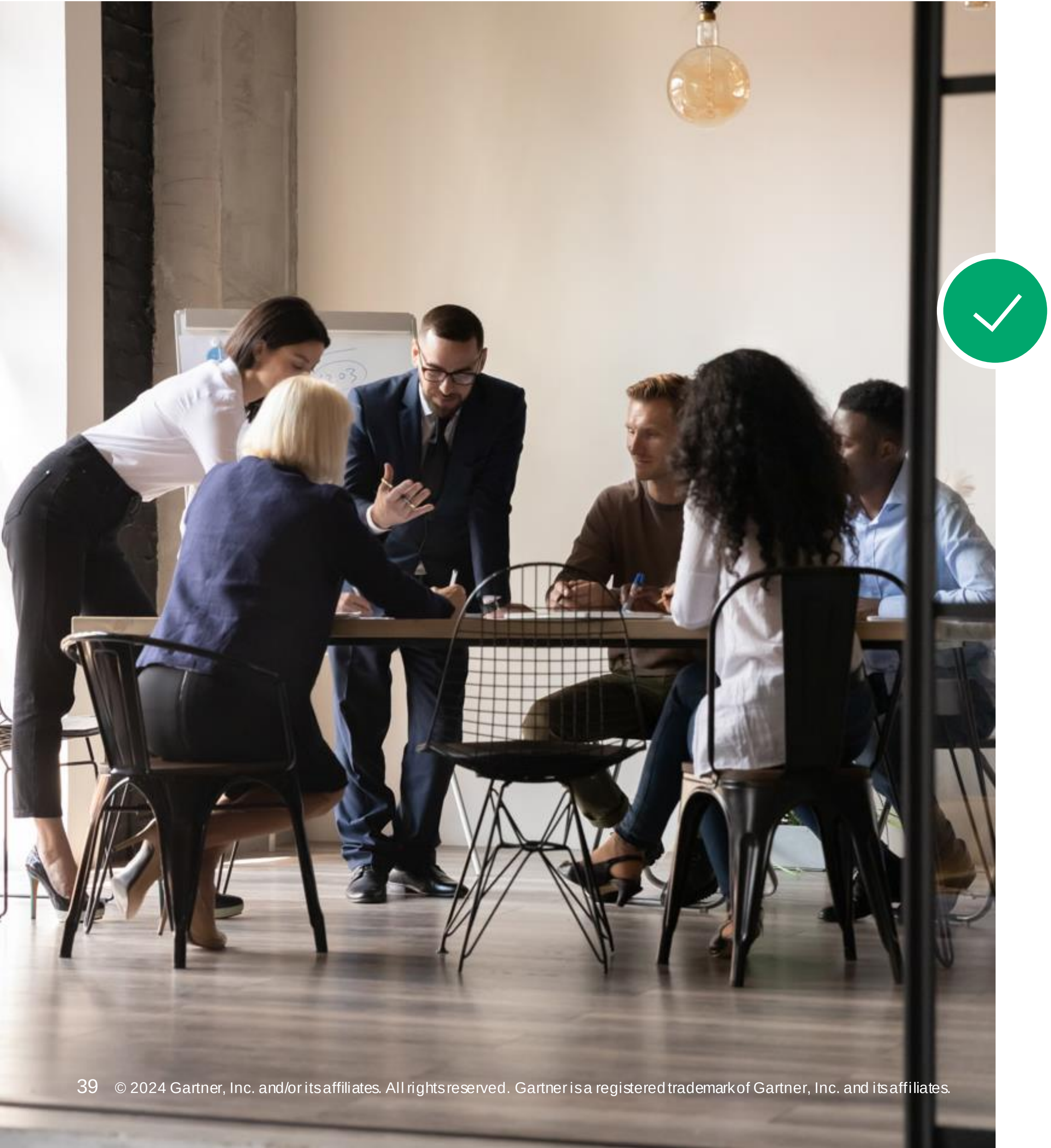
✓ Build in self-care during an active crisis, including exercise, time outside and check-ins.

Actively Manage Team Welfare

✓ Monitor hours and workflows to ensure individuals get rest.

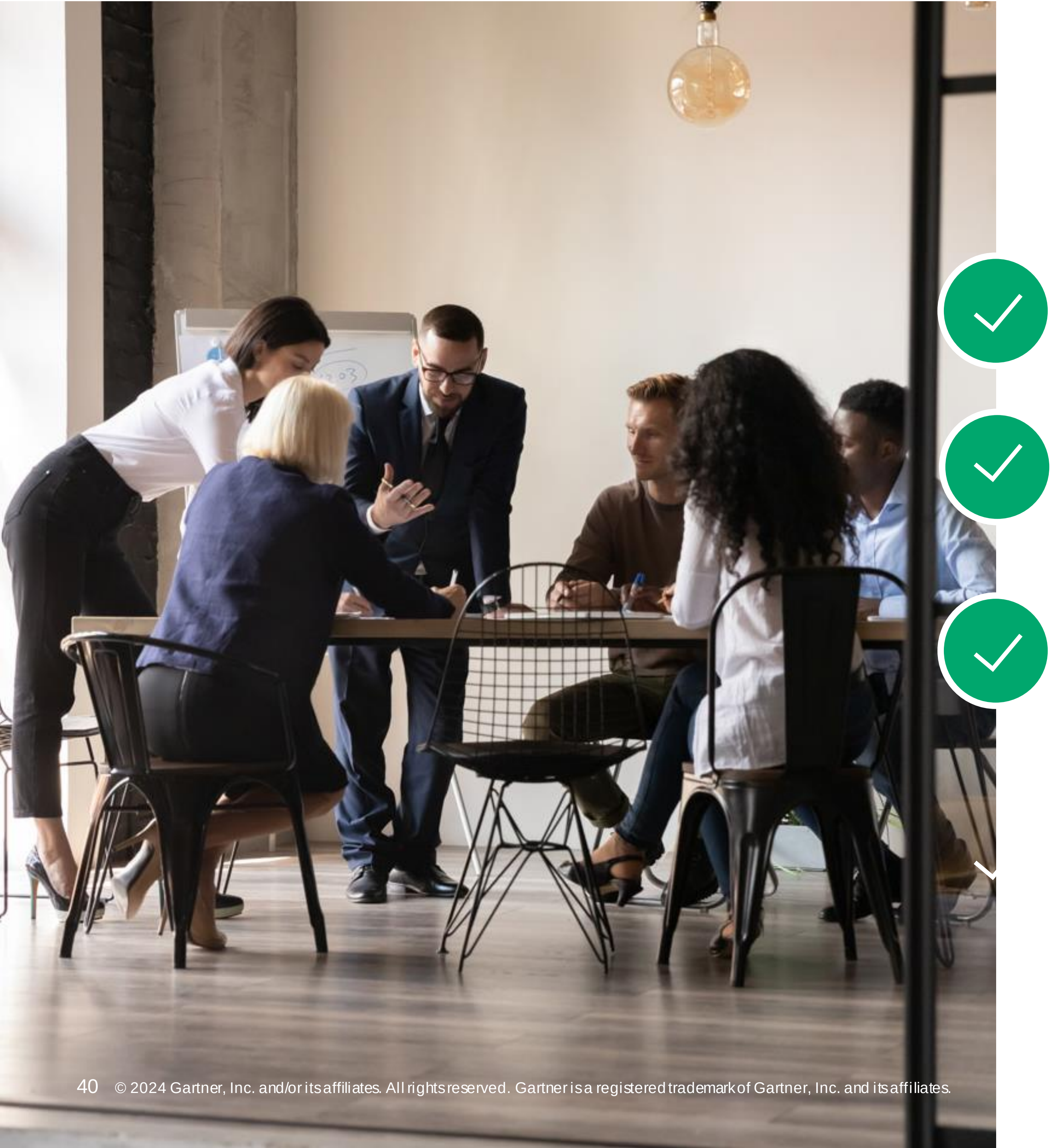
✓ Build in self-care during an active crisis, including exercise, time outside and check-ins.

✓ Celebrate wins and recognize progress.



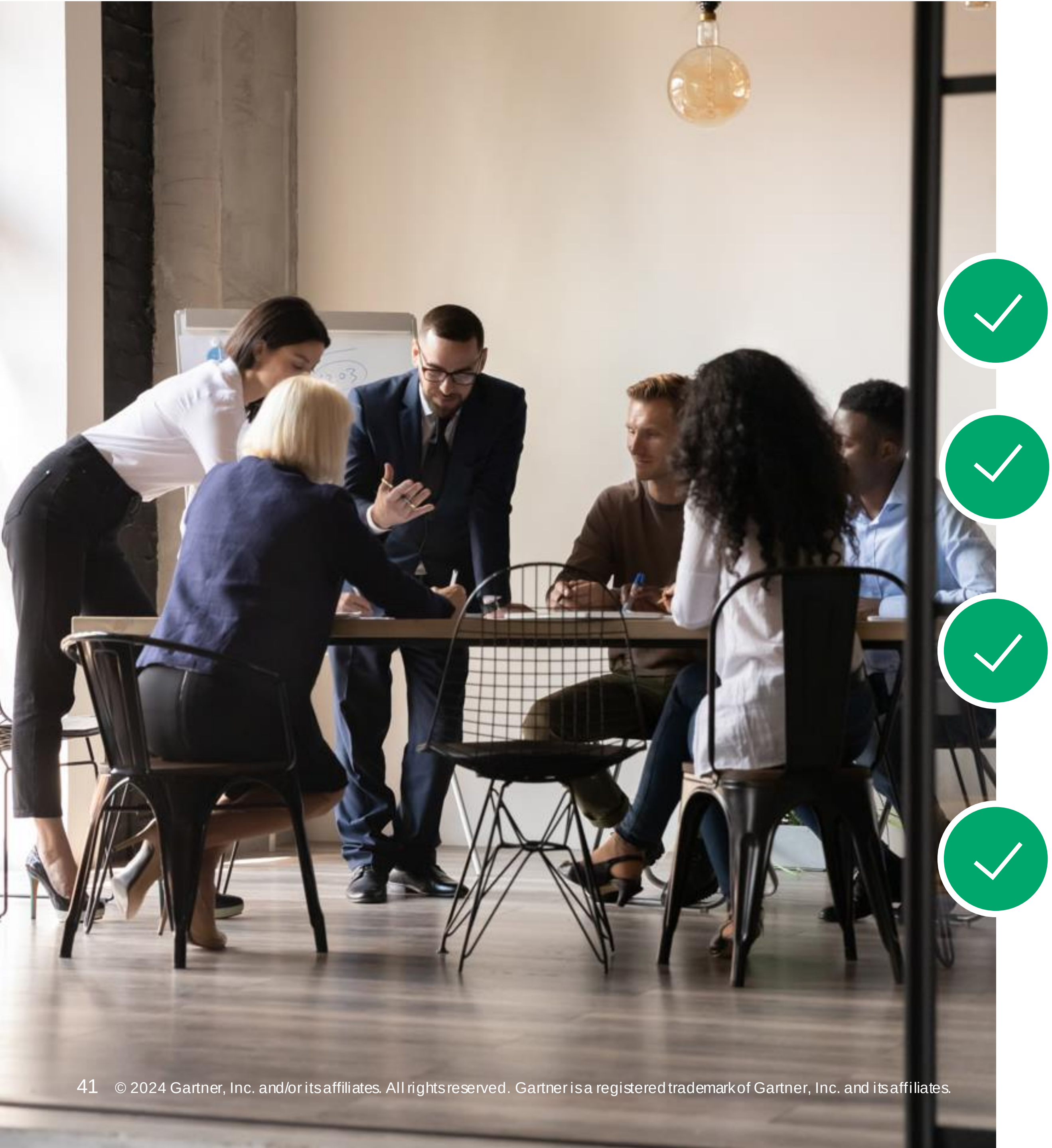
Establish an Incident Response Plan

✓ Restoration priorities.



Establish an Incident Response Plan

- ✓ Restoration priorities.
- ✓ High-level and detailed response processes.
- ✓ RACI throughout each phase of the incident.

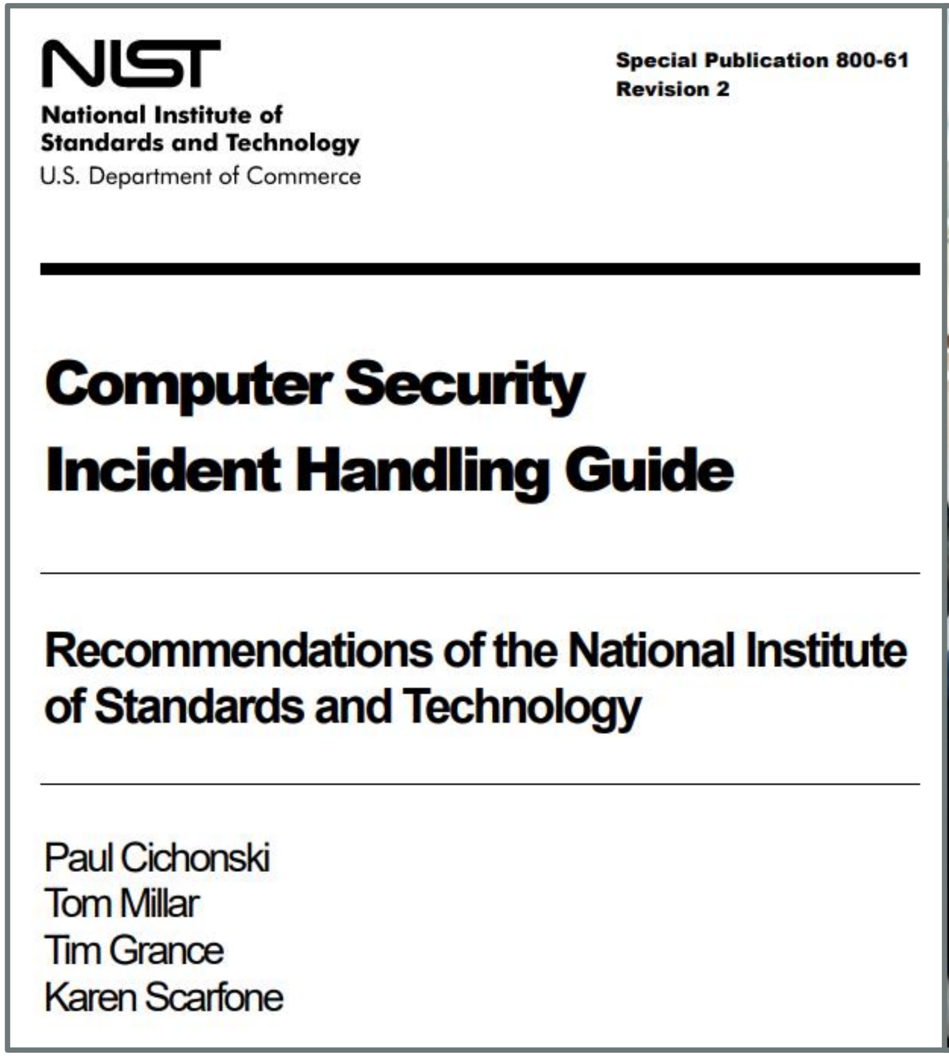


Establish an Incident Response Plan

- ✓ Restoration priorities.
- ✓ High-level and detailed response processes.
- ✓ RACI throughout each phase of the incident.
- ✓ Ransomware playbook.

Gartner®

Practice, Practice and Practice



NIST

National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

Source: Computer Security Incident Handling Guide, National Institute of Standards and Technology.