Transform Your Cybersecurity Into Cyber Resilience With These Key Controls and Metrics

David Gregory

Gartner®

Key Issues

1

The evolution from cybersecurity to cyber resilience.

2

Focus on a cyber resilience program.

3

Key issues to transform cybersecurity into cyber resilience.

Gartner

Key Issues

1

The evolution from cybersecurity to cyber resilience.

2

Focus on a cyber resilience program.

3

Key issues to transform cybersecurity into cyber resilience.

Cybersecurity is the combination of people, policies, processes and technologies employed by an enterprise to protect its cyber assets.

Source: Gartner Glossary

Gartner®

Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources.

Source: Glossary, National Institute of Standards and Technology.

Gartner

The Rise of Cyber Resilience regulations

- **European Cyber Resilience Act (CRA)**
- **Digital Operational Resilience Act (DORA)**
- **NIS 2 Directive (Directive [EU] 2022/2555)**

Digital Operational Resilience Act (DORA)

Digital operational resilience is the ability to **build, assure and review the technological operational integrity** of an organization by ensuring that the organization can support the continued provision of services and their quality in the face of operational disruptions affecting its **information and communication technologies (ICT) capabilities.**

Plethora of Resilience Frameworks

Organizational/operational resilience

- ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes (2017)
- Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA), Bank of England (BOE) Operational Resilience
- Federal Reserve, Office of Comptroller, FDIC Interagency Paper – Strengthening Operational Resilience
- FFIEC Operational Resilience
- Digital Operational Resilience Act (DORA)
- APRA Prudential Standard CPS 230 Operational Risk Management (2023)
- Office of the Superintendent of Financial Institutions (OSFI): Operational Risk and Resilience (2023)
- Basel Committee on Banking Supervision (BCBS): Principles of Operational Resilience
- Central Bank of Ireland (CBI) Cross Industry Guidance on Operational Resilience (2021)
- Hong Kong Monetary Authority (HKMA) SPM Module OR-2 Operational Resilience (2022)
- South African Reserve Bank D10-2021 - Directive on Operational Resilience (2021)
- Vendor frameworks (e.g., Gartner, PwC, Fusion Risk Management, Protiviti, i3 Australia, ServiceNow, ICOR Organizational Resilience Framework, Carnegie Mellon CERT Resilience Management Model (CERT-RMM)

Business continuity/disaster recovery

- ISO 22301:2019 – Business continuity management systems – Reqs
- ISO 22317- Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)
- ISO 22313 - Security and resilience — business continuity management systems — Guidance on the use of ISO 22301
- ISO 22330 - Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity
- ISO 27031:2011 Information technology – Guidelines for info & communication technology (ITC) readiness for business continuity
- FFIEC Business Continuity Management Handbook
- NIST SP 800-34 – Contingency Planning Guide for Federal Information Systems
- Appendix D: Mandatory Procedures for Business Continuity Management Control (Directive on Security Management)
- NFPA 1600 Standard on Continuity, Emergency, and Crisis Management
- UAE NCEMA7000 Business Continuity Management Standard
- (FS) Saudi Arabian Monetary Authority (SAMA) Business Continuity Management Framework
- Hong Kong Monetary Authority (HKMA) TM-G-2 Business Continuity Planning (2022)
- BCI: Good Practices Guidelines – Business Continuity
- DRII: Business Continuity Management Professional Practices

Cybersecurity

- NIST SP 800-160 – Developing Cyber Resilient Systems
- NIST Cybersecurity Framework (CSF)
- U.S. Cybersecurity Maturity Model CMMC
- SEC Rules on Cybersecurity Risk Mgmt, Strategy, Gov & Incident Disclosure by Public Companies
- FFIEC: Cybersecurity Resource Guide for Financial Institutions (cyber resilience)
- Office of the Superintendent of Financial Institutions: OFSI B-13 Guideline on Technology and Cyber Risk Management
- (FS) Monetary Authority of Singapore (MAS) Notice 655 Cyber Hygiene
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- Cyber Resilience Act (CRA)
- European Banking Authority (EBA) Guidelines on ICT and SRM
- European Union NIS2 Directive
- European Banking Authority (EBA): Cyber Resilience Oversight Expectations for Financial Market Infrastructure (FS)
- European Banking Authority (EBA): TIBER-EU Testing Framework (FS)
- Financial Stability Board (FSB): Effective Practices for Cyber Incident Response and Recovery (FS)
- Federal Financial Supervisory Authority BaFin BAIT Supervisory Reqs for IT Security in Financial Institutions (2021)

Supply chain/third-party risk management

- ISO 22318 – Societal security — Business continuity management systems — Guidelines for supply chain continuity
- (FS) PRA: Outsourcing and Third-Party Risk Management
- Office of the Superintendent of Financial Institutions (OSFI) Guideline B-10 Third Party Risk Management
- European Banking Authority (EBA): Guidelines on ICT and Security Risk Management (FS)
- European Banking Authority (EBA): Guidelines on Outsourcing Arrangements (FS)
- Monetary Authority of Singapore: Guidelines on Outsourcing
- Hong Kong Insurance Authority (HKIA) Guidelines on Outsourcing
- U.S. Department of Health & Human Services: Essential Medicines Supply Chain and Manufacturing Resilience
- Organization for Economic Co-operation and Development (OECD) Framework for Supply Chain Resilience
- Interagency Report 7622, National Supply Chain Risk Management Practices for Federal Information Systems

Crisis/emergency management

- U.S. FEMA NIMS/ICS
- ISO 22320:2018 - Security and resilience - Emergency management - Guidelines for incident management
- ISO 22396:2018 – Security and resilience – Community resilience – Guidelines for supporting vulnerable persons in an emergency
- ISO 22361:2022 - Security and resilience — Crisis management — Guidelines to help any organization identify and manage a crisis
- UAE National Emergency and Crisis Management Framework

Gartner's Cyber Resilience Framework

While there are numerous definitions for resilience, many share a common shift from traditional defenses and that is the ability to absorb potential disruptions while continuing to meet service level objectives.

Gartner

Regulations continue to evolve with heightened scrutiny on cyber resilience. This will continue over the coming years.

Gartner®

Key Issues

1

The evolution from cybersecurity to cyber resilience.

2

Focus on a cyber resilience program.

3

Key issues to transform cybersecurity into cyber resilience.

Gartner

Cybersecurity View of Capabilities and Domains

CISO

Governance
- Management & operations
- Business engagement
- External collaboration

Risk & compliance
- Risk appetite
- Risk assessment
- Risk management
- Policies
- Audit & compliance
- Personnel security

Training & awareness
- End user
- Role-based

Technical testing
- Penetration testing
- Red team & scenario testing
- Application security testing
- Threat hunting

Security operations
- Cyberthreat intelligence
- Insider threat
- Log management
- Vulnerability management
- Detection & monitoring
- Active monitoring
- Deception technology
- Forensics
- Incident response

Data security
- Data classification
- Cryptographic controls
- Data management
- Disposal & retention
- Data loss prevention

I&O

IDAM
- IDAM architecture
- Access management
- Identity management
- Privileged access management (PAM)
- Authentication

Infrastructure security
- Network access control
- Network security
- Cloud services
- Cloud cryptography

Change and configuration management
- Asset management
- Configuration management
- Change management
- Documentation management

Endpoint
- Anti-malware
- Application management
- BYOD
- System hardening
- Virtualization

Facilities

Physical security
- Facilities security
- Physical access controls
- Asset security
- Secure asset maintenance
- Network cabling security

DPO/legal

Privacy
- Privacy programs
- Privacy practices

Business

Supply chain management
- Third-party controls
- Component security
- Supply chain risk
- Supply chain audit
- Third-party monitoring

Application security
- Secure development
- Secure coding practices
- Validation requirements
- Software release

Business continuity
- Backup strategy
- Business continuity management (BCM)
- Capacity management
- Business continuity and disaster recovery testing

Cyber Resilience: More Focused View

CISO

Governance
- Management & operations
- Business engagement
- External collaboration

Risk & compliance
- Risk appetite
- Risk assessment
- Risk management
- Policies
- Audit & compliance
- Personnel security

Training & awareness
- End user
- Role-based

Technical testing
- Penetration testing
- Red team & scenario testing
- Application security testing
- Threat hunting

Security operations
- Cyberthreat intelligence
- Insider threat
- Log management
- Vulnerability management
- Detection & monitoring
- Active monitoring
- Deception technology
- Forensics
- Incident response

Data security
- Data classification
- Cryptographic controls
- Data management
- Disposal & retention
- Data loss prevention

I&O

IDAM
- IDAM architecture
- Access management
- Identity management
- Privileged access management (PAM)
- Authentication

Infrastructure security
- Network access control
- Network security
- Cloud services
- Cloud cryptography

Change and configuration management
- Asset management
- Configuration management
- Change management
- Documentation management

Endpoint
- Anti-malware
- Application management
- BYOD
- System hardening
- Virtualization

Facilities

Physical security
- Facilities security
- Physical access controls
- Asset security
- Secure asset maintenance
- Network cabling security

DPO/legal

Privacy
- Privacy programs
- Privacy practices

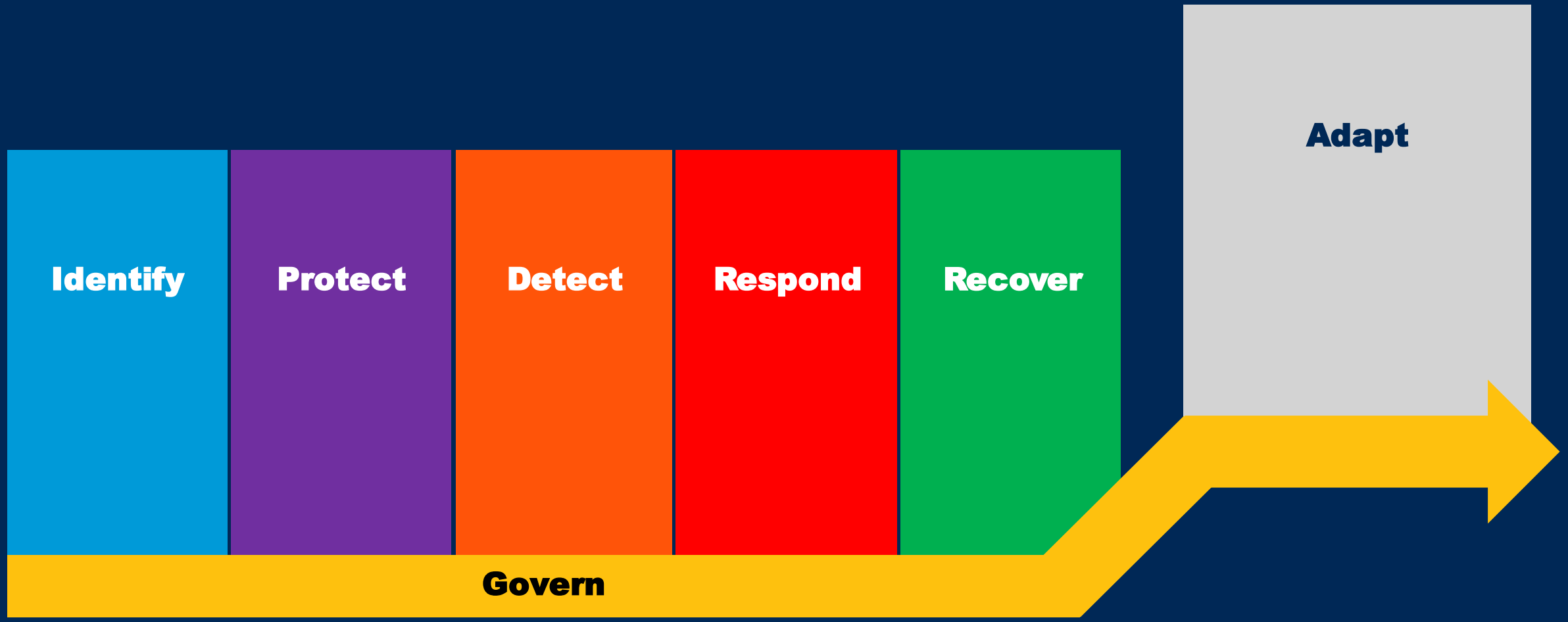
Business

Supply chain management
- Third-party controls
- Component security
- Supply chain risk
- Supply chain audit
- Third-party monitoring

Application security
- Secure development
- Secure coding practices
- Validation requirements
- Software release

Business continuity
- Backup strategy
- Business continuity management (BCM)
- Capacity management
- Business continuity and disaster recovery testing

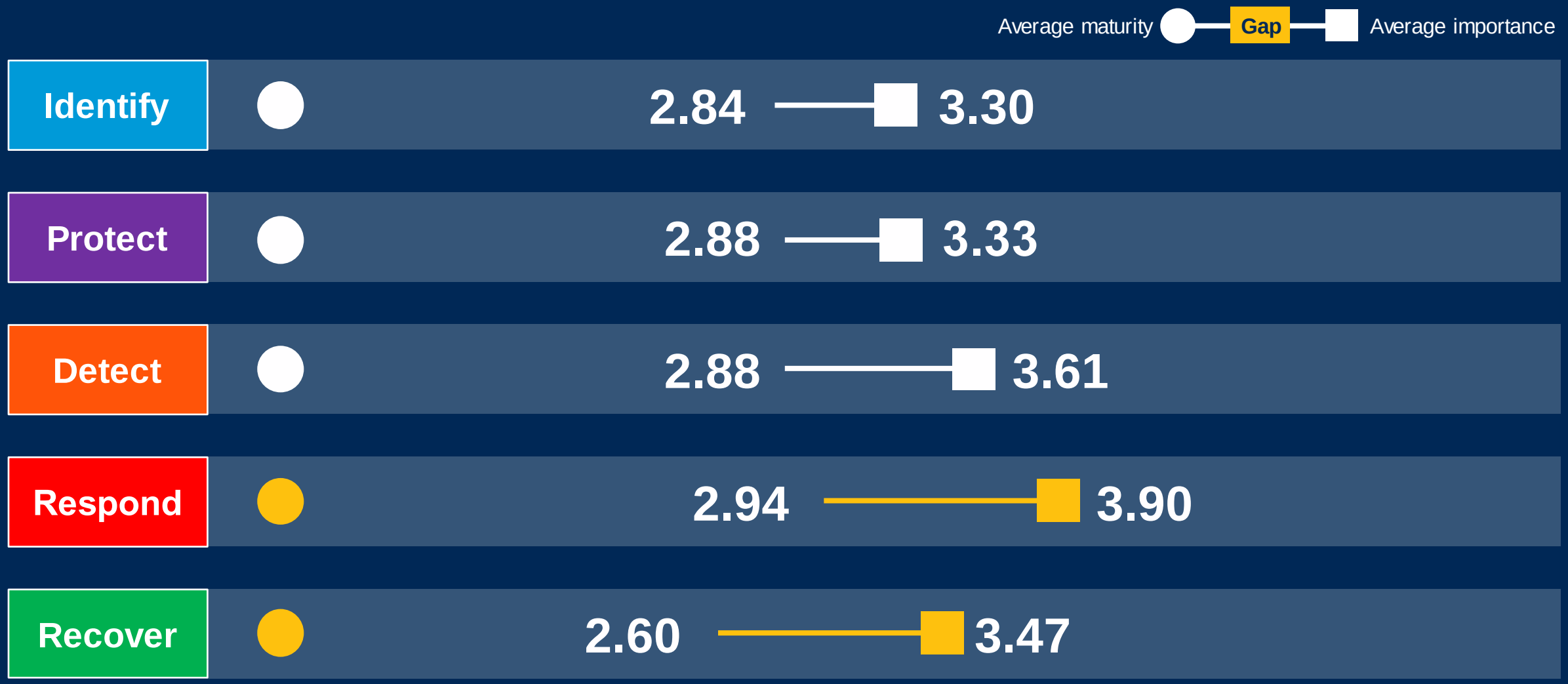
All Controls Are Required for Cyber Resilience, Especially When We Look at NIST CSF v.2.0



Source: NIST Cybersecurity Framework

Gartner®

Cybersecurity NIST CSF View



n = 506; organizations

Source: 2024 Gartner Cybersecurity Controls Assessment

Gartner

Govern — NIST CSF v.2.0

- Risk management strategy (GV.RM)
- Roles, responsibilities and authorities (GV.RR)
- Cybersecurity supply chain risk management (GV.SC)

Identify

3.07 Asset management (ID.AM)

2.69 Risk management strategy (ID.RM)

2.51 Supply chain risk management (ID.SC)

n = 506; organizations

Source: 2024 Gartner Cybersecurity Controls Assessment

Gartner

Protect

2.57	Awareness and training (PR.AT)
2.81	Information protection processes and procedures (PR.IP)
3.00	Maintenance (PR.MA)

n = 506; organizations

Source: 2024 Gartner Cybersecurity Controls Assessment

Gartner

Detect

2.97 Anomalies and events (DE.AE)

3.02 Security continuous monitoring (DE.CM)

2.71 Detection processes (DE.DP)

n = 506; organizations

Source: 2024 Gartner Cybersecurity Controls Assessment

Gartner

Respond

3.13 Response planning (RS.RP)

2.88 Communications (RS.CO)

2.84 Mitigation (RS.MI)

n = 506; organizations

Source: 2024 Gartner Cybersecurity Controls Assessment

Gartner

Recover

2.33 Recovery planning (RC.RP)

2.18 Improvements (RC.IM)

2.80 Communication (RC.CO)

n = 506; organizations

Source: 2024 Gartner Cybersecurity Controls Assessment

Gartner

All cybersecurity controls are important when it comes to cyber resilience standards and frameworks are evolving to reflect this change.

Gartner®

Gartner Cybersecurity Business Value Benchmark

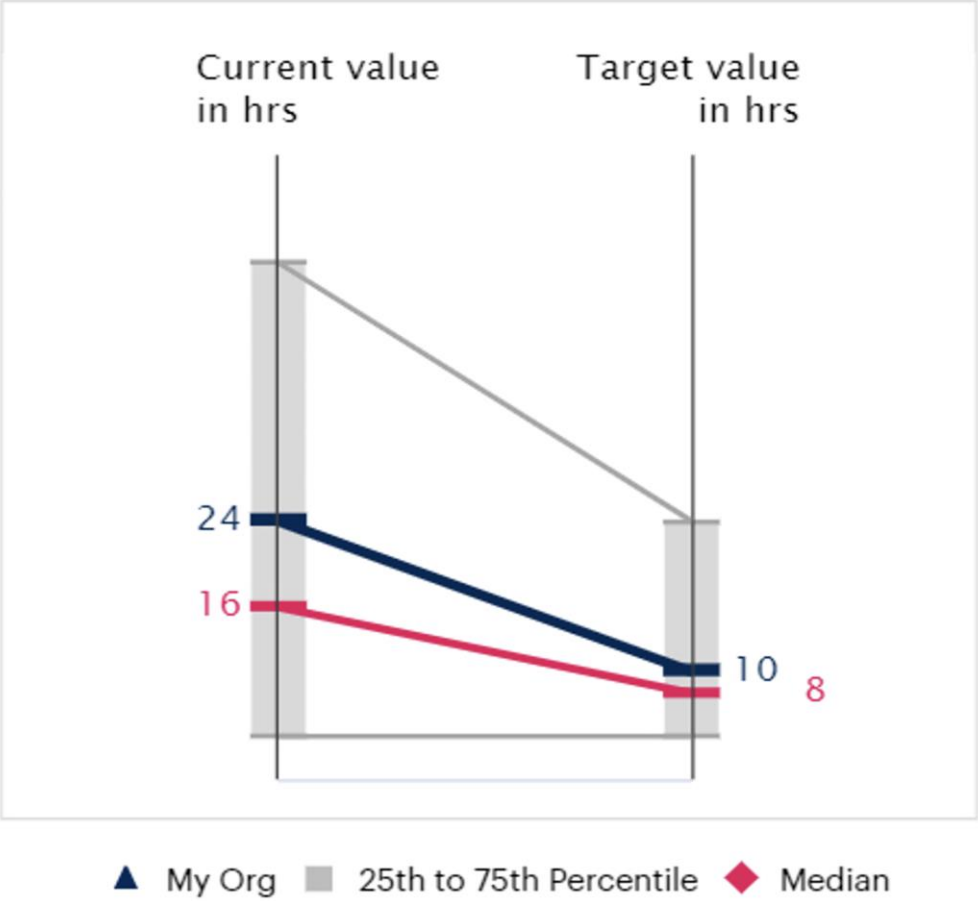
Cyber resilience metrics | Cybersecurity metrics

Incident containment time	Incident remediation time	OS patching cadence	Third-party risk engagement
Unassessed third parties	Expired policy exceptions	Endpoint protection coverage	Ransomware recovery exercise
Ransomware downtime workarounds	Cloud security coverage	Multifactor authentication coverage	Access removal time
Privileged access management	Security awareness training	Phishing training click-throughs	Phishing reporting rates

Source: The Gartner Cybersecurity Business Value Benchmark, First Generation

Incident Remediation

For critical and high-risk security incidents, what is your average time (in hours) between incident detection (ticket generation) and incident closure (ticket close)?



Benchmark comparison group: entire dataset

	Current (n = 89)	Target (n = 95)
My org status	Midleading	Midlagging
My org percentile	38th	44th
My org	**24**	10
Top peer (75th %)	4	4
Mid peer (50th %)	**16**	8
Bottom peer (25th %)	48	24

For this metric, values for improvement trend *lower*↓

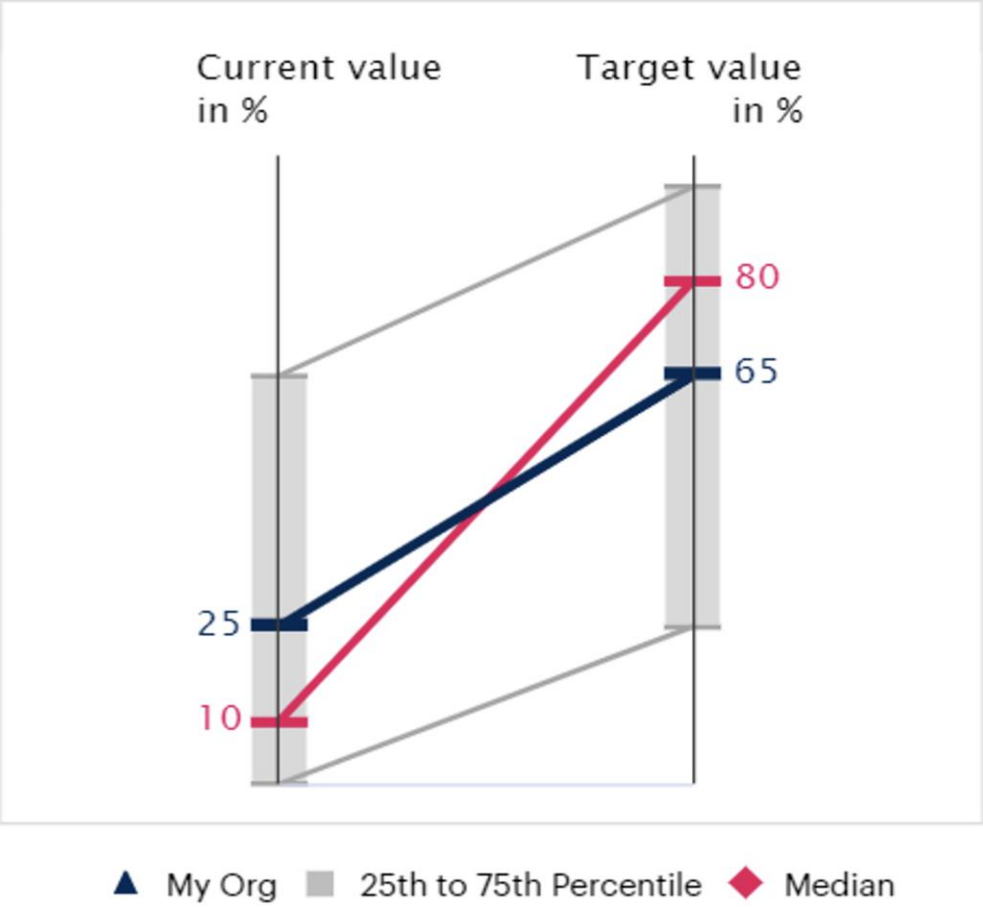
My org value(s) last updated: 10 April 2024 (current) | 10 April 2024 (target)

My org status: org percentile as compared to median

As of January 2024
Source: Gartner Benchmarks

Ransomware Recovery (Mission-Critical)

What is your percentage of mission-critical systems supporting critical business or mission functions that have successfully completed ransomware recovery exercising in the past 12 months?



Benchmark comparison group: entire dataset

	Current (n = 57)	Target (n = 59)
My org status	Midleading	Midlagging
My org percentile	60th	36th
My org	**25**	65
Top peer (75th %)	65	95
Mid peer (50th %)	**10**	80
Bottom peer (25th %)	0	25

For this metric, values for improvement trend *higher*↑

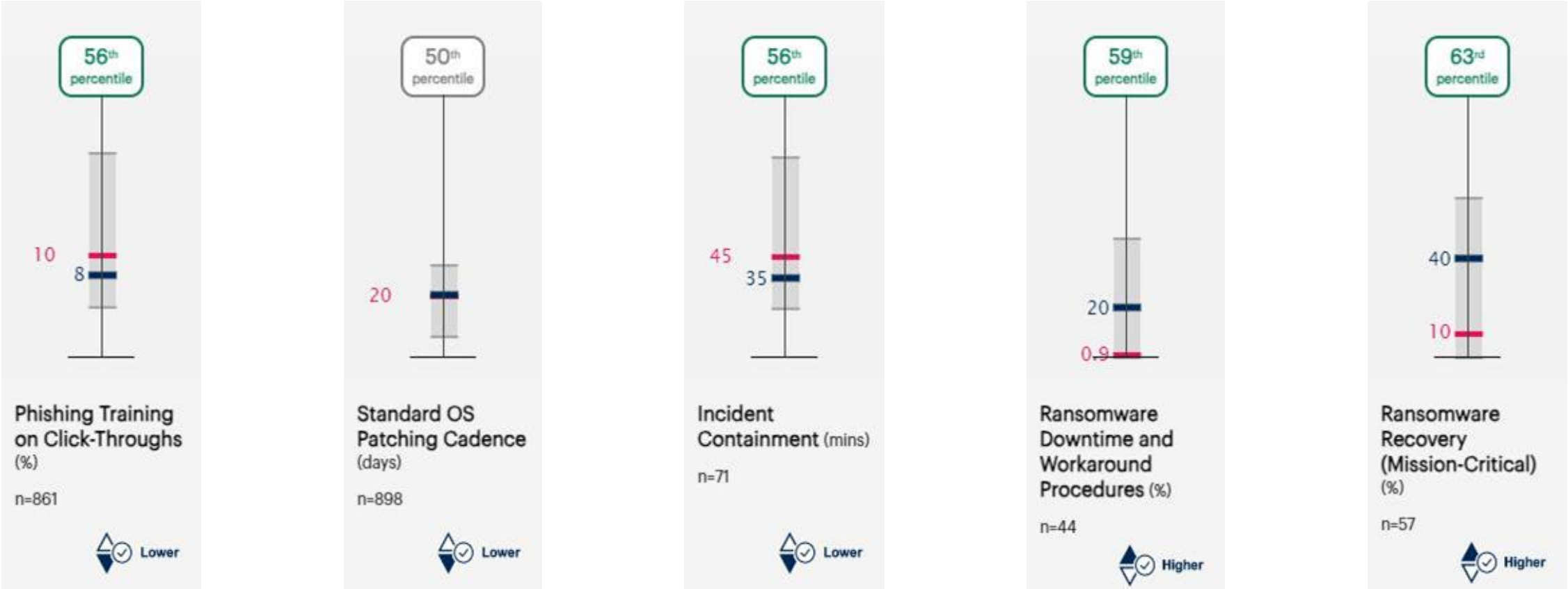
My org value(s) last updated: 10 April 2024 (current) | 10 April 2024 (target)

My org status: org percentile as compared to median

As of January 2024
Source: Gartner Benchmarks

Cyber Attack Readiness

Outcome-driven metrics for conveying readiness to address ransomware attack



My org | Median peer | 25th to 75th percentile

Better protection direction: Higher | Lower

Gartner

Key Issues

1

The evolution from cybersecurity to cyber resilience.

2

Focus on a cyber resilience program.

3

Key issues to transform cybersecurity into cyber resilience.

Gartner

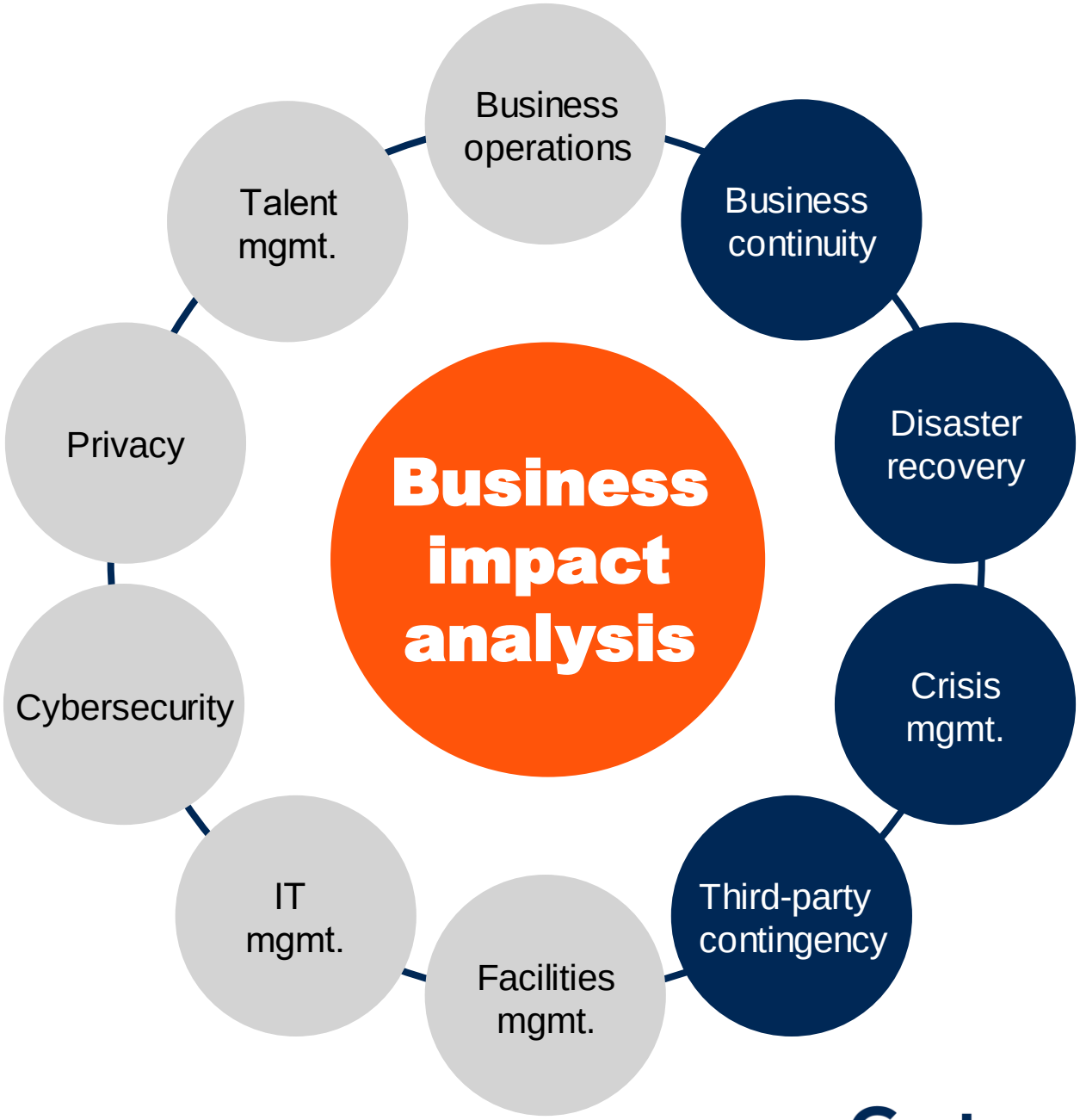
Organizational Resilience Defined

Gartner's definition of organizational resilience:

The ability of an organization to resist, absorb, recover and adapt to business disruption in an ever-changing and increasingly complex environment to enable it to deliver its objectives and rebound and prosper.

Gartner

Resilience framework: The BIA — the "center of the universe" for resilience



Cyber Resilience's Role in the Overall Organizational Resilience

Operational resilience program framework

Executive sponsorship and oversight	• Corporate policy, scope and objectives • Reporting to board and other key stakeholders	
Program governance	• Roles and responsibilities • Policy, standards and operating model • Collaboration for program activities	• Resilience metrics and KPIs • Aligned resilience reporting • Resilience program champion

Operational resilience program management office (PMO)

Human resources	Crisis mgmt.	Risk mgmt.	Business continuity	I&O/ resilience	Cyber-security	Emergency mgmt.	Third-party mgmt.	Facilities/ corp. security

Cyber Resilience Goes Beyond Controls and Metrics

- **Resilient processes:** Ensure their cyber program's critical functions are evaluated from an end-to-end value stream perspective and all requirements and dependencies are identified and strengthened.
- **Resilient people:** Focus on the hiring practices, operations and culture of their department.
- **Resilient partners:** Focus on strong relationships with other key individuals and organizations that play a critical role in their business.

Broader Cyber Resilience Metrics to Get Started …

Resilient processes

- Percentage of cybersecurity team BIAs older than 12 months.
- Backup and recovery incidents = rolling 12-month average number of material security incidents related to backup or recovery processes.
- Percentage of mission-critical cyber tool recovery plans not exercised within 12 months.
- Malware dwell time = average time malware is present before detection.
- Percentage of mission-critical cyber processes without downtime procedures.
- Disaster recovery alignment = number of business services that have recovery point and recovery time objectives that are not supported by existing IT solutions/total business services.

Cyber team

- Percentage of essential cybersecurity team members who do not have a "ready now" successor.
- Security business friction = rolling 12-month average number of help desk calls related to security program issues.
- Percentage of response and recovery team members not trained within the last 12 months.
- Crisis management exercising = number of crisis management exercises conducted within 12 months/total business services.
- Phishing business friction = number of management-reported issues related to phishing training that impact business operations/100 employees.
- Security training incidents = number of material security incidents related to behaviors covered in training.

Supply chain/third parties

- Percentage of suppliers without BCM programs/plans that support our organization's recovery needs.
- Single-source supplier/third party = number of mission-critical single-source suppliers/third parties for which the business service has no recovery plan/total suppliers/third parties.
- Percentage of third parties that are included in your resilience planning efforts.

Cyber resilience cannot be achieved by the CISO alone. There needs to be a cultural shift within the organization and functions need to work together and not in siloes.

Gartner®

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.

- **Roundup of Gartner’s Research on Organizational Resilience**
  David Gregory, Michael Aldridge and Others
- **Cybersecurity Controls Assessment**
  Arthur Sivanathan and Pedro Pablo Perea de Duenas
- **IT Resilience — 7 Tips for Improving Reliability, Tolerability and Disaster Recovery**
  Ron Blair, Belinda Wilson and Others
- **Cybersecurity Business Value Benchmark**
  Christopher Mixter, Paul Proctor and Others

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