Cyber Resilient Maturity Model

CyberRes
A Micro Focus line of business

	Level 1 Reactive	Level 2 Defined	Level 3 Managed	Level 4 Measured	Level 5 Optimized
Strategize	• No singular enterprise view on cyber risk management • No COOP for business continuity and survivability[5] • IT (or ITIL) derived information security • Reactive response to securing the business • Limited secure by design strategy • Regulatory driven • Waterfall development framework • Limited alignment with industry value chain • Limited requirements in third party contracts and Master Services Agreement • Limited user awareness programs	• Enterprise cyber risk management • Controls and regulatory-driven strategy • Cyber resiliency strategy defined and working group operational • Defined COOP[5] structure with cyber resiliency • Manually managed enterprise policies and cyber standards • Enterprise cyber Policies and standards • Agile delivery defined but not executed • Inconsistent application of cyber resiliency • Aligned with enterprise change management • Strategy limited to cyber • No cross-business integration • Regulations and compliance as a basic hygiene and embedded into processes, tools, and people	• Enterprise cyber resiliency management • Anti-fragility and business-centered growth strategy • Enterprise working group (with cyber resiliency as a vested stakeholder) • COOP[5] with defined champion and RACI model • Mission response and recovery latency recovery • Operational sustainability metrics • Cyber supply chain and third-party standards • Secure vendor management program • Cross-functional visibility into cyber resiliency • Cyber-governance framework defined • Corporate strategic goals aligned to cyber framework • Alignment to reference standards • Crisis and distressed predictive event management • Mission-aligned (critical process) tabletop war gaming	• Cyber resiliency metrics measured at the enterprise level • Board reporting of cyber resiliency related to enterprise risk management and resiliency • COOP[5] metric program instituted enterprise-wide • Cyber tied to and measured in concurrence with strategic, operational, and financial resiliency • Enterprise resiliency AI Operations-coordinated workflow • Cyber insights program • Process alignment with Agile workflow • Enterprise cyber-awareness effectiveness program (cyber resiliency tied to employee and departmental performance)	• Cross-enterprise resiliency strategic management insights and oversight • Unified enterprise crisis and distress management program • Intelligence-driven enterprise cyber user resilience program (adaptive to current global threat condition) • Enterprise resiliency tied to growth and strategy enablement • Digital transformation index reporting • Market and customer engagement performance management • Continuous cyber resiliency metrics, improvement, and transformation program
Protect	• Limited documented enterprise cyber defense framework • Protection as part of root cause analysis • Patch and release management • Vulnerability management • Infrastructure-aligned cyber defenses • Reactive application security (secure post deployment) • Incident-driven defensive measures • Limited data classification • Limited user entitlement and role models	• Defined lines of defense, roles, and operational model established • Data classification • Data loss prevention • Database encryption (TDE) • Active vulnerability management • Centralized identity management • Alignment of data classification to cyber defense • Asset management and identification • Lines-of-defense approach	• Protect value chain • Token-based data protection • Mission assurance engineering cyber defense • Intelligent and adaptive multi-layered defense • Continuous posture assessment • Defence interlock • Risk-based authentication • Zero trust • Rapid response release management • Virtual containment cyber defense • Micro segmentation	• Closed feedback loop defense analytics • SODE[3] Proactive Defense • Intelligent Zero Day (IZD[1]) • Defend-forward integrated analytics • Dynamic and context aware • Adaptive Privilege Enforcement (APE[1]) • Privilege restriction • Role and privilege continuous certification • Dynamic representation • SDN adaptive defense • Software-defined data center adaptive defense • Self-healing hypervisor (and cloud) defenses	• Anti-fragility measures (multi-layered) • Zero Latency Recovery (ZLR[1] self-healing enterprise) • Digital immunity • Distressed and strategic adversary condition proactive threat management • AI-aided predictive defense • Least-privilege automated data management • Dynamic risk-based access management • Dynamic positioning defenses • Non-persistent data processing
Detect	• Post-incident log forensics and investigative support • Vendor-provided threat models • No organizational enterprise threat management • Reactionary detective capability • Linear rules-based analysis • Search and analyze workflow • No real-time analysis • Post incident forensics capability • Log coverage limited to perimeter detection	• Managed detect and respond • Tactical threat intelligence • Gen 1 security orchestration and automation (SOAR) • Generalized threat modeling • Vertical campaign (kill chain) capability • Singular malicious code analysis • Investigative-based hunting • Higher dwell time due to reactionary detection capability • Scenario-driven threat modeling • Log coverage extended to applications and databases	• Integrated cross-functional threat operations[4] • Business value chain threat modeling • Predictive analytics • Early-warning detection program • Enterprise detect and response[2] • Gen 2 security orchestration and automation (SOAR) • Advanced intelligence • User and entity behavior analytics • Proactive hunting • Red/blue teaming • Descriptive analytics • Log coverage extended to hypervisor, flow, and instrumentation analysis	• AI Operations (integrated AI, ML, and automation centralized command) • SODE[3] proactive detection and predictive modeling • Counter-adversary threat modeling • Unsupervised detect and response (UDR1) • Integrated threat operations • Automated anonymized sector diversity and behavior, anomaly, and pattern analysis • Tier II advanced intelligence • Automated Tier 1 hunting • Counter-adversary analytics • Expanded spectrum analytics • Signals analytics and real-time Analysis • Cyber reconnaissance	• Integrated threat operations center • Cross-enterprise crisis management • Indicators tied to talent management • Adaptive threat detection • Defensive counter-adversary operations • Defensive counter-adversary analytics • Coordinated deceptive technologies • Community and ecosystem integrated joint operations
Evolve	• One-year cyber planning • Reactionary evolution of cyber maturity • Limited closed loop • Incident response limited RCA and lessons learned • No transformation and continuous improvement strategy • Annually-reconciled cyber budget • Limited mid- or long-term planning • Minimal cyber threat and trend sharing	• Three-year cyber planning • Cyber portfolio management • Enterprise resiliency funding • Evolution and strategic planning tied to digital transformation initiative • Waterfall transformation and budget allocation • Compliance-driven improvement • Threat exchange limited to observables	• Strategic enterprise resiliency transformation • Agile delivery workflow • Centralized enterprise resiliency reporting • Multi-departmental enterprise resiliency planning • Integrated cross-departmental resiliency planning • Organizational digital transformation panel • Integrated disruptive and crisis sensing • Retrospective analytics • Global distressed sensing • Threat exchange extended to behavior and trends	• Cyber resiliency allocation to performance management program • AI insights-aided cyber portfolio management • Causal analytics • Distressed predictive analytics • Cyber resiliency risk intervention analysis • Cyber resiliency transformation efficacy metrics • Threat exchange classified, tokenized, and federated	• Cyber resiliency eco-system strategy • Joint global industry trends and industry trends analysis • Intelligence and insights based on lessons learned and industry response capability • Integrated Security Response Center (Omni-Channel) • Coordinated cyber defense and takedown program • Shared cyber resiliency trust circles

1. cyberresilient.com pending trademark
2. Also known as XDR (source: Palo Alto)
3. Cyber Resilient Strategic Operational Domain Envelope
4. Also know as Cyber Fusion) from Cyber, Physical, Digital and Financial Crime Channels
5. Continuity of Operations Plan is the center of Enterprise and Cyber Resiliency that is centered around mission, business and operational continuity in times of adversities (planned and unanticipated)

Source: cyberresilient.com