



The Cybersecurity Maturity Model:

A Practical Roadmap from
Reactive to Resilient



The Cybersecurity Maturity Model

Cybersecurity maturity is not about having the most security tools. It is about having the right capabilities, processes, people, and accountability in place to consistently identify risk, prevent threats, detect attacks, respond effectively, and recover quickly.

For many companies, cybersecurity maturity develops in stages. A company may begin with basic antivirus and a firewall, add security awareness training after an incident, implement monitoring as threats increase, and eventually develop a coordinated security program tied to business objectives. The challenge is knowing where you are today and what you need to do next.

A cybersecurity maturity model provides a practical way to assess the current state of your security program and establish a roadmap for improvement. The five-level model below is designed for organizations that want to move from reactive security to a proactive, measurable, and resilient cybersecurity program.

Five Stages of Cybersecurity Maturity

01 Reactive	02 Foundational	03 Proactive	04 Managed	05 Resilient
Basic security tools; decisions follow incidents.	Documented controls deployed consistently.	Continuous monitoring and operational visibility.	Security aligned with business risk.	Security embedded throughout, with continuous improvement.

A horizontal progress bar at the bottom of the table, with a blue gradient and a white arrow pointing to the right, indicating the progression from stage 01 to 05.

Using the Checklists

Review each level and check that the capabilities are in place and operating consistently. Use unchecked items to identify gaps and plan improvements. The appropriate target depends on your business risks and operating needs.



Reactive / *"We'll deal with it when it happens"*

At Level 1, cybersecurity is largely reactive. You may have basic security technologies in place, but there is no coordinated security strategy. Security decisions are often driven by individual incidents, insurance requirements, compliance obligations, or recommendations from technology vendors.

There may be antivirus, firewalls, email security, and backups, but they are not necessarily monitored or managed consistently. Responsibility for cybersecurity may also be unclear.

Key Risk: You don't have enough visibility to understand your security gaps.

Reactive Checklist

- ☐ Basic antivirus/endpoint protection is deployed
- ☐ Firewalls are installed and configured
- ☐ Email security/spam protection is enabled
- ☐ Critical systems are backed up
- ☐ Operating systems and applications are patched periodically
- ☐ Basic password policies are in place
- ☐ Employees receive some cybersecurity guidance
- ☐ Cybersecurity responsibilities have been assigned to someone
- ☐ Critical vendors and technology providers are identified
- ☐ There is a basic process for reporting security incidents



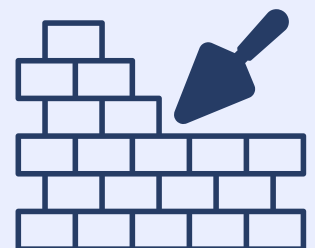
Foundational / *"We have the basics covered"*

At Level 2, you have moved beyond simply responding to incidents. Core security controls are standardized, documented, and consistently deployed. The IT team knows what devices and users it has, has established basic policies, and is beginning to manage vulnerabilities proactively. Multifactor authentication, security awareness training, endpoint detection, and more robust backup practices become standard. However, security operations may still be fragmented, and monitoring may not be continuous.

Key Risk: Controls exist, but gaps in consistency, visibility, and accountability remain.

Foundational Checklist

- ☐ Complete inventory of users, devices, applications, and critical systems
- ☐ Multifactor authentication is enabled for critical systems
- ☐ Endpoint protection/EDR is deployed across managed devices
- ☐ Security patches are monitored and prioritized
- ☐ Regular vulnerability scanning is performed
- ☐ Security awareness training is conducted regularly
- ☐ Backup strategy follows a defined retention and recovery policy
- ☐ Critical data is protected from ransomware and unauthorized access
- ☐ Administrative privileges are limited and reviewed
- ☐ Security policies are documented
- ☐ Cyber insurance/security requirements are reviewed annually
- ☐ An incident response plan has been documented



Proactive / *"We know what's happening"*

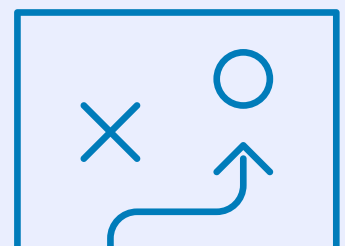
At Level 3, cybersecurity becomes an ongoing operational discipline rather than a collection of tools. IT departments have meaningful visibility into their environments and actively look for threats and vulnerabilities. Security monitoring is continuous, vulnerability management is risk-based, and incident response procedures are tested. Security leaders begin using metrics to understand trends and demonstrate progress to executives.

This is often the point where companies begin using a managed security service provider or security operations center to provide 24/7 monitoring and response capabilities that would be difficult or expensive to build internally.

Key Risk: You can detect threats, but may not yet have fully integrated security processes or mature governance.

Proactive Checklist

- ☐ 24/7 security monitoring is in place
- ☐ SIEM or equivalent security analytics capabilities are deployed
- ☐ Threat detection and response processes are established
- ☐ Vulnerability scanning covers internal and external assets
- ☐ Vulnerabilities are prioritized based on risk and exploitability
- ☐ Threat intelligence is incorporated into security operations
- ☐ Endpoint, network, identity, and cloud security data is correlated
- ☐ Incident response procedures are regularly tested
- ☐ Tabletop exercises are conducted
- ☐ Privileged access is actively monitored
- ☐ Security metrics are reported to leadership
- ☐ Third-party/vendor security risks are assessed
- ☐ Security controls are reviewed at least annually



Managed / *"Security is part of the business"*

At Level 4, cybersecurity is no longer viewed solely as an IT responsibility. It is an established component of enterprise risk management. Security decisions are aligned with business priorities, regulatory requirements, customer expectations, and the organization's risk tolerance. Leadership receives meaningful reporting, security investments are prioritized based on measurable risk, and the organization continuously tests its defenses. Zero Trust principles, identity security, cloud security, data protection, and third-party risk management are integrated into the broader program.

Key Risk: Even mature organizations must continuously adapt as technology, threats, and business operations change.

Managed Checklist

- ☐ Cybersecurity strategy is aligned with business objectives
- ☐ Executive leadership regularly reviews cybersecurity risk
- ☐ Formal risk assessments are conducted
- ☐ Security metrics and KPIs are established
- ☐ Zero Trust principles are being implemented
- ☐ Identity and privileged access are continuously managed
- ☐ Cloud environments are actively monitored and secured
- ☐ Third-party and supply-chain risks are formally managed
- ☐ Data classification and protection policies are established
- ☐ Business continuity and disaster recovery plans are tested
- ☐ Incident response plans include executive communications
- ☐ Penetration testing is performed regularly
- ☐ Security awareness is reinforced continuously
- ☐ Security investments are prioritized according to business risk



Resilient / *"We're built to withstand the attack"*

Level 5 companies recognize that preventing every cyberattack is unrealistic. The objective is resilience: reducing the probability and impact of an attack while maintaining the ability to detect, contain, respond, and recover. Cybersecurity is embedded throughout the organization. Security teams continuously evaluate emerging threats, test defenses, measure performance, and adapt controls. Advanced capabilities such as behavioral analytics, automated response, threat hunting, attack-path analysis, and continuous control validation may be incorporated where appropriate. Most importantly, cybersecurity is treated as a business enabler rather than simply a cost center.

Resilient Checklist

- ☐ Continuous security monitoring and threat hunting are established
- ☐ Security controls are continuously validated
- ☐ Automated detection and response capabilities are deployed where appropriate
- ☐ Attack paths and business-critical risks are regularly analyzed
- ☐ Threat intelligence informs security strategy
- ☐ Advanced identity and Zero Trust controls are implemented
- ☐ Critical data and systems have clearly defined recovery objectives
- ☐ Cyber recovery capabilities are regularly tested
- ☐ Incident response is exercised with executives and business leaders
- ☐ Security performance is measured against defined business outcomes
- ☐ Emerging technologies, including AI, are incorporated into security planning
- ☐ Shadow IT and shadow AI are actively monitored and governed
- ☐ The organization continuously improves its security program based on lessons learned
- ☐ Cybersecurity is incorporated into strategic business decisions



Moving up the Maturity Curve

Cybersecurity maturity is not a race to Level 5. The appropriate maturity level depends on a company's size, industry, risk profile, regulatory requirements, technology environment, and business objectives.

For many small and midsize organizations, the most important objective is to establish a strong foundation before investing in sophisticated capabilities. A company with inconsistent patching, weak identity controls, poor backup practices, or limited visibility should address those issues before pursuing advanced security technologies.

A practical roadmap follows this progression:

Transition	Priority
Level 1 to Level 2	Establish the fundamentals
Level 2 to Level 3	Gain visibility and proactive monitoring
Level 3 to Level 4	Integrate security with business risk
Level 4 to Level 5	Continuously test, adapt and improve

The most important question is not simply, "What security tools do we have?" It is: "How confident are we that our organization can prevent, detect, respond to, and recover from a cyberattack?" That answer provides a much more meaningful measure of cybersecurity maturity.

A Security Program that Evolves

Cybersecurity maturity is a journey, not a destination. Threat actors continue to evolve, cloud environments change, employees adopt new technologies, and emerging technologies such as generative AI create new opportunities and new risks. Companies that regularly assess their maturity can identify the gaps that matter most, prioritize investments, and build a security program that evolves with the business. The goal isn't to buy more security. The goal is to build a security program that is measurable, manageable, and resilient enough to protect the business when the next threat arrives.

Plan Your Next Step

Use your checklist results to focus on the gaps that matter most. Dataprise can help assess your environment and develop a roadmap aligned with your business needs.

Schedule a technology assessment at www.Dataprise.com or call **1.888.519.8111**.

