Emerging Risk Response Toolkit: Cyber Risks

2021 ERM Accelerator Toolkit Excerpt

Gartner®

Roadmap

Assess Controls, Response Efforts and Gaps

- Cybersecurity Functional Maturity
- Common and Notable Cyberthreat Examples
- Deeper Dive: Sample Interview Questions

Understand Risk Impacts

- Potential Cyber-Risk Consequences

Monitor Risk Trends in the Enterprise

- Key Magnifiers of Cyber Risk

Cybersecurity functional maturity

Customizable

Cybersecurity functional maturity can improve the efficacy of controls and risk response. Use this table to document the cybersecurity function's maturity, in consultation with the chief information security officer (CISO) or cybersecurity function's leader. The Gartner IT Score for Security and Risk Management provides CISOs with a comprehensive assessment of functional maturity in IT security and information risk.

Functional management deficiencies	Definition	How does the cybersecurity leader assess cyber-related IT functional maturity in this area?
Workforce planning	Identifying the roles, responsibilities and competencies needed by security staff to minimize potential gaps in talent readiness and prioritize future investments	
Talent recruitment	Acquiring qualified talent necessary to meet the organizational goals	
Skill development	Developing critical skills and competencies in the security staff	
Behavior and culture management	Facilitating employee awareness and culture as it relates to secure behavior	
Strategic development	Identifying strategic goals, coordinating functional plans and priorities, and executing functional plans to achieve the goals	
Budget planning	Developing and maintaining a budget to support the function's short-term and long-term plans and new capabilities	
Organizational structure	Managing decision rights and leadership roles to ensure functional and business goals are met	
Security architecture and design	Maintaining a view of IT systems and interfaces and providing guidance and recommendations for all stakeholders across the enterprise	
Policy management	Structuring and managing a policy program to ensure business requirements are met	
Performance measurement	Tracking operational metrics to provide a high-level view into the functional effectiveness	

Source: Gartner

747590

Gartner®

Common and notable cyberthreat examples (1 of 2)

Customizable

Use this table to discuss the common cyberthreat examples. Document the threat exposure, current and planned mitigation activities to manage the threat.

Threats and vectors	Definition	What is our current exposure due to this threat?	What are the ongoing mitigation activities to manage this threat?	What are the planned mitigation activities to manage this threat?
Phishing and social engineering-based attacks	Threat of information or data exfiltration (including credentials to access classified systems or communications systems, such as e-mail accounts) or unauthorized access that originates with techniques designed to trick credentialed users into taking action. This includes malware/spyware attacks, “spear phishing” (aimed at highly credentialed users, IT administrators) or “whaling” (aimed at senior executives) and attacks that use legitimate-looking but malicious webpages.			
Internet-facing service risks (including cloud services)	Threats relating to the failure of enterprises and partners/vendors to adequately secure cloud services or other internet-facing services (e.g., configuration management failure) from known threats.			
Password-related account compromises	Unauthorized users can gain access to confidential systems, data or assets by guessing passwords, often via software or a hack that reveals user passwords that users reuse. This can occur due to absence of multifactor authentication or poor access management education.			
Misuse of information	Authorized users can disseminate or otherwise misuse information or data to which they have legitimate access, either by design or by accident.			
Network-related and man-in-the-middle attacks	Attackers may be able to eavesdrop on unsecured network traffic, or redirect or interrupt traffic due to a failure to encrypt messages within and outside the organization’s firewall.			

Source: Gartner, “ATT&ACK Matrix for Enterprise,” MITRE

747590

Gartner®

Common and notable cyberthreat examples (2 of 2)

Customizable

Threats and vectors	Definition	What is our current exposure due to this threat?	What are the ongoing mitigation activities to manage this threat?	What are the planned mitigation activities to manage this threat?
Supply chain attacks	Partners, vendors or other third-party assets or systems (or code) become compromised, creating a vector to attack or exfiltrate information from enterprise systems.			
Physical medium, theft and in-person attacks	Attackers may use unauthorized access to enterprise facilities to attack enterprise systems, such as via a USB stick, or may gain access to sensitive information through theft of enterprise devices.			
Post-initial access threats	A wide variety of threats relating to additional malicious access actions (for e.g. discovering network devices) beyond the initial intrusion. (Note: Most intrusions' initial target is not the intended, ultimate target).			
Advanced persistent threats	An expert or well-resourced attacker (sometimes state-sponsored) can use advanced viruses that evade detection but linger in enterprise systems until triggered (automatically or manually by the adversary).			
Denial of service attacks	Attackers may overwhelm enterprise systems in order to cause those systems to temporarily cease functioning or function slowly, either through amassing resources outside the network (e.g. botnets) or by interrupting traffic within the network.			
Ransomware	The threat that the organization's systems might be infected with malicious software restricting access to encrypted data or systems until a ransom is paid to the perpetrator.			

Source: Gartner, "ATT&ACK Matrix for Enterprise," MITRE

747590

Gartner®

Deeper dive: Sample interview questions

Excerpted From Gartner's "2021 Audit Plan Hot Spots"

Use these questions in your interview to gain a more in-depth understanding of risk governance over topics of common concern to assurance and business leaders.

- What third parties provide critical systems or IT services, and how are they kept secure?
- How often do you conduct mock-phishing tests to see how many employees click on suspicious emails?
- What guidance have you provided to remote workers on securing home networks and appropriate security behaviors when they share their home with others?
- What steps have you taken to secure personal devices and provide guidance on employees' use of personal devices?
- What percentage of employees are assigned cybersecurity awareness training, and what is the average completion rate?
- How long, on average, does it take the organization to implement a patch after it has been released?
- How are you monitoring and tracking past-due patches within your business unit?
- How do you ensure every device has appropriate antivirus protection installed?
- How often do you check for security control weaknesses and gaps in the cloud operating environment?
- What is your protocol for addressing ransomware attacks?

Source: Gartner

747590

Gartner®

Roadmap

Assess Controls, Response Efforts and Gaps

- Cybersecurity Functional Maturity
- Common and Notable Cyberthreat Examples
- Deeper Dive: Sample Interview Questions

Understand Risk Impacts

- Potential Cyber-Risk Consequences

Monitor Risk Trends in the Enterprise

- Key Magnifiers of Cyber Risk

Potential cyber-risk consequences

Control gaps, vulnerabilities and threats can manifest in many types of negative consequences.

Consequence	Description
Data and information exfiltration	Attackers may exfiltrate confidential data or information.
Data and information manipulation	Attackers may modify data or information stored on enterprise systems.
Data and information destruction	Attackers may alter or destroy data or information in compromised systems.
System impact	Attackers may shutdown compromised systems, render them inoperable or prevent system restoration.
Account access removal	Attackers may interrupt regular operations by removing legitimate user accounts.
Denial of service	Attackers may overwhelm enterprise systems in order to cause those systems to temporarily cease functioning or function slowly, either through amassing resources outside the network (for example, botnets) or by interrupting traffic within the network.
Resource hijacking and cryptojacking	Employees or hackers may redirect or repurpose enterprise resources to perform resource-intensive computing, such as cryptocurrency mining.
Information misuse	Individuals with legitimate access to information use it in ways that are contrary to information use policies.

Source: Gartner, “ATT&ACK Matrix for Enterprise,” MITRE

747590

Gartner®

Roadmap

Assess Controls, Response Efforts and Gaps

- Cybersecurity Functional Maturity
- Common and Notable Cyberthreat Examples
- Deeper Dive: Sample Interview Questions

Understand Risk Impacts

- Potential Cyber-Risk Consequences

Monitor Risk Trends in the Enterprise

- Key Magnifiers of Cyber Risk

Gartner®

Key magnifiers of cyber risk

Key magnifiers

Unsecure employee behaviors and skills gap

Increasing sophistication of threats and poor threat sensing

Third-party vulnerabilities

Technical debt and legacy systems

Growing network, infrastructure and architectural complexity

Source: Gartner

747590

Gartner®

Key magnifiers of cyber risk

Unsecure employee behaviors and skills gap

Seventy percent of CISOs cite “lack of competent staff” as the most likely reason their company would experience a data breach.

Increasing sophistication of threats and poor threat sensing

Only 12% of C-suite leaders and IT executives are confident they would detect a sophisticated cyberattack. Further, more than 60% of assurance leaders find it hard to keep track of the growing number of information security controls and requirements in their organizations.

Third-party vulnerabilities

According to Gartner’s 2019 State of the Function Survey, 52% of the ERM heads ranked third-party data breaches as the top third-party risk.

Technical debt and legacy systems

According to Gartner’s 2020 CIO Survey, organizations that are good at removing technical debt are more likely to survive a severe information security disruption.

Growing network, infrastructure and architectural complexity

Twenty-five billion IoT connections will exist by 2025, creating a greater number and variety of connections that can be targeted by cyberattacks.

Source: Gartner

747590

Gartner®

Contact Us

Email: gartnerbusinessleaders@gartner.com
Call: 1 855 453 2113
Visit: gartner.com/en/audit-risk

Follow us on LinkedIn for daily risk, audit and legal & compliance insights:
linkedin.com/showcase/gartner-for-legal-and-compliance

Speak to a Gartner representative:
https://www.gartner.com/en/become-a-client