Gartner Research

Cyber-Risk Topic Guide for Legal Leaders

By Legal and Compliance Research Team

7 October 2021

Gartner®

Cyber-Risk Topic Guide for Legal Leaders

Published 7 October 2021 - ID G00759180 - 13 min read

By Analyst(s): Legal and Compliance Research Team

Initiatives: Enterprise Risk Management Process; Legal and Compliance Risk Management Process

This resource provides legal leaders with a guide to the fundamentals of cyber risk and its legal implications. Use this resource to better understand the key concepts underlying cyber risk and enable valuable conversations with critical internal partners.

Overview

Key Findings

- According to the Gartner View From the Board of Directors 2020 Survey, 48% of boards of directors report cyber risk as a top enterprise risk.
- Five factors magnify the impact of cyber risks:
  - Unsecure employee behavior
  - Increased threat sophistication and poor threat sensing
  - Third-party vulnerabilities
  - Technical debt and legacy systems
  - Growing network infrastructure and architectural complexity
- Cyber-risk incidents can have legal, operational, reputational and strategic implications for the organization — and these incidents are growing in number and cost.
- The responsibility of cyber-risk management is divided among multiple functions — with each function playing an independent part. However, these functions are often unaware of the totality of these risks, resulting in blind spots as each function is confined to its limited capabilities.
- Legal leaders can contribute to organizational cyber-risk management capabilities by communicating the legal and compliance implications of cyber-risk events to other functions involved.

Recommendations

To enhance the efficacy of legal and compliance risk management and the organization's cyber-risk response strategies, legal leaders should:

- Facilitate interactions with key stakeholders — including information security (IS) — and provide useful risk control assessments by communicating about the key areas of cyber risk and information risk controls.
- Assess the organization for potential cyber-risk magnifiers to identify ways to bolster cyber-risk response plans.

Introduction

This research has been adapted from "2021 ERM Risk Response Accelerator for Cyber Risks — Topic Guide: Controls, Threats and Consequences."

Controlling for cyber risks is a challenge for any organization due to the complexity of the risk landscape, the connections between cyber risk and other forms of enterprise risks, and quickly evolving threats and technologies. This research provides an overview of key cyber risk concepts and their evolution.

Cyber risk is a significant concern for organizations, with 48% of boards of directors reporting it as a top enterprise risk. [1] It is important for legal leaders to develop a baseline understanding of cyber risks because of the legal and compliance implications they carry. For example, organizations may be subject to regulatory guidelines compelling them to disclose information about a cyber-risk event to specific stakeholders within a certain amount of time. Additionally, cyber-risk events can result in data privacy risks for organizations if sensitive employee or consumer information is seized by malicious actors. These and other implications make it valuable for legal leaders to develop a basic understanding of cyber risks.

Analysis

Understand Key Elements of Cyber-Risk Management

For legal and compliance to play its role in helping the enterprise manage cyber risks, legal leaders and their teams must be familiar with, and develop a baseline understanding of, the terminology and concepts associated with cyber-risk management. These include terms and concepts in the following areas:

- IT and information system control
- IT and cyber control gaps
- Common and notable cyber and IT threats

This understanding is necessary for legal and compliance teams to contextualize their conversations with IS and IT leaders and accurately assess the threat landscape.

Building an understanding of IT and IS system control areas (see Table 1) enables legal leaders to have meaningful conversations about cybersecurity risk with subject matter experts in IT and IS.

Table 1: IT and IS Control Areas

(Enlarged table in Appendix)

Control Areas	Definitions
Network and perimeter security	A network perimeter demarcates the boundary between an organization's intranet and the external or public-facing internet. Network and perimeter security protects and monitors computer networks when sharing confidential information and data among all enterprise computing assets. Vulnerabilities in this area lead to risks involving nefarious entities, both internal and external, which can use the network to attack resources connected to the network.
Endpoint security	Endpoints are network-connected devices, such as laptops, mobile phones and servers. Endpoint security protects these assets — and, by extension, data, information or assets connected to these assets — from malicious actors or campaigns.
Applications security	Applications security protects data or code within applications, both before and after applications are deployed. This includes both cloud-based and traditional applications.
Data security	Data security comprises the processes and associated tools that protect sensitive information assets, either in transit or at rest. Data security methods include encrypting data, ensuring sensitive data is erased and creating data backups.
Identity and access management (IAM) control	IAM is the discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.

Source: Gartner (October 2021)

Advanced technologies alone are not enough to mitigate cyber risks emanating from processes, policies and people. Indeed, Gartner predicts that by 2025, more than 85% of successful attacks against enterprise users will exploit configuration and user errors in legacy systems. Legal and compliance leaders must understand potential control gaps (see Table 2) and have informed conversations with their partners in IT about the cybersecurity flaws that could result in legal risk for the organization.

Table 2: Cyber Control Gaps

(Enlarged table in Appendix)

Control Gaps	Definitions
Vulnerability discovery and remediation	The assessment for vulnerability and security configuration may be done too infrequently. Alternatively, there may be other flaws — for example, it may not be detailed enough, or it may be executed by unqualified staff.
Security event management	The monitoring of networks, systems, applications and users for security events may be done manually. Or, for example, it may not use enough data analytics, or it may have insufficiently defined levels for triggering escalation.
Security incident response	The process for managing and implementing responses to security incidents may have built-in delay, insufficient escalation procedures or insufficient segregation of duties.
Threat tracking and identification	The processes for detecting threats to the organization and managing the indicators of compromise across actors, vectors and platforms may suffer from a lack of updated information in policies. There may not be enough automation and data analytics or process mining, or there may be a lack of definitions for trigger events that should launch a larger investigation.
Managing identity life cycle	This is the process of defining, implementing and maintaining techniques to manage the identity life cycle for entities such as people, robots, services and things as well as the relationships among entities. There may not be an established process or technology to ensure identity privileges are updated in line with the duration of access required.
Authenticating identities	This is the process of defining, implementing and maintaining techniques to establish trust or confidence in the identities of, and relationships between, entities and services throughout all interactions. There may not be sufficient technology in place that enables seamless authentication across interaction types.
Managing access	This is the process of defining, implementing and maintaining techniques to enable federation, single sign-on (SSO) and runtime authorization for all entities. There may not be established processes for authorizing access for one-off or other limited instances.
Administering attributes and entitlements	This is the process of defining, implementing and maintaining techniques to ensure all entities have the proper attributes and entitlements and the quality and reliability of this information is maintained. There may be insufficient processes in place to ensure attributes and entitlements are updated regularly.

Source: Gartner (October 2021)

The extent to which organizations rely on digital information and the increased use of technology in day-to-day work have dramatically increased organizations' vulnerability to cyberthreats. At the same time, the rise of malicious activities such as data theft and denial of service is exposing organizations to more types of cyber and IT threats. Legal and compliance leaders can use examples of common cyber and IT threats (see Table 3) to better communicate with partners in IT about the specific threats that can result in legal risk.

Table 3: Common and Notable Cyberthreat Examples

(Enlarged table in Appendix)

Threats and Vectors	Definitions [2]
Phishing and social-engineering-based attacks	Information or data (including credentials to access classified systems or communications systems such as email accounts) may be exposed to exfiltration or unauthorized access that originates with techniques designed to trick credentialed users into taking action. This includes malware and spyware attacks, "spear phishing" (aimed at highly credentialed users and IT administrators) or "whaling" (aimed at senior executives), and attacks that use legitimate-looking but malicious webpages.
Internet-facing service risks (including cloud services)	Enterprises and partners or vendors may fail to adequately secure cloud services or other internet-facing services from known threats (for example, configuration management failure).
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 as a result of the 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 as a result of a failure to encrypt messages within and outside the organization's firewall.
Supply chain attacks	Partners, vendors or other third-party assets or systems (or code) can 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 (such as via a USB stick) to attack enterprise systems, or they may gain access to sensitive information through theft of enterprise devices.
Post-initial-access threats	This encompasses a wide variety of threats relating to additional malicious access actions beyond the initial intrusion (for example, discovering network devices). (Note: In most intrusions, the 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 by amassing resources outside the network (for example, botnets) or by interrupting traffic within the network.
Ransomware	Malicious software may infect an organization's systems, restricting access to encrypted data or systems until a ransom is paid to the perpetrator.

Source: Gartner (October 2021)

Control gaps, vulnerabilities and threats can lead to many types of negative consequences. Legal and compliance leaders should discuss specific consequences in scenario planning and other activities (see Table 4).

Table 4: Potential Consequences of Cyber Risks

(Enlarged table in Appendix)

Consequences	Descriptions [2]
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 shut down 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 by 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 (October 2021)

Discuss Key Magnifiers of Cyber Risk

Cyber risks are a pressing concern for organizations. Legal leaders need to understand the factors that can amplify these risks to better engage IS and IT leaders by showing how factors beyond technology and technology processes cause cyber risks. Such discussions help IS and IT leaders create comprehensive risk response plans.

The key magnifiers of cyber risks are:

- **Unsecure employee behaviors and skills gaps** — According to IBM, 70% of chief information security officers cite a lack of competent staff as the most likely reason their companies would experience a data breach. [3]
- **Increasing sophistication of threats and poor threat sensing** — According to a CSO article, only 12% of C-suite leaders and IT executives are confident they would detect a sophisticated cyberattack. [4]
- **Third-party vulnerabilities** — According to the 2020 Gartner State of the Function Survey, 52% of ERM heads ranked third-party data breach as their top third-party risk. [5]

- **Technical debt and legacy systems —** According to the Gartner 2020 CIO Survey, organizations that are good at removing technical debt are more likely to survive a severe information security disruption. [6]
- **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. [7]

Evidence

This research draws upon Gartner research across enterprise risk management, IT security and risk management and identity and access management — as well as various external news sources and data.

The definitions for most control areas, control gaps and functional management deficiencies are sourced from IT Score for Security and Risk Management and IT Score for Identity and Access Management, which are based on interactions with hundreds of Gartner clients. The definitions for most threats, vectors and consequences are adapted from the MITRE ATT&CK resource, ATT&CK Matrix for Enterprise.

Endnotes

[1] Gartner View From the Board of Directors 2020 Survey — We sought to understand how boards of directors view the impact of technology on their enterprises and their assessments of their organizations' readiness to deal with technology disruption. The primary research was conducted online from July through August 2019 among 133 respondents in the U.S., EMEA and APAC. Participating companies were verified as midsize, large or global enterprises. Respondents were required to be members of a board of directors. If they served on multiple boards, respondents answered for the largest company (defined by annual revenue) for which they are a board member. The study was developed collaboratively by Gartner analysts and the primary research team that covers digital business. Disclaimer: Results do not represent global findings or the market as a whole, but reflect the sentiment of the respondents and companies surveyed.

[2] The definitions for most threats, vectors and consequences are adapted from ATT&CK Matrix for Enterprise, MITRE.

[3] Cost of a Data Breach Report 2020, IBM Security (registration required).

[4] Top Cybersecurity Facts, Figures and Statistics, CSO.

[5] The 2020 Gartner State of the Function Survey report includes data from 171 respondents from an array of demographic bands, including industries, regional headquarters locations, revenue and ownership. Subcategories in which the sample size was greater than seven were included in analyses that examined the degree of ERM maturation within those organizations. Subcategories with fewer than seven survey responses were excluded. Banking, financial services and insurance organizations comprise the BFSI group, and the non-BFSI group includes consumer discretionary and staples, industrials and materials, energy and utilities, government and public sector, healthcare and IT and telecommunications. Some industry groups are a combination of two industries, such as industrials and materials, for purposes of statistical significance based on the sample sizes of respondents within each industry.

[6] The Gartner 2020 CIO Survey was conducted online from 4 June through 5 August 2019 among Gartner Executive Programs members and other CIOs. Qualified respondents were the most senior IT leaders (CIOs) for their overall organizations or for a part of their organizations (e.g., a business unit or region). The total sample size was 1,070, with representation from all geographies and industry sectors (public and private). Results do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[7] 5G: A Cyber-Attack Could Stop the Country, BBC News.

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Ransomware Response Beyond IT: How Legal Can Help

Corporate Digitalization and the Legal Risk Landscape

Table 1: IT and IS Control Areas

Control Areas	Definitions
Network and perimeter security	A network perimeter demarcates the boundary between an organization's intranet and the external or public-facing internet. Network and perimeter security protects and monitors computer networks when sharing confidential information and data among all enterprise computing assets. Vulnerabilities in this area lead to risks involving nefarious entities, both internal and external, which can use the network to attack resources connected to the network.
Endpoint security	Endpoints are network-connected devices, such as laptops, mobile phones and servers. Endpoint security protects these assets — and, by extension, data, information or assets connected to these assets — from malicious actors or campaigns.
Applications security	Applications security protects data or code within applications, both before and after applications are deployed. This includes both cloud-based and traditional applications.
Data security	Data security comprises the processes and associated tools that protect sensitive information assets, either in transit or at rest. Data security methods include encrypting data, ensuring sensitive data is erased and creating data backups.
Identity and access management (IAM) control	IAM is the discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly

	heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.

Source: Gartner (October 2021)

Table 2: Cyber Control Gaps

Control Gaps	Definitions
Vulnerability discovery and remediation	The assessment for vulnerability and security configuration may be done too infrequently. Alternatively, there may be other flaws — for example, it may not be detailed enough, or it may be executed by unqualified staff.
Security event management	The monitoring of networks, systems, applications and users for security events may be done manually. Or, for example, it may not use enough data analytics, or it may have insufficiently defined levels for triggering escalation.
Security incident response	The process for managing and implementing responses to security incidents may have built-in delay, insufficient escalation procedures or insufficient segregation of duties.
Threat tracking and identification	The processes for detecting threats to the organization and managing the indicators of compromise across actors, vectors and platforms may suffer from a lack of updated information in policies. There may not be enough automation and data analytics or process mining, or there may be a lack of definitions for trigger events that should launch a larger investigation.
Managing identity life cycle	This is the process of defining, implementing and maintaining techniques to manage the identity life cycle for entities such as people, robots, services and things as well as the relationships among entities. There may not be an established process or technology to ensure identity privileges are updated in line with the duration of access required.
Authenticating identities	This is the process of defining, implementing and maintaining techniques to establish trust or confidence in the identities of, and relationships between,

	entities and services throughout all interactions. There may not be sufficient technology in place that enables seamless authentication across interaction types.
Managing access	This is the process of defining, implementing and maintaining techniques to enable federation, single sign-on (SSO) and runtime authorization for all entities. There may not be established processes for authorizing access for one-off or other limited instances.
Administering attributes and entitlements	This is the process of defining, implementing and maintaining techniques to ensure all entities have the proper attributes and entitlements and the quality and reliability of this information is maintained. There may be insufficient processes in place to ensure attributes and entitlements are updated regularly.

Source: Gartner (October 2021)

Table 3: Common and Notable Cyberthreat Examples

Threats and Vectors	Definitions [2]
Phishing and social-engineering-based attacks	Information or data (including credentials to access classified systems or communications systems such as email accounts) may be exposed to exfiltration or unauthorized access that originates with techniques designed to trick credentialed users into taking action. This includes malware and spyware attacks, “spear phishing” (aimed at highly credentialed users and IT administrators) or “whaling” (aimed at senior executives), and attacks that use legitimate-looking but malicious webpages.
Internet-facing service risks (including cloud services)	Enterprises and partners or vendors may fail to adequately secure cloud services or other internet-facing services from known threats (for example, configuration management failure).
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 as a result of the 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 as a result of a failure to encrypt messages within and outside the organization’s firewall.
Supply chain attacks	Partners, vendors or other third-party assets or systems (or code) can 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 (such as via a USB stick) to attack enterprise systems, or they may gain access to sensitive information through theft of enterprise devices.
Post-initial-access threats	This encompasses a wide variety of threats relating to additional malicious access actions beyond the initial intrusion (for example, discovering network devices). (Note: In most intrusions, the 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 by amassing resources outside the network (for example, botnets) or by interrupting traffic within the network.
Ransomware	Malicious software may infect an organization's systems, restricting access to encrypted data or systems until a ransom is paid to the perpetrator.

Source: Gartner (October 2021)

Table 4: Potential Consequences of Cyber Risks

Consequences	Descriptions [2]
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 shut down 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 by 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 (October 2021)

Connect With Us

Get actionable, objective insight to deliver on your most critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Stay connected to the latest insights

Attend a Gartner webinar

View Webinars

Gartner®