Digital Risk Management Guide

How to build a cybersecurity outpost in 2025

Team international

Table of Contents

Summary

In this guide, we explore the importance of effective digital risk management and major market-driving cybersecurity trends that are useful for businesses of all sizes and across all industries. What does it take to build a security-forward company? Let's uncover key steps, essential elements, and measures you should consider when building your cybersecurity outpost in 2025.

Key takeaways

1. Leveraging disruptive technologies, such as AI, IoT, and cloud, is now imperative for organizations that strive to improve their cybersecurity posture. However, those technologies also bring their own digital risks, which you must be aware of.
2. In today's business landscape, digital threats are interconnected and more sophisticated than ever. So, your digital risk management framework should be agile, connected, and continuous as well.
3. Your cybersecurity policies must comply with all major industry regulations and legal rules to earn customers' and investors' trust alike.
4. Applying emerging cybersecurity practices and monitoring your attack surfaces is non-negotiable to stay ahead of rapidly evolving digital risks and mitigate them efficiently.
5. Risk-aware corporate culture and continuous employee training are a must-have.

The modern landscape of digital risks

We're living in a hyper-connected, futuristic world where old sci-fi books and movies are becoming a reality one by one. There are no flying cars yet, but we have humanoid AI robots, self-driving vehicles, virtual reality simulations, and much more. The major common denominator for all these rapid technological advancements is that almost every industry and every business is moving into the digital realm.

Digital business transformation is inevitable — it's a simple fact. However, with it comes the need to focus on digital (or cyber) risk management policies that will safeguard your business assets, such as data, finances, IT infrastructure, or servers. So, it's about constantly raising the bar in your organizational cybersecurity frameworks. As your corporate datasets keep growing, so should increase the integration between internal risk management and IT functions. The worst thing you can do in 2025 is to overestimate your level of cyber protection and underestimate the budget you allocate for digital risk management.

How much can it cost you to fail at digital risk management?

422.61 million data records were breached in the **Q3 2024**

Source: Statista

Only **41%** out of **1,300+** organizations actively work to mitigate cybersecurity risks

Source: McKinsey

$4.45M is the average cost of a data breach globally

Source: IBM

The variety of those risks continues to snowball, and mitigating them is a tough challenge. Even though we now have a pool of IT security automation tools that help risk professionals assess threats and manage incident response more efficiently, the role of experienced risk managers is paramount. Moreover, those managers and organizational executives must work together every step of the way. Attackers continue to develop new, more sophisticated methods for destructive hacks that infiltrate your IT system and leverage its vulnerabilities.

So, while we can't predict the future with 100 percent certainty, it's still apparent that hacking attacks won't go anywhere, and 2024 proved it. The long-term survival of your business now depends on the ability to anticipate and prevent potential operational and digital risks. Digital risk management (DRM) practices evolve, too. So, your risk officers must stay ahead of the game by anticipating emerging risks and updating DRM strategies to meet growing business needs and stakeholders' expectations.

In 2025, you should leverage the projections given by industry experts, emerging tech trends, data-driven threat analysis, and global cybersecurity insights to elaborate proactive risk mitigation plans. That's because it's no longer about 'if' but about 'when' a cyber incident happens at your company. The proactive approach will enable your cybersecurity experts to stay ahead of the most impactful global DRM trends that shape the entire risk management landscape.

The Global State of Digital Risk Management

Growth drivers for the digital risk management market

1. Skyrocketing frequency and sophistication of cyberattacks
2. Increasing regulatory compliance requirements
3. The proliferation of cloud-based solutions
4. Growing importance of proactive risk management strategies

The global DRM market was worth **$64.4B** in 2023, and is projected to hit **$157.8B** by 2028, at a CAGR of **19.6%.**

Source: MarketsandMarkets Research

Limitations that hinder the DRM market growth

1. High upfront implementation costs for DRM solutions
2. The skill shortage of qualified cybersecurity professionals
3. Integration complexities of DRM solutions
4. Rising concerns over data privacy and compliance

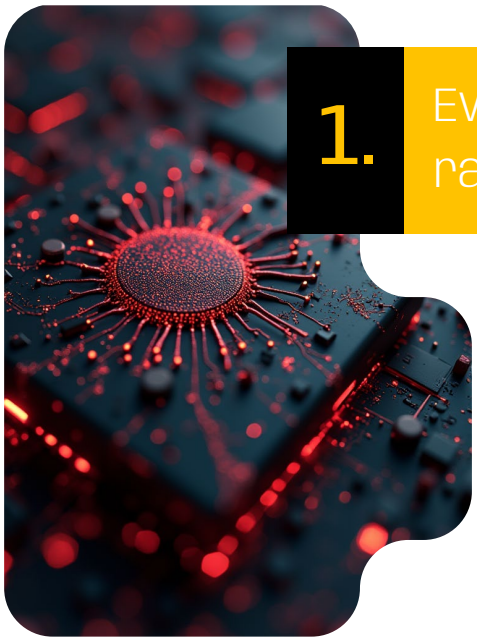
Mitigating and managing risks during uncertain times of frequent disruptions is critical to your organization's sustainability.

Top existing and emerging cybersecurity threats

The last two years broke all prior records in data breaches, and the volume of hacks directed at corporations, civil citizens, and governments only keeps growing. To avoid losing millions of dollars on managing cybersecurity incidents after they happen, you must ensure your company has everything in place to bridge the gaps and prevent data breaches in advance, both digitally and physically. Creating adaptable, agile cybersecurity protection frameworks is a must-have in the turbulent business environment and geopolitical challenges.

The international community of IT security specialists isn't silent and strives to come up with more robust cyber risk management measures to minimize downtime, reduce overall loss, and ensure business resilience. Hence, there are essential trends that dominate the DRM market, enabling faster innovation in the cyber protection space and presenting opportunities for your company to adapt to dynamic changes.

Here are the top three most prominent DRM trends that reflect the demand for more sophisticated and effective risk mitigation strategies in 2025.



1. Evolving malware and ransomware cyber threats

The world saw the first computer worm, known as the Morris worm, in 1988. And then, the first ransomware followed, PS Cyborg1, in 1989. As we've entered 2024, ransomware and social engineering attacks prevail stronger than ever before. The intent stays the same — steal valuable data and get ransom money from a victim — only the cybercriminal tactics advance.

Ransomware cyberattacks

Malware that encrypts parts of or all your data or device functions until you pay a ransom to hackers.

Phishing attacks

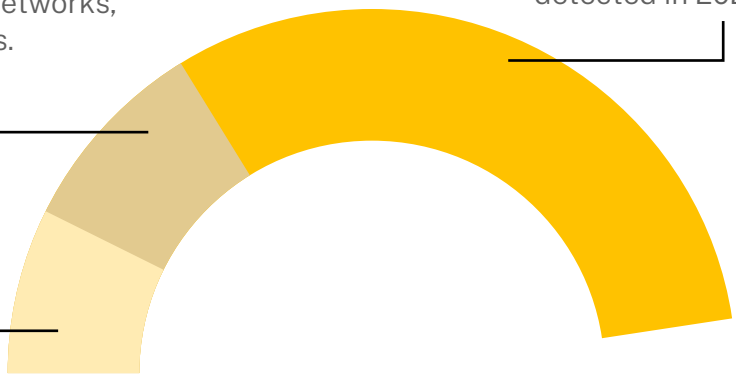
Threat actors try to exploit human errors and expose sensitive information by leveraging phone calls, impersonating a brand (or its CEO) on social media, or sending you scam emails and text messages that contain links to malicious websites.

Cryptomining malware

The practice of using malware to systematically hack machines' processing capacity and redirect it to mine cryptocurrencies by solving difficult mathematical puzzles.

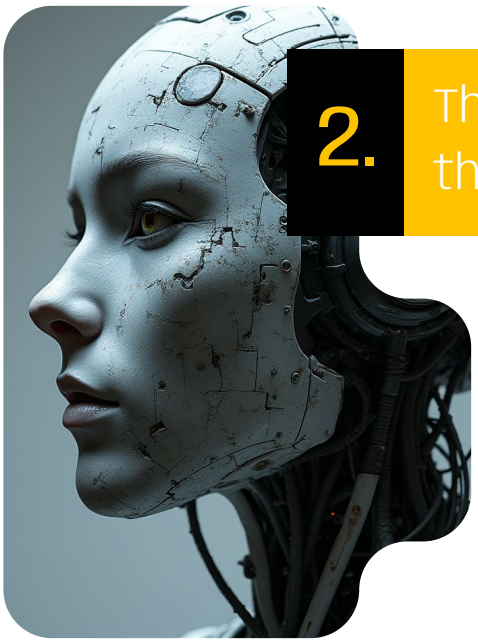
180% increase in attacks involving the exploitation of the MOVEit zero-day vulnerability and other similar ones was detected in 2024.

79% of these attacks were carried out through email, SMS, social media networks, and messaging apps.



43% of all successful attacks on organizations in 2023 used social engineering.

Source: Positive Technologies; Verizon



2. The rise of IoT and AI threats

Even though we praise emerging technological advancements for their incredibly beneficial impact on businesses worldwide, we shouldn't forget that digitalization also poses risks for anyone involved. As we employ artificial intelligence, IoT-connected devices, 5G telecommunication, and *cloud-based ecosystems,* organizations' attack surfaces expand significantly, bringing forth new vulnerabilities. The more digital assets you have, the stronger protection measures you need to safeguard them. It's a double-edged sword, yes.

When it comes to AI, let's just say that, unlike humans, tools like ChatGPT or Bard are less likely to make spelling or grammatical errors when writing phishing text or translating it into another language. So, modern social engineering messages will look a lot more realistic. Moreover, artificial intelligence allows threat actors to automate attacks and increase the complexity of their malware. On the other hand, the growing usage of IoT devices threatens your company's cybersecurity by providing attackers with many additional endpoints to breach your network.

Additionally, the pandemic drastically transformed how we work, so we now have remote and hybrid models in almost every industry. Consequently, remote access policies that regulate the use of virtual workplaces must be enforced with more robust capabilities to prevent network and device hacks. The recent wave of major government-targeting and industrial cyberattacks on high-profile targets (Solar Winds, Colonial Pipeline, OPM, Anthem, Yahoo, and others) is the perfect example of how vulnerable even market leaders can be.

Malicious phishing emails showed a **1,265%** increase in Q4 2022 when ChatGPT launched.

Source: SlashNext

78% of people opened AI-written phishing emails, and 21% clicked on malicious links or attachments.

Source: SoSafe

An **8%** surge in global weekly cyberattacks in the first half of 2023 was connected to the growing misuse of AI by bad actors.

Source: Check Point Research

3. Booming international cyberwarfare

As the wars in Ukraine and Israel continue and countries like Russia, China, and North Korea try to grasp their own piece of global power, cyberwarfare has seen a spiking activity, with *state-sponsored attacks* becoming widespread. These hacks are well-funded and holistic, encompassing national security sabotage, espionage, and massive disruptions to targeted infrastructures. Understanding your scope of geopolitical threats and developing corresponding defense and mitigation strategies is essential.

Over 30%
increase in state-sponsored cyberattacks globally was detected in 2022 compared to 2021.

Source: CrowdStrike

x2
attacks on industrial control systems doubled in 2022, with **40%** of them tied to state-sponsored bad actors looking to disrupt critical infrastructure.

Source: Positive Technologies

Top 10 industry-driving trends in digital risk management for 2025

Aside from obvious proactive steps companies now take to protect their data, such as investing in Disaster Recovery as a Service solutions, developing effective incident response plans, and implementing automated backups of mission-critical data, there are other key risk management trends that shape the corporate cybersecurity landscape.

#1 Ensuring operational resilience and business continuity

Digital risk management and organizational resilience are directly connected, so to secure the latter, you must understand how to handle the former. It means that modern businesses must include as many digital risk disruptions as possible in their business continuity and contingency plans, as well as the other way around. Hence, today, we see an increasing focus on implementing technologies and tools to build companies' resilience, diversify supply chains, and enhance crisis management. This involves AI-powered risk scenario planning and crisis communication strategies.

#2 Navigating data privacy and compliance regulations

Businesses actively capitalize on data monetization models, collecting terabytes of customer-related information. Analytics is the gold mine no one wants to lose, meaning data privacy is now one of the most critical aspects of your DRM frameworks. Regulatory compliance is mandatory to earn both customers' and stakeholders' trust as we have such prominent standards as GDPR, CCPA, HIPAA, the *Secure Artificial Intelligence Act,* the NIS2 Directive, and ISO 27001 guarding everything, from information assets to AI behavior to IT infrastructure. Moreover, data protection regulations will only tighten and evolve in the future, pushing entrepreneurs to prioritize compliance and invest in anonymization and encryption tools.

#3 Managing remote work challenges

Although some companies are slowly returning to the traditional workplace model where employees must visit offices at least three times a week, the overall paradigm shifts toward remote and hybrid work. Hence, the business world faces new risk dimensions and enlarged attack surfaces. In 2025, company executives and chief risk officers will focus on the challenges of managing remote teams and ensuring data security in distributed IT environments. It means introducing holistic risk management policies and technologies that secure both physical and virtual workspaces at the same level of protection.

Global information security and risk management spending is projected to hit over **USD 310 billion by 2028.**

Source: Statista

#4 Mitigating digital transformation risks

As we've mentioned at the beginning, the pace of *digital business transformation* has seen a tenfold acceleration. However, aside from reaping all the benefits it provides, organizations stay vigilant of a plethora of cybersecurity threats it might introduce in 2025. It means reinforcing IT infrastructures, fostering an internal culture of cyber-awareness, and embracing Gartner's continuous threat exposure management (CTEM) practices.

#5 Seizing generative AI opportunities

The duality of AI is astonishing, but we just can't escape the fact that it's a tool both cyber risk experts and bad actors use. So, here, it's about who's able to leverage it most efficiently. And businesses have no intention of backing down as they adopt *generative AI to model* novel cyber defense methods to protect their systems from penetration. Artificial intelligence powers advanced real-time threat analysis, automating routine cybersecurity tasks like compliance reporting, breach detection, and vulnerability management. Also, IT security departments are aware of such threats as AI-generated deceptive content or documents and deep fakes. With smart AI solutions, you can easily capitalize on robust predictive analytics and actionable insights for proactive threat prevention to minimize potential attacks' impact.

#6 Introducing data-driven digital risk management

Today's data availability is astonishing, and those vast amounts of information you collect daily can become great assets for innovations and advancements in corporate digital risk management driven by analytics. Real-time data analysis enables enterprises to leverage risk alerts, identify attack patterns, and practice informed decision-making. *Data-driven DRM frameworks* also operate on predictive analytics, AI and ML algorithms, and other cutting-edge technologies that allow for risk indicators monitoring, early risk detection, automated vulnerability assessment, and risk mitigation strategies adjustments.

#7 Viewing digital risks not as technical but as company risks

Another trend forward-thinking leaders follow is integrating DRM into their strategic and tactical planning. They align risk management with their business targets, internal and external, ensuring that digital risks act as essential factors in the decision-making processes. Such a holistic view of risks shows that an organization acknowledges an increasing interconnection between IT and business risk acceptance thresholds.

"You can't eliminate all risks.
But you'd better be able to foresee a lot of them and do what you can to minimize the impact."

Dan Power
MD, Data Governance,
State Street Global Markets

#8 Focusing on reducing human factors

For instance, most phishing attacks succeed due to human factors, as people lack the knowledge or experience to distinguish malicious content. So, corporate culture, employee behavior, and the board's decision-making now play a critical part in companies' digital risk management. To future-proof their business resilience, organizations start recognizing the importance of human factors for effective risk mitigation. New approaches promote incorporating risk awareness training for all employees and including human behavioral insights into digital risk assessment models.

#9 Continuously adapting crisis management action plans

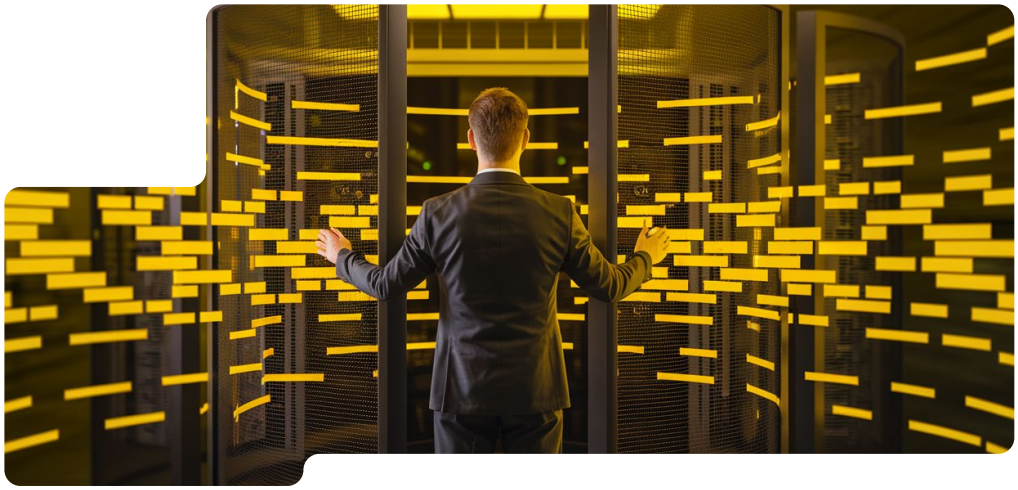
Applying only traditional response-and-recovery approaches is no longer enough. Organizations evolve risk evaluation frameworks by elaborating collaborative risk management plans to combat global permacrisis. The essential components of such plans are information sharing and collaboration between governments, industries, and businesses that stimulate continuous strategy adaptation based on real-time risk anticipation, reassessment, and proactive response. Cross-sector cooperation enables everybody to stay abreast of the most relevant DRM trends to address shared risks, leverage emerging technologies, and timely align business expectations with regulatory requirements.

#10 Exploring cyber self-insurance

Aside from prioritizing threats and optimizing cybersecurity budgets accordingly, an overwhelming number of digital risks pushes CISOs and executives to opt for one of the newest market offerings — cyber insurance. However, there is no standardized approach to specific parametric solutions yet, unlike in property or auto coverage. Each case is highly individual and requires a custom approach to accurately calculate the company's unique risk exposure limits. But global insurance providers and underwriters work hard to come up with concrete metrics and calculations as they're weary of how rapidly the scale of cyberattacks grows. It means that the demand for such insurance services will also keep growing, dictating the market conditions and pricing tiers.

Key challenges of managing risks in digital environments

- The lack of an elaborative Digital Strategy
- The need to assess the appropriateness of the entire existing IT infrastructure
- The skills shortage of the right digital talent
- The necessity to comply with all legal and regulatory requirements



Types of digital risks

In the coming years, DRM will only continue to become more tech-powered and intricate, as well as risk impact will be getting more substantial. Hence, businesses should become well-educated and prepared in terms of what to anticipate ahead. Forewarned, forearmed. So, here are the main types of digital risks you must know about to maintain a strong cybersecurity posture and avoid reputational damage, compliance issues, and regulatory penalties.

What is digital risk?

— Digital risks are the vulnerabilities cybercriminals explore in the field of digital business transformation, e.g., data breach vulnerabilities, remote access control, and others. It's impossible to predict all unwanted consequences and negative outcomes of these risks.

9 types of digital risks

1. Data leaks
Unintentional exposure of sensitive data by any party involved could develop into a full-scale data breach.

2. Cloud-based
Any and all risks associated with cloud architecture, infrastructure, and IT system or platform deployment (e.g., connecting IoT devices to your cloud network).

3. Cybersecurity
All risks of cyberattacks that cover your company's attack surface and aim to access and extract sensitive data.

4. Workforce & Remote work
Talent and workplace-related risks, including cyber skills shortage, human errors that lead to data breaches, identity and access mismanagement, insufficient digital workstation protection, and more.

5. Third-Party
Risks brought to you by external outsourcing service providers and third-party vendors. Could include data leaks, IP theft, credentials theft.

6. Process Automation & AI
Risks that arise when you automate operational processes, modify already automated ones, implement new AI-powered services, or introduce new business models. Also includes plagiarism issues, AI bias, and data accuracy risks.

7. Compliance
Risks directly connected to regulatory non-compliance and usually introduced when you adopt new technologies or onboard new IT vendors operating in highly regulated industries.

8. System Resilience
Any risks related to internal and external IT service availability after a disruption, including damage caused by integrating new technologies or hacks.

9. Data Management and Privacy
Any and all risks that affect the secure management of your sensitive data, whether business, customer, or financial information.

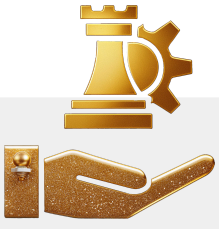
There are three primary areas of digital transformation initiatives that invoke these risks:

1. Increasing operational efficiencies

Related risks:
- Cybersecurity
- Workforce
- Third-party
- Cloud-based

2. Integrating new business models

Related risks:
- Third-party
- Cloud-based
- Compliance
- Process automation and AI



3. Improving value-creation

Related risks:
- System Resilience
- Data management and privacy
- Cybersecurity

Three main digital risk categories

Even the world's biggest enterprises, such as **Microsoft, British Airways, Meta, the UK National Health Service, Sony, Marriott International, Capital One, and T-Mobile,** couldn't avoid being disrupted by state-of-the-art cyberattacks. Is there anything you can do to not end up in their club? Sure, knowing how to categorize threats helps.

When doing a holistic digital risk assessment to evaluate your company's risk appetite, break those risks down into three categories:

A. **Mitigatable**
The amount of risk you can mitigate by investing in cyber tech, employee training, and other additional resources.

B. **Transferable**
The amount of risk you can transfer to a third party under outlined insurances.

C. **Acceptable**
The amount of risk (or loss) your organization can accept in the long run.

Keep in mind that all these risks aren't equal. Some cause more damage than others, so be sure to assess each category and risk type carefully.

Industries most vulnerable to cyberattacks

According to Positive Technologies' report, the top three most attacked industries hacked through social engineering techniques were government agencies **(44 percent)**, military enterprises **(19 percent)**, and science and education-focused organizations **(14 percent)**.

The full list includes the following industries:

Healthcare & Life Sciences	Social Media Platforms	Manufacturing
Military-Focused Industrial Sector	Government Agencies	Energy and Utilities
Telecom & Entertainment	Education and Science	Finance & Banking

What is DRM?

Digital risk management is an essential component of a sustainable method to manage your digital assets. It's a set of tools, processes, and practices that protect your organization from threats and help you mitigate undesired outcomes during digital business transformation. DRM requires the holistic "three lines of defense" approach that engages all the stakeholders and board members to share responsibilities related to the never-ending cycle of identifying, assessing, analyzing, and mitigating risks within your IT infrastructure.

To create a practical digital risk management framework, you must omit reacting to threats after they're discovered and shift to proactive threat detection. Moreover, your risk mitigation framework should be agile and adaptable to anticipate the dynamic cybersecurity environment and address the deadliest risks on time. Additionally, handling *cybersecurity risk management* calls for clearly defined roles and all operational functions to be performed on a daily basis.

5 essential components of your DRM framework

1. Risk assessment
2. Risk mitigation
3. Risk reporting and monitoring
4. Risk governance
5. Risk analysis

How to manage and mitigate digital risks

There are multiple official guides on approaching corporate DRM, but you can stick with two of the most well-known and easy to follow: the ISO 31000 and *ISO 27001 standards.* They have all the guidelines, principles, frameworks, and an outlined process for risk mitigation at any company, regardless of size or industry.

In short, there are seven strategic steps you should follow when navigating digital risks.

1. Assess and frame your risks

You need to understand your company's comprehensive digital footprint and its impact:

1. Outline your most valuable and critical IT assets and evaluate your cybersecurity posture.
2. Define threats and vulnerabilities associated with all digital operations and vendors.
3. Cover all physical and virtual locations with a risk breakdown structure.
4. Map out your dynamic attack surfaces and create a risk register.
5. Identify legal and regulatory rules/requirements that govern your digital activities.

Threat methodologies that can help you learn which vulnerabilities your IT assets could be exposed to		
PASTA	STRIDE	LINDDUN
Attack Trees	Persona Non-Grata	CVSS
Security Cards	Quantitative Threat Modelling	Trike
VAST Modelling	hTMM	OCTAVE
OWASP	EU AI Act	TRiSM

Tip: You can save a substantial amount of time and effort by using a digital solution for attack surface monitoring that will automatically identify all asset vulnerabilities in your organization.

2. Analyze risk likelihood and potential impact

Define a correlation between risks and your organization's performance:

1. Calculate the likelihood of a given risk occurring and estimate the monetary impact of the risk materialization, both quantitatively and qualitatively.
2. Create a risk assessment matrix to visualize the results (probability/impact).
3. Measure your risk acceptance threshold: specify tolerance levels for each risk and evaluate which ones are endurable and which aren't. Risks outside the threshold require closer attention and additional measures.
4. Identify risk triggers and opportunities to reduce your attack surfaces based on the available risk matrix.
5. Model the worst cyberattack/risk scenarios and their probable impact for three different phases: crisis, remediation, and improvement.

Tip: Use advanced *data analytics software tools* and cloud platforms to automate calculations and visualization activities.

Areas you should audit when assessing your risks

3. Prioritize risks based on your business objectives

After you communicate the identified risks to all stakeholders, it's time to prioritize and align them in accordance with your top business goals:

1. Rank the risks based on their severity, likelihood, and available mitigation strategies.
2. Put the risks with the highest probability of occurrence and negative impact at the top of your list.
3. Define company resources required to tackle those risks.
4. Incorporate digital risks into a broader business perspective, like financial implications, for easier communication with the board.
5. Consider adding cybersecurity insurance and risk transferring to your agenda.

4. Elaborate an incident response plan (IRP)

Using a DRM framework and your industry's guidelines:

1. Develop a proactive risk management strategy to treat digital risks identified earlier.
2. Plan and implement risk responses and security measures for each risk category and scenario.
3. Test your incident response plan, analyze the results, and revise the plan if improvements are needed.
4. Harmonize your security controls with all regulatory standards to eliminate gaps with frameworks like HIPAA, GDPR, NIST, HITRUST, and *ISO 27001.*
5. Establish new cybersecurity policies and create a RACI matrix to document all stakeholders' roles and responsibilities and define risk owners. Plus, define which DRM resources your company lacks and elaborate a plan to allocate them.

Tip: Opt for digital risk management software that provides complete visibility into your IT operations and *automates the risk mitigation* and response process. If you don't have one, assemble a risk management department under the guidance of a Chief Risk Officer and a Chief Information Security Officer.

Major risk management approaches to include in your IRP

Risk reduction	Risk remediation	Risk transfer
Lowering the likelihood of a threat or making it more difficult to exploit a vulnerability.	Removing a vulnerability from your system completely to prevent its exploitation.	Transferring risk mitigation to a third party.

5. Foster a progressive culture of enterprise risk awareness

To establish transparent cybersecurity leadership and open communication:

1. Explain all security policies in simple words and provide your employees with intuitive tools for incident reporting.
2. Put humans at the center of this game by introducing regular cybersecurity training and risk awareness programs.
3. Develop a risk-intelligent corporate culture that involves every staff member in DRM processes.
4. Conduct quarterly awareness-raising sessions and exercises aimed at reducing emerging risks and providing employees with a continuous learning curve.
5. Integrate safe online practices that protect employees' work-from-home setups and your cybersecurity posture in the remote work era.

Tip: Use digital tools with features like risk dashboards, impact visualization, risk-related data management, and scenario analysis. You need *an efficient risk management platform* that tracks and reports risk data in real time.

6. Develop a risk-focused IT architecture

Align your company's cybersecurity needs and operating environment:

1. Go beyond general firewalls and implement honeytokens, privileged access management, data leak detection solutions, and zero trust architecture to mitigate data privacy risks.
2. Automate security control QA with continuous control monitoring solutions to ensure that all controls — physical, digital, technical, operational, and administrative — are tested according to a pre-established schedule.
3. Monitor all network traffic and safeguard endpoints with advanced detection and response systems to maintain strict access policies for all sensitive assets. Leverage network segmentation, micro-segmentation, and network security policy management.
4. Fortify your recovery plan with an automated data backup and cost-effective Disaster Recovery as a Service solutions.
5. Integrate cutting-edge AI and ML-based DRM tools for automated threat/fraud detection and prevention. Use artificial intelligence to simulate cyber risk scenarios and reveal hidden vulnerabilities in your IT infrastructure, but don't forget to establish ethical AI governance policies.

Tip: If you have limited internal IT resources, it could be wise to outsource some of these activities to a *third-party technology vendor.* A reliable partner will simplify the integration process, assembling the tools and talents you need for a much lower total cost of ownership.

Improve your cybersecurity posture with advanced tech solutions

Multiple next-generation firewalls	Ransomware protection	Endpoint detection and response
AI-driven threat and real-time anomaly detection	Security information and event management (SIEM)	Zero trust security architecture
Scenario-based risk analytics platforms	Multi-factor authentication & Encryption	Risk Modeling as a Service

7. Monitor and adapt

The cyber threat environment will keep changing dynamically, so you must keep monitoring your organization's risk appetite and DRM results:

1. View your risk register and risk assessment matrix as growing kids: you'll have to identify new threats in an ongoing mode, reevaluating existing vulnerabilities and risk triggers to update your contingency plan.
2. Regularly reassess your cybersecurity posture and risk management processes to prepare your DRM strategies for emerging risks/threats and new regulatory requirements.
3. Continuously upgrade IT network security policies and conduct new risk evaluations to update the risk register.
4. Estimate the effectiveness of your risk management plan and create a database of lessons learned.
5. Monitor your attack surfaces 24/7 to detect suspicious activity and look for the occurrence of risk triggers. Leverage new technologies to improve risk sensing and tracking.

Tip: Risk mitigation never stops — keep your guard up.

Three key cybersecurity areas to monitor

1. Regulatory landscape Stay abreast of industry regulations and emerging shifts to meet all the required standards.	**2. Vendor risks** Assess and document security and compliance controls for each new tech provider you onboard.	**3. Internal IT usage** Know what technologies and devices your employees use and how to cover potential security gaps.

Additional recommendations for optimal DRM

- ***Regularly test*** **new and legacy code and all applications** to uncover hidden vulnerabilities and validate the effectiveness of your cyber defenses.
- **Don't miss the time to patch your software** and update hardware to exclude vulnerabilities related to outdated systems.
- **Enforce strict authentication policies** that provide access only to designated personnel.
- **Isolate data backups** from your main network access points.
- **Integrate third-party risk management into your DRM strategy** to ensure proper vendor due diligence, data security, compliance assessments, certification checks (ISO 27001, HITRUST, and others), and regular monitoring.

Securing business resilience in the event of a cyberattack

1. Alert your crisis team
2. Initiate crisis communication
3. Enforce your IDP/business continuity plan
4. Contact the authorities
5. Activate a disaster recovery plan
6. Handle relations with your insurance provider

Building your cybersecurity outpost in 2025 with agile and interconnected risk mitigation

In our modern hyper-connected world, digital ecosystems evolve as rapidly as cyberthreats do. However, those also become highly interconnected; hence, investing in cybersecurity defense is no longer an option but rather a necessity. And to navigate the uncharted waters, you need a flexible, proactive, and continuous digital risk management framework because it's a matter of "when" a hack hits your company, not "if." Keeping up with the latest trends in the DRM landscape will also help a great deal.

You should accurately assess all your digital risks and system vulnerabilities so that your organization can build its defensive fort around a *tailored cybersecurity strategy* and effectively manage any threats coming your way. This strategy must align with your business goals and risk acceptance threshold, incorporating robust technological advancements for intelligent threat hunting and encouraging all your employees to stay vigilant. Only with a solid foundation in the form of zero-trust IT architecture and enterprise-wide risk awareness culture can you fortify your defenses against emerging cyberattacks and secure digital assets.

TEAM International as your trusted information security partner

When you decide to transfer risks to a DRP vendor, you need a reliable partner you can trust. Third parties usually introduce significant security risks to your IT ecosystem. Consequently, you must vet and assess each tech vendor according to your cybersecurity scoring system before onboarding. One of the most important criteria is whether a provider has all required security certifications obtained under external institutions' audits.

As an officially ISO 27001-certified (including all our 10 R&D centers) digital solutions company, *TEAM International* knows first-hand how to ensure the safety of your assets and business continuity. Having a specialized team of security experts in our TEAM Information Security Studio, we are capable of acquiring and retaining skilled talent your organization lacks cost-effectively and quickly. Our support services cover security control assessments, regulatory mapping, risk assessment and typology, and robust framework development.

With TEAM International, holistic digital risk management is a reality, not a dream.

Cybersecurity as a Service solutions we provide:

- Risk governance and management models
- Cloud security & Predictive analytics
- Uninterrupted real-time cybersecurity monitoring
- Threat exposure assessment with risk scenarios modeling
- Disaster recovery
- DRM consultation and strategy development
- Resource allocation
- Cybersecurity automation
- Comprehensive managed security solutions

By innovating your risk mitigation policies and implementing advanced automation tools, *TEAM Information Security Studio* can augment your decision-making to improve risk response plans and reduce your attack surface. We follow only the best and industry-leading practices of continuous risk evaluation, data observability, threat exposure monitoring, and vulnerability management. Our experts will create a unified, connected, and consistent digital risk management plan that meets your company's needs and budget, enabling you to stay ahead of sophisticated cybercriminals.

TEAM Information Security Studio develops custom DRM frameworks from scratch that are:

We develop advanced cybersecurity solutions that protect your:

IT infrastructure | **Networks** | **Endpoints** | **Data assets** | **Applications**

Your IT vendor risk evaluation checklist

- ☑ When did you last assess your company's digital risks, and what were the results?
- ☑ Do you have any cybersecurity certifications?
- ☑ Which advanced tools do you employ for securing your IT operations?
- ☑ What remote access policies does your company apply?
- ☑ How well-trained are your employees in managing customer data?

Facilitate innovation and address emerging digital risks with TEAM Information Security Studio's expertise and cutting-edge technologies!

Get a free cybersecurity consultation today

www.teaminternational.com

sales@teaminternational.com
US Headquarters
+1 321 300 0087