How do successful organizations develop risk-based security programs to support business agility and resilience?

Digital business transformation and emerging cyber-physical systems create unprecedented security risk. In response, many organizations adopt new cybersecurity approaches. By 2023, 75% of organizations will restructure risk and security governance to address new cyber-physical systems (CPS) and converged IT, OT, Internet of Things (IoT) and physical security needs, an increase from fewer than 15% today.*

But organizations struggle to balance cybersecurity with the need to run the business. Chief information security officers (CISOs) can help by developing processes that enable risk-based decisions while protecting against security threats, and preventing data breaches and other cybersecurity events.

From our expert research and interactions with thousands of companies across industries, we have compiled cybersecurity best practices into a customizable roadmap. Use this roadmap to understand the key stages, resources and people required to plan and execute an effective cybersecurity initiative.

*Source: Gartner

Some of the top questions of the cybersecurity initiative are:

1. How will this support business resilience and growth goals while reducing risk?
2. How can we use an outcome-driven approach to establish cybersecurity priorities and investments?
3. Which leaders and teams need to be involved?
What are the key stages?

This best-practice insight is distilled from interactions with clients who have successfully implemented cybersecurity initiatives. This map shows the sequence of objectives and desired outcomes and is useful for aligning all stakeholders.

A few key milestones and a sample of associated Gartner resources are highlighted below, but the full roadmap will include complete details of all milestones and resources for each stage.
**Align strategy**

**Set objectives and build business case**

Selected tasks include:

- Understand key business priorities; define program mission and vision; and identify business, technology and threat drivers
- Identify goals, program value, and key stakeholders’ roles and responsibilities
- Define security controls in line with organizational strategies and map them to a standardized security framework
- Get stakeholder feedback, define key objectives and finalize initial summary of security strategy document

Sample associated Gartner resources include:

- Consultation by phone: Discuss the key business solutions that can be leveraged to deliver security and risk management in the organization
- Research: Develop your cybersecurity charter in alignment with business goals and communicate it to a wider audience

**Develop action plan**

**Create risk prioritization framework**

Selected tasks include:

- Conduct vulnerability assessment and penetration testing
- Establish current maturity baseline, define target state and conduct gap analysis
- Get executive or board buy-in and resource backing
- Develop security architecture, policy framework and solution layer

Sample associated Gartner resources include:

- Zero-Regret Purchases: Leading the Business to Make Smarter Buying Decisions
- CIOs Must Manage Four Views of Spend to Manage IT Finances
- Tracking and Reporting on Cybersecurity Costs
**Initiate execution**

**Design and adjust team structure**

Selected tasks include:
- Integrate capabilities, tools and technologies
- Establish security team roles and responsibilities and identify stakeholders to be accountable, consulted and informed
- Develop critical competencies and train for desired or missing skills
- Use metrics and incentives to drive accountability among owners
- + more

Sample associated Gartner resources include:
- Consultation by phone: Engage with an expert to discuss “The CARE Standard for Cybersecurity”
- Research: Read about cybersecurity threat and its impact on the business
- On-site workshop: Discuss key steps to be taken to reduce the risk of cyberattacks while working from home
- + more

---

**Build and mature program**

**Maintain accountability and assurance through governance**

Selected tasks include:
- Develop critical incident response capability and an action plan in case of breaches
- Develop a program structure to monitor and combat advanced threats
- Instill a culture of secure employee behavior and initiate tailor training and awareness campaigns
- Develop advanced reporting and response and craft a communications plan for cyber breaches
- + more

Sample associated Gartner resources include:
- Analyst inquiry: Engage with an analyst to finalize the right metrics that can measure the impact of cybersecurity
- Analyst inquiry: Engage with an analyst to discuss the right approach to communicate the business impact of cybersecurity to the stakeholders
- + more
Reassess and optimize

Communicate program value

Selected tasks include:

- Create a plan to communicate value to the organization and the board
- Track metrics and seek feedback to assess and improve program effectiveness
- Revisit maturity assessment to further optimization
+ more

Sample associated Gartner resources include:

- Consultation by phone: Discuss the key points that can help in further optimization of cybersecurity preparation in the organization
- Analyst inquiry: Redo the Gartner IT Score assessment to measure progress and reprioritize
+ more
Who needs to be involved?

The most successful companies establish cross-functional teams for their cybersecurity initiatives. We have outlined the recommended functions to involve and their roles to ensure the best success in hitting the milestones.

<table>
<thead>
<tr>
<th>Function</th>
<th>Roles and Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISO</td>
<td>Leads development of cybersecurity strategy and program; ensures cybersecurity strategy is aligned with business strategy and objectives; directs assessment, action plan and execution; helps communicate cybersecurity strategy and progress across the organizations; collaborates on program implementation with key leaders and stakeholders</td>
</tr>
<tr>
<td>CIO</td>
<td>Collaborates with organizational leaders and guides the building of the cybersecurity program; communicates strategy and objectives across the organization</td>
</tr>
<tr>
<td>Technical professionals team</td>
<td>Design, implement, or improve and maintain security architectures, policies and procedures, monitor and evaluate cybersecurity performance, and improve it on the basis of new threats, improve skills as needed</td>
</tr>
<tr>
<td>Applications leader and team</td>
<td>Key partner for the CISO; assist with implementation and operation of key elements of security programs and operations</td>
</tr>
<tr>
<td>Enterprise architecture leader and team</td>
<td>Collaborate with the CISO and other IT leaders to make sure that security strategy and architecture are aligned and incorporated into overall enterprise architecture</td>
</tr>
<tr>
<td>Infrastructure and operations team and leader</td>
<td>Key partner for the CISO; assist with implementation and operation of key elements of security program and operations</td>
</tr>
<tr>
<td>Security and risk management leader and team</td>
<td>Partner with the CISO to incorporate cybersecurity into overall governance, risk and compliance program and processes</td>
</tr>
</tbody>
</table>
Customer success story: Enabling IT Compliance With Cybersecurity Roadmap

Mission-critical priority
With the aim to streamline business processes and develop a digital-business-ready environment, Pacific Textiles wanted to develop a framework that adheres to IT compliance, minimizing cybersecurity risk.

How Gartner helped
With access to Gartner experts, research and tools, Pacific Textiles was able to digitalize information through an ERP system, automate manufacturing processes with new technology and craft a ready-to-execute cybersecurity roadmap.

Mission accomplished
With the help of Gartner, Pacific Textiles was able to:
• Take a holistic approach to governance and risk management procedures
• Build a strong digital business foundation
• Optimize business processes, saving time and energy for the top management
Gartner roadmaps are designed to help CIOs and IT leaders successfully execute new initiatives and reduce time and costs. Our suite of roadmaps provides extensive coverage of IT leaders’ top priorities, such as:

- Data and Analytics
- Digital Transformation
- Security
- Data Strategy
- Cloud Strategy
- Maturing Information Security
- Cloud Migration
- IT Organizational Design
- Customer Experience
- ERP Transformation

Explore additional resources to learn more about cybersecurity

→ Rethink the Security & Risk Strategy
→ CISO for Digital Business
→ Cybersecurity Conferences
→ Customer success story: Become a World-Class Cybersecurity Leader