CISO Responsibilities

David Pederson
Marianne Muller

September 2024

You've Got a Friend in Your CISO. Know the Complexity of Her Job.

Protecting the organization's data, systems, and digital assets from cyber threats and ensuring compliance with relevant regulations is a big responsibility. Understanding that will help you appreciate your CISO, and she will be impressed that you can at least touch on these parts of her job. Here are the top 40 things a CISO keeps up with to keep your records safe.

	Responsibility	Description
1	Strategic Leadership	Works with senior executives to align organizational security goals with business objectives.
2	Risk Management	Assesses and prioritizes cybersecurity risks and develops strategies to mitigate them.
3	Policy and Compliance	Enforces policies and ensures compliance with regulations and industry standards.
4	Security Governance	Establishes security decision-making frameworks and defines security roles.
5	Security Awareness and Training	Educates employees about security issues and how to avoid security breaches.
6	Security Architecture	Designs and implements secure system architectures, including security technologies.
7	Incident Response and Management	Develops and leads plans to respond effectively to security incidents.
8	Vendor Risk Management	Assesses the security of third-party vendors who have access to company data.
9	Security Monitoring and Assessment	Monitors networks for threats, conducts security assessments, and identifies vulnerabilities.
10	Budget Management	Manages the security budget and justifies investments to senior management.
11	Regulatory Compliance	Ensures compliance with relevant data protection and privacy regulations.

continued ...

. . . continued

	Responsibility	Description
12	Cybersecurity Incident Communication	Communicates with stakeholders during security breaches to control the situation and protect the company's reputation.
13	Security Risk Assessment	Conducts comprehensive risk assessments to identify vulnerabilities and threats to the organization's IT infrastructure
14	Security Awareness and Training Programs	Designs and implements organizational training programs to educate employees on cyber-security best practices.
15	Security Architecture and Design	Collaborates with IT teams to integrate security from the beginning of system and application development.
16	Security Incident Response	Develops a plan for identifying, managing, and recovering from security incidents.
17	Threat Intelligence and Monitoring	Leverages threat intelligence sources and continuously monitors activity to promptly identify and respond to potential threats.
18	Vendor Risk Management	Evaluates the security practices of third-party vendors and work to manage associated risks.
19	Security Policy Enforcement	Ensures that everyone follows established security policies and guidelines.
20	Regulatory Compliance Management	Navigates industry and region-specific regulations, ensuring the organization remains compliant.
21	Security Culture Development	Fosters an environment of security awareness and responsibility.
22	Security Metrics and Reporting	Measures the effectiveness of security measures and provides regular reports to management.
23	Budget Planning and Management	Develops and controls the security budget and demonstrates return on investment.
24	Cybersecurity Awareness Among Leadership	Educates senior executives about the importance of cyber-security and its alignment with company goals.
25	Security Incident Communication and Public Relations	Manages external communications during a breach.
26	Emerging Technology Evaluation	Assesses new security technologies and determines their relevance to the organization.

continued . . .

. . . continued

	Responsibility	Description
27	Security Research and Development	Stays informed about the latest threats and advances through research and professional development.
28	Regulatory and Legal Expertise	Understands laws and regulations related to security, ensuring the organization complies.
29	Security Governance Committees	Leads or participates in security committees that guide the organization.
30	Continuous Improvement and Adaptation	Leads efforts to adapt strategies in response to the evolving threat landscape.
31	Global Considerations	Navigates international laws and ensure compliance with global data protection standards.
32	Vendor Relationships and Procurement	Collaborates on technology purchases, evaluating security risks associated with vendors.
33	Employee Background Checks and Security Clearances	Oversees background checks for employees with access to sensitive systems.
34	Board Reporting	Regularly provides the board of directors with security updates and insights.
35	Crisis Management	Leads crisis response efforts during major security incidents.
36	Ethical Hacking and Red Teaming	Employs ethical hackers to test the organization's security controls.
37	International Cybersecurity Coordination	Works with global partners, government, and law enforcement to address international security threats.
38	Public Policy Advocacy	Engages in advocacy for cybersecurity legislation and regulations.
39	Crisis Communication Planning	Develops plans for communicating during and after a security incident.
40	Integration of Artificial Intelligence (AI) and Machine Learning (ML)	Explores the use of AI and ML to improve security capabilities.

In summary, the role of a Chief Information Security Officer (CISO) is multifaceted and dynamic. It includes strategic leadership, risk management, compliance, incident response, and continually adapting to the evolving cybersecurity landscape. CISOs are instrumental in safeguarding an organization's digital assets, protecting sensitive data, and ensuring its resilience and security. They are crucial in today's digitally connected world, where cyber threats constantly evolve, and data and systems protection is paramount.