Cybersecurity

Basic approach

We consider cyberattacks to be one of the top risks for our business, and we are continuously pressing forward with cybersecurity measures as per our Declaration of Cybersecurity Management.

Declaration of Cybersecurity Management https://www.mizuhogroup.com/who-we-are/activity/cybersecurity

Cyberattacks are on the rise with the advancement of digitalization throughout society

Digitalization continues to advance in many regions around the world, and the Internet has become a space where large volumes of private information circulate and accumulate. There has been an increase in cyberattacks with suspected state involvement, and the number of cyberattacks that target confidential information held by companies is also growing.

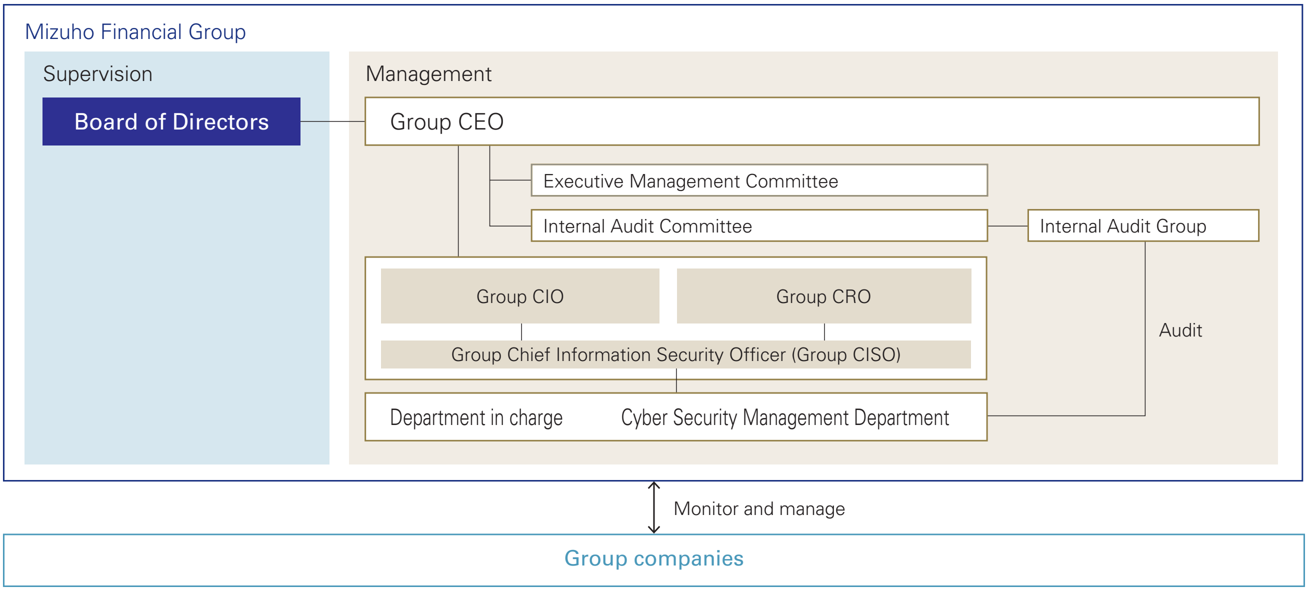
Mizuho's cybersecurity initiatives

With Mizuho-CIRT[1] taking the lead, we have assigned high-level professionals and are drawing on intelligence and cutting-edge technology developed in collaboration with external specialized organizations, while also establishing a 24-hour, 365-day monitoring framework via integrated SOC[2] and strengthening our resilience frameworks, including the analysis of malware and the development of defense-in-depth measures. We are also working to further strengthen measures by having independent bodies make objective assessments to supplement in-house testing. To prepare for emergency situations, we conduct testing and drills that include TLPT[3] and phishing email drills held at least once every six months and also focus on personnel training and development, measures for the supply chain, and raising the awareness of customers.

[1] Cyber Incident Response Team
[2] Security Operation Center
[3] Threat Led Penetration Test (a test to verify the strength of security measures by attempting to infiltrate a system using existing technologies)

Mizuho's cybersecurity management framework

At Mizuho, under the supervision of the Board of Directors, we have established the position of Group Chief Information Security Officer (Group CISO), who administers overall group-wide / global cybersecurity management, and we have also established CISOs at our main subsidiaries. In the interest of clarifying how the check-and-balance system applies to the Group Chief Information Officer (Group CIO) as part of our second line of defense, the Group CISO reports to both the Group CIO and Group Chief Risk Officer (Group CRO). We are striving to enhance our cybersecurity posture by implementing this system of double reporting. In addition, progress made on the various measures taken is reported to the Executive Management Committee and Board of Directors, which review policies and resource allocation related to cybersecurity.


Mizuho Financial Group
Supervision
Board of Directors
Management
Group CEO
Executive Management Committee
Internal Audit Committee
Internal Audit Group
Group CIO
Group CRO
Group Chief Information Security Officer (Group CISO)
Audit
Department in charge
Cyber Security Management Department
Monitor and manage
Group companies