UBS and Cyber Security

Our days are increasingly digitalized. As technology converts our daily life into data, we depend on reliable and secure technology more and more, resilient against modern threats – particularly technology at the core of financial services. As cyber threats to data increase in volume and sophistication, UBS focuses relentlessly on investments to maintain essential cyber and information security capabilities.

UBS defends against cyber threats with a vast array of both internal and external capabilities, aligned to global industry standards, as well as regulatory and legal requirements. These capabilities align across five important functions:

Analyze
Understand the threat landscape using processes, technologies, interactions with industry peers, intelligence sources, law enforcement and regulatory entities. This supports decisions at the business level, and prioritization and investments of resources through a lens of business risk, informed by the threat.

Protect and Prevent
Deploy deep layers of defenses and controls across the physical environment, the perimeter, the internal infrastructure, and the data, from edge to endpoint. Design, implement and operate defenses to ensure that the availability, integrity, confidentiality, and privacy of the data residing within the firm's information systems, meets the Firm's, our clients', and our regulators' expectations.

Detect
Use intelligence and state-of-the-art technology to detect when threats try to attack, to correlate security events, and trigger incident alerts to drive investigations by a global team of professionals.

Respond
Bolster the Firm's preparedness, and measure the Firm's readiness, to act in the event of an adverse incident, driving prompt operational response - by both operational staff and senior management - to mitigate the impact to the Firm, our clients, and stakeholders.

Recover
Once incidents are resolved, safely bring back online critical services and relevant information technology to meet our business objectives.

We integrate these functions within a formal risk and governance framework overseen by an internal governance board composed of senior executives across all business divisions and control functions. Our multiple levels of internal and external risk assessments consider both internal processes and external third parties and dependencies - to address the entire supply chain - and drive continuous control fortification against cyber and information security threats.

The Firm is committed to fostering information security and a cyber-safe culture, continuously raising awareness, and equipping our staff with the knowledge to perform their roles best to protect data privacy and security.

To achieve an optimal level of security, UBS also relies on its customers playing their part, by adhering to guidance and contractual obligations relevant to security measures - including online access for services and products provided by the Firm, and utilizing accepted control principles within their environments. Visit our Cybersafe site for information on how you can stay safe online.