UBS and Cyber Security

Both the volume of cyber–related attacks and their sophistication have increased substantially in the financial industry, and the expectation is that this trend will continue. UBS communicates with its industry peers, regulators, industry intelligence sources and law enforcement to address developments in the threat landscape and the sophistication of attacks.

UBS has increased its investment in cyber security through the recent years, allocating significant resources for the operation of the firm's security control infrastructure and programs to address the evolving threats.

UBS addresses cyber security utilizing accepted control principles. Our approach is built on five major pillars:

Data Confidentiality
processes and technologies designed to protect data against unauthorized or inappropriate disclosure. In addition to client data, UBS takes measures to protect sensitive data such as intellectual property, unpublished financial information and personal data.

Data Privacy
processes and technologies to support UBS efforts to meet legal, regulatory and contractual obligations with respect to the protection of personal data which may include the protection of client and/or employee data.

IT Security
processes and technologies designed to protect the confidentiality, integrity and availability of information that is processed electronically.

Cyber Threat Management
processes and technologies designed specifically to protect the bank against cyber–attacks such as denial of service, external fraud and data theft.

Physical Security
processes and technologies designed specifically to protect network infrastructure and data storage assets where UBS and client data is processed and maintained.

UBS ties the above together with a formal risk and governance framework that includes multiple levels of internal and external risk assessments as well as processes for tracking and remediating known operational risks. UBS examines security measures of our external vendors who connect to our network or otherwise are entrusted with confidential data.

UBS is committed to raising staff awareness and provides staff with information regarding effective protection and defensive measures to mitigate the risks of cyber threats.

To accomplish its security goals, UBS relies on its customers also playing their part, by adhering to all guidance and contractual requirements that apply to security measures and online access for services and products provided by UBS.

Further Information

For further information relating to UBS's information security and cyber threat management capabilities, please talk to your relationship manager.