Bitsight Continuous Monitoring & Security Performance Management at SIX Group

Thomas Koch, Nicolas Berger

May 2024

Agenda

1. SIX Group – who are we
2. Third Party Risk Management – The journey ahead
3. Use cases – how do we use Bitsight

Four Areas of Activity.

One Company.

Exchanges

Third-largest stock exchange group in Europe

SIX Swiss Exchange, BME Exchange, BME Derivatives Exchange, SIX Digital Exchange

- Listing
- Trading
- Market Data

Securities Services

Unbeatable post-trade services from A to Z and more

- Clearing
- Settlement and Custody
- Securities Finance
- Tax Services
- Trade Repositories

Financial Information

Data You Trust

- Reference, Corporate Actions and Market Data
- Tax and Regulatory Services
- Indices
- ESG Data
- Display and Data Feed

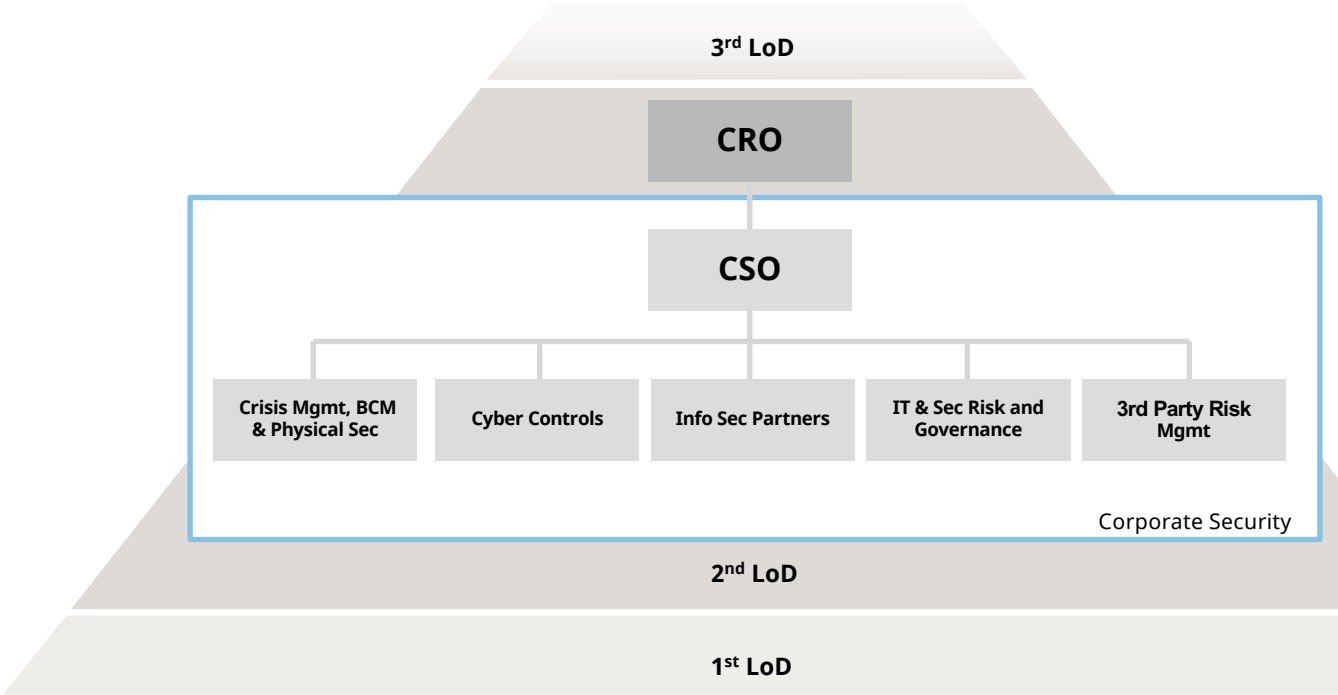
Banking Services

Smooth payment transactions

- Cash
- Connectivity (Open Banking)
- Debit and Mobile Solutions
- Billing and Payments

Corporate Security Organization at SIX Group

SIX Group has adopted a Three Lines of Defense governance model



BitSight is in use in all 2 LoD teams except Crisis Mgmt

1 LoD uses **BitSight** (TPRM & SPM) for Thread Intel and Vulnerability Management

Third Party Risk Management at SIX

WHERE WE ARE TODAY
Tool-based process, risk-based monitoring, defined KRIs, various stand-alone tools

WHERE WE STARTED
Initial Due Diligence focused process
MS Word, Excel and mail-based process
Limited monitoring capabilities
No KRIs

WHERE WE ARE GOING
Fully integrated process and tools (end-to-end), near-real time monitoring and reporting, 4th party risks, strategic risk appetite

The strategic Third Party Risks and Questions

- **Critical Nth Parties** The complexity of the vendor environment is expanding. How far down the rabbit hole do we go? How do we balance the effort and expense of understanding supply chains with the effectiveness of possible controls?

- **Concentration** Lots of eggs in few baskets. This may make sense within a narrow set of procurement or business objectives, but does this compromise objectives of resilience and long-term sustainability?

- **Operational Resilience** For vendors supporting critical operations there is a divergence between acceptable downtime and time to replace. For these vendors, how many are sole/single sourced? How many have viable business continuity plans in the event of an extended vendor outage

BitSight use cases at SIX Group

SIX Group uses SPM, TPRM and Financial Quantification to monitor cyber risk exposure

Security Performance Management (SPM)

- BitSight rating for the various legal entities are monitored, KRIs are reported to Management and Regulator.
- BitSight findings are used for vulnerability management (along with other tools, such as Qualis, Recorded Future).

Third Party Risk Management (TPRM)

- BitSight rating for Tier 1&2 Suppliers is analyzed and reported.
- If rating is outside risk appetite, Supplier is contacted for remediation.
- BitSight Thread Intelligence can trigger involvement of SOC.
- Monitoring of 4th Party relationships Identification of 4th Parties

Financial Quantification

- Cyber risk impact can be quantified.
- Cyber Security strategy can be adjusted to meet risk appetite.

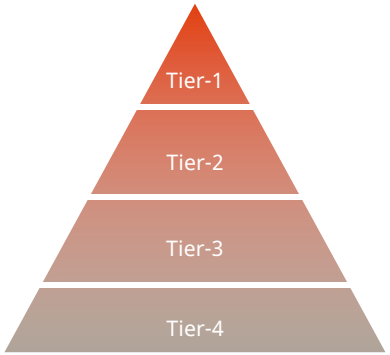
Supplier Risk Management life-cycle at SIX Group

Supply chain risks are managed end-to-end, from on-boarding, monitoring to termination. BitSight TPRM is used for monitoring of key suppliers.

Key activities during Due Diligence

- **Due Diligence**, questionnaire based
- **Approval** required before contract signing
- Assignment of Supplier to **Risk Tier**

Supplier Monitoring and Governance



- Risk-based requirements on **Supplier governance**
- **Risk-based Monitoring** for different risk areas (Tier 1&2)
  - **BitSight Security Reports**
  - Financial stability reports
  - Compliance monitoring
  - ESG risk
- Risk-based re-assessment cycle

Onboarding

Data collection

Due Diligence & approval

Approval

Risk Mitigation

Go-live & Monitoring

Continuous Monitoring of Supplier

Measurement of governance maturity

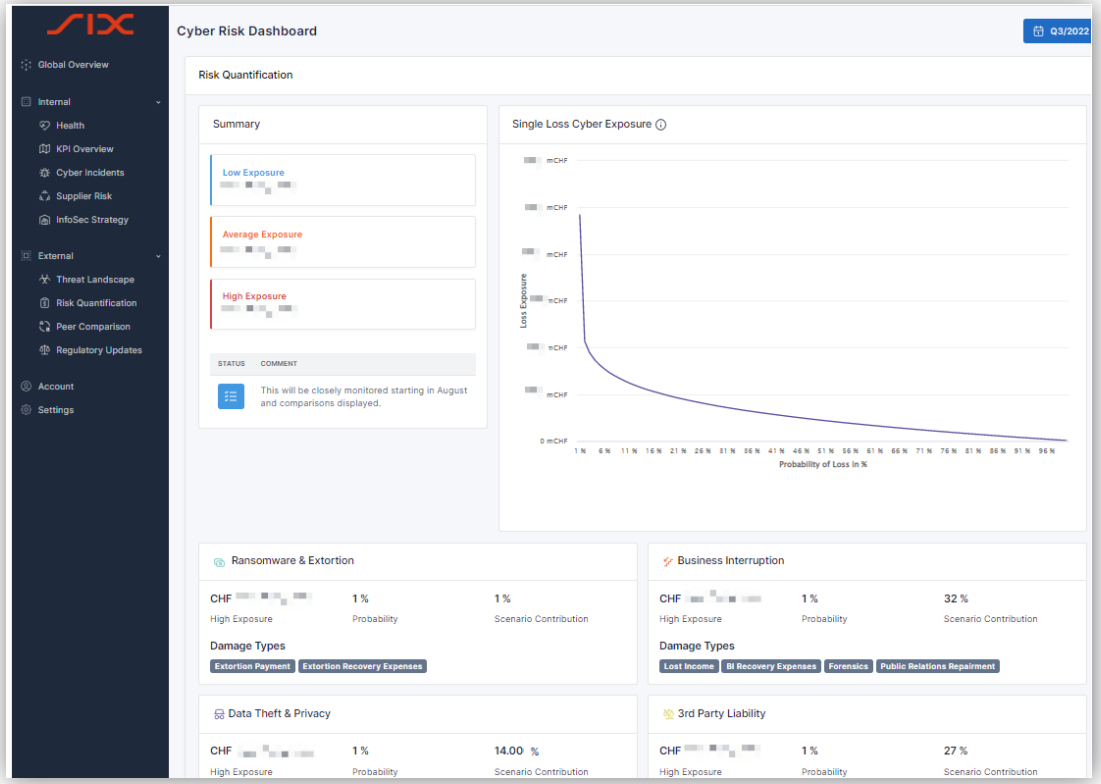
Regular re-assessment

Termination

Update of data & Final assessment

BitSight Financial Quantification module

The output of the Financial Qualification Module is integrated into the Cyber Risk Dashbaord

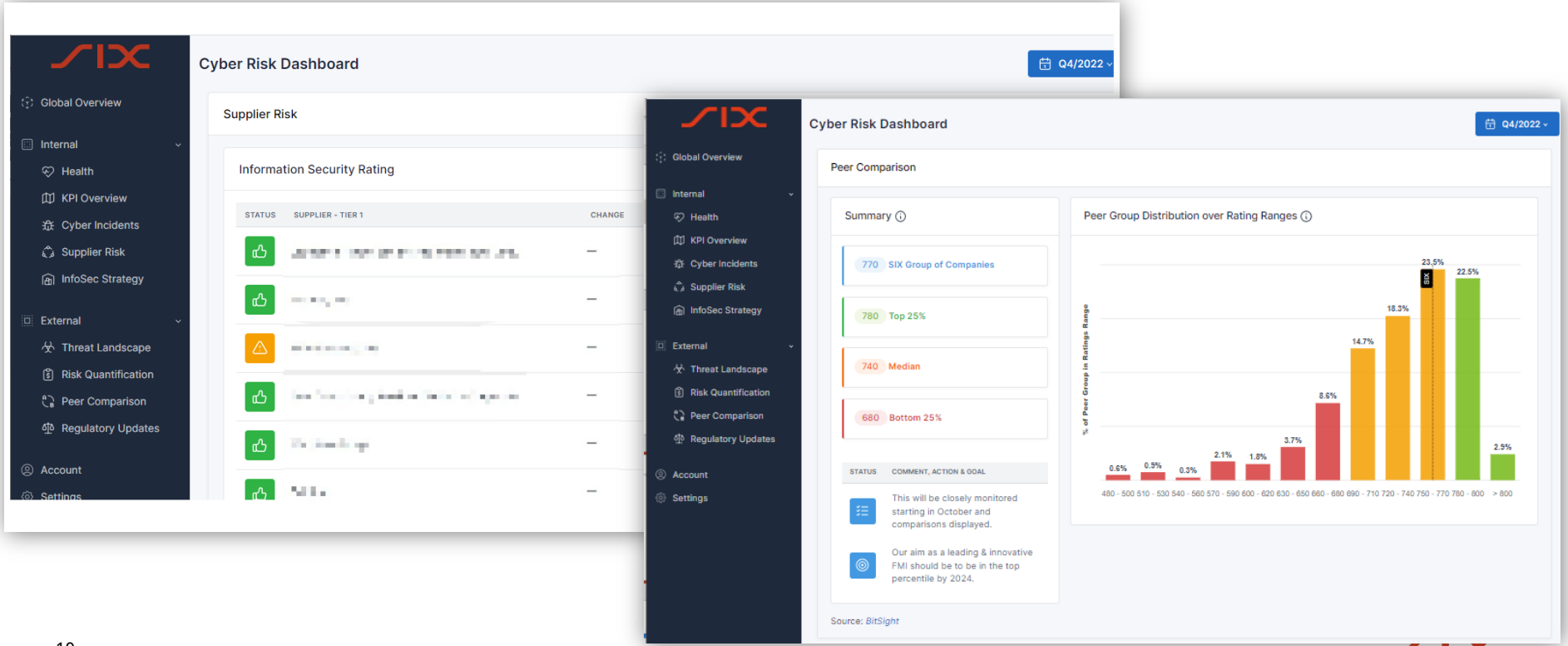


The *Financial Quantification* of Cyber Risks shows the total cyber risk exposure for a single loss event.

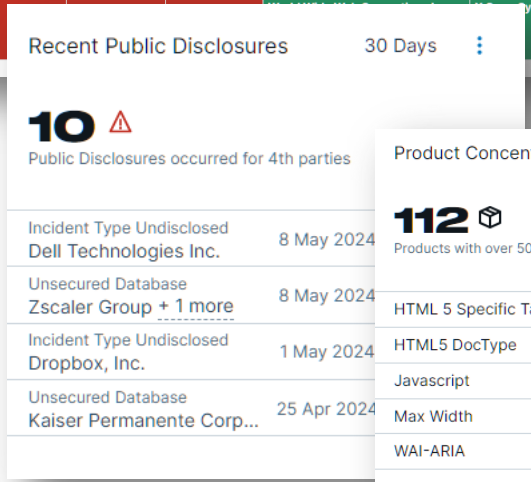
Financial exposure by cyber scenario type, such as Data Theft of 3rd Party Service Provider Failure, helps to adjust the controls and measures

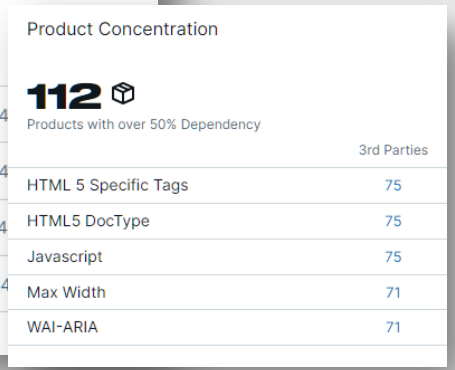
BitSight Modules integrated into SIX Group reporting

The security ratings are fed into the Security dashboard using the BitSight API along with other feeds



4th Party Risk - the module has been onboarded in Q1 2024





The 4th Party Risk module serves as a secondary source for identifying sub-suppliers

4th Party products & incidents can help to identify Cyber Supply Chain Risks.

Q&A

Keep up with the latest news.
Follow us on:

#TheFutureofFinanceIsNow
#TFOFIN

Subscribe to the RED Newsletter:
six-group.com/red

Download our Future of Finance Study:

Disclaimer

This material has been prepared by SIX Group Ltd, its subsidiaries, affiliates and/or their branches (together, "SIX") for the exclusive use of the persons to whom SIX delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. It is solely for information purposes and is subject to change without notice at any time. SIX is under no obligation to update, revise or keep current the content of this material. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by SIX as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material. Neither SIX nor any of its directors, officers, employees, representatives or agents accept any liability for any loss, damage or injury arising out of or in relation to this material. This material is property of SIX and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of SIX.