BITSIGHT®

How Can BitSight Help Organizations Prepare for GDPR

INFOCOM SECURITY CONFERENCE 2018

www.bitsighttech.com

GDPR: The Background

- The General Data Protection Regulation (GDPR) evolved from the 1995 Data Protection Directive.
- The GDPR provides Europeans with broad rights over their personal information**.**
- Individuals in the EU have **the right to withdraw consent to the use of their data.**

Key GDPR Compliance Implications

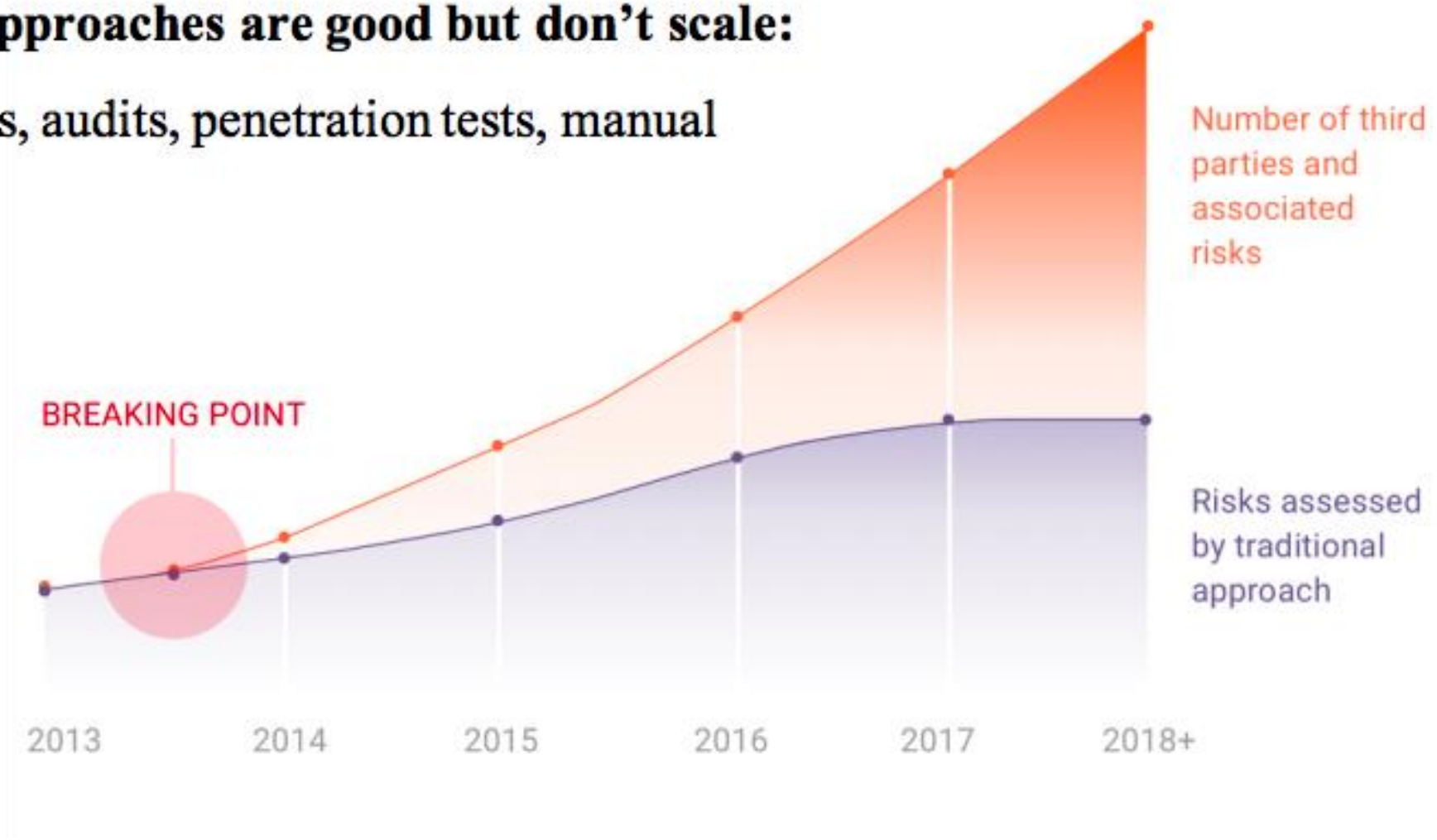
- **Article 32:** Organisations that collect personal data must have rigorous due diligence processes to ensure the appropriate technical and organizational controls are in place before sharing data with vendors. These organizations should establish a process for regularly testing their vendors.
- **Article 32:** Data Processors (third parties) are responsible for the PII they process on behalf of their customers, but Data Controllers (first parties) are still accountable for Data Processors' activity.
- **Articles 24-43:** Organizations must proactively demonstrate they understand the data they have access to, how to use that data, and how to safeguard that data. Therefore, organizations must maintain, document, and enforce data protection policies and procedures.
- **Article 33:** If a data breach takes place, the company collecting the personal data must notify its national regulator of said breach within 72 hours of breach discovery.

- **Articles 44-50:** Any organization anywhere in the world that processes the data of an EU citizen—not only those operating in the EU—must comply with GDPR requirements.

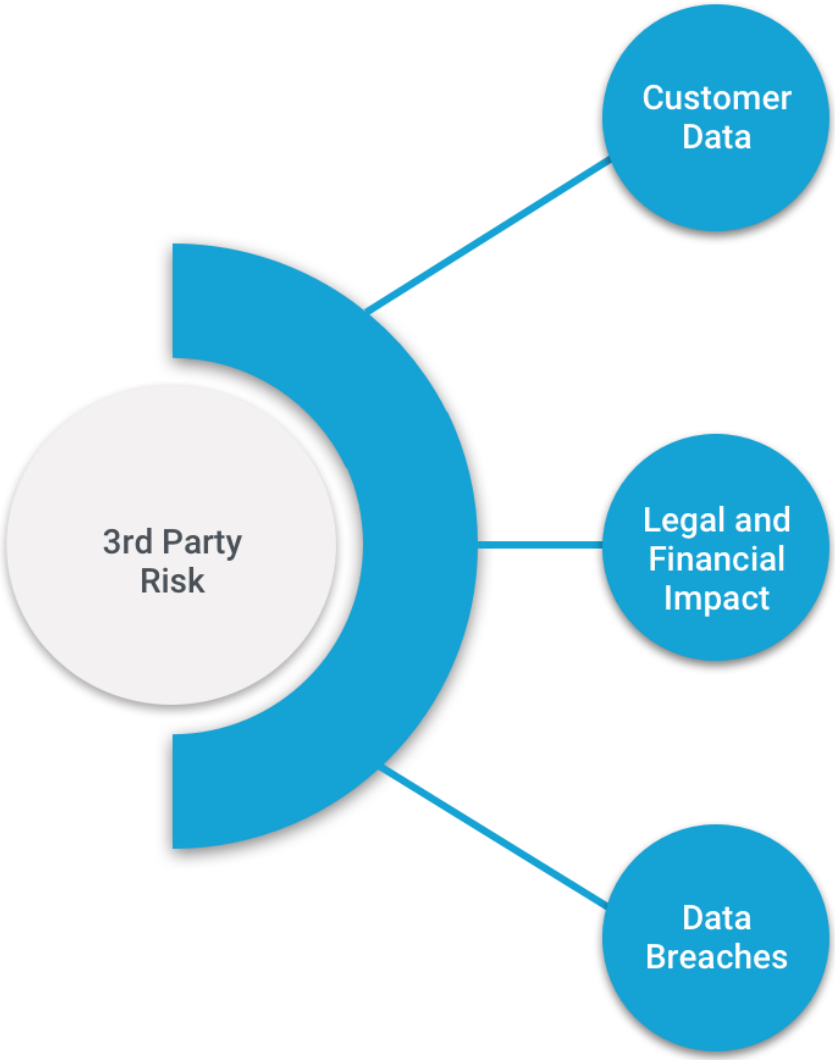
The Evolution of Third-Party Risk Management Challenges

Traditional approaches are good but don't scale:

Questionnaires, audits, penetration tests, manual efforts, etc.



Controllers & Processors: The Importance of Third Party Risk



According to GDPR, organizations are responsible for what their third parties do with their customers' data.

Under GDPR, data breaches can have enormous legal and financial impact. Fines can reach up to 20M Euros, or 4% annual turnover.

50% of data breaches occur through third parties. (eg Equifax, Deloitte, Target)

The Board and Security & Risk Teams are Disconnected

No Common Language

- Lack of effective communication
- Boards don't know what to ask!
- Security & Risk Teams quickly dive into details

...to Create a Common Language Across Enterprise...

BitSight supports critical business functions

Enterprise Risk

Manage Cyber Risk in 3rd and 4th Party Ecosystem

IT/Security

Visualize, Prioritize, and Communicate Security Actions

Procurement

Rapidly Assess 3rd Party Risk during Selection and Onboarding

Audit

Enable Corporate Responsibility and Internal Oversight of Risks Taken and Management of Risks

Marketing

Differentiate Against Competition with Effective Security Posture

Finance

Spend Effectively & Allocate/Prioritize Resources

Legal

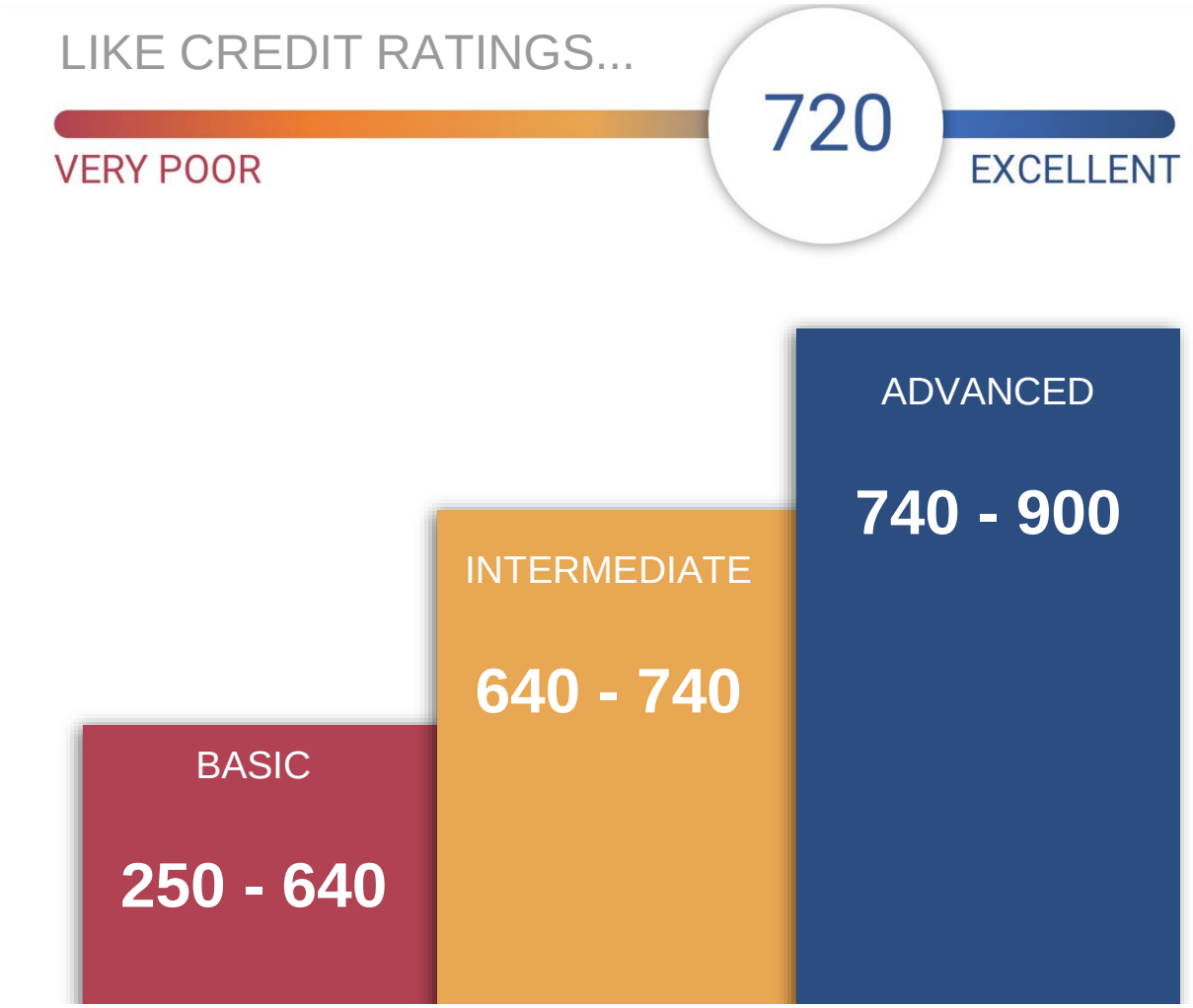
Objectively Evaluate Exposure and Actions Taken

A Standard Metric is Needed…

...to Translate Complex Cybersecurity Issues into Simple Business Context

BitSight Security Ratings

- Data-driven rating of security performance
- Non-intrusive SaaS platform
- Continuous monitoring



How BitSight Security Ratings are Calculated

Collect Data

80+ Billion events daily
Externally observable
World's largest sinkhole

120
DATA SOURCES

QUALIFIED DATA

Research & Assign

Automated & human validated
Public Internet registries
12+ month history for all companies

TESTED AND VALIDATED DATA

110,000
COMPANIES MAPPED

Filter & Process

60% Compromised Systems
30% Diligence Information
10% User Behavior
Breaches when applicable

22 RISK VECTORS

PROCESSED DATA

Calculate Rating

Daily Ratings
Range from 250 to 900

Low ratings correlated to higher likelihood of breach

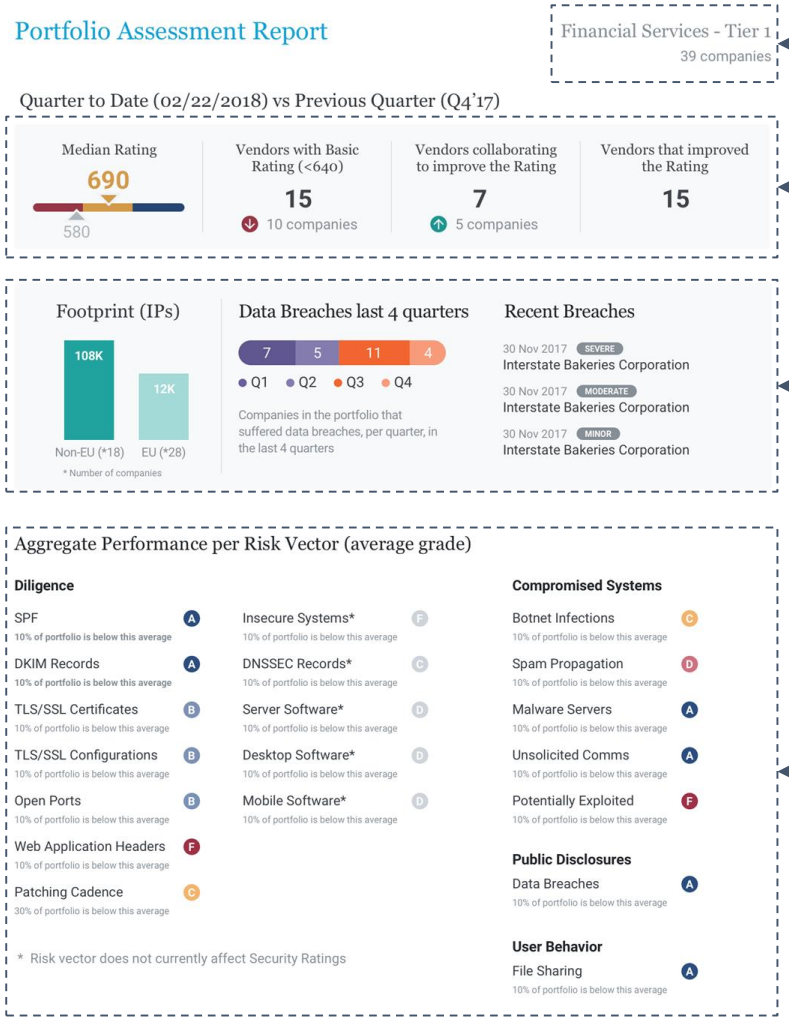
SECURITY RATING

How Can BitSight Help?

- Security and risk teams can use BitSight Security Ratings to gain visibility into the performance of a large portfolio of third parties.
- BitSight provides organizations with:
  - An extensive data ecosystem proven to show correlation to breach as well as a comprehensive data breach history for third parties.
  - Insight into the effectiveness of internal & third party security procedures (identified through 22 risk vectors).
  - Regular testing (continuous monitoring) capabilities that quantify the cyber risk of third parties.
  - The ability to efficiently scale third party risk management programs at the speed & growth of their business with little overhead.
  - Security Ratings that can be instantly shared with critical third parties fostering more effective collaboration around security and reducing risk.
  - The security posture of third parties with operations both within and outside of the EU (or a country separate from their data subjects).

Portfolio Assessment Report

Use case: Quickly assess and communicate important aspects of GDPR compliance



Determine level of risk of data processing activities (relevant for Article 25)

Establish a risk tolerance baseline and quantify aggregated risk (relevant for Articles 25 and 28)

Assess responsibilities of processors in terms of territorial scope (Articles 27, 46) and data breach notification process (Article 33)

Assess effectiveness of technical measures (relevant for Articles 28 and 32)

GDPR risk based approach, encourages organizations that control the processing of personal data to implement protective measures. These should corresponding to the **level of risk** associated with their data processing activities.

Key Takeaways

Easily identify security gaps among your processors using trusted, actionable metrics.

Regularly test and assess your critical processors.

Align your third party risk management program and strategy to the GDPR.

Questions?

Visit www.bitsighttech.com/gdpr for more resources.