CASE STUDY

BearingPoint

Using BitSight to Assess the Effectiveness of the Firm's Internal Security Posture and Third-Party Ecosystem

In recent years, independent management and technology consulting company BearingPoint has experienced accelerated growth – both in Europe and globally.

But, with growth, comes an expanded digital footprint and increased attack surface.

The firm has a global consulting network with more than 13,000 people and supports clients in over 70 countries, engaging with them to achieve measurable and sustainable success. It also has an extensive vendor portfolio, including major technology suppliers, that it relies on to develop and execute client solutions and strategies. Third-party supply chains pose a significant risk because they provide multiple entry points for threat actors.

Discovering and remediating cyber risk across this digital ecosystem was a challenge. But when a client approached the firm and suggested that BitSight could provide insights beyond what they had, David Perstl, Head of Security at BearingPoint, was keen to learn more.

"We knew that if our clients were using BitSight to understand the effectiveness of their security programs – and that of their suppliers – then we should be, too," said Perstl.

A POWERFUL SOLUTION FOR UNDERSTANDING AND MANAGING CYBER RISK IN AN EXPANDING DIGITAL ECOSYSTEM

To take a deep dive into enterprise and supply chain cybersecurity risk, Perstl chose BitSight for Security Performance Management (SPM) and BitSight for Third-Party Risk Management (TPRM).

BitSight provides deep insights into BearingPoint's attack surface. With this holistic, external view, the firm can:

- View where all its digital assets are located – including cloud services and shadow IT applications – and quickly assess the corresponding risk each presents.
- Identify security vulnerabilities and deviation from security policies across all assets.
- Verify the true nature of its vendor's security postures.
- Accelerate third-party cyber risk assessments.
- Work with suppliers to reduce their own risk, and, as a result, pose fewer threats to BearingPoint and its clients.

"Trust, but verify is so fundamental for us. Whenever possible, we verify internal parties' and third parties' claims that they are adhering to security best practices. But with hundreds of thousands of assets on the internet and cloud instances being spun up every day it's not easy. We needed automated and continuous visibility into where cybersecurity falls short – and BitSight delivers that," said Perstl.

> **"With hundreds of thousands of assets on the internet and cloud instances being spun up every day, we needed visibility into where cybersecurity falls short – and BitSight delivers that.**
>
> – David Perstl.

IMPROVED VISIBILITY INTO DIGITAL ASSETS AND RISK

With BitSight for SPM, BearingPoint can easily identify security vulnerabilities and deviations from security policy. Explained Perstl: "Even when our security teams say, 'we're following process,' BitSight automatically discovers vulnerabilities so we can quickly remediate and improve our overall security posture."

BitSight also shines a light on where the firm's data and digital assets are located. Using BitSight Attack Surface Analytics (part of BitSight for SPM), Perstl's team has a complete view of the organization's attack surface – both on-premises and in the cloud – and the corresponding risk associated with each.

"This is a favorite feature of mine. With Attack Surface Analytics, we get an instant visual of our global digital footprint. Seeing where our data and our client's data is so critical to maintaining compliance with regulations such as GDPR," said Perstl.

> **With Attack Surface Analytics, we get an instant visual of our global digital footprint. Seeing where our data and our client's data is so critical to maintaining compliance with regulations such as GDPR.**
> – David Perstl.

A TRUSTED WAY TO ASSESS THIRD-PARTY SECURITY PERFORMANCE

BitSight has also proved invaluable to the firm's Third-Party Risk Management (TPRM) program. "As soon as we implemented BitSight for TPRM, we achieved immediate transparency across our vendor portfolio. BitSight identified every vendor and, importantly, what their security posture is versus what they report to us," explained Perstl.

> **Our vendors are happy when we share that something is wrong in their security program because they often don't have that insight. This allows them to move quickly to fix it. In that way, BitSight makes everyone's jobs easier.**
> – David Perstl.

With BitSight, BearingPoint's compliance and security teams now have the confidence to make faster, collaborative, and more strategic cyber risk management decisions. "While security questionnaires and RFP responses from vendors still play a vital role in our vendor assessments, having the ability to verify responses with evidence and data helps us secure our business twofold."

Perstl also shares BitSight's findings with suppliers – making risk management and remediation a collaborative process. "Our vendors are happy when we share that something is wrong in their security program because they often don't have that insight. This allows them to move quickly to fix it. In that way, BitSight makes everyone's jobs easier," said Perstl.

In addition to reducing the workload on Perstl's team, BitSight also provides outstanding customer support.

"BitSight's Customer Success and Support Team has been fantastic. The response to any request is immediate and that's something we really value – the closeness with the team. It shows us that BitSight values us as a customer."