TECHNICAL NOTE

How To Get Started With BitSight for Fourth Party Risk Management

As businesses continue to outsource more than ever before, the number of relationships and connections between organizations have increased. Many organizations have programs in place to assess and manage the risks posed by third parties. How can organizations extend risk management practices to fourth parties?

With BitSight Discover, risk and security professionals can ensure that any new vendor fits into their organization's business and information security strategy. Below are ways many customers integrate BitSight Discover into broader risk and security initiatives.

1. VALIDATE QUESTIONNAIRE & ASSESSMENT RESULTS

BitSight Discover automatically identifies service providers connected to any given third party or vendor. Risk teams can corroborate questionnaire and assessment results with BitSight data. For instance, if a vendor said they only use one hosting provider, is that accurate? BitSight Discover will also specify the number of domains associated with each service provider.

2. PLAN FOR DISASTER RECOVERY

A recent report by Lloyd's of London and catastrophe modeling firm AIR Worldwide found that the disruption of a major U.S. cloud provider would cause over $19 billion in business losses. Large organizations need contingency plans in the case of a large outage or disruption in order to reduce their possible risk exposure.

BitSight Discover will identify the vendors and third parties affected in the case of an outage. Risk teams can use this data to identify service providers that could be used as backup if a large provider experiences an outage.

3. ASSESS DOWNTIME IMPACTS

In 2016, the outage of Dyn, a DNS provider, rendered many services and platforms unusable for a substantial period of time. BitSight Discover details the level of dependency vendors and third parties have on given service providers. This can help drive discussions about whether or not third parties have back-up and alternative providers ready in the case of a service provider disruption.

4. STREAMLINE BREACH RESPONSE

When a common provider discloses a vulnerability or breach, organizations should identify which of their third parties may have been affected. When vulnerabilities such as Cloudbleed emerge, customers can use BitSight Discover to figure out where data may be at risk beyond their own networks.

ABOUT BITSIGHT TECHNOLOGIES

BitSight transforms how companies manage information security risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of external data on security issues. Seven of the largest 10 cyber insurers, 20% of Fortune 500 companies, and 3 of the top 5 investment banks rely on BitSight to manage cyber risks.

CONTACT US

Want to learn more about BitSight Discover? Reach out to your BitSight Sales Representative or contact us at sales@bitsighttech.com.