NormShield

2018 Guide to Select 3rd Party Cyber-Risk Assessment Tool

A Review of Third-Party Cyber-Risk Assessment & Scoring Tools

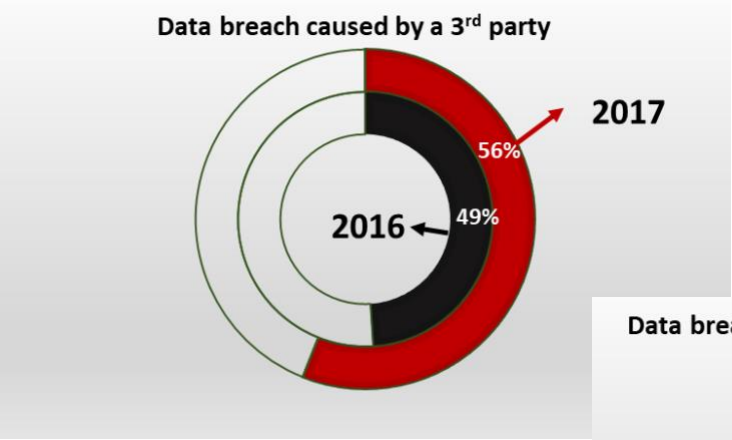
2018 Guide to Select 3rd Party Cyber-Risk Assessment Tool

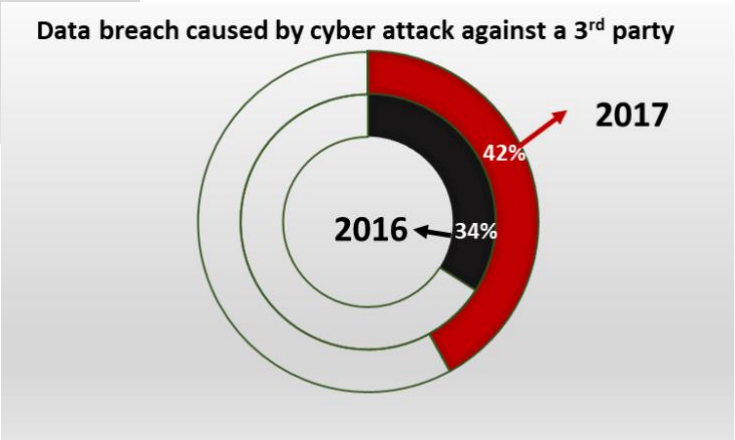
A Review of third-party Cyber-Risk Assessment Tools

Introduction

A recent survey conducted by Ponemon Institute reveals that 56% of companies have experienced a 3rd-party breach in 2017, which is an increase of 7% compared to previous year. Another survey conducted by Deloitte in 2016 was more depressive, reporting that 87% of organizations have experienced a disruptive incident with third-parties in the last 2-3 years. Another research in 2016, sourced by Soha Systems, reports that 63% of all breaches were related to third parties.

The findings in these studies confirm that third-party cyber risk assessment is a must. The goal of this paper is to provide a review on third-party cyber risk assessment/scoring tools that automatically gather and analyze open source data and provide a risk score/security rating.





What is Third-Party

Third-parties include broad range of companies you directly worked with such as data management companies, law firms, e-mail providers, web hosting companies, subsidiaries, vendors, sub-contractors, basically any company whose employees or systems have access to your systems or your data. However, third-party cyber risk is not limited to these companies. Any external software or hardware that you use for your business also poses a cyber risk. Even the JavaScript that is added to your website for analytics may cause a breach by exposing the information of people that visit your website. Recent hacks (like CCleaner in 2017) exposed backdoors to well-known software have confirmed that the definition of third-party should not be limited to only the companies that you directly work with. Even IoT devices can be considered as a third-party and can be source of a breach. Very recently a casino was hacked through its Internet-connected thermometer in an aquarium in the lobby of the casino. For more info on third-party cyber risk, check out our 2018 third-party cyber risk report here.

Breaches Caused by Third-Parties

The figure below shows recent breaches/incidents caused by third-parties, varying from law, accounting, HVAC firms to companies that provide web hosting, data management, e-mail services, etc.

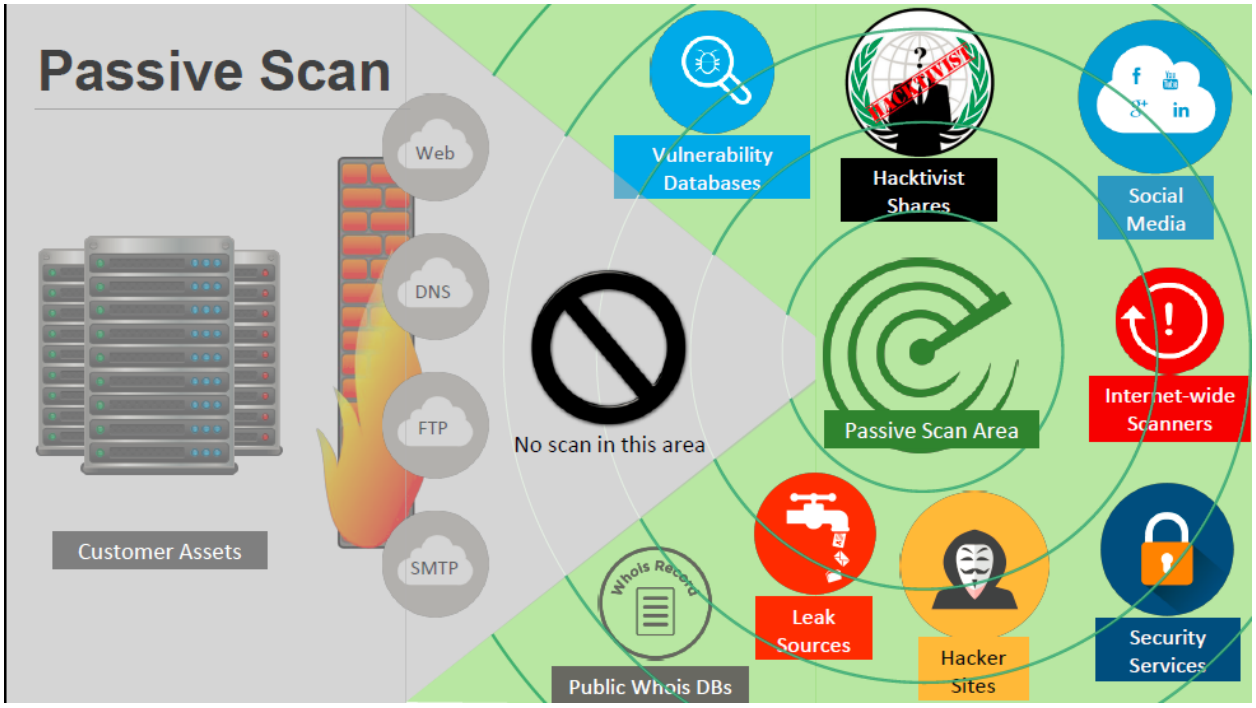
NormShield

Company	Breach/Incident	3rd party caused the breach	Use of 3rd party
T-Mobile	15M customer records exposed (SSNs, birthdays, driver licence # and more)	Experian	Customer credit assessment
Lowe's	Current and former drivers info including SSNs, birthdays, and more	SafetyFirst, E-DriverFile	Online database to store drivers' info
The Home Depot	56B customers' credit card info	Not disclosed	Not disclosed
Sam's Club, Costco Wholesale, Rite Aid, CVS, Walmart Canada, Tesco	Customers' credit card and personal info	PNI Digital Media	Online photo order and print
RT Jones Capital	Personel info of apprx. 100K individuals and 1000s of clients	Not disclosed	Web server hosting
Boston Medical Center	Records about 15K patients posted without authentication	MDF Trancription services	Trancription services
JPMorgan Chase & Co.	Contact info for 76M households and 7M small business	Not disclosed	Management of its Corporate Challenge Race registration
J.P.Morgan, Best Buy, Kroger, Chase, TV5, Target, Walgreens	60M rerords of clients	Epsilon	E-mail management
Target	Data of 70M customers and 40M credit/debit card	Fazio Mechanical Services	Heating, ventialation and air conditioning (HVAC) services
Equifax	Personal info (SSNs, names, Addresses) of 143M consumers that can be used for identity theft	Not disclosed	A 3rd party tool to build web applications
Many major corporations, politicians, celebrities all around the world	11M files detailing offshore tax avoidance (known as Panama papers) + 13 M files in another incident knows as Paradise Papers	Mossack Fonseca, Appleby	Law firms
Domino's Australia	Thousdands of customers names and e-mails	A former supplier	Management of an online rating system
Republican National Committee	Personal info of 200M voters	Deep Root	Marketing
verizon	6M customer records including account and personal info	NICE	Providing customer service analytics
US DoD, DoE, DHS, and DoS, USPS, NIH, Fannie Mae, Freddie Mac, FIFA, and several global banks, airlines, car manufacturers, energy and pharmaceutical co.s	Clients' email info	Deloitte.	Accountancy

How to Assess Third-Party Risk?

Many companies either do not conduct any assessment of the cyber risk of third-parties or use old-school questionnaire methodology (they send a list of questions for third-parties to answer). First of all, questionnaire-based assessment is very time consuming (even though there are some online tools that simplify the process) and answers are not reliable. Even if we assume that answers are correct and we gather the results quickly, there might be some cyber risks that are invisible to third-party. This type of “hidden” risks can only be detected by gathering cyber threat intelligence and evaluating the risk.

Fortunately, there are several platforms that gather third-party cyber risk data and provide a risk score or security rating for companies. The information gathering is done by a method called “passive scan” where non-intrusive methods are used and company assets remain untouched. It is basically a hacker’s view of the third-parties external cyber risk. The open-source intelligence data is collected from many feeds such as reputation services, hacker sites/forums, vulnerability databases, Internet-wide scanners, social media, paste sites, black markets, underground forums, etc. Information gathering should be done for the company of interest and any related third-party company.



Key Players

The top players that provide such cyber risk scoring through passive scanning are BitSight, NormShield, Security Scorecard, UpGuard, and Riskrecon. They all provide risk scores or security ratings for any company. This type of cyber risk assessment can be used for suppliers, joint-ventures, target acquisitions, franchisees, cyber insurance customers, etc.

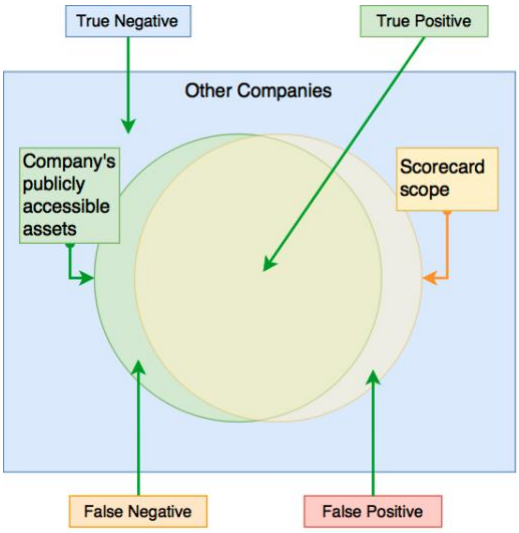
There are also some new players like iTrust and Paris-based company Cyrating. Also few 10+ year-old cybersecurity companies such as RiskIQ, RiskSense, Tenable have been working on cyber risk scoring products and their contribution to this niche market will make it more competitive.

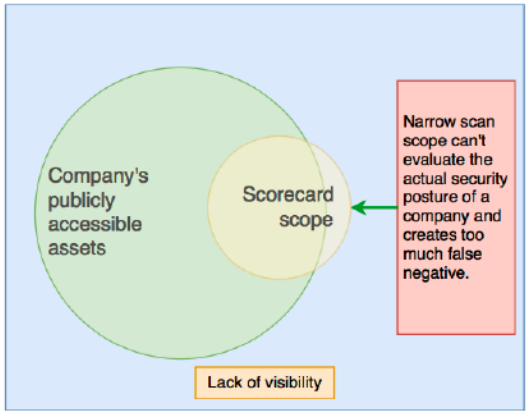
Comparison

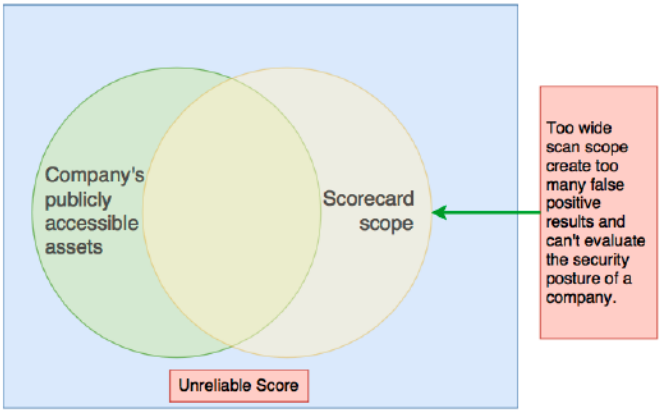
In this study, we compare the key players' cyber risk scoring products with NormShield's Cyber Risk Scorecard. Herein after, we will use notations Company A, B, C, and D for competitors.

Methodology

Since the methodology and data resources are similar, the differentiating factors are data quality, technical depth, reliability (true positive), coverage (true negative), usability and reporting capabilities. The ideal scorecard should sufficiently cover the target company's and related third-parties' assets and must exclude any findings that belong to other companies. In other words, the scoring system should be highly reliable (high true positive rate) and consistent (less false negative).



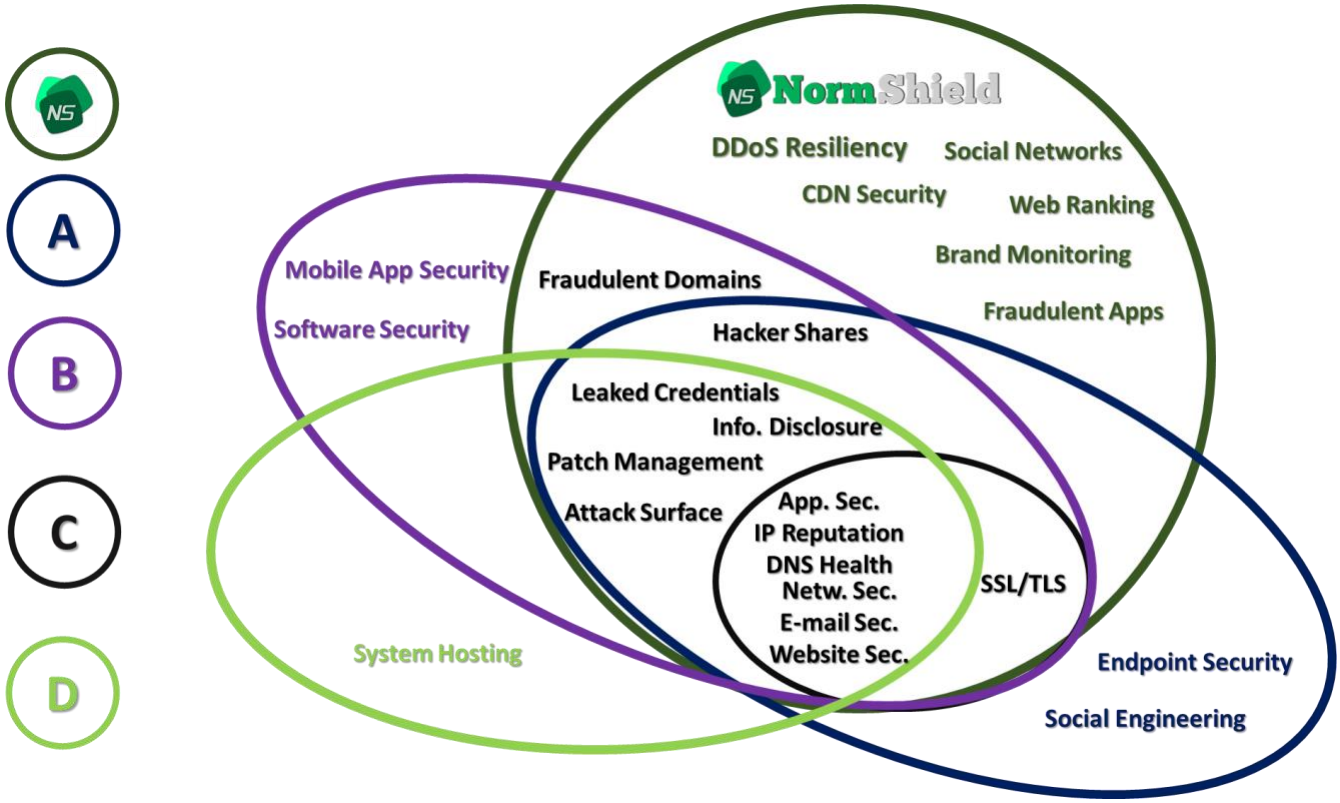




Threat Vectors Considered

We first look at the threat vectors covered. The number of threat vectors indicates the scorecard scope. As seen in the figure below, NormShield provides a large scope for risk scoring. There are some threat vectors, such as DDoS resiliency that other products do not cover. The ability to keep the scope large comes from the ***broad digital footprint*** information gathered. NormShield scorecard collects all domains, subdomains, IP addresses, DNS records, services, emails, ASNs, social media accounts, and company information with its proprietary algorithms. A large digital footprint intel with sensitive false-positive elimination (by computer and human analysts) gives a jump start to NormShield compared to others. Because it increases the visibility and reliability.

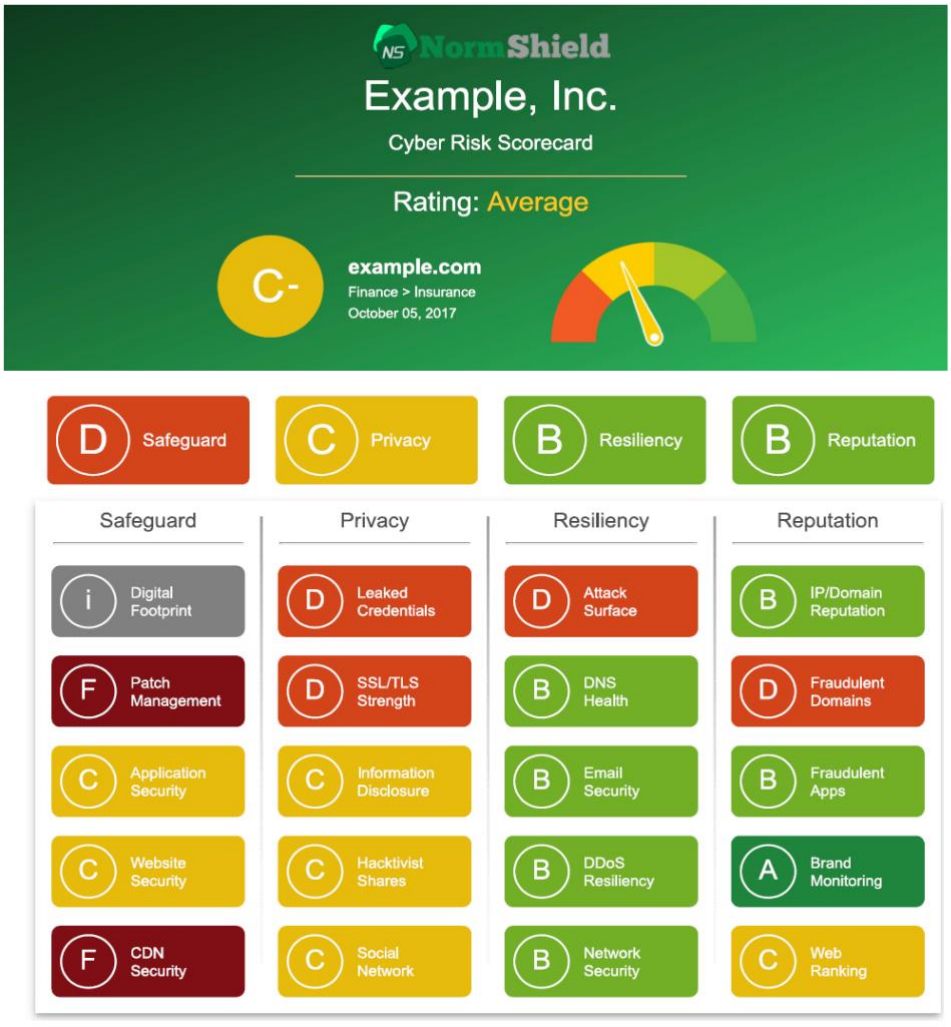
The below figure shows that Company C's product has the narrowest scope. Even though they provide a quick scoring, the information they gather is not sufficient to give a reliable score. They also provide breach information if an add-on feature is separately purchased. Company D has a larger but limited scope that covers some essential threat vectors. Company A and B have both large scopes and provide additional information such as Endpoint Security or Software Security, but they miss threat vectors such as DDoS Resiliency, CDN Security, etc. Another downside of Company A is that it does not monitor fraudulent domains, which are the main source of phishing attacks that target the customers and/or employees of a company.



Scoring

There are no standards on scoring methodologies (yet) for risk scoring products. An easy-to-understand and consistent scoring is very important when assessing the cyber risk posture of your own company and your third-parties.

Some companies used numeric scoring (0 to 900 scoring) and some use letter grades (A to F scoring). NormShield uses both A to F letter grades and percentage (0 to 100 percent) for overall score and all risk categories. Company A has a similar scoring/grading system. Company B, on the other hand, provide a 0 to 1000 overall score and A to F letter grades for subcategories. Company C shows only one score (0 to 1000) and does not provide scores for risk vectors. Finally, Company D provide 0 to 10 score for both overall and subcategories.



Reporting and Alerting

An ideal third-party cyber risk scoring tool should provide useful reports for risk remediation and mitigation and also provide alerts for important risk factors (such as leaked info) via e-mail or SMS.

NormShield Cyber Risk Scorecard provides very rich reports for each risk factor discovered with suggestions for mitigating the risk and also generates alerts via e-mail to notify IT security personnel about critical issues. Company A has similar features for reporting and alerting. Company D goes one step forward and creates a priority matrix based on severity of expected damage and importance of the asset that can be affected. Though, it is questionable how they determine importance of an asset.

While Company B does not provide an easy-to-generate report for remediation of risks, Company C does not give any suggestion at all.

NormShield SSL/TLS Strength Report

Company: Example, Inc.

Scan Date: October 05, 2017

Description: SSL/TLS configurations and vulnerabilities are provided by several third-party online services. The results come from various online SSL grading services like Qualys SSL Labs scanner, HTBridge, Mozilla Website Observatory etc.
This report category has 6% effect on total scan score.

D Poor

Contents:
- SSL Grading Overview
- Top Riskiest Assets
- SSL / TLS Vulnerabilites Matrix
- Supported Protocols and Cipher Suites Matrix
- Vulnerability / Weakness Details

SSL Grading Overview

The methodology consists of four steps:

- Look at a certificate to verify that it is valid and trusted
- Inspect server configuration in three categories: (a) Protocol support (b) Key exchange support (c) Cipher support
- Combine the category scores into an overall score
- Apply a series of vulnerability checks including but not limited to HeartBleed, LogJam, POODLE, FREAK, BEAST etc.

Vulnerability details are given below the summary tables.

Top Risky Assets (Top 10)

IP and Resolving Subdomains	Risk(s)	Grade
hix-it.health.example.com	• SSL Certificate Invalid, Incorrect, Expired or Self-Signed • SSL Insecure SSLv2 • SSL Insecure SSLv3 • SSL/TLS use of weak RC4 cipher	F

Conclusion

In this paper, we provide a review on third-party cyber risk scoring tools that automatically gather information and provide a risk assessment. We evaluated top players in the market and compared their scorecard scope (number of threat vectors considered), digital footprint, scoring methodology, and reporting/alerting systems. We see that the NormShield Cyber Risk Scorecard provides a larger scope with discovery of a larger digital footprint, has a consistent and easy-to-understand scoring, and generates rich reports and alerts.

About NormShield

The NormShield cyber risk scorecards provide actionable and easy to understand cyber risk information to business executives while providing detailed technical data and remediation recommendations to IT security personnel. With NormShield, organizations are able to perform nonintrusive cyber risk assessments to ascertain what hackers know about their external security posture and the cyber risk posture their third-parties (suppliers, target acquisitions, cyber insurance customers, etc.). NormShield's Cyber Risk Scorecards evaluate relevant cyber security of categories and provide a score in each as well as the ability to drill down for additional information about the factors that contributed to each score.

To get company/organization's cyber risk scorecard, please visit https://www.normshield.com and click on Learn Now.

www.normshield.com

1 (571) 335 0222

info@normshield.com

NormShield HQ

8200 Greensboro Drive

Suite 900

McLean, VA

22102