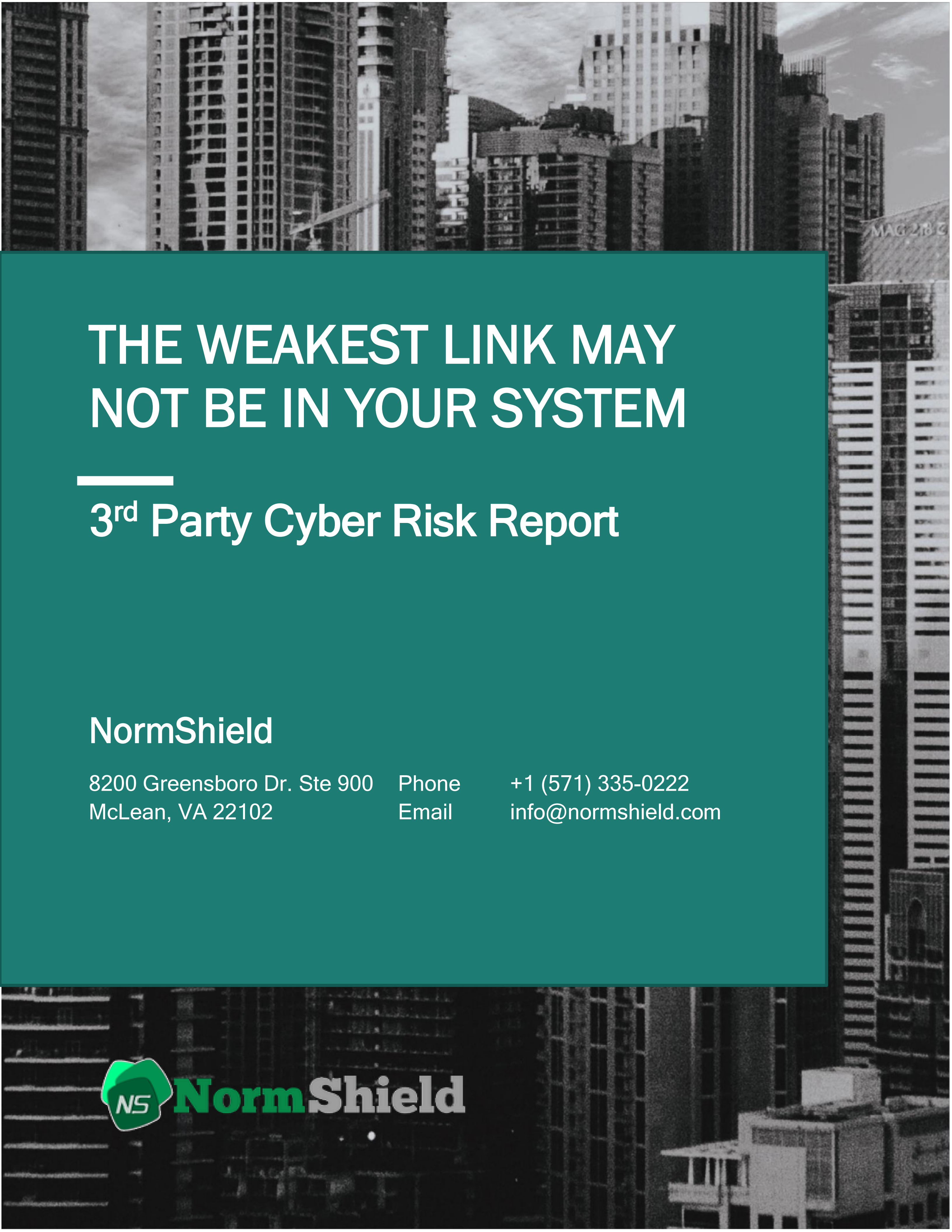


THE WEAKEST LINK MAY NOT BE IN YOUR SYSTEM

3rd Party Cyber Risk Report

NormShield

8200 Greensboro Dr. Ste 900
McLean, VA 22102

Phone +1 (571) 335-0222
Email info@normshield.com

NormShield

The weakest link may not be in your system

Matt, CISO of a large company, comes to office on Friday. He is a very successful Chief of Information Security Office and he is very confident of capabilities of his team. They handle all vulnerabilities inside their own system, continuously scan and monitor their system, they use cutting-edge security tools such as firewalls, WAFs, IDS/IPS, and Data Leak Protection technologies.

The cyber security awareness of the employees is quite high and they do everything to avoid phishing-type attacks. The possibility that something goes wrong is very low. However, that Friday morning, when Matt looks at online news, he shockingly discovers that many of their client information is leaked. He starts to investigate the situation and finds nothing in their own system. But later, he finds out that the leak is originated from a 3rd party, a data management company which manages emails of large companies.

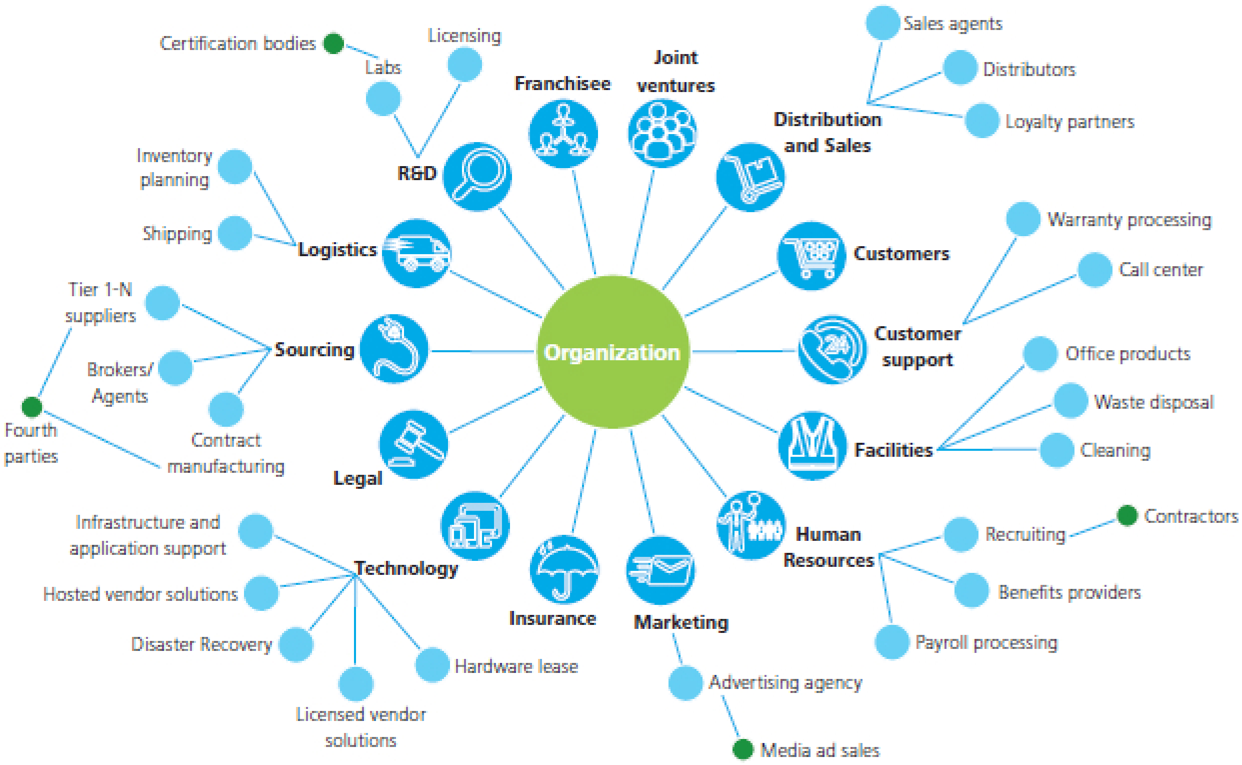
Recently, we have heard similar stories about breaches because of 3rd parties such as vendors, subsidiaries, web hosting companies, law firm partners, firms in supply chain, etc. Large companies such as financial institutions, e-commerce companies have been improving their cyber security system for external or even internal attacks. They can internally identify vulnerabilities of their own system by monitoring and/or scanning tools and take necessary precautions. However, all these efforts might be for nothing if 3rd party cyber risk is unknown. 3rd party risk management and data governance are growing concerns.

It is not surprising that, very recently, the revised version of the U.S. National Institute of Standards and Technology's Cybersecurity Framework (NIST) now includes supply chain cyber risk management[1]*.*

[1] https://www.wsj.com/articles/amid-national-security-warnings-nist-adds-supply-chain-security-to-cyber-framework-1524175900

What is 3rd Party?

3rd 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 some of whose employees have somewhat access to your system or your data. However, third party cyber risk is not limited to these companies. Any external software or hardware that you use for your system also poses a cyber risk. Even the JavaScript that is added to your website for analytics may cause a breach by collection information of people that visited your website. Considering some recent hacks by putting backdoors to well-known software, such as CCleaner in 2017, the definition of 3rd party should not be limited to only the companies that you work. 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.



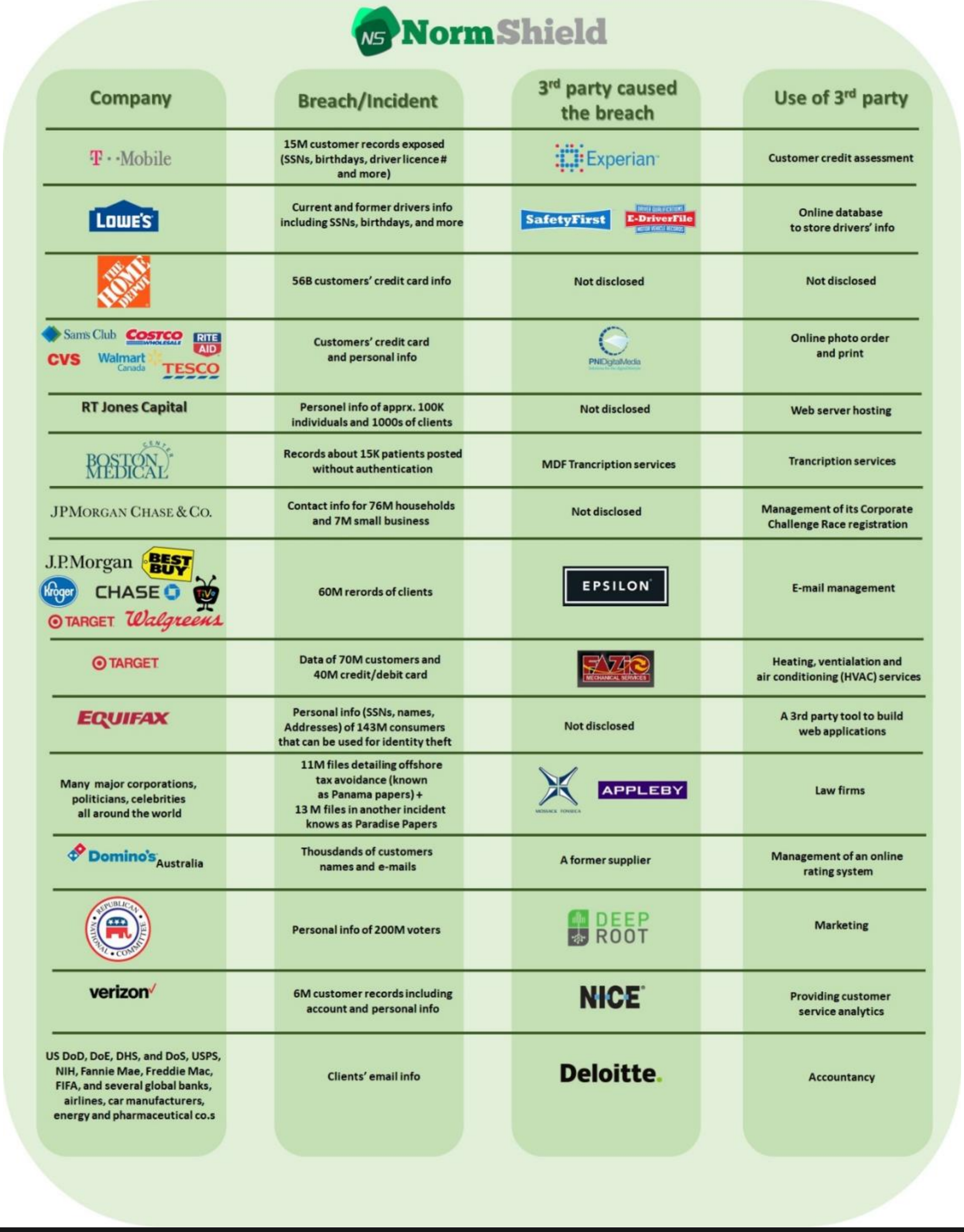
GDPR perspective on third party

The upcoming European Union’s General Data Protection Regulation (GDPR) has the terms third-party data processor and controller. As the name suggests, a third-party data processor is an entity that processes personally identifiable information (PII) on behalf of a controller. Basically, it can be e-mail service providers, customer relationship management services, etc.

A controller is defined by the GDPR as an entity that determines how that data will be processed and for what reason. All companies work with third-party data processors have to ensure that these third-parties comply or intent to comply the upcoming GDPR rules.

Recent breaches caused by 3rd parties

The figure below shows recent breaches/incidents caused by third parties. As seen from these breaches/incidents, the third party that caused a breach might be a law firm (usually the weakest link), an accounting firm, or even a firm that handles HVAC jobs; or it might be companies that provides web hosting, data management, e-mail services, etc.



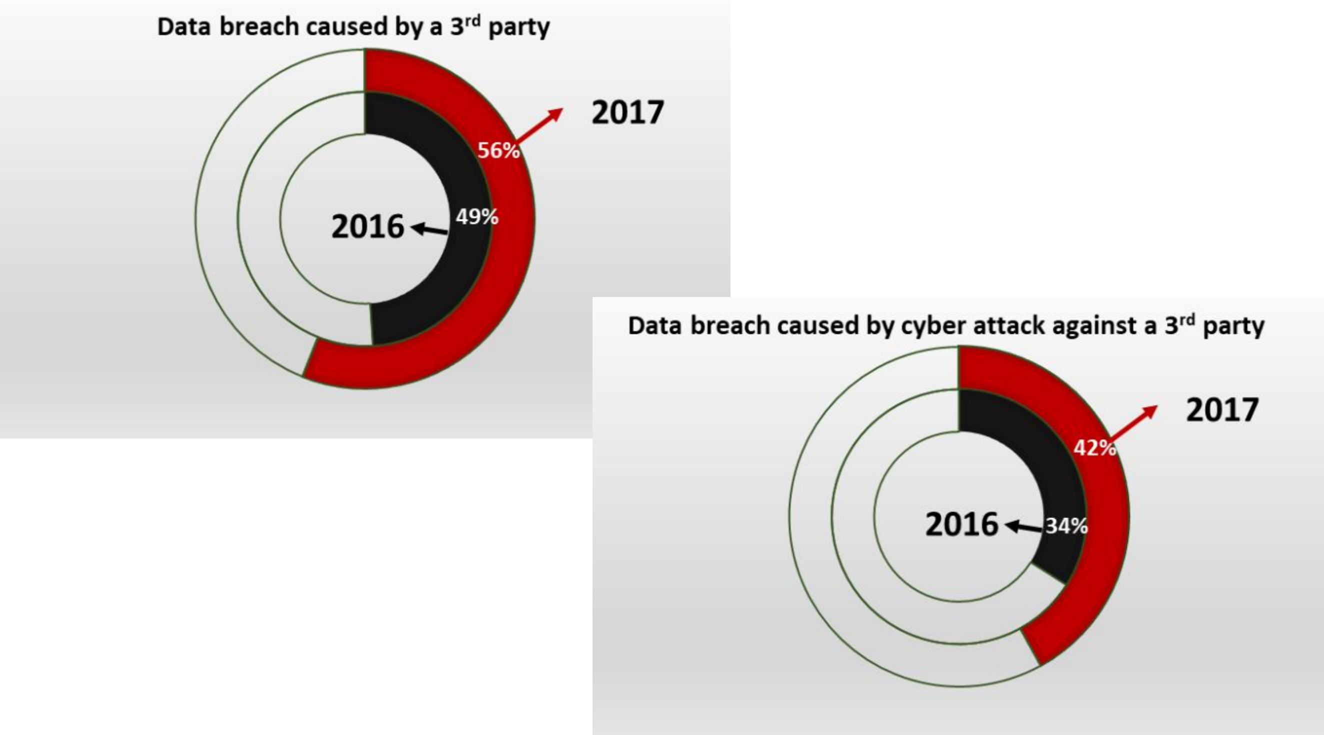
NormShield

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	PNIDigitalMedia	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 TiVo 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 much do you trust the cyber security measurements of 3rd-party companies?

A recent survey conducted by Ponemon Institute reveals that 56% have experienced a 3rd-party breach in 2017, which is an 7% increase compared to previous year[2]. Another survey conducted by Deloitte in 2016 gives more depressive numbers, 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.

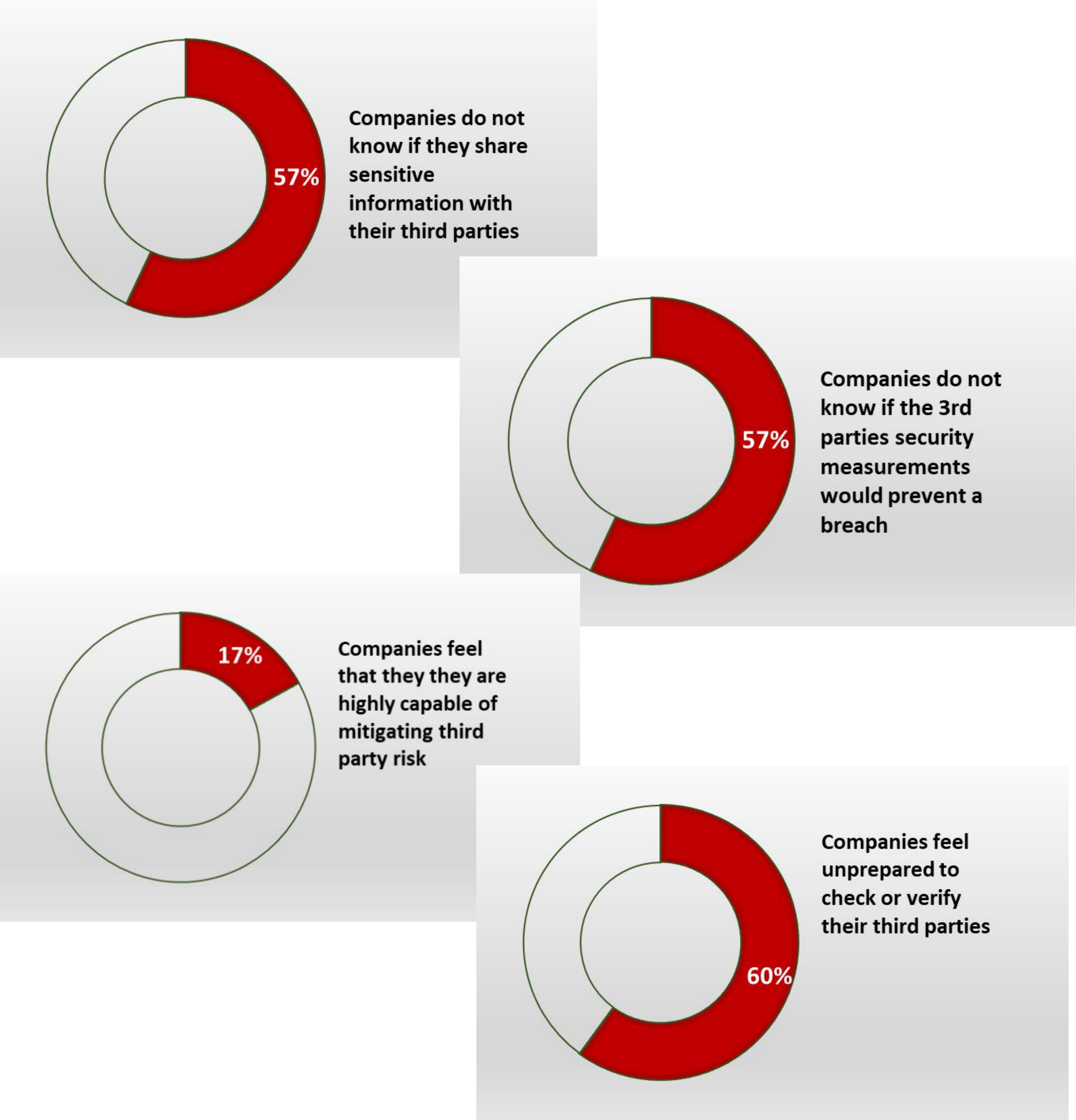
The fines paid because of the breaches are as quite large as more than 7 million $US per breach. For instance, Target paid more than $116 million in civil settlements related to its 2013 breach caused by an HVAC company. The total cost to company because of this breach exceeded $290 million. With upcoming GDPR, we shall see higher fines for each breach related to EU citizens. The GDPR fines can go up to 20 million Euros or 4% of annual global turnover (whichever is the highest).



[2] https://www.opus.com/ponemon/

How much do you know about third parties?

The Ponemon Institute report shows that 57% of companies do not know if they share sensitive information with third parties and they don’t know either if the third parties’ security measurements would prevent a breach. As a result, only 17% feel that they are highly capable of mitigating third party risk and 60% feel unprepared to check or verify their third parties.



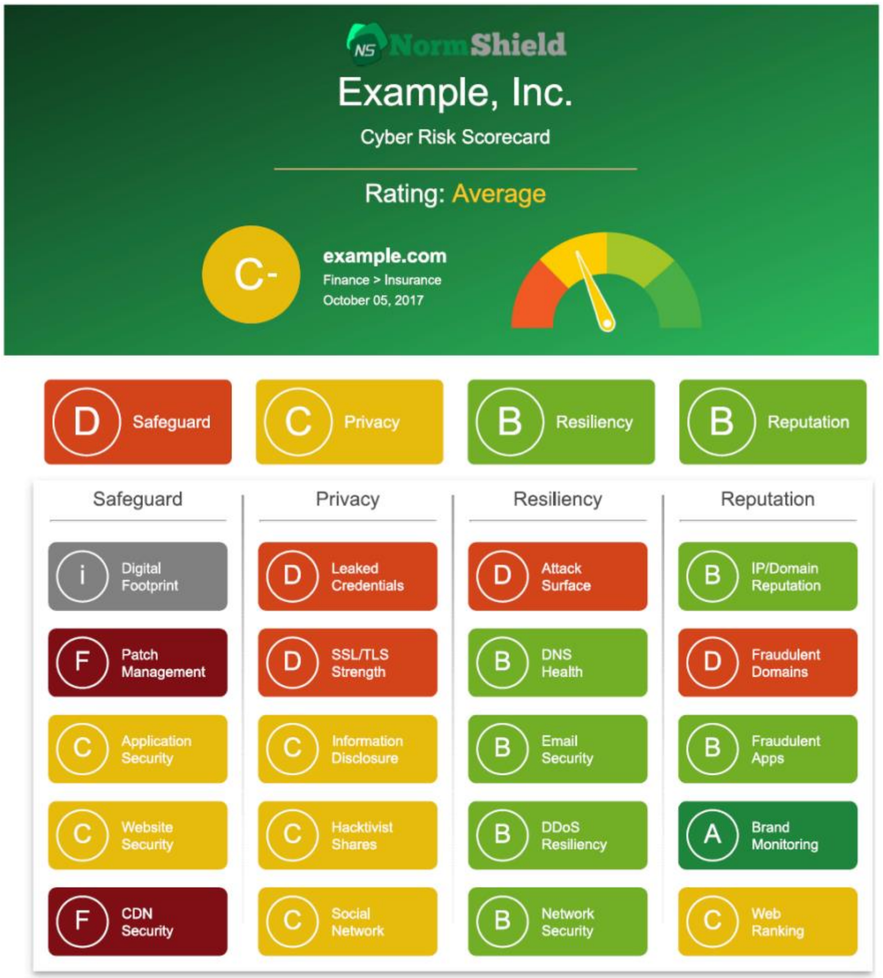
How to assess 3rd party risk?

Many companies either do not have any assessment on cyber risk of third parties or use old-school questionnaire methodology (sending a bunch of questions for third party to answer and assessing the risk based on the answer). First of all, questionnaire-based assessment is very time consuming (even though there are some online tools for it) and answers are not reliable. Even if we assume that answers are correct and we collect 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 data and provide a risk score or security rating for companies related to a certain company. NormShield, BitSight, Security Scorecard, UpGuard, and RiskRecon are top players in the third-party risk scoring business. They all provide risk scores or security rating for any company added as a third-party and assess its cyber risk and how it affects the main company. This type of information can also be used for mergers and acquisitions.

Using NormShield Cyber Risk Scorecard to assess third parties?

As an example, we explain how to use NormShield Cyber Risk Scorecard to assess the third parties for a company. In NormShield Cyber Risk Scorecard, you can create an ecosystem that will includes the main company and all the third-parties to be added. More than one ecosystem can be created such as an ecosystem including the companies/branches owned by the main company or an ecosystem for third-parties or you can even create an ecosystem which includes only law firms that you work with. Then, a third-party can easily be added by only typing its website. NormShield first discover the digital footprint of the third party (domains, subdomains, IP addresses, DNS Records, services, social media accounts, ASN, e-mails, company info, etc.) to *see what hackers see* on this third party. Then NormShield evaluates the cyber risk by its proprietary algorithm on 20 different categories and how the cyber risk of this third party affects the overall ecosystem. Below is a list of some categories taken into consideration;



NormShield

Example, Inc.

Cyber Risk Scorecard

Rating: Average

C-

example.com

Finance > Insurance

October 05, 2017

D Safeguard	C Privacy	B Resiliency	B Reputation
Safeguard	Privacy	Resiliency	Reputation
i Digital Footprint	D Leaked Credentials	D Attack Surface	B IP/Domain Reputation
F Patch Management	D SSL/TLS Strength	B DNS Health	D Fraudulent Domains
C Application Security	C Information Disclosure	B Email Security	B Fraudulent Apps
C Website Security	C Hacktivist Shares	B DDoS Resiliency	A Brand Monitoring
F CDN Security	C Social Network	B Network Security	C Web Ranking

Main company then can contact to third company and discuss the issues found by NormShield Cyber Risk Scorecard and remediate and mitigate the risk.

About NormShield

We provide Cyber Risk Scorecard for companies just like FICO score. Cyber security is on every Board's agenda, and the average total cost of a data breach has risen to $4 million (Ponemon/IBM). NormShield Cyber Risk Scorecards provide the information necessary to protect business from cyber-attacks. The scorecards provide a letter grade and a drill down into the data for each risk category so that remediation of vulnerabilities can be prioritized. Unified Threat & Vulnerability Orchestration Platform and Cyber Risk Scorecard.

To learn your company's risk score, please visit https://www.normshield.com/ and click on Learn Now.

www.normshield.com

1 (571) 335 02 22

info@normshield.com

NormShield HQ
8200 Greensboro Drive
Suite 900
McLean, VA
22102