BITSIGHT

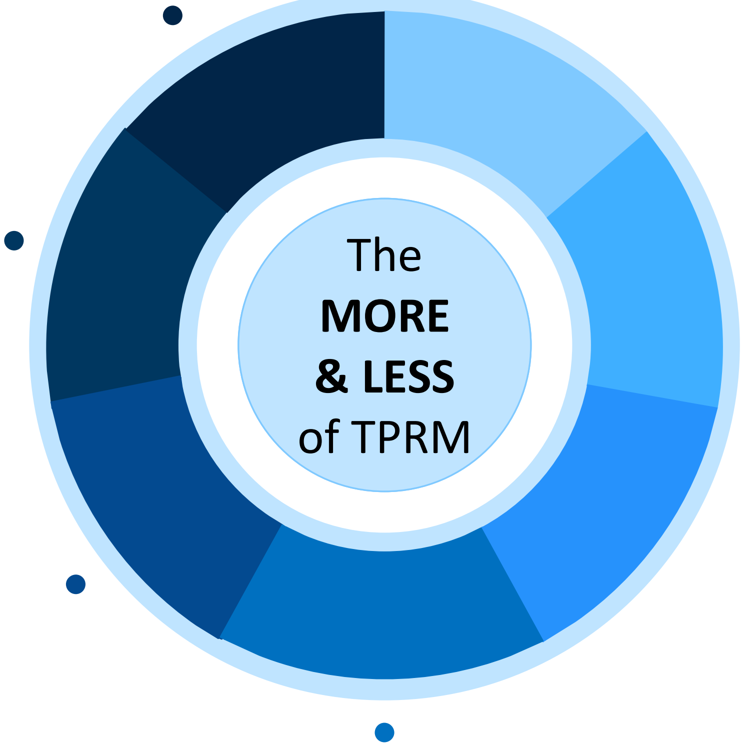
What would you do with **MORE** time?

www.bitsight.com

62% still lack standard process [1]

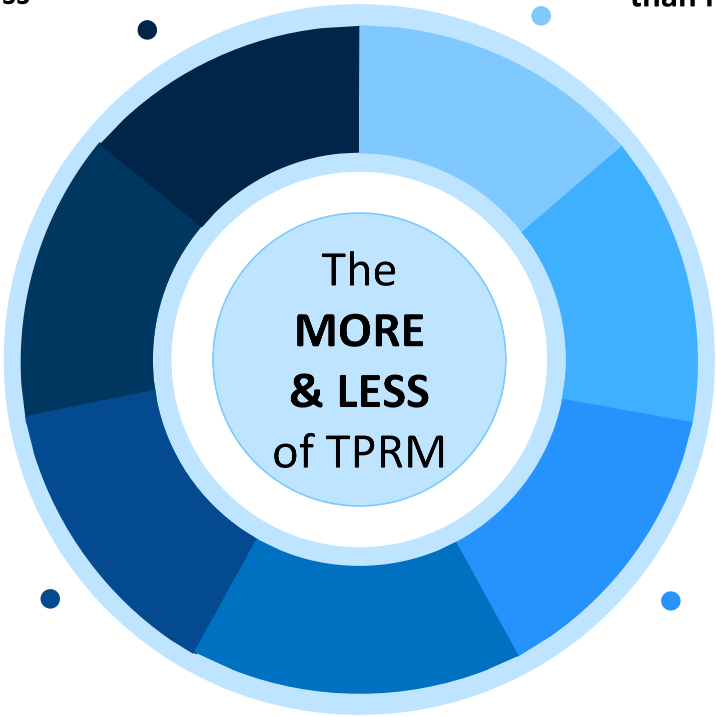
42% say resources (people & time) are biggest challenge [2]

59% struggle to get overall view of third-party risk [1]



The **MORE & LESS** of TPRM

17% of respondents assessed **25% or less** of their third parties [3]



The **MORE & LESS** of TPRM

62% still lack standard process [1]

Average vendor onboarding taking 90 days, **20 days more than it did 4 years ago** [4]

42% say resources (people & time) are biggest challenge [2]

Average company spends **17,000 hours annually** pulling together compliance reports and investigating security anomalies [5]

59% struggle to get overall view of third-party risk [1]

2 or more weeks to compile a board report [2]

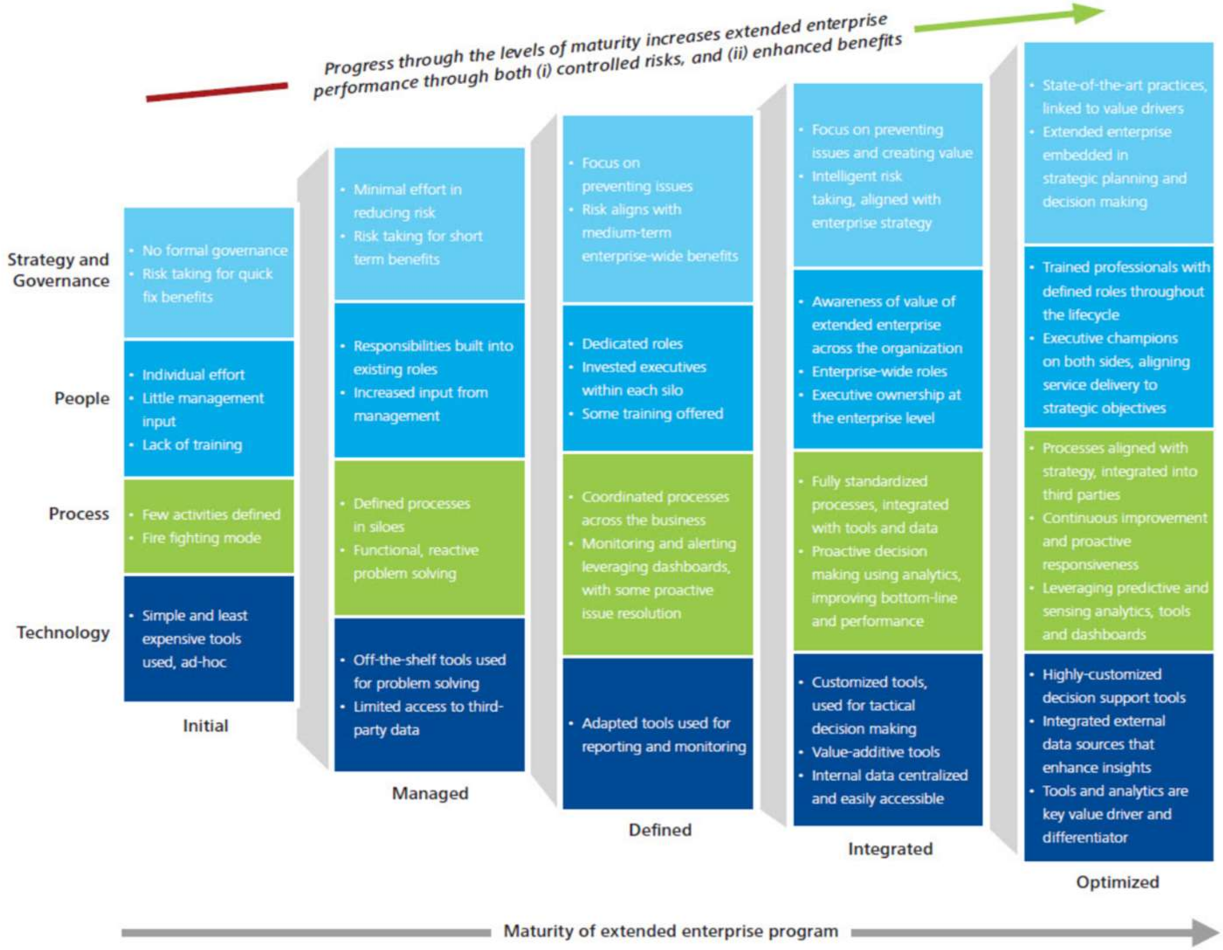
17% of respondents assessed **25% or less** of their third parties [3]

What we'll cover

- **How do you do "more with less"? Let's do the math!**
- What changes are required to be successful?
- Who has already done this successfully?
- What are the next steps?

Kimberly Johnson
Pr. Product Marketing Manager, TPRM
BITSIGHT

Before you begin…know where you are…



Progress through the levels of maturity increases extended enterprise performance through both (i) controlled risks, and (ii) enhanced benefits

	Initial	Managed	Defined	Integrated	Optimized
Strategy and Governance	• No formal governance • Risk taking for quick fix benefits	• Minimal effort in reducing risk • Risk taking for short term benefits	• Focus on preventing issues • Risk aligns with medium-term enterprise-wide benefits	• Focus on preventing issues and creating value • Intelligent risk taking, aligned with enterprise strategy	• State-of-the-art practices, linked to value drivers • Extended enterprise embedded in strategic planning and decision making
People	• Individual effort • Little management input • Lack of training	• Responsibilities built into existing roles • Increased input from management	• Dedicated roles • Invested executives within each silo • Some training offered	• Awareness of value of extended enterprise across the organization • Enterprise-wide roles • Executive ownership at the enterprise level	• Trained professionals with defined roles throughout the lifecycle • Executive champions on both sides, aligning service delivery to strategic objectives
Process	• Few activities defined • Fire fighting mode	• Defined processes in siloes • Functional, reactive problem solving	• Coordinated processes across the business • Monitoring and alerting leveraging dashboards, with some proactive issue resolution	• Fully standardized processes, integrated with tools and data • Proactive decision making using analytics, improving bottom-line and performance	• Processes aligned with strategy, integrated into third parties • Continuous improvement and proactive responsiveness • Leveraging predictive and sensing analytics, tools and dashboards
Technology	• Simple and least expensive tools used, ad-hoc	• Off-the-shelf tools used for problem solving • Limited access to third-party data	• Adapted tools used for reporting and monitoring	• Customized tools, used for tactical decision making • Value-additive tools • Internal data centralized and easily accessible	• Highly-customized decision support tools • Integrated external data sources that enhance insights • Tools and analytics are key value driver and differentiator

Maturity of extended enterprise program

It’s all connected!

People & Process Challenge =
Requires Process Change

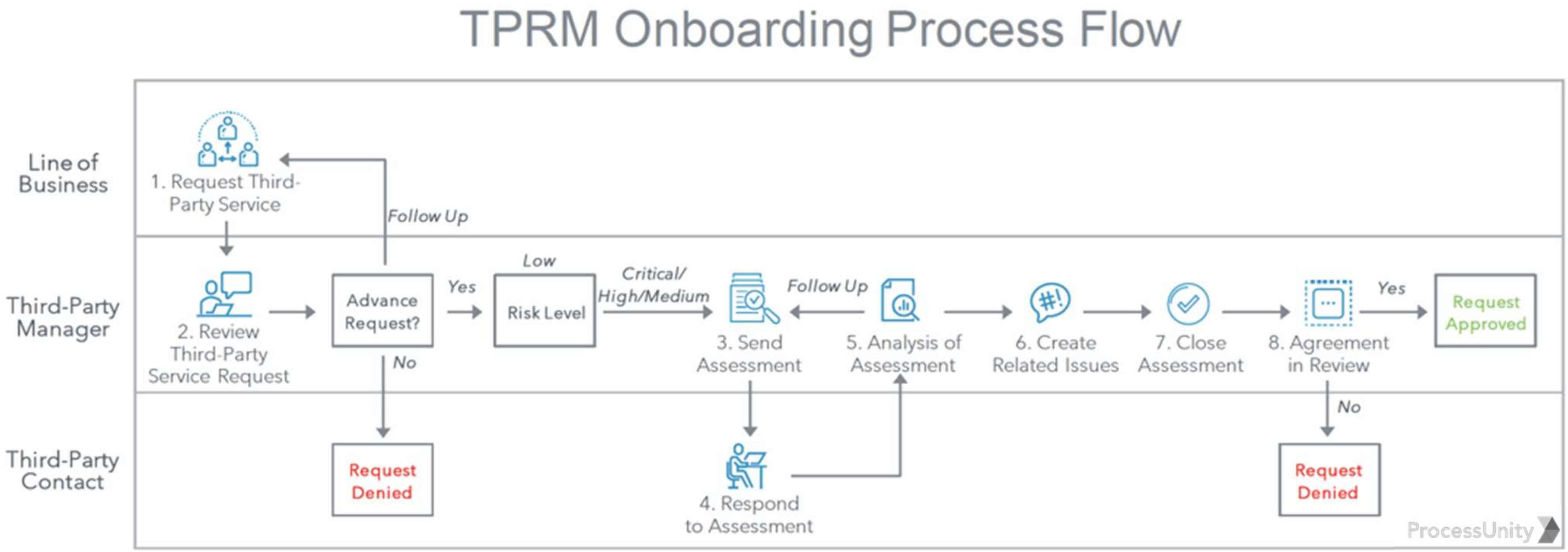
Process Change =
Improves Time & Cost

Improved Time & Cost =
Ability to Scale

Improved Time & Cost =
Ability to Scale

Onboarding 50 New Vendors Per Year

90 Days
16 Hours
$2,000



TPRM Onboarding Process Flow

Onboarding 50 New Vendors Per Year

90 Days
16 Hours
$2,000

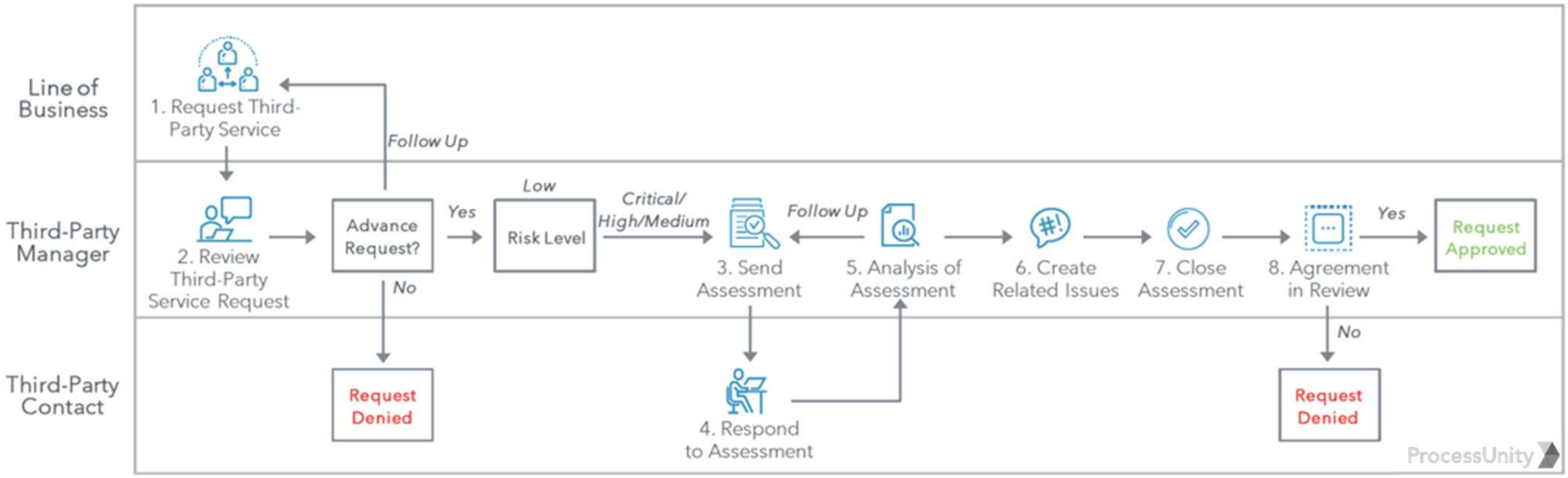
×

50
new vendors/yr

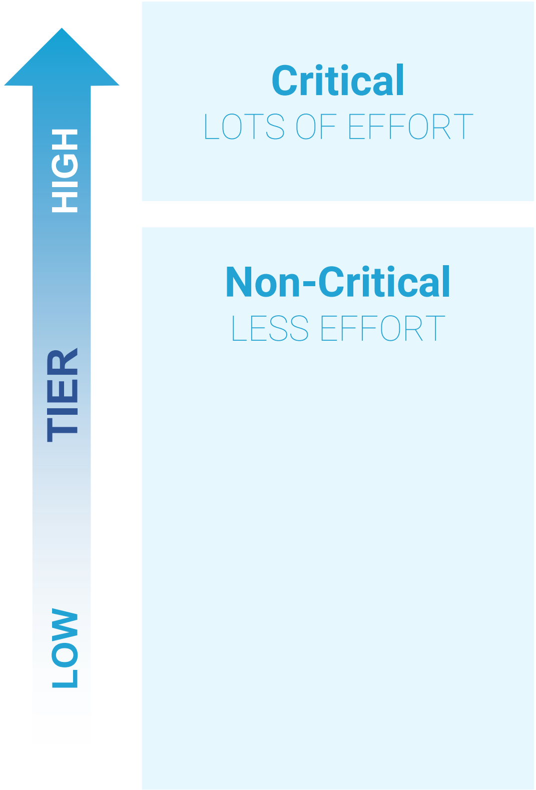
=

800 Hours
$100,000/yr

TPRM Onboarding Process Flow



Tiering is the foundation



HIGH

TIER

LOW

Critical
LOTS OF EFFORT

Non-Critical
LESS EFFORT

How much due diligence do I need to do for this vendor?

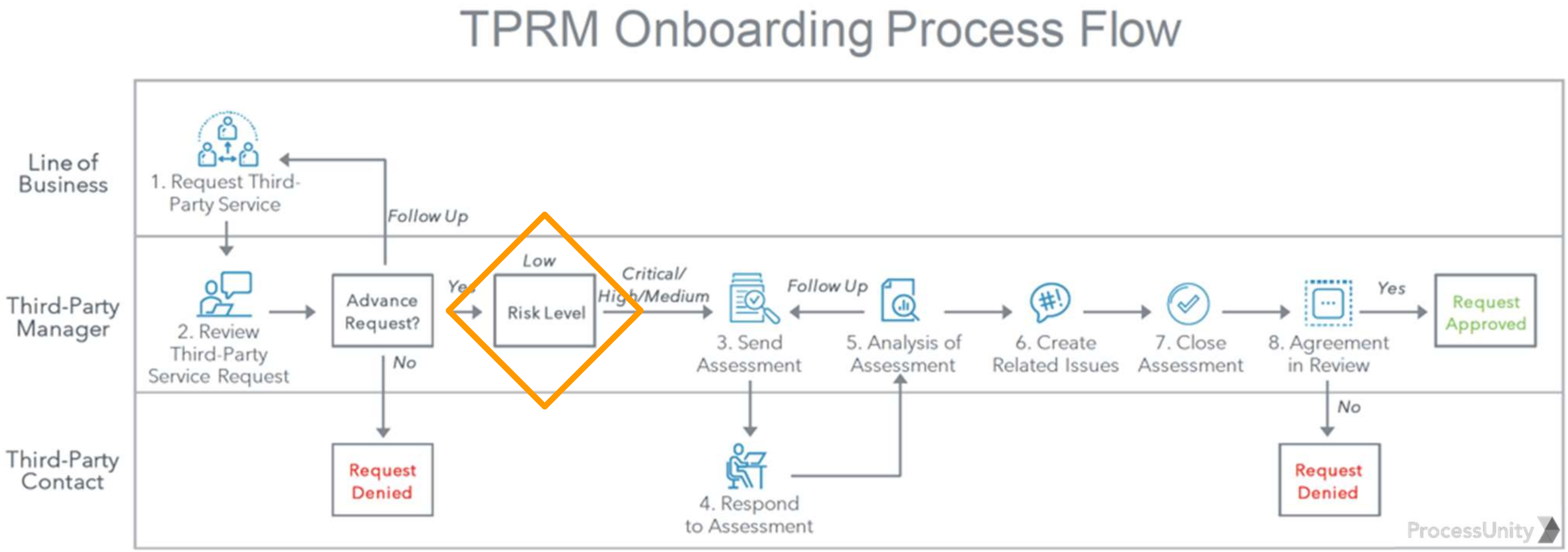
Onboarding 50 New Vendors Per Year

CRITICAL

90 Days
16 Hours
$2,000

NON-CRITICAL

14 Days
10 Hours
$1,200



TPRM Onboarding Process Flow

Line of Business

Third-Party Manager

Third-Party Contact

1. Request Third-Party Service

2. Review Third-Party Service Request

Advance Request?

Yes

No

Request Denied

Follow Up

Risk Level

Low

Critical/ High/Medium

3. Send Assessment

4. Respond to Assessment

Follow Up

5. Analysis of Assessment

6. Create Related Issues

7. Close Assessment

8. Agreement in Review

Yes

Request Approved

No

Request Denied

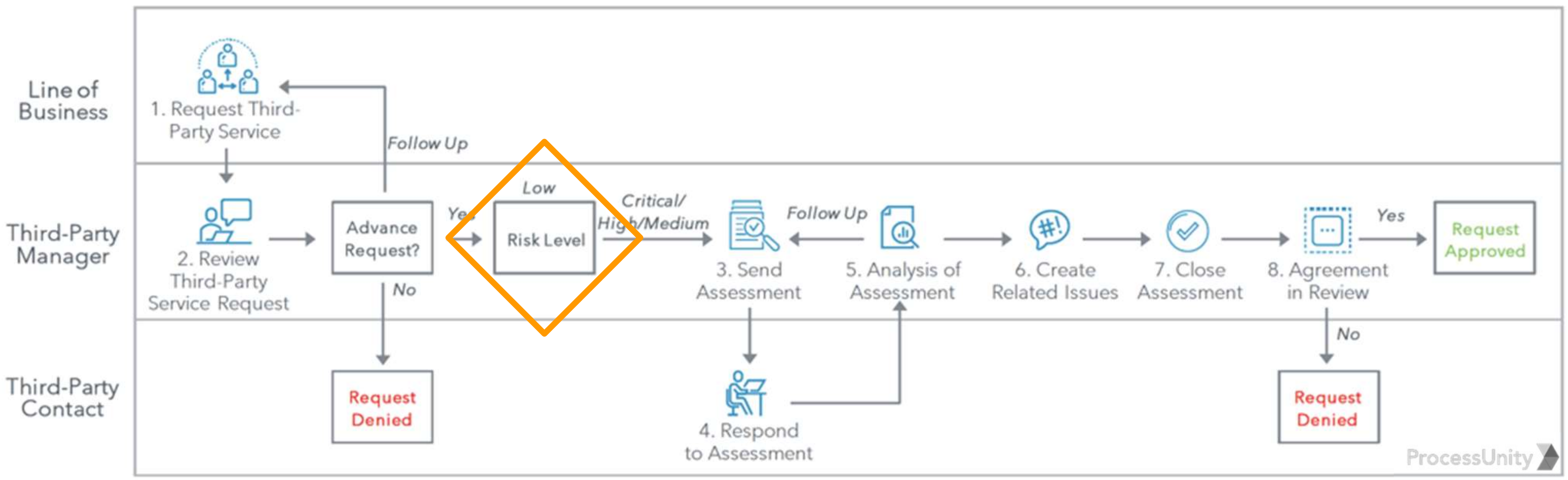
ProcessUnity

Onboarding 50 New Vendors Per Year

CRITICAL	90 Days 16 Hours $2,000	✖	**10** new vendors/yr	=	160 Hours $20,000/yr
NON-CRITICAL	14 Days 10 Hours $1,200	✖	**40** new vendors/yr	=	400 Hours $48,000/yr

TOTAL:
560 Hours (↓240)
$68,000/yr (↓$32K)

TPRM Onboarding Process Flow



More efficient…but is it less risky?

59% struggle to get overall view of third-party risk [1]

Third-Party Risk Manager

More efficient…but is it less risky?

INHERENT RISK

TIER 1 - CRITICAL

RESIDUAL RISK

What controls do they have in place?

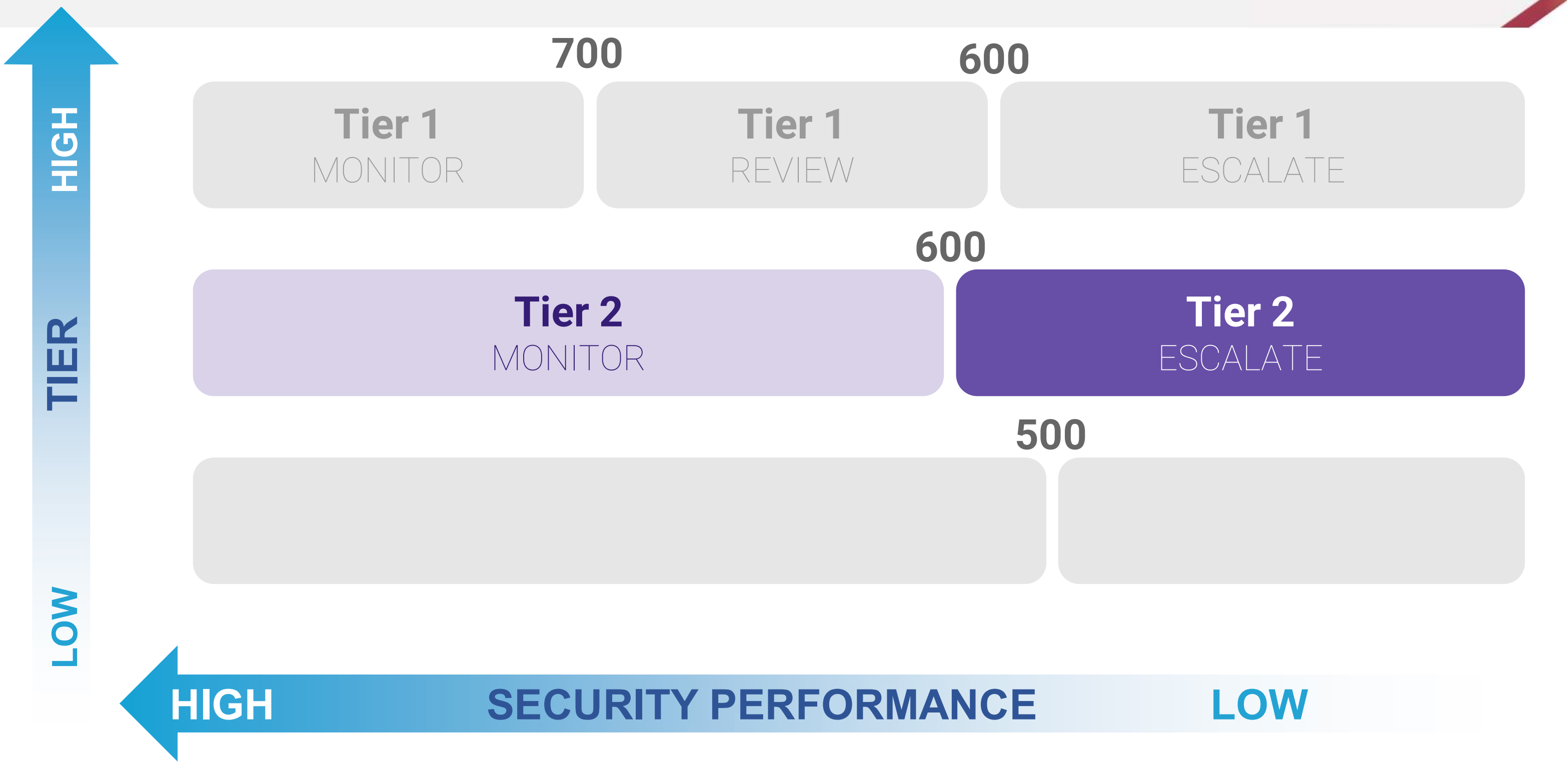
Third-Party Risk Manager

More efficient...but is it less risky?

So the question is...

How much **confidence** do you have in knowing the cybersecurity posture and risk of this third party?
#LIMITED

Security performance completes the picture



HIGH TIER LOW

700

600

Tier 1 MONITOR

Tier 1 REVIEW

Tier 1 ESCALATE

600

Tier 2 MONITOR

Tier 2 ESCALATE

500

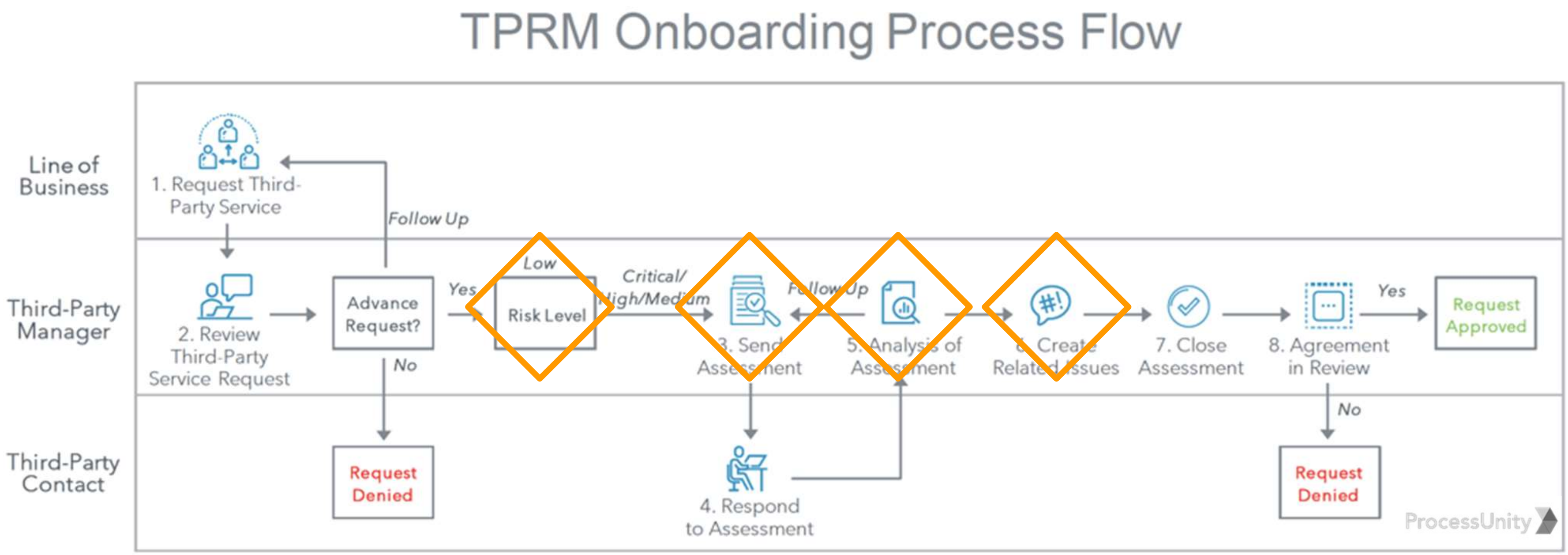
HIGH SECURITY PERFORMANCE LOW

How much due diligence do I need to do for this vendor?

Example: Policy Matrix

Initial Assessment / Onboarding			
	Tier 1	Tier 2	Tier 3
Rating >= 750 AND Botnet = A AND Open Ports > C AND File Sharing = A AND Breach = A	Partial questionnaire / assessment	Attestation (ISO, NIST, SOC)	Onboard (no assessment)
Rating 650-750	Full assessment	Partial assessment, focusing on gap areas	Attestation (ISO, NIST, SOC)
Rating 500-650 OR Botnet <=C OR Open Ports = F OR File Sharing <=C OR Breach >= C	Onsite audit	Outreach, possible onsite audit	Full assessment and Outreach
Rating < 500	Refuse vendor	Onsite audit	Outreach

Onboarding 50 New Vendors Per Year



Onboarding 50 New Vendors Per Year

CRITICAL > Risk Threshold	14 Days 10 Hours $1,200	×	**8** new vendors/yr	=	**80 Hours** **$9,600/yr**
CRITICAL < Risk Threshold	90 Days 16 Hours $2,000	×	**2** new vendors/yr	=	**32 Hours** **$4,000/yr**
NON-CRITICAL > Risk Threshold	2 Days 6 Hours $500	×	**30** new vendors/yr	=	**180 Hours** **$1,500/yr**
NON-CRITICAL < Risk Threshold	14 Days 10 Hours $1,200	×	**10** new vendors/yr	=	**100 Hours** **$12,000/yr**

TOTAL:

392 Hours
$27,100/yr

Onboarding 50 New Vendors Per Year

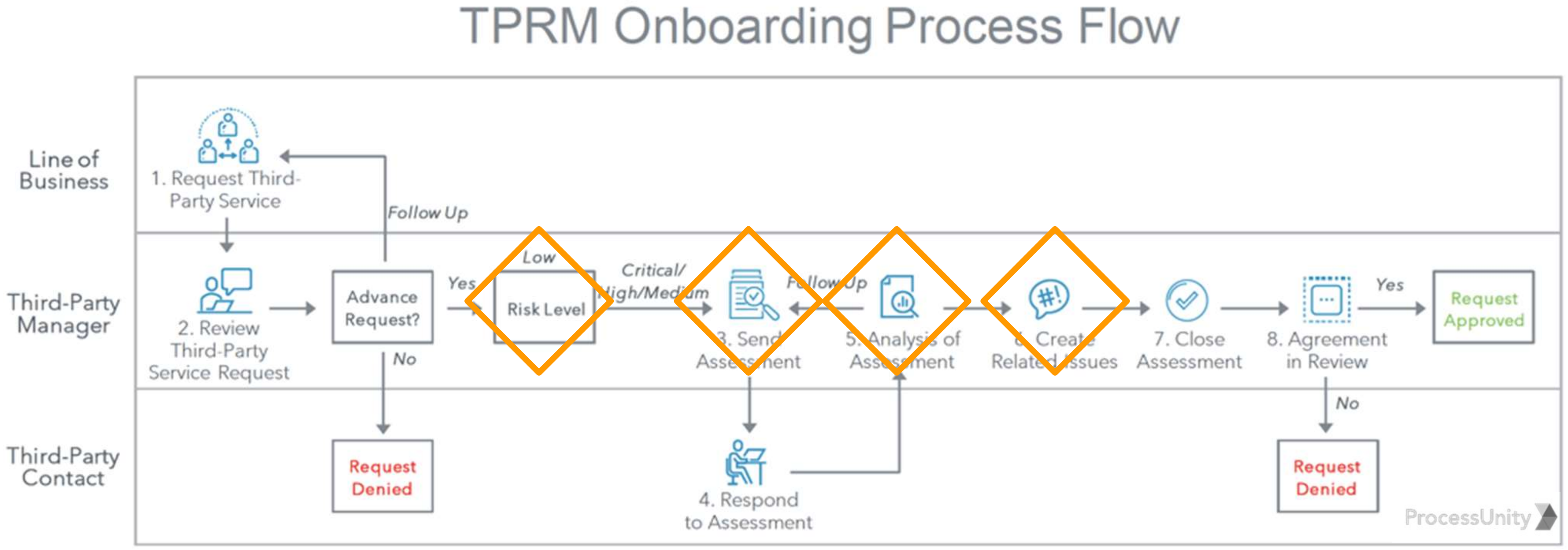
“ONE-SIZE-FITS-ALL”

800 Hours
$100,000

SAVE
408 hours &
$72,900

ADAPTIVE PROCESS

392 Hours
$27,100



Scale for the greatest risk reduction

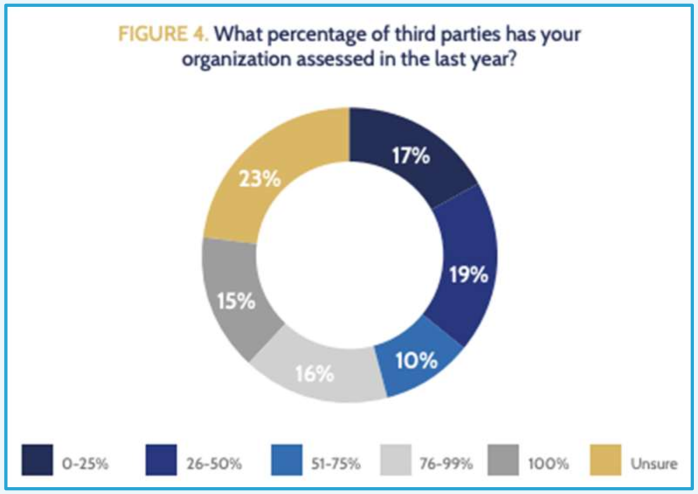


FIGURE 4. What percentage of third parties has your organization assessed in the last year?

Source - Cefpro IMPROVING THIRD-PARTY RISK MANAGEMENT PROGRAMS TO OPTIMIZE OPERATIONS

You can **now cover 80 vendors** using the **SAME resources.**

(800 hours; Avg. 10hrs/assessment)

Success stories

Cabela's

"It used to take us weeks to complete vendor assessments, now it takes us hours."

LLOYDS BANKING GROUP

"If we didn't have a security ratings platform we'd probably have to employ another ten people. It would be an absolute nightmare trying to understand what all the key cyber risks and issues are."

Nationwide Building Society

"BitSight has allowed us to onboard low-risk suppliers much more quickly and that means we are able to get tools and products into the hands of our transformation teams much more quickly."

What’s next?

- Know the maturity of your program to know what’s obtainable
- Look at each part of the program with a keen eye for efficiency not just risk reduction
- Ensure you include security performance for a complete view of risk you can trust

Be confident! that You CAN do more with less!

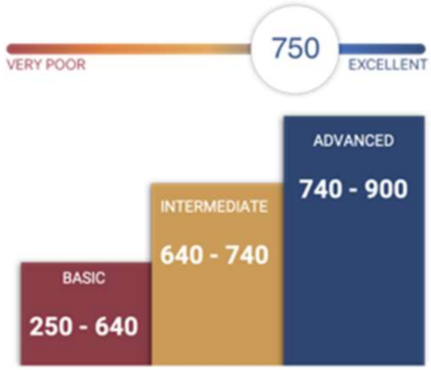
BitSight Helps Customers Tackle Cyber Risk

How secure is my organization?

SECURITY PERFORMANCE MANAGEMENT

- ➔ Assess cyber risk and compare to industry and peers
- ➔ Efficiently allocate resources to address cyber risks
- ➔ Set, track, report on program performance over time

BITSIGHT®



How secure are my third parties?

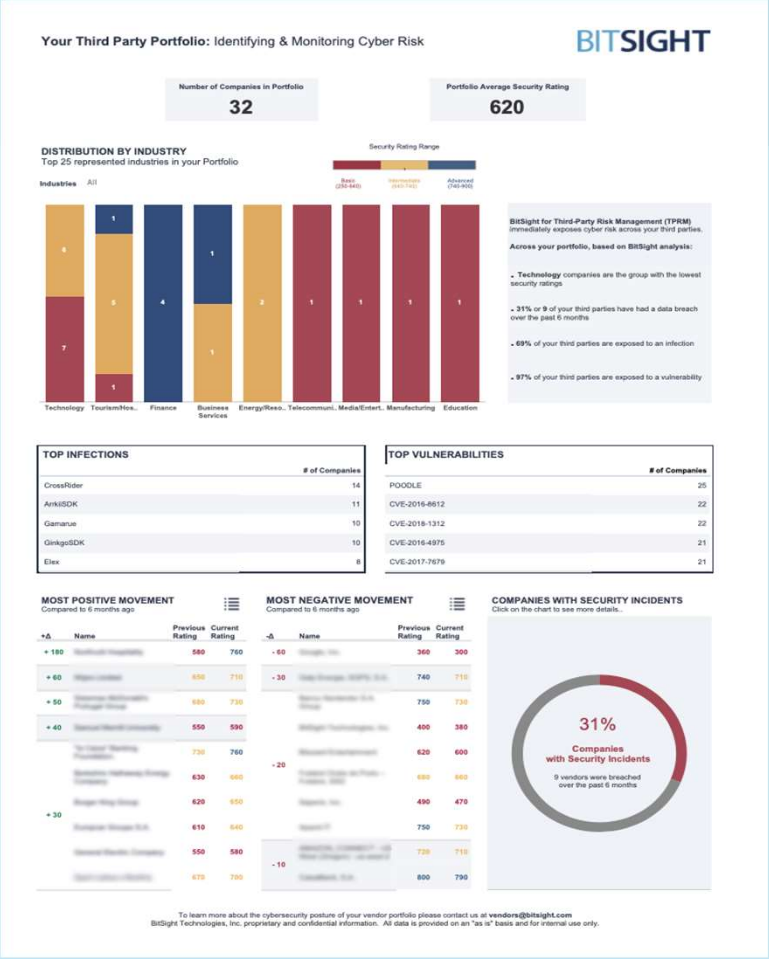
THIRD PARTY RISK MANAGEMENT

- ➔ Make cyber risk decisions at the speed of the business
- ➔ See where the cyber risk is across the supply chain
- ➔ Prioritize resources to focus on riskiest vendors
- ➔ Team up with vendors to remediate cyber risk

Cyber Insurance

Critical National Infrastructure

Mergers & Acquisitions



Your Third Party Portfolio: Identifying & Monitoring Cyber Risk

BITSIGHT

Number of Companies in Portfolio	Portfolio Average Security Rating
32	620

DISTRIBUTION BY INDUSTRY
Top 25 represented industries in your Portfolio

Industries All

BitSight for Third-Party Risk Management (TPRM) immediately exposes cyber risk across your third parties.

Across your portfolio, based on BitSight analysis:

- **Technology** companies are the group with the lowest security ratings
- **31%** or **9** of your third parties have had a data breach over the past 6 months
- **69%** of your third parties are exposed to an infection
- **97%** of your third parties are exposed to a vulnerability

TOP INFECTIONS

	# of Companies
CrossRider	14
ArrkiiSDK	11
Gamarue	10
GinkgoSDK	10
Elex	8

TOP VULNERABILITIES

	# of Companies
POODLE	25
CVE-2016-8612	22
CVE-2018-1312	22
CVE-2016-4975	21
CVE-2017-7679	21

MOST POSITIVE MOVEMENT
Compared to 6 months ago

+Δ	Name	Previous Rating	Current Rating
+ 180	[illegible]	580	760
+ 60	[illegible]	650	710
+ 50	[illegible]	680	730
+ 40	[illegible]	550	590
+ 30	[illegible]	730	760
	[illegible]	630	660
	[illegible]	620	650
	[illegible]	610	640
	[illegible]	550	580
	[illegible]	670	700

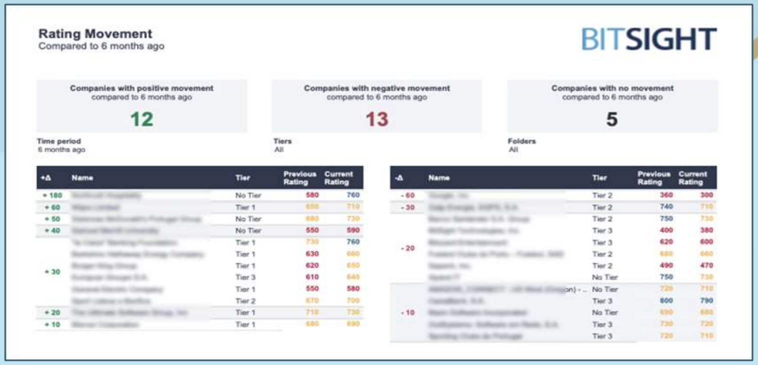
MOST NEGATIVE MOVEMENT
Compared to 6 months ago

-Δ	Name	Previous Rating	Current Rating
- 60	[illegible]	360	300
- 30	[illegible]	740	710
- 20	[illegible]	750	730
	[illegible]	400	380
	[illegible]	620	600
	[illegible]	680	660
	[illegible]	490	470
	[illegible]	750	730
- 10	[illegible]	720	710
	[illegible]	800	790

COMPANIES WITH SECURITY INCIDENTS
Click on the chart to see more details..

31%
Companies with Security Incidents
9 vendors were breached over the past 6 months

To learn more about the cybersecurity posture of your vendor portfolio please contact us at **vendors@bitsight.com**
BitSight Technologies, Inc. proprietary and confidential information. All data is provided on an "as is" basis and for internal use only.



Rating Movement
Compared to 6 months ago

BITSIGHT

Companies with positive movement compared to 6 months ago	Companies with negative movement compared to 6 months ago	Companies with no movement compared to 6 months ago
12	13	5

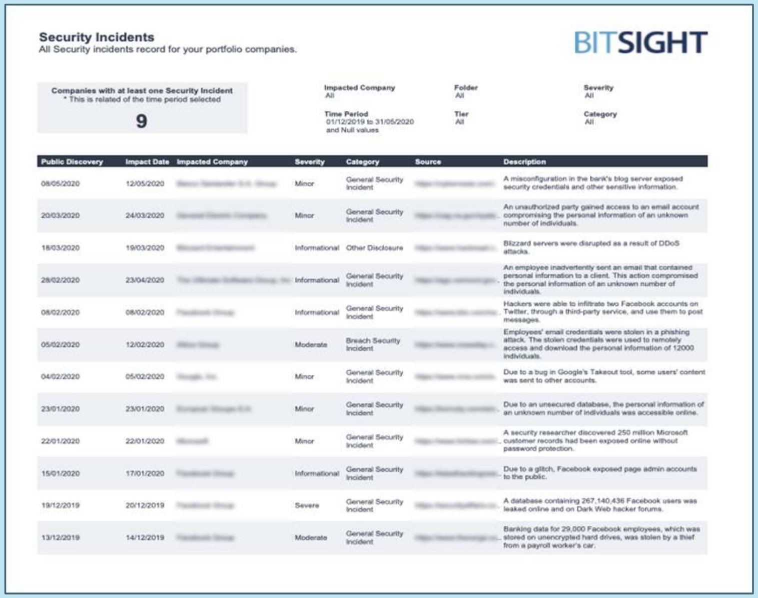
Time period
6 months ago

Tiers
All

Folders
All

+Δ	Name	Tier	Previous Rating	Current Rating
+ 180	[illegible]	No Tier	580	760
+ 60	[illegible]	Tier 1	650	710
+ 50	[illegible]	No Tier	680	730
+ 40	[illegible]	No Tier	550	590
+ 30	[illegible]	Tier 1	730	760
	[illegible]	Tier 1	630	660
	[illegible]	Tier 1	620	650
	[illegible]	Tier 3	610	640
	[illegible]	Tier 1	550	580
	[illegible]	Tier 2	670	700
+ 20	[illegible]	Tier 1	710	730
+ 10	[illegible]	Tier 1	680	690

-Δ	Name	Tier	Previous Rating	Current Rating
- 60	[illegible]	Tier 2	360	300
- 30	[illegible]	Tier 2	740	710
- 20	[illegible]	Tier 2	750	730
	[illegible]	Tier 3	400	380
	[illegible]	Tier 3	620	600
	[illegible]	Tier 2	680	660
	[illegible]	Tier 2	490	470
	[illegible]	No Tier	750	730
- 10	[illegible]on) - ...	No Tier	720	710
	[illegible]	Tier 3	800	790
	[illegible]	No Tier	690	680
	[illegible]	Tier 3	730	720
	[illegible]	Tier 3	720	710



Security Incidents
All Security incidents record for your portfolio companies.

BITSIGHT

Companies with at least one Security Incident * This is related of the time period selected
9

Impacted Company
All

Folder
All

Severity
All

Time Period
01/12/2019 to 31/05/2020
and Null values

Tier
All

Category
All

Public Discovery	Impact Date	Impacted Company	Severity	Category	Source	Description
08/05/2020	12/05/2020	[illegible]	Minor	General Security Incident	[illegible]	A misconfiguration in the bank's blog server exposed security credentials and other sensitive information.
20/03/2020	24/03/2020	[illegible]	Minor	General Security Incident	[illegible]	An unauthorized party gained access to an email account compromising the personal information of an unknown number of individuals.
18/03/2020	19/03/2020	[illegible]	Informational	Other Disclosure	[illegible]	Blizzard servers were disrupted as a result of DDoS attacks.
28/02/2020	23/04/2020	[illegible]	Informational	General Security Incident	[illegible]	An employee inadvertently sent an email that contained personal information to a client. This action compromised the personal information of an unknown number of individuals.
08/02/2020	08/02/2020	[illegible]	Informational	General Security Incident	[illegible]	Hackers were able to infiltrate two Facebook accounts on Twitter, through a third-party service, and use them to post messages.
05/02/2020	12/02/2020	[illegible]	Moderate	Breach Security Incident	[illegible]	Employees' email credentials were stolen in a phishing attack. The stolen credentials were used to remotely access and download the personal information of 12000 individuals.
04/02/2020	05/02/2020	[illegible]	Minor	General Security Incident	[illegible]	Due to a bug in Google's Takeout tool, some users' content was sent to other accounts.
23/01/2020	23/01/2020	[illegible]	Minor	General Security Incident	[illegible]	Due to an unsecured database, the personal information of an unknown number of individuals was accessible online.
22/01/2020	22/01/2020	[illegible]	Minor	General Security Incident	[illegible]	A security researcher discovered 250 million Microsoft customer records had been exposed online without password protection.
15/01/2020	17/01/2020	[illegible]	Informational	General Security Incident	[illegible]	Due to a glitch, Facebook exposed page admin accounts to the public.
19/12/2019	20/12/2019	[illegible]	Severe	General Security Incident	[illegible]	A database containing 267,140,436 Facebook users was leaked online and on Dark Web hacker forums.
13/12/2019	14/12/2019	[illegible]	Moderate	General Security Incident	[illegible]	Banking data for 29,000 Facebook employees, which was stored on unencrypted hard drives, was stolen by a thief from a payroll worker's car.

Contact vendors@bitsight.com for your **free Portfolio Performance Report**

Thank You & Questions

BITSIGHT

info@bitsight.com
www.bitsight.com