SAFE

WHY CYBERSECURITY RISK RATINGS ARE NOT ENOUGH

A Third Party
Risk Management Special

Whitepaper | May, 2022

www.safe.security

EXECUTIVE SUMMARY

> *"Businesses have moved through the journey of self-provision to being supplemented by cloud, third-party, and SaaS services. Current third party risk management practices are failing to address this"*
>
> - **David Reilly, CIO (Bank of America),**
> in *The CIO Perspective, 2022*[1]

Enterprise cyber risk management is growing in complexity, and some of the most critical and damaging risks are borne not within an organization but in its third, fourth, or *'nth*-party' supply chain.

According to a 2020 Ponemon Sullivan Report[2], "the typical enterprise has an average of 5,800 third parties." This dependence on vendors results in an exponentially increasing attack surface that becomes more difficult to manage. To alleviate this, third party risk management (TPRM) has been largely reliant on Security Rating Services – but it's an approach that creates a false sense of security.

In 2018, industry analysts Forrester reported:
"Cybersecurity Risk Ratings Tackle A Ballooning Third-Party Problem"[3]

Pivoting in 2021 to:
"Cybersecurity Risk Ratings Are Not Yet Ready For Prime Time"[4]

Why? Cyber risk exists across your employees, policies, technologies, third parties, and supply chain. Each of your vendors has risks and vulnerabilities that you will automatically inherit when you outsource functions to them, and grant permission to access your data and systems.

Your questionnaire-based surveys, SRS services, and the subsequent security rating scores do NOT reflect the volume or impact of this critical risk – providing you with an incomplete, inaccurate representation of your third party cybersecurity risk. Moreover, these services offer limited capabilities to contextualize the risk - leaving your ratings mostly unactionable.

If you already have an SRS solution in place, whether it's DIY or outsourced, the positive news is that you're already halfway there. This whitepaper will examine the strengths and limitations of outside-in vs. inside-out approaches to third party risk assessment and explore the solution: a shift from identifying risk to quantifying risk.

HOW EXPOSED IS YOUR ORGANIZATION TO THIRD PARTY RISK?

Third party attacks are dominating global news more than ever before. It's no coincidence that organizations depend on external vendors and supply chains for business operations to remain competitive. Every part of a business is open to attack and compromise: its people, processes, technology, vendors, and suppliers.

Unless you understand the level of access vendors have, why they have it, who uses it, and how, you will not have complete visibility of the risk you're exposed to.

The extent of your exposure might surprise you. Consider the following:

- Are you sharing your data? Do you know exactly what or how much?
- Are you sharing your code or IP with a co-development partner?
- Are you sharing data with your agencies?
    - Does your marketing agency hold customer data or Personally Identifiable Information?
    - Do your vendors have access to your Intellectual Property?
    - Does your company insurance provider store your employee's Personal Health Information?

In turn, this increases the risk of a multitude of attacks:

- A vendor might accidentally share sensitive data.
- A malicious employee within your supply chain could misuse proprietary information.
- Ransomware could be deployed in your vendor's network, leaving your data vulnerable.

You are spending millions of dollars to defend your network and data, **but is an outside-in-based security rating enough to address the magnitude of risk posed by your third parties?** Let's take a look at the case for using Security Ratings Services.

THE CASE FOR SECURITY RATINGS SERVICES

Questionnaire-based TPRM and the Security Rating Services (SRS) markets are projected[5] to reach USD 6.8 billion by 2024. SRS, in particular, provide a quicker, cheaper method to perform third party risk assessments, making them a popular choice. They attempt to represent an organization's level of risk in the form of a score – not dissimilar to credit ratings in finance.

They work by performing an outside-in scan of publicly available databases for vulnerabilities across all third parties of a business. This process, known as *digital footprinting*, requires *just* the vendor's domain name to complete. Once the details are fed into an automated system, the scan corroborates its findings to generate a single risk rating or 'score' for the firm's third party cybersecurity risk posture.

According to The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021 report[4], the most common use cases supported by these solutions include cybersecurity vetting and continuous monitoring within third-party risk management (TPRM), enterprise security risk management and benchmarking, M&A due diligence, executive or board-level communication, and cyber insurance policy underwriting.

The Case in Favor of Cybersecurity Risk Ratings

- Non-intrusive
- Quick
- Simple representation as a score
- Economical
- Minimal resources and effort
- Point-in-time reports for audits

Security Risk Ratings will continue to have relevance in the industry, but **when it comes to protecting your enterprise from advanced attacks and having complete visibility of your networks, they have severe limitations that you need to be aware of.**

Why Security Risk Ratings May Leave You Open To Attack

Imagine you're trying to assess the risk of fire in an apartment. Would you be confident that it is secure by only looking at its external surface, bricks, and mortar? Would you not want to look around the inside of the apartment - for dangerous appliances, faulty electrical sockets, potential fire hazards, or any maintenance logs?

By only assessing from an *outside-in* perspective and excluding an inside-out inspection, your visibility and judgment of risk are not just restricted but **inaccurate, incomplete, and potentially misleading.**

Forrester's analysis echoes this[4]:

> *"The market has come a long way since the last Forrester New Wave™ published in 2018, with many improvements in ratings accuracy, asset attribution, and workflow improvements made by many of the CSR platforms. However,* ***the market is still immature, with several improvements required before it's ready to be considered as a mature, enterprise-ready class of security solutions.****"*

OUTSIDE-IN APPROACH	INSIDE-OUT APPROACH
Use outside in knowing there are risks and limitations	Use inside out alongside outside-in for complete visibility of risk
Score represents incomplete measurement of risk	Score represents complete measurement of third (nth) party risk
Low accuracy and risk visibility	High accuracy and complete risk visibility
High risk of misleading information providing a false sense of security	High confidence and trust from the board, stakeholders, investors
Periodic, point-in-time assessment	Continuous, real-time assessment

The Limitations of Security Risk Ratings

- **Only provides point-in-time assessments, with no dynamic and real-time updates to reflect the changing threat landscape.** This results in the score becoming dated, providing just a snapshot view of third party risk, making it untenable for future initiatives.

- **Only covers external-facing assets. It does not account for internal endpoints, employees, policies, and cloud assets that represent a significant risk percentage.** Vendors often patch their public-facing vulnerabilities without attributing resources to continuously maintain internal cyber hygiene, leaving your organization exposed.

- **The scan leverages multiple publicly available databases but remains superficial** as it does not factor in internal audit reports or due diligence analyses.

- **They typically do not map vendor risk data against globally accepted compliance frameworks,** reducing the transparency of their algorithm, a concern that Forrester, in a 2021 report, echoes[4].

- **The SRS output often shows a high number of false positives, misleading security teams** into action or inaction, with a knock-on effect of yielding low confidence.

- **The score generated by SRS scans only indicates the cyber risk posture of your vendor ecosystem without providing prioritized solutions** to accept, mitigate, or transfer the risk.

Case Study: The Okta Breach, 2022 Underscores Why You Must Go Beyond SRS

The compromise was a successful breach of a Sitel employee's insecure device. The Lapsus$ group gained remote access to a laptop belonging to their employee containing sensitive information belonging to Okta.

With known external vulnerabilities patched, Okta *believed* that Sitel's cybersecurity risk posture was good. Why? **Sitel's outside-in cybersecurity rating score was 4.3 out of 5, or Grade A - considered higher than the industry average.** However as you'll recall, outside-in assessments do not include internal risk assessments of endpoints, cloud assets, people, or policies.

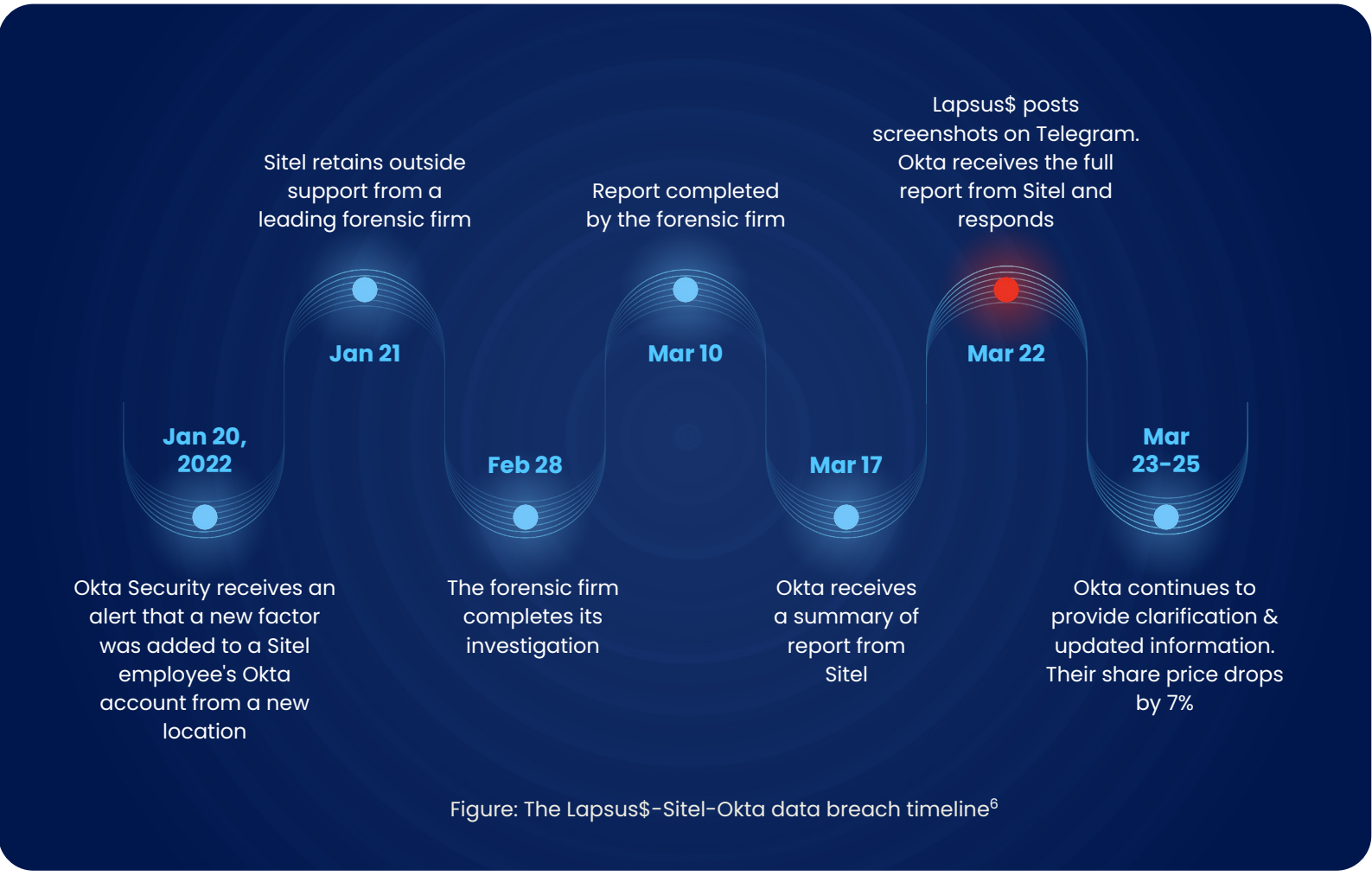

Figure: The Lapsus$-Sitel-Okta data breach timeline[6]

Okta trusted the outside-in assessment of their vendor's risk, and faced negative consequences. How might it have been avoided?

1. Monitor, measure, and mitigate risk in real-time
2. Evaluate the internal risk introduced by its third (and nth) party vendors
3. Gain complete and accurate visibility of who had access to their company's sensitive data, why they had access, when they used it, or if they even needed it.

UNLOCK VISIBILITY OF YOUR ENTIRE RISK POSTURE WITH INSIDE-OUT

If you are starting your journey toward proactive and quantified third party risk management, SRS provides a good starting point. However, it will only achieve so much, and you must be aware of its limitations. Let's explore the inside-out assessment of your vendors.

Inside out is activated by accessing API keys used by your third parties. To streamline the process, prioritize and select vendors for assessment according to criticality: their size, revenue, type of data shared, level of access, permissions, etc. The significant benefit of inside-out solutions is that they also assess your vendors, PLUS *their* vendors (*nth* parties)[7].

The Case for Inside-Out:

- Assesses **People Risk:** Assessing compromised systems to detect systems and applications involved in malicious and/or unusual activity
- Assess **Policies and Permissions**: Breach Exposure Assessment for identification of accidental or intentional exposure of potentially sensitive information
- Assesses **Technology Risk**: Email Security, DNS Security, Application Security, Network Security, and System Security assessments
- Performs **cyber reputation analysis** to identify threats that may damage your brand's reputation and revenue. In Okta's case, the company not only hit the headlines following news of the Lapsus$ breach, but their share price dropped by more than 7%[8].

A word of caution: Combining the two approaches may create an overwhelming volume of risk data – too much for your security team to find an efficient method of risk assessment, prioritization, and management. **This is why cyber risk management remains fundamentally broken and requires a new mindset: moving beyond risk identification to Cyber Risk Quantification.**

Using Cyber Risk Quantification for Proactive Cyber Risk Management

By combining the traditional outside-in approach with an inside-out assessment, you'll gain 360° visibility of your third party risk posture across your attack surface. Plus,

A real-time indicator of how likely your organization is to be breached via a third party

- ✓ You get total transparency of the inside-out risk your vendors are posing, not just from their publicly exposed data but also from internal cybersecurity risk posture analyses.
- ✓ You'll gain the ability to ringfence your critical assets from your riskiest vendors and inform what level of access you're safe to grant and to whom - with confidence.
- ✓ You'll be equipped with the ability to identify assets that do not match your required security benchmarks and retire them based on your risk appetite and tolerance.

You transform your third party risk communication to the board

- ✓ You will be equipped to move away from technical reports. You get access to a real-time representation of your third party risk in a language your board understands – the potential cost of third party cyber risk to your business.
- ✓ Remove the guesswork from your cybersecurity planning using the 'dollars and cents' data to justify and prioritize your security budget.

Avoid unfair cyber insurance premiums and rocketing costs

- ✓ CRQ solutions provide continuous, real-time assessment of your entire risk profile. With this data, you can negotiate a better deal, and insurance underwriters may be less inclined to inflate the cost of your coverage to account for uncertainties.
- ✓ Optimize your strategies for accepting, mitigating, or transferring risk through enhanced visibility and accuracy of your risk posture assessment.

CONCLUSION

Cybersecurity Rating Services will continue to lead the market in the immediate future, but leaders must use these solutions knowing their limitations. The process may be quick and economical, but the assessment will date quickly, adding limited value to data-driven decision-making.

To achieve complete, accurate, and continuous third party risk visibility, your business need to move beyond potentially misleading SRS that are leaving it open to a potential breach, and adopt a new mindset that resolves the shortcomings of modern cyber risk management.

By embracing the combination of inside-out and outside-in assessments using Cyber Risk Quantification, you will gain more accurate and real-time visibility of the cyber risk you've inherited across your vendors' people, processes, technologies, and third (*nth*) party ecosystems.

We are already seeing CRQ gain traction in the market. The failures of modern risk management are more apparent as major third party attacks become a regular occurrence. Forrester has already pivoted away from SRS and acknowledges its shortcomings as the answer to TPRM[4].

The journey to combine the results of questionnaire surveys, Cybersecurity Risk Ratings, and inside-out is long and requires an in-depth understanding of the process. This capability cannot be built overnight. Safe Security's whitepaper "How to Measure, Manage, and Mitigate third Party Risk in Real-Time" gives you a guide and 25-point checklist to get you started[7].

ABOUT SAFE SECURITY

Safe Security is a **leader in "Cybersecurity and Digital Business Risk Quantification" (CRQ)**
We help global enterprises across industries navigate towards a more accurate, effective, and cost-efficient system that proactively protects them against sophisticated and advanced cyberattacks.

For more information, visit our website for case studies, whitepapers, and other useful resources to help you begin your journey to Cyber Risk Quantification: www.safe.security

REFERENCES

1. Webcast (2022): The CIO Perspective: Why Your Board Must Take Action on Cyber Risk. Available to watch on: https://us.resources.cio.com/whitepaper/protecting-critical-infrastructure-in-an-age-of-uncertainty-4/

2. Report (2020): Digital Transformation & Cyber Risk: What You Need To Know To Stay Safe, Ponemon Institute and Sullivan Privacy Report. Available for download from: https://ponemonsullivanreport.com/2020/07/digital-transformation-cyber-risk-what-you-need-to-know-to-stay-safe

3. Report (2018): The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018. Available for download from: https://www.forrester.com/report/The-Forrester-New-Wave-Cybersecurity-Risk-Rating-Solutions-Q4-2018/RES142874

4. Report (2021) The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021. Available for download from: https://www.forrester.com/report/The-Forrester-New-Wave-Cybersecurity-Risk-Ratings-Platforms-Q1-2021/RES161625

5. Report (2019): Third-Party Risk Management Market by Component and Service , Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2024. Available for download from: https://www.marketsandmarkets.com/Market-Reports/third-party-risk-management-market

6. News (2022): SiliconANGLE, Ripple effects from the Okta security breach are worse than you think. Available to read on: https://siliconangle.com/2022/04/09/ripple-effects-okta-security-breach-worse-think/

7. Whitepaper (2022): How to Measure, Manage, and Mitigate Third Party Risk in Real Time, Safe Security. Available for download from: https://www.safe.security/resources/white-papers/measure-manage-and-mitigate-third-party-risk/

8. News (2022): Business Insider, Okta plunges after hackers claim cyberattack that puts thousands of the company's business customers at risk. Available to read on: https://www.businessinsider.in/stock-market/news/okta-plunges-after-hackers-claim-cyberattack-that-puts-thousands-of-the-companys-business-customers-at-risk/articleshow/90379821.cms

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306

www.safe.security
info@safe.security