SAFE

A False Sense of Security:

Why Cybersecurity Risk Ratings Are Not Enough *(and how they could lead to a breach)*

Take the recent **Lapsus$-Okta** breach. It originated from a vendor subsidiary, **Sitel** - a contact center organization. With known external vulnerabilities patched, Okta *believed* that Sitel's cybersecurity risk posture was good. Why? **Sitel's outside-in cybersecurity rating was 4.3 out of 5, or Grade A - considered *higher* than the industry average.**

Jan 20, 2022
Okta Security receives an alert that a new factor was added to a Sitel employee's Okta account from a new location

Jan 21
Sitel seeks support from a leading forensic firm

Feb 28
The forensic firm completes its investigation

Mar 10
Report completed by the forensic firm

Mar 17
Okta receives a summary of the report from Sitel

Mar 22
Lapsus$ posts screenshots on Telegram
Okta receives the full report from Sitel and responds

Mar 23-25
Okta continues to provide clarification and updates. Its share price drops by 7%

But how did this breach happen, if they had such a high outside-in security rating? Here's where it all went wrong for Okta:

1. They didn't measure, monitor, or mitigate risk in real-time
2. They didn't evaluate the internal risk introduced by third (and *nth*) party vendors
3. They had limited visibility of who had access to their sensitive data, why they had access, when they used it, or if they even needed it

This data breach demonstrates why you must go beyond SRS alone.

Outside-in assessments provide an incomplete and inadequate view of risk

Cybersecurity Risk Ratings have their place in the industry but it's important to know their strengths and limitations

OUTSIDE-IN

- Non-intrusive; no access required
- Only assets deemed of interest are assessed
- Only external-facing assets of the third party are assessed
  Risk from internal sources such as endpoints, cloud assets are not included
- Does not map information against compliance frameworks
- Sources data from public provider databases
- Quick, point in time assessment
- High number of false positives
- Decision Usefulness: Low

INSIDE-OUT

- Requires API keys to assess risk within the organization
- All third parties' risk are measured, including *nth* party risk
- Risk from external and internal assets - endpoints, cloud assets of third and *nth* parties - are measured
- Maps information against compliance frameworks
- Gathers data from external databases and vendor's internal reports
- Not as quick, but provides a continuous and real-time assessment
- Low number of false positives
- Decision Usefulness: High

Cyber Risk Quantification combines outside-in assessments with inside-out capabilities for 360° visibility of third party risk

- The score represents complete measurement of third (nth) party risk
- Continuous and real-time assessment
- High accuracy and complete risk visibility
- High confidence and trust from the board, stakeholders, and investors
- Prioritized recommendations to accept, mitigate, or transfer risk

Okta breach timeline source: Ripple effects from the Okta security breach are worse than you think - SiliconANGLE

Building a native 360° third party risk assessment capability is not possible overnight. **Safe Security is a leader in Cybersecurity and Digital Business Risk Quantification (CRQ).** We enable multiple Fortune 500 companies and global enterprises to create agile and real-time third party risk management strategies.

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

www.safe.security

SAFE