A Guide to Outcome-Driven Metrics for Supply Chain Cyber Risk Management

- ✓ The need for outcome-driven metrics
- ✓ Crafting outcome-driven metrics
- ✓ Security Operations: Third-party cyber risk reporting
- ✓ Operational metrics
- ✓ Tactical metrics

SecurityScorecard

The need for outcome-driven metrics

Senior executives and boards demand assurance that cybersecurity investments deliver expected outcomes. However, the current state of cybersecurity metrics, which are typically backward-looking and do not support decision-making, fail to align with business goals.

For instance, the National Institute of Standards and Technology (NIST) cybersecurity audit questions, while valuable for assessing the existence of controls, need more depth to evaluate their performance or levels of protection. This is where outcome-driven metrics come in, as they allow CISOs to demonstrate the benefits of cybersecurity investment by measuring metrics against threats that could impact revenue.

Crafting outcome-driven metrics

Corporate security executives continue to prioritize supplier oversight in the wake of extensive software supply chain attacks. High-profile breaches show how quickly a hack of one widely used software tool or service provider can spread.

To build effective outcome-driven cybersecurity metrics, ask these critical questions:

- ✓ What metrics align with business objectives?
- ✓ How can these metrics empower executive decision-making?
- ✓ Which security issues pose the greatest threats to revenue?

Cyberattack on Change Healthcare crippled revenue flow across the healthcare sector

For example, the 2023 cyberattack on Change Healthcare, a major player in medical claims processing in the United States, had profound repercussions across the healthcare sector. With the company forced to disconnect over 100 systems, medical claims processing ground to a halt. This disruption, termed by the president and chief executive of the American Hospital Association as "the most serious incident of its kind" in healthcare, brought many medical providers to the brink of closure.

An AHA survey of 1,000 hospitals found that 60% of respondents said the impact on revenue was $1 million or more a day.

The group behind the attack, known as ALPHV or BlackCat, has been linked to a series of high-profile cyberattacks on critical infrastructure companies. Notably, this group shares ties with the criminal organization responsible for the infamous Colonial Pipeline attack in 2021.

A glaring vulnerability highlighted by this incident was the overreliance of many healthcare providers on Change Healthcare for claims processing. This reliance created a single point of failure, leaving physician-owned medical groups, psychiatry practices, and private practitioners across the U.S. stranded as their cash flow dried up. Faced with such financial strain, many healthcare organizations were forced to take drastic measures – including staff furloughs and dipping into personal funds to meet payroll.

In the wake of this incident, corporate security executives are doubling down on efforts to bolster supplier oversight and cybersecurity measures. Every organization must scrutinize its data security practices, assess third and fourth-party access to sensitive data, and identify critical vendors essential to revenue.

75%

of third-party breaches targeted the software and technology supply chain.

SecurityScorecard Global Third-Party Breach Report, 2024

Drawing from real-world scenarios, here are concrete examples of outcome-driven metrics:

- ✓ The time it takes to deploy patches
- ✓ Percentages of vendors that have failed security assessments
- ✓ Number of incidents where third parties created a liability
- ✓ Percentage of revenue dependent on risky third parties by business unit
- ✓ Benefits can also be cost savings, such as reducing the cost of recovering from ransomware

Let's use the time it takes to deploy patches as an example. For the business narrative, it is important to note:

Slow patching creates more opportunities for a third party to have a security incident.

The faster known vulnerabilities are patched, the less time they are available to attack.

However, executives also need to know that patching faster is typically more costly, as it may require more resources or disrupt business operations.

This trade-off between speed and cost is essential to explain to non-technical executives and board members.

Security Operations: Third-party cyber risk reporting

Convincing non-technical executives to invest in security operations (SecOps) is a notorious challenge. Because SecOps relies on many sources of data — each with disparate uses, dashboards, data formats, and ways of accessing data — it's quite challenging to consolidate that data and derive meaningful, consistent metrics from it. This is one area where security ratings and continuous monitoring are mission-critical.

Strategic metrics must be reported to the board. An executive can use these metrics to report the overall impact of the security function, including security operations, to other executives.

Examples include:

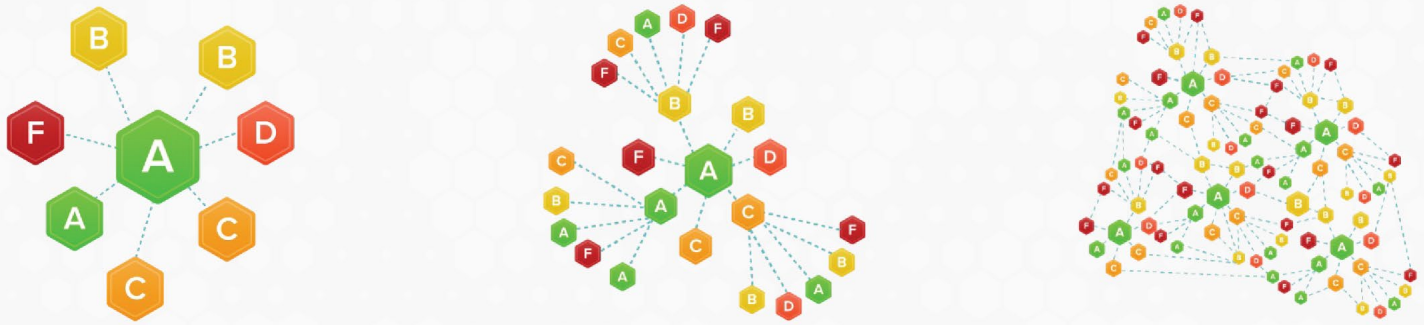
- Number of breaches of IP due to a third party over the past 12 months
- Number of third-party-originating incidents relative to the total number of vendors
- Revenue lost due to supply chain cybersecurity issues

The cost of a third-party cyber breach is typically

40%

higher than the cost to remediate an internal cybersecurity breach.

Gain a complete view of your vendor ecosystem



Know More

Visualize your full vendor ecosystem of known and unknown benders, and the products they use

Streamline Workflows

Simplify risk mitigation and quickly identify threat exposures

Scale Higher

Drive targeted discussions with your supply chain

Operational metrics

SecOps must also track and report on operational metrics to report to the CISO and VP of SecOps, including:

- Percentage of material security incidents detected (first, third, and nth-party)
- Percentage of detected incidents that require customer breach notification
- Average time to notify customers of a breach

Tactical metrics

Tactical metrics are reportable to members of the SecOps function. Examples of tactical metrics are:

- Mean time to acknowledge: Do security analysts have the appropriate bandwidth?
- Mean time to triage: How much time it takes to triage an incident?
- Third-party incident response process adherence: Is your incident response process easy to use and accurate?

Conclusion

With the new SEC cybersecurity incident disclosure requirements, the demand for cybersecurity reporting on third-party cyber risk management has never been higher. Senior executives and boards require tangible evidence that cybersecurity investments yield expected outcomes. Yet, traditional metrics often fall short, needing more depth and relevance to align with business goals.

By identifying critical security threats that could impact revenue significantly, CISOs can develop metrics that resonate with stakeholders. From strategic metrics reported to the board to tactical metrics monitored within security operations, outcome-based metrics play a crucial role in demonstrating cybersecurity effectiveness.

> *"The nature, scale, and impact of cybersecurity risks have grown significantly in recent decades. Investors, issuers, and market participants alike would benefit from knowing that these entities have in place protections fit for a digital age."*
>
> SEC Chair Gary Gensler

In conclusion, by aligning metrics with organizational objectives, CISOs can effectively communicate the value of cybersecurity investments. Outcome-based metrics spotlight cybersecurity's pivotal role in safeguarding business continuity in an increasingly interconnected digital economy.

Additional Resources

Additional reading on cybersecurity metrics and supply chain risk management:
https://securityscorecard.com/resources/research/

SecurityScorecard Global Third-Party Cybersecurity Breach Report, 2024:
https://securityscorecard.com/reports/third-party-cyber-risk/