SecurityScorecard

Assessing supply chain risks under the NIS Directive

Where to start and where to stop?

Anne Klebsch

Director Customer Success
SecurityScorecard

CISA | GICSP | GSNA

With over 12 years experience in projects across a wide range of business, IT and ICS security themes, Anne is practiced in assessing and implementing security. Her core competencies include the development of Security Frameworks and Roadmaps, Risk Assessments and the integration of IT Security Controls in operational processes.

Work experience

2021 – Today	Director Customer Success International
2019 – 2020	Advisor for Implementation of Supplier Assurance
2018 – 2019	Industrial Security Consultant for OT – Applied Risk
2014 – 2018	Senior IT Auditor – HEINEKEN Global Internal Audit
2008 – 2013	Senior IT Auditor - Deloitte

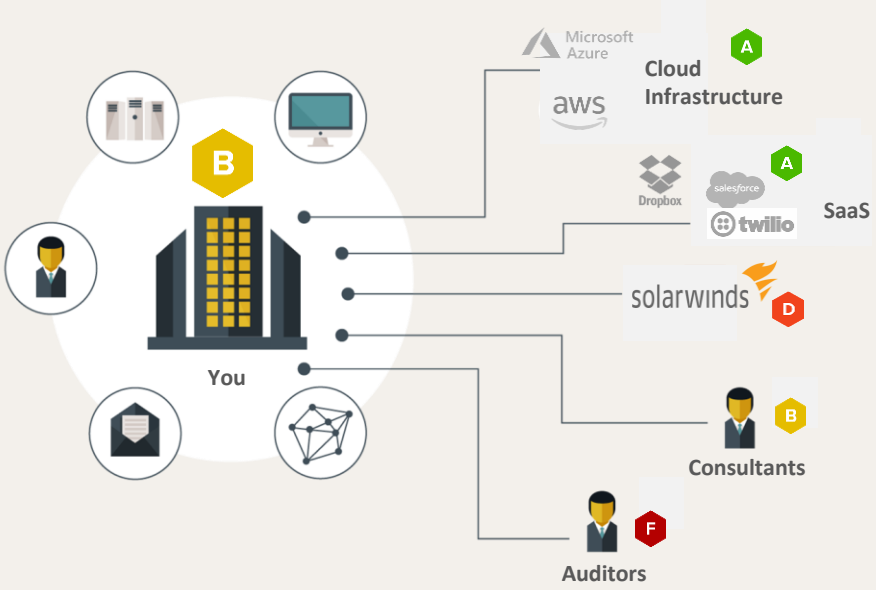
Relevant Projects

- Provided consulting services around cyber security, compliance and ICS security for major Manufacturing organizations, Oil and Gas companies, Logistics, Power Distribution and Banks
- Advised customers on the implementation of Third Party Risk Management Strategies and vendor audits
- Created IT Security Policies for the ICS domain for multiple customers and led risk assessments and gap analysis based on ISO 27001, NIST and IEC 62443

SecurityScorecard

How to address supply chain risks under the NIS Directive?

How do I understand and communicate **the impact of third parties, fourth parties etc. on my critical processes**?



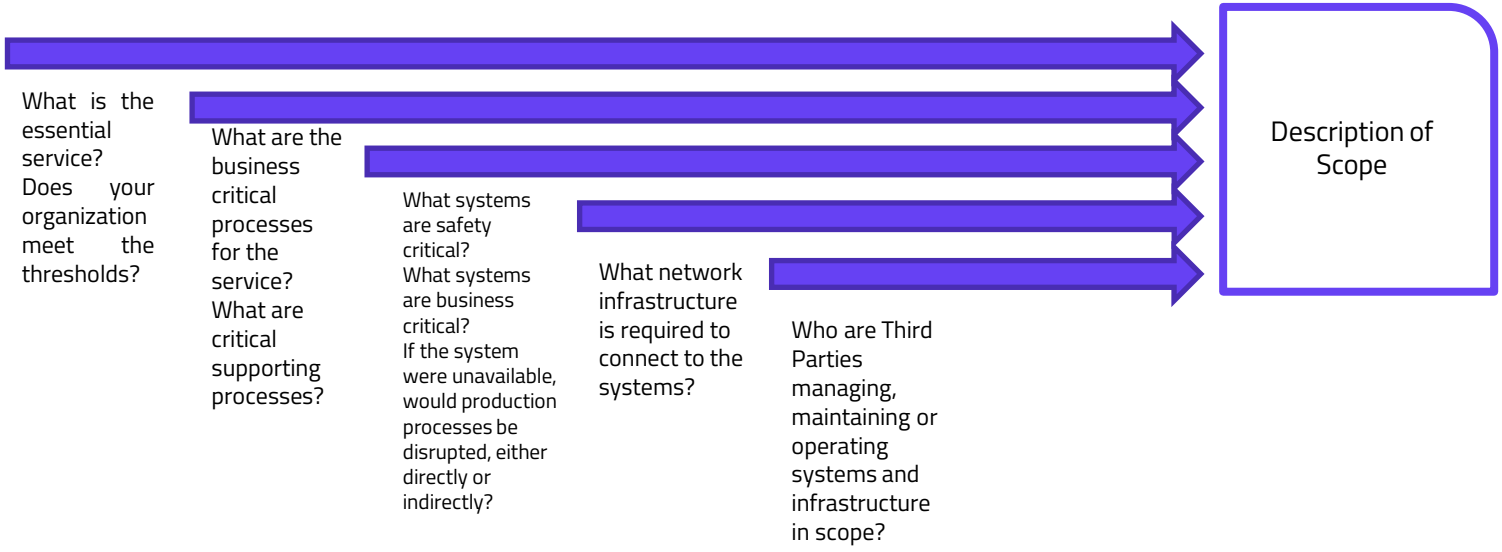
How do I know if my third parties are diligent about security?

63% of data breaches are linked to third parties

SecurityScorecard

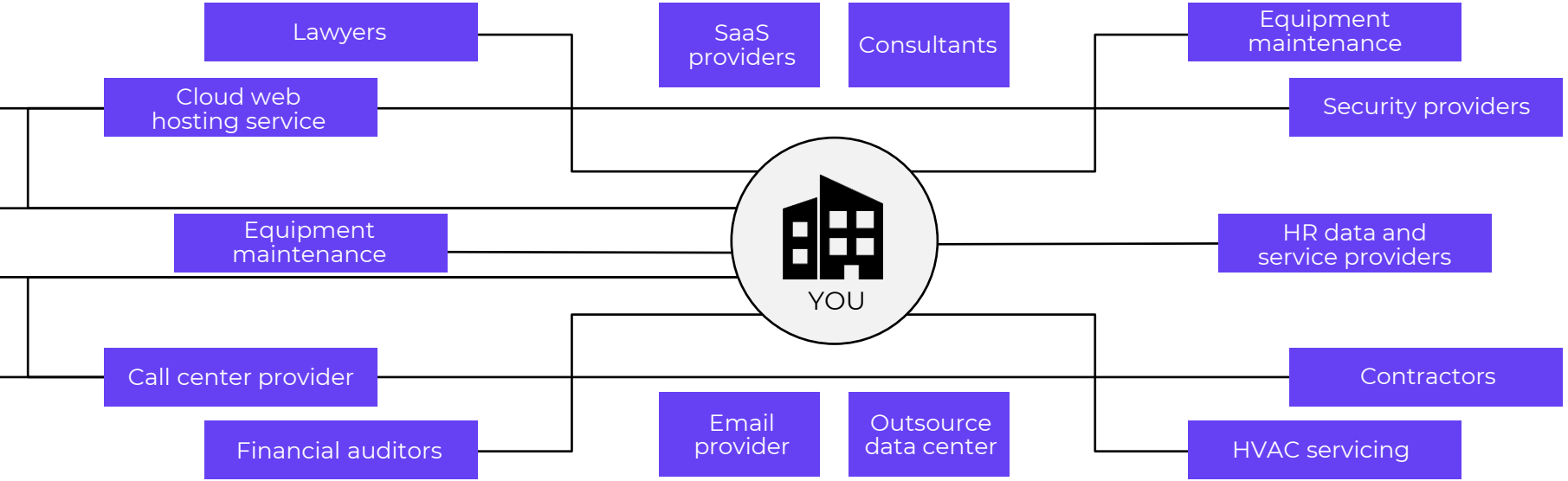
NIS compliance starts with defining the primary and supporting systems and services required to provide the essential service

This scoping should also consider Third Party services, vendors and suppliers



SecurityScorecard

Problem: Organizations Rely on an Increasing Number of Third Parties for Business Operations



60% of organizations work with more than 1,000 third parties and this number will grow.

*Source: Gartner

SecurityScorecard

Most Organizations Don’t Have a Full Understanding of their Vendor Ecosystem

65%

of organizations don’t know which third parties have access to their most sensitive data.

51%

of organizations have experienced a data breach due to a third party.

** Sources: 2021, A Crisis in Third-Party Remote Access Security,* Ponemon Institute

SecurityScorecard

Who impacts your critical processes?

There are different ways to identify your relevant suppliers...

Finance and Procurement

Based on contracts and Accounts Payable

Network

Based on network connections and interfaces

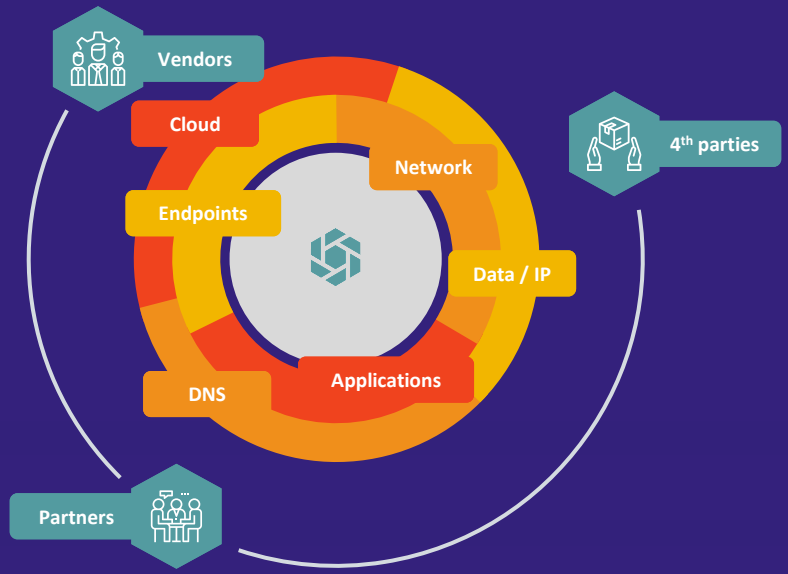
Existing inventory

Based on existing inventory and risk assessment

Inquiry

Based on documentation review and interviews

... but it does not stop at suppliers



SecurityScorecard


You
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties
Fourth Parties

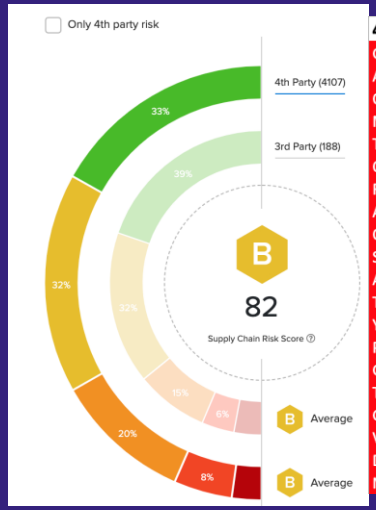
4th party concentration risk

Some Aggregate Risk vendors may seem obvious:

- Google
- Microsoft
- Amazon
- Salesforce

Others may not be so obvious:

- Chef Software
- JetBrains
- Modernizr
- Lightbend



4th Parties	4th Party Concentration	
Google, LLC	260	91.2%
Amazon Web Services, Inc.	250	87.7%
Open Source	246	86.3%
Microsoft Corporation	239	83.9%
The PHP Group	239	83.9%
Oracle Corporation	238	83.5%
Facebook, Inc.	236	82.8%
Adobe, Inc.	226	79.3%
OpenJS Foundation	224	78.6%
Salesforce.com, Inc.	213	74.7%
Automattic, Inc.	209	73.3%
The Linux Foundation	207	72.6%
Youtube, LLC	202	70.9%
Python Software Foundation	202	70.9%
General Technology	201	70.5%
The Apache Software Foundation	199	69.8%
GitHub, Inc.	196	68.8%
VMware, Inc.	195	68.4%
Docker, Inc.	193	67.7%
Nginx Software, Inc.	192	67.4%

There could be hidden catastrophic risk across your 3rd party ecosystem

Once you understand your supply chain, you have to meet the NIS requirements

Below are the relevant paragraphs/ chapters that were identified to include Supply Chain requirements.

ENISA

- The operator establishes a **mapping** of its ecosystem, including but not limited to suppliers, in particular those with access to or managing operator's critical assets.
- Identify and **evaluate the potential risks** represented by the relations consider parameters such as technical capabilities regarding cybersecurity, maturity, trust, access level and dependence on the third party
- The operator establishes a **policy** towards its relations with its third parties and **security requirements** must been taken into account for CIS-components operated by third parties.
- The operator ensures via **service level agreements (SLA)** and/or **auditing mechanisms** that his suppliers also establish adequate security measures

Link to ENISA baseline

UK CAF

- You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces.
- You can clearly express the security needs you place on suppliers in ways that are mutually understood and are laid in contracts.
- All network connections and data sharing with third parties is managed effectively and proportionately.
- You have confidence that information shared with suppliers that is essential to the operation of your service is appropriately protected from sophisticated attacks.
- When appropriate, your incident management process and that of your suppliers provide mutual support in the resolution of incidents.

IT

ISO 27001: 2013

- A.15.1 Information security in supplier relationships
  - Information security policy for supplier relationships
  - Addressing security within supplier agreements
  - Agreements with suppliers shall include requirements to address the information security risks associated with services and product supply chain.
- A.15.2 Supplier service delivery management
  - Organizations shall regularly monitor, review and audit supplier service delivery.
  - Managing changes to supplier service

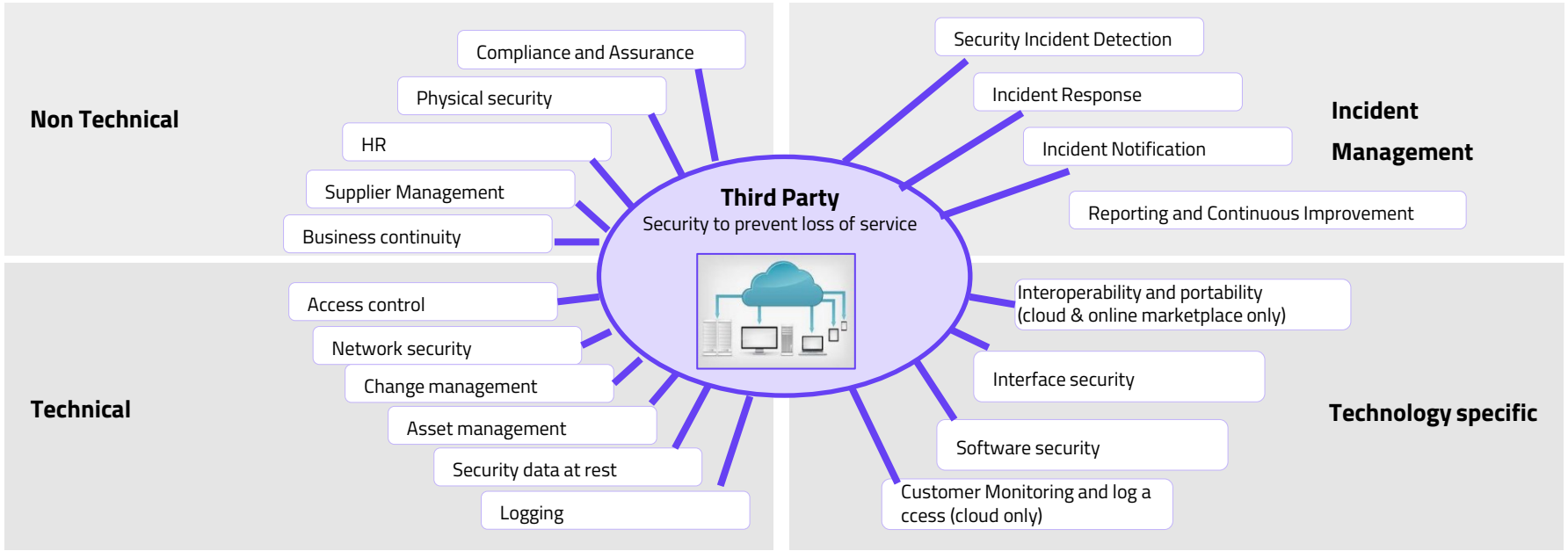
OT

IEC 62443-2-1

- 4.3.4.3.1: The security functions and capabilities of each new component of the IACS shall be defined up front, developed or achieved via procurement.
- A.2.2.5.1: Capture risks associated with value chain and other third-party business partners. Developing business impact analyses for value chain or other third-party business partner.
- A.3.2.3.4.1: Establishing or modifying contracts to address cyber and physical security policies and procedures of Third parties

SecurityScorecard

Overview of requirements



Most organizations have frameworks and technologies in place to measure vendor risk

"Which of the following best describes your company's current approach to the way vendor risk management/ecosystem risks (VRM) are managed, communicated, and reported across the company?"

Base: 158 North American enterprise security and compliance technology decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Security Scorecard, March 2018

SecurityScorecard

But there is room for improvement...

Frequent challenges when assessing supply chain risks

How to **continuously monitor?**

I **don't have time** to stop and think about a strategy.

Business won't be happy to hear **vendor's security is terrible**...

I have **too many vendors to assess**!

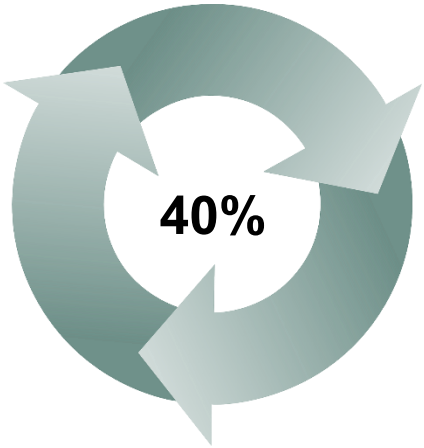
Third-parties are so **secretive about their cyber health**!

Every vendor **assessment is an emergency**.

SecurityScorecard

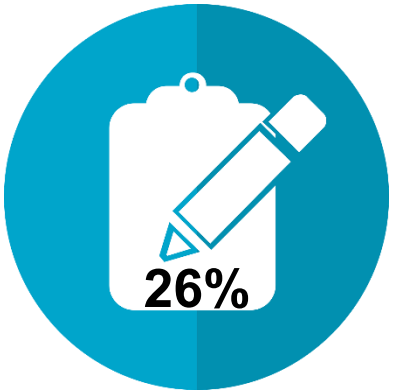
Current state of Vendor Risk Management

Which of the following best describes your company's process for vendor risk management (VRM)?"



Continuous monitoring solutions connected to vendor systems

Periodic audits of third-party systems



Annual or semi-annual questionnaires sent to vendors

Base: 158 North American enterprise security and compliance technology decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Security Scorecard, March 2018

SecurityScorecard

This poses challenges to the Business and Board

Cybersecurity metrics are **difficult to understand.**

Reports **don't align with business needs**.

No common language to talk about cybersecurity.

I have **no time to compile** concise reports and metrics!

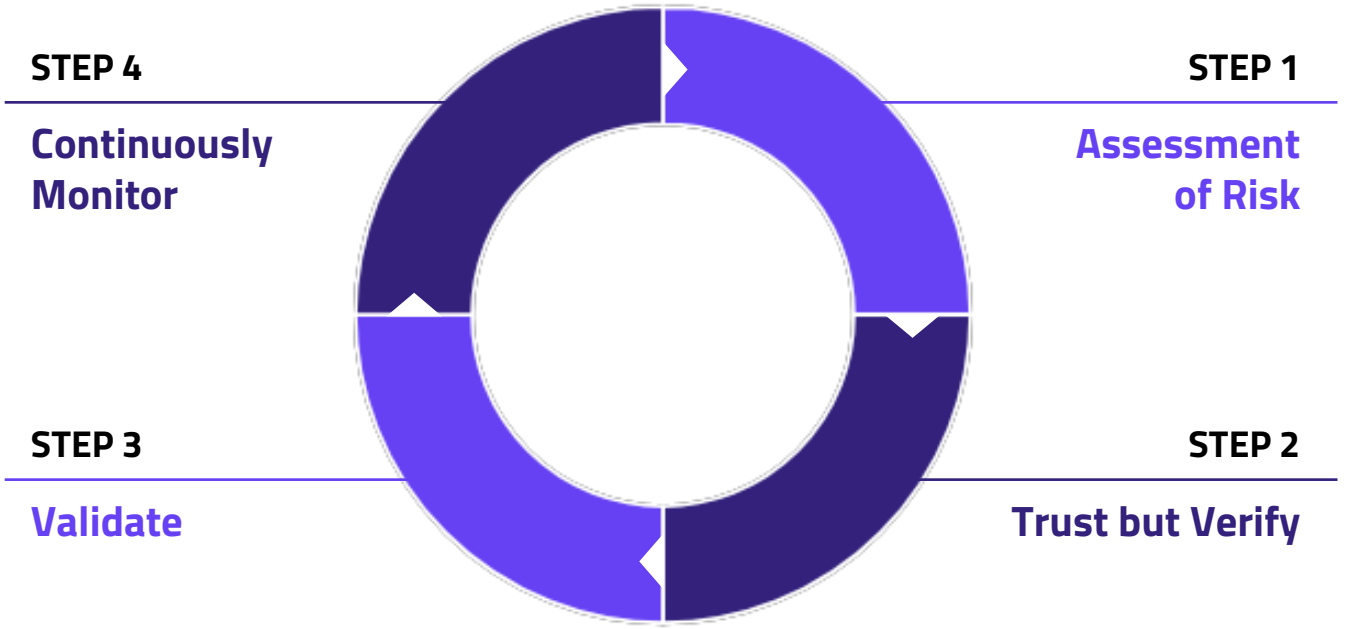
We don't collaborate so it's hard to strategize.

Metrics **aren't actionable** and we waste a lot of time and money.

SecurityScorecard

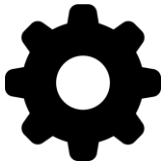
Dynamic Third-Party Risk Management Workflow

The ideal process enables you to have visibility of thousands of companies but applied **enhanced due diligence where it is needed.**



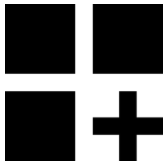
SecurityScorecard

To get there it takes



Scalable Processes

How do you build a maintain a dynamic and effective program?



Data Utilization

How can you integrate and take action on multiple data sources?

Continuous Visibility

How do you continuously monitor a large and growing population of vendors?

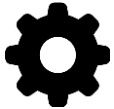
Effective Reporting

How do you effectively report third-party risk to the board?

The process for effective vendor risk management

Increase oversight and drive engagement

Do not limit scope to the most critical vendors you know but also consider concentration risks of nth parties, business partners etc.



Implement a risk based approach

Based on the inherent risk different depth of assessment and key focus areas should be applied.

Define Thresholds

Before you start the assessment, have for every level of vendor the acceptable risk defined.

Take action on key rsisks

Vendor assessments should not just be check-the-box exercises. If there are issues, agree with the vendor the key actions

Monitor continously and communicate effectively

Track the progress of remediation and security of your Third Parties continuously.

SecurityScorecard

Executing

1 The entity who provides the critical service is accountable for the supply chain. Third Party contracts need to allow them to exercise its obligations.

2 Supply Chain requirements to include in the contract:

- Provide evidence of implementation of IT Security standard
- Support the OES or DSP in performing audits
- Notify the OES or DSP of incidents

Key stakeholder

Business Application Owner and Information Security Officer, to identify relevant required security controls in relation to the services

Business Legal, to help frame the requirements in relation to the service and overall contracting

Local Legal Counsel, to verify gaps in relation to contract requirements from a country perspective

Contracts and Procurement, to update CP contracting process to include required clauses / appendix

Assessment Diligence Example

Inherent Risk	Scorecard Value	Diligence Requirements
Critical	C, D, F	• Review Audit reports • Perform Onsite Assessment • Pen-Tests
High	A, B	• Review Audit reports • Perform Remote Attestation
Medium		• Conduct Questionnaire / Self-Attestation
Low		• Conduct Light Self-Attestation • Monitor Security Ratings

SecurityScorecard

Key Takeaways

Discover critical vendors

Consider 4th party risk

Use a risk-based approach to differentiate vendor assessments

Automate data-driven workflows

Implement continuous monitoring

Collaborate with third parties

SecurityScorecard

Thank you.

Why SecurityScorecard?

SecurityScorecard

For Modern Risk Management

Security Ratings

Atlas

Data

Integrate 360° Marketplace

Professional Services

Platform

Making the world a safer place

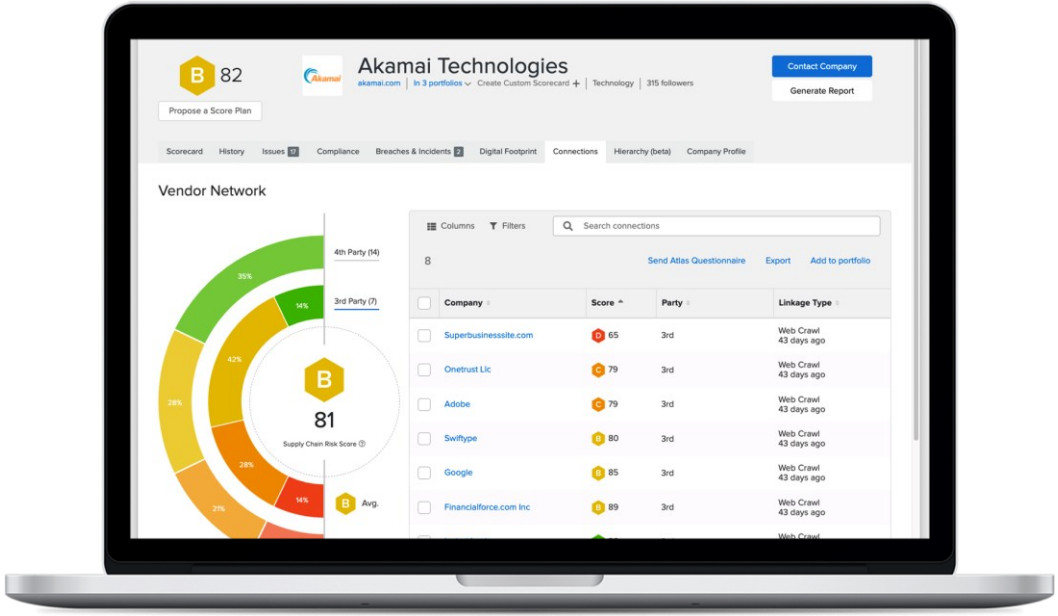
SecurityScorecard

SecurityScorecard Rating Are Optimized with Breach Likelihood

SecurityScorecard

Security Ratings

Automatic Vendor Detection



SecurityScorecard's Automatic Vendor Detection module empowers companies with instant supply chain risk analysis.

SecurityScorecard

Active Member of Multiple Cyber Policy-Focused Alliances

Institute for Security & Technology's Ransomware Task Force

- SecurityScorecard is a founding member, and the only ratings company
- Time-boxed effort (work will conclude in first half of 2021) to provide actionable recommendations to combat increasing impact of ransomware on government, education, health care and other critical sectors

Microsoft
McAfee CITRIX

Defending Digital Campaigns

- The only ratings company out of 30+ solutions provided
- All solutions must be provided to Federal campaigns/parties at low, or no cost - we chose no cost
- Offered to both Trump and Biden campaigns
- Biden Campaign accepted use for Vendor Risk Management.

Google FACEBOOK
Microsoft

Cyber Threat Alliance

- SecurityScorecard is an affiliate member of Cyber Threat Alliance, and the only ratings company part of their roster of 29+ others
- CTA focuses on threat intel sharing

paloalto NETWORKS
CISCO
Symantec

Global Cyber Alliance

- SecurityScorecard is a premium partner of the Global Cyber Alliance
- Offering expanded free access in their small business and election toolkits
- GCA focuses on measurement and making the Internet safer

Microsoft intel
PayPal FACEBOOK

Our Journey

2013

Founded by Dr. Aleksandr Yampolskiy and Sam Kassoumeh; both are cybersecurity practitioners and leaders

SEED

boldstart ventures evo/ution EQUITY PARTNERS

2015

Collaboration Tools Launch

SERIES A

SEQUOIA

2016

Instant SecurityScorecard, Automatic Vendor Detection, and ThreatMarket Launch

SERIES B

2017

Malware Grader Launches

Partnership with the London Digital Security Centre

200K Companies

Continuously Monitored

SERIES C

NGP Intel Capital Moody's

2018

Milestone achievement provides unmatched amount of historical data to contextualize cybersecurity risk

Atlas Launches

MILESTONE

1,000,000 SCORED

2019

SecurityScorecard closes

$50 million Series D financing round led by Riverwood Capital, bringing the company's total funding to $110 million, to continue expanding its platform

SERIES D

RIVERWOOD CAPITAL

2021

Raising the bar for unmatched historical data to contextualize risk with 10 Million companies scored

Marketplace launched with 40 technology and alliance partners

MILESTONE

10,000,000 SCORED

2021

$180 million Series E financing round led by Silver Lake Waterman bringing total investment to $300 million to expand globally and enhance solutions

SERIES E

SILVERLAKE WATERMAN

2022

SecurityScorecard acquires LIFARS, a global leader in digital forensics, incident response and cyber resiliency services, adding a suite of new response and preventative services.

LIFARS your digital world, secured

SecurityScorecard