Managing Third-Party Risk in the Age of DORA & NIS 2

Turning Third-Party Risk Management from Compliance to Competitive Advantage

Michael Strobl
Senior Solutions Architect
CEH - CISSP
SecurityScorecard

Michael Strobl

CISSP, CEH

Greater Munich Metropolitan Area · Contact info

500+ connections

SecurityScorecard

Technische Universität München

23 years in IT – Telko, Enterprise, Security

Contact Information

Email: mstrobl@securityscorecard.io
Mobile: +49 160 1700011
LinkedIn: *https://www.linkedin.com/in/michael-strobl-029b884/*

„…as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know …"

Donald Henry Rumsfeld – former United States Secretary of Defense

Why The Topic?

- Third-Party Breaches Are Blooming
- Attackers Target the Weakest Links for Scalable Breaches
- NIS2 and DORA Requirements
- We Are All Targets. What Is Your Weakest Link?

The Valio Breach – A Case Study in Third-Party Risk

https://yle.fi/a/74-20133008

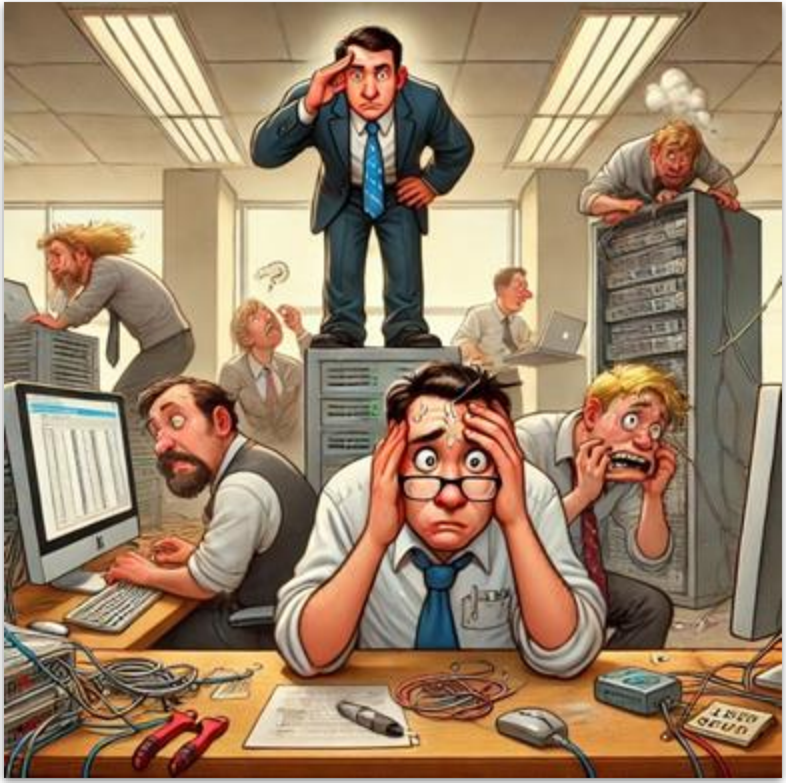
- **Affecting up to 70 000 individuals**
  - Names, ID numbers, salary details, bank accounts, and health-related information
- **Attack Vector:**
  - Unauthorized access via compromised credentials of IT service provider Vincit
- **10 Vincit Customers affected**

Third-Party Risk Requirements in NIS2 and DORA

- Stronger Vendor Oversight
- Continuous Risk Management
- Mandatory Incident Reporting
- Operational Resilience Expectations
- Board-Level Accountability

Regulatory Pressure vs. Execution Gap

- Manual, Inefficient Processes
- Point-in-Time Assessments
- Supplier Discovery and Collaboration Challenges
- Resource Constraints. DIY vs. Service
- Disconnect Between Security & Procurement
- Lack of Executive Buy-In



Making TPRM a Competitive Advantage

- Data-Driven Vendor & Business Decisions
- Prevention of Supply Chain Disruptions
- Cost Savings & Optimized Security Spend
- Regulatory Confidence & Avoidance of Fines

Best Practices for Effective TPRM – Automate with Purpose

- Know Your Third Parties
- Prioritize Based on Risk
- Streamline Assessments & Onboarding
- Monitor Continuously, Not Just Periodically
- Adopt Proactive Incident Response & Vendor Remediation
- Enable Executive Visibility & Decision-Making

Getting Started – Practical Steps

- Assess Your Current TPRM Maturity
- Evaluate Your Execution Capabilities
- Start with High-Risk Suppliers
- Define a Clear Roadmap for Improvement
- Leverage Tools to Enable Automation

Key Takeaways

- Third-Party Risk is a Growing Threat
- Regulatory Pressure is Here & Enforced
- Proactive TPRM is a Competitive Advantage
- Automate to Scale
- Get Started Now!

Questions?

Michael Strobl
Senior Solutions Architect
SecurityScorecard