4 TAKE AWAYS

SUPPLY CHAIN SECURITY IN THE FINANCIAL INDUSTRY

1 NOVEMBER 2023, AMSTERDAM

Great to see all of you at our Secura event on supply chain security in the financial sector.

We identified 4 main takeaways during the afternoon led by our host **Eward Driehuis**, cybersecurity strategist.

For instance, no matter how well protected you are, smart hackers will most likely be able to circumvent your security measures. This is why regular pentesting is so important.

You can also find the other three key learnings in this summary. Thank you all for coming and we hope to see you at our next event in the spring of 2024.

The importance of securing the supply chain: that was the main focus of the day. **Anne de Nies, Secura's Finance Manager**, gave a brief introduction of the upcoming DORA regulation.

DORA has a broad focus: you have to take responsibility for risks that occur within your supply chain and among your critical vendors.

Secura
A BUREAU VERITAS COMPANY

The DORA requirements in short

1. Implement a risk management framework.
2. Establish a process for incident response.
3. Regular testing/monitoring of operational resilience.
4. Managing third-party risk.
5. Information sharing arrangements.

Questions we discussed as a group

- How to deal with the large vendors that don't give any room in contracts?
- Should we include every vendor in our risk management? And in our approach?
- How to handle running contracts?
- Do we include critical applications in our operational resilience testing?
- 'We are already ISO27001 certified'/'we are already NIS1 compliant'/'we follow a framework such as NIST or the Good Practices for information security': are we ready for DORA?

1

Takeaway 1: During a supply chain attack transparent communication is key.

Alan Lucas, current CISO at Homefashion Group and former CISO at LiteBit, shared valuable insights from his tenure in the cryptocurrency sector. While at LiteBit, securing vast sums of money against cyber threats was a daily task, made more complex by the significant transaction volumes and the inherent need for anonymity, all within a lightly regulated environment.

LiteBit's commitment to good cybersecurity practices was put to the test when a key supplier fell victim to a cyber attack, which in turn left LiteBit exposed to potential threats. This incident reminded us of the importance of securing every part of the supply chain.

Alan shared some learnings on how they handled this supply chain attack:

- Transparent communication between the vendor and the client.
- Get the right incident response team involved from the start.
- Involve the incident response teams from both sides in your crisis team. Otherwise you have two black boxes, collaboration is key.
- Correlate logs and data from both parties to get a full overview.
- Communicate as early as possible. Ask (contractually) from your vendors that they communicate incidents as soon as possible.

2 Takeaway 2: The automotive industry can serve as an example for getting supply chain security in order.

Razvan Venter, from Secura's Manufacturers market group, shared some insights into how the automotive industry approaches supply chain security. This sector is ahead of other sectors in this area, as they have always been heavily dependent on their suppliers to manufacture their products. The industry adheres to cybersecurity regulations R155/R156, established by UNECE.

These regulations cover a range of areas including general requirements, hardware, software/firmware, and service back-end software, along with updates. Razvan has helped create a supplier program with one of Europe's top car manufacturers. It was tested with a pilot involving 42 suppliers across manufacturing, cloud services, and back-end application development.

Razvan shared some of his key learnings with us:

- It took more than a year to get the pilot group of 42 suppliers compliant.
- All suppliers were willing to comply, but some of them could not account for the financial consequences of the request.
- New suppliers were willing to comply much easier than existing suppliers.
- There were recurring topics that caused issues or delays. For example security monitoring and information storage.
- Not one supplier complied without legal involvement.

3 Takeaway 3: Even if you are well protected, you can still get hacked, so pentesting is important.

Michael Schouwenaar from Secura provided a technical perspective on the complexities of defending against cyberattacks, especially when using third-party tools. He illustrated this with an incident involving an internet banking platform compromised through a package manager tool.

Despite developers often relying on external sources for operating systems, development frameworks, and libraries, the bank had stringent cybersecurity measures in place. Nevertheless, attackers managed to upload a malicious package, which the bank's package manager tool then inadvertently distributed within the banking system, circumventing established security protocols.

Fortunately, this weakness was discovered during a penetration test, highlighting the critical role of security testing for third-party tools that are integral to essential processes.

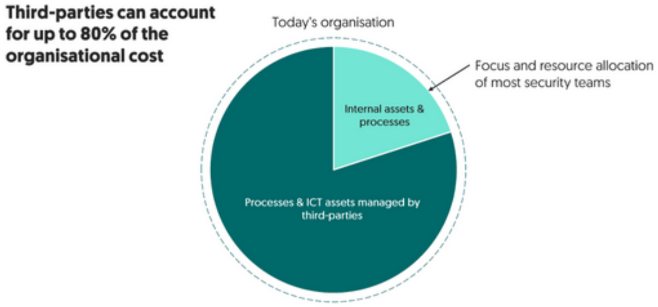
Takeaway 4: Working closely with your suppliers on security is key.

Jelle Groenendaal and Bram Ketting, from 3rd Risk, provided insights into the importance of third-party risk management within supply chains, emphasizing its relevance not only to cybersecurity but also to sustainability, geopolitics, resource scarcity, and compliance with regulations.

While DORA focuses on entities under contractual agreement, Jelle and Bram point out the broader spectrum of third-party relationships, such as alliances, partners, resellers, agents, distributors, and customers, that can also introduce risks.

Collaboration with third parties is often necessary for specialized expertise or innovation despite these risks. Jelle and Bram see an increasing dependence on third parties while security teams tend to focus on internal assets and procedures, which highlights a potential disconnect.

This is particularly concerning given that up to 60% of data breaches today are linked to third parties. A balanced approach to managing both internal and external security risks is becoming crucial.



Jelle and Bram shared some insights from their experience working in this field for many years.

- Start with a scalable methodology from the start.
- Think about risk, not only about compliance.
- Work with your suppliers to understand them. Don't just throw a spreadsheet at them.
- Don't solely rely on assessments and ratings.
- Avoid spreadsheets.
- There is no silver bullet.

Let's get in touch

Would you like to talk to us about becoming DORA compliant? Please contact us.

Anne de Nies | Market Group Director Finance
anne.denies@secura.com

Serge Leclercq | Senior Account Manager
serge.leclercq@secura.com

Rijad Muratovic | Account Manager
rijad.muratovic@secura.com

Learn more about DORA and our services

Visit our website to learn more about DORA implementation, board room training, gap assessments and more:

SECURA.COM / DORA