Chris Russell-Miller, Head of IT and Cyber Risk, BNP Personal Finance – *August 2nd, 2022*

1. Expert background

- CISO for Northern European territories for BNP Paribas Personal Finance (Benelux, Sweden, Finland, Holland, Latvia, Croatia, South Africa except France).

2. Network of Vendors and Set up at BNP Paribas PF

- Wide range of suppliers in the security space: they are using a lot of managed cyber services, such as managed SoCs, managed CIMs, vulnerability management services, patching, etc.
- BNP PF tends to outsource a lot on these activities, for the following reasons:
  - Maintaining the skill base within the bank is difficult because skills are in short supply and require very high salary packages.
  - In-house skills not sufficiently available.
  - Doing everything house is very expensive, far easier to buy managed services especially when they are relatively low-skill based, like applying patches on a server.
- Wide range of providers used, like Capgemini Cyberservices, Orange Cyberdefense (5 years), Rapid7, Qualis (primarily tools rather than services for this one), because:
  - It is somewhat unrealistic to have only one provider for all these countries. No organization has full coverage of all areas at the same time.
  - Sometimes political sensitivities: as a bank, tend to use more European-based service providers.
- Colleague based in Paris covers France, Spain, Portugal, Italy: he has a different subset of suppliers. Vendors based in Paris are expensive. Expert works with vendors based in Madrid, which are cheaper.
- They have a preferred supplier list at the Group level for services, but no dictation. This is because there are very few global providers of services able to engage.
- However, for products (*vulnerability scaling tools*) they have a group policy to comply with.
- They engage managed services, but vendors use BNP's products, as per group policy.
- Outsourcing of Capgemini resources in Eastern Europe (Hungary, Croatia) + India: managed vulnerability scaling services for them, but use their tools, because it's cheaper.

3. Overview of tender process

- They retender every 3 years, group mandatory policy.
- To retender, they invite organisations to offer a master services agreement (MSA). They draw a list with a series of products and services: product, product with service, purer buying of technical resources, subcontracting of resources, … Suppliers are invited to offer as many products as they can.
- Once MSA is in place, they are free to choose any services offered by the vendor they listed in the MSA. If they have for example 3-4 vendors for a specific product, they will choose 1-2 of them, and cycle them around. They can switch the provider within the 3 years!
- If this is managed service (SoC, etc): not easy to swap, takes time to implement those tools. But for vulnerability scanning, API testing, red team exercise, those products are not sticky so they may choose different vendors at different times. Example : 2 - 4 penetration test per year: don't use the same vendor on this.
- Where it's high value or expertise or implementation is high: full 3-year contract, no switch. Stickier.

4. Evolution of the relationship with vendor over time

- Need to create a detailed but vague MSA. Ideally should have a clause mentioning: "cybersecurity consultancy services", because very vague, so more flexible on the services offered. The reason for this is that the cybersecurity market evolves much faster than their procurement & legal department, so it'd be impossible to have contracts ready on time.

- If there is a good working relationship with incumbent vendor, this vendor will always have an advantage, despite the tender. They are in their 2nd renewal with Orange, and 3rd renewal with Capgemini.
- An MSA does not have pricing elements in it. They compare prices of the suppliers part of the MSA in place.
  - Commodity product: pure cost based or license for a tool.
  - For services: more complicated, they will have a team looking at the response from the 3 MSA holders. He can put them in competition, especially because he works in cybersecurity, and has a kind of a "free card", return on investment hard to calculate and hard to demonstrate that a decision is cost-saving. They are never buying the same thing, because after 3 years, end of a product entire lifecycle, replaced by something completely new.
- Managed services: they may buy the service rap only (and supply the product). They always ask 2 vendors to have a like-for-like comparison: then a preferred supplier status is assigned, then opportunity to finesse ("*faire passer*") the offer. Possibility to add in other value-add products.

5. Key decision criteria for choosing service supplier

- Price is key, has to justify his budget!
- Technical competencies, then with reputation, track history, and previous engagement.
- They will go to the OEM (product manufacturer or integrator) and ask them who is good at managing their product in the marketplace.
  - They are currently implementing a new product: a data classification and data discovery tool from Veronis. They asked Veronis which integrators they would recommend.
- If it's pure managed services: they are vendor agnostic, they don't dictate the end product. Fully agnostic service: 50%. Group catalogue of preferred products: 50%. Managed service: no capital purchase so no need for group catalogue product.
- Likes the fact that players like Orange are vendor agnostic. Capgemini is McAfee vendor so will do an implementation for them.
- Local presence: most of their bigger vendors will have a set-up partner organization that is very local. BNP needs to be notified in case partner outsources to a third-party supplier. No impact on pricing.

6. Nomios/Infradata

- Used in Germany for an initiative to introduce a zero-trust network.
- Nomios had not been part of his tenders for now, not a reseller for Northern market, based in France.
- Infradata: very much present in Central Europe, they are using them in Holland, Belgium, Luxembourg and Germany. Quite good reputation. They were service provider for Fortinet and Palo Alto (firewall.) Managed service provider for firewall rule set for them. They have not been replaced. Since prior to 2018.
- Phenomenal amount of M&A: quite a risk for him. Because when they assess a vendor in product, they take into account stability of partner, and take over is something they consider. They have an example of a hardware vendor taken over as part of an M&A: within a short space of time, their suite of product has been replaced. Happened quite a lot with Dell. Consolidation of smaller, much niche start-ups.

7. Key trends / Clients' needs

- Cloud posture checking.
  - They launched an IBM/Microsoft partnership to create a private cloud instance. Between now and 2025, all of their 23 datacenters will be migrating to multi-cloud environment)
- Security zoning, zero trust orchestration
- Extended detection response.

- 40% of his budget is product, 60% is services. But that should change to 75% services and 25%. Products will be paid through a part of managed services (because no capital accounting then). A revenue item rather than capital one.

8. Quality of the SoC assessment

- Every supplier is audited by BNP at least once during lifecycle of the contract. Keep a close track on service level agreements.
- Assessed criteria:
  - HR resources: how many people, training level, staff turnover.
  - Softer CSR.
  - Number of false positives: sample of alerts that come through and follow triage process.
- Suppliers come to the BNP with new innovative offerings. There is a continuous "improvement clause" in every MSA (cost saving, value add product). They don't have to take it, but expect the supplier to present it.