Cyber Security Innovators: KPN

A custom report for

kpn

Patrick Donegan, Principal Analyst, HardenStance

February 2018
Executive Summary

- KPN has used the negative experience of its own data breach in 2012 to propel it forward to become the largest cyber security service provider in the Netherlands.

- KPN is focused on its acquisition of small Dutch companies to grow expertise and market share in cyber security. For now, bigger deals with bigger players are not being considered.

- The company’s stated intent is to allow acquired companies’ own brands to continue to thrive. A lot of deep integration work remains to be done with each company’s back-end systems, though, including with their Security Operations Centres (SOCs).

- New security services to look out for from KPN in 2018 include virtual firewall services delivered as a service; additional security forensics; a network-based Intrusion Detection System (IDS) for building automation systems; technical security assessments; and something in the quantum-safe computing space where KPN wants to build differentiated capabilities.

Market Context

The Netherlands is a highly developed ICT market, being one of the world’s leading data centre hubs. The Amsterdam Internet Exchange (AMS-IX), for example, is among the most important in the world. KPN is the country’s incumbent telecom operator. It operates fixed and mobile networks, delivering services to consumers and enterprises. In 2016 KPN generated €6.8 billion in revenues with an EBITDA margin of 39.7%.

Like many European telco peers, KPN needs to offset revenue erosion in its core communications business. For 2017, KPN recently reported that its annual enterprise revenues fell by 4.8% over 2016. This was an improvement compared with the 7.2% decline reported the previous year.

The cyber security context

KPN’s cybersecurity strategy should be seen in the context of a number of factors:

- **As much of the Netherlands is below sea level, cyber threats to its digital water management systems are taken very seriously.** Given the economy’s dependency on transportation and logistics, the same is true of these sectors.

- **KPN itself was hacked back in 2012.** Attackers exploited an unpatched server with a single vulnerability to gain access to 300 systems within KPN.

- **In light of the recent acquisitions it has made, KPN is now able to position itself as the largest provider of cyber security services in the Dutch market.** Its competitors in cyber security include Fox IT (acquired two years ago by the UK cybersecurity company, NCC Group); Systems Integrators like Capgemini; and local branches of the world’s ‘Big 4’ accounting firms. Managed Security Service Providers (MSSPs) like SecureWorks and IBM Security are well placed in terms of serving Fortune 500 companies. Among its core competitors in telecom services, Vodafone is also building its position in security services.

Cyber Security Strategy

KPN’s current cybersecurity strategy was formulated in light of the bitter first-hand experience of the 2012 attack. Its goals can best be broken down as follows:

- Make cyber security understandable and accessible to everyone - consumers, businesses and government.

- Drive security as a value proposition into enterprise sales to support the company’s strategy of recovering revenue momentum in the enterprise market;

- Be the single largest provider of cybersecurity services in the Netherlands;
The pace of change has accelerated markedly with key M&A activity in 2016 and 2017.

- Develop competitive advantage in select next generation security technologies;
- Grow a strong position in the Netherlands over a sustained period before contemplating if and how to expand in international markets.

**Progress Report**

The data breach of 2012 hit KPN hard. The resulting investigation, presented to the company’s board, shone the light on a flawed, compliance-driven, security culture that was common in most organizations five years ago, and is still to be found amongst lagging companies today.

This compliance-driven culture meant that from a security perspective, KPN was aiming at fulfilling a baseline of regulatory requirements with respect to data security – and not much more than that. This, during a time when the resources and technology available to attackers was enabling them to consistently get ahead of regulators and break through these bear minimum defences at will. The investigation concluded that the legacy culture was the root cause of how the 2012 breach had come about.

Since 2013, the company’s cyber security strategy has been led by Chief Information Security Officer (CISO), Jaya Baloo (see page 7). Over that time KPN has made solid progress against its security goals, but the pace of change has accelerated markedly with key M&A activity over the last two years.

**Secure services rather than security services**

Today, KPN offers a solid portfolio of security services to businesses. These are categorized on its website as:

- enterprise mobility management;
- compliance monitoring;
- authentication;
- penetration testing;
- anti-DDoS protection;
- managed firewall;
- mobile threat defence.

As with other telecom operators – and other players in the ICT and cybersecurity ecosystem – KPN faces increased demand for migration to the cloud from business customers. This presents a business model challenge in terms of transitioning from shipping and managing dedicated security equipment on the customer’s premises to delivering security services as a service from its data centre and cloud infrastructure. In the interests of both easier customer consumption and higher efficiency, KPN is looking to support a rapid migration to the security-as-a-service model.

Like any incumbent telecom operator, KPN leverages its installed base of communications service as a differentiator to embed and upsell security services. According to the model pursued by most telcos until recent years, KPN used to focus on protecting its own infrastructure while selling security as a separate add-on product or service to provide additional protection to customers. Today’s goal is increasingly to embed security software directly into those services.

KPN’s management identified that to strengthen its hand in the ICT sector and become the largest cybersecurity player on the Dutch market it needed to substantially strengthen its headcount; its account footprint; and its access to competitive security technologies. It determined that investing in smaller Dutch companies serving the local market was the best way to do that.
In the ICT space KPN has gone about this with acquisition of RoutIT (a wholesale cloud services provider for the SME market); Internedservices (a managed hosting and cloud services provider); Divider (a cloud and IT services provider); Net Ground B.V (managed servers and services); Redbee B.V (hosting services) and CAM IT Solutions (a cloud-based provider of IT services to health and public sector organisations).

As shown in Figure 1, KPN has also made a number of complementary acquisitions in the cyber security space. The acquisition of Fortytwo B.V was completed in 2016. Those of DearBytes BV and QSight IT were completed last year, adding cyber security account footprint and additional headcount amounting to around three hundred people.

### Figure 1: KPN’s cyber security acquisitions and VC investments

<table>
<thead>
<tr>
<th>Company</th>
<th>Investment</th>
<th>Completed</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortytwo B.V.</td>
<td>Acquisition</td>
<td>March 2016</td>
<td>Consultancy, management and audit services related to network and security environments – penetration testing, vulnerability scanning.</td>
</tr>
<tr>
<td>EclecticIQ B.V. (Amsterdam)</td>
<td>Venture Capital</td>
<td>May 2016</td>
<td>Cyber threat intelligence provider. KPN invested as part of a Series A 5.5 million Euro investment round.</td>
</tr>
<tr>
<td>Security Matters (Eindhoven)</td>
<td>Venture Capital</td>
<td>September 2016</td>
<td>Monitors, analyses and protects industrial OT environments, translating complex problems and threat indicators into actionable intelligence.</td>
</tr>
<tr>
<td>DearBytes B.V. (The Hague)</td>
<td>Acquisition</td>
<td>January 2017</td>
<td>85 people strong company focused on SMEs. Expertise in malware protection and mobility</td>
</tr>
<tr>
<td>QSight IT (Delft)</td>
<td>Acquisition</td>
<td>October 2017</td>
<td>An IT and cybersecurity company with about 250 people (including InSpark) and a turnover of approximately €50 million in 2016. Skilled security professionals with detection and prediction capabilities as well as a base of corporate and large enterprise customers. Completed in October 2017.</td>
</tr>
</tbody>
</table>

The acquisitions are highly complementary to one another. DearBytes is focused on the SME market and product lines like end point protection. QSight IT provides services to large and corporate enterprises, differentiating by means of services delivered from its Security Operations Centre (SOC). Fortytwo operates more as a consultancy and auditor. Via its stakes in EclecticIQ and SecurityMatters, KPN has access to start-up threat intelligence platforms and security for SCADA and Industrial Control Systems (ICS).

This consolidation of cyber security expertise into the larger KPN parent company has potential to pay dividends in terms of talent retention. The global shortage of cyber security professionals is well known. The best of them only want to work for the very best companies. If KPN can grow competence and scale in the cyber security space, rival companies should prove less alluring for its newly acquired employees than they might have done had they continued as stand-alone SMEs.

Rather than strip acquired companies like DearBytes of their identity and absorb them lock, stock and barrel into the greater KPN, the company prefers to manage its acquisitions lightly from a branding perspective.

The company states that it intends to allow each of their individual brand names to live on independently and gives each operating company a level of autonomy while driving integration of their back-end systems and the products and services they sell. RoutIT, acquired in April 2016, still has its own brand name and own-branded website.

---

The acquisitions of DearBytes and QSight IT are highly complementary.
**Evolution of the SOC infrastructure and services portfolio**

One of the integration challenges KPN faces is in the case of its Security Operations Centre (SOC). Opened in 2012, KPN’s new SOC in Hilversum broke with its previous approach to security operations in a fundamental way.

Whereas KPN had previously operated separate, dedicated, SOCs at separate sites to manage the security of its own infrastructure and that of large paying customers respectively, the new SOC houses both internal and external-facing SOC resources and supporting teams under one roof. Rules and processes are nevertheless in place to enforce strict separation of the two domains.

The next step in the evolution of the SOC is establishing common processes and threat intelligence sharing across the core KPN SOC and the additional SOCs which DearBytes and QSight IT bring to the company. Whereas the SOC acquired with DearBytes is relatively small (reflecting its focus on the SME market), QSight IT’s capabilities in the SOC space are considered its most valuable asset according to some of those who were involved in negotiating the acquisition.

When it was first launched around five years ago, QSight IT’s SOC was based largely on a traditional SIEM-based approach to security monitoring. Over the last five years, however, additional investments have been made in a big data and analytics platform. The latest iteration is based on the Hortonworks Apache Metron Framework.

**Leveraging the Apache Metron Framework for security analytics**

Apache Metron integrates a variety of open source big data technologies into a centralized tool, running on Hadoop, to help SOC analysts rapidly detect and respond to threats. The Apache Metron Framework certainly shows promise among new technologies for use in the SOC. KPN appears to be among the first in Europe to be deploying it.

The challenge is initially to integrate and enable threat sharing between the three separate SOC resources that currently serve KPN’s customers. It’s then to allow threat intelligence sharing across KPN’s internal SOC domain and its externally facing SOC resources – but only in so far as permitted by the legal requirements that KPN is held to by Dutch law and by the customized contractual commitments it has to its customers.

**Figure 2: The evolution of KPN’s Security Operations Centre (SOC)**

![Figure 2: The evolution of KPN’s Security Operations Centre (SOC)](image)
As well as commercial proof-points for its progress against strategy, KPN can also point to some key achievements in terms of the security outcomes it is able to point to. Among these are the following:

- **A huge reduction in the time taken to mitigate the most serious threats.** Perhaps of greatest importance, and according to KPN’s own internal metrics, the average time it takes to mitigate “high” vulnerabilities that also have a “high” ease of exploitation has been reduced by almost a hundred percent compared with a few years ago – from several months to a matter of hours now.

- **No impact arising from MIRAI or WannaCry.** Whereas high profile attacks featuring the so-called MIRAI botnet and the WannaCry exploit have impacted other large European telco peers in the last eighteen months, KPN’s security team takes pride in not having been affected by them.

- **A marked reduction in abuse of the KPN email domain name.** Just over a year ago, KPN research found that its own email domain name was the one most abused in the Netherlands for phishing attacks. During 2017 the company’s “SafeMail” project implemented Domain-based Message Authentication, Reporting and Conformance (DMARC) and the Sender Policy Framework (SPF) anti-forgery approach across KPN’s many hundreds of email servers. This has drastically reduced abuse, better equipped KPN to spot abuse when it arises, and established processes for better customer communications.

- **MyBee has been launched,** enabling under six-year olds to safely take their first steps online.

- **In 2016 96% of KPN’s customers impacted by malware were helped within eight hours.** This was up from 72% in 2015.

Other notable security achievements include:

- **Cyber Central was founded in 2017 along with Cisco Systems and McAfee.** This is a non-profit organization to help make security understood and available to everyone. Based in the Innovation Quarter of Rotterdam Harbour, Cyber Central also serves consumers and regularly hosts workshops for school children.

- **Domain Name System Security Extensions (DNSSEC) has been deployed across KPN’s entire installed base of DNS servers.** This enhances the security of the DNS servers that translate easily recognized domain names used for naming websites into numeric IP addresses enabling servers to associate with one another.

- **KPN has taken the lead in implementing Mutually Agreed Norms for Routing Security (MANRS).** MANRS is a community-driven initiative coordinated by the Internet Society. It provides a minimum set of low-cost and low-risk actions that, taken together, help improve the resilience and security of the routing infrastructure. KPN has implemented all four of the MANRS requirements in its own routing infrastructure – filtering, anti-spoofing, coordination and global validation. This is certainly good as far as it goes but it only reaps benefits in the case of carriers and ISPs that reciprocate and do the same thing – i.e. show ‘good MANRS’.

- **KPN’s own security policies and several tools for security professionals have been made available in open source** via a free iPad app including the Common Vulnerability Scoring System.

**Seeking leadership in quantum-safe computing**

One of the long-term challenges of the ICT industry is to prepare for the availability of quantum computers. Eventually these will be powerful enough to break the current encryption algorithms that protect much of the world’s digitally stored sensitive data. Very few experts in this field believe this is likely to happen within ten years. Most think it’s more likely to be twenty or more years away.
As shown below, KPN CISO, Jaya Baloo, has expertise in this area. KPN certainly benefits from this in the somewhat abstract sense of "thought leadership" and "vision". But the strategy here is also geared towards more tangible, short-term, gains.

The logic goes that there are three clear commercial advantages to be gained from KPN seeking to be a leader in developing and implementing quantum safe algorithms:

- There is differentiation to be had – and money to be made – from developing Intellectual Property (IP) around new quantum safe algorithms themselves.

- There is latent, near-term, demand for quantum services that will start customers on a journey towards lowest cost migration to quantum security over time.

- Implementing quantum safe algorithms will be challenging and potentially very expensive. Those companies that try multiple iterations over a period of time – those who try and 'fail fast' – will be in a better position to implement them early, effectively, and at lowest cost once viable solutions are available.

A test on an innovative high security Quantum Key Distribution (QKD) link between KPN’s Hague and Rotterdam data centres was successfully completed in 2016. Driven in part by KPN’s goals in the quantum safe computing space, KPN CISO Labs was set up at the end of 2017. Amongst its leading lights is no less a figure than Phil Zimmermann. Zimmermann is the inventor of Pretty Good Privacy (PGP), the widely used data encryption protocol, who is now a KPN employee.

**KPN’s very modern CISO**

Since her appointment following the 2012 data breach, the person driving KPN’s security strategy has been its Chief Information Security Officer (CISO), Jaya Baloo.

Having started her career with KPN back in the late 1990s, Baloo landed the CISO role back with her first employer via cyber security roles at other telcos like France Telecom and Verizon.

To say Baloo is atypical is an understatement – and not just because she’s one of few female CISOs. Most of her peers in European telcos still abide by the default convention of the security profession that believes nearly all communication belongs behind closed doors. Given the higher profile that cyber security has in business and in the media nowadays, Baloo has distinguished herself with the very public stances she takes on key issues.

**The NIS Directive? “It sucks”**

Among the things she is most vocal about at conferences, in media interviews and social media posts is insecure software. In a 2017 press interview she stated: “I find it inexcusable that KPN has to hack the software and hardware of our vendors before it’s placed in our network”. In January 2018 she also criticized the EU’s Network and Information Security Directive (NIS) for failing to properly address this issue, stating bluntly that the Directive “sucks”.

This same person that communicates IT security in plain language also gives highly technical TED Talks. Presenting to some of the world’s leading cryptographers, Baloo will go toe to toe with anyone on Quantum Information Systems. The security of genetic data is another area of particular interest.

**Peeping out from behind the curtain**

This CISO follows through with solid and differentiated commercial acumen as well. She’s the driver of the new KPN CISO Labs, which is looking to grow and monetize KPN’s intellectual assets in quantum safe cryptography (described on this page).

While it’s notoriously hard to measure accurately, KPN evidently recognizes the brand enhancement that someone like Baloo brings to the company. She is certainly a new kind of modern, high visibility, CISO. These days, every telco should want one.

**Gap Analysis and Next Steps**

KPN’s priorities for the next couple of years revolve around driving back end as well as service portfolio integration across its cyber security assets. A key priority will be driving more services as-a-service from the cloud, including managed services. Consistent with that, in the case of managed services the emphasis will be on delivering services remotely from the SOC and relying less on having to dispatch security consultants to the customer’s own premises.
Among the new cyber security services that can be expected from KPN are the following:

- A virtual firewall as a service proposition during the first half of 2018. This will be delivered from the KPN cloud without requiring any vendor-specific hardware on the customer’s premises.

- One particular area of focus in managed SOC services is digital forensics. KPN will pursue the certification required from the Dutch government so that when investigating serious incidents its people are able to go beyond passive attribution and participate in active prosecutions against the perpetrators of cyber-attacks.

- KPN is working on ways to embed security into home routers, extending the same ‘clean pipe’ principle already offered to businesses to Dutch consumers.

- One of the areas where KPN believes it can differentiate is in Operational Technology (OT) and Industrial Control Systems (ICS). It has already started working with customers in this area but more should be expected. For example, the company is currently working closely with SecurityMatters on a network-based IDS specifically developed for the protocols used in building automation systems like Building Automation and Control Network (BACnet).

- An initial offering that provides a way for enterprises to begin preparing themselves for the quantum safe computing challenges that lies ahead.

As already stated, KPN takes pride in the dramatic reduction it has achieved in the time it takes to mitigate high security vulnerabilities. Increasingly now, the emphasis is on reducing the time it takes to mitigate those vulnerabilities that rank as medium in terms of the risk associated with them and the ease of exploiting them.

**KPN has no plans for international acquisitions**

Like many medium sized telcos, successive generations of KPN management have gone back and forth over the years as regards what ambitions it should have outside its home market. The current management’s emphasis is firmly on the home market and this is reflected in the cyber security space. As shown in Figure 1, to date all three acquisitions and both its VC investments in cybersecurity have featured local Dutch companies.

The company is so insistent on sticking to a home-first approach that when market rumours circulated in December 2017 that KPN was exploring M&A options with telcos in other countries, management took the unusual step of issuing a formal press release to deny it. The release stated emphatically that “KPN’s M&A strategy is focused on small in-country acquisitions and it has no plans to make international acquisitions.”

There is a lot to be said for the pragmatism of this approach. But, as of today, it does leave KPN with geographic limitations when it comes to serving the largest companies - in particular Fortune 500 companies. Although KPN doesn’t have an international play on the scale of the large, global managed security services arms of bigger telco peers like BT, NTT Security and Telefonica, KPN does provide its cyber security services across the globe. Both international organizations and global corporates leverage KPN’s expertise in a number of cyber security fields, including security monitoring, penetration testing and ICS assessments. Over time, KPN can be expected to explore ways to further expand the security portfolio it can offer global customers.

**About KPN**

KPN is the leading telecommunications and information & communications technology (ICT) service provider in the Netherlands. KPN offers a broad portfolio of services to the business, consumer and wholesale market, varying from fixed and mobile telephony, fixed and mobile internet, and TV to a wide range of ICT services, such as cloud, hosting, digital workspace, data services, internet of things and security.

For contact information for KPN and HardenStance see the last page.