Cyber Security Innovators: Deutsche Telekom

Service Providers # 1

Corporate Strategy

By Patrick Donegan, Principal Analyst, HardenStance

March 2018

A custom report for

T · · Systems ·

HardenStance

"Best in Class Research, Analysis & Insight in IT & Telecom Security"

Executive Summary

- The German market is characterized by especially high expectations of data privacy.
- Deutsche Telekom wants to be the leading security service provider in Europe.
- Deutsche Telekom's 1,250-strong Telekom Security unit is entering its second year of commercial operations.
- Driving sales in Europe is the near-term priority. Longer term, Deutsche Telekom will have to consider global partnership options.

Market Context

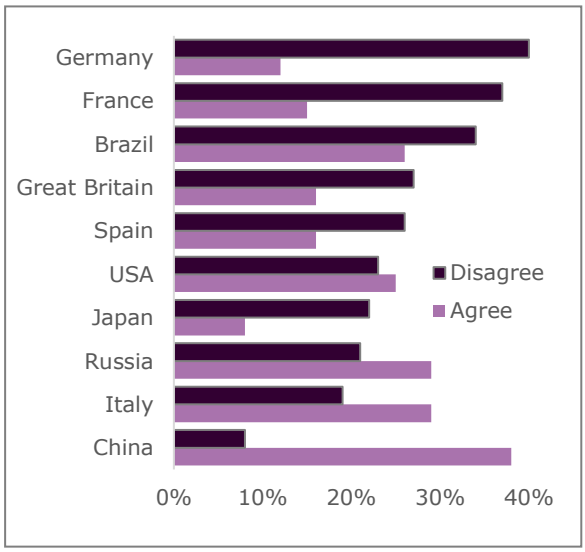
For historical reasons modern Germany has always been especially protective of its citizens rights to privacy. As shown in **Figure 1**, German consumers are among the most protective of their personal data anywhere in the world.

In 2017 a new law came into effect prescribing how providers of critical infrastructure must protect against cyber-attacks.

This differential was already embedded in German society long before Edward Snowden exposed U.S monitoring of Chancellor Angela Merkel's mobile phone in 2014 – and long before Russian adversaries hacked into German government websites in 2015 (supposedly in response to Germany's close relationship with the western-leaning government of Ukraine).

These attacks on national sovereignty merely heightened what were long-standing social concerns. Add to that mounting anxiety at the exploitation of encrypted communications by terrorists throughout the world and it's easy to see how Germany finds itself at the epicentre of global policy questions around cyber security and data privacy.

Figure 1: Consumer readiness to share personal data for rewards



Source: Statista, January 30th, 2017

Germany's politicians and regulators have responded to this cocktail of often-conflicting and contradictory public policy questions with a flurry of new laws and regulations.

In 2017 a new law came into effect prescribing how 2,000 providers of critical infrastructure in Germany must protect against cyber-attacks and report data breaches. The country's telecom operators are among those that have to comply.

New laws have also been tabled - some of which have been passed, some haven't – that redefine the rights of the state to monitor the activities of suspected criminals.

This gives unprecedented clarification in areas previously shrouded in secrecy, according to supporters of these measures. Opponents view them as an unacceptable increase in state powers. Consistent with this, the associated legal requirements imposed on telcos are now subject to closer public scrutiny than ever.

Within the EU, going back some years, Germany has also been the key driver of the far-reaching General Data Protection Regulation (GDPR) that comes into force in May 2018.

The German cyber security market

The German cyber security market is highly fragmented. In the consumer space, there are a number of vendors and operators selling their own solutions on line. For the SME and German 'Mittelstand' market there are a myriad of IT companies providing security.

In the corporate segment Deutsche Telekom's security arm, Telekom Security, faces large IT companies like ATOS, IBM Security and DXC Technology. Vodafone and Telefonica as well as the security arms of BT, Orange and NTT Security are among the cyber security arms of other telecom operators it also encounters in the business market. The likes of Siemens and GE are dominant in Industrial Control Systems (ICS) - and by extension the security of those systems as well.

Deutsche Telekom is investing €250 million per year in upping its commitment to cyber security.

The structure of the economy is important in shaping the unique character of the German market from a cyber security perspective.

- **Banking, manufacturing and the public sector are the largest industry verticals** measured in terms of their annual spend on cyber security.
- **According to current World Bank data, industrial output still accounts for 23% of German GDP.** This is more than twice as high as neighbouring France (11%) and UK (10%). The security challenge this creates lies in the way the Operational Technology (OT) used in industrial manufacturing environments world-wide is much less protected against cyber-attack than the Information Technology (IT) that supports office environments and white-collar industries. These OT environments are evolving from the still widespread security practice of being disconnected from the Internet to a more mature stance that embraces being securely Internet-connected whenever the opportunity outweighs the risk.
- **The 'Mittelstand' creates specific opportunities in cyber security**. While it is celebrated as the heart of Germany's economy, many of the medium-sized companies that make up the Mittelstand have almost – but not quite - enough resources to justify doing their own cyber security competitively themselves long-term. In principle this represents an unusually large demand pool for managed security services.

Cyber Security Strategy

Over the last three years, Deutsche Telekom has been investing €250 million per year in upping its commitment to cyber security. Whilst it has always taken the baseline security of its own infrastructure at least as seriously as any other telco, the company is late to market compared with some telco peers in seeing security as a strategic incremental revenue opportunity.

Deutsche Telekom's strategy focuses on the following:

- Providing a comprehensive portfolio to consumers, SME and large enterprises;
- Simplifying security with new cloud-based delivery models such as on-demand software from Deutsche Telekom's own trusted data centres in Germany;
- A formal company target of 'zero impact' to customer services from cyber-attacks;
- Strong emphasis on designing, regularly reviewing, and adhering to strong security practices and processes before, during and after a cyber-attack;
- Aligning with the requirements of all German and EU legislation;
- Becoming the leading security service provider in Europe.

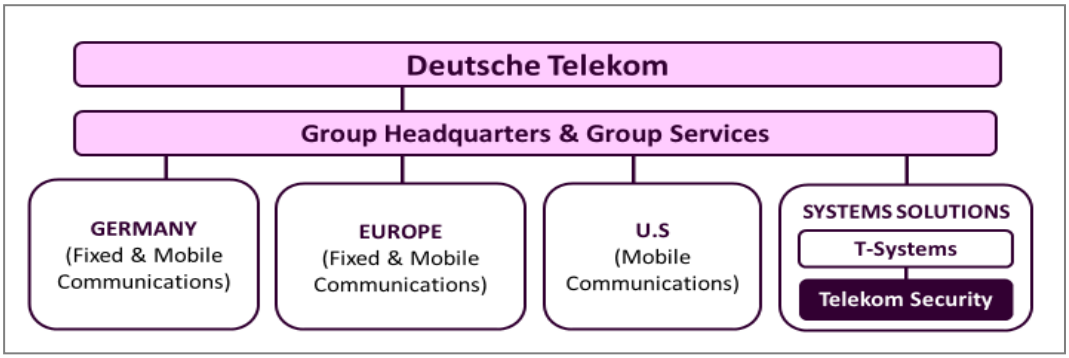
Progress Report

Over the last two years, execution against the strategy has been dominated by organizational restructuring accompanied by investment and build out of an extensive security product portfolio.

Effective January 1st, 2017, Deutsche Telekom assembled and restructured its security assets into a new organization called Telekom Security. Due to the largest security spending coming from the business sector, Telekom Security reports into T-Systems, one of Deutsche Telekom's four main Business Units as shown in **Figure 2**.

Telekom Security designs, procures and delivers cyber security policy and services for Deutsche Telekom itself – protecting the company's own infrastructure and employees – as well as for its customers.

Figure 2: Telekom Security is integrated into T-Systems



Source: HardenStance/Deutsche Telekom

Deutsche Telekom protects its own infrastructure as well as that of its customers from the same Telekom Security resources. The organization is structured in a way that is designed to assure customers that resources are always available to prioritize their contracts, independent of the needs of the parent company. Despite reporting into T-Systems, Telekom Security develops security services for consumers via Deutsche Telekom's consumer sales channels as well as to businesses via T-Systems and other business sales channels.

Telekom Security started 2017 with around 1,000 employees and ended the year with 1,250.

Telekom Security started 2017 with around 1,000 employees and ended the year with 1,250. This was quite an achievement in what is a very tight global market in cyber security skills. By way of comparison, BT currently has twice as many security professionals but that's because it already serves global customers world-wide with a sizeable presence in the Americas and Asia as well as the UK and the rest of Europe.

"Made in Germany"

Given the market context, Deutsche Telekom brands all of its Open Telekom Cloud services delivered from its own data centres as being "trusted", "compliant with strict German privacy regulations" and "the European alternative". This drives security as a core component of the company's value proposition, independent of generating incremental revenue from selling premium cyber security services. Customers have a choice, though. They can also have their data managed and stored in Telekom's data centres in other countries, at lower cost than using German facilities.

The company is extending this value proposition to the way it works with global cloud providers. T-Systems is a key partner in building out Microsoft's first cloud data centres in Frankfurt and Magdeburg, for example. T-Systems serves as the "data trustee" for Microsoft Cloud services, providing additional controls for customer data that can only be accessed with the permission of T-Systems or direct from customers themselves.

To give consumers a trusted, single sign-on, platform for online authentication as an alternative to the likes of Facebook, Deutsche Telekom has joined several other leading German companies in building out Verimi – which stands for 'Verify Me'. Other founding shareholders are Allianz, Axel Springer, Bundesdruckerei, Core, Daimler, Deutsche Bank with Postbank, Giesecke & Devrient HERE Technologies and Lufthansa.

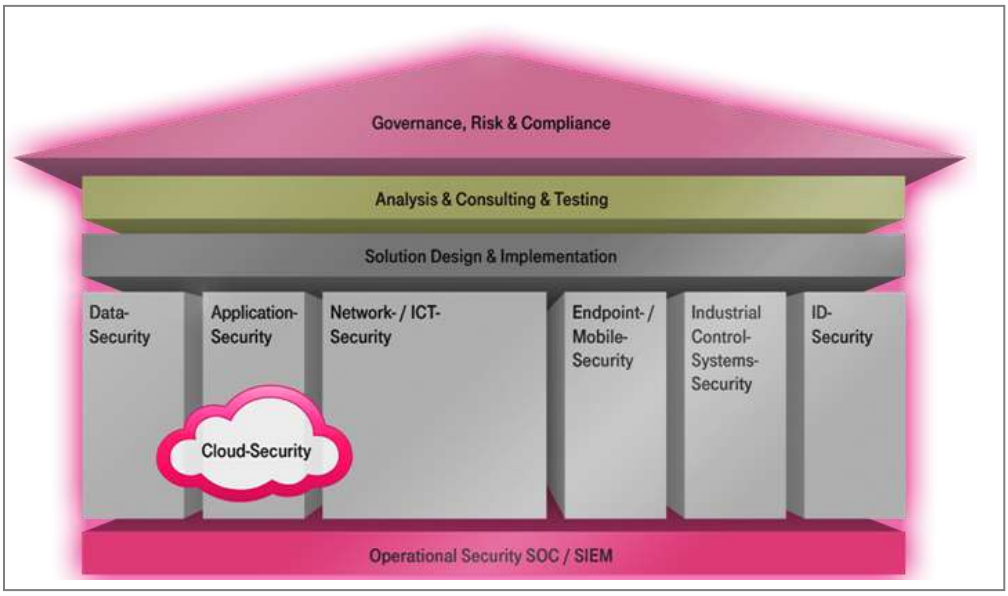
Security from the cloud – and to the cloud

Both the IT and the networking environments that Deutsche Telekom straddles are undertaking a migration to cloud delivered software – from equipment in central offices in the networking case and from on-premises equipment in the IT case.

In several respects, cyber security is undertaking the same migration – from the deployment of physical security devices such as firewalls to the consumption of firewall software as a service delivered from the cloud.

Deutsche Telekom has joined several other leading German companies in building out Verimi.

Figure 3: The Magenta Security portfolio



Source: Telekom Security

In addition to traditional on-premises delivery, Telekom Security wants to differentiate by also delivering cyber security services to enterprises and consumers as a service from its own cloud. In the case of enterprise customers that means offering services on premise, from the cloud, and to the customer's increasingly diverse cloud environments.

When it comes to incremental revenues from cyber security services anyone that questions Deutsche Telekom's commitment to this market nowadays really ought to take a look at the company's cyber security services portfolio, dubbed 'Magenta Security' (after the company's famously garish corporate colours).

The portfolio supports products from nearly fifty security vendors

Figure 3 depicts the six pillars of the Magenta Security portfolio:

- Data security;
- Application security;
- Network/ICT security;
- Endpoint/Mobile security;
- Industrial Control Systems (ICS) security;
- Identity security.

Figure 4: Magenta Security: partner vendors

Source: Telekom Security

With the Magenta Security portfolio offering cyber security products and services from nearly fifty different vendors as shown in **Figure 4**, Telekom Security has built out what is quite likely the broadest cyber services portfolio in Europe in a very short timeframe.

Customers can choose from three different supported endpoint security vendors. The three supported vendors are Kaspersky, Sophos and Symantec. The "Industrial Protect Pro" solutions for Industrial Control Systems (ICS) security leverage products from four vendors: Cyber X, CyberArk, Radiflow and Genua.

Magenta Security even supports truly niche products like Drone Protection. Developed with Dedrone, this detects drones intruding on private and public premises using a range of sensors including video cameras, frequency scanners and microphones.

Around a dozen Proof of Concept trials of the Industrial Protect Pro portfolio of customized firewall, encryption and anomaly detection products were carried out in 2017. Examples include German based automotive, chemical and other industrial firms with global presence that need central repositories from which to securely manage connections to all their products and customers throughout the world.

Internet Protect Pro and APT Protection are already all-cloud delivered services.

Internet Protect Pro (delivered in partnership with Zscaler) and Advanced Persistent Threat (APT) Protection (delivered with Check Point) are already all-cloud delivered services. In the case of most of the rest of the portfolio, Telekom Security has to continue supporting legacy on-premise, device-based, deployment models while it continues to drive migration to the cloud-based model.

The strategy for driving sales of the Magenta Security portfolio outside of Germany and achieving the target of being the leading security service provider in Europe, relies on several channels. The primary ones are:

- Deutsche Telekom's operator affiliates that give access to more than 165 million mobile customers, 29 million fixed lines and 19 million broadband lines world-wide.
- Local subsidiaries of T-Systems in more than 20 countries.
- Resale through partners and indirect sales channels.

Outside Germany, the markets that are seeing security sales pick up the fastest are Austria and Hungary as well as South Africa (where T-Systems has a sizeable presence).

An integrated Cyber Defence Centre in Bonn

The single most high-profile achievement since the formation of the new Telekom Security has been the opening of its new integrated Cyber Defence Centre Security Operations Centre (SOC) in Bonn at the end of last year. Around two hundred cyber security professionals are operating the new Master-SOC and the connected national and international SOCs.

Nowadays the SOC is the centrepiece of any large organization's own cyber security strategy – and the centrepiece too of any company wanting to provide comprehensive managed security services 24/7 to the full spectrum of business customers. In the SOC itself, as well as throughout the broader organization and its facilities, a key thing that separates leaders from also-rans in cyber security is their development of detailed operational processes for how security is implemented and managed; regular reviews of those processes; and strict adherence to these processes. This needs to be adhered to in "peace time" as well as when mitigating an attack. In this key area of security process management and Incident Response, Deutsche Telekom has shown clear leadership over the last 12 months. Two specific examples demonstrate this:

In cyber security process management and Incident Response, Telekom has shown clear leadership over the last 12 months.

- **The response to the 'Spectre' and 'Meltdown' vulnerabilities.** On January 4th, 2018, the world learnt of the 'spectre' and 'meltdown' vulnerabilities impacting many leading processors. In less than a day Deutsche Telekom had published a customer advisory – in German and English - stating that it had already started deploying the microcode updates provided by Intel in the Open Telekom Cloud. The advisory also informed customers that Telekom had already started implementing some workarounds for hypervisors and operating system kernels to ensure all processors, containers and virtual machines were once again properly protected.
- **The response to The MIRAI Botnet attack:** At 5.00 p.m. on Sunday November 27th, 2016, 900,000 home routers of Deutsche Telekom customers were taken offline by a cyber-attack. The attack leveraged the same MIRAI botnet that took out Dyn one month earlier, triggering the most large-scale Internet outages yet seen anywhere in the world. By any standards, Deutsche Telekom's Incident Response was first class. Within hours, packet filtering rules were applied in the network to prevent further impact. Patches to the affected products were also rapidly deployed. The following day a detailed customer advisory was published. The same advisory content was published in the form of online video interviews with Thomas Tschersich, Head of Group Security Services (again in German and English).

Some security professionals would doubtless prefer to focus on how the home router vulnerabilities should have been addressed before the 2016 attack. In one sense, this perspective is always right. The reality, however, is that in today's threat environment no organization should count on its defences being 100% impregnable. Planning to minimize harm if – when – an attack gets through is a critical layer in any multi-layered security stance. It's also an indicator of maturity in security that is often overlooked.

Figure 5: Investments in cyber security companies by Telekom Capital Partners

Company	Country	Description
Anomali	U.S	Critical threat intelligence capabilities
Boku	U.S	Use of mobile phone numbers for secure payment.
Callsign	U.S	Secure mobile access to websites
CipherCloud	U.S	Virtual appliance or hosted service to secure sensitive customer data across public/private cloud applications.
Lookout	U.S	Protects mobile devices against malware and spyware,
Safebreach	Israel	A "hacker's view" of an enterprise's security risks
ZenMate	Germany	Encrypts browser traffic, hides real location, unblocks geo-restrictions, and provides Wi-Fi security.

Source: Telekom Capital Partners

Lastly it's worth noting how the company's security strategy has been built out leveraging support from its venture capital arm. This is Deutsche Telekom Capital Partners, which manages $1 billion in holdings across seventy companies. The seven start-ups profiled in **Figure 5** are the most focused on cyber security in the company's VC portfolio but there are others whose remit also touches on the security space. While its market focus is very centred on Germany and the rest of Europe, U.S companies account for five out of the seven cyber security start-ups that DT has invested in.

Gap Analysis & Next Steps

Characterized as they were by organizational change, new hiring and heavy investment the years 2016 and 2017 were disruptive. Over the next eighteen months, the focus now needs to be on executing against the existing plan for the business:

- The remaining T-Systems units outside Germany that haven't yet fully ramped up the sales drive around the enterprise security portfolio will do so during the first half of this year (Consumer security services are already being offered in every European country where Deutsche Telekom has a network operator affiliate).
- A high priority in 2018 is to continue supporting customers in their migration to the cloud-based service model as soon as this is feasible and provides added value. Rapidly growing the number of business customers buying SOC-based services is also key to achieving growth targets.
- Consistent with the above, another goal is to accelerate the migration of threat detection from end devices to Deutsche Telekom's own network. In the case of Mobile Protect Pro, for example, detection of malware picked up on third party Wi-Fi networks will continue to have to be done on the user's device. But detection of cellular-delivered malware is being moved to the network. Users should benefit from malware being removed before it even reaches the device (as well as from longer battery life).

The breadth and depth of the portfolio has its advantages but it wouldn't be a surprise to see a bit of portfolio-pruning in 2018.

The breadth and depth of the Magenta Security portfolio certainly has its advantages. All the same it also has potential to serve as a drag on efficiency - from the number of vendors that need working with to the investment in salesforce training. It wouldn't be a surprise to see a bit of portfolio pruning during 2018.

Deutsche Telekom should communicate more on its own value-add

Whilst using its size to extract competitive pricing and responsiveness from its security vendors is a core part of the company's value proposition, security vendor partners arguably featured a little too prominently in the positioning of Telekom Security during its first year. Deutsche Telekom brings a lot of its own networking smarts to its cyber security stance. This is important to emphasize against the charge often levelled against telcos in general that they are nothing more than "dumb pipes".

For example, vendors Arbor Networks and Link 11 feature in the Magenta Security portfolio as recommended DDoS protection providers. But look under the hood of how Telekom Security protects itself and its enterprise customers against DDoS attacks and there's a lot of home-grown engineering embedded in the Deutsche Telekom network complimenting the solutions of its vendor partners.

There are some encouraging signs that DT's own technology value-add will feature more prominently in the company's marketing from now on. At the end of last year, for example, the company began promoting the capabilities of its so-called "Honeypots" – fake infrastructure or software designed to first attract cyber threat traffic and then respond to it in a way that confuses, deflects or counteracts the attacker. These are deployed, managed and monitored by DT and leveraged across its infrastructure to benefit all its customers. They're not a portfolio item that any one customer gets to buy.

Changes to the legislative framework Deutsche Telekom has to operate in continue to attract close public scrutiny. Deutsche Telekom nevertheless believes there are potentially some clear positives for customers arising from some of these changes. One example consists of important new rights – actually legal requirements – to quarantine traffic that looks like it may form part of a cyber-attack on behalf of customers. Done right, customers should benefit from this.

Zero-Touch Automation – but not yet in response to adversaries

At group level, Deutsche Telekom has set the ambitious long-term corporate objective of arriving at 100% automation in the way its overall network is programmed: "zero-touch network service management with no human involvement" as articulated by Arash Ashouriha, the company's Deputy Chief Technology Officer at a leading industry trade show at the end of last year.

The way Deutsche Telekom responds to sophisticated cyber-attacks won't be in the first wave of processes that align with that corporate goal. This is because the complexity of analysing and interpreting traffic to differentiate real threats from patterns which only appear to be threatening continues to require human intervention by skilled security analysts. Over time threat responses will need to become more automated too, though.

A global partnership play will have to be addressed sooner or later.

Leading U.S firms are bound to table global partnership offers

There is one obvious gap in Deutsche Telekom's positioning in the cyber security market. But with the near-term focus on sales in Europe it can likely wait until at least 2019.

That gap is a global dimension to enable Deutsche Telekom to compete in serving Fortune 500 companies all over the world - most likely via means of a global partner. Given the global distribution of cyber security expertise – and above all the global distribution of cyber security spending – that almost inevitably requires a U.S partner.

Any large European company with the goal of becoming a European leader can't have that as the ultimate end objective. There is bound to be greater ambition than that. That could materialize in attempts at partnership or M&A activity with specialists in managed security services like IBM Security, SecureWorks or Symantec. Alternatively, it could end up in talks with more culturally familiar telco partners with managed security services businesses like AT&T, Verizon or a smaller player.

This is pure speculation at this time. It's quite likely that at this stage the question is just as speculative inside Deutsche Telekom as it is outside the company. But if the European strategy succeeds over the next two years the question of a global partnership play will have to be addressed sooner or later.

Is local M&A activity likely?

Whether Deutsche Telekom will follow other telco peers like KPN in the Netherlands and Sweden's Telia Company that have acquired small and medium sized IT and cyber security companies in their local markets to strengthen their hand is much less clear. To date, Deutsche Telekom and T-Systems have grown their presence in the German market organically. Given management's emphasis on near-term consolidation rather than further organizational upheaval, security-related M&A activity within Germany in the next twelve to eighteen months looks unlikely.

How Deutsche Telekom will go about achieving its growth targets elsewhere in Europe is perhaps another matter. Confining itself to the same organic growth model it has relied on in Germany runs the risk of falling short of its growth targets. Acquiring one or more managed security providers in Western Europe on the other hand, might just help achieve them ■

For contact information for Deutsche Telekom and HardenStance see the last page.

About Deutsche Telekom

Deutsche Telekom is present in more than 50 countries. With a staff of some 218,300 employees throughout the world, the company generated revenue of 73,1 billion Euros in the 2016 financial year, about 66 percent of it outside Germany.

For more information about HardenStance, visit **www.hardenstance.com**

For more information about the sponsor, visit **https://www.t-systems.com**