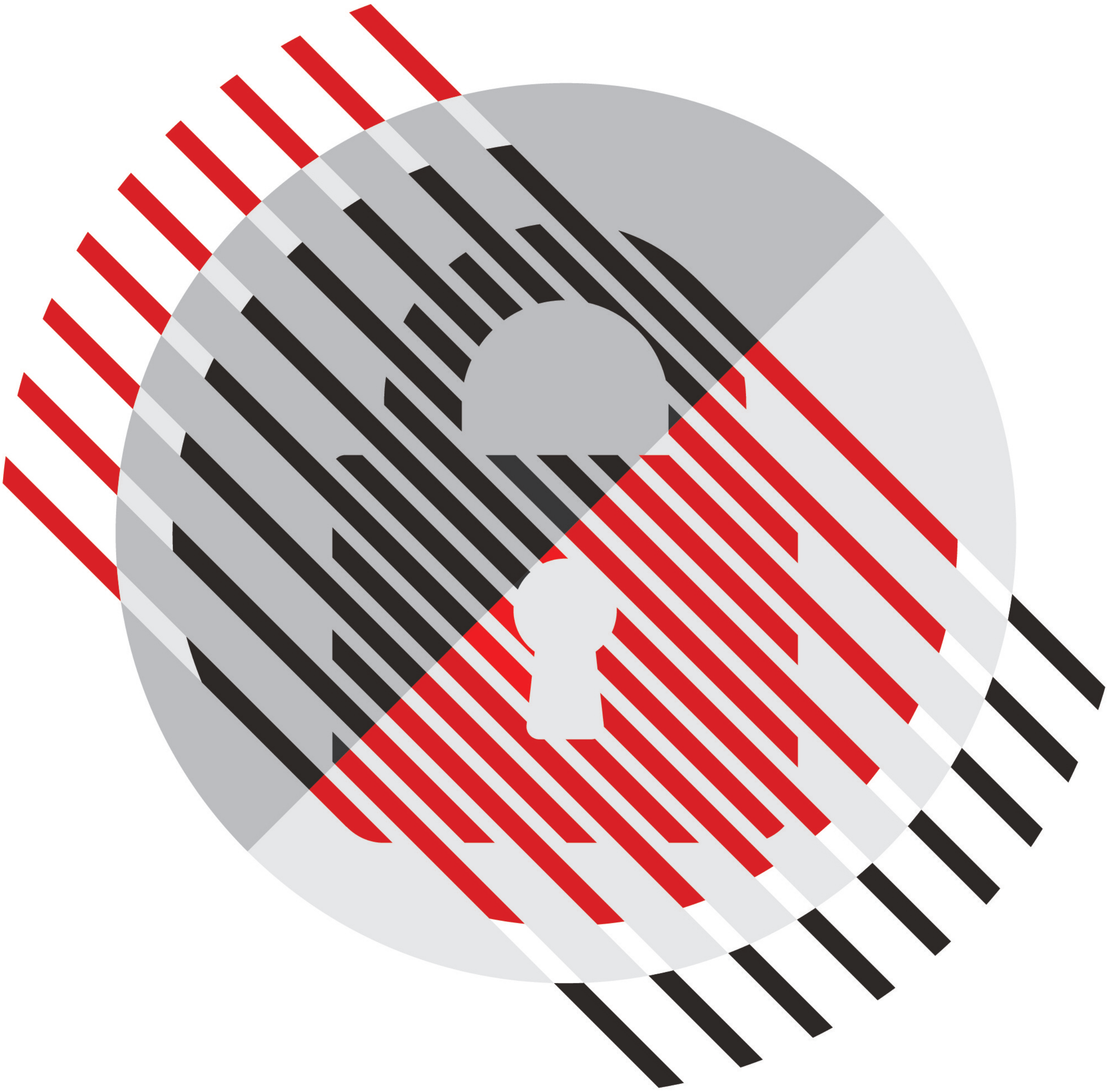
SECURITY IMPERATIVES FOR DIGITAL TRANSFORMATION

Author: Patrick Donegan, *Principal Analyst, HardenStance Ltd*
Editor: Dawn Bushaus, *Managing Editor, TM Forum*

August 2019



Sponsor:

amdocs

Contents

03 The big picture

05 Section 1: Assessing risk from an organizational perspective

07 Section 2: Data governance, data protection and liability in the cloud

09 Section 3: Sourcing secure software

12 Section 4: Shifting from DevOps to DevSecOps

15 Section 5: Securing APIs is essential

18 Section 6: AI is a double-edged sword for cybersecurity

21 Section 7: Make it happen – Strategies for improving cybersecurity

23 Additional feature: Taking a proactive approach to cybersecurity

26 TM Forum Open Digital Framework

27 TM Forum research reports

28 Meet the Research & Media team

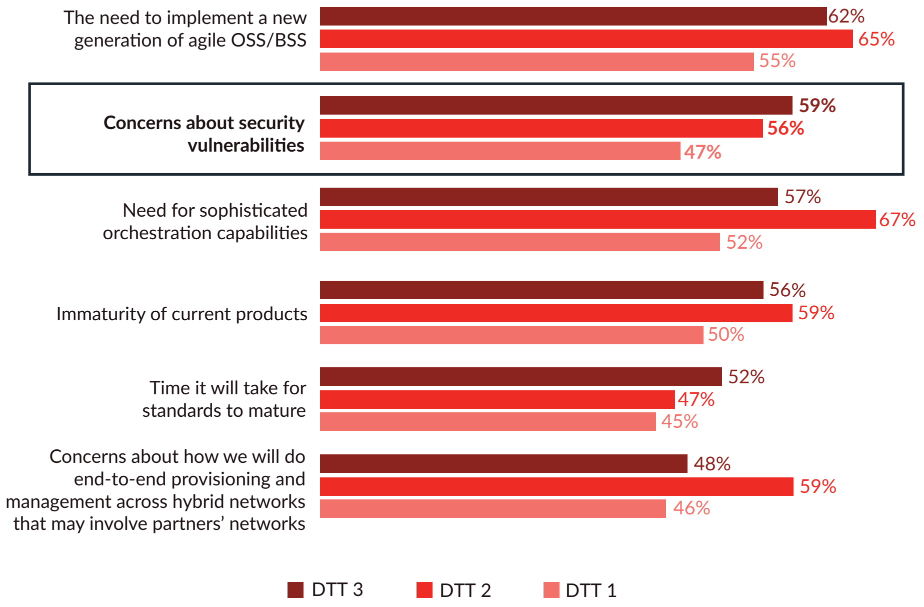
The big picture

As well as creating new opportunities, digital transformation creates new information security risk for communications service providers (CSPs). Taking into account requirements in terms of people, processes and technologies, this report looks at some of the key ways in which CSPs need to enhance and upgrade their security stance to mitigate new risk.

By drawing on examples of harsh lessons learned and tangible progress made by telcos at the forefront of transforming their security operations, it is possible to identify key areas where new vulnerabilities are likely to arise, why addressing them needs to be prioritized, and best practices for fixing them.

TM Forum's research shows that CSPs are aware of the threat that security risk poses to the success of digital transformation programs. Concern about security vulnerabilities is one of only two challenges whose absolute score and relative importance have risen with each of the Forum's Digital Transformation Tracker (DTT) surveys. In the latest one conducted a year ago, security had risen to second place among telco respondents' concerns, up from fourth place in the first survey (see graphic below).

Ranking the challenges of network transformation



TM Forum, 2018

Reason for concern

The names of CSPs haven't featured in news headlines announcing the most severe data breach impacts. No event in the telecom sector compares with the Equifax data breach in terms of the number of people adversely affected, for example. Nevertheless, individual operators have been publicly cited dozens of times as victims of information security breaches and cyberattacks in recent years.

Telcos should be proud of their rich heritage of protecting the availability of network infrastructure and the confidentiality of customers' data in transit – their track record is pretty good. But the market is changing, and digital transformation is helping to drive the change (see panel on page 4).

Digital transformation adds to security risk for CSPs

The following aspects of digital transformation combine to create a much larger attack surface and make security more challenging to design and implement in a way that's effective, scalable and easy to operate:

Operators are breaking down data silos within their organizations, which makes data more accessible to employees and trusted business partners, but it also makes it more vulnerable to attack.

The number of endpoints in the network – including internet of things (IoT) devices and sensors – is set to increase exponentially as the telecom network becomes increasingly open, virtualized, distributed and complex, especially as 5G is deployed.

Artificial intelligence is considered key to digital transformation and indeed to cybersecurity, but it also introduces new risks around privacy and regulatory compliance.

Automation saves time and money and accelerates time to market, but using corrupted insights propagates risky outcomes as rapidly as positive ones; it's also helpful to attackers in the case of inadvertent malware distribution.

CSPs regularly suffer from the same enterprise security breaches experienced by other types of businesses. For example, operators have been directly impacted by the WannaCry outbreak, exposure or theft of customer data from insiders and cyberattacks, and DDoS outages. Other real-world impacts have arisen from vulnerabilities that are specific to the telecom sector. These include the use of Signaling System 7 exploits to steal money from customers' bank accounts, hijacking of customers' routers and SIM card fraud.

CSPs are exposed to increasing business risk arising from data breaches and other attacks, and attack vectors are becoming increasingly sophisticated. Data protection regulations like the EU's General Data Protection Regulation (GDPR) threaten stiffer penalties on all businesses for not protecting against and reporting data breaches. The telecom network also risks being center stage when nation states take to the cyber domain to attack one another. As Remy Harel, Network Security Manager, Orange, puts it:

> "I believe the next wars will be in cyberspace. The problem is the battlefield will be my network."

Make money too

Failing to adequately protect customers' data can result in increased costs. The price can be paid as a direct cost in the form of fines from regulators or lawsuits from customers, as an indirect cost in the form of overall brand damage, or as foregone revenue (for example, new business cases being postponed or cancelled because customers lack confidence in the security that supports it).

The upside of this is that if security is well managed, it can be a positive differentiator for CSPs. As Ruza Sabanovic, Group CTO at Telenor Group, explains:

"Security and privacy are the secret weapon we have in building trust. We haven't really monetized it yet."

Assessing risk

CSPs need to undertake an end-to-end cybersecurity risk assessment around this changing landscape in security threats and opportunities. Operators should focus more than they have in the past on protecting the integrity of the network and packets in the network. They also should focus more on the confidentiality of data, both at rest throughout the telco organization as well as in transit. The assessment also must investigate the risk that comes with digital transformation and determine the necessary steps to mitigate it.

Read this report to understand:

- How security requirements around people, processes and technology are changing
- Why end-to-end security is more important than ever, and why good data governance is key as CSPs develop multi-cloud environments
- Lessons learned from telco data breaches
- How to source software that can stand up to security threats
- Why CSPs must evolve from DevOps to DevSecOps
- Why it's critical for CSPs to secure application program interfaces
- The role for artificial intelligence in cybersecurity
- What CSPs at the leading edge of innovation in cybersecurity have learned so far

Section 1

Assessing risk from an organizational perspective

Simply put, a communications service provider's (CSP's) cybersecurity 'posture' means its overall security strength. The posture must cover all four of the organization's technology domains – internal IT, operational and business support systems (OSS/BSS), customer-facing channels and the network. Each domain has exposures, and once in, attackers can move between them. This section of the report looks at how CSPs can assess risk end to end from an organizational perspective.

The CEO needs to lead in communicating how security failings can undermine digital transformation goals, hence why they must be addressed. The security team should be the servant of development teams rather than their master, and employees should be celebrated as security monitors or sensors as much as they are feared as points of vulnerability.

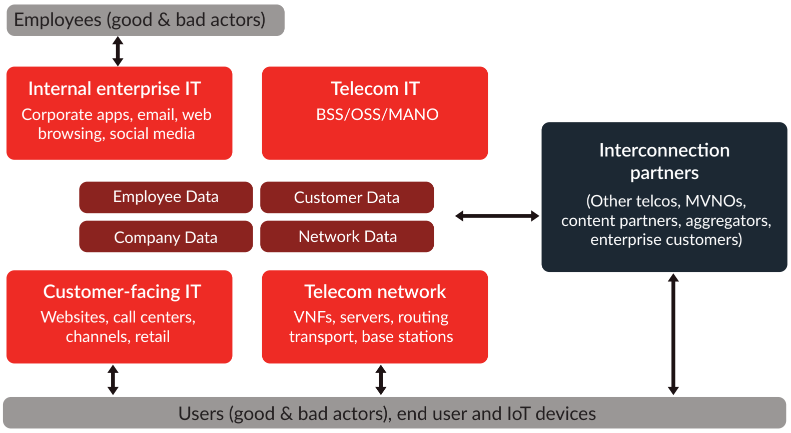
The graphic below provides a starting point in explaining why both risk and opportunity increase with digital transformation and why an end-to-end cybersecurity posture that spans the four technology domains of a CSP is required.

The notion that perimeter security alone is effective began disappearing before CSPs even considered digital transformation. Today, perimeter security controls like firewalls are assumed to be compromised. A robust cybersecurity stance increasingly mandates a zero-trust environment in which no device or application is inherently trusted and where investment is made in detecting and mitigating the subset of threats assumed to have evaded perimeter controls.

As illustrated in the graphic, each of a CSP's domains is driven by different technology requirements and communities, and each has its own security requirements. However, alignment or tight coupling is needed with adjacent domains.

From a cyberthreat perspective the boundaries often have blurred. As an example, four years ago a complex multi-vector attack was launched by an Iranian threat group targeting telcos in Africa and the Middle East. It started in the enterprise IT domain with a social engineering attack via LinkedIn on operations personnel that lured them into a trusted relationship. The hackers then shared malware-infected documents aimed at gaining access to the operator's operations environment. This provided a bridge into manipulating the telecom network itself. This kind of lateral movement across domains – enabled by software and facilitated by weak security controls within and between domains – is a common attack vector.

Risk and opportunity increase with digital transformation


Employees (good & bad actors)
Internal enterprise IT
Corporate apps, email, web browsing, social media
Telecom IT
BSS/OSS/MANO
Employee Data
Customer Data
Company Data
Network Data
Interconnection partners
(Other telcos, MVNOs, content partners, aggregators, enterprise customers)
Customer-facing IT
Websites, call centers, channels, retail
Telecom network
VNFs, servers, routing transport, base stations
Users (good & bad actors), end user and IoT devices

HardenStance & TM Forum, 2019

No security by obscurity

Digital transformation puts CSPs, together with their data assets and networking capabilities, at the center of a digital ecosystem of customers, partners and suppliers. To succeed, the ecosystem must be as open, dynamic and as frictionless as possible. The challenge with this is that openness serves to undo much of the so-called 'security by obscurity' that telcos have traditionally enjoyed.

For example, data silos impede agility, which CSPs must address, but from a security perspective silos are advantageous because only a select few developers can easily access and navigate each one. Similarly, proprietary interfaces between telecom network elements take a very long time to specify and at high cost. But at least it's a small, rarified community that understands and uses them, which creates a higher barrier to entry for attackers than open standards.

In a successful ecosystem, a low level of friction between trusted organizations, individuals and behaviors must be balanced by a high level of friction for those that are not trusted.

Leadership is key

Addressing new risk as part of an end-to-end cybersecurity risk assessment requires leadership from the very top of the CSP organization. This should start with explicit recognition from the CEO that:

- Telcos have a track record in security that is mixed rather than outstanding.
- Digital transformation creates new security risks, some of which the company may not fully understand or have complete fixes for, yet must address.
- Digital transformation targets will be missed without supporting investments in security people, processes and technology.

The CEO also needs to take responsibility for ensuring that the company has a customized, robust cyberattack response plan in place. This should map out the procedures to be followed, as well as the responsibilities of departments and named individuals, in the event of a suspected data breach or other impact. The CEO also needs to support the plan being rehearsed by key stakeholders with cyberattack simulation exercises, and reviewed following those simulations.

In terms of the CSP's security organization, a change is needed in the way this team interacts with the rest of the organization. The leaders of the security team need to peer with other parts of the organization – or indeed view them as customers. This is more likely to stimulate real demand for the security team's services rather than imposing its will on another department because a reporting structure says it can (for more on this as it relates to DevSecOps, see Section 4). Similarly, the importance of diffusing security principles throughout the organization increasingly requires the security team to engage in more training of others within the organization than traditionally has been the case.

Adding skills

Deutsche Telekom's Chief Security Officer, Thomas Tschersich, believes he has the staff he needs for internal security today, but when it comes to the skills that he expects to bring into his team in the coming years, he points to people with intimate knowledge of how adversaries think and behave as a priority.

"I can see that for selling additional security services to enterprises, we are going to want to grow headcount significantly," he says. "But for our internal security requirements, I think the headcount we have today should be okay for the next five years or so."

> Humans are often a security strategy's weakest link. People can easily break security policy out of forgetfulness, frustration with the constraints that policy imposes or indeed malicious intent. Measures need to be taken to be taken to protect against all these scenarios.

That said, the sheer number of employees across a CSP organization, together with the role that many have in the frontline of interactions with customers and suppliers, also makes employees uniquely well placed to serve as a network of protective sensors. This, however, is on condition that there is investment in sufficiently high-quality training to motivate them to serve in that role.

There are also areas where human factors need to be negotiated between the security team and employees in other departments. It's a legitimate and important requirement of the security organization to access more log data from throughout the organization to obtain a better, more dynamic view of security threats. But people can be reluctant to provide data for fear of being held accountable for errors they have made on their machines. Setting the right culture that promotes good cybersecurity hygiene without being unduly punitive is key.

In the next section, we'll look at the need for good data governance, particularly as CSPs develop multi-cloud environments.

Section 2

Data governance, data protection and liability in the cloud

Communications service providers (CSPs) face new challenges in protecting data that is stored and used within their organizations and exchanged with partners. Data protection must be anchored in the foundational building block of a data governance framework, which increasingly includes liability exposures spanning complex multi-vendor and multi-cloud environments.

Data governance is the set of unique rules and processes for managing the integrity, availability, usability and security of data. A data governance framework – developed in conjunction with a CSP's legal department from the outset – is the foundation upon which a telco's digital transformation strategy should be built. Good decision-making depends on good quality, trusted data, and this, in turn, depends on good data governance.

The importance of data governance in underpinning digital transformation also makes it the foundation of any CSP's information security strategy. The relationship between the two isn't static; they are deeply intertwined.

The goals, enablers and outcomes of digital transformation also drive changes in the requirements for data governance as much as the other way around. The use of application program interfaces (APIs) to break down data silos enables digital transformation, but this must be factored into data governance.

For digital transformation to drive successful edge use cases, data governance must take proper account of how data is generated, stored, analyzed and protected at the edge.

And artificial intelligence (AI) can only be applied to use cases according to the terms provided for by the telco's own data governance framework. As Mario Meir Huber, Head of Big Data Analytics and AI Centre of Excellence at A1 Telekom Austria Group, puts it:

> “
>
> Data scientists can do almost nothing without data governance.”

Embracing Agile

Eric Muse, Verizon's Executive Director, Information Security, says it's critical to adapt data governance and management to the much more open and dynamic environment enabled by digital transformation.

“Establishing line of sight with so many other parties involved besides your own IT team is where I have to put a lot of my focus,” he explains. “You have to support other lines of business signing up for cloud services, for example.

> “
>
> You have to be able to establish where the data is, where it's living, how it's protected and cared for, while all the time continuing to bolt different third parties onto that ecosystem. That's perhaps the biggest challenge with digital transformation.”

To support this, automated discovery tools must feature prominently in a master system of record that can generate an inventory of where specific data resides at any given time. The tools should be able to reach into every corner of a CSP's organization and touch every part of its IT estate, including 'shadow' IT projects managed outside the IT team.

Data controllers vs. data processors

Data controller

- Owner of data
- Decides why and how personal data should be processed

Data processor

- Processes data on behalf of the controller
- Usually an external third-party

TM Forum, 2019

Handling data

Digital transformation also creates substantial new complexity – and new risk – around the optimal attribution of liability for data protection between data controllers and data processors (see graphic above). CSPs perform both roles for their own data and for customers' data.

In the telco context data processors are defined as third-party partners. Effective implementation of data governance and liability relative to data protection regulations like the EU's General Data Protection Regulation (GDPR) get very complex as telcos move applications and services to the cloud.

Take an example of a CSP offering enterprise services from a public cloud using an operational model that involves multiple parties processing sensitive data. These could include a public cloud provider, an IT outsourcing company and one or more network equipment vendors – and any of their sub-contractors – as well as the CSP. In this increasingly common scenario, operators need to arrive at robust legal agreements with each party that clearly establish liability in the event of a data breach.

A chain of responsibility for end-to-end data security across the parties must incorporate service level agreements (SLAs) for confidentiality, integrity and availability (CIA), which are core security tenets, as well as for data anonymization and in some cases restrictions on data leaving any one country or region. Increasingly, the operator and its partners each must be able to demonstrate to their own legal departments what their liabilities are and that they have the appropriate internal processes in place to support them.

The more complex the cloud environment in terms of the number of parties involved, the harder it is for cause, effect and liability to be established in the wake of a data breach. As part of their transformation programs, CSPs should ensure that data governance, information security and legal departments are engaged in the sales process earlier and at a more detailed level.

This requirement extends to disaster recovery, which has risen in prominence in recent years due in part to heightened cybersecurity risk. Being able to understand, map and capture flows of data – which vendors touch it, and where – in order to meet disaster recovery targets gets increasingly challenging in a multi-vendor, multi-cloud, software-driven environment.

Public clouds

As they transform digitally, some CSPs may want to use third-party public clouds to run core public telecom services as well as value-added services. A key security barrier to doing this is the flat administration, single root architecture of public clouds, which allows all the administrators within an environment to share the same cryptographic root of trust independent of their role or seniority. This tends to merely prohibit administrators from accessing restricted areas, whereas many operators will want the potential to access these areas to be eliminated altogether.

CSPs and their suppliers are exploring how to support this, focusing on how to separate the vast majority of non-sensitive or partially sensitive traffic from sensitive traffic in a third-party public cloud environment. The idea is that a small subset of highly trusted engineers can then manage sensitive traffic from within a wholly isolated zone served by its own dedicated root of trust.

One foundational approach to this is offered by an ETSI technical specification released earlier this year which provides extra security for sensitive telecom network functions down to individual virtual machines. The spec introduces a trust hierarchy onto the flat administration architecture of public clouds so that only a subset of telco engineers or processes can access sensitive functions. For more on this, see this HardenStance Briefing.

In the next section, we'll look at how CSPs can ensure they are sourcing software that can stand up to security threats.

Section 3

Sourcing secure software

The coincidence of telecom networks becoming more software-driven during a new era of geopolitical polarization has put secure software sourcing at the top of the political agenda. Hence it has become a critical dependency in the digital transformation plans of communications service providers (CSPs). But operators often struggle to understand what kinds of risk they should prioritize mitigating – and how. Fortunately, new requirements for improving security around telco software sourcing are emerging.

The sharpest focus is on the risk of nation states directing telecom vendors headquartered in their home country to install backdoors to spy on foreign telecom infrastructure or carry out other types of attack. The media representation of telecom software security through the lens of this issue has been unhelpful to the telecom sector. Poorly informed coverage, often citing entirely politically driven perspectives, has promoted a weak understanding of software security challenges, particularly among the politicians who exercise so much influence in this area.

Strikingly, public dialogue has not focused on how to mitigate such risk by building networks capable of containing the damage arising from such incidents. As Ciaran Martin, CEO of the UK's NCSC, pointed out in a speech in June 2019, telcos must mitigate the risk of major incidents arising from operational mistakes by any of their vendors. They also must mitigate the risk of a hostile nation state inserting and exploiting malicious code covertly into a foreign vendor's software or indeed placing human operatives inside a foreign vendor's organization to cause similar disruption. Viewed in this context, the risk of malware being melted into a vendor's code on the orders of a nation state is just one among many comparable risks, each of which can be addressed with mitigation techniques.

Silver lining?

Like it or not, it's also inevitable that this poor-quality public dialogue seeps into the private dialogue between the leaders of the political, cybersecurity and telecom worlds. There is nevertheless a potential upside to all this: The intense focus on this threat vector presents an opportunity to shine a light onto the much broader security vulnerabilities of the telecom industry's approach to creating and sourcing software securely.

Canada's TELUS is an industry leader that's looking to drive higher security standards. At the FutureNet World conference in March, CTO Ibrahim Gedeon relayed the need for greater software resiliency, saying:

> “None of the software available is resilient. On a scale of one to five, today as an industry we are at about a two.”

He added that TELUS has enjoyed a 15% discount with NFV, but software resiliency is not yet on the practical roadmap of the vendors.

At another conference in May, TELUS Chief Security Officer Carey Frey explained that a couple of years ago TELUS suffered delays lasting months after discovering a major software vulnerability. The vulnerability, which was found in a master certified image of a network functions virtualization (NFV) platform delivered by one of the company's vendors, was the Shellshock security bug, also known as Bashdoor. This is a very well-known vulnerability that was first discovered in September 2014.

Telcos should be raising the bar for their vendor partners on the security of their software development processes. It's not enough to evaluate a new release to see what it does and make sure it doesn't break anything. Developers must also evaluate and test for the potential to break something or cause a data breach weeks, months or years down the line.

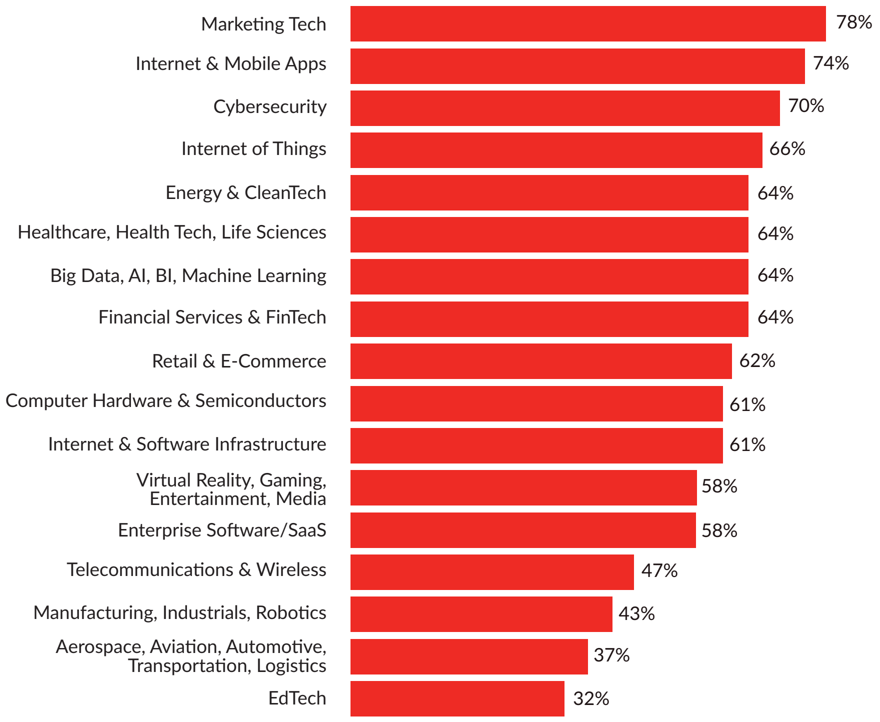
The reality is that even if a vendor – or an external intruder into the vendor's development process – planted a backdoor into a product, it wouldn't necessarily look like one. Since attacks can just as easily be carried out by exploiting existing benign bugs as through malicious backdoors, telcos should be paying a lot more attention to this. As Stefan Schröder, Senior Expert, Mobile Network Security, T-Systems International, puts it:

> “The biggest problem with software security is bugdoors rather than backdoors. Our focus is on removing these ‘normal' bugs.”

Open source risk

Telcos are also increasing their dependence on open source software, which includes their own software development activities and the increasing dependence of their vendor partners on open source software. The graphic above shows the average percentage of open source in each audited codebase by industry, as reported in Synopsys' *2019 Open Source Security and Risk Analysis report*.

Average percentage of open source code by industry



TM Forum, 2019 (source for data: Synopsys)

The merits and risks of open source software from a security standpoint are generally well understood in telco circles. Many more pairs of eyes look over the code of Linux, Kubernetes and OpenStack than is the case with any proprietary software, for example. On the other hand, this increased scrutiny doesn't necessarily mean all bugs will be found.

CSPs must discriminate between open source products and projects. Products are supported by commercial vendors and can be considered for use in a production environment, whereas projects are more akin to startups in that they require one or more organizations to volunteer additional injection of time, resources and commercially mature controls to get them over the line to being commercially deployable. Operators must also discriminate between the open source projects they commit to as they vary tremendously in terms of maturity.

Now that so many CSPs are deeply engaged in their own telecom-focused open source projects like Open Network Automation Platform (ONAP), ETSI's Open Source MANO (OSM) and the Telecom Infra Project (TIP), they are also benefitting from the open source model from a security perspective. As an example, before ECOMP was released to form the core of ONAP, ONAP members did a lot of work to overcome interoperability barriers. Initially, ONAP couldn't run in a third-party container environment because it assumed specific security rules and policies that were at variance with the third-party environment. The ONAP community has invested time and resource to address this.

Commercial challenge

There's also an emerging commercial challenge in the intersection between proprietary and open source software, where CSPs buy software from vendors that combines the two. Historically, suppliers have used a full-stack model where they sign up for service level agreements (SLAs) that include security clauses against their product's performance. It's a different matter doing that when their own software's performance is dependent on updates to open source components that the vendor doesn't control.

There may be some wiggle room for other ways of doing business, but most operators must make a choice between two options. Conceding to only using a vendor's supported version of open source components increases the chances of getting a comprehensive SLA from that vendor on par with traditionally SLAs. Alternatively, CSPs can buy the vendor's proprietary software and source the supporting open source components from a third-party platform or directly from the open source communities.

The second model certainly promises lower capital expense and greater agility, but there are several downsides:

- The CSP has to do the integration
- The SLA is likely to be a lot less comprehensive
- The operator needs to manage fault finding and security issues more proactively

As Remy Harel, Network Security Manager, Orange, explains:

> “With a vendor, they have 30 days to implement a security patch or pay [a penalty]. With open source, who will give me the security patch in the right timeframe?”

As CSPs move in the direction of DevSecOps (see the next section), they must factor in evaluation, verification and testing of code for security flaws. Pending that change, the effort should be led by existing IT, engineering, development, operations or security teams.

Section 4

Shifting from DevOps to DevSecOps

Drawing on different global standards across all their domains, most communications service providers (CSPs) handle security well from an architectural perspective. Where failings usually manifest is in development and especially in the operations environment. CSPs must implement best-in-class security practices while pursuing goals to reduce time to market with new services. This requires evolving from DevOps to DevSecOps.

The migration from waterfall development models to Agile and DevOps practices is central to successful digital transformation. The problem is that along with fueling new revenue growth, DevOps environments are also highly susceptible to introducing security vulnerabilities.

What is DevOps?

Agile
Focuses on **processes**, highlighting **change** while accelerating **delivery**

Continuous integration/ continuous delivery
Focuses on **software-defined lifecycles**, highlighting **tools** that emphasize **automation**

DevOps
Focuses on **culture**, highlighting **roles** that emphasize **responsiveness**

TM Forum, 2019 (based on a Synopsys graphic)

What is Agile methodology?

In February 2001, 17 software developers met to discuss lightweight development methods. The result of their meeting was the Manifesto for Agile Software Development which laid out the principles below. Today, many businesses have adopted them for software development and apply them to other parts of the business as well.

- Customer satisfaction is achieved through early and continuous delivery of software
- Changing requirements are always welcome – even late in development
- Working software is delivered frequently (within weeks rather than months)
- Close, daily cooperation between business teams and developers is required
- Projects are built around motivated individuals who should be trusted
- Face-to-face conversation is the best form of communication
- Working software is the principal measure of progress
- Development is sustainable and able to maintain a constant pace
- Continuous attention to technical excellence and good design are required
- Simplicity – ‘the art of maximizing the amount of work not done’ – is essential
- The best architectures, requirements and designs emerge from self-organizing teams
- The team reflects regularly on how to become more effective and adjusts accordingly

TM Forum, 2019 (source for data: The Agile Alliance)

New to the party

DevOps is still a relatively new operating model. Sonatype's sixth-annual *DevSecOps Community Survey 2019*, which surveyed 5,558 IT professionals in January and February of 2019, found that 25% of respondents rated their own DevOps environment as immature. About half considered their maturity to be improving, while only 27% said their DevOps environment is mature. With 58% of respondents hailing from North America, the global benchmark can be assumed to be significantly lower.

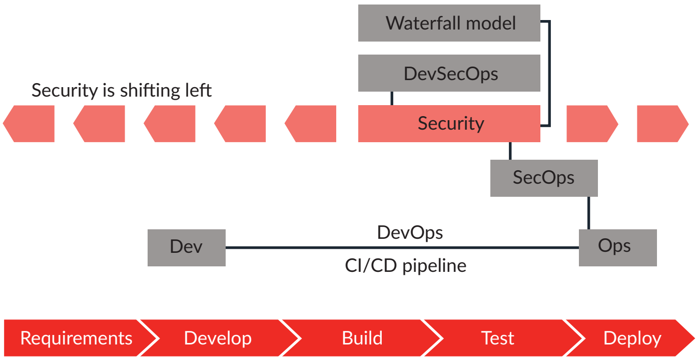
The days of the security team undertaking a six-week review at the end of a development process and then disengaging completely are over. CSPs are adopting a more dynamic model that aligns with continuous integration and continuous delivery (CI/CD) principles. But merely porting the same waterfall-based security model into a DevOps environment acts as a drag on agility rather than an enabler.

With digital transformation, security must be integrated into the DevOps environment using a DevSecOps model. As shown in the graphic above, this is achieved by 'shifting left'.

By shifting left, security can be embedded into development earlier. The idea is to remove flaws as early as possible in the development process and automate security as code the same way DevOps automates infrastructure as code.

However, consistent with building a CI/CD pipeline, simply shifting left doesn't make for an optimized DevSecOps environment. Engagement on the right is also necessary and key to generating a feedback loop from the operations team around attacks seen in the network, which can then be fed back into development.

Security is shifting left (and right)



HardenStance and TM Forum, 2019

Training is key

In some cases, implementing DevSecOps can mean that qualified security professionals are permanently assigned to development teams. More typically it entails the security organization providing extensive training for development and operations teams to upskill them in security best practices.

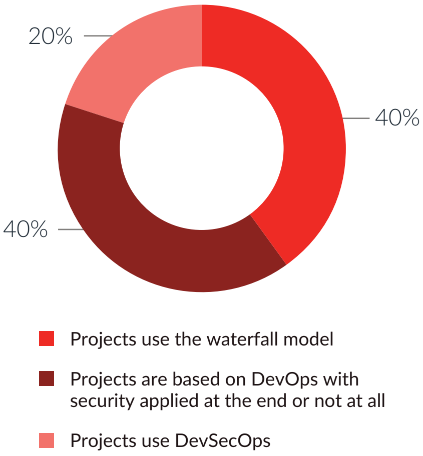
> This is critical for DevSecOps: Developers must have the right training, insights and learning environment to view security as a business enabler rather than a burden.

In addition to solving security problems, the security team needs to communicate its ability and willingness to be an enabling partner. Team members should feel motivated to impart security know-how to developers and members of the operations team. Similarly, DevOps teams should not view security teams as a delay-inducing security enforcer that has to be tolerated (or avoided). This requires the right culture and organizational structure with reporting lines that promote the right peering behaviors.

DT's security champions

Deutsche Telekom supports around 3,000 projects a year. From a security perspective the company categorizes them according to two key metrics: security requirements and development model. Teams determine whether the security requirements for a project are brand new, familiar or unimportant and then decide which development model to use. The company currently is using DevSecOps for one in five projects but plans to increase use.

Deutsche Telekom's use of DevSecOps



TM Forum, 2019

DT's DevSecOps model involves training individuals in the development and operations teams as 'Security Champions'. Once individuals have achieved this status, they enjoy the same freedom from supervision in enforcing security to the certified level of competence as a member of the security team.

By the end of 2019, DT plans to use the DevSecOps model for any project other than those for which security is not considered important. Although DevSecOps is becoming the preferred approach, DT will continue to support waterfall and DevOps models, depending on the requirements of the company's CIO and CTO teams. Says Thomas Tschersich, Deutsche Telekom's Chief Security Officer:

"I've been a security professional for many years with Deutsche Telekom. In the past, I was used to escalations on a daily basis. Sometimes developers were explicitly instructed not to consult the security team. With the new model, I have far fewer escalations. Nowadays escalations are more likely to be because I can't immediately meet the demand for my team's resources. The game-changer was for me to come to view the CIO and CTO as my customers, even though the reporting lines say we are peers."

The phrase 'embedding security' into development – especially 'from day one' – tends to be overused, often inappropriately. For example, it's entirely possible to implement a security model that is consistent with DevSecOps principles yet doesn't extend to the furthest edge of the shift to the left. At that far edge is an environment in which security carries every bit as much weight at the outset of the design process as functional design and performance. Says Shankar Arumugavelu, Senior Vice President and Global CIO at Verizon:

> "We certainly see ourselves scaling the DevSecOps model over the next year or two, but that's still a fundamentally reactive model. Beyond that, we are looking at the next level. Here, the new normal is one in which you are a lot more proactive. For example, you're doing threat modelling as a pre-requisite right at the very outset rather than further down the line."

In the next section we'll look at why it's critical for CSPs to secure application program interfaces.

Improving basic cybersecurity hygiene in CSPs' operations

Whatever progress CSPs are making to improve security, the pace isn't fast enough for some experts from outside the telecom sector. Speaking at an international industry conference in the Netherlands in May 2019, Dr. Ian Levy, Technical Director of the UK's National Cyber Security Centre (NCSC), cited some examples of telcos falling victim to cyberattacks. In one case, Russian threat actors attacked customer edge networks in the UK with the simplest of attack vectors that accessed devices via Telnet. He emphasized:

"Operational security in the telecom sector sucks and we have to fix it. We have to do better."

DevSecOps models can improve some of the more mundane aspects of cybersecurity hygiene like patching and monitoring. Infrequent patching (and sometimes nonexistent) of IT systems is still quite common in CSP organizations. As with the example of the Equifax breach caused by an unpatched Apache Struts server, these are a common source of security breaches.

Even operators whose DevSecOps strategies are advanced are taking two to four weeks to implement some critical patches. With accelerated process automation, the target should be 24 hours. Similarly, with monitoring most telcos are not yet capturing all the potentially useful samples of log data from within their organizations and feeding them into their security and information event management environment (SIEM).

Section 5

Securing APIs is essential

Application program interfaces (APIs) are a key enabler of digital transformation. Precisely because of the access they provide to data, they are vulnerable to attack. Communications service providers (CSPs) have already suffered data leakage arising from flawed API security controls, so it is critical that they develop strategies to address the threat.

APIs are key to breaking down a telco's internal data silos as well as exposing data to customers and ecosystem partners. With 5G, 3GPP even mandates the use of open APIs between different components of the service-based architecture instead of traditionally defined, closed interfaces.

But APIs represent a significant and growing attack surface. The most common impacts include:

- Customer account takeover and data exposure
- Fraud
- Service or application disruption arising from distributed denial of service (DDoS) attacks

Organizations that have been impacted by API-related data breaches include Amazon, T-Mobile USA (see panel opposite), the US Postal Service, Facebook and Google.

Risk around APIs has increased not just with the marked acceleration in their use, but also with the shift from using APIs internally to exposing them externally, as the T-Mobile breach highlights. Considering the sheer scale and variety of customer data and other data that CSPs could potentially share (subject to the constraints imposed by their data governance frameworks), their risk of exposure through APIs is greater than most organizations'.

While API security is a branch of application security, it must deviate from some of the norms of application security because from a security perspective, regardless of whether a human request is behind an API call, an organization only sees an API as a machine-to-machine call. This requires that an organization's framework for API security policy discriminate between good and bad traffic. This is well understood by a subset of API security specialists, but the understanding has only recently started to percolate down through the information security community.

Leaky API results in breach at T-Mobile

T-Mobile USA knows what it means to suffer a data breach arising from poor API design. In October 2017, the company announced that it had notified 2.3 million customers by SMS of a risk that a subset of their personal information had been exposed by a leaky API.

The breach arose from an identity and access management flaw in APIs that allow customers to access their accounts via the T-Mobile website. The URL returned to the user by the API featured a string of digits concluding with the user's mobile phone number. Appropriate API security ensures that a user can only access data associated with the phone number associated with their account. However, in this case the flaw allowed the same user to input a different T-Mobile customer's mobile number and access the same subset of that other customer's account information including name, address, email, mobile number and international mobile subscriber identity numbers.

The harvested data was then available to use for potential fraud on the operator and its other customers such as SIM fraud. While T-Mobile did not publicly elaborate in detail how it remedied the breach, the right type of fix in this instance would be restricting access to data other than that associated with a user's own mobile number and rate-limiting the number of times a given API token can be used.

API inventory

API security must be built in as organizations evolve from DevOps to DevSecOps, and the framework must consider the following:

- Which services need to be exposed
- How the target audience (whether internal or external) will interact with the service
- The type of data that can be legitimately exposed to different channels and what the authorized channels are

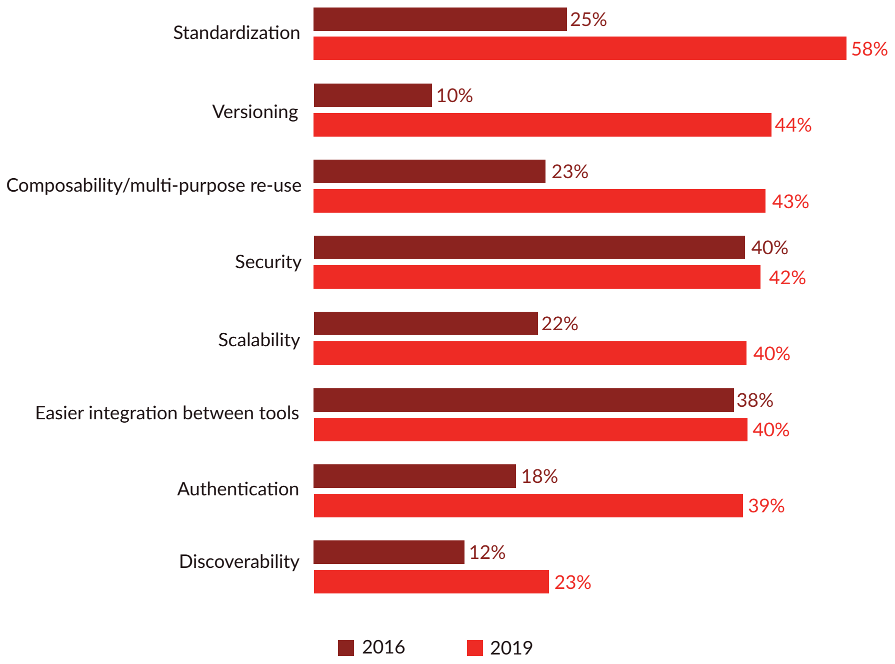
Maintaining an inventory of all APIs in use can be challenging in large organizations like telcos, but it is a fundamental requirement.

Within the underlying infrastructure, security controls typically are derived from three sources: identity and access management engines, which authenticate legitimate requests and authorize access only to the information that each API call needs; API management features from an API gateway; and threat detection and mitigation controls, such as via web application firewalls (WAFs) which are widely deployed in this context. In some architectures, these components may be integrated, but for the highest security requirements, dedicated elements are often preferred.

There is evidence that the right fixes for API security are readily available and becoming better understood. The annual *SmartBear State of API survey*, which surveyed 3,372 developers across multiple industry verticals in November and December 2018, offers a comparison of data for 2016 and 2018 (see graphic above). It shows that in 2016 security was at the very forefront of developers' minds in terms of API technology challenges they wanted to see solved. The 2019 survey, however, suggests that greater familiarity and technology maturity are making API security less challenging.

Nevertheless, some CSP leaders fear their companies are behind in terms of understanding and implementing the necessary security requirements. Says Ibrahim Gedeon, CTO of TELUS:

Biggest API technology challenges



TM Forum, 2019 (source for data: SmartBear)

> "In the telco world, very few people understand APIs properly, especially not with a high level of security. A lot of people don't know what they need to secure, let alone how to do that properly. I see some telcos putting an off-the-shelf EMS system in there without even changing the root password. As an industry we have a way to go in this area."

CSPs and suppliers collaborate on cybersecurity best practices for operations

Two new, important pieces of work from the TM Forum Open Digital Architecture (ODA) project aim to help operators assess and contain cybersecurity risks by incorporating security and privacy by design into operational and business support systems (OSS/BSS).

Part of the Open Digital Framework (see page 26), the ODA is a technology architecture and set of best practices for delivering Agile, next-generation OSS/BSS. It applies DevOps practices to network operations, which helps CSPs increase automation, improve flexibility and reduce costs.

Members are drawing on previous work in the Open API Program and the Platform and Security Management Technical Report. As part of TM Forum Release 19 they have created two new ODA Information Guides:

- ODA Governance and Security Vision is a business-level view of the concepts and requirements for security.
- ODA Enterprise Risk Assessment is a detailed set of concepts and tools to carry out enterprise risk assessment from functional and implementation perspectives.

Together the documents cover a full enterprise lifecycle vision for security and governance and provide detailed methods for assessing risk that support DevSecOps (see Section 4). Following are some highlights:

Security and privacy by design requires a methodology and tools for analysis, as well as governance to address relevant security requirements and threats in all lifecycle stages.

Cloud-native agility is achieved by assembling configurations of run-time components, each containing collections of ODA functions exposed by Open APIs. The security solutions must now work for rapidly changing software-defined trust boundaries, which require automated security models and tools.

Enterprise risk assessment provides a set of methodologies and analysis techniques including risk mitigation to automate security and privacy through DevSecOps for ODA cloud-native implementations.

The DevSecOps opportunity is to enhance DevOps development tools with automated configuration of security based on the risk assessment methods and use of deployment monitoring tools for threat detection.

If you'd like to learn more or get involved in TM Forum's work on security, APIs and automation, please contact George Glass.

In the next section, we'll look at the role for artificial intelligence in cybersecurity and explore lessons learned by early adopters.

Section 6

AI is a double-edged sword for cybersecurity

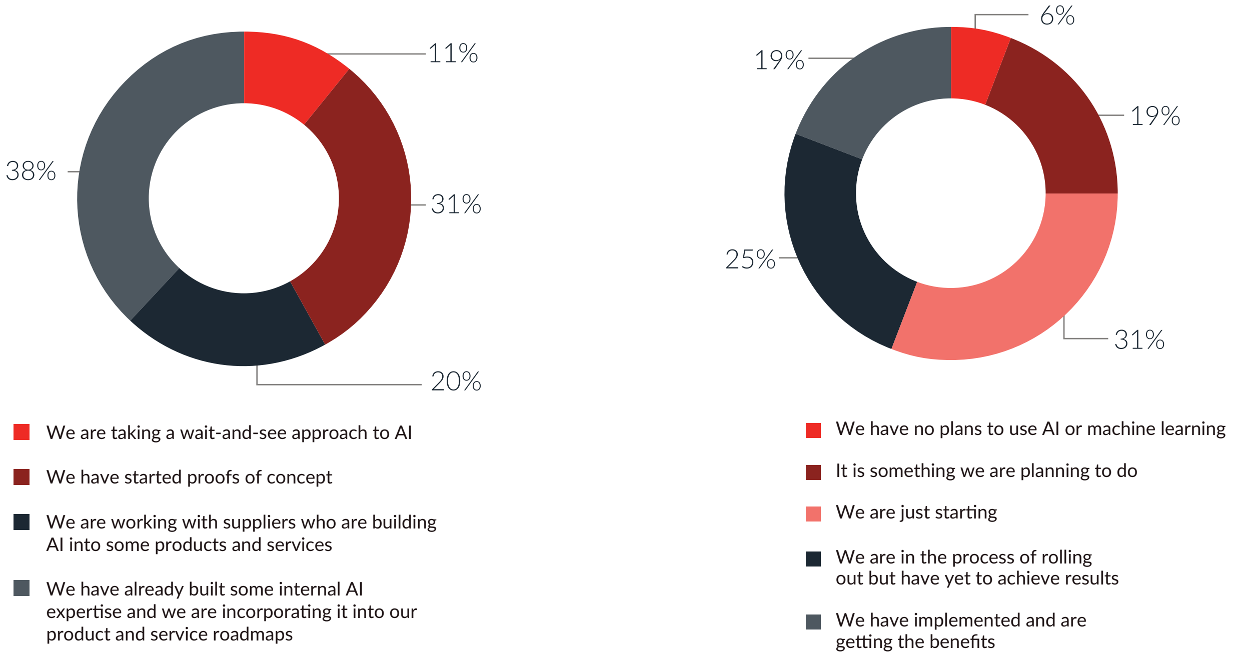
Some communications service providers (CSPs) are introducing security controls driven by artificial intelligence (AI) to protect their internal IT environments and sell as a service to enterprise customers, but they should also be committed to creating a security framework to protect the growing number of AI use cases in their businesses.

AI features in most operators' digital transformation roadmaps, often prominently. According to two recent TM Forum surveys, a large majority of CSPs are either deploying AI in some parts of the business or testing it in proofs of concept and trials (see graphic below, and for links to the survey reports, see page 27).

In terms of how AI is used in the security domain, machine learning algorithms have been working in the background in a wide variety of security products for many years. Many of the automated threat detection decisions made by web application firewalls and next-generation firewalls are already driven by machine learning algorithms.

Several new players have entered the market for endpoint protection, endpoint detection and response, and network traffic analysis (NTA) with products supporting unsupervised as well as supervised learning pitched as AI products. CSPs have been among the early adopters of these technologies, primarily in their internal enterprise environments rather than in their telecom infrastructure.

AI deployment gets underway



2018 AI survey reults

2019 CXO survey results

TM Forum, 2019

Lessons so far

There are four primary takeaways from the experiences of AI security early adopters:

AI security products can spot threats other security controls miss. For example, earlier this year Orange Polska stated that the NTA product it deployed in its network in the first quarter of 2018 has proven effective at detecting banking and crypto-jacking malware, internal data exfiltration and other high-risk threats that the company's other defenses missed.

AI alters the security operations model. Rather than rendering traditional binary decisions, AI security controls tend to be a lot more ambiguous (see panel opposite).

Vendor marketing is creating confusion around the value proposition of applying AI to cybersecurity. As Jaya Baloo, Chief Security Information Officer, KPN, notes, "It's still hard for me to poke through the marketing and find out what some of these products really do. Honestly, it can be hard to tell."

Learning how to work with AI in the cybersecurity context takes skill and time. Product selection needs to align with not only the use case and security objective the CSP wants to reach, but also the skill levels of the team that will be using it and the support level that vendors can provide.

Ambiguity is problematic in security operations

Traditional security controls tend to yield binary outcomes. Traffic is either allowed to pass through or it is blocked, for example. This has given rise to the problem of false positives and false negatives in security operations, where security controls make binary judgments, some of which (sometimes many of which) are wrong. Much as security operations teams see this as one of the banes of their existence, they find it difficult to adjust to the alternative model AI introduces.

Rather than being binary, the decisions or recommendations served up by AI security controls tend be a lot more ambiguous. For example, it may spot a threat in a split second which another algorithm wouldn't find and which a human would take weeks or months to identify. That's brilliant, except that the security team now must reach a decision on whether to trust the algorithm's recommendation.

The process of becoming familiar with AI-driven security tools and learning when to trust and when not to trust their findings is long, typically taking six to 12 months. Even those AI-driven security tools that have proven capable of delivering high-value detections within a short period of time still tend to deliver significantly higher value over time, borne of greater familiarity with how it works.

Linked to that is arriving at a level of confidence that's high enough to allow an AI algorithm's recommendation to be used as the basis for automating a response to it. For the most part, early adopters are still intervening manually to trigger responses to AI-driven security controls. Leadership in security requires being at the forefront of building the confidence to automate those responses.

Securing AI use cases

What is arguably even more important than using AI cybersecurity tools is ensuring that AI use cases implemented throughout the CSP's business are secure and do not introduce vulnerabilities. For example, this means making sure AI instances don't violate data governance rules.

"AI is more of a live puppy than a stuffed toy," says Rob Claxton, Chief Researcher, BT, who also leads TM Forum's collaborative work on AI.

Professor Steve Babbage, Distinguished Engineer, Security Research Manager and Chief Cryptographer, Vodafone, adds:

> "Human-defined limits are needed on what any AI system can do."

Standards are clearly needed in this area. One option could be standards that generate certification or labeling of AI algorithms assigning them a score that benchmarks the level of autonomy they're capable of.

Watch BT's Rob Claxton discuss the importance of AI management standards:

Open to attacks

Another issue is that while AI algorithms may differ from other types of algorithms in keys ways, what they share is vulnerability to being hacked. An attacker that breaches an AI algorithm and instructs it to make bogus decisions leading to harmful outcomes becomes a major security risk as CSPs deploy AI.

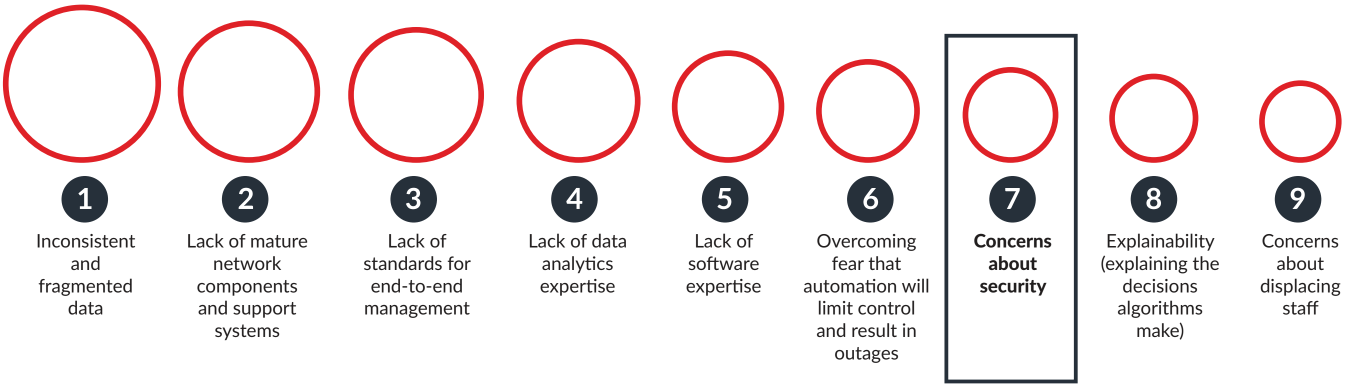
Poisoning attacks on training data can corrupt the learning process and the final trained model. Adversarial samples can be crafted to fool the AI and cause it to misclassify. New detection and repair methodologies can protect against this.

Security teams should also plan for algorithm diversity rather than relying too much on master AI algorithms. As shown by some of the results of TM Forum's 2018 AI survey, all these areas are receiving a lot less attention and investment than exploiting the upside of AI (see graphic below).

Regrettably, security is near the bottom of respondents' concerns. Protecting against the risks is just as important as adopting AI tools, and telcos need to be at the forefront of both.

The next section outlines concrete steps CSPs can take now to make security an imperative for digital transformation.

Ranking the challenges to deploying AIOps



TM Forum, 2018

Section 7

Make it happen – Strategies for improving cybersecurity

It's clear that digital transformation creates new information security risk for communications service providers (CSPs). As part of the transformation process, operators should undertake an end-to-end cybersecurity risk assessment and focus on protecting the integrity of data throughout the entire business. Here are some steps to take:

Be humble but bold

CSPs should recognize that their track record in security across their organizations is mixed rather than outstanding and that new security threats pose a real risk to their digital transformation goals. The security team needs to be positioned as a supplier of critical security services to internal customers, and internal customers should be incentivized to welcome their services. In addition, operators should look at their employees as being in the front line of security policy, not just as sources of vulnerability.

Build upwards from a solid foundation

CSPs should provide ongoing investment in a strong data governance framework as the foundation of their approach to information security. As well as hardening the organization's security stance, a strong framework is also key to ensuring the quality of the data available to realize digital transformation targets.

Drive security from DevSecOps

In the development environment, telcos should have a roadmap for incentivizing teams to embed security earlier and earlier in the development cycle by upskilling development and operations teams with security best practices. For some services, this should lead to security being on a par with functional design and performance right at the outset of the design process.

Think mitigation and automation

Whether it's application program interfaces, artificial intelligence or vendor software, importing these technologies into a CSP's environment carries clear risk as well as opportunity. Some of the fixes for this are mature, some maturing, some still quite immature. Leadership in security requires high levels of competence in mitigating these risks, and automation is the key to mitigating quickly.

Commit to security as a differentiator

Security is becoming an area where leading CSPs can distinguish themselves from competitors. Ambitious operators should invest in security as a differentiator, especially for 5G vertical industry use cases. Operators should target a highly automated and orchestrated security model comparable to that practiced by leaders in the airline industry.

Get involved in collaboration

Consider joining TM Forum's Collaboration Community to develop security best practices for the Open Digital Architecture. A security working group is exploring how to assess and contain cybersecurity risk by designing security and privacy into operational and business support systems. To learn more, please contact George Glass.

Taking a proactive approach to cybersecurity

A solid cyber-defense strategy is increasingly critical to the enterprise business. Each year, the volume of threats continues to climb, with some estimates indicating as many as 300,000 new types of malware being identified daily. Regulations too, such as GDPR are increasingly common. Security breaches as a result, can be devasting, leading to fines, negative publicity and stock price declines.

The threat landscape is both dynamic and complex. Attacks are becoming smarter and more persistent, with zero-day threats far more common. Meanwhile, agencies are attributing increasing numbers of attacks to rogue governments and well-funded organized crime gangs.

The overwhelming majority of today's cyber-security industry practices are reactive. Indeed, a VMWare study found this to be the case for 80% of enterprise IT security investments. This is also reflected in the venture capital industry, where the 2018 Cyber Defender Report indicated 72% of VC investments were awarded to security start-ups whose product and service focus is reactive.

While there is no replacement for a solid, reactive, cyber-security defense strategy that focuses on the core best practices of patch management, log monitoring, SIEM, SOC and so on, such an approach on its own is insufficient to mitigate the threat. A formidable defense can only be built by increasing investments in proactive cyber security, focusing on the "how" of preventing an attack rather than the amount of time it takes to do so. Examples of a proactive approach include analyzing the number of attempts thwarted by employees, improving application design and proactively repairing vulnerabilities. Crucially, with prevention far less costly than remediation, such a strategy can also greatly improve the bottom line.

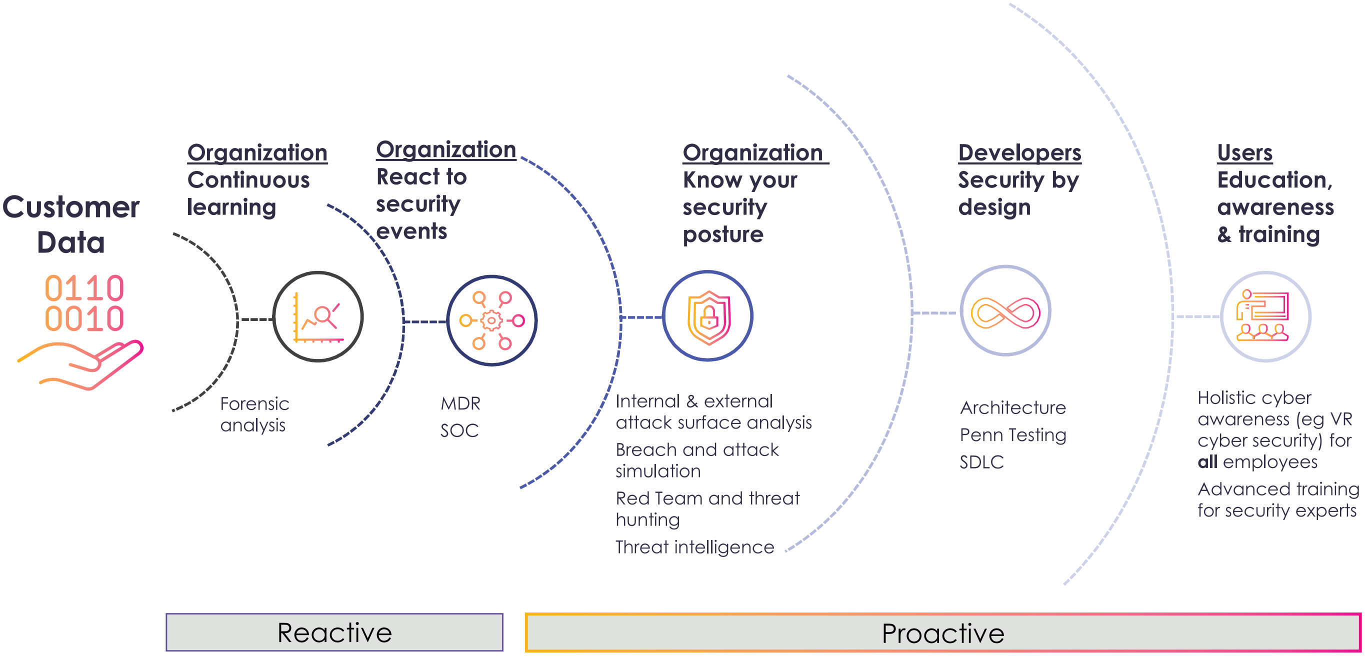
Lessons from the FIFA Women's World Cup 2019

Take football as an analogy. Every team positions their defense with the objective of defending their goal. While the goalkeeper role is critical, the more other players prevent the competing team from shooting for goal, the higher the chances of success.

The United States conceded only three goals in their seven matches on their path to winning the FIFA Women's World Cup winner's trophy. But what set them apart was the relatively low number of shots against their goal. This was attributed to their strong offense tactics and the ability of their defenders to keep the competing team's attackers at bay.

The same holds true for cyber-security. First, to minimize or prevent attacks via phishing scams and suspicious downloads, enterprises must raise awareness amongst their entire workforce of the risks. Second, they must ensure a solid defense is built into their applications, bolstered by the capability to detect attacks from the outset. Thirdly, they require a solid detect & response mechanism – the "goalkeeper" – in order to minimize the impact of any attack.

For these reasons, enterprises will be far better positioned to market themselves as a trusted partner if they can maintain a strong security posture as part of a more secure ecosystem. With this in mind, let's examine the main layers of a proactive security strategy:



Customer Data

0110
0010

Organization
Continuous learning

Forensic analysis

Organization
React to security events

MDR
SOC

Organization
Know your security posture

Internal & external attack surface analysis
Breach and attack simulation
Red Team and threat hunting
Threat intelligence

Developers
Security by design

Architecture
Penn Testing
SDLC

Users
Education, awareness & training

Holistic cyber awareness (eg VR cyber security) for **all** employees
Advanced training for security experts

Reactive

Proactive

It's all about awareness

Employees represent the front line. They need to know every email they receive and every website they visit can potentially damage your enterprise systems. Yet raising such awareness represents a significant challenge. One of these is overcoming human nature: Many emails contain malicious links that seem genuine, increasing the temptation to click. And despite the known security risks, employees may be tempted to use their private email for work purposes. However, raising awareness requires a creative approach that ensures employees pay attention to your security messages and act accordingly. Moreover, such efforts must also be ongoing, rather than an isolated campaign.

Best practice examples:

- Use innovative experiences such as VR and escape rooms to increase employee engagement.
- Continually drill employees with fake phishing exercises; post a running tally of how well the organization is performing and encourage employees to increase their alertness
- Hold cyber-awareness events at least annually
- Build awareness into employee onboarding

Security by design – a "shift-left" approach

Another key ingredient of a proactive approach is embedding security into enterprise applications. While many organizations suffice with building firewalls around their applications, if a cyber-criminal penetrates that firewall, there is no additional level of defense to protect the business. True application security demands measures to be built into every application, beginning from the very start of the development process, i.e. a "shift-left" approach. This increases the probability that any security vulnerability will be identified early on. It also enables the issue to be remediated before the application goes into production, thereby saving time and money, while ensuring the application has a more solid security foundation.

Know your security posture

The breadth and depth of enterprises' attack surface has grown significantly over the past several years. Whereas it was once sufficient to be aware of all the assets you owned, organizations now must also contend with:

- Employees using unsecured connections in airports, coffee shops, etc.
- Cloud-based applications that connect into their ecosystem
- IoT devices, which are often poorly protected
- Partner ecosystems that connect to their network

To plan the design of security systems and understand where vulnerabilities lie, it is therefore critical to understand the nature of every possible entry point into the enterprise ecosystem.

Practice! Practice! Practice!

For security professionals on the enterprise team, practice is key. Simulating cyber-attacks provides training to identify issues faster, defend enterprise assets – all while continuing to ensure seamless customer operations.

Such training can take place in many ways, for example:

- Red team and threat hunting: a "red" team is assigned to try penetrating the enterprise system or an application, looking for soft spots in the defense. This helps identify vulnerabilities in the ecosystem, enabling defense mechanisms to be strengthened before they can be compromised.
- Simulated attacks: use technology and people to carry out simulated attacks across the organization and across the kill chain, from probing for weaknesses to lateral movement once inside the network. This helps security experts learn how to identify breaches while they're still in progress and devise the best methods and procedures to eliminate the threat.

Security employees should also be trained on the latest technologies to keep them current and motivated. This holds even more true, as according to (ISC)2 , there is currently a global shortage of skilled cyber-security employees, with nearly 3 million unfilled positions in the workforce worldwide.

Continuous learning drives improvement

When an attack occurs, it's important to harness the opportunity to learn from experience and improve the overall process. This includes performing a post-mortem, analyzing what happened and drawing conclusions on how to ensure similar attacks do not recur.

Leading by example

Amdocs, a leading vendor of solutions for communication services providers, provides a full suite of cyber-security solutions for enterprises of all sizes, while partnering with leading solution providers across the industry. Our focus is primarily proactive, ensuring enterprises can avoid attacks, while minimizing the impact of any attack that does occur.

In addition, we provide a full array of detection and remediation solutions, as well as forensic analysis capabilities, complemented by our state-of-the art security operations center, enabling us to identify, isolate and remediate the root cause of issues, minimize their impact and drive continuous improvement.

About Amdocs

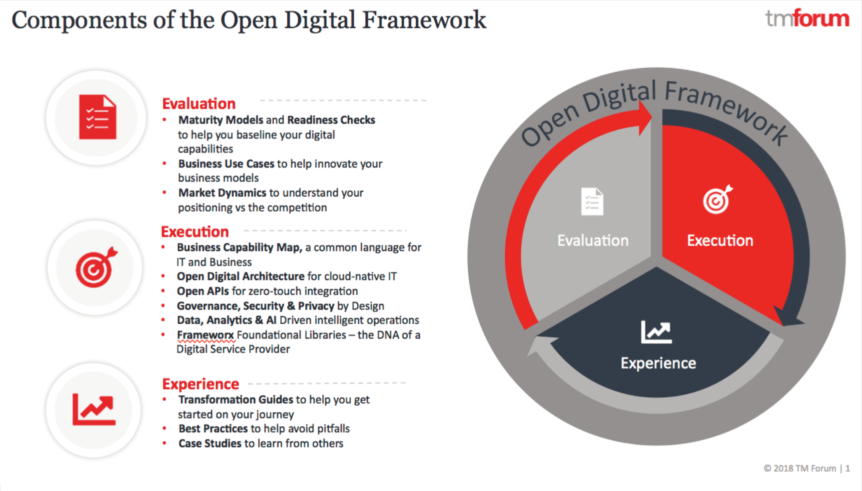
Amdocs is a leading software and services provider to communications and media companies of all sizes, accelerating the industry's dynamic and continuous digital transformation. With a rich set of innovative solutions, long-term business relationships with 350 communications and media providers, and technology and distribution ties to 600 content creators, Amdocs delivers business improvements to drive growth.

Amdocs and its 25,000 employees serve customers in over 85 countries. Listed on the NASDAQ Global Select Market, Amdocs had revenue of $4.0 billion in fiscal 2018.

For more information, visit Amdocs at **www.amdocs.com**

TM Forum Open Digital Framework

Delivering the tools to go from concept to cash in just 18 days



Components of the Open Digital Framework

tmforum

Evaluation

- **Maturity Models** and **Readiness Checks** to help you baseline your digital capabilities
- **Business Use Cases** to help innovate your business models
- **Market Dynamics** to understand your positioning vs the competition

Execution

- **Business Capability Map,** a common language for IT and Business
- **Open Digital Architecture** for cloud-native IT
- **Open APIs** for zero-touch integration
- **Governance, Security & Privacy** by Design
- **Data, Analytics & AI** Driven intelligent operations
- **Frameworx** Foundational Libraries – the DNA of a Digital Service Provider

Experience

- **Transformation Guides** to help you get started on your journey
- **Best Practices** to help avoid pitfalls
- **Case Studies** to learn from others

© 2018 TM Forum | 1

The TM Forum Open Digital Framework is an interactive, continuously evolving collection of tools, knowledge and standards that give communications service providers (CSPs) an end-to-end migration path from legacy systems to modular, cloud-native IT components. Simply put, it is a blueprint for service providers to deliver intelligent operations fit for the 5G era.

A prototype version of the framework is available now for TM Forum members to explore. It is being developed through the TM Forum Collaboration Program and Catalyst Program, and builds on the success of the Forum's established Open APIs and the Frameworx suite of standards. Specifically, it includes:

- **Open Digital Architecture (ODA)** – an enterprise architecture blueprint, common language and key design principles for modular, cloud-based, open digital platforms that can be orchestrated using AI
- **Open APIs** – 50+ standardized REST-based APIs to facilitate zero-touch integration and zero-touch partnering
- **Data & AI standards** – an industry-agreed data model, together with standards maximizing the potential of AI to enhance customer experience and increase operational efficiency
- **Reference implementations** – a framework for assembling and validating ODA components in the Forum's Open Digital Lab, fostering the creation of a services marketplace
- **Practical guidance** – guides and videos showing how the Open Digital Framework can be used to transform the core business and enable new business growth
- **Foundational libraries** – normalized models providing a common language for business processes and information that simplifies and de-risks transformation projects

The goal of the Open Digital Framework is to help service providers increase agility and drastically reduce the development cycle for products and services from 18 months to 18 days. Much of the collaborative work that is part of the framework is already available, but it helps to organize it and make it more accessible. The framework is a work in progress and will improve through crowdsourcing.

If you would like to learn more about the project or how to get involved in the TM Forum Collaboration Community, please contact Andy Tiller.

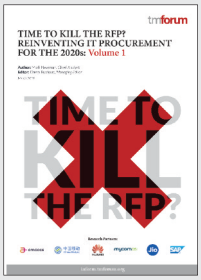
tmforum

TM Forum research reports

tmforum

CTIO OUTLOOK 2020: TRANSFORMING OPERATIONS TO MONETIZE 5G

inform.tmforum.org


tmforum

TIME TO KILL THE RFP? REINVENTING IT PROCUREMENT FOR THE 2020s: Volume 1

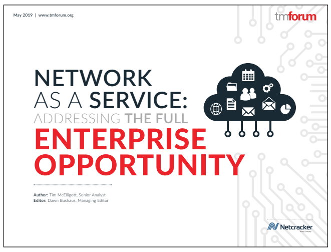
inform.tmforum.org

May 2019 | www.tmforum.org

tmforum

BLOCKCHAIN: WHERE'S THE VALUE FOR TELECOMS?

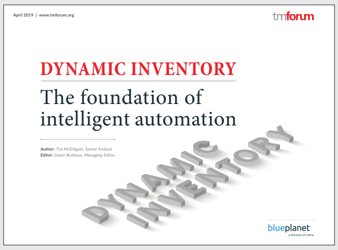
accenture


May 2019 | www.tmforum.org

tmforum

NETWORK AS A SERVICE: ADDRESSING THE FULL ENTERPRISE OPPORTUNITY

Netcracker


April 2019 | www.tmforum.org

tmforum

DYNAMIC INVENTORY

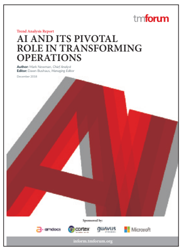
The foundation of intelligent automation

blueplanet

tmforum

5G: EVOLUTION AND REVOLUTION

inform.tmforum.org


tmforum

AI AND ITS PIVOTAL ROLE IN TRANSFORMING OPERATIONS

inform.tmforum.org

tmforum

REDEFINING THE CTIO

ESSENTIALS FOR THE DIGITAL AGE

inform.tmforum.org

Digital Transformation Tracker 3:

WHY IS NETWORK TRANSFORMATION SO DIFFICULT?

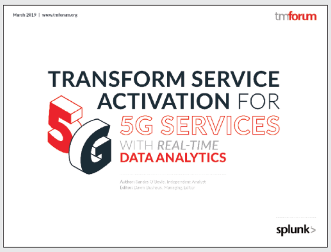
tmforum

5G MONETIZATION: OPERATIONAL IMPERATIVES

Author: Catherine Haslam, Senior Analyst

Editor: Dawn Bushaus, Managing Editor

July 2018


March 2019 | www.tmforum.org

tmforum

TRANSFORM SERVICE ACTIVATION FOR 5G SERVICES WITH REAL-TIME DATA ANALYTICS

splunk>

April 2019 | www.tmforum.org

tmforum

CUSTOMERS AS INDIVIDUALS: USING IDENTITY TO IMPROVE EXPERIENCE

amdocs

TM FORUM QUICK INSIGHTS REPORT

tmforum

AI & CUSTOMER EXPERIENCE: EMERGING BEST PRACTICES

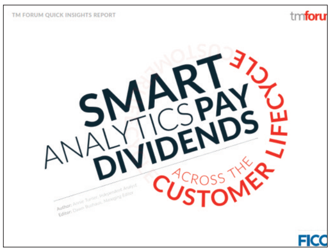
NUANCE

TM FORUM QUICK INSIGHTS REPORT

tmforum

WANT TO DRIVE BUSINESS BENEFITS? IMPROVE CUSTOMER EXPERIENCE

Mahindra


TM FORUM QUICK INSIGHTS REPORT

tmforum

SMART ANALYTICS PAY DIVIDENDS ACROSS THE CUSTOMER LIFECYCLE

FICO

Meet the Research & Media team

Report Author:
Patrick Donegan
Principal Analyst,
HardenStance Ltd
patrick.donegan@hardenstance.com

Chief Analyst:
Mark Newman
mnewman@tmforum.org

Senior Analyst:
Tim McElligott
tmcelligott@tmforum.org

Customer Success & Operations Manager:
Ali Groves
agroves@tmforum.org

Global Account Director:
Carine Vandevelde
cvandevelde@tmforum.org

Report Editor:
Dawn Bushaus
Managing Editor
dbushaus@tmforum.org

Editor, Digital Content:
Arti Mehta
amehta@tmforum.org

Commercial Manager, Research & Media:
Tim Edwards
tedwards@tmforum.org

Chief Marketing Officer:
Paul Wilson
pwilson@tmforum.org

Vice President of Marketing:
Charlotte Lewis
clewis@tmforum.org

Advisors:
George Glass,
VP, Architecture & APIs
wgglass@tmforum.org

Dave Milham,
Chief Architect, Service Provider Engagement
dmilham@tmforum.org

Report Design:
Intuitive Design UK Ltd
info@intuitive-design.co.uk

Published by:
TM Forum
4 Century Drive,
Parsippany,
NJ 07054
USA
www.tmforum.org
Phone: +1 973-944-5100
Fax: +1 973-944-5110
ISBN: 978-1-945220-56-2

The Forum would like to thank the sponsors and advertisers who have enabled the publication of this fully independently researched report. The views and opinions expressed by individual authors and contributors in this publication are provided in the writers' personal capacities and are their sole responsibility. Their publication does not imply that they represent the views or opinions of TM Forum and must neither be regarded as constituting advice on any matter whatsoever, nor be interpreted as such. The reproduction of advertisements and sponsored features in this publication does not in any way imply endorsement by TM Forum of products or services referred to therein.

For more about TM Forum’s Collaboration Community,
please contact **Andy Tiller**