September 2023 | www.tmforum.org

tmforum knowledge

REPORT

Cybersecurity strategies:

risk management moves firmly into the telco spotlight

Author: Patrick Donegan, Principal Analyst, HardenStance
Editor: Dawn Bushaus, Contributing Editor, TM Forum

sponsored by:

NOKIA

contents

03 the big picture

07 section 1: threat intelligence-led risk management is driving security strategy

12 section 2: risk management responsibilities are driving change in the CISO's role

17 section 3: better visibility and use of threat intel drives spending on new tools

24 section 4: make it happen – strategies for optimizing cyber risk management

27 additional resources

We hope you enjoy the report and, most importantly, find ways to use the ideas, concepts and recommendations detailed within. You can send your feedback to the editorial team at TM Forum via editor@tmforum.org


the big picture

A new TM Forum survey yields critical insights into how communications service providers (CSPs) around the world are evolving their cybersecurity posture for the challenges of an evolving cyber threat ecosystem, more prescriptive government regulations, and the risks that accompany the shift to cloud operating models.

In June 2023, TM Forum carried out an online survey of CSPs about how they are formulating cybersecurity strategy and putting it into effect. This report draws on insights from 59 individuals from 40 unique operating companies around the world. Nearly all respondents were at director level and above, with significant knowledge of their company's approach to cybersecurity.

As well as our survey, interviews were carried out among executive-level decision-makers to gauge sentiment in the industry.

All sectors of industry are grappling with heightened risks to their business operations. Cybersecurity risk is just one, alongside climate change, geopolitical risk, AI risk and the possibility of another pandemic. Our survey paints a picture of the approach CSPs are taking to protect their organizations and their customers against cybersecurity risk.

Cybersecurity is evolving from a highly technical discipline to one that is focused on managing broader business risk. Once the preserve of a small team of technical experts, cybersecurity is evolving to require organization-wide engagement by all stakeholders – from the board room down to every individual employee. It's also evolving toward rapidly detecting and mitigating the subset of threats that will inevitably get past protective defenses rather than counting on those defenses to keep them all out.

As one among an elite group of industries that are defined as critical infrastructure, the telecoms sector has some unique attributes that affect how CSPs determine their target cybersecurity posture. Telco networks are the nervous system of the digital economy. In addition, CSPs are more impacted than most sectors by cyber threats arising from growing geopolitical tensions, whether those threats take the form of adversaries spying on customers' communications or other malicious activities.

For these two reasons CSPs are also more susceptible than most – including most other critical industries – to more stringent cybersecurity regulation. Operators also face unique technology-related risk in cybersecurity as they undertake the disruptive migration of old and new network services, and old and new networking protocols, to less familiar cloud-native architectures.

Cybersecurity is evolving from a highly technical discipline to one that is focused on managing broader business risk.

Frameworks, roles and spending

This report explores several key aspects of the goals and supporting frameworks that are driving cybersecurity. Because CSPs are regulated entities, cybersecurity is inevitably driven in part by regulatory compliance. That, however, should typically be viewed as no more than a bare minimum baseline. Hence our survey sought to understand where compliance fits as a factor and which other frameworks, metrics or other considerations – if any – are being used to augment or exceed basic compliance requirements.

We also look at the roles of individual leaders and other stakeholders within the CSP organization in terms of formulating and executing on cybersecurity strategy, including identifying spending priorities. The survey sheds light on which individual leaders tend to call the shots as well as the interdependencies between stakeholders.

Key to this is understanding the role of the chief information security officer (CISO) or chief security officer (CSO). As the cybersecurity discipline has evolved, these roles have evolved with it. The survey looks at how the role of telco CISOs and CSOs has changed in the last 18 months and explores what is driving those changes in the context of an environment where cybersecurity spans the unique operations environment of a telco network as well as a more generic enterprise IT environment.

Cybersecurity risks for CSPs

CSPS ARE **VULNERABLE TO ATTACKS** AGAINST ENTERPRISE IT, NETWORK INFRASTRUCTURE AND OPERATIONS

RISK TO TELECOMS SERVICES FROM NATION STATE CYBER THREAT ACTORS IS INCREASING WITH HEIGHTENED TENSIONS AMONG KEY GEOPOLITICAL ADVERSARIES SUCH AS THE US, THE EU, RUSSIA, CHINA AND IRAN

AS WITH ANY MAJOR CHANGE IN ARCHITECTURE OR OPERATIONAL PRACTICE, **THE MOVE TO CLOUD ARCHITECTURES INTRODUCES NEW** CYBERSECURITY **RISK**

RAPID INNOVATION IN THE CYBER THREAT ECOSYSTEM DEMANDS AN APPROACH TO CYBERSECURITY THAT IS AGILE, OPTIMIZED FOR REDUCING RISK THROUGHOUT THE ORGANIZATION AND TAILORED TO MINIMIZING HARM WHEN ATTACKS GET THROUGH

AS PROVIDERS OF CRITICAL INFRASTRUCTURE CENTRAL TO THE FUNCTIONING OF THE DIGITAL ECONOMY, **GOVERNMENTS ARE IMPOSING STRINGENT NEW REGULATIONS** PRESCRIBING HOW CSPS MUST MANAGE THEIR CYBERSECURITY POSTURE

TM Forum, 2023

We look at how spending on cybersecurity tooling is being prioritized in the context of budget constraints, and which features and value propositions are most likely to help distinguish security tools as critical rather than just "nice to have". The scope extends to the balance between spending on protective or defensive tools on one hand, and detection and response tooling on the other.

We also discuss hot-button value propositions from the different perspectives of security analysts investigating incidents and security engineers responsible for building, operating and maintaining the CSP's security operations center (SOC) infrastructure. Finally, we examine the adoption of software-as-a-service (SaaS) in the context of telco security operation.

Read this report to understand:

- What's driving cybersecurity strategy in CSPs
- What cyber risk management is and why CSPs are adopting it
- Why the role of the telco CISO is changing to a more business-oriented focus throughout the telco organization, spanning both enterprise IT and network domains
- Rates of adoption of SaaS in CSPs' SOCs
- The types of cybersecurity tooling that CSPs are prioritizing for investment – and why.

The role of the telco security officer is changing to span both enterprise IT and network domains.

section 1

threat intelligence-led risk management is driving security strategy

Cybersecurity strategy is influenced by many competing factors, claims, considerations and requirements from outside as well as within the telco organization. But which ones carry the most weight and why?

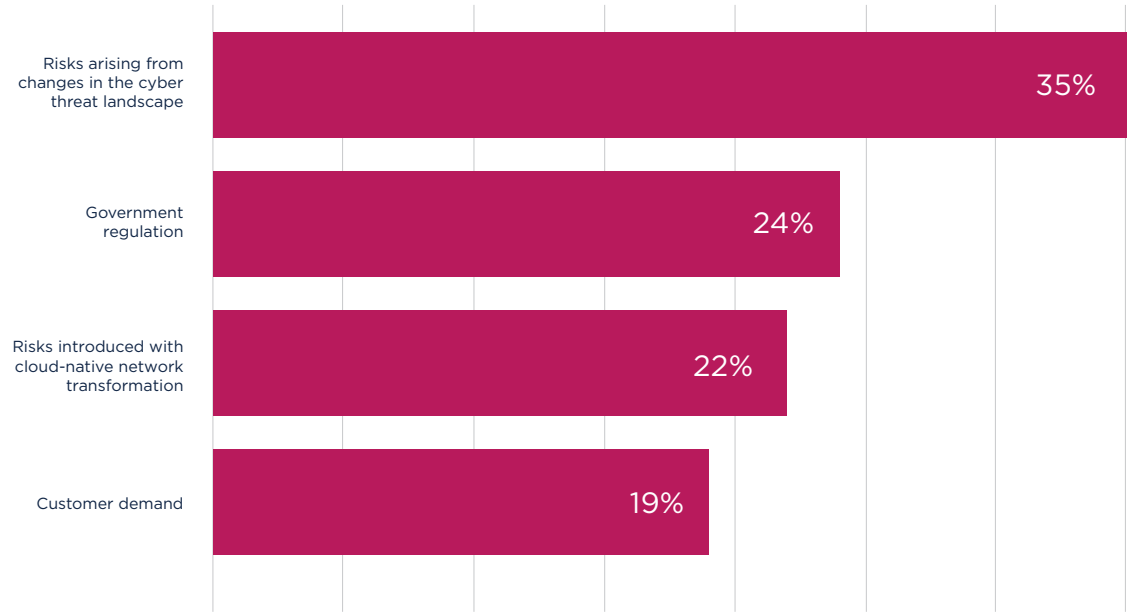
We asked CSP respondents to rank the most important factors driving telco cybersecurity strategy. As shown in the graphic, the most critical by far is understanding and mitigating risk arising from the cyber threat landscape.

It scored 3.5 out of 4.0, with about two thirds of respondents ranking it as their top choice. This reflects the threat posed by change and innovation in the cyber threat ecosystem. It also reflects the importance of an organization being able to rapidly interpret change in terms of risk for the organization – and then adapt to it.

Government regulation is also a significant driver, but only 17% of respondents ranked it as the number-one factor. On one hand this suggests that while compliance with cybersecurity regulations is recognized as critical and non-negotiable, traditional 'tick-box' compliance is no more than a minimum baseline for defining telco security strategy.

That said, the much lower score may also imply that most CSPs are not yet feeling the full force of the new wave of cybersecurity regulations set to impact them. Many of these go well beyond tick-box compliance relating to specific products, features or certifications. New regulations are prescribing increasingly detailed processes for how telcos should execute on a wide range of cybersecurity issues.

Most important factors driving CSPs' security strategy



TM Forum, 2023

In many cases, these are processes that regulators have previously addressed with a light touch or not addressed at all, such as more detailed and more stringent requirements relating to incident detection, management, mitigation and reporting in CSPs' SOCs (see sidebar).

Customer demand doesn't score highly as a driver of telco security strategy because the primary objective is to protect the CSP organization itself – protecting customers is just one aspect of that. Responses to our survey question about security spending reinforce this (see graphic on page 10).

From the perspective of a security team, the 'customer' is typically an internal business unit rather than the end customer. However the customer is defined, most just want to buy secure services. Most customers tend not to be very involved in prescribing how they are secured. So, while customers are central to telco security strategy, they're generally not all that active in directly driving it.

Risk management is key

One of the most significant survey findings is illustrated in the graphic on the next page, which identifies risk management as the most important factor determining how telco cybersecurity spending is prioritized. More than 60% of respondents identified risk management as one of the two most important factors compared with half who chose regulatory compliance.

Stricter government regulation is a rising global trend

The following examples illustrate the regulatory wave that is building globally but has yet to fully break in many countries. Estonia and Germany implemented the EU's European Electronic Communications Code (EECC) into national law in 2018 and 2020, respectively. However, Ireland didn't implement it until 2023. The EU's Network and Information Services Directive (NIS2) impacts telcos among other critical industry sectors but doesn't have to be implemented in national law until October 2024.

The UK's Telecommunications Security Act – the most prescriptive new legislation to come into effect, allowing for fines of up to 10% of revenues to be imposed for non-compliance – came into force at the end of 2021. Paul MacKenzie, Head of Security for Hyperoptic, a leading internet service provider (ISP) or altnet in the UK, says of the Telecommunications Security Act: "There are few areas of our operations that are untouched by this legislation."

In the US, the Federal Communications Commission (FCC) has proposed more stringent requirements for how telcos report data breaches. The Notice of Proposed Rule Making issued in December 2022 seeks to eliminate a mandatory waiting period for notifying customers of a breach, requires that customers be notified of inadvertent breaches and requires operators to notify the Commission, the FBI and the Secret Service of all reportable breaches. The FCC is soliciting comments on the proposal.

Advanced markets may be leading on this, but other countries are also following suit. "In Thailand we have a Cybersecurity Act applicable to all critical infrastructure," says Pepijn Kok, CISO for AIS in Thailand. "The regulator started with the banks, now we are the second industry they are turning their attention to. As part of this new process, for the first time at the start of this year, we've had to submit an internal audit report and risk assessment. Now they are planning to circle back and do a deep dive into our infrastructure."

Most important factors in prioritizing security spending

TM Forum, 2023

An approach driven by risk management denotes a more advanced cybersecurity posture than one that is more compliance driven. Cyber risk management typically forms part of a broader risk management strategy for managing legal, commercial and other types of business risk. Risk management does, nevertheless, overlap with compliance because risk management strategies take account of risk associated with non-compliance.

Crucially, risk management relies on quantifying risk. At a high level, a potential cybersecurity incident that is assessed as having an estimated cost of $100 million, with a 40% chance of happening in any one year, is considered a $40 million-a-year risk. It's because these types of assessments require such a detailed understanding of one's own risk exposure and cybersecurity posture – and because such quantifications can generate alarmingly high numbers – that embracing cyber risk management implies a relatively high level of cybersecurity maturity.

Cyber risk management is being explicitly incorporated into some of the new wave of cybersecurity regulations. For example, the EU's NIS2 Directive specifies that "a culture of risk management, involving risk assessments and the implementation of cybersecurity risk management measures appropriate to the risks faced, should be promoted and developed".

Such a high profile for cyber risk management in telco security circles is to be expected. That said, it's important to recognize that embracing it is a journey; it can be adopted in phases.

For example, cyber risk management can be factored into some decisions or all decisions. It can be no more than one factor in decision-making, or it can lead decision-making. Hence the high score in the survey doesn't necessarily mean a large proportion of CSPs are already at an advanced stage of using cyber risk management as of today.

Embracing cyber risk management implies a relatively high level of cybersecurity maturity.

At 51%, regulatory compliance isn't that far behind risk management. This reinforces how traditional compliance remains a key factor determining how security spending is prioritized. While compliance is increasingly subordinate to cyber risk management, some telcos may still be more heavily influenced by traditional compliance.

Risk introduced with cloud-native network transformation is likely to increase in importance as CSPs move more support systems applications and network functions to the cloud. The scope for hackers to break out of a Kubernetes container to compromise other containers or the underlying infrastructure is just one example. As Anil Pawar, SVP and Head of Technology, Architecture and Strategy, Rakuten Mobile, puts it: "Cloud native is small decomposed microservices in a software-driven architecture, so security became a huge, huge challenge for us."

Who calls the shots?

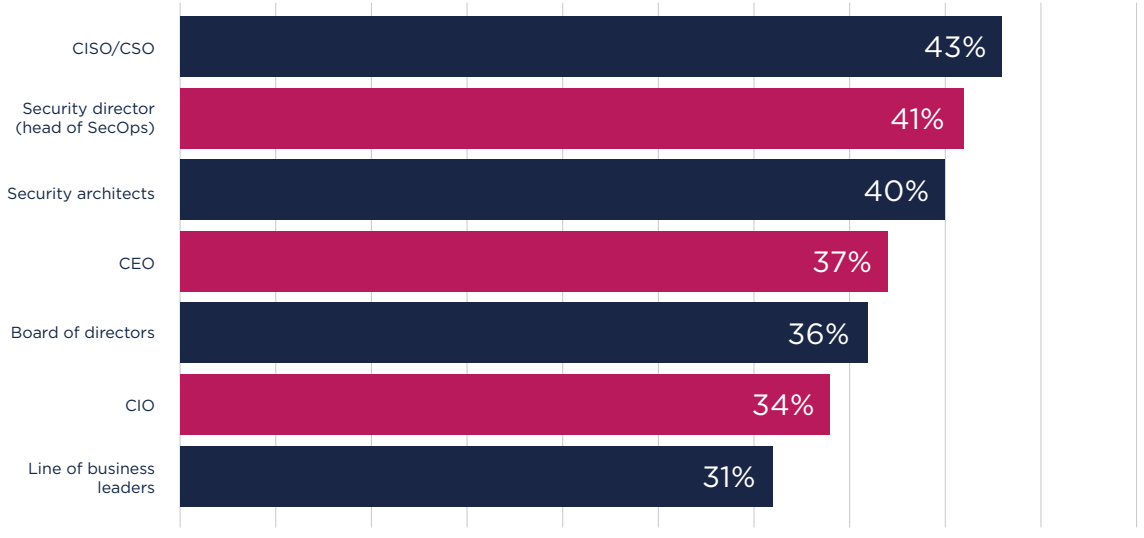
In common with all businesses that are dependent on large investments in operations technology, several stakeholders have input into a telco's cybersecurity strategy. The weighting of the influence that each has on a scale of 1 to 5, where 1 is little influence and 5 is a lot, is depicted in the graphic opposite.

Predictably, survey respondents identified the chief security officer (CSO) or chief information security officer (CISO) as holding the most influence over how telco cybersecurity requirements are prioritized, with 56% of respondents rating their influence a 5.

Respondents rated security directors and security architects as exerting greater influence over security requirements than the CEO or board of directors. In many cases, this delta probably does not reflect the relative influence of these stakeholders in terms of prioritization of spending. In some cases, it may reflect respondents addressing prioritization of technical requirements from among competing approaches for executing on priority objectives.

The next section explores how the role of the CISO or CSO has changed and continues to evolve, as well as the role of other stakeholders.

Who influences prioritization of cybersecurity requirements most?



TM Forum, 2023

section 2

risk management responsibilities are driving change in the CISO's role

Across all sectors of industry, the CISO's role has had to evolve at pace to keep up with cybersecurity risk. Here's how those changes are playing out in the context of the telecoms sector and how telco CISOs are going about protecting their organizations and their customers.

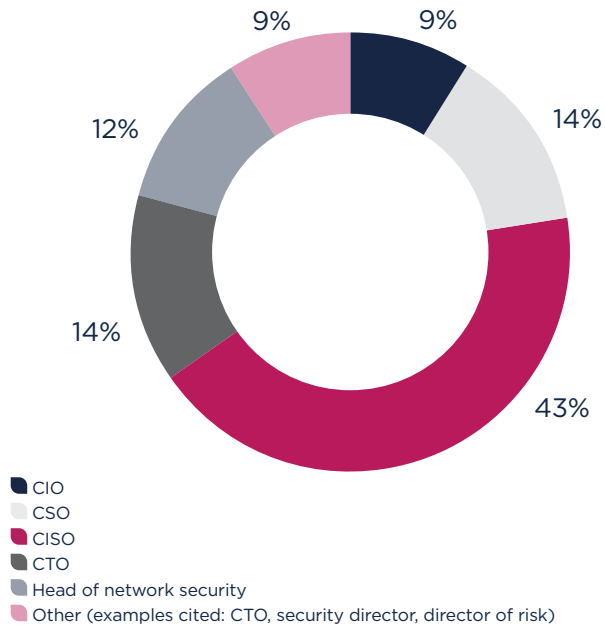
A full 71% of respondents to our survey said their organization has a single CISO or CSO across both enterprise IT and network domains. To give a few specific examples, the CISOs of Telefónica, KPN and Telus all have responsibility across both domains today.

Speaking at HardenStance's Telecom Threat Intelligence Summit in June 2023, David Rogers, Chair of GSMA's Fraud and Security Group (FASG), reaffirmed that "CISOs are now becoming responsible for cybersecurity covering all of the IT and telco network security." Only 29% of survey respondents said different individuals are still responsible for the security of each domain.

This convergence has gathered pace in recent years. In some cases, it has happened at the level of both a formal job description and in day-to-day practice. In others, the CISO that presides over both domains is less hands-on with the network than they are with enterprise IT.

This reality is implied in answers to our survey question asking which individual is responsible for the cybersecurity of the telco organization's public telecoms network assets (see graphic opposite).

Who's responsible for cybersecurity of public network assets?



TM Forum, 2023

Closer look at network security

Going back several years, the starting point in the evolution of the telco CISO's role was a focus on enterprise IT security. The security of the telecoms network tended to be largely separate, hence assigned to the CTO and/or one or more in their team.

There were good reasons for this bifurcation. Since employees have a legitimate need for direct access to internal operational systems and sensitive corporate data, misbehavior by them, whether benign or malicious, is a bigger cybersecurity risk to CSPs than customers. Hence a CISO was expected to focus on the CSP's internal enterprise network. In addition, the enterprise IT and telecoms technology environments were fundamentally different. Most CISOs knew more about enterprise IT than telecoms technology.

Several factors are extending the CISO's responsibilities further into the telco network domain. Perhaps the most important is broader and ongoing changes in the CISO role (see graphic on page 15). This is evolving away from a narrow technical focus on trying to prevent attacks from breaching IT systems to a broader one that is more focused on high-level business requirements and minimizing harm once preventive defenses are breached (as they inevitably will be).

These factors are forcing telco CISOs to engage more extensively throughout the organization. This requires greater engagement up and down the organizational hierarchy – from the board and senior leadership team at the top to the lowest rank of employees at the bottom (as well as third-party contractors and supply chain partners at any point in between). It also requires greater engagement across the organization's many units, departments and domains including CSPs' enterprise IT and network domains.

The convergence of all the telco organization's security under a single CISO is also being driven by convergence throughout the telecoms security landscape:

As shown with network functions virtualization (NFV) and cloud-native 5G standards, telecoms technologies, architectures and protocols increasingly are borrowing from the IT world. Telco CISOs with an IT background are therefore starting to find telecoms security challenges more familiar than in the past.

Whether they're financially motivated criminal gangs, politically motivated hacktivists or nation state threat groups focused on disinformation, espionage or disruption of services, some cyber threat actors are dynamically adjusting their motives and business models as well as intersecting, allying and converging with one another. A threat group targeting a telco's IT may change its goals and its supporting tactics, techniques and procedures to target network operations next time. And just as borrowing from the IT world makes defending telecoms networks more accessible to CISOs, it also makes them more accessible to cyber threat actors.

The CISO role is evolving from a narrow technical focus to broader high-level business requirements.

Many aspects of telcos' cybersecurity best practices are converging too. Many advanced telcos such as Deutsche Telekom, KPN and Telefónica have already converged their internal IT, network and SOCs into a general or unified SOC. Tunisie Telecom will converge its three separate SOCs under a single general SOC by the end of 2023.

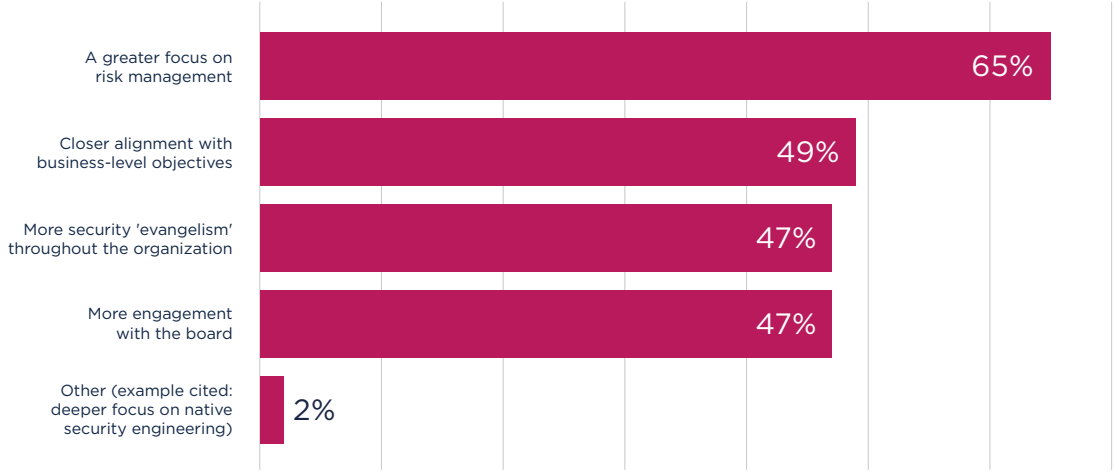
Expanding incrementally

Just as cyber risk management can be adopted in phases, the same is true of extending a CISO's responsibilities into the telco network domain. Take the example of a radio access network (RAN) or transport network upgrade. Upon taking responsibility for telecoms security – and then for a period of time after – a CISO may expect no more than to start signing off on the exact same long-standing security requirements that were previously signed off on by, say, the CTO.

Our survey may capture this nuance, where only 57% of respondents point to the CSO or CISO as responsible for cybersecurity of the network. This appears inconsistent with the 71% who said those roles handle both enterprise IT and network cybersecurity. The journey some telco CISOs are on in terms of assuming responsibility for the network incrementally may explain this slight discrepancy.

The survey asked respondents to choose the two most important ways the role of CISO has changed in the last 18 months. Most strikingly, and strongly echoing the survey's findings about the drivers for cybersecurity, 65% of respondents pointed to a greater focus on risk management (see graphic above right).

How has CISO/CSO role changed in past 18 months?



TM Forum, 2023

Clearly, CISOs are aligning with the organization's focus on cyber risk management or driving this change themselves (or both).

The other response options also scored highly – chosen by just under half of all respondents. Closer alignment with business-level objectives continues to be important – moving away from making technology-driven decisions to decision-making that's driven by minimizing harm to the business. More stringent regulation, such as new incident reporting rules, increases accountability on the part of the board. That's driving a tendency to forego passively delegating cybersecurity decisions to the CISO, as in the past, in favor of engaging more directly and more often.

CISOs need to be chief security evangelists

Increasing demands are also being placed on the CISO to serve as the lead cybersecurity evangelist throughout the telco organization. The role has long ceased to be confined to leading a team of cybersecurity specialists. It increasingly requires engaging all the organization's stakeholders in aligning with the principle of cybersecurity being "a team sport". As an example, the CISO team should be training and supporting cybersecurity 'champions' within different teams and departments so as to embed security awareness and best practice throughout the telco organization.

Independent of how it is created, who leads it and which guiding frameworks it uses, cybersecurity strategy always comprises a combination of people, processes and technology.

The next section looks at key criteria that tend to determine prioritization of spending on new cybersecurity tools.

Cybersecurity strategy always comprises a combination of people, processes and technology.

section 3

better visibility and use of threat intel drives spending on new tools

Within their cybersecurity budgets, telcos must prioritize tools for spending. Survey responses yielded valuable insights into what makes investment in new cybersecurity hardware, software and services critical versus merely "nice to have".

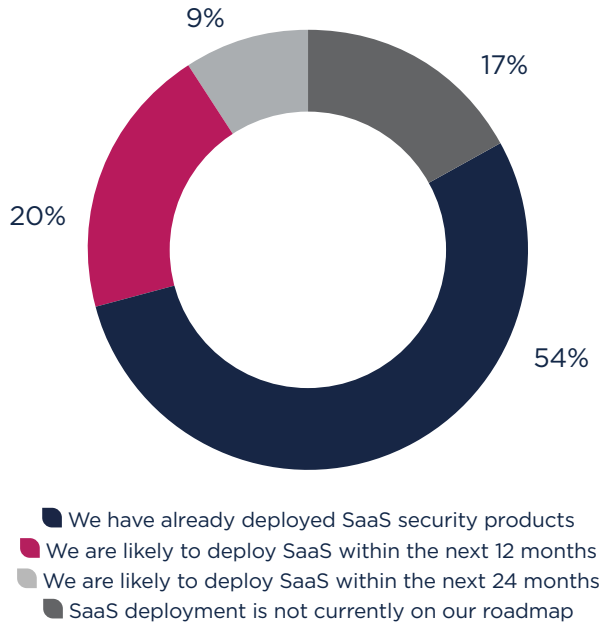
Whether it's in IT or on the network side of the house, SaaS tools represent both opportunity and risk for CSPs. Just over half of survey respondents say SaaS is already being used in their organization's security operations.

One obvious example is endpoint security software which is often delivered using a SaaS model. Some telcos also include SaaS in the mix of the DDoS (distributed denial of service) protection software they use. Among those that have yet to deploy SaaS in security operations around two thirds intend to over the next two years. Only 17% of respondents say SaaS deployment is not on their organization's roadmap for security operations.

The graphic on p.19 points to the main drivers of SaaS adoption. Almost two thirds of respondents believe it's business agility. With SaaS, CSPs no longer need to make a significant upfront investment; rather they can 'fail fast' without incurring significant losses. They can also scale investment up or down according to demand rather than having to invest up front for peak expected capacity.

Higher security efficacy emerges as joint second among drivers for SaaS adoption, chosen by 44% of respondents. This suggests that while some security

CSPs' use of SaaS tools in security operations



TM Forum, 2023

concerns about placing additional trust in third-party vendors using a SaaS model are still in play, CSPs remain aware of the inherent risk in traditional procurement models.

Spending priorities

At a simplified level, any organization's cybersecurity can be viewed in terms of two domains. The first is where cyber risk is defined and protections are put in place to prevent breaches from happening. The second is where breaches get past those initial protections, hence where threat detection and response measures are needed to minimize damage and allow for a rapid and robust recovery.

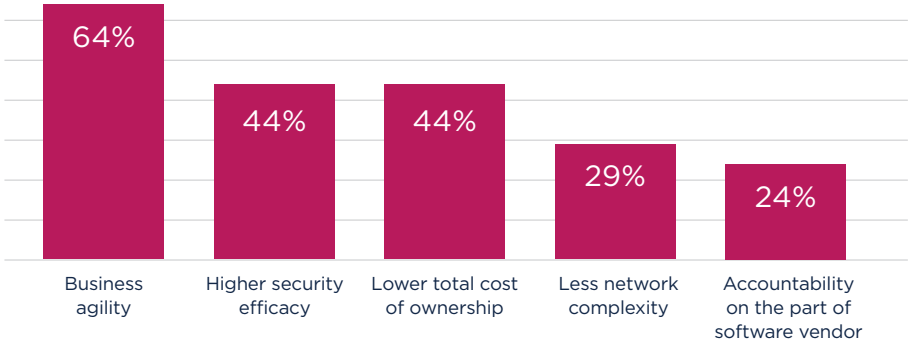
It's a basic tenet of cybersecurity that a security posture is only as strong as its weakest link, so in one sense the two are of equal importance. However, at any one point in time, depending on the stage of the investment lifecycle for different parts of an organization's cybersecurity tooling, spending priorities may favor one more than the other. This reality is reflected in the graphic below.

In the context of the telecoms network, a couple of factors may have affected how respondents answered the question. As 5G standalone (SA) is rolled out, 3GPP prescribes several new security features that are embedded in the architecture. These largely can be thought of as being on the preventative or protective side of the ledger.

24/7 threat monitoring lacking

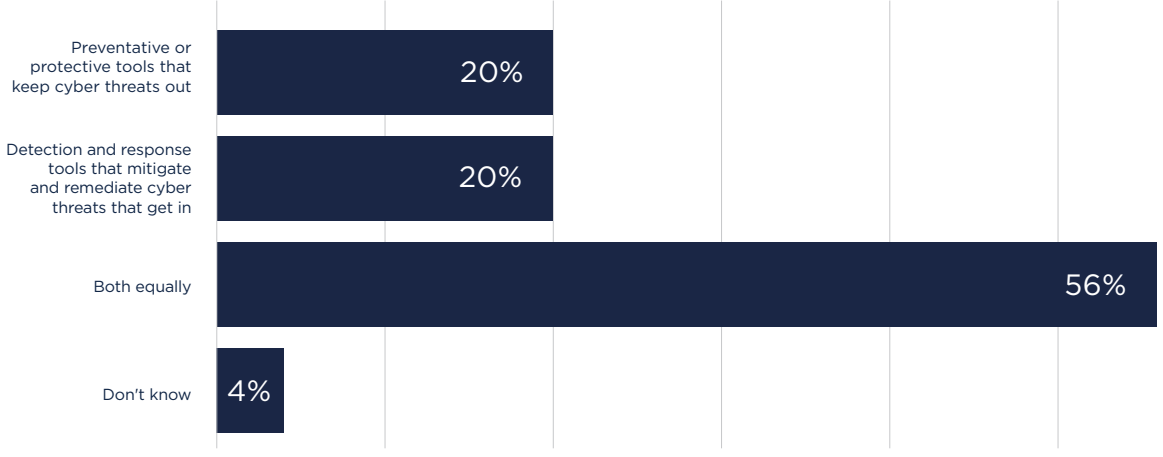
In the case of cyber threat monitoring, detection and response capabilities, investment in telecoms infrastructure is generally considered to be less advanced than in enterprise IT environments. "One

Main drivers for adopting a SaaS model in security operations



TM Forum, 2023

Cybersecurity tools most likely to require substantial upgrade within 3 years



TM Forum, 2023

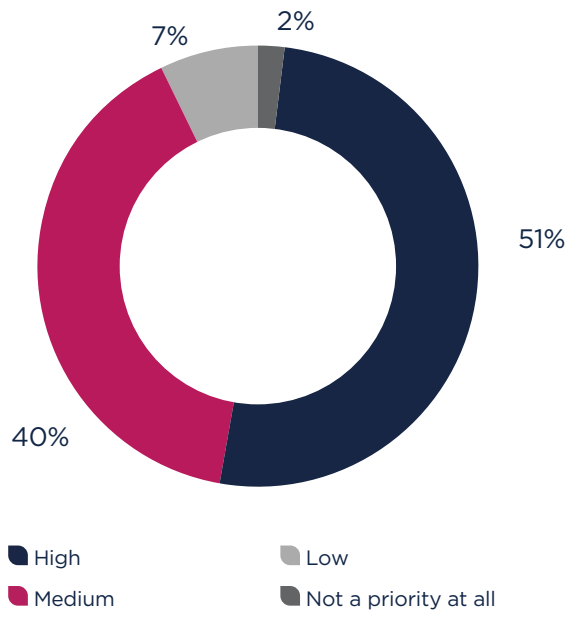
of our main challenges is we are required to be able to monitor for security violations 24/7 in our telecom network infrastructure," says Kok at AIS. "I've asked around and I've yet to find a peer telco here in Asia or any telco vendor that knows of anyone monitoring their telco infrastructure 24/7 for security violations. We have started to import logs into our SOC and are starting to assemble our own approach to doing this."

Hence there is a clear need to invest in re-tooling. Two additional drivers are the rollout of 5G SA with all the new risk it introduces, and the focus of a lot of new government regulation on prescribing more stringent requirements for incident management and reporting. The progress a given telco has already made with these investments – and how much further it plans to go and how quickly – are just two factors that determine the balance of priorities.

As shown in the graphic opposite, within the detection and response domain 90% of respondents state that extended detection and response (XDR) and security orchestration and response (SOAR) are a medium or high priority. Many already have endpoint detection and response (EDR) deployed in their internal enterprise IT environment.

The general direction of travel with XDR is two-fold. The first is to evolve endpoint-based frameworks to ingest, normalize, correlate and act on data from the network as well as many other sources. The other is to extend the XDR framework from the enterprise IT domain into the network.

CSPs' investment priorities for XDR and SOAR in the next 2 years



TM Forum, 2023

> I've yet to find any vendor that knows of anyone monitoring their telco infrastructure 24/7 for security violations."
>
> – Pepijn Kok, CISO, AIS

Justifying spending

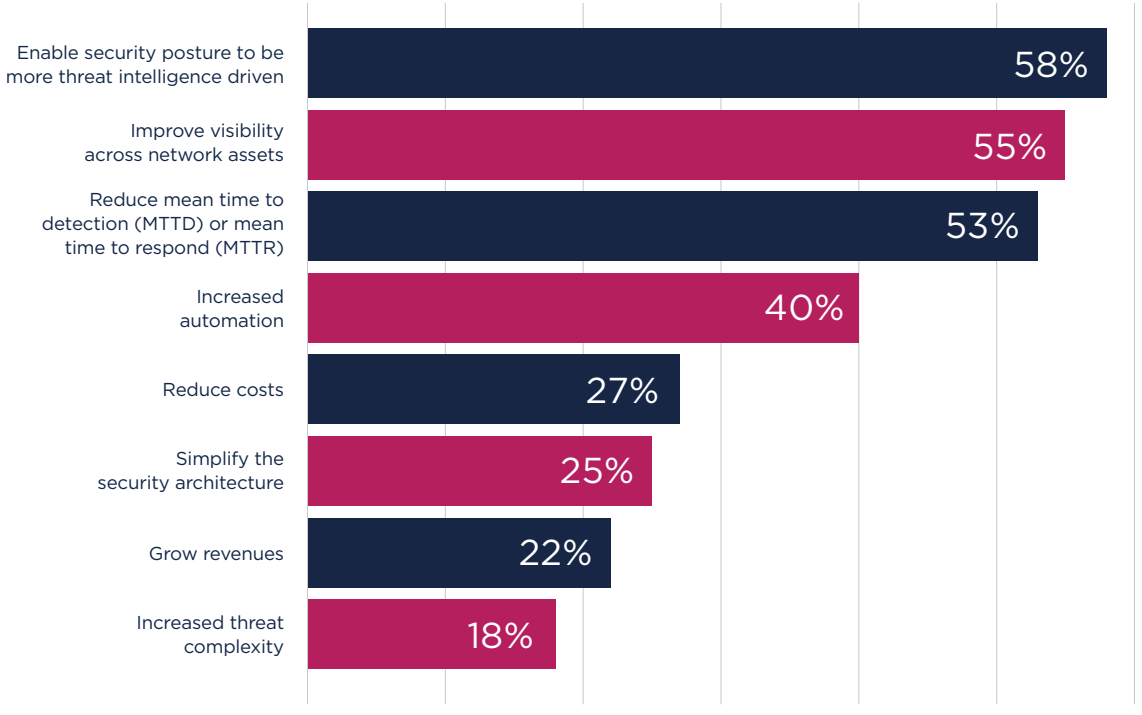
The graphic opposite depicts the factors that make it easiest to justify spending on new security tools in a telco SOC. Echoing the survey's findings about the top drivers for cybersecurity, enabling security posture to be more threat intelligence driven is perceived as the most valuable feature.

Close behind is improving visibility across network assets. It's a lot easier to protect your assets effectively when you have granular visibility into exactly what (and where) they are. Telcos tend to have limited, if not poor, visibility into their assets, especially the vast sprawling estate of their telecoms network assets. They may only have partial visibility – incomplete information – into many of their assets. They may have none at all into some of them. And the visibility they do have may not be centralized and viewable in any one place.

In third place in terms of justifying spending are tools that can drive a reduction in mean time to detection (MTTD) or mean time to respond (MTTR). Lowering these metrics is key to reducing the impact or "blast radius" of a cyberattack.

These top justifications for investing in new tooling align well with the paramount importance of cyber risk management frameworks identified throughout the survey. For example, they all help to enable realistic quantifications of the probability and costs associated with specific incidents.

Easiest way to justify investment in a new security tool in the SOC



TM Forum, 2023

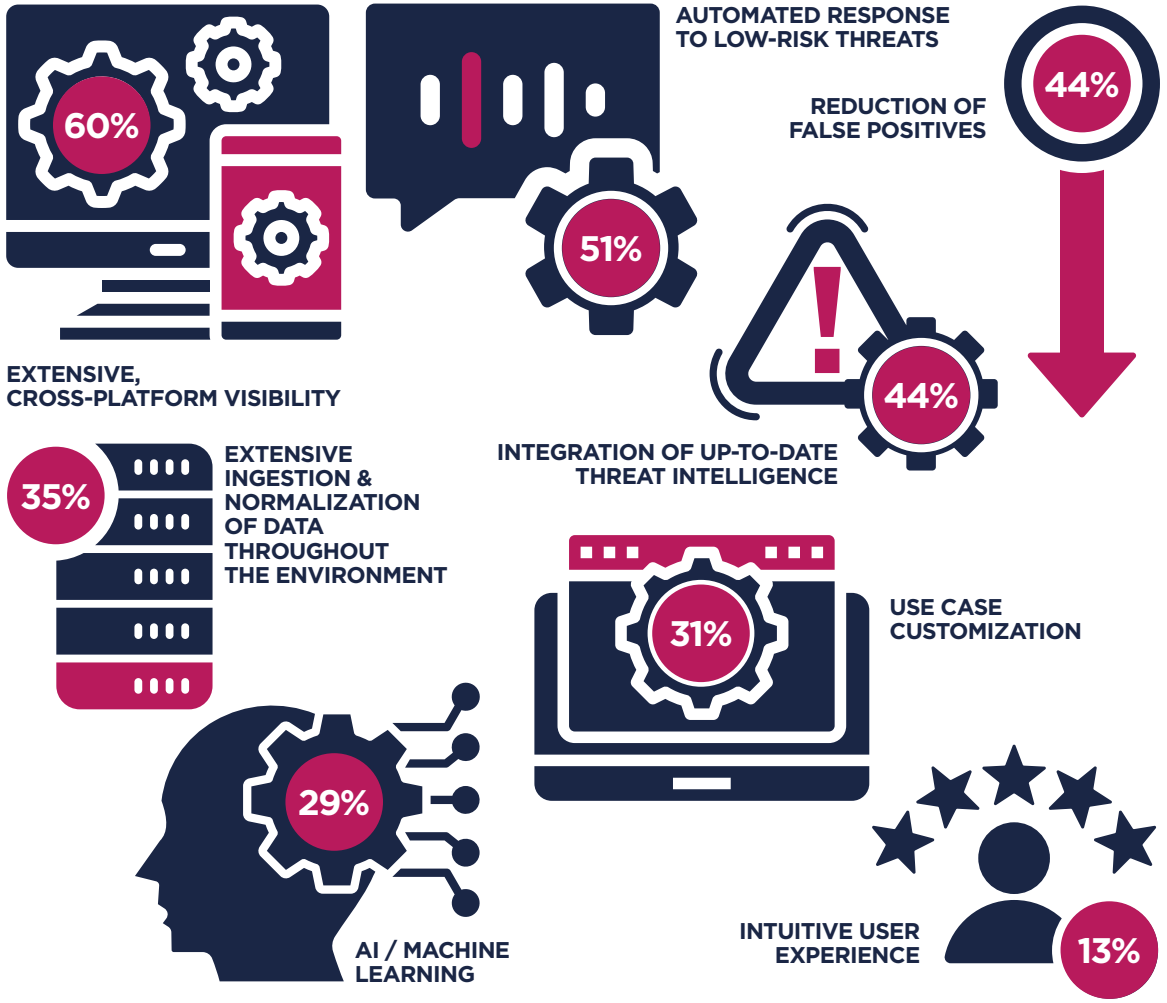
Desired tool features

Within a CSP's security organization, it's useful to separate the function of SOC analysts, who look into specific threats, and the function of SOC engineers, who are responsible for the efficient operation of the SOC infrastructure. SOC analysts value extensive cross-platform visibility above all other enabling characteristics of new security tools (see graphic). It's a baseline that they work from when investigating incidents – a key building block in determining how much confidence they can have in the conclusions they reach.

The second most popular feature is automating responses to low-risk threats. Alert fatigue – having to spend time manually addressing alerts that pose a low-level risk to the organization – is a common barrier to efficiency in cybersecurity operations. It keeps security analysts from prioritizing higher-risk threats as effectively as they otherwise could and therefore undermines job satisfaction, which drives up analyst churn rates in a market where talent is scarce.

The more the SOC can automate low-risk threats, the better it can be at detecting and mitigating higher-risk threats as well as retaining key security analysts. Integration of up-to-date threat intelligence features prominently again. This time it shares third place with reduction of false positives – alerts which incorrectly suggest a threat when there isn't one.

Features SOC analysts value most



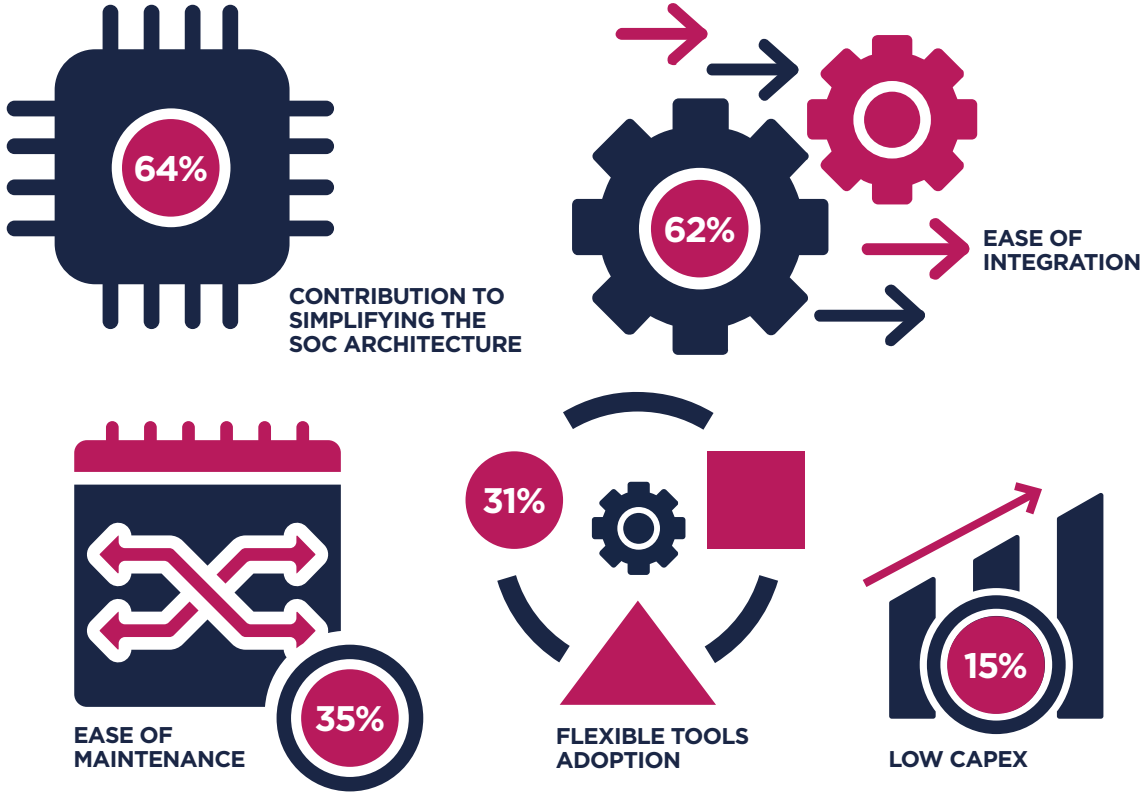
TM Forum, 2023

Simplification of the SOC architecture and ease of integration were identified as the features SOC engineers most value in new security tools. Simplification of the SOC architecture refers to factors such as the number of different vendors deployed in security operations by large organizations like CSPs.

These often run into the several dozens, and more than a hundred is not uncommon. It's not uncommon, either, for architectural simplification requirements to result in the retirement of two legacy security tools being mandated as a condition for investing in one new one. Ease of integration refers to factors such as just how open a given vendor's APIs are, hence how easy – or not – they are to implement.

The next section outlines some key steps operators can take to optimize cyber risk management and improve cybersecurity posture.

Features SOC engineers value most



TM Forum, 2023

section 4

make it happen – strategies for optimizing cyber risk management

Risk management is central to building a roadmap of people, processes and technology to harden a CSP's cybersecurity posture over time. Here are some key steps operators should take:

Put risk management front and center

Build a multi-phase roadmap for aligning cybersecurity strategy with risk management principles. Ensure tight alignment between the organization's capabilities and the goals targeted with each phase – as well as with current and expected iterations in cybersecurity regulations targeting the telecoms sector.

Engage with regulators and peers

Work with government to ensure maximum possible alignment between the organization's goals and future regulations and to ensure that proposals that prescribe the means of achieving goals are well suited to achieving them in practice. Collaborate closely with CSP peers to both reduce the investment of time in navigating regulatory requirements as well as present a common industry position to regulators on key issues.

Integrate cyber threat intelligence everywhere

Cyber threat intelligence should be pervasive throughout the organization, and this needs to go well beyond simply improving the flow of relevant and up-to-date threat intelligence in day-to-day cybersecurity operations. Collaborative threat modeling requires that business leaders engage cybersecurity leaders early in the cycle of launching a new product, entering a new market or engaging with a new business partner. This allows for a granular risk assessment at the outset of the project, when it's easiest to minimize risk, rather than halfway through when adjustments tend to be more complex and costly.

Cyber threat intelligence should be pervasive throughout the organization.

Align the CISO role with risk management goals

A CISO shouldn't be reporting to a technology leader like a CTO or CIO these days because their reporting line should focus on the goal of mitigating cybersecurity risk to the business. Whatever the reporting line, ensure alignment of the CISO's role with cyber risk management principles.

Consider the wider impact of new security tools

Ensure adequate consideration of how new tools contribute to the organization's broader security posture as well as their effectiveness for the specific role assigned to them to maximize return on investment (ROI). The contribution that security tools make to broader network visibility and a cybersecurity posture that's led by threat intelligence are good examples.

Ensure alignment of the CISO's role with cyber risk management principles.

tm forum
open digital framework

A blueprint for intelligent operations fit for the 5G era

The TM Forum Open Digital Framework provides a migration path from legacy IT systems and processes to modular, cloud native software orchestrated using AI. The framework comprises tools, code, knowledge and standards (machine-readable assets, not just documents). It is delivering business value for TM Forum members today, accelerating concept-to-cash, eliminating IT and network costs, and enhancing digital customer experience. Developed by TM Forum members through our Collaboration Community and Catalyst proofs of concept and building on TM Forum's established standards, the Open Digital Framework is being used by leading service providers and software companies worldwide.

Core elements of the Open Digital Framework

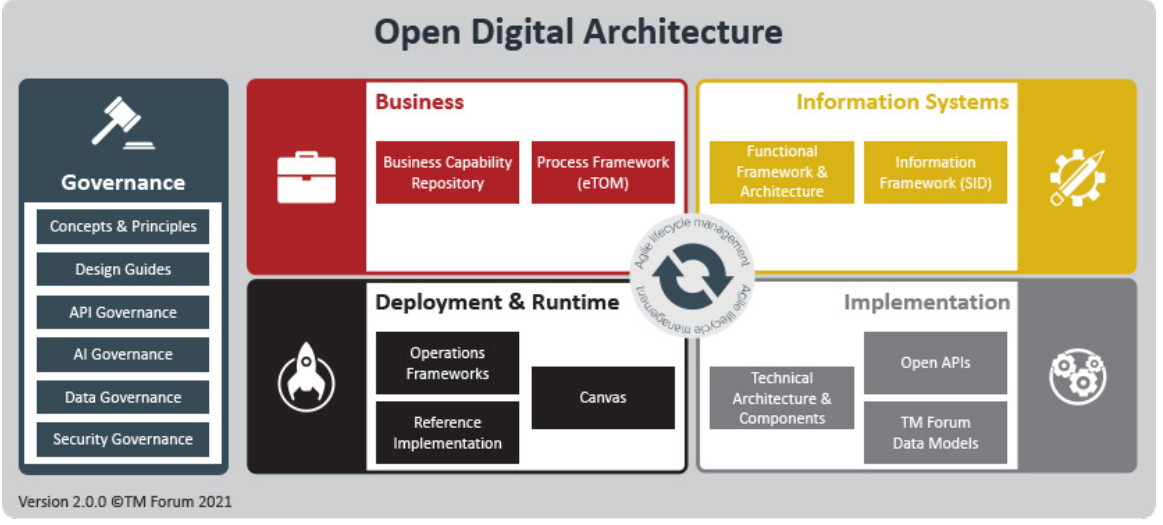
The framework comprises TM Forum's Open Digital Architecture (ODA), together with tools, models and data that guide the transformation to ODA from legacy IT systems and operations.

Open Digital Architecture

- Architecture framework, common language and design principles
- Open APIs exposing business services
- Standardized software components
- Reference implementation and test environment

Transformation tools

- Guides to navigate digital transformation
- Tools to support the migration from legacy architecture to ODA



Maturity tools & data

- Maturity models and readiness checks to baseline digital capabilities
- Data for benchmarking progress and training AI

Goals of the Open Digital Framework

The Open Digital Framework aims to transform business agility (accelerating concept-to-cash from 18 months to 18 days), enable simpler IT solutions that are easier and cheaper to deploy, integrate and upgrade, and to establish a standardized software model and market which benefits all parties (service providers, vendors and systems integrators).

Learn more about collaboration

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

tm forum research reports


telco revenue growth:
time for

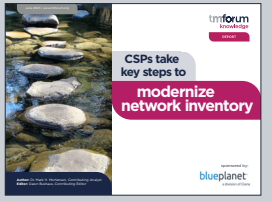

leveling up:
achieving Level 3 autonomous networks and beyond


wholesale changes:
rethinking support systems for new fiber operators


Reigniting
telecoms growth
a Playbook for CEOs


how software-as-a-service
is reshaping business support systems


Digital Transformation Tracker 7
cutting complexity
with automation and AI


CSPs take key steps to
modernize network inventory


transforming BSS:
racing to a flexible, customer-focused future


standout
strategies:
how telcos are innovating in a crowded market


making waves:
the future for Open RAN technology


IoT at the edge:
taking opportunities beyond connectivity


partner ecosystems:
who does what


establishing links:
platform models in the Open API economy


counter intelligence
using AI to improve customer


a roadmap for
Asia-Pacific
telecoms growth


5G core:
exploring CSP approaches

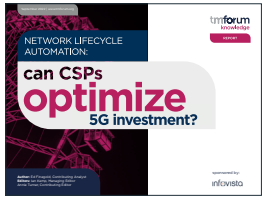

the sustainable telco:
engineering networks for net zero


evolving
business support systems
for future services


DIGITAL OPERATIONS MATURITY:
achieving business value
from transformation


telco revenue growth:
taking it to the next level


mainframe modernization:
charting a course to cloud native


NETWORK LIFECYCLE AUTOMATION:
can CSPs optimize 5G investment?


microservices:
paving CSPs' path to the cloud


autonomous networks:
from concept to reality


into the future:
can telcos monetize the metaverse?


MEC: operators on the edge


DIGITAL ECOSYSTEMS
setting new standards for integration


dish wireless
Next-generation telco

meet the research & media team

Meet the Research & Media team

Report Author:
Patrick Donegan
Principal Analyst
HardenStance

Chief Analyst:
Mark Newman
mnewman@tmforum.org

Practice Lead:
Dean Ramsay
dramsay@tmforum.org

Head of Operations:
Ali Groves
agroves@tmforum.org

Commercial Manager:
Tim Edwards
tedwards@tmforum.org

Digital Media Coordinator:
Maureen Adong
madong@tmforum.org

Report Editor:
Dawn Bushaus
Contributing Editor
TM Forum

Managing Editor:
Ian Kemp
ikemp@tmforum.org

Editor in Chief, Inform:
Joanne Taaffe
jtaaffe@tmforum.org

Global Account Director:
Carine Vandevelde
cvandevelde@tmforum.org

Sponsor Success Manager:
Maryssa Ramsey
mramsey@tmforum.org

Marketing Manager:
Ritika Bhateja
rbhateja@tmforum.org

Published by:

TM Forum
181 New Road
Suite 304
Parsippany, NJ 07054
USA

www.tmforum.org

Phone: +1 862-227-1648

ISBN: 978-1-955998-66-6

Report Design:

Paul Martin

tmforum knowledge

For more information about
TM Forum's ~~Open Digital Architecture~~
please contact **George Glass**