Managing Digital Risk

A blueprint for safeguarding digital transformation initiatives
Contents

Summary................................................................................. 3
   In brief .............................................................................. 3
   Ovum view ...................................................................... 3
   Key messages ................................................................... 3

Next steps............................................................................... 4
   Recommendations to increase the profile of digital risk ....... 4

Act now: digital transformation cannot be ignored.................. 5
   Definitions vary but the implications are broadly similar ....... 5

Get involved: digital risk is an organization-wide issue......... 5
   Handling digital risk is a team effort ............................... 5
   There are many potential definitions of digital risk – all of them involve issues wider than cybersecurity................. 7
   Digital transformation initiatives expand the risks to be considered ................................................................. 8

Plot your course: approaches to managing digital risk are varied but require a guiding star .......... 9
   Security is being addressed early in digital transformation initiatives............................................................... 9
   Organizations are already managing risk in digital transformation projects – but some still leave it late........... 10
   People are at the heart of digital risk challenges ............... 11
   Quantification of digital risk enables risks to be prioritized .............................................................................. 12

Build a coalition: addressing digital risk requires a team effort ................................................................. 13
   Dealing with digital risk doesn’t “just happen” – it needs time and effort ...... 13
   Low-hanging fruit includes education and training ......... 14

The research............................................................................ 15

About the author

Maxine Holt

Maxine leads Ovum’s security proposition, developing a comprehensive research program in this area to support vendor, service provider, and enterprise clients. Having worked with enterprises across multiple industries in the world of information security, Maxine has a strong understanding of the challenges faced and how organizations can look to overcome these challenges.

Maxine rejoined Ovum in 2018, having spent over two years at the Information Security Forum (ISF) developing research in areas including Protecting the Crown Jewels and Securing Collaboration Platforms. Prior to the ISF, Maxine spent 15 years at Ovum covering topics including security, human capital management, and identity and access management. Maxine has a particular interest in how all the component parts of security combine to make up an organization’s security posture.
Summary

In brief

Digital transformation is not a single project – it is an ethos, an approach focused on continuously translating business challenges into a series of technology-focused initiatives and projects to drive the organization forward. Such initiatives, however, introduce risks not previously encountered by organizations.

In July and August 2019, sponsored by RSA, Ovum interviewed 14 senior executives in leading US organizations to investigate the extent to which digital transformation projects are being embraced and how the expanded risks the projects create are handled. This paper shows the teamwork, planning, quantification, challenges, first steps, and education programs being undertaken, throwing light on this relatively new but vitally important subject. These interviews have led to a series of recommendations (see “Next steps”) to help enterprises build and/or develop the management of digital risk.

Ovum view

Handling new risks is a consequence of expanding digitalization. The need and ability to manage risk does not cease at an organization’s boundaries in this increasingly connected world.

It is impossible to ignore the new opportunities unlocked by embracing new applications through the digital transformation of processes and IT. However, these opportunities inevitably create new risks. To be sufficiently effective and efficient, the ability of organizations to discover, manage, and mitigate digital risk requires greater integration between internal functions – particularly risk management and security – as well as across the partners that supply or underpin many of the newer technologies being exploited. Ignoring the opportunities presented by digital transformation initiatives leads to a risk of losing out to competition, becoming less relevant to customers, and suffering from falling financial results.

A plan to handle digital risk must be developed in line with the organization’s size, industry sector, location, experience, and overall attitude to risk. Some already have the option of adopting “best practices” and controls from their industry associations, standards authorities, and/or service suppliers as part of the solution, but these only apply to a small proportion of those launching digital transformation initiatives.

The number of chief risk officers (CROs) hired in larger organizations is expected to rise to handle these growing challenges, although in most companies, multiple board members will continue to be involved. Ultimately, the CEO is responsible for handling risks to the organization and they can (and do) lose their job when things go terribly wrong.

This paper comprises a set of recommendations derived from the experience of research interviewees, and this experience is covered in depth through the key messages highlighted below.

Key messages

• Act now: digital transformation cannot be ignored.
• Get involved: digital risk is an organization-wide issue.
• Plot your course: approaches to managing digital risk are varied but require a guiding star.
• Build a coalition: addressing digital risk requires a team effort.
Next steps

Recommendations to increase the profile of digital risk

Research respondents were extremely open and willing to share their experiences around digital transformation and digital risk. Distilling the feedback throughout this paper has enabled Ovum to provide a series of recommendations that an enterprise can follow to increase the profile of digital risk in their respective organizations. However, not every enterprise will have the range of skills and expertise to take this on in-house, and many organizations will often choose a partner to help design the practice or adjust existing capabilities and technology where they may need support.

Ovum recommendations are provided in Table 1, and organizations can use this list to determine their current position for each recommendation.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Complete/in progress/not started</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide an organization-wide definition of digital transformation initiatives to support recognition of digital risk early in a project.</td>
<td></td>
</tr>
<tr>
<td>Appoint a digital risk officer (or similar) to be responsible for organizational digital risk.</td>
<td></td>
</tr>
<tr>
<td>Form a team under the remit of the digital risk officer to address the risks of digital transformation projects based on senior risk, compliance, IT, technology, legal, audit, and cybersecurity staff.</td>
<td></td>
</tr>
<tr>
<td>Adopt a wide definition of digital risk, including threats to the organization beyond IT systems and applications.</td>
<td></td>
</tr>
<tr>
<td>Assess digital risk when undertaking a digital transformation project. Review the opportunity to address with existing controls and industry best practices.</td>
<td></td>
</tr>
<tr>
<td>Include the security function in early planning for each digital transformation project.</td>
<td></td>
</tr>
<tr>
<td>Incorporate digital risk assessment into the project initiation phase, revisit throughout project gates, and review regularly post-implementation. Include relevant stakeholders, with project sponsor sign-off.</td>
<td></td>
</tr>
<tr>
<td>Consider human factors as the basis for digital risk challenges, including senior executives, specialists (such as engineers), other staff, partners, third-party suppliers, customers, and prospects.</td>
<td></td>
</tr>
<tr>
<td>Use a formal risk assessment process to identify risk for each digital transformation project and prioritize addressing risks based on assessments.</td>
<td></td>
</tr>
<tr>
<td>Understand the organization’s overall attitude to risk.</td>
<td></td>
</tr>
<tr>
<td>Don’t bite off more than you can chew. Break digital risk down into parts (such as internal and external processes), work out their governance, and address them incrementally.</td>
<td></td>
</tr>
<tr>
<td>Look for “quick wins” to demonstrate the value and importance of digital risk management.</td>
<td></td>
</tr>
<tr>
<td>Encourage and inspire all employees to consider how they can play a part in addressing digital risk. Handling individuals at all levels who ignore risk is a practical issue that must be addressed.</td>
<td></td>
</tr>
</tbody>
</table>

Source: Ovum

Each of these recommendations has been developed from the key messages, which are expanded upon in the remainder of this paper.
Act now: digital transformation cannot be ignored

Definitions vary but the implications are broadly similar

At Ovum, digital transformation is defined as follows:

"Digital transformation is not a single project – it is an ethos, an approach focused on continuously translating business challenges into a series of technology-focused initiatives and projects to drive the organization forward."

Respondents were broadly in agreement with the definition. The status of the programs across interviewees’ organizations varied between ad hoc, early stages, and established. Initiatives range from minor to major, but what they all have in common is that the technology being used opens the organization to greater opportunities and greater risk than previously.

All respondent companies are engaging in digital transformation projects, with over 40% having implemented a formal program. Unsurprisingly, half of those with established formal digital transformation programs are in the largest (more than 10,000 employees) organizations. The respondent’s role also highlighted differences: formal programs were more prevalent where the interview respondent has a security role, whereas individuals with an IT role reported ad hoc programs.

Despite wide interpretations of the subject, digital transformation is being universally accepted as a process, with formal programs beginning to replace ad hoc ones.

Recommendation: Provide an organization-wide definition of digital transformation initiatives to support recognition of digital risk early in a project.

Get involved: digital risk is an organization-wide issue

Handling digital risk is a team effort

Current organizational approaches to handling and addressing digital risk vary widely. It is clear, however, that a range of functions are involved in determining digital risk but that ultimate responsibility lies with the CEO (see Figure 1).

Figure 1: Board-level players involved in assessing digital risk

Source: Ovum
On average there are 2.2 senior staff involved in determining digital risk, with more involved in larger organizations. The immaturity of the subject and its practice is demonstrated by the fact that only three of the 14 organizations participating in the research have a CRO, and that in one case the CRO doesn’t take the lead in determining the risks for the company. Ten research respondents cited the involvement of the CIO/CTO; indeed, individuals in this role lead the work in over half of these organizations (see Figure 2).

The CISO is the second most important role in understanding digital risk, followed by non-technical specialists (including CFOs, audit, and legal directors). For those organizations without a CRO or digital risk officer there was little by way of intention to hire such a position (perhaps due to this being an issue for the CEO and others more senior in the organization).

The research shows that determining digital risk is a very wide subject requiring board-level involvement; however, there is no standard way of organizing and leading the team. The approach is more mature in highly regulated industries (e.g., finance, insurance, healthcare) or in areas of the world where privacy regulation requires a privacy officer reporting to the board (e.g., in Europe for the General Data Protection Regulation – GDPR – or California, for the California Consumer Privacy Act – CCPA).

There is no evidence of standard governance models; indeed, some respondents are uncertain about where overall responsibility lies. One respondent indicated that the process is a joint responsibility between the CIO and head of legal counsel, although the CIO leads overall. Another pointed out that the CEO is ultimately responsible for everything – mission, people, and processes – and so, by implication, the analysis of digital risk as well. This is borne out by the resignation of CEOs from companies that have suffered from major data breaches and their financial consequences.

**Recommendation:** Appoint a digital risk officer (or similar) to be responsible for organizational digital risk.

The frequency of activity also varies significantly within the sample – with one organization having meetings every three days, while another has weekly meetings and a third undergoes major reviews on a half-year and annual basis for a range of areas, as well as running penetration and other tests on their IT systems “all the time.”
Those interviewed were broadly of the opinion that today, if there is no one primarily responsible for digital risk, the IT and cybersecurity departments should take the lead for now. Approaches can be customized according to industry sector, size, and values.

Recommendation: Form a team under the remit of the digital risk officer to address the risks of digital transformation projects based on senior risk, compliance, IT, technology, legal, audit, and cybersecurity staff.

Interviewee quotes

Our head of security’s drive (she has experience of working for PayPal and Google) helps us implement policies and accept risks.

We have a 2025 strategic initiative in which we’re predicting the risk landscape and working out how we come up with risk analysis of crypto currency, data intelligence, etc.”

The CRO has a meeting every three days with the CIOs.

There are many potential definitions of digital risk – all of them involve issues wider than cybersecurity

Overall, senior executives involved in this research are well versed in thinking and planning for digital risk, which covers a wide spread of internal, external, technological, criminal, legal, financial, and organizational issues.

Most interview respondents included information risk in their definition of digital risk. The information lifecycle (create, process, store, transmit, destroy) can introduce risk. And the potential for exposure of confidential information is of concern, driven by compliance expectations (e.g., the US Health Insurance Portability and Accountability Act – HIPAA, GDPR, and CCPA) and corporate reputation in a breach scenario. In addition to confidentiality, data integrity and availability were also highlighted, and this is where the strong link between the functions of information security, risk, and IT is forged.

Few organizations operate entirely “on premises” today, and using public, hybrid, or even private cloud adds an extra dimension of digital risk to the enterprise that must be included in assessments. Recognition of risk extending beyond technology – bringing in people and process – was common among all interview respondents.

However, digital risk is also recognized as “essential” inasmuch as the organization must take risks if they are to move forward – the most risk-averse organizations could avoid digital transformation but simultaneously are likely to lose the edge on their competitors or provide a poorer service to citizens. As such, some enterprises include the risk of doing nothing as part of a digital transformation project. This requires a clear understanding of organizational risk appetite.

Recommendation: Adopt a wide definition of digital risk, including threats to the organization beyond IT systems and applications.
For organizations without a definition of digital risk, consider the following examples:

<table>
<thead>
<tr>
<th>Ovum</th>
<th>“Digital risk extends beyond technology. It incorporates the people, process, and technology risks brought about by digital transformation projects. Owned by the project sponsor, driven by the chief digital risk officer, and measured against organizational risk appetite, these risks must be assessed and addressed as part of each project.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>“The unwanted and often unexpected outcomes that stem from digital transformation, digital business processes, and the adoption of related technologies.”</td>
</tr>
</tbody>
</table>

**Interviewee quotes**

- We’re in the middle of our initial project – embedding some of our existing controls and developing some new ones.

- Digital transformation includes both audit and the engagement mechanisms. It’s not only about security risk, but risk in general. Risk is a wider subject.

**Digital transformation initiatives expand the risks to be considered**

The respondents show that digital risk grows as the world turns to a greater use of computing through digital transformation initiatives and that potential disruption increases as systems are opened up to increasing numbers of (often unknown) people and organizations – some with malicious intent. The research also identified that there are extra risks in gathering and analyzing data from multiple sources. Organizations tend to take on a deeper role through these new processes – for example, becoming the custodian of customer data that must be protected from access by its competitors.

Research interviews showed that traditional, typically longer-established, enterprises have a tough digital journey, needing to modify legacy systems and processes through digital transformation initiatives. Those organizations “born in the cloud” – or at least formed when digital transformation got underway – are on the front foot, adapting rapidly to the ever-changing digital environment.

**Recommendation: Assess digital risk when undertaking a digital transformation project. Review the opportunity to address with existing controls and industry best practices.**

**Interviewee quotes**

- The technology has got easier – it’s about user acceptance and adoption now.

- The number one risk is losing our data, or our customers’ data, to another company.
Plot your course: approaches to managing digital risk are varied but require a guiding star

Security is being addressed early in digital transformation initiatives

Over half of interviewed organizations address security either up front or in the design phase of the digital transformation project (see Figure 3).

![Figure 3: The status of security in digital transformation projects](source: Ovum)

Research interviewees from medium-sized companies (1,000–9,999 employees) indicated that this size of organization is the most advanced. All address security up front or during the design of the initiative. Typically, organizations of this size have well-established processes for dealing with security in digital projects. Although larger organizations are expected to also have well-established processes, they are frequently less agile than their slightly smaller counterparts.

In general, security is well understood and being addressed relatively early on in organizations’ digital transformation projects. There were a wide range of discussions with interviewees around the topic; for example, one respondent discussed a methodology incorporating DevOps, cloud, and cybersecurity risks separately (outside of individual projects) as part of its up-front approach to digital transformation. Another organization takes a project-by-project approach, with big differences for initiatives designed for internal staff versus those for external customers. A third respondent in a manufacturing company focuses primarily on addressing security at a product level to handle Internet of Things (IoT) data.

Many of our respondents take a wide view, including “physical” and “cyber” subjects in security and “physical” and “digital” subjects when looking at risk.

**Recommendation:** Include the security function in early planning for each digital transformation project.

**Interviewee quotes**

- Security is an essential element of digital transformation. It includes lots of activities including moving to the cloud. You have to make sure you’re secure. It’s non-negotiable.
- It’s not a single thing – security has to be part of everything.
- We look at it on a project-by-project basis depending on where it comes from. It differs depending on whether it’s for internal or external use (for customers and/or members).
Organizations are already managing risk in digital transformation projects – but some still leave it late

Risk management is being dealt with up front by more organizations than are dealing with security at the same stage of digital transformation projects. However, the majority of interview respondents address digital risk during development or after the fact (see Figure 4).

Research interviews show that medium-sized companies typically address risk management issues up front, while the largest organizations have a greater spread across the categories. The smallest enterprises only address risk management during design or after the fact. Ovum’s ICT Enterprise Insights survey shows that only 39% of small organizations have either developed or are well advanced in having a proactive approach to cybersecurity and digital risk, compared with 45% of medium-sized companies and 51% of large organizations. As with security, the larger the organization, the more established the processes will be, and this includes risk.

The two respondents with financial roles reported that their organizations addressed risk management challenges up front in these projects, while those with a security role reported the greatest spread of results, perhaps demonstrating a greater knowledge of how these issues are being addressed. Additionally, the security function is used to regularly review risk assessments with stakeholders once a project has been delivered.

The research demonstrates that managing risk is less prevalent than handling security in digital transformation programs – in other words, addressing security as part of a digital transformation project is more advanced than assessing the associated risks. Organizations are gradually broadening their approach to digital risk beyond security, but this discipline requires more development within most enterprises.

One way that some interviewed organizations look at digital risk is to separate its components according to their external and internal effects (see Figure 5 for combined examples).
Broken service-level agreements, data and privacy breaches, and non-compliance with industry regulations mainly affect an organization’s customers, partners, and suppliers, resulting in fines and/or reimbursements. The risk of service unavailability, the loss of intellectual property rights, and the ever-widening threat landscape are considerations that will affect the organization internally in the first instance, despite having knock-on effects for customers.

**Recommendation:** Incorporate digital risk assessment into the project initiation phase, revisit throughout project gates, and review regularly post-implementation. Include relevant stakeholders, with project sponsor sign-off.

**People are at the heart of digital risk challenges**
Almost all interview respondents cited human factors when asked about the challenges they face with digital risk. Familiar scenarios abound, such as finding a way around implemented controls, not understanding the need for controls, and a general mistrust of digital data and information. Reference was also made to the “push” to deliver a new product or service ahead of the competition without fully assessing the associated risk.

The general opinion of the research sample is that the challenges of digital risk are about people, whether they deliberately ignore the controls put in place, are prejudiced against new procedures, or are simply ignorant of the dangers.

**Recommendation:** Consider human factors as the basis for digital risk challenges, including senior executives, specialists (such as engineers), other staff, partners, third-party suppliers, customers, and prospects.

**Interviewee quote**

*Speed of process, understanding of issues, conservatism – we consider all of these.*
Quantification of digital risk enables risks to be prioritized

The classification of digital risk is complex. Most organizations assess risk in some way, but it is not always incorporated into digital transformation projects, or sometimes even considered when such projects are proposed.

There were a wide variety of responses from interviewees on how digital risk is quantified. Common advice is to look at the data and its ownership and think about governance. Examples include using guidelines from the International Organization for Standardization (ISO) or the National Institute of Standards and Technology (NIST), or models built into processes.

The "cost of doing nothing" also contributes to the risk discussions of enterprises. Digital transformation projects come about from enabling technology being used to deliver organizational strategy. If a company does not undertake a project, what are the risks to the business? Will it lose ground to competitors? These factors are taken into consideration alongside the risks that actually doing the project will bring.

Ovum has undertaken research into risk quantification. Threats are considered in three broad groups: adversarial, accidental, and environmental. For digital risk, adversarial and accidental threats are grouped together to become the focus of consideration – examples include organized criminal groups, nation states, malicious insiders, and accidental insiders (an "insider" is anyone with access to organizational systems that an outsider would not have).

The quantification of risk requires a calculation. Within the context of each project, some organizations use the following process:
1. Identify the threat.
2. Determine likelihood of that threat happening to the organization – allocate a score of between 1 (very low) and 5 (very high).
3. Determine the potential impact of that threat on the organization – allocate a score of between 1 (very low impact) and 5 (very high impact).
4. Multiply the two numbers to give a risk quantification score.

The scores can be mapped to a matrix to determine the risk level (see Figure 6).

Not every organization will assess risk in the same way. For example, risk-averse organizations would have a greater spread of red in the above diagram. Most organizations do not want to stifle innovation, so that is also taken into account when considering how to address risk. Understanding the organization’s attitude to risk – its "risk appetite" – is an essential foundation for quantifying digital risk.
The objective of risk quantification is to prioritize risks that could cause the greatest harm to the organization. The higher the resulting number, the greater the risk. Identified risks are then addressed in one of three ways:
1. Accept the risk and take no action.
2. Mitigate the risk by applying controls (using a combination of people, process, and technology).
3. Transfer the risk (e.g., to an insurance company).

It is not possible to eliminate risk in any digitally connected organization. Instead, organizations must be able to manage their risk in line with their risk appetite. The lower the appetite for risk, the more stringent the controls.

Build a coalition: addressing digital risk requires a team effort

Dealing with digital risk doesn’t "just happen" – it needs time and effort
Building a plan with an open mind, doing the research on best practices for specific industries, understanding where responsibilities lie, and addressing risks incrementally were highlighted by some interview respondents. From an internal perspective, the plan should be clearly articulated to all levels, including C-suite, and cover each risk assessment. Any implemented controls should be easier to follow than to circumvent, users must be trained on not only the controls but the reason for the controls, and it should be possible to demonstrate the value of the new digital processes (i.e., the risks were worth taking).

Common approaches for many include increasing awareness among those unfamiliar with digital risk (including very senior employees) and widening the number of employees involved in finding solutions or developing controls.

Interview respondents were asked to advise others outside their organization on where to start with digital risk. Suggested actions include the following:
- Identify the ownership of the data and the areas of influence within the organization.
- If possible, find the people who already know the risks, the business, and which areas are affected, then benchmark where you are today.
- If appropriate in the specific industry sector, look for formal guidelines from ISO or best practice models built into the tools used already.

One respondent summarized the first steps to take as getting the IT team involved and thinking about digital risk in terms of people, process, and technology – a combination that many will recognize.

Recommendation: Don’t bite off more than you can chew. Break down digital risk into parts (such as internal and external processes), work out their governance, and address them incrementally.

Interviewee quotes
- Back to basics – plan a program, understand digital risk, what ethics the organization has, and how you’re going to approach the risks.
- People need an open mind to look for research into how things work in their industry and embrace best practice into our business.
- You don’t want security measures to stifle innovation.
Low-hanging fruit includes education and training
People, process, and technology were all highlighted as vehicles to get moving quickly on digital risk. Given that people are at the heart of digital risk challenges, awareness and education programs are strongly recommended. A single program is unlikely to be appropriate — role-based and seniority-based programs were among the approaches used by some research respondents. Key to successful education is to demonstrate that digital risk is a serious issue in the first place.

From a technology perspective, embracing automation is recommended. Attitudes to automation are continually evolving, and most enterprises take a gradual approach, tweaking the amount of automation, becoming comfortable with it, then tweaking again. Other technology-based recommendations include knowing what data the organization has and where it resides, alongside having strong identity management and access controls.

Process-focused recommendations include robust change management controls and having a single source for best practice.

Recommendation: Look for “quick wins” to demonstrate the value and importance of digital risk management.

Interviewee quotes

I am a person of quick fixes. The department people can do whatever they want at the privacy stage: I’ll do my three assessments and between us we’ll get everything covered.

Having a foundational model will help you adopt digital transformation initiatives faster.

It’s about automating the mundane, not just looking for the ‘moonshot’ of artificial intelligence and/or machine learning.

Nearly every interview respondent had direct experience of handling individuals who expose the organization to digital risk.

Recommendation: Encourage and inspire all employees to consider how they can play a part in addressing digital risk. Handling individuals at all levels who ignore risk is a practical issue that must be addressed.
The research
Telephone interviews were conducted with 14 senior executives of US-based organizations in July and August 2019. The breakdown by industry sector is shown in Figure 7.

Organizational sizes grouped in terms of large, medium, and small (measured in employees) are shown in Figure 8.

The smaller organizations interviewed were all in contract manufacturing or IT and services companies with experience of working with large organizations.

Figure 7: Ovum interviews by industry sector

Figure 8: Ovum interviews by organizational size group
The respondents’ job titles are summarized in Figure 9.

Figure 9: Ovum interviews by job title area

Source: Ovum

For analysis, anyone with both security and IT in their title were grouped into “security.” The actual job titles/areas of responsibility varied significantly and included the following: CFO; CIO; CISO; CPO; CSO; cybersecurity; cybersecurity and governance, risk, and compliance (GRC) projects; digital operations and transformation; digital strategy and delivery; enterprise cybersecurity and technology risk; finance and business affairs; IoT and analytics; IT; network infrastructure; and security and privacy.

Open and closed questions were asked, exploring the subjects in detail, which were then compiled and analyzed before adding Ovum inputs from experience and research.
OVUM CONSULTING
Ovum is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy.

Through our 150 analysts worldwide, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients to profit from new technologies and capitalize on evolving business models.

Ovum is part of Informa Tech, a B2B Information Services business serving the Technology, Media, and Telecommunications sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum’s consulting team may be able to help your company identify future trends and opportunities. Please contact us via

https://ovum.informa.com/contact/contact-us
consulting@ovum.com
https://www.linkedin.com/company/ovum/
www.twitter.com/Ovum