IDC FutureScape

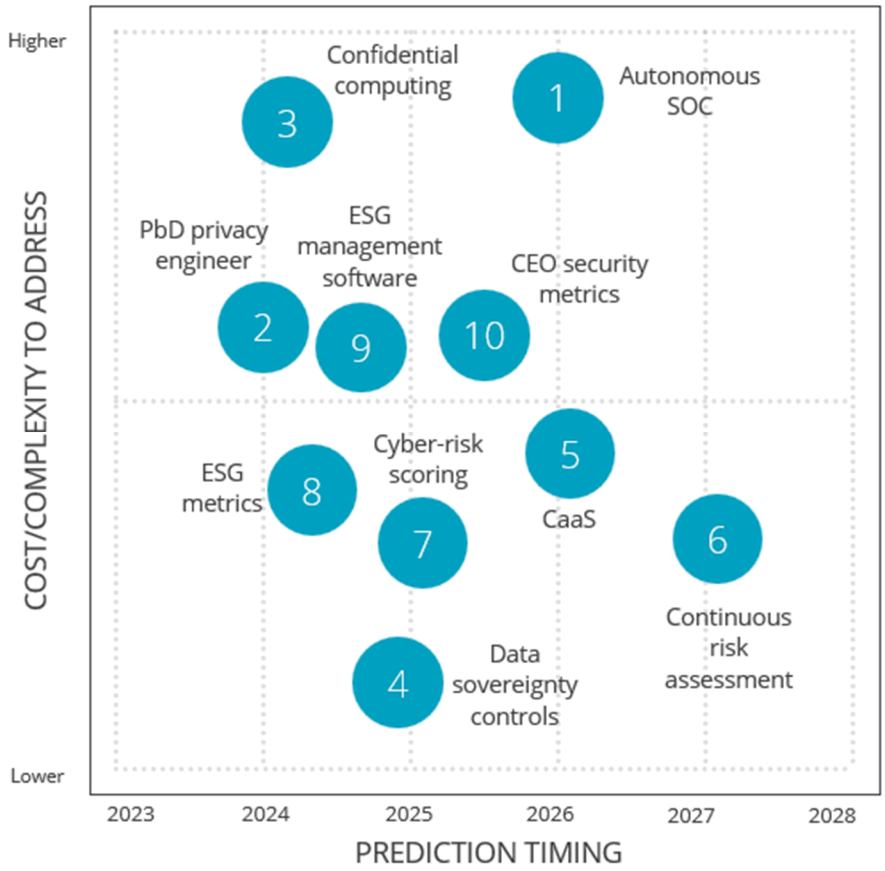
IDC FutureScape: Worldwide Future of Trust 2023 Predictions

Grace Trinidad
Craig Robinson
Phil Goodwin
Shilpi Handa
Frank Dickson
Ryan O'Leary
Joel Stradling
Michelle Abraham
Romain Fouchereau
Claudio Stahnke
Michael Suby
Bill Latshaw
Curtis Price

IDC FUTURESCAPE FIGURE

FIGURE 1

IDC FutureScape: Worldwide Future of Trust 2023 Top 10 Predictions



Note: Marker number refers only to the order the prediction appears in the document and does not indicate rank or importance, unless otherwise noted in the Executive Summary.

Source: IDC, 2022

October 2022, IDC #US49755022

EXECUTIVE SUMMARY

It would be hard to talk about the future of trust without acknowledging the impact of the COVID-19 pandemic on computing. Pushed into remote and now hybrid work environments, organizations scrambled to set up the infrastructure needed to continue operating, and citizens incorporated greater amounts of technologies and digital identities into their everyday experience. In the future of trust predicted here, we see the push and pull digital services present: cloud-based services mean more and more data is collected and analyzed, leading to greater insights needed by automation and artificial intelligence (AI) innovations that promise to alleviate pain points experienced by organizations and their customers. At the same time, consumers are ever more aware and concerned about potential exposure of their data as cyberthreats increase in number and sophistication. "Privacy by Design" (PbD) principles are being reevaluated now as customers become more curious and cautious about how their personal information is used. Rules and regulations regarding location of data and concerns around protecting the data of a nation's citizens are changing how data is stored and transmitted. Meanwhile, customers also require zero disruptions to the digital infrastructures that undergird their work and daily lives.

In all of this uncertainty, we are increasingly turning to the certainty of data. In the following predictions, we see the thread of data-driven insight running through privacy, security, compliance, risk, and environmental, social, and governance (ESG) — the Framework of Trust.

IDC's top 10 predictions for the future of trust in 2023 and beyond:

- **Prediction 1:** By 2026, 30% of large enterprise organizations will migrate to autonomous security operations centers accessed by distributed teams for faster remediation, incident management, and response.
- **Prediction 2:** By 2024, 35% of organizations will employ a privacy engineer to operationalize Privacy by Design principles into IT systems, processes, and product development strategy.
- **Prediction 3:** By 2024, 30% of heavily regulated organizations will adopt confidential computing technologies to combine and enrich sensitive data critical to multiparty compute applications while preserving privacy.
- **Prediction 4:** By the end of 2024, 65% of major enterprises will mandate data sovereignty controls from their cloud service providers to adhere to data protection and privacy regulatory requirements.
- **Prediction 5:** By 2026, driven by steep regulatory growth, talent gap, and cost efficiency measures, 40% of organizations will invest in compliance-as-a-service offerings to meet their regulatory mandates.
- **Prediction 6:** By 2027, 60% of G2000 companies will adopt continuous risk assessments over annual security audits, leveraging service providers to limit the burden of policies, practices, and technical debt.
- **Prediction 7:** By 2025, the SEC will publish standards for cyber-risk scoring, and publicly traded companies will be required to update and report this score on an annual basis.
- **Prediction 8:** By 2024, 30% of organizations will advance their ESG metrics and data management beyond reporting capabilities to generate sustainably driven cost and competitive advantages.

- **Prediction 9:** By 2024, 75% of large enterprise firms will implement purpose-specific ESG data management and reporting software as a response to emerging legislation and increased stakeholder expectations.
- **Prediction 10:** By 2025, 45% of CEOs, fatigued by security spending without predictable ROI, will demand security metrics and results measurement to assess and validate investments made in their security program.

This IDC study presents IDC's top 10 predictions for the future of trust in 2023 and beyond.

"The relationship between data-driven insight and trust is cyclical. Customers confer trust onto organizations that transparently share data-driven insights, but trust is a prerequisite to overcome consumer reluctance to share the personal data required to generate high-quality organizational insight." – Grace Trinidad, research director, IDC's Future of Trust

IDC FUTURESCAPE PREDICTIONS

Summary of External Drivers

- **Geopolitical reality** – Sovereignty in the digital world
- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Meaningful intelligence** – Differentiated decision power
- **Ecosystem-based innovation** – Driving enterprise value
- **Mainstream ESG** – Sustainability is measured and mandatory
- **Work mode upheaval** – New models and leadership
- **Everything as a service** – Thriving through the change

Predictions: Impact on Technology Buyers

Prediction 1: By 2026, 30% of Large Enterprise Organizations Will Migrate to Autonomous Security Operations Centers Accessed by Distributed Teams for Faster Remediation, Incident Management, and Response

The confluence of continued hybrid and remote work, a cybersecurity talent shortage that will not see relief in the near term, and the increasing volume and sophistication of the threat landscape will necessitate, for many organizations, adoption of autonomous security operations centers (SOCs). Autonomous SOCs, using AI/ML to continually scan the threat landscape for new and emerging threats, promise the identification, triage, and remediation of threats at scale, allowing distributed cybersecurity teams to focus on the largest, most pressing problems wherever they may be located.

AI and analytics have unlocked not only the ability to decipher attacker code and process large amounts of cyberthreat information efficiently but also the ability to detect mounting, planned threats before they are completed and deployed. One such example is identification of the name Mirai to mean botnet. *Mirai* was a term developed by attackers to evade detection by law enforcement – using AI, this new term was identified quickly and efficiently.

Associated Drivers

- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Meaningful intelligence** – Differentiated decision power
- **Ecosystem-based innovation** – Driving enterprise value

IT Impact

- An autonomous SOC will be dependent on the quality of data provided to train the security models and on cybersecurity analysts' ability to decipher the decisions made by the provided AI/ML model.
- Autonomous, data-driven SOC models will accelerate the pace of the cyberthreat arms race. Attackers will turn to methods such as reinforcement learning and generative adversarial networks to produce novel cyberattacks that may evade detection. In this scenario, adoption of autonomous SOC may become non-optional.

Business Impact

- CEOs are growing fatigued of the increasing proportion of organizational spend allocated to security (see prediction 10). Autonomous SOCs may flatten this trend over time despite the initial expenditure to establish an autonomous SOC.
- Incorporation of autonomous SOCs will necessarily occur on top of existing security infrastructure until the right skill balance is achieved. It may take time to see security expenditures level.

Guidance

- Large enterprise organizations with heavily cloud-based systems should consider investment in autonomous SOCs to aid their existing cybersecurity workforce. While not perfect, autonomous SOCs can provide insight into threats that might be missed by an overworked and fatigued cybersecurity team or are beyond traditional defenses.
- Organizations that decide to defer or abstain from adoption of autonomous SOCs should keep an eye on developments around autonomous SOCs. Use of artificial intelligence techniques such as reinforcement learning to identify attacks may introduce changes to the threat landscape that will impact all businesses.

Prediction 2: By 2024, 35% of Organizations Will Employ a Privacy Engineer to Operationalize Privacy by Design Principles into IT Systems, Processes, and Product Development Strategy

Privacy by Design, PbD, coined by Ontario Privacy Commissioner Ann Cavoukian, refers to the proactive architecture of data privacy protection into all information systems, products, and applications. PbD positions data privacy as the default setting of any information technology (IT), whereby the purpose of data collection, use, and retention is specified in its purpose, limited to these purposes, and minimized to the least amount of data collection necessary. It is an approach that is fundamentally user and customer centric and operates with the assumption of privacy for all.

While many organizations likely aspire to some degree of Privacy by Design, operationalization requires extensive knowledge and planning and will necessitate talented "privacy engineers" with the right skill set to undertake the challenge of designing privacy-first and user-centric information systems. Users and consumers are demanding greater transparency into the use of their data, and employment of a privacy engineer can help provide centralized accountability that the data collected and used is specified for purpose.

Associated Drivers

- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Mainstream ESG** – Sustainability is measured and mandatory
- **Work mode upheaval** – New models and leadership

IT Impact

- Incorporation of Privacy by Design into all information systems will likely slow development of information technologies at the outset, resulting in longer time to delivery of new products and applications.
- Specification of limited data collection, use, and retention according to PbD principles call for a revision of existing IT development processes. Staff may require training on Privacy by Design principles to understand the rationale behind this approach and its impact.

Business Impact

- Organizational leaders worldwide indicate that consumer interest in understanding the security, privacy, or compliance capabilities of their organizations has grown. Privacy by Design principles are aligned with consumer interest in the management of their personally identifiable information (PII) and can be used to promote trust and transparency efforts.
- Organizations looking to incorporate Privacy by Design into their information system architecture should anticipate the friction that PbD will create for their teams. Longer development timelines and communication at every level of the organization will be necessary until PbD principles become baked into IT development processes.

Guidance

- The employment of a "privacy engineer" is a strong signal to clients and consumers that an organization is serious about end-to-end privacy for the full life cycle of data in marketing and communications efforts to engender trust.

Prediction 3: By 2024, 30% of Heavily Regulated Organizations Will Adopt Confidential Computing Technologies to Combine and Enrich Sensitive Data Critical to Multiparty Compute Applications While Preserving Privacy

Confidential computing protects and encrypts data in use, as opposed to data that is encrypted in storage or in transit. This is of particular importance to healthcare organizations that handle PHI or any organization handling sensitive PII as confidential computing provides the ability to perform computation in a hardware-based trusted execution environment. In so doing, organizations mitigate threats to an application or a system where users need to dynamically access and use sensitive information across multiple sites or geographic locations. Confidential computing will also protect the intellectual property of algorithms and AI and eliminate the need for data replication for any organization.

Confidential computing can also accelerate innovation and collaboration. Using healthcare as an example, healthcare researchers training AI models with patient data can deploy their protected AI to several hospitals. Those hospitals, in turn, can use their patient data to further train the AI model and send back the trained model for reconciliation with the findings of their healthcare peers without sharing, distributing, or replicating patient health information.

Associated Drivers

- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Ecosystem-based innovation** – Driving enterprise value
- **Work mode upheaval** – New models and leadership

IT Impact

- Confidential computing technologies will necessitate substantial changes to existing applications and will require technical expertise managing data enclaves.

- Data users will experience a steep learning curve as they acclimate to a more controlled data environment.

Business Impact

- Confidential computing will allow more sensitive workloads to move to the cloud and, as discussed in the aforementioned example, allow for collaboration with other organizations without exchanging or revealing sensitive data owned by the organization. This can eliminate the need for on-premises management of data.
- Organizations will have to invest in teams with strong technological skills to realize the potential of confidential computing, exacerbating the skills shortage already experienced by most organizations. Organizations will need to decide whether to be optimistic about attracting skilled prospects or if training internally will be the more sustainable approach.

Guidance

- Organizations looking to implement confidential computing should look for confidential computing partners that are prepared to provide broad custom support for their organization.
- Confidential computing can become an initial bottleneck for data with many users and uses. Fully conceptualize all use cases and consider deployment in a stepwise manner to reduce disruption.

Prediction 4: By the End of 2024, 65% of Major Enterprises Will Mandate Data Sovereignty Controls from Their Cloud Service Providers to Adhere to Data Protection and Privacy Regulatory Requirements

Data sovereignty requires that the personal information of a customer is stored in a way that complies with the data protection laws and regulations of the host country where the data is physically located. Although many countries have had data sovereignty laws in place, GDPR compliance has made data sovereignty non-optional as fines have been levied against organizations that are in violation of GDPR. 40 of these fines issued for GDPR violations since 2018 are greater than €1 million with a running total of almost €500 million in fines levied against organizations in breach of GDPR. In the United States, a drafted executive order intends to prevent foreign adversaries from accessing Americans' personal data via mobile applications or other sources. Data sovereignty compliance will first depend on identification of where the data collected by your organization resides.

Associated Drivers

- **Geopolitical reality** – Sovereignty in the digital world
- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Everything as a service** – Thriving through the change

IT Impact

- Data discovery and mapping, or identification of where your organization's data resides, is the first step to ensuring compliance to data sovereignty laws and regulations.
- Organizations employing a multicloud strategy might find data mapping more complex and difficult, depending on cloud vendor.

Business Impact

- Personally identifiable information includes full names, social security numbers, driver's licenses, mailing addresses, financial information, and health information. Organizations may need to audit their data and data collection approach to find out whether these types of personal identifiers have been stored.

- Availability of data sovereignty controls will relieve businesses of the burden of having to track emerging regulations regarding the location of data. On-premises data may be moved to cloud platforms as buyers become more confident in their cloud platforms' ability to assure compliance.

Guidance

- Strategies to prepare for this complex regulatory landscape and adhere to privacy regulations are to minimize data collection, cull data unnecessary to your organization, and invest heavily in data discovery and mapping tools to understand the exposure of your sensitive data.

Prediction 5: By 2026, Driven by Steep Regulatory Growth, Talent Gap, and Cost Efficiency Measures, 40% of Organizations Will Invest in Compliance-as-a-Service Offerings to Meet Their Regulatory Mandates

If a visualization could occur that would represent the number of regulations that have expired or been repealed, the vision would be quite narrow. On the contrary, growth of regulations that organizations need to be cognizant of and adhere to continues to grow. If a chief compliance officer, or the persona who tries to fulfill this role, is honest, most would say that compliance is not in their organization's DNA.

Good compliance does not necessarily equal good security. Good compliance, though, can help reduce fines, minimize the attack surface, and protect organizational reputation by minimizing the damage when cyberattacks are launched or when organizations are audited. Utilization of a compliance-as-a-service (CaaS) offering will increasingly be seen as the norm, just like other managed services such as IT operations, payroll, or more recently cybersecurity has become.

Associated Drivers

- **Geopolitical reality** – Sovereignty in the digital world
- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Everything as a service** – Thriving through the change

IT Impact

- Lack of data, or more accurately, the lack of data that has been collected and turned into information and insights to help drive compliance efforts, inhibits compliance validation. CaaS can alleviate the time-consuming and costly processes required to audit, document, and certify your organization's compliance posture.
- Elevated awareness of the need to be compliant by utilizing CaaS offerings will likely spur additional needs to change how and where data is stored, viewed, and processed.

Business Impact

- Compliance as a service can simplify complex business processes that have been set up in response to changing governance and regulatory standards. At its best, CaaS can ensure that data is protected in accordance with industry-specific regulations.
- Since CaaS is a service that can aid and have impact on compliance, security, and risk teams, it will be important for these groups to work closely in selecting their CaaS solution.

Guidance

- The increasing use of IoT/OT data to validate compliance in areas such as ESG compliance will require appropriate controls to be put in place to protect these new data streams.

- Proper data classification and a data inventory go hand in hand with proper classification. As data gets properly identified and classified, be prepared to make additional investments in areas like data obfuscation to hide PII/PHI and increased encryption.
- A good compliance solution will likely unveil a need for process changes. Proactively work across departmental boundaries and engage the C-suite to prepare for the inevitable changes.

Prediction 6: By 2027, 60% of G2000 Companies Will Adopt Continuous Risk Assessments Over Annual Security Audits, Leveraging Service Providers to Limit the Burden of Policies, Practices, and Technical Debt

When adversaries are continually scoping the Internet looking for opportunities, organizations need to understand their risk on a continuous basis as well. An annual security audit is only a single point in time view that tells the organization how it performed only at that single point in time.

There are security tools for continuous monitoring of the environment that enable continuous risk assessments, and some organizations will use them in conjunction with human resources in security, risk, and compliance departments. Others will outsource the burden to a third party to avoid buying yet another security system and hiring more people to do the work.

Associated Drivers

- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Meaningful intelligence** – Differentiated decision power
- **Work mode upheaval** – New models and leadership

IT Impact

- IT and security teams will need to collaborate on setting up the continuous assessments to make sure the data is flowing without interruption.
- There needs to be complete visibility into the security environment to include assets and identities, both physical and ephemeral, human and machine.

Business Impact

- Continuous monitoring provides real-time evaluation of threats against a given IT system. If partnered with a third-party provider for your continuous audits, organizations might experience shock as unexploited vulnerabilities are discovered, resulting in larger, unplanned workloads for compliance and security teams.
- Greater visibility into security operations, paired with the right visualizations to communicate issues quickly, can mean increased engagement from teams outside of security, especially at the outset. As reporting moves away from "check the box" approaches, education may be necessary to rightsize expectations.

Guidance

- Ensure that a continuous visibility monitoring solution is in place because unknowns can cause great harm.
- Understand the options for performing the work in-house versus outsourcing. This determination will be different for every organization looking to implement continuous risk assessment based on in-house skill and talent, among other factors.
- Because security risk is assessed continuously, information assurance and cybersecurity, along with information technology teams, will likely need to set reporting expectations and timelines for C-level decision makers. Since security audits are currently done annually for

many organizations, risk of disengagement and "falling off the agenda" is high for a more frequent reporting cadence. Given the high prioritization of security for CEOs worldwide, it is important to not internalize this spirit and maintain commitment to reporting even when things are quiet. These periods provide information and insight and allow teams outside of cyber and IT to better conceptualize issues that might arise and interpret their magnitude.

Prediction 7: By 2025, the SEC Will Publish Standards for Cyber-Risk Scoring, and Publicly Traded Companies Will Be Required to Update and Report This Score on an Annual Basis

In March 2022, the SEC stated, "Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs. Today, cybersecurity is an emerging risk with which public issuers increasingly must contend." While the SEC's current proposed rules cover reporting of cybersecurity incidents, policies, and procedures for managing cyber-risk, and management (including board of directors) expertise in overseeing cyber-risk, IDC expects the SEC will go further in the future in time publishing standards for the management of cybersecurity risk. A cyber-risk score that takes into account visibility into the environment, mitigations put in place, security team preparation in the form of regular red teaming/tabletop exercises, and cybersecurity insurance coverage will allow for easier assessment of companies for investors.

Associated Drivers

- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Meaningful intelligence** – Differentiated decision power
- **Work mode upheaval** – New models and leadership

IT Impact

- There needs to be means of ensuring that all the cybersecurity tools that are in place have been implemented to their full potential. There cannot be tools that are there just to check a box.
- IT and cybersecurity departments will need to establish new routines of reporting to accommodate the SECs standardized disclosures of cybersecurity risk management.

Business Impact

- Compliance, cybersecurity and information assurance, and IT staff will work more closely together if not already.
- Organizations will require dedicated staff for monitoring their organization's cyber-risk score and ensure that minimum requirements are met in compliance with investor information needs.
- The board of directors will require frequent updates on the organization's security posture so it can keep abreast of risk changes.

Guidance

- Do not wait for an SEC mandate; develop an internal risk score with the help of current vendors and monitor factors that change it over time.
- Determine who is responsible for developing and auditing the cyber-risk score.
- Work with auditors to fully understand what impacts the score.

Prediction 8: By 2024, 30% of Organizations Will Advance Their ESG Metrics and Data Management Beyond Reporting Capabilities to Generate Sustainably Driven Cost and Competitive Advantages

In the United States, the SEC is considering rules requiring detailed disclosure of climate risk and greenhouse gas emissions. If enacted, the rule will likely lead to mandatory reporting in line with the Task Force on Climate-Related Financial Disclosures (TCFD) reporting framework. Organizations that are already reporting climate risk and greenhouse gas emissions in line with TCFD will be positioned to rise to the top of their markets should these rules go into effect. Beyond rules and regulations, consumers are becoming more educated and curious about how the organizations they engage with are performing in terms of sustainability and social impact.

Associated Drivers

- **Meaningful intelligence** – Differentiated decision power
- **Ecosystem-based innovation** – Driving enterprise value
- **Mainstream ESG** – Sustainability is measured and mandatory

IT Impact

- Organizations will need to evidence commitment to ESG initiatives in their communications with clients and buyers. In a recent IDC's *Future of Trust Survey,* public cloud vendors that ranked low on ESG measures were ranked as such because of a failure to demonstrate commitment to and delivery of diversity and inclusion initiatives in one case and failure to communicate KPIs related to employee health and well-being in another.
- Advancement of ESG metrics may require new data skill sets to understand the meaning behind the ESG data provided (i.e., data analysts skilled in understanding and unpacking environmental data pertaining to land use, water consumption, and waste; social data such as living wages, DEI, employee engagement; or governance measures such as taxes or ethics).

Business Impact

- That the SEC is considering rules requiring climate change disclosure shows how critical ESG initiatives have become for investors. The SEC writes that "as investor demand for climate and other environmental, social, and governance information soars, the SEC is responding with an all agency approach." This includes examination of firm policies, procedures, and practices related to ESG and use of ESG terminology. Businesses may need to evaluate their approach and ensure that ESG advertising and marketing are consistent with coming SEC regulations.
- Advancement of ESG metrics and data management will provide greater credibility to organizations pursuing strong sustainable and ethical operations and strengthen brand image and communications.

Guidance

- As the approach to ESG matures, organizations will need to signal commitment to ESG initiatives in a concrete, measurable way.
- Curious and educated consumers have decreasing patience for performative ESG and may examine organizational approaches to ESG closely. Organizations that are proactive in their approach to ESG measurement – even if that means failing fast and revising the approach often as lessons are learned and insights gained – will engender greater trust with consumers and clients.

Prediction 9: By 2024, 75% of Large Enterprise Firms Will Implement Purpose-Specific ESG Data Management and Reporting Software as a Response to Emerging Legislation and Increased Stakeholder Expectations

According to IDC forecast research, environmental, social, and governance, or ESG, objectives are expected to grow to $158 billion in 2025. Defined by IDC as professional services centered around goals related to environmental and social sustainability and governance of that process, the main areas of focus of ESG business services were business strategy, human capital management solutions, and risk management, with the largest proportion of spend going to strategy consulting.

ESG strategy consulting is a high-priority first step for organizations planning sustainable transformation. Because sustainable transformation can be daunting, organizations are working to leverage available service providers to gain competitive advantage over peers. Purpose-specific ESG data management and reporting, or ESG data management and reporting that aligns with organizational goals and corporate mission, will allow organizations to evaluate their progress toward sustainable transformation and enable confident reporting of progress on ESG initiatives to stakeholders.

Associated Drivers

- **Mainstream ESG** – Sustainability is measured and mandatory
- **Work mode upheaval** – New models and leadership
- **Everything as a service** – Thriving through the change

IT Impact

- IT services was one of the top 3 areas where organizations reported needing the most assistance in meeting ESG objectives over the next two years – organizations will look to define technology and innovation needs to support ESG efforts and effectively leverage their data.
- Certain ESG efforts evade direct measurement. For these measures, identification of suitable proxies for indirect measurement, agreed on by participants at every level of the organization, will help assure continuous data collection and analysis, as well as shared commitment to how an organization's ESG approaches are measured. Indirect measurement should be interpretable and impactful.

Business Impact

- In alignment with prediction 8, organizations may determine that implementation of ESG data management and reporting software is the more sustainable approach to maintaining compliance with coming rules, regulations, and legislation. Multinational companies in particular may find this approach attractive, as ESG data management and reporting software providers report compliance with SASB, TCFD, WEF, CDP, and GRI.
- Referring again to prediction 8, certain ESG efforts evade direct measurement. Business leaders may be tempted to align ESG efforts with available data management and reporting platforms, instead of pursuing less well-defined and easily measured but still impactful ESG efforts. Data management and reporting may cause uncertainty about or reevaluation of what ESG efforts are pursued.

Guidance

- Consider current sustainability and ESG-linked business services and determine where your own organization's strengths and weaknesses might be found. For organizations beginning

their ESG transformation, identification of ESG priorities begins with a clear-eyed view of organizational capabilities and determination of where and what kind of support is needed.

- Although ESG outcomes research shows a generally positive effect on revenue, correlation does not mean causation. Critics of ESG initiatives posit that an interaction effect undermines ESG analyses. For organizations embarking on data-driven ESG and reporting, stay the course, even if data shows weak or no association with financial performance. As measures improve, organizations that have practiced and promoted their ESG initiatives will have done the internal work necessary to meet coming regulatory requirements and consumer expectations.

Prediction 10: By 2025, 45% of CEOs, Fatigued by Security Spending Without Predictable ROI, Will Demand Security Metrics and Results Measurement to Assess and Validate Investments Made in Their Security Program

Over half of CEOs rank cybersecurity threats as *the* most important board priority of not only 2022 but of the foreseeable future. In response to the ever-persistent threat of malware, ransomware, and password attacks, spending on security technologies has topped the list of areas of prioritized organizational spending. And at the top of the list, it remains. CEOs are more concerned about growing expenditures on security than any other area of their organization, and yet only 34% of these same respondents indicate that there are plans to reduce security expenditures. For the remaining 64%, there are not yet plans to rein in security spending (source: IDC's *Worldwide CEO Survey,* January 2022). While this might sound positive for partners offering security services, CEOs are running low on patience and spend cap and will look to justify the increasing proportion of spend going to security services. Leaders will turn to objective, measurable outcomes to improve explainability of expenditures and to prove and improve ROI.

Associated Drivers

- **Cybersecurity and risk** – Scaling and evolving threat environment
- **Meaningful intelligence** – Differentiated decision power
- **Ecosystem-based innovation** – Driving enterprise value

IT Impact

- Although security expenditure is not forecast to slow in the next two years, security spend, in time, will be yoked to objective measures to justify additional expenditures or to maintain current expenditure levels.
- Provision of objective measures will fundamentally change how security services are packaged and sold.

Business Impact

- Although CEOs indicate concern about security spending, it is worth revisiting that for 64% of these concerned CEOs, and there are not yet plans to reduce security expenditures. As businesses prepare for measurable security investment, evaluation of the total security infrastructure may be needed across the organization. For instance, organizations may undertake review of legacy applications and the overall expenditure needed to maintain unsupported technologies.
- These concerns signal an overall shift in how security is regarded. Money spent does not equal strength of security posture. Executives should consider their total enterprise and the most important security considerations to undertake.

Guidance

- Defining the problem will be the first hurdle — because the nature of cybersecurity threats are such that the problem keeps moving; problem definition will have to be broad enough to accommodate fluid change but narrow enough to get to the next hurdle: definition of an outcome. Definition of a suitable outcome will, ideally, lead to identification of objective measures to meet the need for measurable value. AI/ML techniques may assist in the identification of measures.
- Security services should turn to their data now for objective measures, if they haven't done so already. Be ready to show clients longitudinal data on security outcomes to reassure CEOs and provide justification for increased expenditure if necessary.

ADVICE FOR TECHNOLOGY BUYERS

- Objective measurement will define expenditure and investment in the areas of not only privacy, security, risk, and compliance but ESG initiatives as well. When evaluating technology solutions, buyers should consider how the priorities of their own organization in the areas of privacy, security, risk, compliance, and ESG might themselves be expressed through objective measurement and decide whether the measures offered by the technology solution being considered map to your own envisioned organizational measurement goals.
- Now is the time to assess the volume and quality of data collected and the manner in which it is used. Organizations should not be reluctant to let go of data collection streams that have provided little to no value to their organization. Trimming data collection to only specified purposes for use will be positively received by customers and end users and shows a commitment to privacy.
- Many of the predictions here indicate the need for strong technical skills. In addition to the thread of data and measurement running through many of these predictions, buyers may need to view future investment in additional technologies through the lens of available skill sets within their organization — or be prepared to seek new talent or train internally to skill up and prepare for the investments to come.

EXTERNAL DRIVERS: DETAIL

Geopolitical Reality — Sovereignty in the Digital World

- **Description:** In many ways, technology has brought the modern world closer together, yet geopolitical realities are strengthening a widening divide. The Russia-Ukraine War sparked a global crisis and unprecedented reaction. Western democracies and NATO responded with a strengthened and reunified resolve, at least temporarily. China seems to have taken a wait-and-see approach to its heightened cooperation with Russia, but the threat of a bifurcated global landscape — the United States/Europe/West versus China/East (with an advantage in low-cost labor) — has increased dramatically. Control and the reassertion of digital sovereignty is becoming an imperative for many. Even the gig economy is affected due to the impact on hundreds of thousands of highly skilled Russian and Ukrainian tech workers. The influx of millions of displaced migrants creates new demands and strains governments' ability to provide services. Cyberwarfare, already an everyday occurrence, is an increasingly visible component of the projection of nation-state power and the new hybrid war. Social, economic, and political divisiveness and widespread misinformation — driven internally and from cyberactions — fuel the accelerating erosion of "social cohesion." Global competition and

divergence in outer space, with growing commercialization, militarization, and weaponization, is threatening existing systems and complicating collaboration for the common use of space, adding risk to a divided geopolitical reality.

- **Context:** Certainly, the Russia-Ukraine War is the highlight of geopolitical tensions in 2022. IDC's First Take (see *The Impact of the Russia-Ukraine War on the Global ICT Market Landscape – IDC's First Take, March 4, 2022,* IDC #EUR148926122, March 2022) predicts multiple impacts, including significant slowdowns in both countries' IT markets and major operational issues for their businesses, digital skills emigration, exchange rate fluctuations, inflationary pressures, supply chain issues, cybersecurity attacks, digital sovereignty issues, accelerated decarbonization, and Chinese tech vendors focusing on Russia. BlackRock and others consider accelerated "global technology decoupling" as one of the highest risks for 2022 and beyond. So just as globalization and new technologies have provided unprecedented connectedness around the globe, other factors are creating new or exacerbating existing "us versus them" mentalities, often fed by misinformation. And that's just the start of it. Accelerating climate change is being felt in terms of water, fire, crops, migration, and more, whereas the World Economic Forum reports "climate action failure" to be an immediate and severe risk.

Cybersecurity and Risk — Scaling and Evolving Threat Environment

- **Description:** The exponential proliferation of digital transformation, the increasing distribution of data and workflows, hybrid work models, hybrid multicloud, edge computing, and so on have thrust the world onto a new trajectory of digitalization and interconnectedness, accompanied by the increasingly frequent, costly, and damaging occurrence of cyberincidents, sometimes even paralyzing critical services and infrastructure. Data breaches add to the increasing concerns and governmental interventions regarding privacy. Ransomware has increased exponentially, while the texture of attacks is much more targeted and personalized. The dark web is teeming with hacking services that offer comprehensive skills, affordable pricing, and quick engagements. At the same time, organizations find it challenging to respond to cybersecurity incidents due to the severe shortage of skilled professionals. Small and medium-sized enterprises, most affected by the skills shortage, represent a weak link that puts the whole ecosystem at risk. Beyond zero trust approaches, cyber-resilience – the ability of an organization to anticipate, withstand, recover from, and adapt to any threats to its resources – is the new name of the game in not only defending against cyberattacks but also preparing for swift response and recovery when an attack does occur. Artificial intelligence will permeate all aspects of cybersecurity, both in attack and defense. In a deeply connected society, digital trust is the currency that facilitates future innovation and prosperity.

- **Context:** Nation-state attacks – such as NotPetya, originally targeted at Ukraine but which quickly wreaked havoc globally – are increasingly common. Ransomware, the most common cyberthreat today, saw a significant increase in the first half of 2021, with global attack volume increasing by 151% (per the World Economic Forum (WEF) Global Cybersecurity Outlook, 2022). Also, 70% of attacks in 2021 were personalized and targeted, not malware based. Cybercriminals – "black hat" hackers – can be hired to break into social media accounts (for about $230), erase debts, and even change students' grades (for $394-526), according to the same report. In the past several years, the WEF report says that indirect attacks – successful breaches coming into an organization through third parties – have increased from 44% to 61%. And 43% of attacks are aimed at SMBs; only 14% are prepared to defend themselves, according to Accenture. At the same time, 53% of cyberleaders say they have gaps in key talent and skills. IDC reports that 45% of organizations would need to increase spending by 20% to maximize risk mitigation.

Meaningful Intelligence — Differentiated Decision Power

- **Description:** Data is now well embedded at the core of strategic capability for every organization. Data-centric capabilities and infrastructure are now critical to empowering performance-intensive computing and unleashing business value. Meaningful intelligence has moved beyond technical challenges of speed and precision, and organizational intelligence is now expected to enable better decisions, be more efficient, and improve knowledge across the organization. Differentiated decision power leverages real-time insight as the critical capability to keep up with the speed of change. Further, where trust is now paramount in all enterprise activities, ethical data strategies demand a balance between the potential of data and the critical respect for people's privacy and preferences; data and ethical use expectations have reset the bar for privacy, trust, visibility, and responsibility — both with respect to customer stakeholders and in the context of government interventions, regulations such as GDPR, and antitrust actions. Speed and experimentation are now also critical to meaningful intelligence, making digital twins a mainstream strategy that is broadly leveraged in support of measurably differentiated decision power. Data literacy and democratization have shifted organizational focus from straightforward distribution of data to more immersive strategies to find and leverage truly differentiated decision power. Metadata is a critical decision support tool, providing context through workflow linkages and automation. Data optimization and democratization are core strategies to mitigate skills shortages, create data-driven decision value, and deliver strong competitive advantage.
- **Context:** The differentiating power of data is a fact: IDC's August 2021 *Future of Intelligence Survey* indicates that 77.3% of respondents have a senior-level executive responsible for enterprise intelligence (see *IDC FutureScape: Worldwide Future of Intelligence 2022 Predictions,* IDC #US47913321, October 2021). According to IDC's 2022 *Business Intelligence and Analytics Survey,* 40% of organizations have started tracking new KPIs in the past 18 months. IDC's *Future of Intelligence Survey* also indicates that investments in enterprise intelligence (including data culture and democratization) improved employee retention and productivity. Yet the focus on ethics and trust has never been higher, with the European Commission proposing regulation of artificial intelligence systems described as "the first ever legal framework" on AI (**digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence**). If that regulation follows the GDPR path, it will set the benchmark for most global economic sectors. The worldwide data integration and intelligence (DII) software market grew over 10% in 2021, indicating an unprecedented focus on gathering intelligence about data and leveraging data capture that "listens" to database transactions to inform on what is happening in the business (see *Worldwide Data Integration and Intelligence Software Market Shares, 2021: Accelerated Growth in a Digital-First World,* IDC #US47920522, June 2022).

Ecosystem-Based Innovation — Driving Enterprise Value

- **Description:** Innovation has shifted from tactical DX investments that aggregate siloed strategies to holistic, ecosystem-aligned enterprise commitments. Strategic innovation, led by the CEO, boards, and C-suite, now demands clear and measured links between technology innovation and outcomes. IT organizations are seeing a shift in investment priorities, with ecosystem-driven models now materially impactful to strategy, planning, and execution. Ecosystem commitments carry new challenges including consideration of IP protection and cybersecurity, where intelligent innovation has hastened business evolution across the workload, enterprise, and ecosystem control planes. Accelerated digitalization has also forced companies to fundamentally reimagine how they can leverage ecosystem relationships. The enterprise that is positioned to be bold has the most ecosystem leverage, realizing high-value

outcomes to the benefit of both the enterprise and discrete workloads. This next generation of innovation has moved beyond bridging historic gaps and siloed investments with respect to customers, cost, and supply chain; it is now driving long-term and measurable strategic integration of enterprisewide business functions. Successful ecosystem alignment is now leading the C-suite discussion in terms of driving enterprise value and what success looks like. Organizations are investing in creative ways to leverage the ecosystem for both co-innovation and industry leadership.

- **Context:** Trusted ecosystem models are leading organizational response in the drive to digital business, empowering high-value innovation and tangible outcomes that can be delivered at scale. Ecosystem-based, multipartner solutions will drive speed and value through commercial intelligence, operational value, and increased value and differentiation, with insights driven by AI/ML (48%) and value metrics for pricing (49%) at the top of immediate digital business priorities (see *IDC FutureScape Webcast: Worldwide Digital Business Models and Monetization 2021 Predictions,* IDC #US47028620, December 2020). Tech spend by business leaders will overtake spend by IT by 2023 (see *Worldwide Line-of-Business Forecast, 2021–2025: C-Suite Tech Spending in a Digital-First World,* IDC #US48459721, December 2021). The need to reassess use cases and ensure alignment will drive commitment across the "digital dream team." Planning and budget cycles will be driven to become more dynamic in response to evolving ecosystem models. Technology architectures will be driven to support the needs on the broader C-suite for business models of the future (see *The C-Suite Tug of Digital Value in the Future Enterprise,* IDC #US48052721, August 2021).

Mainstream ESG — Sustainability Is Measured and Mandatory

- **Description:** Environmental, social, and governance (ESG) is a globally adopted framework that supports understanding and actions to achieve a better and more sustainable future for all. The United Nations has adopted 17 Sustainable Development Goals, which guide strategies to address global challenges such as poverty, inequality, climate change, environmental degradation, peace, and justice. Pending regulatory changes will require disclosure of sustainability-related risks and opportunities as part of new International Financial Reporting Standards (IFRS). Increasing global thought leadership is pressing ESG as more than just a measure. ESG will be foundational to business purpose and value; care is now a recognized currency and diversity, equity, and inclusion (DEI) affecting the bottom line. Increased scrutiny on both investment and operational sustainability is driving organizations to move from platitudes and posters to actually demonstrating practices that support ESG goals. The focus on measurement demands data and analysis that goes beyond a traditional bottom-line focus, creating new data requirements and exposing new risks. Accuracy, trust, and integrity are drivers for all stakeholders, with these new reporting demands exposing unprecedented reputational risk; ESG data is now viewed on par with financial reporting, so the trust bar is set very high to avoid perceptions of "greenwashing." The shift of sustainability to a mainstream operational requirement is magnifying known data issues, particularly where the required data is difficult to identify, gather, and validate.
- **Context:** Global rules and reporting reality (IFRS sustainability and climate standards in 2022) will drive focus among the C-suite and board of directors, where reporting accountability will rise to the same standards as financial statements. According to IDC's *Global Sustainability Software Survey,* 2022, about 40% of organizations globally cite some form of executive mandate to invest in sustainability tools that is aligned with new industry focus on strategy and regulatory requirements. Measuring and tracking sustainability progress, particularly in the social dimension, will be essential for vendors and ecosystem partners. Internal and external sources for data, analysis, and reporting will be driven to align in support of previously

unmeasured targets; in 2021, more than half of the surveyed practitioners stated that their organization spent more on ESG reporting than they did during the previous year; almost 60% expect spending to further increase by 2024. Recent SEC filings also create impactful financial considerations, such as imposing $1.5 million in fines on BNY Mellon for allegedly misstating and omitting information about ESG (**www.sec.gov/news/press-release/2022-86**).

Work Mode Upheaval — New Models and Leadership

- **Description:** The past two years have seen workforce dynamics disrupted through widespread adoption of hybrid work, accelerated investment in automation, a new focus on employee experience, and the pipeline of talent for both general and IT sector jobs. Automation and augmentation of work have been accelerated, with technologies like AI and RPA making everything from onboarding to secure access much more fluid. Modes of work have raised the bar for skills and driven increased attention to employee experience. Remote and hybrid work has gone beyond a focus on physical workplaces and digital workspaces to spotlight skills, workforce management, automation, changing demographics, and as-a-service talent resourcing. New modes of working are now intrinsic to leadership and organizational resilience and go well beyond traditional staff planning methods. New work models require cross-functional teams – including HR, IT, LOB, finance, and operations – to leverage new disciplines and modes of work aligned with each company's business goals. Automation, multi-disciplinary capabilities, and democratization of data and workflow add operational complexity, with dynamic resource models like "as a service" causing planning and operational changes that extend beyond the work and impact enterprise risk policies. Employee and customer experience leaders must work together to recalibrate culture, augmentation, and space models that are competitive and aligned with more dynamic and refined work models.
- **Context:** Who is working and what workers expect has changed: With a significant number of workers expecting to change jobs in 2022, IDC's 2022 *Future Enterprise Resiliency and Spending Survey* reports that, worldwide, over half of organizations have felt negative effects of worker attrition resulting in increased workload on remaining employees, security risks, and loss of critical knowledge. The recognized criticality of skill retention is pushing major technology sector players such as Microsoft (**www.wsj.com/articles/microsoft-boosts-pay-in-fight-for-talent-11652738482**) and Apple (**www.wsj.com/articles/apple-boosting-pay-budget-for-workers-amid-tight-labor-market-11653527996**) to boost pay in the fight for talent and to visibly respond to inflationary pressures. Work mode dynamics and labor-centric policies and strategies are taking on new power across the business community, with HBR reporting a 658% increase in the frequency of CEO discussions of equity, fairness, and inclusion during earnings calls (**hbr.org/2022/01/11-trends-that-will-shape-work-in-2022-and-beyond**). The C-suite is critical in representing organizational values; 69% of Gen Z workers prioritize diversity, according to a survey by Tallo (**tallo.com/blog/genz-demands-diversity-inclusion-strategy**), and a *New York Times* report indicates that tech firms will be deprioritized based on employee concerns about the sector's moral qualities (**www.nytimes.com/2020/01/11/style/college-tech-recruiting.html**).

Everything as a Service — Thriving Through the Change

- **Description:** Everything as a service (XaaS) is a driver for change in every sector and ecosystem, with real impacts on both the supply side and the demand side of every business. Organizations are adopting as-a-service models at varying speeds out of necessity, but the multidimensional delivery strategies make requirements more complex and impacts less predictable. The shorter decision cycles of on demand are letting industry leaders do things differently, but the commitment models are fundamentally changing. On the supply side,

demand and customer expectations are rising, so suppliers are driven to convert and enable offerings more quickly in a secure services-based model. Change is rampant in terms of accountability and control, as suppliers are more committed in a shared-responsibility model. Buyers are now making decisions based on commitments to measured outcomes in terms of optimization, reliance, and financial models. Architecture and solution strategies are now critical to the service provider, where proprietary systems that are being maintained or migrated can materially impact the efficacy of the as-a-service solution. Nonproprietary requirements are serving as a starting point for integration, so solutions and vendors are pressed to be dynamic and interchangeable. Leaders are challenged to find new financial, operational, and governance models that support success in an iterated move to as a service. Critical factors for organizations to thrive through the as-a-service change landscape include solution control, contractual clarity on roles and responsibility, and accountability alignment including geoeconomic assurance and data sovereignty risks.

- **Context:** Typical 2020 enterprise workloads had 5 to 15 dependencies; that is expected to be 6x greater by 2025 (see *IDC FutureScape: Worldwide Future of Digital Infrastructure 2022 Predictions,* IDC #US47441321, October 2021). According to the IDC worldwide forecasts, CAGR in spending is materially shifting toward as-a-service constructs over the next three years, with infrastructure as a service projected to be up 21%, dedicated cloud projected to be up 31%, and the services to support as-a-service investments projected to be up 16.9%. Software as a service is projected to have CAGR at 15.3%. To support an as-a-service foundation, software-defined everything will drive attention to policy automation, programmability, and analytics instead of hardware-specific configuration and control. There is also extensive evidence that the as-a-service segment is building in dominance: SaaS-based APM solutions are expected to increase at a five-year CAGR of 23.7% compared with 2.8% for on-premises solutions (see *Worldwide Application Performance Management Software Forecast, 2021-2025: Market Pivots to Observability,* IDC #US48353021, November 2021); SaaS-based network security solutions are creating traction, estimated to bring greater than 7% annual growth in the sector (see *Worldwide Network Security Forecast, 2021-2025: SaaS Adoption Brightens Market Outlook,* IDC #US48185721, September 2021); the IoT security market, enabling autonomous operations across all segments, has a CAGR of 16.3% (see *Worldwide IoT Security Forecast, 2021-2025: Critical Applications Accelerate Demand for Contextualized Security,* IDC #US48347020, December 2021).

LEARN MORE

Related Research

- *Critical External Drivers Shaping Global IT and Business Planning, 2023* (IDC #US49631122, October 2022)
- *Future of Trust: Battling Data Discovery Confusion* (IDC #US49631721, September 2022)
- *IDC PlanScape: Future of Trust -Implementing Automated Compliance Management for Better Efficacy and Efficiency* (IDC #US49617722, September 2022)
- *Worldwide Security Governance, Risk, and Compliance Software Forecast, 2022-2026* (IDC #US49627922, September 2022)
- *What Security Services are Seeing Increased Funding?* (IDC #US49353722, September 2022)
- *Trusted Cloud Vendors: Features and Criteria Most Important to Buyers* (IDC #US49616222, September 2022)
- *Actionable ESG Strategies for the CIO* (IDC #US49675622, September 2022)

- *Collaboration Security: A Security Discipline Born from Hybrid Work* (IDC #US49535122, August 2022)
- *IDC PlanScape: Future IT Strategies to Ensure and Manage Compliance Ecosystems* (IDC #US49536422, August 2022)
- *The SOC and the Mainframe: The Requirement for Analytics* (IDC #US49534922, August 2022)
- *Worldwide Cloud Workload Security Forecast, 2022-2026: Complexity Drives the Market Up and to the Right* (IDC #US49522022, August 2022)
- *Worldwide Data Privacy Compliance Software Forecast, 2022-2026* (IDC #US49422221, July 2022)
- *Future of Trust: Creating Trust Through Data Privacy Compliance* (IDC #US49086521, May 2022)
- *Worldwide ESG Business Services Forecast, 2022-2025* (IDC #US48579022, May 2022)
- *Analysis of Sustainability Management Solutions* (IDC #US48578622, April 2022)
- *IDC PlanScape: Data Privacy (CCPA/GDPR) Regulatory Compliance* (IDC #US45692219, December 2019)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com