Publication date:
August 2020
Authors:
Maxine Holt, Tanner Johnson

Security Transparence and Assurance in a 5G World

In this new cyberthreat landscape, security transparence and assurance are more essential than ever

Brought to you by Informa Tech

Contents

Executive summary

Catalyst

Over the past century the world has witnessed enormous leaps in technological capabilities, including the dawn of the digital age that gave birth to the global internet. The speed of adoption of interconnectivity and mobility today sees nearly five internet connected devices for every human walking the earth. While these achievements are monumental and revolutionary for organizations, and essential for swift and convenient access to information for individuals, they do not come without substantial risks. As the fifth generation (5G) of cellular network connectivity begins to take shape, and introduces functionality that scales new heights, it will simultaneously expand the cybersecurity threat landscape to the largest ever known.

Omdia view

While organizations' and individuals' innate desire for greater access to data appears unquenchable, the protection and security of that information is frequently an afterthought. The very foundations of the infrastructure for the modern internet were not built with security in mind, and thus these measures have often been introduced in an inefficient and piecemeal manner. The speed of technological advancements, along with demands surrounding time-to-market for new products and services under the umbrella of "digital transformation," means that this approach lingers. Efforts to build security into a system after its creation gives rise to complex security challenges that are often more costly and time consuming than baking it into the development process. The sheer scale of 5G functionality demands that this habit is broken prior to the global adoption and implementation of 5G connectivity.

Key messages

- 5G offers countless opportunities for further digitalization, which itself has been underway for many years.
- Comprehensive assurance in security is essential throughout the entire ecosystem in the 5G era – from IoT devices to 5G networks, through to regulation and operations.
- To be truly effective, this will demand collaboration and coordination from all parties involved, as well as regular assessments to meet evolving threats.

Digitalization has been underway for many years

Digitalization continues to be pursued to advance the organization

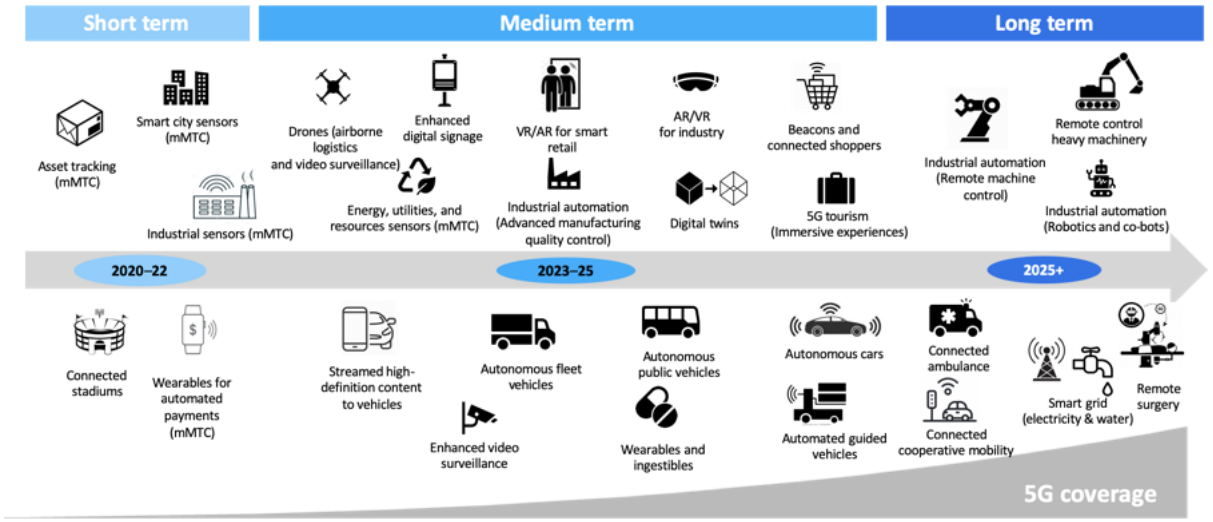
Digital transformation, or digitalization, is not a single project. It is an ethos – an approach steered toward continuously translating business challenges into a series of technology-focused initiatives and projects to drive the organization forward.

Some enterprises have formal digitalization projects, whereas others take a more ad hoc approach. What all the projects have in common, however, is that the technology being used opens the organization to greater opportunities, and greater risks, than previously.

Security needs to be by design

Far too often, risk and security strategies around digitalization projects and initiatives have been reactive in nature. This must change: the sheer volume of devices engaging in simultaneous connections via 5G technology demand proactive measures be taken before widespread deployment takes place (see Figure 1).

Figure 1: 5G coverage opportunities



Source: Omdia

While the current limitations for simultaneous device connections on fourth-generation cellular technology (4G LTE) can support around 4,000 devices per square kilometer, 5G capability will allow for 250 times that number of connections, or roughly 1 million devices, within the same perimeter. Additionally, the exponential increase in simultaneous connections will correspondingly be met with a proportional increase in bandwidth and speed.

While connectivity can usher in advancements in convenience and capability, the stark reality is that every component connected to the global internet introduces a potential node of compromise. As the volume of 5G connected devices continues to grow, so too do the opportunities for unauthorized interception or access.

Adding further complexity to the issue is that widespread adoption of connectivity, and the reduced costs associated with its application, have removed any previous limitations on the forms these devices can take. This means that cameras, thermostats, building automation, heating, ventilation and air conditioning (HVAC) systems, televisions, point-of-sale systems, fridges, printers, vehicles, and even toothbrushes are now internet accessible (for better or worse).

While the amount of data being generated, transmitted, received, analyzed, and categorized will open opportunities for truly innovative technological advancements in automation, it poses a huge cybersecurity challenge that must be permanently considered, assessed, and addressed in near real time.

Changing working patterns will also push digitalization efforts

The unprecedented complexities introduced as a result of the COVID-19 pandemic have placed greater emphasis on continued evolution and development of digitalization efforts. With more people relying on technology to work, shop, and socialize than ever before, the move to next-generation technologies, services, and strategies is accelerating at an unprecedented rate.

A significant increase in demands surrounding remote working, plus clear evidence that organizations are reducing their real estate, means that digitalization projects will focus on making their current transitional offerings more permanent options. Ultimately, this will demand a long-term assessment of the various risks that digitalization efforts can introduce to an organization's ecosystem, as well as additional resources surrounding asset management, data governance, and compliance requirements.

While the world begins to settle into the "new normal" of a post-COVID-19 era, the ramifications of the decisions made now will influence the global market for years to come. Traditionally, investment in security capabilities often followed ever-changing network traffic requirements. This trend is projected to not only continue, but demand is likely to grow exponentially as the number of concurrently connected devices increases year over year, resulting in a cascading effect of new devices being introduced to an already enormous threat landscape. In turn, this will introduce increasingly complex challenges for security functions to navigate.

Comprehensive security assurance is needed

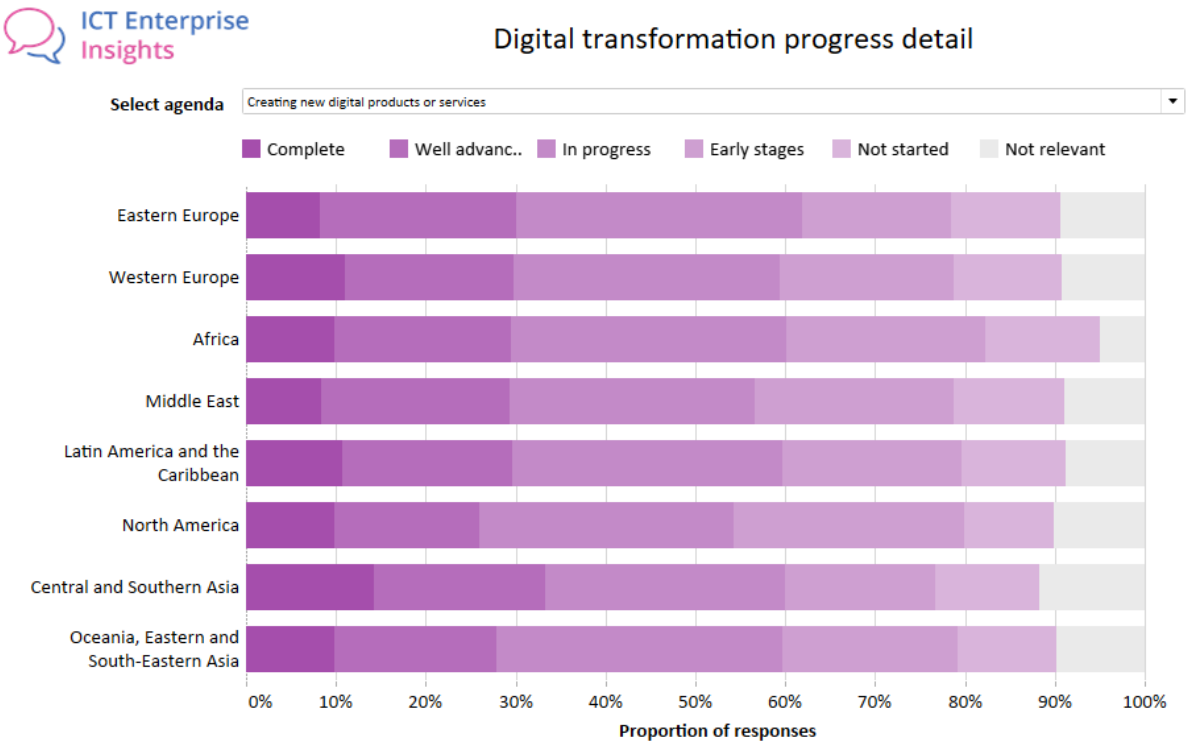
Security assurance in line with risk appetite

At the heart of cybersecurity is the need to protect the confidentiality, integrity, and availability (CIA) of organizational information: the starting point for security assurance.

For many (but not all) enterprises, organizational governance drives security governance. Appropriate strategies are put in place to provide security governance in line with objectives, "setting the tone" for security and cybersecurity within the organization. In turn, this drives security assurance focused on protecting the CIA of information. 100% secure systems do not exist; instead, organizations seek assurance that any associated risk has been addressed appropriately and adequately – in line with risk tolerance.

However, Omdia's ICT Enterprise Insights Survey suggests that organizations are struggling with security assurance, with significantly fewer than 40% having a complete or well-advanced approach to cybersecurity and digital risk (see Figure 2).

Figure 2: A proactive approach to cybersecurity and digital risk

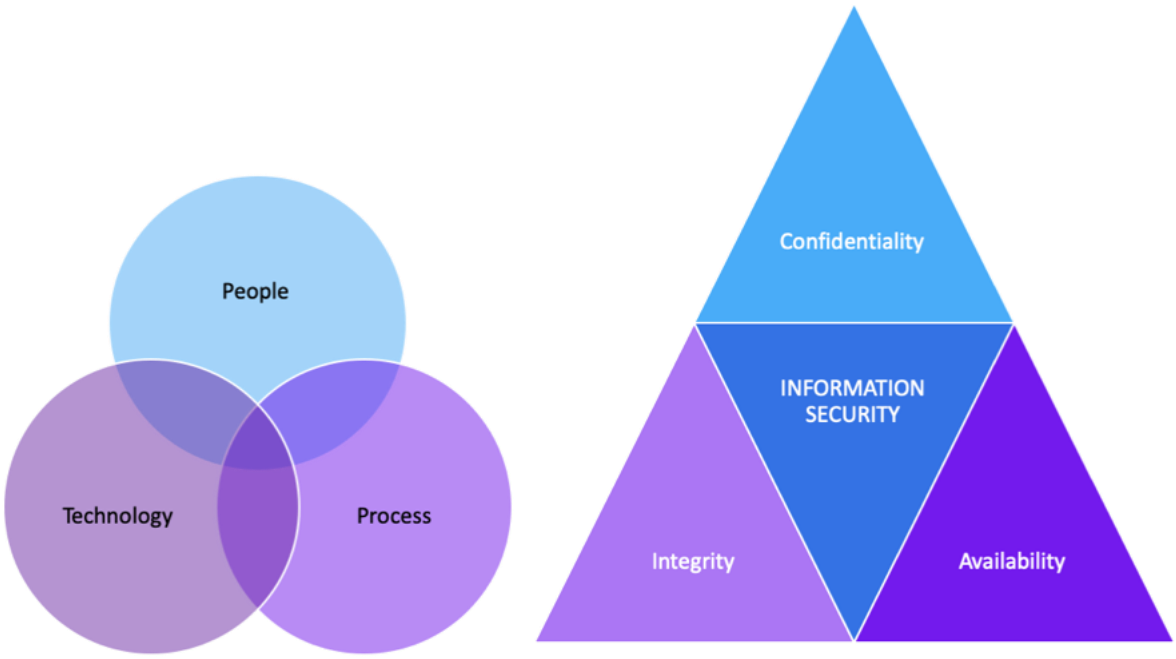


Source: Omdia

Europe is behind its North American counterparts when it comes to having a proactive approach to cybersecurity and digital risk.

Addressing digital risk is rarely one individual's responsibility, as such an endeavor usually demands a team effort. Thinking about digital risk in terms of people, process, and technology to protect the CIA of information is a combination that many organizations will recognize (see Figure 3).

Figure 3: People, process, and technology combine to protect the CIA of information



Source: Omdia

People, process, and technology combine to prevent security incidents and breaches, and protect the CIA of information:

- **People** controls include security and cybersecurity education and awareness, as well as changes to people's behavior to make the organization and its information more secure
- **Process** controls are there to be followed and not circumvented
- **Technology** controls are the software and services in place to work with people and process.

On its own technology is insufficient to protect the enterprise, but it is a crucial component in cybersecurity.

Security assurance involves managing the security risk with the appropriate controls to achieve acceptable levels.

Achieving acceptable assurance

Good practice for security assurance involves both a top-down and bottom-up approach. Properly assessing risk using the standard equation of likelihood multiplied by impact enables the organization to see that the risk has been accepted, mitigated, transferred, or declined – thus providing security assurance.

However, there is never a single approach to security. Security controls are delivered in layers to prevent security incidents and breaches, and protect the CIA of information. The more security-mature an organization, the greater the breadth and depth of the layers of protection (without making it too complex to manage). Developing and maintaining a security-positive culture, where every individual takes responsibility for their contribution, is a part of security assurance that is not easily quantified but is visible in the day-to-day behaviors of individuals.

Cybersecurity standards are likely to be reviewed in light of the development of 5G networks. Consideration must be given to how the loss of each individual application, asset, or function might affect the wider network. The greatest risk could be faced by the user, the IoT device data, the manufacturer, or beyond. Only by understanding the risk can the storage of applications and assets on these devices be assessed.

Digitalization relies on security assurance

While implementing security from the onset of technological developments is finally being recognized as an essential investment rather than a luxury, comprehensive cybersecurity demands a more holistic approach than historically practiced.

One potential ambition is a drive toward a regulatory framework that covers the complexity of the supply chain, from IoT manufacturers to software solutions. To achieve this, regulatory bodies and cybersecurity experts will need to work together to create systems to appropriately manage information and digital technologies end-to-end.

Effective security governance, risk assessment, and compliance requirements will ultimately steer security assurance through policy deployment. The paradigm shifts that COVID-19 has introduced to the world have accelerated the removal of the traditional concept of a controlled perimeter, as more organizations and entities virtualize their workloads and interactions. The loss of this perimeter demands that security be assured through a top-down or bottom-up endeavor.

Transparency is essential for security assurance

Unfortunately, many security regulations are diversified along industry lines as enterprise, financial, medical, and industrial entities have circumstances that demand unique considerations and approaches. Examples include the Health Insurance Portability and Accountability Act (HIPAA) in the US for the medical industry and the EU's Network and Information Systems (NIS) Directive for critical infrastructure. Additionally, the diversity of connected components introduces an equally wide range of device owners and users, often spread across multiple geographic locations within an organization.

These considerations add a further dimension to security assurance, which must be incorporated in reporting. These entities want assurance on the protection of information and systems when being transmitted, handled, or delivered by external suppliers, and that these suppliers and partners be open with their security assurance – and reserve the opportunity to test or audit them directly.

Advanced security controls from the outset

These added layers of complexity and depth will demand advanced security controls that are properly developed from the outset and are designed in accordance with evolving risk assessment

requirements. While risk assessments can be challenging, they are essential in establishing comprehensive security priorities by outlining exactly what the “crown jewels” are within an organization that demand the greatest protection. Traditional calculations of these risks revolve around the likelihood and impact of a potential compromise to determine the risk and, correspondingly, the security controls that must be applied (see Figure 4).

Figure 4: Risk calculations determine necessary security controls

Source: Omdia

With the number of access points increasing substantially through the deployment of 5G, assessing risk and developing the appropriate security controls can become quite an elaborate challenge to address.

Furthermore, these controls need to be designed and built with diverse groups of people, processes, and technologies in mind. However, technology alone cannot address the evolving security risks that will be introduced within the era of 5G – collaboration, transparency, and openness are required to defend, protect, and respond to evolving threats.

Building trust and security at ZTE in a 5G world

Security assurance today at ZTE

The hurdles within the current landscape of connected devices are numerous and will only be exacerbated if not addressed effectively during the upcoming deployments of 5G technology. Recognizing this, ZTE is devoting resources on researching proactive solutions to the future challenges of global 5G deployments.

Standards and certifications

One of the primary methods an organization can use in its efforts to promote security assurance is attaining compliance with various security standards and certifications. ZTE has achieved the following:

- ISO 27001 (information security management): This certification was first awarded to ZTE in 2005 and is updated annually. According to the International Organization for Standardization (ISO), using the ISO 27001 suite enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details, or information entrusted by third parties.

- ISO 28000 (specification for security management systems for the supply chain): ZTE has incorporated cybersecurity requirements in its business processes, including supplier and material certification and management, manufacturing, storage, transportation, and repair processes. This certification was awarded to ZTE in 2017.

- ISO 22301 (business continuity management): This certification, awarded in 2019, is a process to examine various risk factors and the potential fragility of the business when faced with unpredicted situations. ZTE has established a business continuity mechanism and a set of solutions based on ISO 22301 to ensure that the company can maintain the delivery of products and services.

- ISO 27701 (privacy information management): Awarded in 2020, this covers the provision of R&D and maintenance services of 5G new radio (NR) and user management engine (UME) systems. ZTE's data protection compliance system is covered by the certification, focused on international information security standards.

- Customs Authorised Economic Operator (AEO) Trade Security: According to the European Commission, the EU established its AEO concept based on the internationally recognized

standards and is a partnership program between the customs authority and the AEO. This implies that there must always be a relationship between customs and the applicant/AEO. This relationship must be based on the principles of mutual transparency, correctness, fairness, and responsibility.

- ZTE invests in relevant product assessments and certifications, such as the GSMA Network Equipment Security Assurance Scheme (NESAS), Common Criteria, and 3GPP, and has adopted the industry-recognized people, process, and technology (PPT) approaches to build its corporate-wide cybersecurity assurance system.

- In June 2020, ZTE was listed by GSMA as one of the mobile network equipment vendors that has undergone an assessment and independent audit of its development and product lifecycle processes to demonstrate how security is integrated into its design, development, implementation, and maintenance processes. The summary report shows that ZTE's RAN and Core Network product line's development and product lifecycle processes meet the requirements of NESAS.

ZTE continues to develop 5G patent applications and contribute to global standards relating to 5G.

Although standards and certifications do not guarantee cybersecurity, adherence and annual updates provide organizations with external recognition of a proactive approach toward security assurance.

Cybersecurity labs

ZTE has developed cybersecurity labs across Europe (Brussels, Belgium, and Rome, Italy) to provide a wider range of access to the external verification of ZTE's products, services, and processes.

In these labs (also located in other regions of the world) external parties can conduct various in-depth security evaluations, including source code reviews, security design audits, procedural document reviews, and penetration testing on the entire line of ZTE's 5G products. These external parties include regulators and clients. In 2020, ZTE announced the establishment of a 5G industrial Internet Security Lab in Nanjing, China.

Layered approach

ZTE acknowledges the need for a comprehensive and layered approach for effective information security, and has implemented a series of layers for its cybersecurity specification system:

- **Layer 1 – General policy for cybersecurity**: Effectively "setting the tone" for cybersecurity in the organization.

- **Layer 2 – Cybersecurity management specifications and procedures**: Supporting the operation of the overall general policy for cybersecurity and the policies within it.

- **Layer 3 – Cybersecurity guidelines**: Providing more detail for applying the specifications and procedures.

- **Layer 4 – Cybersecurity records**: Creating an auditable trail of implementation processes and results.

ZTE comments that during the practical implementation of the above layers of specifications for individual products and projects, the corresponding results and records are captured (Layer 4) and made available to relevant parties for auditing.

Baking security into the product development lifecycle

The challenges that come from bolting security onto a product rather than baking it in from the onset are recognized by ZTE and, following on from the cybersecurity specification system, the company's product development lifecycle has security as a fundamental, non-negotiable component. ZTE has established a cybersecurity assurance mechanism that covers a wide range of areas, including product development, supply chain and manufacturing, engineering services, security incident management, verifications, and security audits.

Such benchmarks help to bolster security assurance by ensuring that all security solutions are reviewed from a wide range of perspectives, guidelines, and policies to meet evolving market demands. ZTE brings in people, process, and technology approaches to build its corporate-wide cybersecurity assurance system.

Security in 5G product development

ZTE seeks to continue this evolutionary process into the upcoming deployments of 5G mobile edge computing (MEC) telecommunications. 5G functionality will forever alter the IoT landscape as the technology connects architectural technological infrastructure across a wide range of industries. This will allow for mobile network connections to advance beyond just person-to-person contact, toward machine-to-machine communications. Such capabilities can simultaneously introduce additional threats, because many of the components targeted by adversaries are located at the network edge, making MEC node security vital.

Product Security Incident Response Team

A Product Security Incident Response Team (PSIRT) has been established at ZTE. The PSIRT works to identify and analyze any and all security incidents by tracking the handling processes, and coordinates with the respective stakeholders to disclose any vulnerabilities as quickly as possible with the objective of minimizing their respective impacts. With this in mind, ZTE has joined the Forum of Incident Response and Security Teams (FIRST) and has been named a CVE Numbering Authority (CNA).

ZTE security roadmap

With decades of engagement in the telecoms industry, ZTE recognizes that effective security demands diligence, which requires that an organization's security strategies and policies are reviewed and updated regularly. This mindset is perpetuated through the evolution of its security roadmap, which involves consistent and routine assessments for security assurance baked into its

own product development lifecycle. Additionally, ZTE invites transparency through collaborative efforts among professional organizations and certification authorities.

The company seeks to continue to bolster its efforts by adopting three lines of a defensive cybersecurity governance model in order to implement and review cybersecurity solutions:

- **First line**: The business unit implements self-management over the cybersecurity of its products, using 1,500+ security specialists.
- **Second line**: The Product Security Department utilizes three cybersecurity labs, implementing independent security assessment and supervision, currently with over 80+ employees in China and Europe.
- **Third line**: ZTE's Internal Control and Audit Department, customers, and external parties audit the effectiveness of the first and second line.

The objective of this approach is to provide in-depth defense by not only applying multiple layers of internal organizational review, but by inviting cooperation through the promotion of collective scrutiny from other entities. This multi-layered approach is also designed to help address the "single point of failure" scenario. The three lines of defense model, plus PSIRT and the cybersecurity labs, present ZTE's view on the value of transparency and openness in cybersecurity.

Cybersecurity is a global challenge to which all players must contribute in order to achieve and maintain a secure and reliable 5G network with high performance. ZTE believes that its existing security capabilities and experience (standards and certifications, PSIRT, cybersecurity labs, and layered approach), alongside its roadmap, demonstrate a mechanism for collaboration, transparency, and openness to address the upcoming security risks and challenges that will undoubtedly be introduced in the 5G world.

Appendix

Authors

Maxine Holt
Senior Research Director, Cybersecurity
maxine.holt@omdia.com

Tanner Johnson
Senior Cybersecurity Analyst, Connectivity and IoT
tanner.johnson@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia 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 global base of analysts, 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 profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms 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, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer