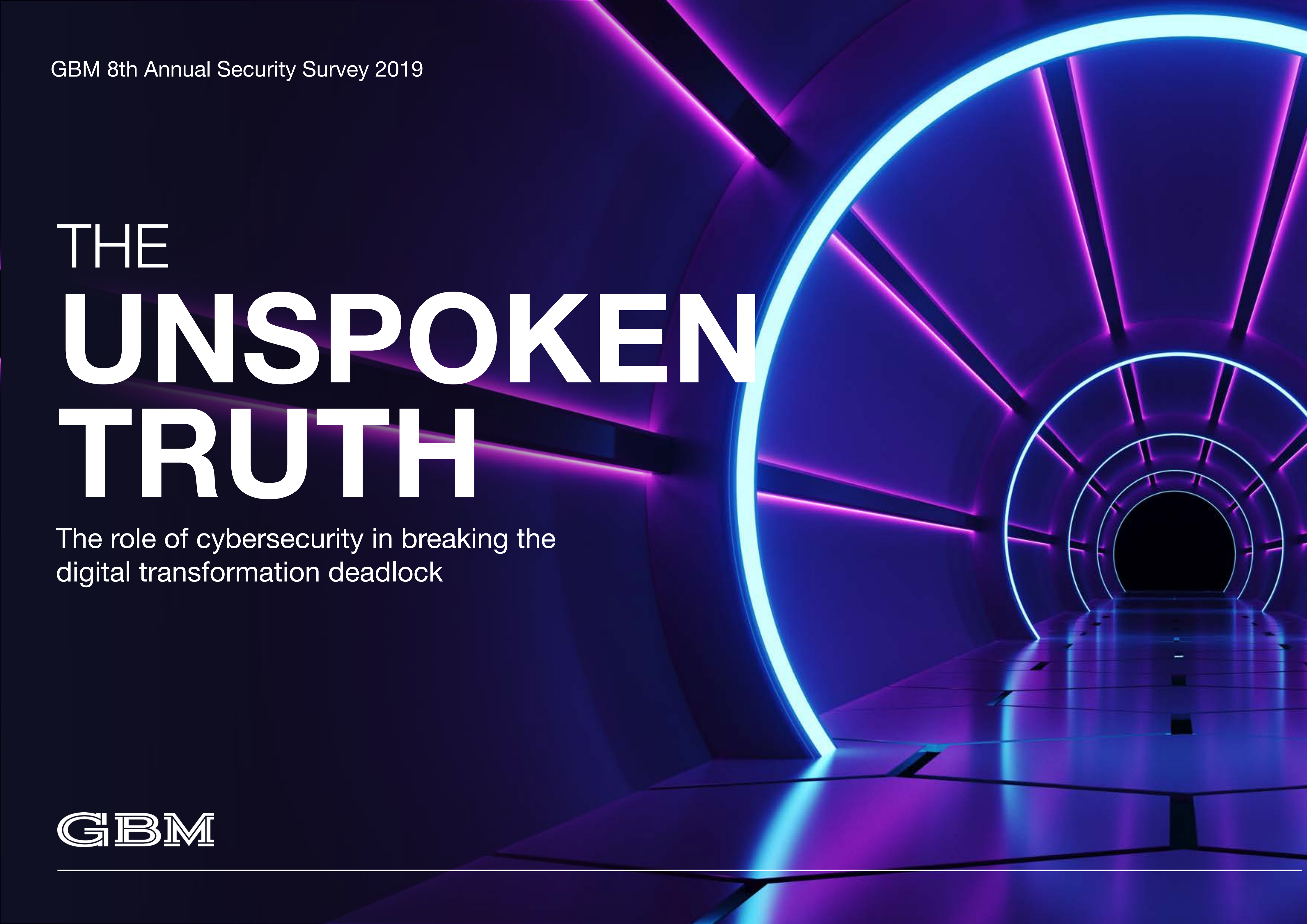
GBM 8th Annual Security Survey 2019



THE UNSPOKEN TRUTH

The role of cybersecurity in breaking the digital transformation deadlock

GBM

CONTENTS

FOREWORD

Data is growing in both value and volume. That is inspiring businesses to digitally transform, in order to tap the value of data and compete in the changing marketplace. However, digital transformation also exposes data to greater security risks, and cyber criminals are also keen to exploit its value through theft, fraud, ransomware and many other kinds of cyber-attacks. This gets organizations trapped in a "digital deadlock", which keeps them from successfully transforming. So, how can organizations embrace the opportunities of digital transformation, while keeping themselves, their data and their customers protected?

The answer is, naturally, through effective cybersecurity. Yet designing and implementing a security strategy and architecture to meet the needs of the data-driven organization might be more difficult than many realize. Are organizations in the Gulf region prepared to meet the security challenges of digital transformation?

For the eighth year in a row, we asked them directly. With a focus on digital transformation, the GBM 8th Annual Security Survey gathered insights from more than 750 cybersecurity and IT professionals based in the United Arab Emirates, Oman, Kuwait and Bahrain. This white paper presents the results, provides a comprehensive review of the cybersecurity landscape, and makes key recommendations for organizations who want to break the digital transformation deadlock and successfully transform their business.

Digital transformation brings many security challenges. Whether you are planning your journey or have already started it, this white paper can help you take the next step.

Hani Nofal
VP of Intelligent Network Solutions, Security and Mobility

Hani Nofal

INTRODUCTION

We are living in an era of digital disruption. Multiple industries are being disrupted, or fear being disrupted in the near future. Business models are evolving to cater to the dynamic markets and digital transformation that seems to be the answer to changing business models. Digital transformation is rapidly becoming a key priority in most industries, as organizations adapt to changing markets by leveraging technologies to build IT-centric business models. In general, organizations are using digital transformation to reach their goals of achieving greater agility, improving operational efficiency, improving customer experiences, and developing new revenue streams.[1]

"Speed" is the name of the game now. Customers want services to be delivered seamlessly, quickly and efficiently with minimal human intervention. Technology is maturing to be able to deliver these services online and organizations are restructuring their business to remain relevant in their markets. Customer experience is a primary catalyst for organizations undergoing or planning a business transformation.

[1] Breaking the Deadlock and Accelerating Digital Transformation, An IDC Whitepaper Sponsored by GBM

When we look at industry-specific examples, we see that governments and public sector organizations are working to redesign citizen, resident and tourist experiences in transformation-ripe sectors such as transport, public safety, and utilities. Smart parking initiatives, smart meters to improve resource efficiency, and smart video surveillance to improve public safety are typical examples.

In banking and finance, where improving back-office process efficiencies through increased automation is the priority, transformed digital experiences are delivering results; mobile applications are enabling customers to perform fast online transactions, while virtual assistants allow customers to use natural language instead of IVR menus. Many sectors, e.g. government services, banking and finance, are pushing for paperless offices, reducing numbers of physical locations and front desk employees to by delivering more services online. Organizations are also striving to reduce time to market for new products or services, improve efficiencies, reduce errors and optimize their operations.

[2] ibid

THE DIGITAL DEADLOCK

As well as being at different stages in their digital transformation journey, organizations are not all at the same level of digital maturity. Many are able to execute relatively small digital projects within departmental or functional silos; a large proportion of organizations are unable to move beyond these ad hoc digital projects and achieve scale. They are stuck in a “digital deadlock”, which is a common occurrence and is estimated to affect nearly 60% of organizations. The key technology barriers that lead to digital deadlock are:

1. **Lacking the agile, secure technology infrastructur**e that is required to achieve scale,

2. **Information silos** that prevent organizations from effectively utilizing their data,

3. **Manual, misaligned, and outdated business processes** that result in unpredictable outcomes.

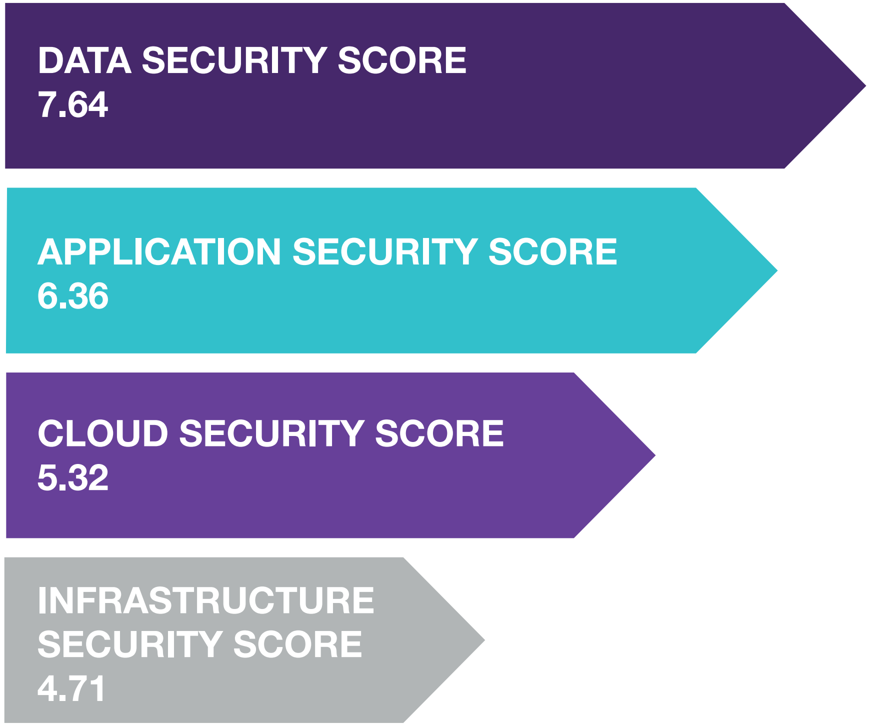
Security is a critical component in all these technology barriers, and with this whitepaper our aim is to highlight the role of cybersecurity in digital transformation and to explore how security helps break the deadlock and accelerate organizations’ transformation journeys.and with this whitepaper our aim is to highlight the role of cybersecurity in digital transformation and to explore how security helps break the deadlock and accelerate organizations’ transformation journeys.

DIGITAL TRANSFORMATION IN THE GULF

The results of the GBM 8th Annual Security Survey, which gathered insights from more than 750 security and IT managers and professionals from organizations based in the UAE, Kuwait, Oman and Bahrain, reveal four leading priorities around digital transformation in 2019. Process automation was the core initiative for 69% of the respondents. Moving to cloud was the second-most important initiative, prioritized by 28% respondents. Migration to new on-premise infrastructure and new on-premise applications were the lead priorities for the remainder of respondents.

Organizations in Gulf countries have long been targeted by cyber threats, and security incident numbers have grown in recent years. In a survey conducted by GBM and IDC, 86% of Gulf organizations were found to be either planning or in the midst of a digital transformation journey. However, it was striking to note that only 15.4% of the responding Gulf organizations involved their security teams in their digital transformation processes. This is a concerning trend that may represent an obstacle to the success of digital transformation projects in the Gulf region. In this paper we discuss why cyber security is essential for digital transformation success and report the complete results from our survey

According to GBM's 8th Annual Security Survey, the Top 4 most challenging security domains in the digital transformation journey are:



DATA SECURITY SCORE 7.64

APPLICATION SECURITY SCORE 6.36

CLOUD SECURITY SCORE 5.32

INFRASTRUCTURE SECURITY SCORE 4.71

DIGITAL TRANSFORMATION AND CYBERSECURITY: FRIENDS OR FOES?

Digital Transformation is led by different teams in different organizations. At some businesses, the IT team is responsible for transformation while at others it is business managers. Few organizations realize the complexities involved or the need to include all stakeholders in the process; and unfortunately, many organizations undervalue the role of security in their journey. digital transformation activities, whether they include process automation, re-engineering or cloud migration, mostly increase the risk of threat exposure for the organization. Speed is one of the fundamental objectives of digital transformation, and haste to transform can very easily lead organizations to compromise on security controls and overlook the underlying risks. Identifying risks and quantifying the impact becomes much harder when important stakeholders (e.g. security, business, IT, procurement, projects, and governance) are absent from the journey.

An IBM study reveals that the rush to achieve digital transformation increases risks of a data breach (by 72%), as well as risks of a cyber-attack or threats to high value assets (by 65%).[2]

> **A security breach can sometimes bring disastrous results ranging from CXO resignations to erosion of market share, brand reputation loss, drops in profitability or all of them together. Simply put, the stakes are too high to ignore security risks when digitally trans-.forming**

Some of the technical security challenges that arise during digital transformation are as follows.

1. Expanded attack surfaces – Cloud, Social and Mobile

As more business processes and information are digitized as applications, data and workloads, opportunities for cyber-criminals to attack organizations grow. Digital transformation opens up new network entry points, such as cloud, social and mobile, resulting in increased and diverse risks. These new platforms stretch organizations' boundaries, give rise to new threats, and require specific approaches to security. Adopting new digital platforms is fundamental to digital transformation; however, organizations should ask themselves whether their security strategy or program is ready for the new risks, skill requirements and compliance needs they bring.

Internet-connected devices are also used in critical infrastructure and services, such as the energy grid, emergency healthcare and transport. With the increasing number of connected "things" estimated to reach 41 billion in the next 5 years with 5G adoption, these connected devices are at risk from cyber-attacks that could have severe consequences, ranging from disruption to daily activities to loss of life. As organizations increasingly depend on digital technologies, these risks will grow.

2. Data is the new oil

The impacts of a security incident, such as a data breach, are greater today than ever before. Data is a valuable resource that is highly attractive to criminals, while consumers are attuned to impacts on their privacy. Organizations are quickly realizing the value they can gain by analyzing the data they have (such as customer behaviors, patterns, markets and so on) and are prioritizing implementation of data analytic solutions. These solutions often include data lakes that improve data visibility and business decision making. With digitization, critical data is stored and transferred across organizations' networks; a strategy to protect data is therefore a must. The task of securing data is made more complicated by:

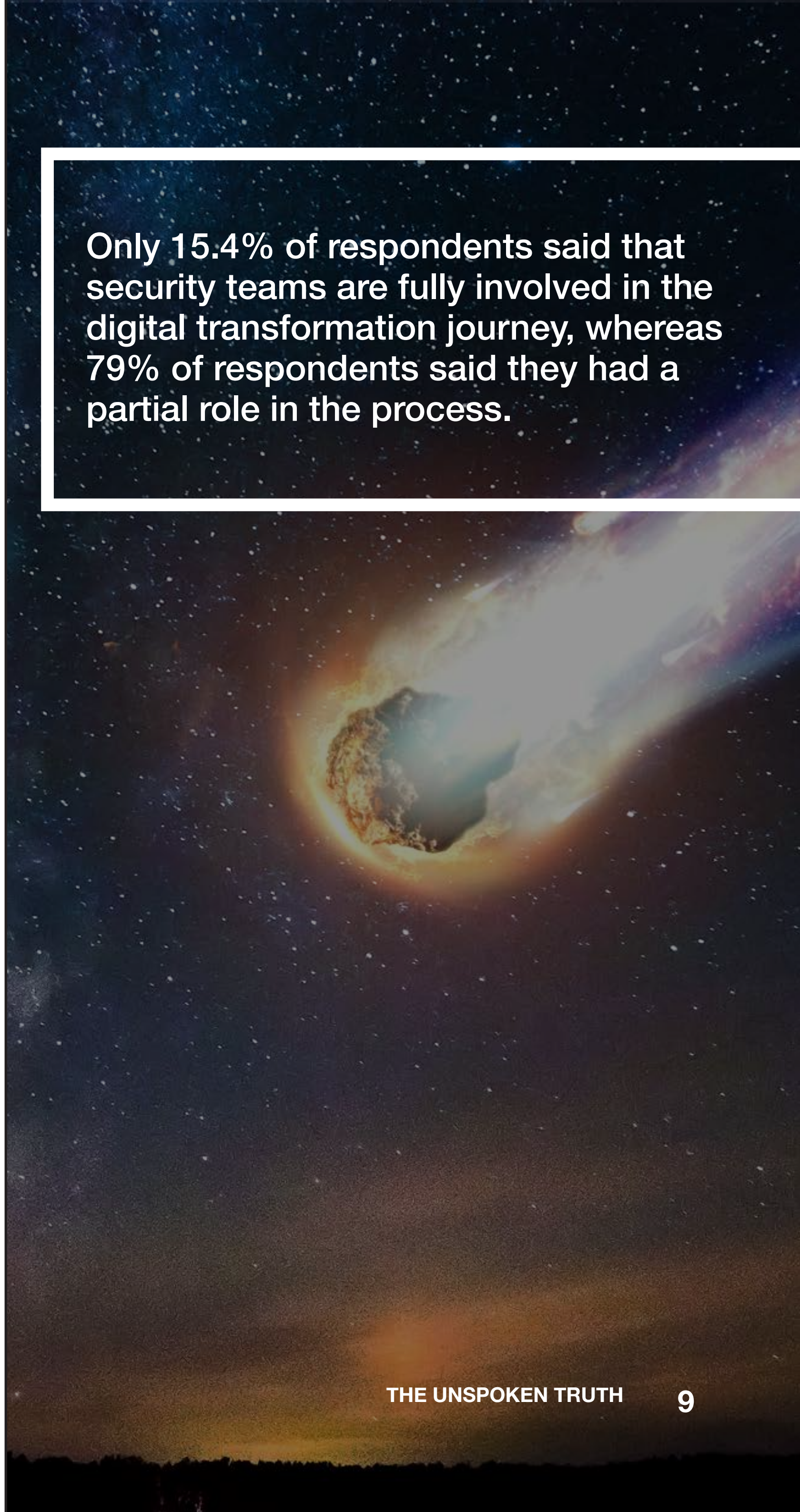
- the huge and growing size of the data volumes, both structured and unstructured, residing on premises or in the cloud
- the need to make data accessible from any location, at any time and any device.

[2] Bridging the Digital Transformation Divide: Leaders Must Balance Risk & Growth, Ponemon Institute, March 2018

The severity of the risks posed by cyber-threats, as well as the importance of digital technologies and data security to business success, make cybersecurity a boardroom issue rather than a business operations issue. Organizations will be vulnerable until they make security a key stakeholder in the digital transformation journey.

However, responses to the GBM 8th Annual Security Survey indicate that security teams have only a very small degree of involvement in creating organizations' digital transformation strategies. Only 15.4% of respondents said that security teams are fully involved in the digital transformation journey, whereas 79% of respondents said they had a partial role in the process.

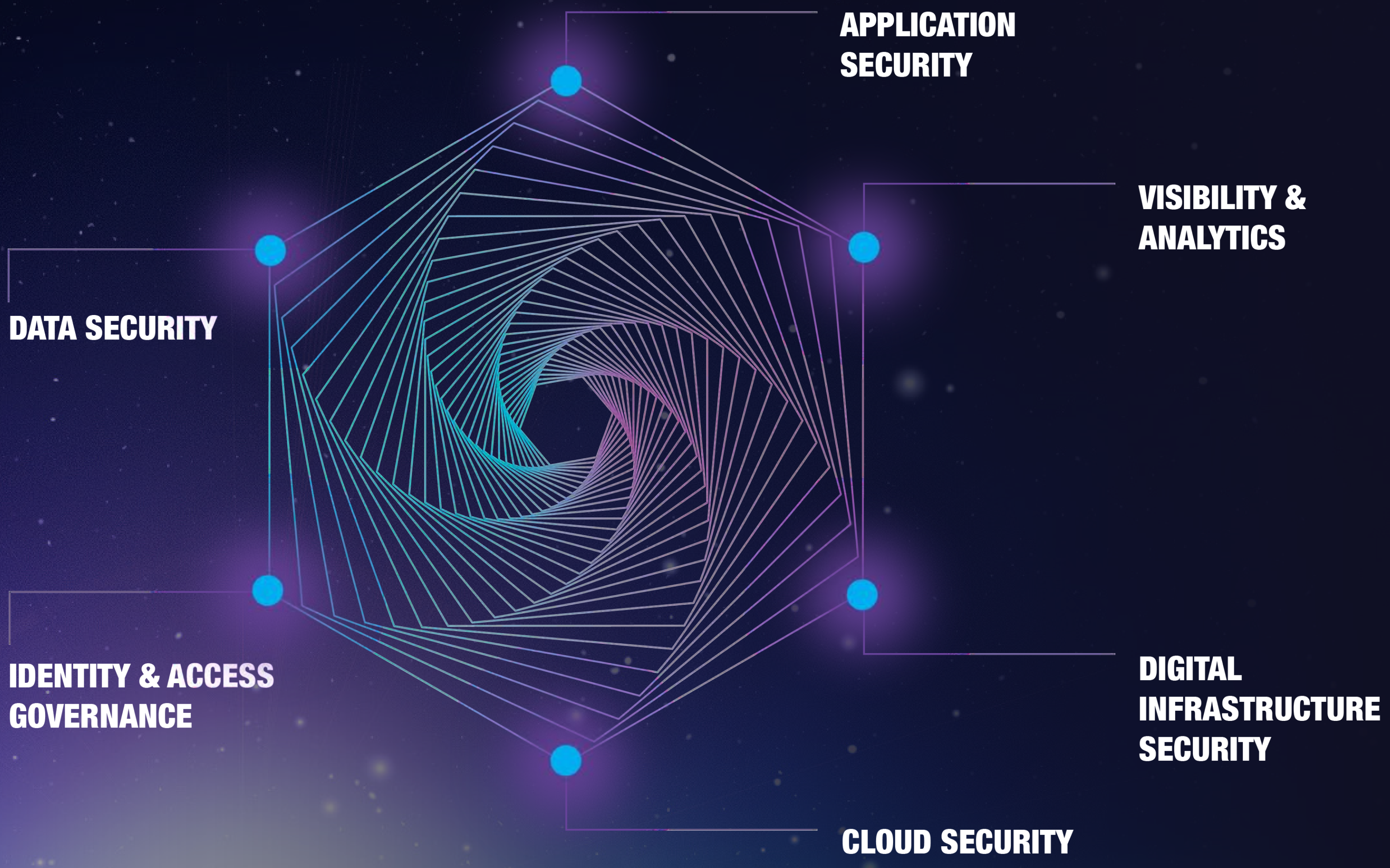
The risks introduced by digital transformation demand that organizations make cybersecurity a key element of their transformation plans. It is time for organizations to recognize the importance of cybersecurity in strategy design and to have a continuous model of detection, response and prediction to ensure maximum resilience. The innovation and pace of digital transformation mandates the need for effective security.

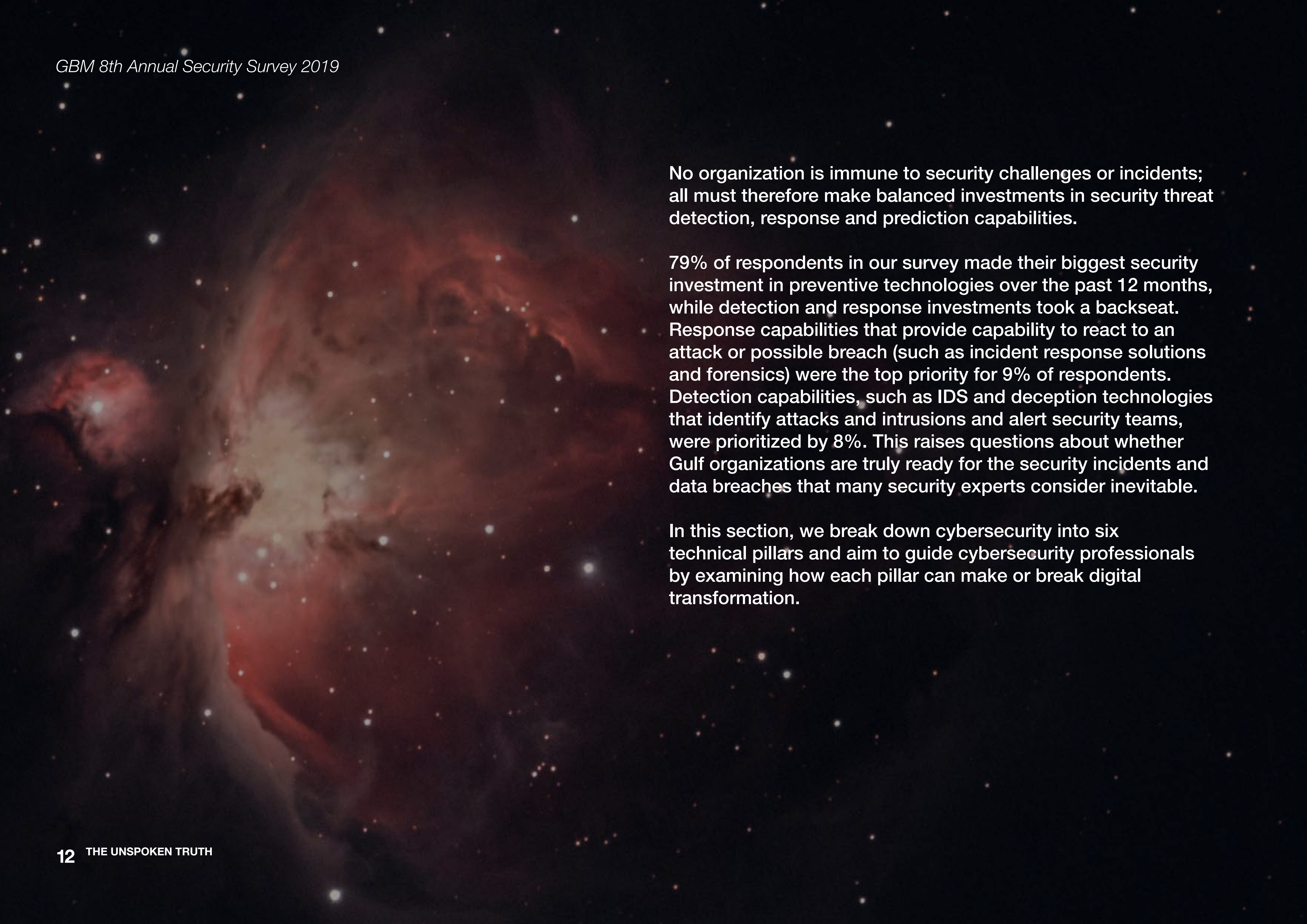


Only 15.4% of respondents said that security teams are fully involved in the digital transformation journey, whereas 79% of respondents said they had a partial role in the process.

The Wheel of Cybersecurity

How the 6 pillars of cybersecurity impact digital transformation


APPLICATION SECURITY
VISIBILITY & ANALYTICS
DATA SECURITY
IDENTITY & ACCESS GOVERNANCE
DIGITAL INFRASTRUCTURE SECURITY
CLOUD SECURITY



No organization is immune to security challenges or incidents; all must therefore make balanced investments in security threat detection, response and prediction capabilities.

79% of respondents in our survey made their biggest security investment in preventive technologies over the past 12 months, while detection and response investments took a backseat. Response capabilities that provide capability to react to an attack or possible breach (such as incident response solutions and forensics) were the top priority for 9% of respondents. Detection capabilities, such as IDS and deception technologies that identify attacks and intrusions and alert security teams, were prioritized by 8%. This raises questions about whether Gulf organizations are truly ready for the security incidents and data breaches that many security experts consider inevitable.

In this section, we break down cybersecurity into six technical pillars and aim to guide cybersecurity professionals by examining how each pillar can make or break digital transformation.

> **“Prevention alone will fail to protect organizations; mindsets and budgets must shift to include detection and response technologies, which can keep up with evolving attacks.[4] ”**

1. DATA SECURITY

Trying to undergo a digital transformation before putting effective data security in place is like trying to run before you can walk. It puts the business and its customers at risk.

81% **of Gulf organizations, securing data is the biggest challenge during the digital transformation journey.**

Organizations must treat their **sensitive data** – the basis for any digital business strategy – as a valuable and irreplaceable asset. Sensitive data must be protected to establish and maintain data quality, availability, and integrity.

Organizations face multiple challenges when creating a data security strategy. Data is being generated at a faster pace than ever before and organizations are keen to use it to derive insights that guide their digital transformation journey. Data is therefore bigger than ever before, and it is also diverse: it can be structured or unstructured and stored in a range of physical and cloud locations and on various devices. It is therefore impractical to apply the same security controls across all data in the organization. This brings the biggest challenge, data classification. Data classification, aims to answer important questions such as “which data is critical or sensitive?” and “where does it reside and in which formats?” By answering these questions, organizations can find the right starting point for securing data.

[3] GBM 7th Annual Security Survey 2018

Once an organization has classified its data and discovered how its data flows in each department, the next step is to define appropriate policies and deploy security controls. In our survey, 87% of Gulf organizations rated the first few steps “Data Classification” and “Data Security Policy” as their biggest obstacle. This suggests a lack of data security maturity in the region, since organizations must get the first steps right if they are to implement effective controls. This is set to change for the better, however, with the introduction of new privacy rules and regulations in the Gulf region that have either already launched or are launching within the next 6 months. Organizations can opt to build an execution plan and governance plan around these privacy laws to ensure they adopt best practices within their country.

Only a strategic approach to data protection in a digital transformation initiative can limit the risks of digital business

Only a strategic approach to data protection in a digital transformation initiative can limit the risks of digital business. Paths to establishing a strategic data protection capability include:.

- **Develop a strategy:** Creating a strategy, defining a policy and classifying data are the fundamental steps to starting the data security journey. These steps include defining current state and target state, classifying data, documenting data flows, creating policies and rules and forming a roadmap for the organization.

- **Implementing data privacy controls:** Data protection capabilities must evolve to support multi-cloud operations; a key feature is BYOK (bring your own key) which provides encryption with local key control.

Control 1 - Database and application-level encryption should be implemented.

Control 2 – Tokenization and database access monitoring with strong authentication should be implemented.

Control 3 - Data loss prevention (DLP) solutions should be implemented to ensure sensitive data does not leave the organization or reach unauthorized users within or outside of the organization.

Control 4 – Public key infrastructure (PKI) and certificate key management should be used to maintain security across different applications and to create a trusted or untrusted environment.

Control 5 – Cloud Access Security Broker (CASB) should be used to monitor, encrypt and prevent exposure of sensitive data in the cloud.

An important aspect to keep in mind is “residual risk”, since technology related to data leaks is not fool-proof.

For example, when deploying a DLP solution, organizations might not be able to control snapshots of data taken by a mobile device. It is important to explain the residual risk concept to management teams, so that either the risk is accepted or alternate (non-technical) measures can be adopted.

CYBERSECURITY AND BIG DATA

Big data refers to the huge volumes of information organizations process and analyze today, drawn from diverse sources including billions of network-connected devices and IoT sensors. When an organization can collect, organize and analyze big data effectively, it can gain valuable and actionable business insights. Data analytics is one of the pillars for an organization's digital transformation and we will look at its cybersecurity linkage to big data later in this paper.

As data is being generated exponentially, the ability of traditional technology to detect incidents or correlate logs to help in root cause analysis is reducing in such environments. Therefore, many organizations are choosing to explore a different approach, namely security analytics integration with big data. According to our survey, less than 5% in the Gulf are expected to implement this approach.

Using big data in security analytics

Within cybersecurity, big data insights are geared towards insights that make it possible to predict and stop cyber-attacks. When organizations can recognize the patterns that represent a threat or impending attack, they can strengthen their security posture. A typical approach is to use historical network data to identify a statistical baseline that represents ‘normal’ network behavior, and then compare that live data against the baseline to discover ‘abnormal’ behavior. Additional intelligence data can be sourced from third-party solution vendors.

Using big data to enhance cybersecurity also advances digital transformation projects by:

- Protecting the digital organization by identifying anomalies in device and user behavior
- Protecting the network by detecting anomaly-based intrusions
- Supporting machine learning-based malware detection
- Supporting online fraud detections with the ability to analyze large data sets

Security challenges arising from big data analysis

Collecting, storing and processing huge data volumes inevitably raise some major security challenges. Because data is a valuable resource, cyber-criminals are more likely to target organizations that use big data. Storing big data often requires the use of multiple public cloud storage services, which must be secured with robust and identity and access management. Many big data analytics tools are also built with open source software, which offers security of varying effectiveness.

For organizations planning to accelerate digital transformation with big data, then, there are important issues to consider.

- **Security not included** – There are many popular tools designed to optimize big data processing jobs, which organizations need to secure separately. For example, Hadoop distributes processing across multiple systems to speed jobs up but has no built-in security functionality. The NoSQL database platform is very efficient in processing big data but is perceived to offer weaker security than other databases. Organizations need to be aware of these shortcomings and add their own security where required.

- **Complex storage –** Big data generally requires lots of storage, and in recent years a 'tiered' storage approach – where critical data is placed on fast flash storage, while rarely-accessed data is placed on tape or in the cloud – has become commonplace. This adds security complexity, as each storage type might require its own IAM solution and security strategy.

- **Securing the results –** Tools used to analyze big data must also be secure against external attacks and inside threats, who may seek unauthorized access to the insights produced.

- **Securing metadata –** Analyzing big data also creates a huge amount of metadata, which can identify data sources, access activity and other potentially sensitive information. This too must be secured.

The true value of big data insights comes from driving action within business teams. Organizations need to have the operational capabilities to protect this value by sifting through their data, finding the right signals and events, and then triggering the right security action. With these capabilities, they will be enabled to:

- Automatically cut off devices that are stealing data
- Set up systems that provide notifications when employees access suspicious amounts of data
- Send alerts to the right people when potential threats appear

2. APPLICATION SECURITY

Customer experience is a key differentiator in the age of digital transformation. Now consumers have accepted digital platforms (e.g. e-commerce websites, social media and mobile apps), transformed organizations are dependent on software or applications to achieve business goals. It is a competitive landscape, and organizations are in a hurry to deploy new applications that deliver enhanced customer experiences.

Gulf-based security professionals recognize the significance of application security challenges, according to our survey.

49% **named application security as the most challenging security domain within digital transformation projects after data security.**

This perhaps reflects how digital transformation shifts focus from hardware platforms to applications that run on many devices, as well as the challenges of shadow IT and modern application development discussed above.

The space of application security is dynamic and complex. Risks are high and surface level has increased exponentially since mobile applications became the norm. It is therefore necessary to develop an application security program to ensure alignment and risk mitigation. The absence of an application security strategy can lead to poor decisions, increased risk, wasted budgets and conflicts within the organization. Per our survey, 50% of Gulf organizations lack an application security strategy or program while undergoing digital transformation.

55% **Asked about their biggest application security challenges, more than 55% named secure development skills were toughest to find**

As more organizations develop applications in-house, and deploy them on private and hybrid clouds, being able to develop web applications securely will continue to be a valuable skill.

Traditionally, developers have focused on developing core application functionality and are not well versed in developing secure code. To address this issue, developers are advised to embed security early in the software development lifecycle and to continuously check the code for security flaws. This can be achieved by using automated security testing tools, which enable developers to correct flaws and strengthen security.

Software is the true differentiator in the age of digital transformation, and many companies are using DevSecOps to ensure their software meets the right standard. Here are a few best practices for using DevSecOps to keep up with the pace of digital transformation:

- **Ensure Alignment between Security and Developers:** Some security teams do not understand or are unaware that DevOps teams have moved from a waterfall to an agile method during the digital transformation drive. The agile method represents a major change in the way organizations plan, develop and roll out applications to users; and security teams need to be involved from the beginning. If development and security teams do not communicate and contribute to digital transformation initiatives, they cannot understand or adjust to each other's requirements. This can lead to conflicts, delays, security incidents or all of the above. 47% of organizations in the Gulf rated lack of alignment as either their top or 2nd-biggest application security challenge. [4]

- **Automate deployment:** Being able to fix application security flaws quickly is essential to protecting data. Taking a continuous deployment approach, which automates testing and app deployment, means the latest fixes and dependencies can be deployed without human intervention.

- **Make security a development standard:** The race to shorten the development cycle and go to market faster must not overshadow the importance of proper security analysis and testing of release candidates. Organizations must include security standards in the baseline of what is fit for deployment. Security testing also helps developers build skills in writing better application tests and code. By shortening the software development cycle, DevSecOps speeds the pace of innovation for an organization. It also helps earn customer trust and improve retention.

[4] GBM 8th Annual Security Survey 2018

3. CLOUD SECURITY

Many organizations that are using innovative, multi-channel digital experiences to engage their customers are leading their respective fields; and at the foundation of transformed experiences is cloud computing.

28% **Gulf Organizations plan to move on premises applications to cloud under their digital transformation journey.**

This move involves placing critical applications and customer data in the cloud, despite concerns related to regulatory compliance and cyber-threats. Organizations should asses risks related to cloud and either mitigate or accept them, depending on their security strategy.

In Gulf countries, regulations demand that government and semi-government organizations maintain data 'sovereignty' by hosting it locally, in their home nation. However, the region's cloud infrastructure is perceived as still emerging, with a lack of Tier III and Tier IV datacenters physically located within Gulf countries.[5] Organizations might therefore have difficulty in finding public cloud services that can store and process data locally. Our survey data supports this: 58% of respondents cited location of data as their biggest challenge to adopting the cloud for digital transformation purposes.

[5] Telecommunications Regulatory Authority

25% of respondents mentioned that their biggest concern when considering cloud adoption was the recent data breaches cloud providers have suffered. These incidents were partly caused by a shortage of expert cloud security skills in the region. 12.01% of our survey respondents spoke of concern about their organization's lack of a cloud security policy. Overall, there is fear about moving data off-premise, because it could create a point of weakness; so, while transformation and cloud may drive new experiences and competitiveness, it could also compromise data security in ways that threaten an organization's future.

> **Ultimately, responsibility for security is shared by organizations and their cloud providers. While those responsibilities should be carefully and clearly defined in service contracts, organizations should do everything they can to protect the environments, applications and data they deploy on private and public cloud.**

4. VISIBILITY AND ANALYTICS (AI & ML)

Artificial intelligence (AI) is playing an important role in the digital transformation of many organizations across industries. AI powers everything from chatbots in service industries, to diagnosis improvements in healthcare, to digital assistant support in telecommunications. Gartner forecasts that 30% of B2B-focused organizations will employ AI to augment at least one primary sales process by 2020.6 Organizations are being drawn to adopt AI by the promise of benefits that include:

- Time and money savings made possible by process and task automation
- Productivity improvements and new operational efficiencies
- The ability to speed up business decisions and improve customer experiences based on deeper, faster insights

[7] Telecommunications Regulatory Authority

Our survey states that automation of processes is the number one priority of 69% of organizations undergoing digital transformation. Organizations are increasingly evaluating and developing use cases for using AI to automate processes and reduce costs while maintaining, or in some cases enhancing, customer experience.

Organizations are using AI/ML to aggregate and analyze threat intelligence and are putting that intelligence to work when responding to attacks and remediating security breaches. AI-based security solutions can learn which network behavior is 'normal' and which represents an anomaly.

Cognitive computing takes this further, leveraging various forms of AI including ML algorithms and deep-learning networks that become smarter over time. For example, IBM's Watson for Cyber Security learns with each interaction to connect the dots between threats and provide actionable insights. The use cases for Watson in SOC include faster root cause analysis and reduced need for human analysts at L1, thereby increasing overall efficiency and reducing costs.

62%

When we look at the Gulf regions ,62% of organizations surveyed are likely to utilize AI in securing their organization [7]

Use Cases of AI in Cybersecurity to enable Digital Transformation

Fill skills gaps – Demand for skilled cybersecurity professionals generally outstrips supply, but AI security technologies can help organizations achieve security goals with fewer staff and in-house skills. AI also helps small security teams to cope with high volumes of alerts and attacks, by responding automatically at machine speed. This automation can also free security professionals to spend more time on high-value projects such as digital transformation.

Predict and prevent security incidents – ML 'learns' by analyzing massive volumes of data, in near real-time, to find long-term patterns of normal and anomalous activity. This enables it to predict with accuracy if something is wrong: including whether a website might be malicious, whether a file is likely to contain malware based on its attributes, and even when a user logging into to an organization's cloud platform is really a bot.8 With this intelligence, transformed organizations can automatically predict and prevent attacks with greater accuracy and less effort.

Don't be outgunned – When cyber-criminals are using AI maliciously, digitally transformed organizations also need to adopt the technology in order to counter threats. AI and ML is now being incorporated in multiple security technologies to improve accuracy, increase agility and improve detection of zero-day malware, e.g. with threat hunting, threat assessment, UEBA, deception and more.

Organizations that fail to evolve their security capabilities with AI may fall behind competitors.

[7] GBM 7th Annual Cyber Security Whitepaper, 2018

[8] https://www.cisco.com/c/en/us/products/security/machine-learning-security.html

5. IDENTITY AND ACCESS GOVERNANCE

In a nutshell, identity and access governance (IAG) is the discipline that enables the right individuals to access the right resources (such as applications, databases and networks) at the right times and with the right authorization. Traditionally, companies had limited external collaborators and employees were mostly office-based. In the application-centric world enabled by digital transformation, organizations are utilizing cloud services and mobile devices to improve productivity and cost efficiencies. More employees are working remotely and flexibly, rather than being tied to a single desk or computer. Digital collaboration with external partners, by sharing access to corporate IT resources, has become commonplace.

Improved collaboration and mobility are valuable advantages for digitally transformed businesses. However, the cloud and expanded networking technologies that underpin them magnify the challenge of verifying identities as well as managing and governing access. IAG solutions must be ready to control access to distributed applications and critical data by consumers, employees and business partners, from multiple devices and locations. This presents a significant challenge for organizations undergoing digital transformation.

Modern IAG approaches

Modern IAG measures include using the following to cover privileged users (admins), users or customers.

- **Role based access** to make sure right individual has appropriate access

- **Time based access** to make sure right individual has appropriate access for required time only

- **Access governance** to make sure access posed by user is sufficient to perform his/her job functions

- **Multifactor authentication** to protect against identity theft

- **Single sign-on (SSO) systems** to give users seamless access to all of the organization’s cloud applications

- **Risk-based authentication**, which uses data analytics to assess user behavior and adjust access rights accordingly. When an IAG solution identifies suspicious user activity or attributes, e.g. when a threat actor tries to gain unauthorized access to a resource via MFA or SSO, authentication can be stepped up to ask for additional authentication.

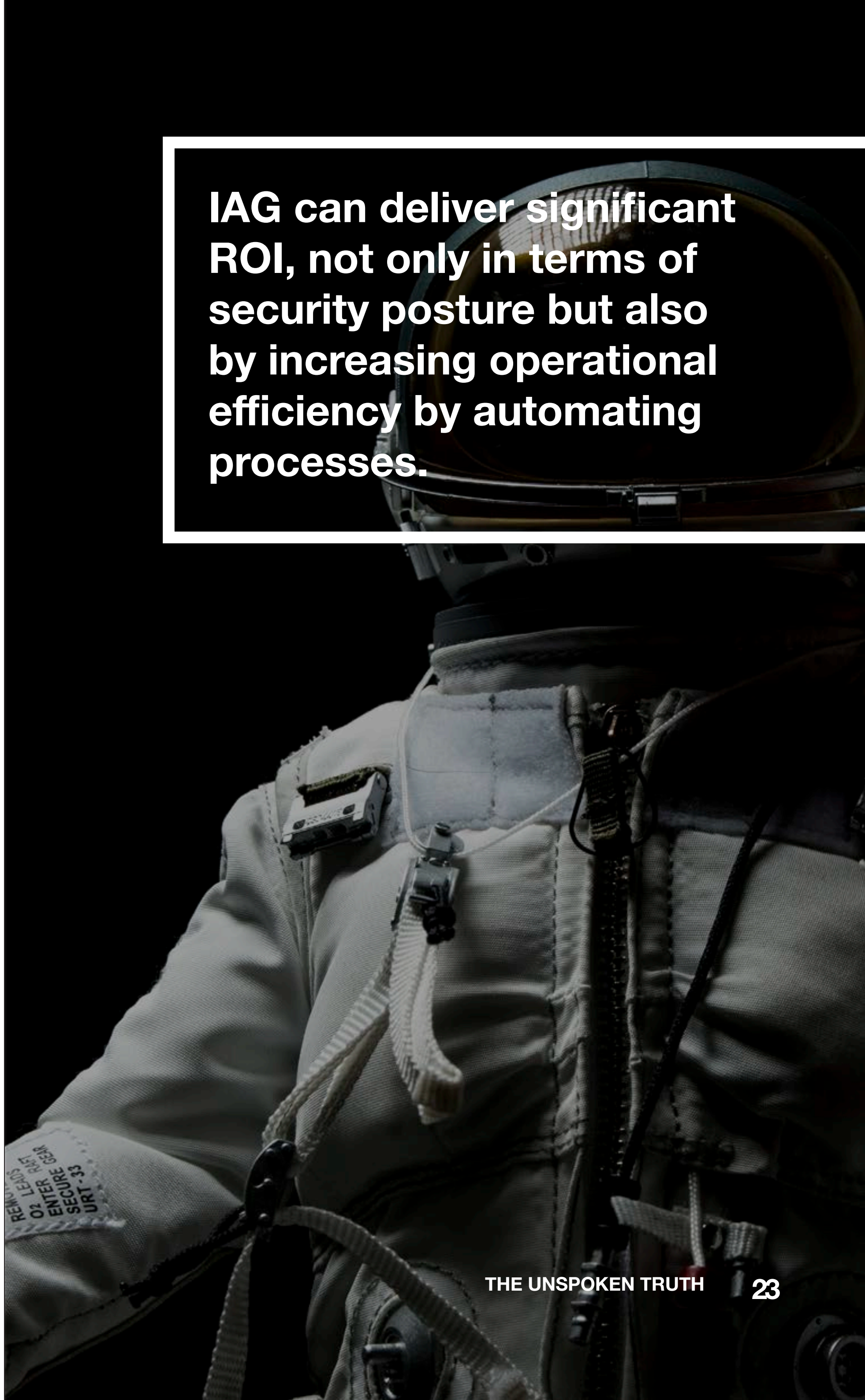
Modern, centralized IAG is not only about locking out bad actors but providing faster and smoother experiences for authorized users, as well.providing faster and smoother experiences for authorized users as well.

[9] Why Identity and Access Management is Crucial for Digital Transformation, CSO

There is a common misconception within the cybersecurity industry that effective IAG is complex to adopt. Our survey results show that only 21% of respondents have found IAG solutions complex to roll out and manage; a greater challenge is delays in adoption of IAG solutions, which was reported by 50% of respondents. Putting in place an effective IAG strategy can help to overcome both of these challenges.

IAG often takes more time to implement in comparison with other security solutions such as firewalls and gateway security. However, IAG can deliver significant ROI, not only in terms of security posture but also by increasing operational efficiency by automating processes. A solution deployed by GBM for an insurance group reduced the organization's employee onboarding time from 2 days with involvement of 7 staff members to 1 hour with involvement of 2 staff members.

IAG can therefore be both a facilitator of digital transformation and a potential weakest link, depending on how well it is implemented. With a robust IAG system in place, organizations can scale up their operations with confidence. Without a robust IAG solution, organizations are more vulnerable to exploitation by unauthorized users, threat actors and devices. Applications, infrastructure and data may also be at serious risk.



IAG can deliver significant ROI, not only in terms of security posture but also by increasing operational efficiency by automating processes.

6. DIGITAL INFRASTRUCTURE SECURITY

Digital transformation requires a robust and versatile digital infrastructure that is simple, intelligent, agile, automated, and secure. Organizations need to ensure this infrastructure can adapt to evolving technology, providing a foundation on which to innovate at speed and meet changing business needs.10

So, while traditional data centers still exist and are useful for storing and processing critical data on-premises, digital organizations are also using a broader range of infrastructure that includes cloud and edge computing sites.

Securing diversifying infrastructure

This broader range of infrastructure attracts a broader range of cyber-threats, which target not only the datacenter but cloud services, network endpoints and the many kinds of devices that connect to them. From ransomware to stolen physical media, organization leaders and cybersecurity teams have a tough challenge in working to secure their expanded infrastructure landscape. [11]

Our survey data suggests IT and cybersecurity professionals in Gulf countries are well aware of the risks. Under our weighted scoring system, respondents named infrastructure security as one of the Top 4 most challenging security domains when tackling digital transformation. Scalability is the most pressing infrastructure security challenge for cybersecurity professionals in the Gulf region, according to our survey data; 43.76% of respondents named it as the most important, and it ranks as the most challenging under our weighted scoring system. As transformed organizations achieve growth using a range of new technologies, including cloud, IoT and edge computing, the ability to scale infrastructure rapidly and securely is understandably crucial.

Respondents' second-biggest challenge was the need for agile infrastructure that can adapt to changing needs. To build agile infrastructure, organizations must also have in place agile security technologies that continue to keep data and applications secure when requirements and business models change.

Under the light of these results, it is vital that the region's security experts utilize best-practice measures to be ready to defend against attacks anywhere, any time. The most important measures are as follows:

[10] https://www.cisco.com/c/en/us/solutions/digital-transformation/index.html#~stickynav=2

[11] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/vmw-techtarget-cyber-security-essentials-for-digital-infrastructure.pdf

Most important measures are as follows:

1. Apply zero-trust to endpoints including IoT: Bring your own device (BYOD) programs and IoT solutions have led to an exponential increase in the number of endpoints on organizations' networks, creating new security requirements. BYOD devices introduce a range of evolving vulnerabilities, including connections to unsecure networks, all while holding sensitive corporate information data. It is impossible to upgrade the security of many IoT devices, yet data flows continuously from them into the datacenter. The answer is a zero-trust approach, requiring verification of all endpoint connections, as well as encryption of traveling data.

2. Secure VMs, virtualize for security: The ubiquity of application and workload virtualization, thanks to its efficiency benefits, has made virtual machines (VMs) a target for attackers. VMs must therefore be secured with portable encryption, data protection and threat detection solutions that are easy to migrate across infrastructure.

3. Do not overlook edge sites: Edge computing means creating and processing data outside the central data center, at sites closer to the end-user where latency can be minimized, and external servers and devices can be utilized. Edge computing meets needs for distributed computing power, but also creates security challenges. Hardware is often both unconventional and out of sight, and therefore can be overlooked by security teams. Edge sites and devices need to be secured with the same IAM and data access controls that apply to every other piece of hardware connected to the network.

4. Be cloud compliant: Public cloud usage is widespread today, and hybrid cloud is integrating services with organizations' digital infrastructure. It is vital to gain insights needed to protect data in the cloud, and to validate the security and compliance of cloud-based data with Gulf-region data sovereignty rules. Because organizations often move data between cloud services and on-premises data centers, the best approach to cloud-based cybersecurity is to use a common hybrid platform that supports both on-premises data centers and cloud-based services.

65% **of enterprises say that a cyberattack or breach resulting from insecure digital transformation has disrupted or damaged their critical infrastructure**[12]

[12] "Bridging the Digital Transformation Divide: Leaders Must Balance Risk & Growth," Ponemon Institute, March 2018

THE DIGITAL TRANSFORMATION SECURITY ARCHITECTURE

In a fast digitalizing environment, safeguarding the security of data is a critical objective for organizations planning or carrying out transformation initiatives. Many CIOs struggle with the preservation of confidentiality, integrity, and availability of information used in business processes, applications, and technology. Achieving these security objectives requires a holistic and integrated approach from the start: security by design.

Because the main objective of enterprise architecture is to address and govern changes in the organization and IT through a holistic approach, the objectives of enterprise architecture and security are closely aligned and even partly overlapping.

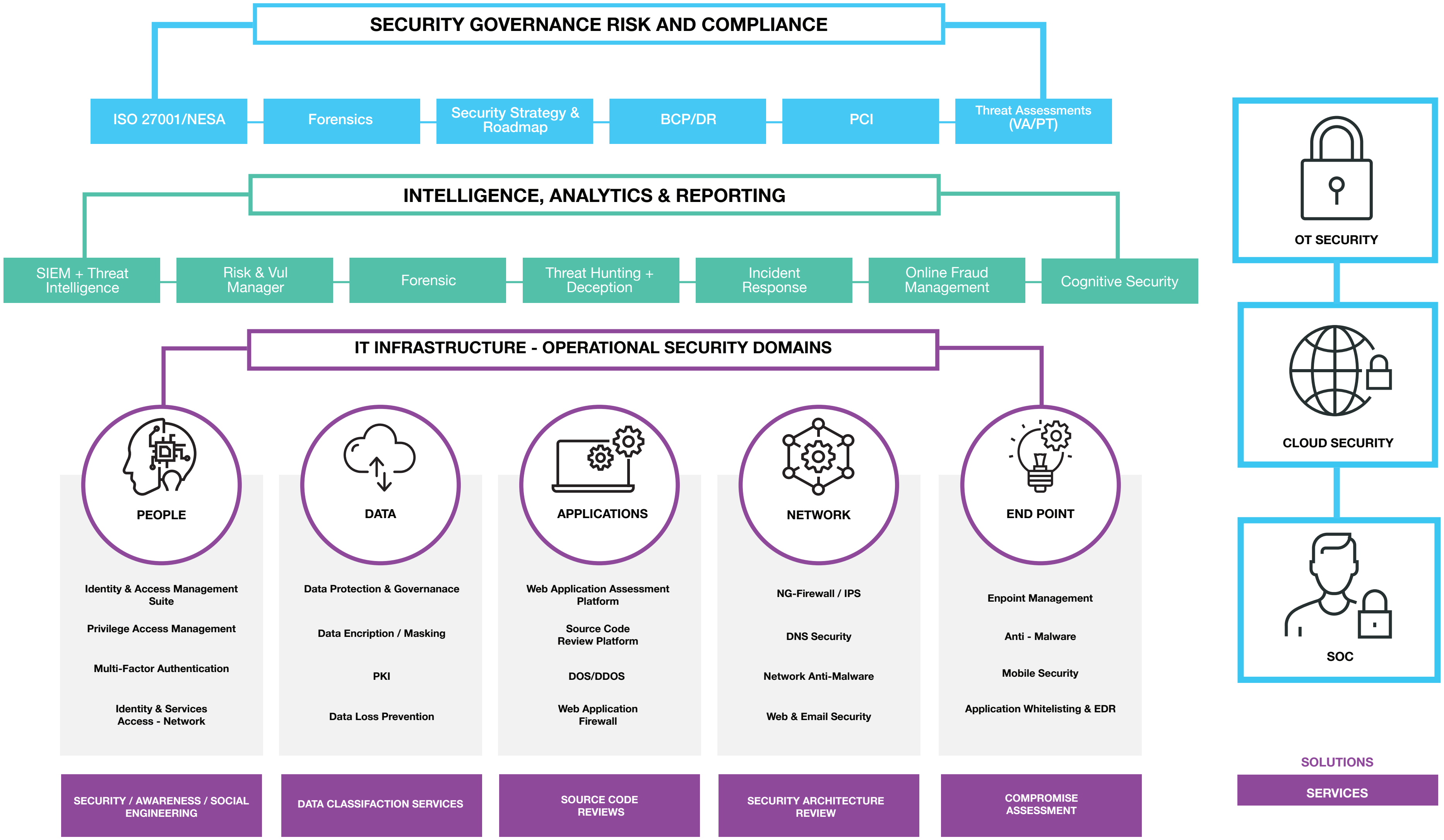
Many organizations have invested heavily in IT security, but because of budget and time pressures, most have ended up layering new security infrastructure on top of their existing IT architecture.

This creates a heterogeneous architectural landscape in which individual systems are haphazardly ring-fenced. In this landscape, there is a need for continuous manual intervention and system updates are difficult to carry out. Instead of resulting in a more secure architecture, this siloed approach to IT security often creates greater complexity and unidentified gaps in the company's cyber defenses.

It is recommended that organizations undergoing digital transformation journey adopt an architectural approach to cybersecurity. Some of the benefits of security architectures are as follows:

- Providing an effective and efficient IT environment
- Meeting regulatory compliance needs
- Implementing effective security governance procedures as well as standardization across the organization
- Educating employees about possible threats and how they can help the organization address them

Sharing security data and insights and developing an ecosystem across cybersecurity silos is a transformational concept for the industry — one that requires people, process and technology adaptations. As organizations embrace secure digital transformations, security professionals need to adopt a risk-based approach to security management built on insights from several sources that include both technical and business contexts. From data governance and firewalling to protecting applications, on-premises and in the cloud, organizations need to build the right security strategy for their business – and to predict, prevent, detect and respond to every kind of risk.



SECURITY GOVERNANCE RISK AND COMPLIANCE

ISO 27001/NESA

Forensics

Security Strategy & Roadmap

BCP/DR

PCI

Threat Assessments (VA/PT)

INTELLIGENCE, ANALYTICS & REPORTING

SIEM + Threat Intelligence

Risk & Vul Manager

Forensic

Threat Hunting + Deception

Incident Response

Online Fraud Management

Cognitive Security

IT INFRASTRUCTURE - OPERATIONAL SECURITY DOMAINS

PEOPLE

Identity & Access Management Suite

Privilege Access Management

Multi-Factor Authentication

Identity & Services Access - Network

SECURITY / AWARENESS / SOCIAL ENGINEERING

DATA

Data Protection & Governanace

Data Encription / Masking

PKI

Data Loss Prevention

DATA CLASSIFACTION SERVICES

APPLICATIONS

Web Application Assessment Platform

Source Code Review Platform

DOS/DDOS

Web Application Firewall

SOURCE CODE REVIEWS

NETWORK

NG-Firewall / IPS

DNS Security

Network Anti-Malware

Web & Email Security

SECURITY ARCHITECTURE REVIEW

END POINT

Enpoint Management

Anti - Malware

Mobile Security

Application Whitelisting & EDR

COMPROMISE ASSESSMENT

OT SECURITY

CLOUD SECURITY

SOC

SOLUTIONS

SERVICES

Reference Security Architecture - GBM

REDISCOVERING THE TRUTH: SECURITY RECOMMENDATIONS TO BREAK THE DIGITAL TRANSFORMATION DEADLOCK

Digital Transformation is changing the way industries operate and is rapidly becoming a key priority. However, while it is an exciting journey, initiatives can bring anxiety to an organization's cybersecurity team and IT professionals. In the light of our 8th Annual Security Survey findings, as well as the regional and global landscape, we recommend we recommend four key security actions to break the digital transformation deadlock and to accelerate organizations' transformation journeys:

A. Align security strategy to digital transformation

Though it sounds like a cliché, organizations must start by formulating a security strategy that is aligned to its business and digital transformation strategy. Risks increase when adopting new technologies and applications across platforms on-premises and in the cloud. For example, a finance organization launching a new payment gateway that connects its customers with third-party partners via a mobile app requires a specific security approach. When an organization's roadmap includes moving critical or non-critical applications to cloud, its security strategy around data, identity, application, infrastructure and analytics needs to be aligned accordingly.

B. Build collaborative teams

A successful digital transformation journey is complex and involves the entire organization; that is why it is called a "transformation". While some functions like business and IT are fundamental, it is equally important to include security, procurement, legal and projects. This committee of all stakeholders must define the KPIs for each function and meet regularly to govern the process of digital transformation. The fact that only 15% of Gulf organizations involve security teams fully is a dangerous sign. Ignoring security is not an option; do it at the cost of success. Involving security ensures that security is built in at the design stage rather than bolted on as an afterthought.

C. Create a blueprint or architecture to implement your security strategy

Practical implementation of the transformation-aligned security strategy, which invariably means selecting and deploying new technologies, is a major challenge. Typically, organizations have difficulty integrating new and existing technologies, dealing with resource constraints and navigating the hugely dynamic technology landscape. This often leads to an ad-hoc deployment of security technology on a piecemeal basis, or failure to achieve the level of security integration needed to achieve high visibility.

The answer to these problems is to create an architecture or roadmap which is customized to the organization's needs from strategy, technology and skills perspectives. Having a 3-year implementation roadmap supports a holistic and integrated approach to security, helping to ensure goals are met. In the section above we have provided a brief on how the blueprint, including use cases, can be drawn.

D. Determine on governance

Security transformation journeys are long, complex and dynamic. Organizations may set out KPIs and objectives for different facets of security (e.g. risk, compliance, cloud, application, mobile, data and others) they need to achieve. However, it is natural to lose track of a few, or dilute them as we go along. This is why governance is a must. Investment in governance helps to keep projects on track and measures the organization's progress towards its goals. Unfortunately, our survey results show that Gulf organizations are not currently focused on governance; only 15% of respondents named governance among their top 3 initiatives.

Author

Hani Nofal
VP of Intelligent Network Solutions, Security and Mobility
Hani@gbmme.com

For questions please contact:

Irmak Parlat Yilmaz
Alliance Marketing Manager
Irmak@gbmme.com +971 4 316 2373

Confidentiality Statement

GBM Legal Notices

Other Third Party Trademarks

About GBM

With more than 29 years of experience, 7 offices and over 1500 employees across the region - Gulf Business Machines (GBM) is an end-to-end digital solutions provider, offering a broad portfolio, including digital infrastructure, digital business solutions, security and services.

GBM has nurtured deep partnerships with some of the world's leading technology companies and have invested in skills and resources to assist their customers on their path towards digital transformation. As IT continues to be a major driver and enabler of business across the region, its increasing influence is changing the way people live, work, collaborate and make decisions; this requires smarter IT solutions that GBM is uniquely placed to provide.

GBM understands the various challenges faced by CISOs and has built a robust cybersecurity framework, comprised of solutions and services, to protect organizations with IT security industry best practices and enhanced risk mitigation. The framework addresses traditional and emerging challenges faced by organizations and leverages best-of-breed solutions from partners with proven security expertise. GBM offers solutions and services in the following areas to mitigate the increasing risks facing businesses today.

- GBM focuses on people, processes and technology to provide a holistic approach to mitigating risk.

- The GBM framework effectively safeguards brand name, reputation and assets.

- GBM offers comprehensive, end-to-end strategies that protect against external and internal threats and which may include solutions for endpoint security, applications, database, people and regulatory compliance.

GBM

www.gbmme.com