GBM SECURITY REPORT 2022

GBM

# DEEP DIVE INTO DIGITAL TRUST

THE IMPORTANCE OF TRUST IN THE DIGITAL FIRST-WORLD &
THE OUTLOOK GULF ORGANIZATIONS NEED TO EMBRACE

# CONTENTS



# FOREWORD

Can you imagine a world without electricity? Probably not, similarly one cannot begin to imagine a world without digitalization as it has become embedded in our daily lives and is now the new normal. Over the past 2 years, digitalization has had an exponential growth. It was found that approximately 4.5 billion people now use the internet, sadly that also means that nearly half of humanity is at risk of being a victim of cybercrime. Apart from that, it implies that the number of cyber criminals has exponentially increased too.

With modern work from home and hybrid business strategies, the cost of a data breach has increased by 9.4% during the past year in Saudi Arabia and the UAE. This resulted on average a loss of $6.53 million per breach, business disruption and a negative brand image.

What many businesses don't realize is when they have a potential breach, this doesn't only compromise their business data but also their partners' data. So how can this be addressed and prevented all together?
The answer is simple, effective zero trust cyber security measures, controlled access and a good understanding of Digital Trust by business entities, governments & individuals in their roles to play.

This report takes a deep dive into Digital Trust and elaborates exquisitely about what cyber security strategies businesses and individuals should adopt in order to reduce hefty breach expenses, as well as the top eight risks that have become a predicament, followed by eight key areas that needs to the focal point going forward in 2022 for successful, seamless and agile business years to come.

This report also suggest the steps to be taken by governments, enterprises and individuals as "partners", in order to ensure Digital Trust, and it zooms into Enterprise Trust to address how to improve the scores in the cyberwarfare we are all engaged in today.

Hani Nofal

**VICE PRESIDENT**
DIGITAL INFRASTRUCTURE SOLUTIONS

# ACCELERATED SHIFT TOWARDS A DIGITAL-FIRST WORLD

The ubiquity of technology in our highly digitized lives has made it almost invisible, the same way electricity and the internet are now so embedded in daily life, that they are considered part of the very fabric of existence. From the moment you are conceived, the data trail that becomes the digital construct of your life begins. Medical data is collected with images and reports, over time this grows as organizations begin to capture education experiences, then on to work and personal lives where the data trail multiplies.

Leveraging a range of underlying and relatively new technologies, businesses have been actively creating new operating models, products and services, and channels to cater to the new habits and experiences of the "digital-first" consumer. New born-digital entrants, **direct-to-consumer (D2C) companies**, fintechs and others have been disrupting most industries and nibbling away at the customer bases of traditional players. By adopting technologies such as cloud, mobile and analytics, and relatively new technologies such as Artificial Intelligence, automation, IoT, robots and augmented/ virtual reality, businesses are also striving to reshape themselves as **"digital enterprises"** to adapt and capitalize on the changed conditions.

The pandemic has accelerated the shift to a **"digital-first"** world – during which we witnessed unprecedented changes such as large-scale work and study from home, massive growth in online commerce, adoption of telemedicine, and a rapid growth in the use of contactless platforms for government, banking, and other essential services. **GBM's Security Report 2020 indicated that 60%** of Gulf organizations had invested in cloud services in the first half of 2020, with a key focus on collaboration tools by **57%** of organizations in response to the need to work remotely. The disruption over the past year has added new consumer habits and created new segments of **"digital-first" consumers**. In addition, today we have entire generations that are Digital Natives, those that have grown up since the Internet and smartphones became ubiquitous globally and have extensive online personas.

# THE STRUGGLE TO KEEP PACE WITH THE EXPANDING THREAT LANDSCAPE

Increased use of technology creates a rich playground for the cyber criminals of the world. The earliest adopters of cryptocurrency, for example, were the ransomware groups. The ability to take a payment from anywhere globally and in any currency, with full anonymity, plays into the hands to the criminal element – whilst Interpol's cybercrime unit have highlighted ransomware as a significant global threat to all businesses. Cyber security, however, has long been challenged to keep pace with the threat landscape and struggles to gain significant support from business leaders, often not until it's too late.

The cost of a data breach in Saudi Arabia and the UAE – the Arab world's two largest economies – has increased 9.4 per cent over the past year costing companies $6.53 million (Dh23.98m) per breach on average, according to the latest report from IBM Security, **and IDC's Future Enterprise Resiliency Spending Study 2021 showed that 37% of businesses that were struck by ransomware had their business disrupted for a week or more.**

**A cyber incident costs time and money, but more importantly, can also impact the brand and image of an organization if it is not handled correctly.**

For the individual, security falls into the need to remember a range of passwords and pin numbers. Whilst useful at one time, these authentication methods are easy to forget, lose, and worse, have stolen.

**For enterprises and governments, the challenge is how to protect the critical assets of identity and data, but allow customers, employees and partners to access the broad range of digital tools required to function.**

Conflicting with this is a broad range of threat actors - from cyber criminals to nation-states, script-kiddies to hacktivists and even cyber terrorists. The ability to secure all systems all the time against all these potential threats is almost impossible under such circumstances, so the rules of the game have to change.

# DEVELOPING THE SECURITY CONVERSATION AROUND DIGITAL TRUST

For too long the IT security teams have been challenged to align the need to protect the business, with the desired outcomes and metrics that businesses focus upon, such as profitability and return on investment. As a result **"Digital Trust"** is the conversation that we need to be having across all levels of society and business.

Trust is built up over time based upon our actions, processes and, in the case of businesses, our ability to fully address the business risks that cyber threats bring with them. By aligning our cyber security investments to the desired business outcome of trust-enabled commerce, we can more clearly understand the importance and value of our cybersecurity investments even if we have not experienced a hack. At the same time, the tools we invest in for security need to evolve from perimeter security, to one of distributed integrity, one component of which is the currently popular **Zero Trust** model – where we have a better understanding of high and low risk areas and are able to adjust our monitoring focus.

**The goal of security is also evolving.** Whilst many of the more mundane attacks can be prevented at the edge, before doing too much damage, there is a growing need to monitor critical assets and systems more often to be able to sense when unexpected activities take place and to take the right types of action to respond to a full-scale breach before it is able to manifest itself.

To achieve this trust requires a partnership between business entities, governments and individuals. In this cyberwar this group is on one side, whilst the threat actors are on the other side. We need to align the following expectations:

- **Trust in the digital life of the individual**
- **Trust in government and digital enterprises**

**In this respect, all three groups have roles to play in the goal of engendering mutual online trust that benefits all of society, whilst reducing the opportunities for threat actors to negatively impact any of us.**

The desire of individuals to have instant online secure access to their favorite products and services

The desire of governments to protect their populations and commerce

The desire of businesses to successfully and profitably serve the ever-increasing needs of customers

# TRUST IN THE DIGITAL LIFE OF THE INDIVIDUAL

2020 was the year that changed the face of internet connectivity for everyone. The pandemic forced many people to work remotely. Indeed without mobile and internet connectivity many parts of the community would have been totally cut off. As a result, IDC noted that:


of individuals worldwide used telemedicine for the first time


of individuals worldwide used mobile ordering for the first time

**The use of video conferencing app both for laptops and mobile dramatically increased both for private and commercial use**

**But this increased use of online tools brought with it a fresh set of risks that many individuals are not aware of.**

When you post the pictures of your newborn onto social media, share a post about your vacation, a video of your new home **all this data becomes locked into the global data networks for almost anyone to view. Many of those looking for this data want to use it for criminal activities.**

**"In a world where more than 4.5 billion people are online, more than half of humanity is at risk of falling victim to cybercrime at any time"**

*Interpol in October 2020*

## INDIVIDUALS NEED TO CONSIDER WHAT IS SHARED ONLINE

### Social media is full of interesting quizzes:

1 

**What was the name of your first pet?**

2 

**What is the name of the street you where you first lived?**

3 

**What was your first car?**

These, harmless seeming questions are designed to gain information that will help a criminal breach your personal security for a variety of reasons. The rise of e-commerce means more people are providing credit card details online than ever before, accelerated in part by the pandemic as more people engaged in online shopping from home, since the physical alternative was not possible. These ecommerce sites become targets for criminals since they often host a range of information that can permit their illegal activities. **Passwords, usernames, credit card details, addresses are all hosted in many locations**. Once stolen, this information can be used by criminal gangs to immediately fund their activities – and an individual financial security is also compromised in the process.

## BE RESPONSIBLE FOR INDIVIDUAL DATA PRIVACY

Protecting passwords, pins and other authentication details is a challenge, but a critical aspect of personal data security that individuals need to consider. **As we better understand the threats facing any organization, our individual concerns need to reflect the changing dynamic of IT security and acknowledge that breaches do happen.**

Consider what gets posted online, what personal data goes into an email, how often you re-use a password. Any one of these actions could assist a criminal to steal or hijack an individual identity.

Whilst European Union implemented one of the world's most stringent and complete data privacy regulations, the EU General Data Protection Regulation (GDPR) that was designed to protect the data of the individual from misuse. A significant consideration within the legislation is that most individuals do not fully understand the implications of sharing their data without any form of control, and this continues today. This also places the onus onto organizations of all type to secure, with integrity, the data they collect on individual customers. Failure to do so, and failure to disclose breaches can result in significant financial penalties.

In many markets, businesses are legislated to protect the data their customers provide, but individuals need to realize that they can help in this process by paying attention to what they share, how and where they share, and the potential risks involved.

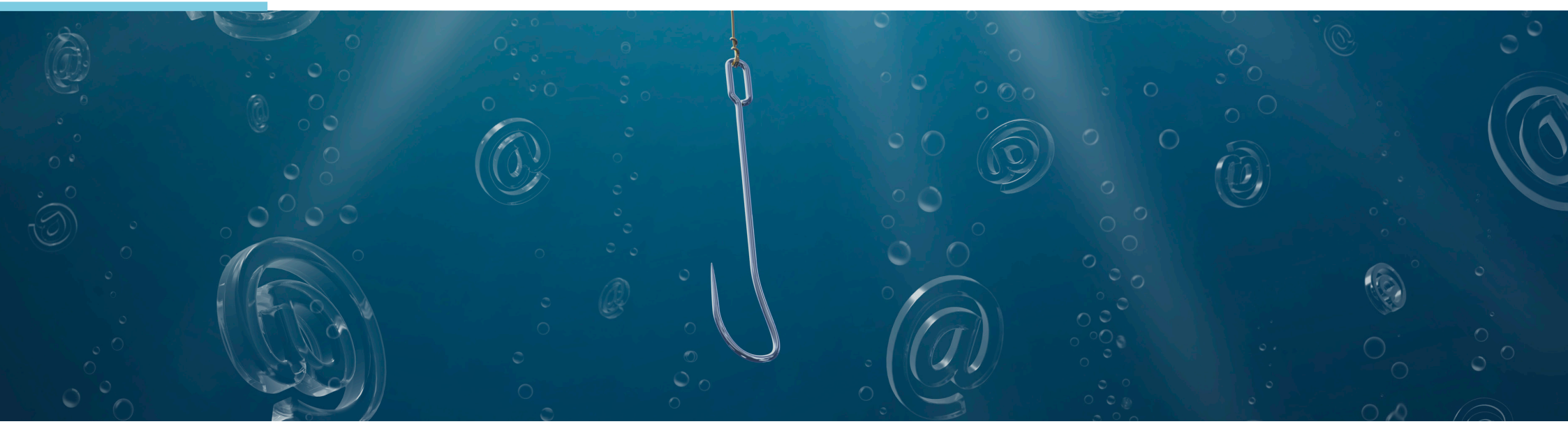
Individuals who are also employees have an extra fiduciary responsibility to ensure they do not become the threat vector for their employers. According to the **GBM Security Report 2020**, **66%** of the organizations found that managing identities and access of end users to be a challenge, especially in multi-hybrid cloud environments.

Whilst individuals will need and want to protect their personal online activities, ultimately many are also employees, as such there is a need to understand the impact and implications to businesses.

Governments play an important role as facilitators of how data is governed to protect the rights of businesses and individuals, while driving economic growth and driving social good. The **digital-first mindset** of businesses and governments in the **GCC** has also increased the awareness related to the way data is collected, processed, stored, shared, and maintained. Over the last decade there has been number of new laws that has been passed across the region to regulate data governance.

This lays the foundation in terms of how UAE government approaches data governance. In the UAE, regulations for data protection in free trade zones and in the remaining areas are different. An example to the regulations in free trade zone can be **DIFC (Dubai International Finance Center) Data Protection Law**, which has been effective since **1 July 2020**. The law embodies international best practices and is aligned with the **EU and OECD** guidelines. It aims to raise awareness across stakeholders, protect privacy and confidentiality, maintain transparency during data processing, and govern outsourced business operations. The UAE government also has federal laws to combat cybercrime as well as to govern Internet access management, electronic transactions, and copyrights, patents, and trademarks. Privacy protection in the **UAE Penal Code** is also available to solve privacy related issues and conflicts.

The Kingdom of Bahrain is another country with a strong focus on data protection. One of the most recent regulations is the Personal Data Protection Law that entered into force on **1 August 2019**. Laws related to regulation of state information, cybersecurity, processing of electronic information are also in place.



# TRUST IN GOVERNMENT AND BUSINESS DIGITAL ENTERPRISES

For business users the implication of a breach is more significant, as stated earlier. Aside from the data concerns stated, there are significant operational and even potential life-threatening concerns to take into consideration.

**As we emerge from the pandemic, organizations in the Gulf need to consider the risk of a potential cyber threat. IDC's CIO Digital Transformation Survey 2020 indicated that whilst 43% of businesses have fully recovered, still one third of all organizations are experiencing revenue slowdown, in which case the costs associated with a breach could have a more negative impact.**

Among the following five stages of business continuity/recovery from COVID-19

**Which one best describes your organization's current status?**

**23%**

**Stage 1:** We are focused on business continuity

**21%**

**Stage 2:** Revenue is slowing down, we are in a cost optimization mode

**7%**

**Stage 3:** Revenue is expected to be in prolonged decline, we are focused on building business resiliency

**6%**

**Stage 4:** Revenue is returning, we are looking to invest more aggressively

**43%**

**Stage 5:** Business is stabilizing into what is now the new normal

## IMPACT OF IT/OT INTEGRATION

The “digital-first” strategy is resulting in enterprises seeking new and innovative ways to automate systems and data flows through the integration of a range of new technologies. Perhaps none is more fraught with risk than that of **IT/OT integration**, due in large part to the fact that the OT systems were not initially designed with IT integration in mind and, as a result, many OT systems are considerably less secure, by design, than the IT systems they connect to – and yet are critical to the business operations – so interconnecting them is a logical technical evolution to follow.

As more organizations, especially those in the manufacturing and resources industries **such as oil and gas, energy and utilities, integrate IT and operational technology (OT), the potential for a digital terrorist and cyber criminals to impact physical systems becomes a reality.**

Many will recall the Stuxnet virus, designed by a nation-state to impact the nuclear ambitions of another nation state by compromising the **SCADA** tools needed to run a nuclear program. More recently the Colonial Pipeline hack in the USA was an email delivered ransomware package that affected the billing systems. Colonial chose to shut the pipeline until a resolution was found resulting in fuel shortages at airports in the US and ultimately impacting a number of flights. Whilst the pressure sensors, thermostats, valves and pumps that are used to monitor and control the flow of diesel, petrol and jet fuel across hundreds of miles of piping were not directly impacted, this does not mean they could not have been. As an example in February, a hacker gained access to the water system of Florida city and tried to pump in a “dangerous” amount of a chemical. A worker saw it happening on his screen and stopped the attack in its tracks.

This is not only an example of the ability to traverse IT/OT connection to create physical impact with a hack, but also of the changing nature of IT security. **No longer a static “set and forget” technology but an area that today requires constant monitoring with the ability to immediately take remediating actions if necessary.**

## UNDERSTANDING AND RESPONDING TO THE THREATS

Business organizations need to better understand the motives and tactics of hackers. **GBM's Annual Security Report 2020 and a recent study by research firm IDC indicates that organizations in the Gulf States see the following threats as more likely:**

- **Advanced Persistent Threats (APTs)**
- **Insider threats**
- **Ransomware attacks**
- **Application Programming Interface (API) compromise**
- **Cyberespionage / Nation state sponsored attacks**
- **Social media attacks**
- **Data leakage**
- **IoT Device compromise**
- **End User based targeted attacks** (Phishing, email compromise, spamming etc)
- **External hacking**
- **Cloud related attacks**
- **AI driven deepfakes**

Ransomware is a growth business for cybercriminals, where they can earn millions of dollars for a single breach, but at the same time earn $1 a million times from individuals. All are at risk from this form of attack, which these days is most often being delivered as-a-service.

A nation-state attack is possibly the most challenging to face. In most cases only extensive monitoring of all connected assets will, possibly, allow an organization to identify such a breach and therefore respond to it, but in this category, the stealth of the attack, a need not to be identified, is usually present, making it particularly challenging to identify and halt.

Social media is a huge source of data for cybercriminals to augment their reconnaissance prior to an attack. All too often individuals reveal too much that can not only compromise their personal security, but in this highly interconnected world, their employee credentials too. Data leakage occurs all the time; an inadvertently emailed file with data, an insecure cloud storage system, data left on old hard drives sent for “recycling”. Addressing this is as much about robust data management strategies as IT security, but can be addressed with a range of solutions.

**APIs** are rapidly becoming the glue that holds much e-commerce together, but in the rush to make them available and make use of them, the **DevOps** world has often forgotten about the security implication. By definition, **APIs** are supposed to be user-friendly, but being overly friendly can lead to creating a new threat vector.
**Cloud and IoT deployments** have also led to various risks emerging, especially when the fundamentals of IT security are not engaged in the early stages of deployment.

More recently the issue of AI deepfakes has emerged, where AI is able to almost fully replicate the likeness of an individual online, usually in a compromising manner. As this technology mature, it will be a cat-and-mouse game for security AI to stay one step ahead of the new threats that this type of attack will create.

# REPRIORITIZATION OF RISKS AMONG GULF ORGANIZATIONS

# REPRIORITIZATION OF RISKS AMONG GULF ORGANIZATIONS

Organizations need to deeply consider how they will respond to a cyber-attack or breach, whilst maintaining the trust of their community. Cleary this is something that is currently top-of-mind for organizations in the Gulf region as evidenced in the following report. GBM's Annual Security Report 2020 described the reprioritization of risks among CIOs in the aftermath of the pandemic. **The report identified 8 key risks which radically shifted in priority and as concerns among Gulf organizations:**

**01** | Growing end user security risks

**02** | Risk of cloud security breaches

**03** | Growing identity risks

**04** | Risk of data and service unavailability in distributed environments

**05** | Risk of internal delays to incident response

**06** | Data and privacy risks due to unsecured applications

**07** | Third-party access risks

**08** | Risk of regulatory complexity and non-compliance

# SECURITY FOCUS AREAS IN GULF ORGANIZATONS IN THE NEXT 12 MONTHS

The report went on to say that in order to address the risk priorities described above, and to build security capabilities, organizations in the Gulf are planning to invest in the following key areas:


**Data security tops the list of concerns, and for a very good reason.** Traditionally data management has been the role of the storage team, however this group have never been formally tasked with responsibility for the security of data. Likewise, the cyber security team has traditionally been responsible for securing systems, network and applications. We are at a pivotal point in data management and cyber security whereby organizations need to decide where this responsibility lies. Mature data management is a complicated issue; hot, warm and cold data of varying degrees of business and compliance importance exist both on and off-premise.

Who better to understand the implications of these data values than the data management team? Except, in today's world a far better use of these skills would be the ability to identify the data that has current, potential and latent value to an organization. For cyber security professionals, the move to cloud is revealing the need to consider data security, as are a slew of new legislations, but until recently this was never a focal point – **but things need to change here.**

Concerns about remote access are well-justified. With many working from home or in a hybrid model, the network perimeter has evaporated and IT teams in many markets are having to manage the security of home networks to secure their own corporate ones.

For many the focus on endpoint as well as identity and access management could address not only the remote working concerns, but also cloud access and data security issues.

Ensuring only the legitimate users and devices are access data, with integrity, can help to resolve many of the risks faced by security, and data management professionals.

# CRITICAL CYBER SECURITY RESOURCING CHALLENGES

Finding the skills to address cyber security is, however, becoming a key challenge. **GBM's Annual Security Report 2020** mentions that **64%** of Gulf organizations currently face challenges in addressing skill gaps. The early days of IT security, the demands were very network-centric. Firewalls, VPN and network monitoring took the forefront. Today however, this is a highly data-driven discipline and the need to have strong data analytic and indeed interpersonal interrogative capabilities are higher.

**With many organizations observing millions of potential threat alerts daily, the ability to program the tools to identify the "signal" of a probably malicious event from the "noise" created by networks and the underlying protocols is becoming the key differentiator of a successful cyber defender.**

The **IBM Cost** of a **Data Breach Report 2021** indicated that for organizations where security AI and automation was fully deployed, their breach expenses were **80% less than** for those organizations with less mature cyber security strategies.

**IDC's Security Survey asked organization to indicate their own security maturity and the results show that some markets need to increase their focus on the topic of cyber security more than others.**

Organizations in the GCC should go beyond that by implementing a more proactive monitoring and response mechanism to mitigate potential security risks including to a **Security Operations Center (SOC) and a Security Incident and Event Management (SIEM)** platform to tackle these challenges. More importantly having a skilled and experienced IT security team is an important element for implementing and operating such platforms successfully.

Therefore there is heightened advocacy for working with Managed Security Service Partners. Organizations who make cyber security their business, as such organizations can invest more into cyber security since it is their business. Clearly the risk is not outsourced, but there are many tasks within the cybersecurity arena that should be outsourced. **Across the Gulf Managed Security Services have become a priority.**

# IMPACT OF DIGITAL TRANSFORMATION

Digital Transformation demands that organizations focus on innovation within their business models. Investments need to be made to create a “better you” and this takes time, patience, skills and resources that are all in high demand and often at odds with incremental investments into IT security. **Underpinning this is the hybrid multi-cloud architecture, which brings with it a new set of challenges for cyber security specialists.**

**Cloud shifts the cyber control points from endpoints, networks and systems to endpoints, data, identity and applications. For many security professionals this is a large shift in attitude and skillsets, especially in a hybrid environment where both approaches are required.**

Similarly, that simple act of innovating is about taking risks – which is at odds with the IT security mantra of reducing risks. As such it is important that enterprises have a robust risk management process to address not just financial, but also cyber and brand risk issues that may arise in the event of a security breach.

# ON THE ROAD TOWARDS DIGITAL TRUST

## CUSTODIANS OF DATA PRIVACY

Individuals, for the most part, have outsourced security to the organization they transact with. The attitude of individuals is, “I buy from you, share my personal data and credit card: I expect you to keep that information secure forever.”

Whilst this approach is more common in the younger generations it is also prevalent across many non-IT consumers of technology. Consider when an individual signs up to a new streaming service. Such a service in many markets will publish their data retention and privacy policies, and customers will need to “accept” the policy to use the system. How often are these policies read? This is the same when buying a new smartphone, as it addresses what is and is not tracked. All too often the majority of the population will accept the terms and conditions without ever looking at them.

## SUPPLY CHAIN AS A THREAT VECTOR

More often than not, cybersecurity maturity is appearing in business RFPs, and with a highly connected digital supply chain the expectation is that you will not become a threat vector to your business partners. Such threat vectors are becoming more prevalent. The now-famous 2014 Target hack in the US, was initiated through their HVAC provider. The infamous Lockheed Martin hack was initiated through cyber security vendor RSA, and more recent supply chain hacks such as SolarWinds and Kaseya were delivered via the software vendors own update systems.

Investing in cyber security is no longer just about protecting your own organization, but also about being sure you are not a threat to your own business partners within the supply chain.

**Trust takes years to build up based on communication, actions, approach, ethics and perception … but leaves at the speed of lightening when it is breached. However, all economic activity is underpinned by trust, so how do we, considering all these challenges faced in our digital world, protect those important digital assets we use, nurture and expect?**

# LEVERAGING THE EXPERTS WITH RISK-BASED DECISION MAKING

As leading organizations outsource more of their own security processes to professional partners, they can refocus security investment and resources into areas that add more value, such as hiring individuals to monitor for ongoing breaches.

**GBM believes that, unless the technology you are investing in delivers clear core competitive differentiation, it should be outsourced, and this is the role of Managed Security Service Providers. Cyber security is one of the functions that all organizations need, so may not provide any differentiation, and yet it is also psychologically a difficult choice to outsource.**

A strong risk management process will help organizations identify those areas that can and should be managed externally, along with those assets and processes that should be retained internally.

## CYBER SECURITY STRATEGY OR TACTIC?

Many of the more complicated attacks today do not impact on arrival. Yes, ransomware can explode on impact of an email arriving or a compromised web page being loaded, but there are many approaches in the market today that can neutralize this impact.

Addressing the more sinister advanced persistent threats (APTs) and nation-state hacks is a much more demanding and needs a longer-term approach. Many of these hacks take their time to collect information, often dwell within systems for years before detonating and causing the havoc that we ultimately hear about in the press.

Today's IT security solutions need to encompass a sprawling terrain of threats. The **MITRE ATT&CK Enterprise Framework** covers over 14 tactics and more the 200 techniques used to breach an organization, and for each there is a tool that could be applied. But this approach does not equate to a successful security strategy.

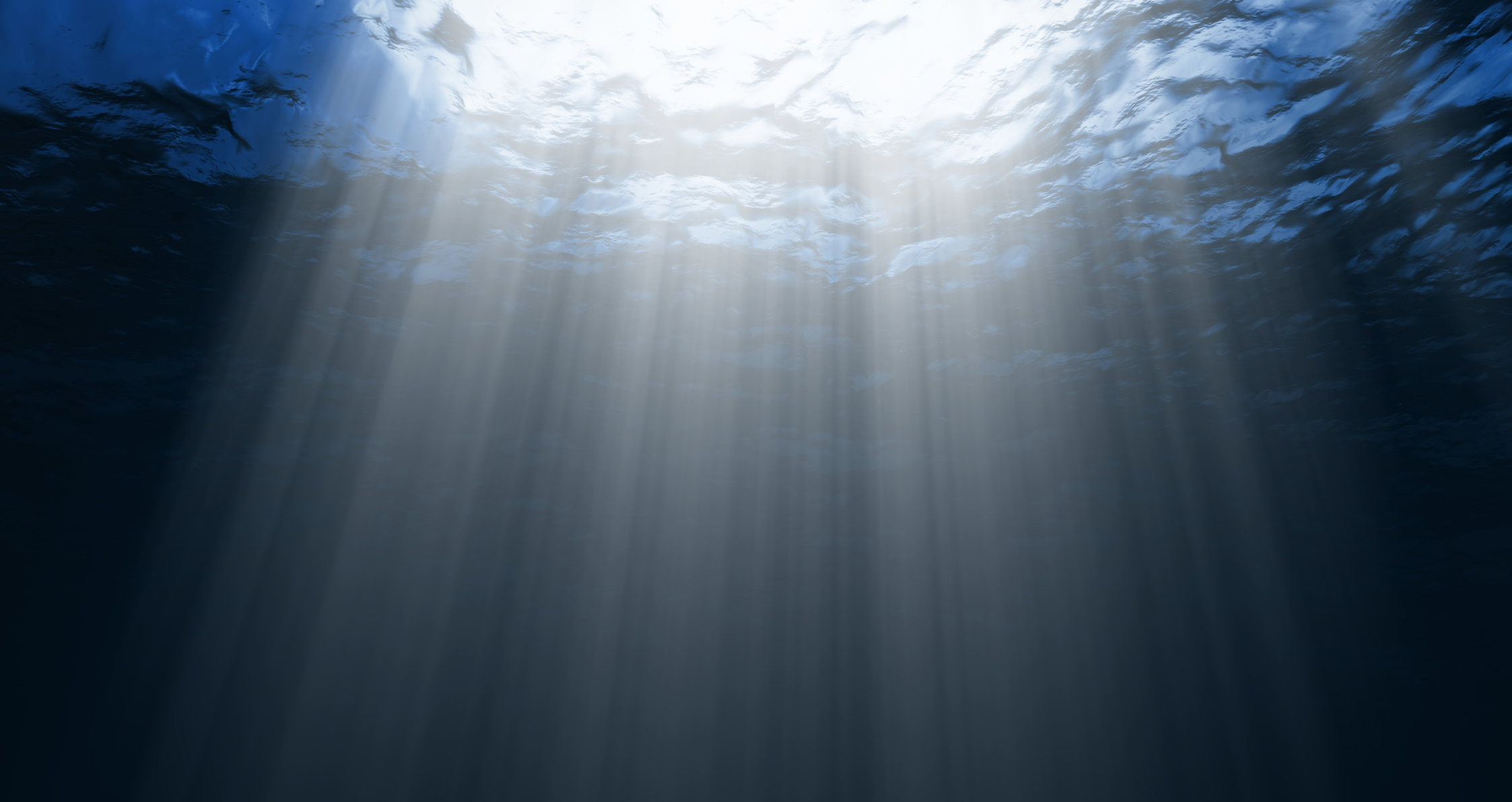
Cybersecurity practitioners have continually added security vendors and tools to their inventory over the past eight years. **With this rising inventory, the enemy of security - operational complexity - increased.**

In parallel, organizational IT environments were expanding as growing number of companies embraced digital transformation strategies and added new tools, services, and solutions inside and outside of the security perimeter. In 2020, practitioners sought to address this complexity with solutions consolidation via an integrated architectural approach.

**As a result, IDC predicts that by 2023, to reduce security complexity faced by limited staff, 55% of enterprise security investments worldwide will be on unified ecosystem and platform frameworks.**

This starts with a full understanding of what needs to be protected in today's hybrid multi-cloud architecture. Refocusing cyber security teams from the infrastructure to more **focus on data, identity and applications**, and working with partners to look at networks and systems creates higher performing cyber security teams, providing them with much needed relief to be able to observe anomalous activities, and remediate before it manifests as a business-threatening hack.

The approach to addressing the more sophisticated attacks is one of constant monitoring and understanding the nuances of your own environments. It takes time to build this profile, compounded by the ever-changing dynamic of remote workers, IoT and a range of systems and devices logging in and out throughout the day.



# FUTURE TRUST: A SUMMARY

**Online economic activity exploded in 2020** and does not look to be slowing down. At the same time the  there is evidence  that shows that financial motivation is the top threat actor motive, and that appears to be accelerating.

**In this ongoing cyberwar there are two sides. Those doing the targeting and those being targeted.**

On the targeting side, the players are well-funded, highly motivated set of conglomerates and cooperatives that share intelligence, tools, processes and best practices. They use cryptocurrency to successfully get paid, but hide their identities, have cybercrime-as-a-service offerings and are generally, extremely financially successful. The pandemic brought to this group a fresh set of new opportunities to make more money.

**The targets, however, do not benefit from this accelerated data sharing.** They do not work together to overcome the enemy and act as individuals in this war. Their governments do what they can to protect them and their customers, but ultimately extract fines when the targets get hacked.

**If things are to improve then there are obvious steps that should be taken:**

01 | **Government regulators** should mandate the sharing of breach data – since we learn more from others mistakes then their best practices.

*Fines and regulation should focus on breach disclosure and adequate security controls being in place*

02 | **Enterprises** must realize they are fighting a war against experts and need expertise to help - it cannot be won alone.

03 | **Technology and service providers** need to work with both groups, as technical advisors, to help identify how best to implement and apply regulations, and how best to comply with said regulations.

**Achieving these goals will be a journey, but if enterprises and governments don't all agree on the direction we are to be heading, we will most certainly fail.**

**Cybercrime, like other crimes, may never be eradicated, but we should be able to reduce the impact and burden to enterprises and individuals if we work together more effectively.**

## Enterprise trust needs to embrace three constituents:


The **customer** relationship is often more keenly focused upon, and clearly adhering to customer expectation towards data privacy and online security is more critical than simply complying with legislation – customers expect more than this.


**Employees**, who are the front line in any customer engagement, need to feel safe and secure in their working environments, which must translate into secure devices, identities, systems and a simple way to ensure this remains so. Arduous security processes will create friction at an employee level which can leak into customer interactions.


**Business partners** are becoming more digitally-connected, and so ensuring an enterprises integrity within the industry supply chain is becoming a requirement these days.

**All areas demand a robust risk management capability: understanding the risks to the enterprise and its connected ecosystem, understanding not all risks are the same, and applying the appropriate level of control for the identified risks.**

**Cyber security is rapidly evolving to a highly targeted, risk-based, practice that is also agile enough to respond to the changes in risk profile of an enterprise. Only by doing so can organizations become to improve the scores in the cyberwarfare we are all engaged in today.**

## ABOUT GBM

With more than 30 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 CIOs 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 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.

**Author**
Hani Nofal
VP of Digital Infrastructure Solutions
hani.nofal@gbmme.com

**For questions please contact:**
Irmak Parlat Yilmaz
Alliance Marketing Manager
Irmak@gbmme.com +971 4 316 2373


GBM
WWW.GBMOMAN.COM