



# Securing digital supply chains

How cyber security drives resilience  
in business transformation

**forv/s**  
**mazars**



## Contents

- 4** Introduction
- 5** Balancing risk management and digital transformation
- 8** The future of cyber security means protecting the ecosystem
- 9** How effective cyber security improves business resilience
- 10** Future-proofing for cyber security requires a transformation mindset
- 11** Cyber security is a business-critical function
- 13** Cyber security for all: why Egyptian businesses need a risk assessment
- 15** Navigating digital Egypt: government reforms and business adaptations

# Introduction

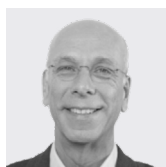
As outlined in our [C-suite barometer report](#), technology transformation remains among the top priorities identified by business leaders across industries. However, as digital supply chains and tech surfaces grow, so does the cyber risk landscape.

This risk is compounded by global expansion; not only do growing businesses make for more attractive targets of cyber crime, but expanding businesses also mean expanding supply chains, especially when localised solutions are required.

Regulation further complicates the matter; as requirements vary from country to country, they can also exacerbate the tendency to take a compliance-based approach to cyber security as opposed to a true risk-based approach.

However, for businesses who truly embrace cyber security as essential, the benefits go beyond reduced risk. **As awareness and priority of cyber security improves across the market, cyber-conscious businesses will have a reputational advantage in their supply chain.**

“Digital transformation isn’t optional, which means cyber security is more essential than ever.”



**Jan Matto**

Partner & Head of Cyber Security,  
Forvis Mazars Group

This report delves into the most critical cyber security challenges identified by our experts, examining how businesses can navigate a rapidly evolving threat landscape. Our experts provide actionable insights on adopting a risk-based approach to cyber security, ensuring resilience and competitive advantage in an increasingly complex and interconnected digital environment.

With global expansion, evolving regulations, and sophisticated cyber threats, the need for robust cyber security has never been more essential for sustainable business transformation.

# Balancing risk management and digital transformation

The COVID-19 pandemic was a major accelerant for digital transformation initiatives. Not only did businesses have to adapt to survive, but the expectation moving forward, especially from a workforce embracing work-from-home and work-from-anywhere arrangements, was that digitisation would persist. The use of internet-based cloud services has only continued to grow, especially as new innovations like AI cloud services have been introduced.

“Cyber security is paramount. It’s not just about technology; it’s about protecting the heart of your business: your assets, investments, and reputation.”



**Omar Shawki**  
Managing Partner,  
Forvis Mazars, Egypt

However, every one of these advancements creates new cyber risk; and because most businesses had to adapt quickly, many digitisation decisions were made without the recommended level of cyber due diligence and in many circumstances without any conversation or risk evaluation with Cyber security experts. Every addition to a business’s technology environment creates a new branch in their complex web of suppliers, and their suppliers, ad infinitum.

Unfortunately, cyber crime has evolved in lock-step with the cyber landscape as a whole, if not more rapidly. It exists at an industrial scale, and digital innovations like AI only make it easier for bad actors to execute sophisticated attacks. This includes state-sponsored cyber crime, which is more and more prevalent in line with geopolitical developments.

## How a risk-based approach to cyber security can enable digital transformation

So, how can ambitious businesses balance digital transformation with cyber security? It may seem easiest to start with an assessment of the current tech surface, but digital supply chains change daily, meaning the sands shift too quickly for a point-in-time security review to be meaningful.

Instead, we recommend taking a risk-based approach that starts from the business infrastructure:

### 1. Start with your core business infrastructure

Instead of focusing on what suppliers are in place and working backwards, begin by mapping out critical business functions in a supplier-agnostic way. This can then be used to identify where and in what state the most sensitive and business-critical data and processes exist.

# Balancing risk management and digital transformation

## 2. Understand your risk areas and potential impact

Once you can identify the “crown jewels” of your business, you can start to quantify the impact of any of them being compromised to varying degrees. This will allow you to more objectively evaluate access and integration risks throughout the infrastructure.

“Real-life digital transformation projects prosper when risk management is integrated from the start, ensuring a smoother adoption of new technologies while protecting the organization’s assets and reputation.”



**Amr Youssef**  
Partner, IT Outsourcing,  
Forvis Mazars, Egypt

## 3. Know your cyber landscape and cyber threats

Cyber security is a crucial part of due diligence, and it goes beyond a compliance checklist. By starting from that core business infrastructure, every decision can be made with true risk management in mind. This necessitates in-depth cyber expertise, including knowledge of local and global cyber security risks, methods and regulations.

## 4. Define cyber security requirements

Only after the above steps are complete (and understood by business leadership) can true risk-based cyber security policies and requirements be defined. These will likely be tighter or more restrictive in higher impact areas, but those decisions and resulting measures will be proportional to the value of the affected assets.

Note that a true risk-based approach goes beyond the digital supply chain, too. Security controls should be incorporated into the design phase of software development, for example, through continuous code review, security testing, containerisation, etc.

This risk-based approach to cyber security means policies and requirements will be a true reflection of the business’s value and priorities, instead of trying to validate technologies according to an externally defined (and therefore somewhat arbitrary) standard.

## How a risk-based approach to cyber security can improve IT collaboration

IT and security are often seen as restrictors or even blockers of organisation’s growth. Whilst the average employee’s perception of this may seem justified, it can be dangerous to allow an oppositional mindset to emerge between IT and the rest of the workforce.

As those entering the job market are more and more technologically savvy, employees are requesting (and often simply arranging) access to more point solutions than ever before. If the IT and security teams evaluating these requests are seen as obstructions to business operations, it creates the risk that these employees will look for workarounds, likely creating even more risk as a result.

# Balancing risk management and digital transformation

Another benefit of a risk-based approach is that it can facilitate education. If the rest of the business understands the infrastructure and the possible impact of it being compromised, policies and approaches to new technology will make more sense to non-cyber professionals.

## A risk-based approach may introduce good friction

Don't shy away from good friction to help protect business-critical data and assets; speed is not always the best solution.

Integration is a core part of digital transformation, but when that integration gives suppliers unrestricted or unmonitored access to the company's core assets, or creates a risky environment, it may not be worth the risk. This applies as well to technology solutions that offer a "one-stop shop" experience; whilst this may be attractive from financial and operational perspectives, too much reliance on a single solution is inherently risky. Well-considered segmentation can help keep the business safe.

“While AI offers powerful tools for cyber security defense, it also empowers cyber criminals. We must remain alert and aware, constantly adapting to this evolving threat landscape.”

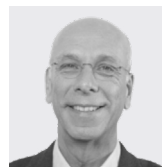


**Mohamed El Abrak**  
Partner, Audit,  
Forvis Mazars, Egypt

This is also true for expansion into higher risk territories. Segmentation within the business may create friction, but if it helps mitigate the risks with the highest impact to the company, it deserves consideration.

Taking a risk-based approach requires time and expertise, but ultimately enables businesses to grow confidently — both globally and across their technology surface — because there is an innate understanding of what needs to be protected, at what level, and why.

“Good friction may seem to go against digital transformation, but it actually decreases risk and increases resilience. This is how you do digital transformation in a responsible, sustainable way, and the market will reward you for this effort as the focus on cyber security increases.”



**Jan Matto**  
Partner & Head of Cyber Security,  
Forvis Mazars Group

# The future of cyber security means protecting the ecosystem

As cyber threats become more sophisticated, with threats such as cascading supply chain attacks or state-sponsored initiatives, the potential impact of these threats increases. Entire ecosystems and industries can be devastated by a single incident. And unfortunately, this pace of evolution will only get faster thanks to the advent of generative AI.

For this reason, much of the newest pieces of legislation – such as the Digital Operations Resilience Act (DORA) or the Digital Services Act (DSA) – talk about “protecting the ecosystem.” This language reflects the fact that, essentially, each business is only as secure as its least secure supplier, and a threat to one is a threat to all. This makes securing the entire supply chain essential to a good security program.

And it's not just a matter of compliance; regulatory requirements are reflecting an overall market demand for cyber secure suppliers, creating a reputational and competitive imperative to look beyond the individual business.

However, it's impossible to adequately identify, evaluate, and mitigate risks throughout the entire, end-to-end supply chain, even focused only upstream. The web of suppliers and solutions is too complex and changes too frequently.

**“Safeguarding the inter connected digital ecosystem, from individuals to global corporations, through collaboration, awareness, and robust security measures is essential for future cyber security.”**



**Mohamd Emara**  
Director, Consulting,  
Forvis Mazars, Egypt

Instead, businesses can help protect their ecosystems by doing the following:

## 1. Taking a risk-based approach

Regulations and compliance standards vary, so a true risk-based approach as outlined above will help identify the overlap and fill in the gaps between the different requirements.

## 2. Integrating policies into commercial agreements

This is mandated by some new regulations, but regardless, companies should commercially require suppliers to adhere to or exceed the standards deemed necessary for the nature and level of access being granted. In the case of suppliers touching business-critical pieces of the infrastructure, these agreements should guarantee the level of support and assurance required to cover the possible impact of an incident. Where possible, agreements should include cyber and business KPIs to help measure compliance.

## 3. Enforcing these agreements

If compliance standards have taught us anything, it's that a requirement is often only seen as such if it's enforced. Otherwise, noncompliance isn't a risk. Audits and reviews should be conducted regularly, including a service owner (i.e. someone not from IT or security), to review compliance on an evidence basis, including any relevant KPIs as defined in the agreements.

If every business in an ecosystem were to take this approach, it would create a radiating effect, reducing risks for all organisations in the ecosystem and shielding one another from possible harm.

# How effective cyber security improves business resilience

Because of the increased frequency and sophistication of cyber threats, both malicious and incidental, it's no longer a question of "if" but "when." This is exacerbated by the pace at which tech surfaces expand, including software, operational technology, and Internet of Things (IoT).

One of the biggest lessons learned during the CrowdStrike incident of July 2024 was that many businesses were powerless to do anything to help restore their systems. Impacted businesses threw all their IT and security resources at the problem, but ultimately, they were reliant on a single supplier to issue a patch; a supplier which many of them may not have even been aware of within their digital supply chain.

An effective cyber security programme includes the ability to detect, identify, respond to and quickly bounce back from cyber incidents. This will help minimise the impact of incidents that do occur, ensuring business continuity and reducing vulnerability. This resilience is so important that it's being referenced in new regulations; one of the most notable examples is DORA.

**"Protecting critical assets, mitigating risks, and ensuring business continuity through robust security measures enhances an organization's ability to withstand and recover from disruptions."**



**Waleed Hammad**  
Senior Manager, Risk & IT Consulting,  
Forvis Mazars, Egypt

These policies also need to be tested thoroughly via staged simulations or even red team exercises (reflecting "real world" conditions to assess levels of security). If at any point a third party is required for restoration, recovery, or any other part of the process, they should also be involved in testing.

The most important way to build this resilience is to define and test cyber security policies. Risk-based approaches to cyber security should include processes for restoring access, rerouting data, isolating threats and vulnerabilities, and communicating in the event of an incident.

**"Resilient organizations are better prepared to navigate uncertainty, maintain stability, and ensure business continuity and competitive edge in a rapidly changing environment. Key components of organization resilience include risk management and supply chain agility."**



**Rania El Gazzar**  
Partner, Head of Audit,  
Forvis Mazars, Egypt

# Future-proofing for cyber security requires a transformation mindset

According to [recent research](#), global cyber attacks on corporations are increasing; up by 30% in Q2 2024 alone. What this means is that cyber security measures sufficient for today won't be sufficient next year, or even six months from now. Therefore, the only way to approach future proofing is to adopt a transformation mindset. The principle of perpetual adaptation has been embraced in other areas of business, including technology, but it must apply to cyber security as well.

“Bad actors have enormous resources, and they're very sophisticated. Cyber teams must continually adapt and evolve to keep the business protected.”



**Omar Chaabouni**  
COO, Forvis Mazars, Tunisia

According to Dr Abbas Shahim, professor at Vrije Universiteit Amsterdam and renowned cyber security researcher, a transformation mindset is a key part of cyber security education, with the best education occurring in three phases:

- 1. Awareness** – helping leaders and workforces understand that things can go wrong, and how
- 2. Training** – teaching teams how to handle it when (not if) things go wrong, as well as how to make things go right
- 3. Transformation** – businesses must continually evolve, grow, and repeat steps one and two to protect themselves and their ecosystems

Some ideas for applying a transformation mindset to cyber security include:

- Organising cyber security as a management cycle, like in the NIST cyber security framework 2.0
- Focusing on collecting operational resilience data to help identify weak points in the cyber security strategy
- Evaluating the strategy regularly via comprehensive penetration (or pen) testing, simulations and red team exercises
- Acquiring and retaining knowledgeable cyber security experts whose focus is on evaluating new and emerging risks rather than IT management
- Reporting thoroughly on key behaviour, risk and resilience metrics, including upward, downward and lateral reporting
- Including cyber security experts at the C-level so risk is at the forefront of critical business discussions and decisions
- Incorporating security updates and education into all-hands meetings and other business-wide communications

# Cyber security is a business-critical function



Despite the increased awareness of cyber security in the market, many businesses still view it as an extension of IT, or as a nice-to-have. However, the prevalence of this mindset is an illustration of why it is so important for forward thinking, resilient businesses to prioritise cyber security.

## Educating the workforce on cyber security

The C-suite is the first level that needs improved security awareness. Not only are they likely to be the decision makers around cyber resources, but they are also the most attractive targets for cyber criminals due to their relatively unrestricted access to critical business data. Before any other education initiatives, it's important to educate company executives on the reality of cyber security threats, as well as the possible impact an incident could have on the business. This knowledge will allow them to take a cyber secure approach to decision making, hopefully including cyber experts in some of those decisions.

Once the C-suite is on board, it's important to educate the rest of the workforce as well. They need to understand that they're the last line of defence, and how to identify and report suspicious

activity. However, the real benefit of a cyber educated workforce is that it makes it much easier to collaborate. Employees who understand the nature and impact of modern cyber incidents are less likely to bypass policies and controls to get what they want, and they're more likely to tolerate good friction in the form of reduced access and due diligence in exchange for improved protection of company data.

One of the most effective ways to educate the workforce is to share the results of penetration testing, phishing campaigns, and red team exercises. Hearing about hypothetical scenarios is one thing, but it's far more of a wake-up call to see those scenarios played out in their day-to-day.

## Cyber security requires sufficient resources to operate well

With several high-profile breaches and outages in international media over the last couple of years, businesses are more aware of cyber risk and its possible impact than ever before. Unfortunately, when the time comes to invest, many companies fall short, failing to allocate adequate people, budget and prioritisation to truly secure the business.

# Cyber security is a business-critical function

All the measures outlined here - monitoring, investigation, strategy, reporting, testing, due diligence, education, etc. - can require significant budget to execute, which can put many business leaders off investing and prioritising. A sufficient programme requires sufficient budget, and even more for a best-in-class one. However, when compared with the quantified impact of a cyber incident, that investment is worth it for the assurance and resilience it brings to the business. Reputational impact and competitive advantage are not to be underestimated either, with a follow-on effect for the bottom line.

That said, it's rare that a business can cover all aspects of a robust cyber security programme internally. Where internal resource or expertise is unavailable, it's better to supplement with qualified third-party experts than to go without.

## The best way to gain cyber engagement is to speak in business terms

One of the benefits of digital transformation is the amount of data available about the business. By combining operational, financial and security data, it's more possible than ever to quantify the potential impact of cyber threats to the business. These metrics are useful not only in reporting, both internally and to fulfil regulatory requirements, but also as KPIs to use with customers who apply the same risk-based approach to their relationship with you as a supplier.

“Mitigating emerging threats, adapting to evolving technologies, and safeguarding sensitive data through a proactive and adaptive approach prioritizing innovation, flexibility, and continuous improvement is essential for long-term cyber security.”



**Mohamed El Abrak**  
Partner, Audit,  
Forvis Mazars, Egypt

Even more, it's possible to take it a step further by combining those risk and impact metrics to determine cyber cost. By multiplying the risk of a certain incident by the likely impact of that incident, businesses can quantify the cost of a particular threat. This can then be applied to purchasing decisions, and even to return on investment calculations.

When the numbers exist in currency value, it's much easier for leaders and their businesses to understand the value of cyber security to the organisation. This allows them to secure the investment required to protect the business in the long term and provides the ability to weigh cyber investments against other business initiatives.

At Forvis Mazars, we help businesses remain cyber secure. With decades of experience assessing, training, and testing, our team of cyber security professionals can help you create a risk-based cyber security approach that will not only support compliance but also build resilience and longevity.

[Learn more about our cyber security solutions here.](#)

“Securing sensitive data is a fundamental function. Adhering to strict regulatory requirements for data protection and cyber security, such as GDPR, is essential. Non-compliance can lead to substantial fines and legal consequences, resulting in significant financial losses and harm to reputation.”



**Hala Rashed**  
Partner, Head of Outsourcing,  
Forvis Mazars, Egypt

# Cyber security for all: why Egyptian businesses need a risk assessment

In Egypt, the rapid digital transformation across industries has made securing digital supply chains a critical focus for businesses. As organizations increasingly rely on interconnected systems and third-party vendors, the risk of cyber threats has escalated. Cyber security breaches can disrupt supply chains, leading to significant operational, financial, and reputational damage. Egyptian companies, especially in sectors such as manufacturing, logistics, and finance, are recognizing the importance of implementing robust cyber security measures to protect their supply chains from vulnerabilities.

To address these challenges, businesses are adopting a holistic approach to cyber security that includes risk assessments, continuous monitoring, and the establishment of secure protocols for data exchange with suppliers and partners. This involves not only securing their own networks but also ensuring that their vendors adhere to cyber security best practices. By fostering a culture of security throughout the supply chain, Egyptian businesses can mitigate risks and enhance their overall resilience.

## How cyber security drives resilience in business transformation

As Egypt undergoes significant economic reforms and embraces digital innovation, the role of cyber security in driving resilience has become increasingly apparent. Businesses embarking on digital transformation initiatives must prioritize cyber security to safeguard their assets and build trust with customers and partners. A strong cyber security framework not only protects against potential threats but also enhances a company's reputation, fostering customer confidence.

In the context of business transformation, effective cyber security practices enable organizations to leverage advanced technologies, such as cloud computing and the Internet of Things (IoT), without compromising security. By integrating security measures into the transformation process, Egyptian companies can ensure that their digital initiatives are sustainable and secure. This proactive approach helps organizations to be agile in responding to market changes and customer demands while minimizing the risk of cyber incidents that could derail their progress.

Moreover, resilient cyber security practices can lead to improved operational efficiency. By implementing automated security solutions and continuous monitoring, businesses can quickly identify and respond to threats, minimizing downtime and disruptions. This not only protects the bottom line but also supports innovation, allowing companies to focus on growth and expansion in an increasingly competitive landscape.

## Lower premiums through cyber security

Cyber insurance has become an essential tool for businesses to protect themselves against the financial risks associated with cyber attacks. However, securing a favorable policy often depends on a company's cyber security posture.

By conducting a thorough risk assessment, businesses can pinpoint weaknesses in their IT infrastructure, evaluate their compliance with industry standards, and determine the most critical threats. This information enables organizations to develop tailored cyber security strategies, allocate resources effectively, and minimize the impact of potential cyber attacks.

# Cyber security for all: why Egyptian businesses need a risk assessment

To help companies reduce cyber risks and secure optimal insurance policies, we offer a comprehensive approach:

## 1- Cyber risk assessment and check-up:

Conduct in-depth assessments to pinpoint weaknesses in your security infrastructure, evaluate your organization's compliance with industry standards and best practices, and prioritize critical risks.

## 2-Cyber security consulting and implementation:

Develop customized strategies to address specific security needs, provide expert advice on security architectures and incident response plans, and assist in deploying security controls and technologies.

## 3- Cyber insurance brokerage:

Identify the most suitable cyber insurance policies based on your risk profile, leverage our expertise to secure competitive premiums, and assist in the claims process to ensure timely and efficient payouts.

Forvis Mazars offers comprehensive solutions to mitigate cyber risks and optimize cyber insurance coverage. By conducting thorough cyber risk assessments, we identify vulnerabilities and recommend tailored security measures. Our expert team helps implement robust security controls, ensuring compliance with industry standards and regulatory requirements.


With a strong cyber security posture, businesses can significantly reduce the likelihood of cyber incidents, leading to lower insurance premiums. Additionally, Forvis Mazars leverages its deep understanding of the insurance market to secure optimal cyber insurance policies, providing comprehensive coverage and minimizing financial losses in the event of a cyber attack.

In summary, securing digital supply chains and integrating robust cyber security measures into business transformation are essential for Egyptian organizations aiming to thrive in a digital economy. By prioritizing cyber security, businesses can enhance their resilience, foster trust, and drive successful transformations that contribute to the country's economic growth.

“Enhancing the security of digital supply chains in Egypt is crucial for maintaining the integrity, reliability, and efficiency of operations in a rapidly evolving digital landscape.”



**Mohamd Emara**  
Director, Consulting,  
Forvis Mazars, Egypt



# Navigating digital Egypt: government reforms and business adaptations

Egypt's digital transformation under Vision 2030 reflects the government's commitment to fostering an inclusive, efficient, and technology-driven economy. Central to this vision is the modernization of critical systems across various sectors, with a focus on improving public services, enhancing transparency, and boosting economic competitiveness.

Among the most impactful initiatives is the implementation of the e-invoicing system, which has become a cornerstone of financial digitalization. This system mandates businesses to electronically submit invoices, ensuring compliance, improving efficiency, and bringing more SME's. Complementing this is the anticipated rollout of a comprehensive digital tax filing system, making it easier for individuals and businesses to meet tax obligations while reducing administrative burdens. These efforts are laying the groundwork for a more streamlined, transparent, and digitally advanced Egypt, setting the stage for broader economic growth and development.

## Smart cities and technological infrastructure

Beyond financial systems, Egypt's government is driving significant progress across various sectors to ensure its digital transformation aligns with Vision 2030. For example, the development of smart cities such as the New Administrative Capital is a pivotal part of this strategy. These cities integrate advanced technologies for energy efficiency, improved transportation, and better resource management.

The New Administrative Capital is designed to be a model for modern urbanization, with IoT-enabled systems to monitor and manage everything from traffic to waste management, all aimed at sustainability and convenience.

Securing digital supply chains

## Digital payment solutions: the rise of Meeza Cards

Another significant initiative is the adoption of digital payment solutions like Meeza Cards, which are part of Egypt's broader effort to promote cashless transactions and financial inclusion. Meeza is a national payment card designed to facilitate direct transfers, e-commerce, and government transactions, especially for individuals who were previously excluded from traditional banking. It helps streamline payments for both citizens and businesses, making transactions faster, more secure, and more accessible.

## Building a strong technological backbone

To further enhance Egypt's technological infrastructure, the government has made strides in internet connectivity and data centers. Projects like the Egyptian National Data Center aim to boost the country's cloud capabilities and make data storage more secure, both for the public sector and businesses. This expanded infrastructure supports the growing demand for cloud computing, which is enabling businesses to reduce costs and increase flexibility in operations.

## eSIM in Egypt

The National Telecom Regulatory Authority (NTRA) launched eSIM services on December 5, 2024. This technology, embedded directly into devices, allowing users to switch carriers or activate numbers without a physical SIM card. The rollout aligns with Egypt's push towards digital transformation, improving convenience, security, and efficiency in telecommunications. It is supported by all four major mobile operators in the country, ensuring compatibility with most modern devices.

# Navigating digital Egypt: government reforms and business adaptations

## Embracing cloud computing and big data analytics

For businesses, the rapid pace of these reforms presents both opportunities and challenges. Companies are increasingly leveraging cloud computing to enhance scalability and reduce overhead costs. Services such as Amazon Web Services (AWS) and Microsoft Azure are widely used across industries, enabling businesses to store vast amounts of data, scale their operations seamlessly, and collaborate across borders. Moreover, big data analytics allows companies to gather insights into consumer behavior, market trends, and operational performance, driving more informed decision-making and targeted strategies.

## New era for SMEs financing: Oliv's digital factoring license

Oliv, an SME-focused fintech firm, has secured Egypt's first digital factoring license, poised to revolutionize SME financing. By leveraging the government's e-invoicing infrastructure and advanced data analytics, Oliv offers invoice financing in under 48 hours, a significant improvement over traditional methods that can take weeks or months. This digital approach eliminates paperwork, streamlines due diligence, and makes factoring accessible to smaller businesses previously underserved by traditional factoring companies.

Oliv's data-driven process assesses creditworthiness within minutes, allowing SMEs to quickly access working capital by selling their invoices at a discount. With plans to expand its product offerings and significantly grow its client base, Oliv aims to drive substantial growth in Egypt's factoring industry, potentially increasing its market size several fold and unlocking significant economic potential for SMEs. This innovative approach demonstrates the transformative power of fintech in addressing critical financing gaps and fostering economic development.

Oliv's pioneering digital factoring license in Egypt not only transforms SME financing but also underscores the critical role of cyber security in fintech innovation. By leveraging the government's e-invoicing infrastructure and advanced data analytics, Oliv facilitates rapid invoice financing while minimizing traditional paperwork. This digital approach inherently relies on robust cyber security measures to protect sensitive financial data and maintain the integrity of transactions. Secure data transmission, storage, and access controls are paramount to prevent fraud, data breaches, and other cyber threats.

As Oliv expands its product offerings and client base, ensuring the highest standards of cyber security will be crucial to maintaining trust and fostering the growth of Egypt's digital factoring industry. This highlights the increasing interconnectedness of finance and technology, where cyber security is not just a supporting function but a fundamental building block for innovation and success.

## Mobile Payments Solutions

Apple Pay became available in Egypt on December 12, 2024, through partnerships with Mastercard, the Central Bank of Egypt, and local banks like the National Bank of Egypt, Banque Misr, and Commercial International Bank. Apple Pay allows for secure contactless payments in stores, online, and via apps. Payments are authenticated using Face ID, Touch ID, or a device passcode, ensuring privacy and security through unique dynamic.

These developments reflect Egypt's efforts to modernize its digital ecosystem, promoting cashless transactions and enhancing convenience for users and businesses alike.

# Navigating digital Egypt: government reforms and business adaptations

## Empowering SMEs: a key pillar of Egypt's digital transformation

A critical focus of Egypt's digital transformation is empowering small and medium enterprises (SMEs), which form the backbone of the economy. However, the transition can be daunting for SMEs, given the financial and technical resources required to adopt digital systems. Recognizing these challenges, the government and private sector are stepping in with initiatives such as microloans, subsidized tech tools, and dedicated innovation hubs to encourage digital adoption. These efforts, combined with digital literacy training programs and mentorship initiatives, are helping SMEs overcome barriers and fostering a culture of entrepreneurship and innovation.

## Digital transformation: driving Egypt's vision 2030

The push for digitalization is not just about compliance but also about enabling businesses to thrive in a competitive global market. Companies are leveraging fintech solutions to enhance customer experiences, expanding cyber security measures to protect sensitive data, and exploring artificial intelligence to improve decision-making. These changes are also aligned with Egypt's broader goals of sustainability and innovation, ensuring that the country remains a dynamic player in the global economy.

## Looking ahead: Egypt's digital future

The opportunities provided by digitalization, combined with Egypt's strategic investments in infrastructure, have positioned the country as a leader in the digital transformation space within the Middle East and Africa. However, businesses must continue to adapt quickly, navigate potential regulatory changes, and remain agile in a rapidly evolving technological landscape. With sustained effort and the right investments, Egypt's push toward modernization could drive economic growth and elevate its global competitiveness in the coming years.

As Egypt advances in its digital transformation journey, collaboration between the public and private sectors will be crucial. Government reforms set the stage, but businesses must seize the opportunity to modernize and innovate. With sustained efforts, the Vision 2030 strategy could not only revolutionize Egypt's economic landscape but also position it as a leader in the Middle East and Africa in embracing the digital age.

“As the Egyptian market becomes a suitable hub for startups, a lack of robust cyber security measures could expose many companies to significant risks.”



**Mohamed El Abrak**  
Partner, Audit,  
Forvis Mazars, Egypt



Thank you for your time reading our publication, we are always passionate about spreading knowledge through the business community. For more information about our services, please visit the following link:

<https://www.forvismazars.com/eg/en/services>

## Contacts

### **Omar Shawki**

Managing Partner, Forvis Mazars, Egypt  
omar.shawki@forvismazars.com

### **Hala Rashed**

Partner, Head of Outsourcing, Forvis Mazars, Egypt  
hala.rashed@forvismazars.com

### **Rania El Gazzar**

Partner, Head of Audit, Forvis Mazars, Egypt  
rania.said@forvismazars.com

### **Mohamed El Abrak**

Partner, Audit, Forvis Mazars, Egypt  
mohamed.elabrak@forvismazars.com

### **Amr Youssef**

Partner, IT Outsourcing, Forvis Mazars, Egypt  
amr.youssef@forvismazars.com

### **Mohamed Emara**

Director, Consulting, Forvis Mazars, Egypt  
mohamed.emara@forvismazars.com

### **Natalie Vatavalis**

Business Development Analyst, Forvis Mazars, Egypt  
natalie.vatavalis@forvismazars.com

### **Waleed Hammad**

Senior Manager, Risk & IT Consulting,  
Forvis Mazars, Egypt  
waleed.hammad@forvismazars.com

Forvis Mazars Group SC is an independent member of Forvis Mazars Global, a leading professional services network. Operating as an internationally integrated partnership in over 100 countries and territories, Forvis Mazars Group specialises in audit, tax and advisory services. The partnership draws on the expertise and cultural understanding of over 35,000 professionals across the globe to assist clients of all sizes at every stage in their development.

© December 2024

[forvismazars.com/eg](https://www.forvismazars.com/eg)

**forvis  
mazars**