

THE HUB

INJAZAT DATA SYSTEMS' OFFICIAL NEWSLETTER



ISSUE 15

INSIDE:

SECURITY SPENDING
TRENDS

SEVEN SECURITY
MISTAKES YOU ARE
MAKING

SECURING
ENTERPRISES IN
THE UAE



PROTECT YOUR DATA

HOW TO KEEP YOUR INFORMATION SAFE IN A DIGITAL WORLD

Injazat CEO Message



**Yours truly,
Ibrahim Mohamed Lari
CEO
Injazat Data Systems**

Currently the top concern of many organizations is whether or not their security is sufficient to protect their information and IT infrastructure. With cyber-attacks on the rise, we need to lead the way in information protection and maintain vigilance to ward off and prevent security breaches. This can seem like a daunting task for anyone.

The last year has been fraught with stories of security breaches, from individuals to multi-national companies, and even government entities. Admittedly, the war against cyber-criminality can seem like an uphill battle.

As businesses move into the cloud, potential security threats may increase. Cloud computing and services can be business enablers, without a doubt. However, we need to keep in mind that each company will have applications and data that are appropriate for the cloud, and those that are not. In short, not every business is the same, and we need to address the unique needs of our customers with every partnership.

As businesses continue to adopt BYOD policies and enable their workforces to become more mobile, additional cyber-security measures need to be put into place. Companies need to ensure that their employees keep all devices protected, and apply policies that will ultimately thwart the advances of criminals looking to leverage mobile devices.

From breaches that have been top news for months, to advice for individual end-users, this issue of the Hub will provide an overview of information security to help you gain information to protect and manage your IT assets.

→ Avoid a Weak Password ←

**DON'T REUSE
PASSWORD**

for at least a year

DON'T

use a duplicated good password
example - create your own



**DON'T USE
THE SAME PASSWORDS**

for multiple accounts.



Don't use password with

**PERSONAL
INFORMATION**

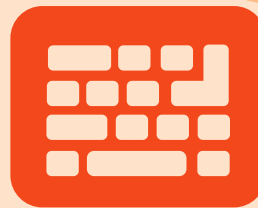
(name, birth date, etc.)



Don't use

**DICTIONARY
WORDS**

Don't use keyboard patterns



QWERTY

or sequential numbers

12345

Don't make your passwrd all
numbers, uppercase letters or
lowercase letters

MIX IT UP

Don't use repeating characters

222TT



Research HUB

Security spending trends

Did you know that organizations that spend more of security also spend more time investigating security breaches? A recent study by CNME Research Hub reached out to 250 IT leaders in the Middle East to gain a better understanding of what is driving IT security investments in the region.

Current spending on IT security solutions still makes up a small fraction of most companies' overall IT budgets. More than 40% of IT leaders report that their department spends less than 1% of their total IT budget on security. This is particularly true for small to medium sized businesses who employ 501-1000 employees. The majority, 52%, of small to medium sized dedicate less than 1% of their IT budget to security.

When addressing possible investment in new or updated technologies, IT decision makers value a number of criteria.

Financial methodology is important while deciding whether or not a particular security solution is the appropriate fit for the company. A notable 71% of all IT leaders reported that "business value" was their top financial priority when determining which security solution to procure. This is in contrast to other possible



More than

40%

of IT leaders report that their department spends less than 1% of their total IT budget on security.

71%

of all IT leaders reported that "business value" was their top financial priority when determining which security solution to procure.



26%

of IT leaders in plan on increasing their security budget in the next 12 months.

responses, "return on investment" and "total cost of ownership" which took, collectively, only 13% of responses in the study. An additional 16% of respondents put forth that "all of the above" financial methodologies were important, an addition which goes to strengthen the perceived importance of "business value" to IT decision makers.

The majority of respondents - 88% - indicated that their department did intend to plan new security initiatives in the next year, both in terms of IT security and operational technology. However, only 26% of participants indicated that they anticipated increasing their security spending budget over the next 12 months. This indicates a desire to increase security with a corresponding need to remain within current budget parameters.

Though causation is difficult to pinpoint, correlations between spending habits and other demographic markers can be made clear. Which criteria come into play when making an IT investment, potential barriers and what concerns IT decision makers have in regard to IT security will all effect potential spending. ▽

What the Sony hack can teach us about protecting our email

Any electronic communication, no matter how private, could eventually be made public.

While the buzz around the

Sony hack has shifted to the impact on free speech, and terrorist threats against movie theaters that dare to show the movie *The Interview*, there are many layers to the Sony debacle. One element that made for headlines immediately following the hack, but has since faded from the spotlight, was the hackers' dumping of company emails onto the Web.

The messages of Sony executives were undoubtedly

damaging. The fallout should remind us that there are likely a few things in all our email archives that could be a problem if a hacker published the contents. Many of us have thousands of emails, going back for years.

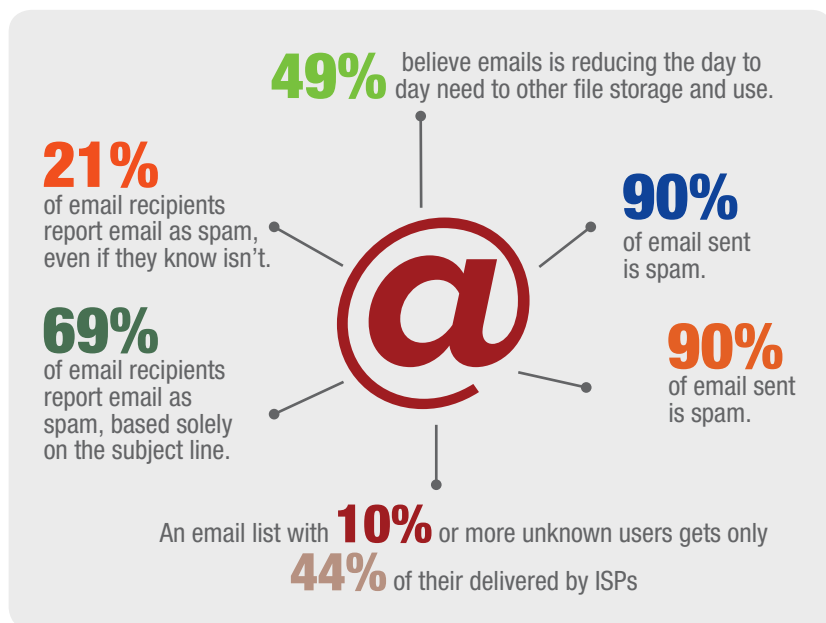
Ironically, careful storage policies could contribute to the risk. Disk space is inexpensive, so organizations tend to err on the side of storing things like emails for longer than is strictly required. Many industries and

organizations are subject to legal and compliance requirements that dictate what must be stored and for how long, but exceeding the rule just exposes more data to hackers.

Offloading email archives to remove them from the direct path of server-sniffing hackers may be a solution. A regular practice of archiving older emails to a removable storage device makes it possible to access emails when you need them, but it is much harder for an attacker to gain access.

That said, each of us has to be aware that we have little--if any--control over protecting that email once it's sent. We also have to accept some responsibility for what we say via email, and take steps to safeguard our own reputations. Operate from the perspective that any electronic communication--no matter how private--could eventually be made public.

While Disney has a policy for its workers stressing that they are "on stage" when they're on the job. In our always-on, connected 24/7, BYOD, mobile, social networking world, though, it's possible that there's no such thing as being "off stage" anymore. ▽

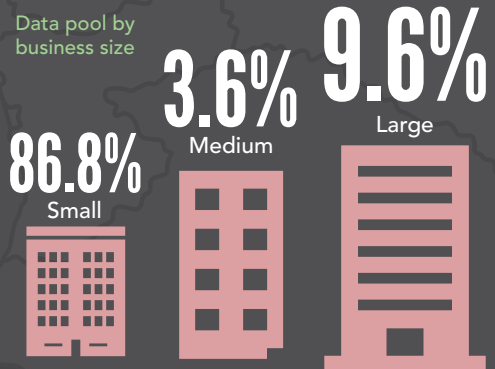
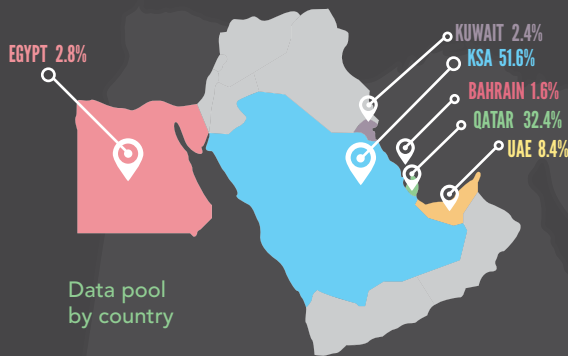




Research HUB

IT SECURITY

CNME Research Hub interviewed 250 IT leaders in the M



SPENDING IN THE MIDDLE EAST

Middle East...



40% of companies that spend **10%** of their IT budget or more on security also spend **one to two weeks** on average to investigate a breach.

68% of companies that spend less than **1%** of their overall IT budget on security spend only a **few hours** on security breach investigations.



3% of IT decision makers rely on peer references at all when selecting a vendor.



86% of respondents indicated that knowledge of their particular vertical industry was a top factor in choosing a potential vendor.



88% of companies indicated that their department did intend to plan new security initiatives in the next year.

26% of participants indicated that they anticipated increasing their security spending budget over the next 12 months.



86% of participants indicated that they are satisfied with their current vendors' product choices.



7 Seven simple security mistakes you may be making! (and how to fix them)

Every recent study of security vulnerabilities has come to the same conclusion: The human factor is a greater risk to organizations than flaws in technology.

Bad behavior that can lead to IT security breaches, most experts agree, is in large measure due to a lack of security awareness -- people are either unaware of increasingly sophisticated threats, or they get careless.

There is, of course, no such thing as 100 percent security. But it could be a lot better if workers at every level, in every organization, avoided the common security awareness mistakes listed below.

1 Falling for phishing: One of the most common mistakes. It can include clicking on malicious links or attachments in phishing emails, on social media sites like Facebook and Twitter or even "ads" on websites that look legitimate. Criminals have gotten much better at making them look authentic, as if they come from a friend, family member or major, established companies like those that ship products to your home.

THE FIX: Be skeptical of everything, and to click only on links that they are certain have come from a trusted sender. Never include information of a personal nature, like credit card numbers, with an email.

2 Unauthorized application or cloud use: Dan Lohrmann, chief strategist and CSO at Security Mentor, said this includes posting private, or uncontrolled, data to the cloud.

This comes in a lot of forms. Anything from installing 'gotomypc' to

buying cloud virtual machines and using them for corporate purposes. It is amazing how people can do these things without realizing the dangers.

THE FIX: Use a trusted cloud storage system, and make yourself aware of what is appropriate to store in the cloud. If the data being stored is confidential, it should probably stay on premise.

3 Weak or misused passwords: It doesn't take an expert to know that using a default or simple password is like leaving your door unlocked. But misuse also includes using the same password for multiple sites and sharing them with friends or coworkers.

Because everything demands a password we tend to do a lot of credential duplication between our various sites. But this is a critical and sometimes tragic error. Many crucial accounts are hacked because an attacker gets access to email or some other seemingly innocuous account where users have reused their credentials with another far more sensitive account, such as banking or health care.

THE FIX: Make it easier to manage multiple, complex passwords, to reduce the incentive to re-use them. Security and encryption guru and Co3 Systems CTO Bruce Schneier is among numerous experts who have recommended creating passwords by using the first letters of a phrase or sentence that is easy to remember, with a few numbers and/or symbols thrown in. He and others also recommend using a password manager -- there are a number available.

Two-factor authentication also improves security, especially for common apps such as Google Gmail or Facebook, experts say. So don't rely on a password alone.

4 Remote insecurity: This is the common practice of transferring files between work and personal computers when working from home, or allowing family members to use a work device at home. It can also include backing up corporate data to a third-party cloud service. This not only exposes the company to malware, but also leaves data and data residue -- data left post deletion that can be retrieved with proper tools -- on an unmanaged system.

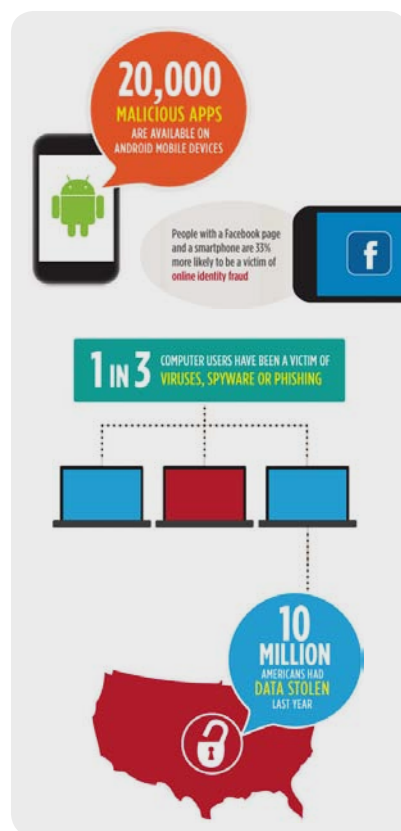
THE FIX: Be sure not to mix business with recreation. Keep your work devices for work, and your personal devices to use at home. This will ensure that you keep your data separated, and protect both your work and your personal devices.

5 Clueless social networking: The advantage of social networking is that it allows us to be much more collaborative and productive. But, among obvious risks is that confidential information gets posted on networking sites or in the cloud, where it is beyond our control.

THE FIX: Stay abreast of new social media scams and tricks. These sites are changing on a regular basis, so make it a priority to sit down and learn about their changing threat landscapes on a regular basis.

6 Poor mobile security: Millions of devices are being used in coffee shops, on mass transportation and other places with public Wi-Fi. Far too many of them are not even protected by rigorous encryption or good mobile device management (MDM). Even more are not even protected by a PIN.

THE FIX: Have a PIN for your device. Be aware of their surroundings in public places -- coffee shops, airports, train stations, shopping malls and other areas



where criminals can get personal information from something as low-tech as shoulder surfing. Make sure that your corporate data is encrypted, end-to-end.


7 Failure to update or patch software: One of the most common security mistakes, mostly the result of the "can't be bothered" syndrome. The risk is obvious -- it leaves devices exposed to new threats, whose creators are actively seeking targets before their window of opportunity closes.

THE FIX: This is as obvious as the risk -- install updates as soon as they are available, or if that's impossible, create a reminder to do it as soon as possible. Most take less time to install than a trip to the water cooler. ▽



Securing Enterprise in the UAE

Ibrahim Mohamed Lari, Chief Executive Officer, Injazat Data Systems

 **In the era of global** economy, ever-changing enterprise risk, cross-organization collaboration and online trade, IT security threats globally and in the Middle East have grown exponentially and are more sophisticated than ever. Therefore, the market has seen a shift towards the adoption of managed security services as a response to the growing cyber-attacks. Enterprises have started considering outsourcing security solutions as they find themselves ill equipped to handle complex and multiple cyber threats.

A recent study by Frost & Sullivan shows that the adoption

of managed security services in GCC countries is set to grow as organizations struggle with the complexities of securing their networks against targeted attacks. The report also found that the managed security services market in GCC that earned revenues around \$58m in 2013 is expected to reach \$215.6m by 2020.

Now more than ever, it is critical to protect the uptime of businesses, information and data within the UAE by implementing proactive steps to safeguard against threats whilst abiding by global best practices. It is critical that enterprises in the UAE be more proactive with security monitoring

Managed security services in the GCC are expected to grow

4x
by 2020

in order to identify, react and respond to security events and incidents.

With this need for robust defense measures to minimize security incidents causing

disruptions to critical business functions and affecting customers, Injazat Data Systems, an industry-recognized market leader for IT, Cloud and Data Center Managed Services, has designed the next generation Security Operation Center services. The new services are aimed at supporting the IT security needs of UAE enterprises in line with global best practices, as well as with local government regulatory and compliance requirements.

Injazat's locally based Security Operation Center solutions for enterprise customers are delivered from the UAE's most resilient and secure government-owned Tier 4 facility on a 24 x 7 basis to meet enterprise customer security requirements. The Security Operation Center solutions deliver a tailored set of security services and solutions to meet local security requirements and needs of UAE public and private enterprises. They also offer Managed Security Log Collection and Retention Services, Managed Security Information and Event Management and Managed Security Incident Management Service.

The ever growing and rapidly changing threats and vulnerabilities in the UAE will make enterprise IT security highly complex, requiring services of experienced managed security services providers such as Injazat. As more and more commercial and government

EMPLOYEE SPOTLIGHT

*Mariam Eissa, Information Security Professional,
Injazat Data Systems*



Mariam Mohammed Eissa has been a part of the team at Injazat since 2006. As an Information Security Professional at the company, she knows more than most how important it is to keep the data and information generated at Injazat, and with Injazat partners, secure. In her role, she performs business impact analysis exercises with a variety of clients and provides consultancy to the Chief Information Officers of Injazat clients.

Not only is she passionate about providing appropriate information for company clients, she is also determined to keep Injazat employees abreast of changes and developments in the security threat landscape. As such, she develops training and

awareness programs for Injazat Data Systems and promotes information security compliance throughout the company.

In case something does go awry, Eissa investigates noncompliance and alerts as well as executes disaster recovery procedures. In short, when it comes to security compliance and awareness, Eissa is an employee that Injazat is lucky to have.

To keep her finger on the pulse of Injazat, Eissa coordinates with other departments frequently. Her organizational skills and ability to work effectively in teams has contributed to her success at the company. From her software skills to her ability to update hardware, Eissa has a reputation for providing solutions – both in fluent Arabic and English.

organizations in the UAE view security as a core consideration, we will see a steady investment and adoption of various security

technologies and are confident that our fresh technologies and cutting-edge solutions will help mitigate security threats within the UAE. ▀

A man with a beard, wearing a white thobe and a white ghutra with a black agal, is sitting at a dark wooden desk. His hands are clasped in front of him. He is looking directly at the camera with a neutral expression. The background is a plain, light-colored wall. A black office chair is visible behind him.

INTERVIEW:
**Atif Albraiki – Head of
Applications Division**



Welcome to Injazat! As you are new to the company, perhaps you can tell us a little bit about your history and what brought you to the company.

Thank you. Well, I completed my Bachelor of Science and Master of Science degrees in Computer Engineering from Syracuse University, New York. I started my career at Zakum Development Company (ZADCO) and later joined C4 Advanced Solutions (C4AS). In 2013 I was appointed as Applications Group Manager in C4AS. In that capacity I was leading software development delivery capabilities for one of C4AS' main managed services account. About five months ago I joined Injazat Data Systems as Head of Applications.

Injazat Data Systems is recognized as a pioneer in IT Outsourcing, Application Services, Cloud and many other innovative solutions in the UAE market. What brought me to Injazat is to be a key player within the organization to further shape the ICT sector in the UAE and to further challenge myself as I grow in my career.

What are your goals for the Applications Division at Injazat?

Supporting our clients in meeting their goals and exceeding their expectations will always be our primary focus. In turn, our goal in the Applications Division will be to ensure that our delivery model is agile enough to adapt to the rapid changes in the technology

market. We will continue building our current capabilities, with more focus put into further building our Enterprise Mobility and Big Data Analytics capabilities. We will be looking at introducing innovative market offerings that leverage Injazat's core strengths and key differentiators.

The technology sector has gone through tremendous transformation in the past few years. This has brought opportunities as well as challenges that we as Injazat need to consider and address in order to strengthen our market position and play a lead role in shaping the ICT sector in the UAE.

What strengths do you see in your team at Injazat so far that you hope to leverage to achieve your goals?

Strong technical delivery capabilities, team dedication, and collective

ownership spirit are core strengths of Injazat's Applications team. These team qualities are the key success factors of our application services. These qualities are also totally aligned with our core values at Injazat: Commitment, Honesty

with Respect, Accountability, Results Driven, and Trust (CHART).

We will leverage these core strengths to achieve our goals while knowing that the journey to excellence never ends. Therefore, it is crucial that we continuously strive to improve and excel, especially in the dynamic technology sector we are in. We have identified improvement initiatives within applications team, some of which we have already initiated. We will also continue introducing more initiatives to adapt to changes and streamline our

technological expertise as part of our continuous improvement efforts. ▀

The technology sector has gone through tremendous transformation in the past few years. This has brought opportunities as well as challenges that we as Injazat need to consider and address in order to strengthen our market position and play a lead role in shaping the ICT sector in the UAE.

Injazat accelerates innovation and supports UAE's economic growth in partnership with SAP

IDC Projects IT Spending in UAE Will Grow by 74 Percent by 2017

Injazat Data Systems signed an agreement with global technology corporation SAP to accelerate innovation in the UAE.

Under the agreement, SAP and Injazat will join forces to provide customers with SAP Business Applications on a fully-managed secure cloud that enables real-time analysis of Big Data, while reducing cost, time to value, and risk.

Both the Abu Dhabi Vision 2030 and UAE Vision 2021 call for enhancing a safe and secure society, backed by a sustainable knowledge-based and globalized economy, driven by strong growth in the education, healthcare, and infrastructure sectors.

The UAE's public sector is playing a key role in the country's IT growth, with researchers at IDC projecting the country's IT market to grow by 74 percent from USD 4.63 billion in 2014 to USD 8.06 billion by 2017.

With SAP HANA Enterprise on the Cloud (HEC), Injazat can expand its portfolio of data storage solutions, online and mobile initiatives, while supporting its regional expansion plans.

Providing a single gateway for business solutions, services, and expertise, SAP enables organizations on SAP HEC to access fully array of SAP solution such as Financials, CRM, SCM, Procurement, and Financials.

Mubadala acquires HP's 40% stake in Injazat Data Systems

Hewlett-Packard has sold its 40 per cent stake in UAE cloud services firm Injazat Data Systems for an undisclosed amount to Mubadala.

Abu Dhabi strategic investor Mubadala, which has stakes in General Electric and private equity firm Carlyle, now owns 100 per cent of Injazat, which provides information technology outsourcing, and cloud and data center

managed services.

Injazat built the region's first tier 4 data center — designed to the highest possible security and environmental standards.

"We combined local expertise with HP's knowledge and global reach ... We will continue offering HP's exceptional services, in addition to a broader range of IT products," said Ibrahim Lari, the chief executive of Injazat.

Injazat Data Systems cooperate with Kaspersky Lab to develop the security industry in the region

Injazat signed an agreement with Kaspersky Lab to develop high-quality IT solutions powered by Kaspersky Lab's leading security technologies and expertise to make IT systems in the region more secure.

Under the terms of the agreement, Injazat and Kaspersky Lab will share expertise in various cyber security domains and jointly pursue business opportunities in the UAE and other parts of the GCC. The MoU anticipates a wide range of services and activities, including:

- professional training on cyber security forensics and malware binary reverse engineering;
- educational initiatives to raise cyber safety

- awareness among employees;
- remote and on-site malware incident response handling;
- security intelligence including malware statistics, epidemic alerts, and global malware tracking;
- security assessments including pen-testing and IT security audits;
- provision of services to regional customers based on Kaspersky Security Network data;
- web site security.

The signatories will initially work to prepare a training program schedule for 2015, deploy Kaspersky Lab products at Injazat's premises, and develop an interaction protocol to respond to malware incidents that will eventually form part of customer services, among others.

Injazat Data Systems & Abu Dhabi Polytechnic sign MOU to develop UAE National Capability in the ICT industry

Injazat Data Systems has signed a Memorandum of Understanding (MOU) with Abu Dhabi Polytechnic to collaboratively train and develop select Information Security (IS) recruits to support the increasing demand of cyber security experts in the UAE.

Under the terms of the MOU, Injazat and Abu Dhabi Polytechnic will co-develop scholarship opportunities and unique training programs for selected elite students from the Polytechnic's Information Security Program. Injazat will also develop employment prospects for these students.

Abu Dhabi Polytechnic, a governmental entity managed by Abu Dhabi's Institute of Applied Technology, is a promising source of tomorrow's business experts,

professionals and leaders. It offers various courses geared towards harnessing emerging technologies in support of Abu Dhabi Economic Vision 2030. The institution provides rigorous education and training, often requiring its students to go outside of the country to find the best facilities for highly specialized training.

Injazat currently has more than 91 Emiratis in strategic managerial, technical and professional positions accounting for 15 per cent of its workforce. It regularly enrolls UAE Nationals in globally-recognized certification programs, provides them with intensive coaching and mentoring support, and develops clear and comprehensive Career Development Plans (CDP) for them.

Injazat showcases innovative services at GITEX 2014

Injazat Data Systems participated at GITEX Technology Week, which took place at the Dubai World Trade Centre.

During the tradeshow, Injazat displayed its secure and

smart IT solutions that help develop and transform the UAE into an Information and Communications Technology (ICT) hub. It also specifically focused on cloud computing, security and mobility.

Al Ain City Municipality collaborates with Injazat Data Systems in developing and implementing a Smart Government Transformation Program

The Abu Dhabi Government has the goal of becoming one of the top e-governments in the world. It aspires to achieve its ambitions by improving its service delivery and customer satisfaction while aiming at E-Government Excellence. In line with this strategy, the Al Ain City Municipality (AACM) and Injazat Data Systems announced the implementation of a comprehensive Business Integration Platform, which will act as a strong foundation for the Smart Government initiative. This move is expected to further improve government services, customer experience and help achieve the strategic objectives set forth by the Abu Dhabi government.

AACM is amongst the first few Abu Dhabi Government organizations to achieve such a milestone, Falling in line with Abu Dhabi Systems and Information Centre (ADSIC) objectives of having a Service Oriented Architecture (SOA) based infrastructure and services, the project transformed existing challenges such as lack of real-time visibility, integration complications, and inefficiency into an integrated, more effective, agile, scalable and reliable platform that could cater to current and future needs of the UAE citizens. The solution is based on Oracle Fusion Middleware technology stack and HP Enterprise Management tool sets.

About US

Injazat Data Systems is an industry recognized market leader in the region for Information Technology Outsourcing, Data Center and Managed Services. The Injazat Data Center is both Tier IV design and ISO 27001 certified, a distinction that differentiates it as one of the unique facilities in the region.

Our SERVICES

IT outsourcing:

We offer end-to-end IT services to enable our clients in building and managing a highly available IT platform that meets their business and security objectives.

Enterprise Cloud Services:

Injazat supports your business with a pay-as-you-go approach without any upfront capital investment, delivered locally from its Data Center.

Data Center Managed Services:

We offer a wide range of managed services out of our Tier IV design and ISO 27001 certified Data Center, which provides a highly reliable and secure platform, along with world class 24/7 delivery standards.

Learning and Development:

The Injazat Institute aims to enhance the competency of UAE professionals and improve their ability to support their organizations.

Enterprise Applications:

We collaborate with clients to align their organizations' applications with business priorities and operational requirements.

Consulting and Business Process Outsourcing:

Our portfolio of BPO, consulting solutions, and project management will help you drive revenue growth and maximize operational and organizational efficiency.

Our VISION

To be the trusted technology partner of choice for Enterprise Clients and to play a catalyst role in transforming the ICT industry in UAE.

Our MISSION

To support the success of our clients by providing reliable, high quality and innovative IT services and solutions while accomplishing our social obligations and responsibilities for developing ICT sector and talent pool in UAE.

Our CORE VALUES

At Injazat we live by a set of values that drive our behaviors daily and enable us to achieve our vision and goals.

Our values express the expectations we have of each other and ourselves and identify how we conduct business with our clients. Each employee is personally accountable for reflecting the following values in his/her business decisions and actions.

Trust: We take pride in building trust with our clients, ourselves and others.

Honesty with Respect: We will be as open as we can be with our clients and our people, consistent with keeping the business on a sound footing.

Commitment: We recognize the importance of providing excellence and creating an environment where commitment is part of the fabric of who we are.

Accountability: We behave in responsive manner, providing feedback, following through and by being accessible.

Results driven: We seek to deliver excellent results and ensure our clients and customers experiences exceed their expectations.