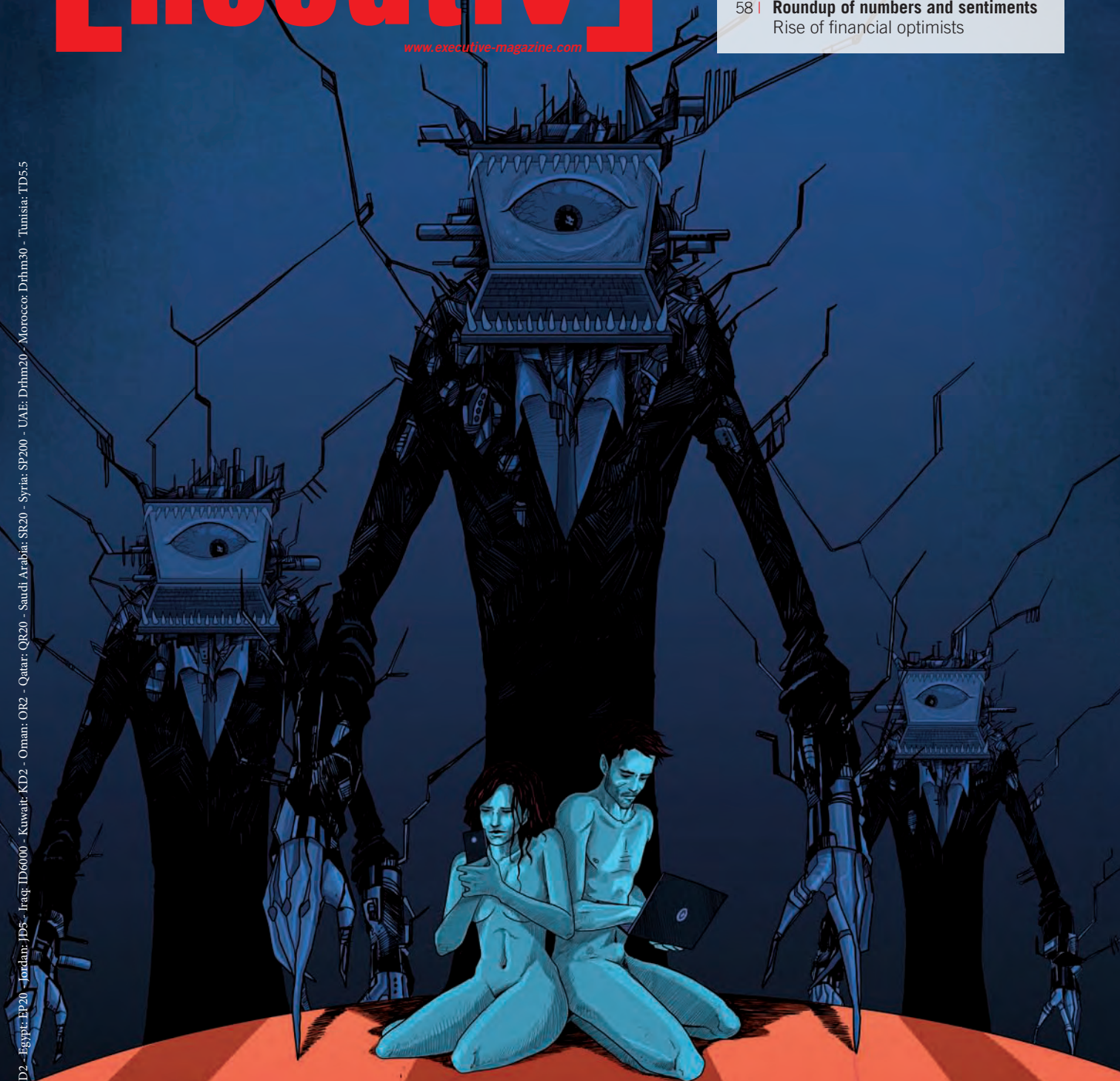


Executive3

www.executive-magazine.com

- 10 | **Dashing our hopes for reform**
After a four-year Parliament extension, we demand elections in 2017
- 52 | **Access to information law**
Obstacles, benefits and the need for anti-corruption commission
- 58 | **Roundup of numbers and sentiments**
Rise of financial optimists

Lebanon: LL 10,000 - Bahrain: BD2 - Egypt: EP20 - Jordan: JD5 - Iraq: ID6000 - Kuwait: KD2 - Oman: OR2 - Qatar: QR20 - Saudi Arabia: SR20 - Syria: SP200 - UAE: Dh100 - Morocco: Dh100 - Tunisia: TD5.5



EXPOSED

The state of Lebanon's cyberdefense

THE 2017 TERRAIN

READY FOR ANYTHING
STARTING FROM \$29,900
VAT INCLUDED &
FREE REGISTRATION



GMC

COMMANDS RESPECT

VISIT GMC.RYMCO.COM OR VISIT OUR SHOWROOM FOR MORE INFORMATION

*Specifications may vary by trim



1599

Rasamey Younis Motor Company is listed on the Beirut stock exchange

RYMCO
DRIVE LIFE

EDITORIAL

#211

Recourse to reform

I can remember hiding from the bullets and bombs in the bathroom with my mom and brother. My father was out trying to earn a living, and the worry that he would not make it home made me sick to my stomach on a daily basis. We lived in hell as militias destroyed this country and its once-strong economy and currency. When we finally escaped, we headed for Canada. Arriving as immigrants, we were graciously welcomed and provided with every right the developed country had to offer. Except one. The most precious right. The right to vote. We were told that only after we proved worthy would that right be granted to us.

The men who literally destroyed this country were somehow entrusted with rebuilding it. They have unequivocally failed. This country is a crumbling mess, when it has the potential to be a regional economic powerhouse. The gross mismanagement is shameful. We have the drive and the talent, what we need now are elected officials who will take immediate action to improve Lebanon's physical and legal infrastructure.

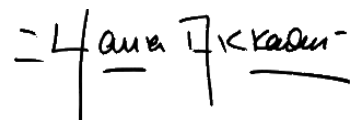
Take the national approach to cybersecurity, for example. We don't have laws to protect citizens online, much less laws to enable and nurture business development on the web. Hell, we don't even have the infrastructure for modern internet connections. Passing laws and investing in infrastructure are low-hanging fruit the people have been begging for over the last ten years. This is simple, but our politicians are deaf. Instead of a booming digital economy, we have broken promises and draft laws ignored by an arguably unconstitutional Parliament.

The failure to find a fair and representative electoral law is unacceptable. I'm sick to death and angry, but sadly, not surprised. In the 1980s, our politicians were combatants who did not respect our right to live. Why would they respect our right to vote 30 years later?

Let's not lie to ourselves, there is no real opposition to the ruling class in this country. We call ourselves a democracy, but our election results are no different than those in dictatorships. People took to the streets to protest during the garbage crisis in mid-2015. Today, as our most precious right is being stolen AGAIN, the streets are silent.

We must begin to fight back. We deserve a standard of living that is very easily within reach. It will not take a generation to pull us out of the mess we are in, if we take the work seriously. Our problems are very well understood. Solutions are literally on the table. We need parliamentarians willing to work for Lebanon, and no matter which electoral law our princes decide on, we must stand against them.

Stealing back just a few parliamentary seats at a time would be a win. We need unity and focus. We have the ideas as well as the solutions. Let's make sure our grandchildren do not end up hiding in a bathroom or queuing in an immigration line.



Yasser Akkaoui
Editor-in-chief

CONTENTS

#211

LAST MONTH

- 6 February's essential headlines

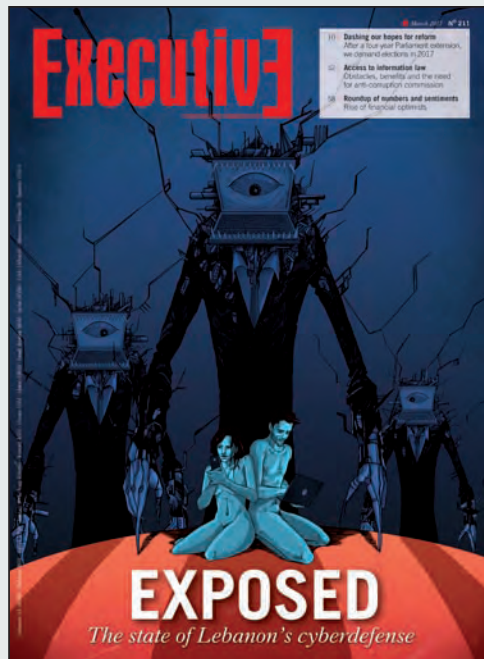
LEADERS

- 10 **Dashing our hopes for reform**
After a four-year Parliament extension, we demand elections in 2017
- 12 **Protect us from the modern plague**
Lebanon remains overwhelmingly vulnerable to cyberwarfare
- 14 **Rare opportunity**
People now have the right to request information from public entities

52

**SPECIAL
FEATURE
ACCESS TO
INFORMATION
LAW**

- 52 **A step towards transparency**
Obstacles, benefits and the need for an anti-corruption commission
- 53 **Q&A with Ghassan Moukheiber**
On the ACC, its tasks and potential formation
- 54 **Explainer**
Infographic



CYBER SECURITY

- 16 | The battle between good and evil goes virtual
- 24 | Cyber (in)securities
- 30 | Securing the entrepreneurship ecosystem
- 32 | The Lebanese cybersecurity landscape
- 38 | Propaganda goes viral
- 40 | The public sector's vulnerability to a cyberattack
- 44 | Cyberthreats in the GCC and the Middle East
- 48 | How to protect your email from cyberattacks

BANKING & FINANCE

- 58 **Roundup of numbers and sentiments**
Rise of financial optimists

HOSPITALITY & TOURISM

- 62 **A grand hotel plots a new course**
Phoenicia Beirut's GM talks upcoming plans and her vision for 2017

EXECUTIVE LIFE

- 66 **Nada Abou Farhat delivers in tailor-made "Heble, En Cinq"**
Gabriel Yammine's dark comedy at Metro Al Madina
- 70 **Blind date at Sfeir-Semler Gallery**
Art exhibition opens space for seven new artists

BUSINESS ESSENTIALS

- 72 Company bulletin
- 76 Conferences & exhibitions

LAST WORD

- 80 **Lebanon's national budget**
A strategic instrument for adequate policymaking

blombank.com
+961 1 753000

LOST YOUR CARD WHILE ABROAD AND NEED TO CANCEL IT?

Easy! With eBLOM's Live Chat service, you can connect with a BLOM representative anytime, anywhere in the world, and get the instant banking support you need.



Executive

Responsible director Antoine Chidiac
Managing director & editor-in-chief Yasser Akkaoui

Editor-at-large Thomas Schellen
Real estate & industry editor Matt Nash
Hospitality & tourism editor Nabila Rahhal
Economics & policy editor Jeremy Arbid
Deputy editor Sarah Shaar
Executive Life editor Olga Habre
Photojournalist Greg Demarque
(Additional photos from AB, NET, ID, G.)
Illustration Ivan Debs
Art direction Tanya Salem of Smart Box sarl
Visualization & infographics Ahmad Barclay
Contributors Nicole Purin, Magali Hardan

Operations manager Lucy Moussa
Web development manager Magali Hardan
Marketing representative Karine Ayoub Mattar
Print & online advertising Michele Hobeika
Public relations manager Maguy Ghorayeb
Subscriptions manager Roula Emanuel
Subscriptions Gladys Najjar
Distribution manager Katia Massoud
Accountant Fadi Bechara

Published by NewsMedia sal

Sehnaoui Center, 7th floor, Ashrafieh, Beirut
Tel/fax: 01/611-696
editorial@executive.com.lb

Contact us – We need your input.
Please contact us with any suggestions or comments at:
www.executive-magazine.com or
editorial@executive.com.lb

For subscriptions – subscribers@executive.com.lb

© 2015 All rights reserved. Copying for purposes other than personal or internal reference use without express written permission from NewsMedia sal is prohibited.

AIRFRANCE

FRANCE IS IN THE AIR



A PEACEFUL HAVEN

Discover the intimacy of our Premium Economy cabin

FROM BEIRUT

PARIS

BORDEAUX

STARTING FROM

\$699

 R/T
ATI

\$1039

 R/T
ATI

AIRFRANCE KLM

AIRFRANCE.COM.LB

*Round trip fares, all taxes included, in Premium Economy Cabin. Buy until 31/03, travel until 30/11/2017, on AF565 flight only from Beirut. Black out period between 13 and 23/04/2017. Call us on 01 999169, visit airfrance.com.lb or your usual point of sales.

LAST MONTH

ZOOM IN



Right-wing French presidential candidate, Marine Le Pen, raises eyebrows during a visit to Lebanon.

Trump says two-state solution to Israeli-Palestinian conflict not only option

In an extraordinary dismissal of long standing US government policy, President Donald Trump seemingly threw aside previous insistence that any peace solution come with a separate Palestinian state during a joint news conference with Israeli Prime Minister Benjamin Netanyahu on February 15.

Speaking at the conference, the new American president stated, “I’m looking at two-state and one-state, and I like the one that both parties like. I’m very happy with the one that both parties like. I can live with either one. I thought for awhile it looked like the two-state might be the easier of the two – but honestly if Bibi, if Israel and the Palestinians are happy, I’m happy with the one they like the best.”

During the press conference, Trump was seemingly unaware of many of the finer points of the Middle East peace process. His comments sparked widespread controversy and concern globally.

He has since partially clarified his comments to Reuters on February 25, stating a pref-

erence toward a two-state solution but stopping short of reasserting US commitment to Palestinian statehood.

Le Pen cancels meeting with Grand Mufti over veil controversy

French far-right leader, Marine Le Pen, scored a PR victory during her visit to Lebanon on February 21, after a meeting between her and Grand Mufti Abdel-Latif Derian was cancelled over her refusal to wear a headscarf.

Le Pen, a leading candidate in the poll for the first round of presidential elections in France set for April 23, is running on a platform of anti-immigration and anti-EU policies. The National Front leader is a controversial figure, despite her efforts to detoxify the party’s image. Similar to other far right movements in Europe, Le Pen has been capitalizing on fears of terrorism to push an anti-Islam, anti-immigrant agenda.

Her refusal to wear the veil, a traditionally accepted practice when meeting with the Grand Mufti, was hailed a feminist victory by her supporters, yet reports suggested that Le

TRUST ONE SIGNATURE ONLY

We Keep Our Word.®

**FREE YEARLY COMPULSORY
MOTOR INSURANCE FOR
BODILY INJURY**

**LIFE INSURANCE ON
CARD'S OUTSTANDING
BALANCE**



**DOUBLE POINTS/MILES
AT AROPE INSURANCE**

**SPECIAL DISCOUNT ON
INSURANCE POLICIES**

Apply Online

WWW.AROPE.COM

VISA



We Keep Our Word.®

AROPE INSURANCE S.A.L. Fully Paid Capital, LBP 43,200,000,000 | Zalka . Michel Murr Str. AROPE Bldg.,
P.O.Box 113 - 5686 Beirut . Lebanon **T.** 961 1 905777 | **F.** 961 1 886786 | arope@arope.com | www.arope.com



BLOM BANK GROUP

LAST MONTH

QUOTE OF THE MONTH

"I hope France will make a better choice than this right-wing fascist."

Lebanese Druze leader Walid Jumblatt

Pen had been well aware of the requirement in advance of the meeting, offering no objections until she arrived at Dar al-Fatwa in Beirut.

Her visit to Lebanon was also reported on by far-right site Breitbart, who wrote she was coming to show her support to the country's "persecuted" Christians. During her visit Le Pen met with President Michel Aoun, her first official one-on-one meeting with a head of state, along with other Lebanese officials.

Comments made by Le Pen during her visit, including renewal of her support for the Assad government, also proved controversial.

Israeli raid strikes Lebanese-Syrian border

Israeli warplanes struck posts along the Lebanese border with Syria on February 22, during pre-dawn raids around 3am. At least six rockets were said to have hit in the outskirts of Qalamoun, near the Lebanese town of Nahleh.

The target of the strikes however, was not clear. Hezbollah issued a statement on Twitter that denied the raid had targeted their posts near the town's outskirts. Israeli newspaper Haaretz reported comments from the head of the Syrian Observatory that confirmed the raid took place, but said that it was not clear if it targeted Syrian army or Hezbollah sites.

Israel has remained quiet about the raid, but reports suggest it was targeting weapons heading for Hezbollah and was taken as part of the red lines the country has drawn to prevent the group from gaining advanced weaponry.

Israel has struck targets in Syria in the past and frequently violates Lebanese airspace.

Abbas visits Lebanon amid Ain al-Hilweh unrest

Palestinian President Mahmoud Abbas arrived in Lebanon on February 23, on a three-day visit to meet with Lebanese officials amid tensions between Palestinian factions in the country. His was the first visit by an Arab leader since the election of Michel Aoun in October 2016.


Clashes had erupted the same day in the Ain al-Hilweh camp, the largest refugee camp for Palestinians in Lebanon. The Lebanese army was placed on high alert after gunbattles erupted in the Safsaf neighborhood of the camp, a stronghold for Islamists. The troubles allegedly began after a woman from the Barakat neighborhood was verbally harassed when passing by Safsaf. A tentative cease-fire brokered collapsed on February 28 with renewed clashes.

The latest security incidents come after the joint Palestinian security force, implemented in 2014, was dissolved on February 25, following several factions in the Higher Palestinian Security Committee resignation. Each faction in the camp now secures its own territory.

New election law remains a distant dream

Lebanon remains without an update to its controversial 1960 vote law in advance of upcoming elections scheduled for May 21. Interior Minister Nouhad Machnouk and Prime Minister Saad Hariri have both signed a decree calling for voters to participate in the upcoming elections that by law was necessary three months prior to the elections on February 21. However, no agreement has been found over any proposal to change the current majoritarian electoral law into one with more proportional representation.

Speaking on February 27, Speaker Nabih Berri stated that adopting the 1960 law would be a better option than extending the Parliament's tenure, offering a new deadline for agreement on a new law by April 17.

Parliament has extended its mandate twice, citing security concerns along with opposition to the current voting law among many parties. The last general election took place in 2009. 



EXCLUSIVELY MADE IN ITALY & AVAILABLE AT:

Paul&Shark Boutique - 27/6 Allenby Street • ABC Dbayeh - ABC Mall, L3 • ABC Ashrafieh - ABC Mall, L3

Paul&Shark Boutique - El Mina Street, Tripoli • City Centre Beirut - Hazmieh, L2

Customer Care + 961 1 97 18 18 • www.paulshark.it

MALIAMODA
Member of Malia Group

LEADERS

ELECTORAL LAW

Dashing our hopes for reform

After a four-year Parliament extension, we demand elections in 2017

Back in 2013, Parliament extended its own mandate in part to allow it more time to agree on a fair and representative electoral law. Instead of spending four years working toward this goal, the legislature did very little with the four extra years in office it granted itself. From the second the ink dried on Parliament's second term extension (remember, the four years were granted in two chunks), it was clear a new law needed to be agreed prior to February 21, 2017—the date on which the current law says voters must be welcomed to the polls scheduled for May 21.

Missing that deadline is inexcusable. When President Michel Aoun as-

sumed office in late October 2016, it was clear the government formed as a result of his election would be short-lived, with a very narrow mandate: choosing a new electoral law. Instead of immediately getting to work on agreeing to a more fair and representative electoral law during cabinet sessions, this debate has been held in secret among political parties. While some of the work cabinet and Parliament have done since December is important and helps build confidence (such as passing the oil and gas decrees and legislating the right to information), political life in this country is once again seemingly grinding to a halt, evidenced by deadlock over not only a new electoral law, but over the country's first budget in more than 10 years.

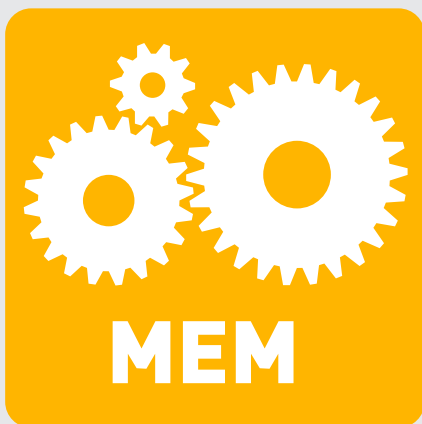
At the moment our economy needs confidence more than anything. Even if the political class had passed a "reformed" electoral law, there's no doubt it would have been

fine-tuned to best serve the parties in power. So while we defend and still hope for the actual implementation of the constitution (including elections free of sectarian quotas and creation of a Senate), we realize getting there will be a slow process. In the immediate term, we simply need the government to meet the minimum requirement of holding parliamentary elections as soon as practicable.

Parliament Speaker Nabih Berri recently set April 17 as a new deadline by which a decision on an electoral law must be made. Our politicians cannot miss another deadline. We want the process of drafting a new electoral law to be transparent. We want that law to be fair and representative. We are, however, realistic and reluctantly accept that reform might not materialize this year. No matter which law is used, we demand elections in 2017. We've waited long enough.



■ Parliament Speaker Nabih Berri recently set April 17 as a new deadline



MASTER EN MANAGEMENT

RECRUTEMENT EN COURS

Un cursus conçu pour une intégration rapide
sur le marché du travail

2 diplômes internationaux à la clé

UN PARCOURS EN DEUX ANS:

Année 1 - MASTER 1

Formation généraliste en management

Année 2 - MASTER 2

2 choix :

1-Parcours ESA : parcours de spécialisation

Deux Majeures de spécialisation au choix :

- Finance
- Marketing

2-Parcours d'échange avec une des Écoles partenaires
de l'ESA : ESCP Europe – Skema Business School –
Neoma Business School

Voyage d'étude international

Le MEM forme les futurs managers destinés à évoluer aisément dans des environnements compétitifs. Les entreprises de leur côté recherchent des jeunes diplômés répondant aux besoins des milieux économiques libanais et internationaux.

L'objectif de la formation est d'amener les étudiants à approfondir et maîtriser les théories et les outils nécessaires pour une insertion professionnelle réussie. Le programme procure aux élèves une vision stratégique de l'entreprise, des compétences opérationnelles et une capacité à prendre des décisions et induire le changement dans le but de devenir des collaborateurs efficaces dans leurs domaines respectifs.

En partenariat avec



une école gérée par la



**LEADERS
DE DEMAIN**

LEADERS

CYBERSECURITY

Protect us from the modern plague

Lebanon remains overwhelmingly vulnerable to cyberwarfare

When modernity was sending out its first rays of thought in the Enlightenment Age, thinker Thomas Hobbes wrote speculatively that the natural state of man is “war of all against all.” Overcoming the universal conflict to him was the central historical argument for the formation of states. Captivating and influential as his frightful idea of constant warfare as man’s original *modus operandi* was, it stands in history as a construct that could not be corroborated. We desire peace and are accustomed to existing in an interplay of conflict and harmony, in which we grudgingly live through periods of war, only in hope of a new peace. Until now.

More than ever before, the digital age could bring mankind closer to a situation of, albeit virtual, war of all against all. This is not talk of some online game. Cyberwarfare, cyberterrorism and organized cybercrime comprise a devilish triangle that is growing more sophisticated, more intense in its attacks, more devious, more profitable and greedier by the minute. Microsoft’s Chief Technology Officer for the Middle East, Nasser Kettani, tells *EXECUTIVE* of assumptions that cybercrime will grow from a \$500 billion impact on the world economy in 2015 to a staggering \$4 trillion impact by 2020 (see overview page 16). Cybercrime already reaps more profit than the illicit drug trade, but if the projections above prove correct, the impact of cybercrime will scale up from less than 1 percent of the world’s GDP to over 4 percent in just a few years – the International Monetary Fund (IMF) projects world GDP for 2020 to be \$93.6 trillion.

This is bad enough for an illicit

economic impact and sure to bring about unwelcome distortions to the societal equilibriums within states around the world, raising the specter of the type of disorder that existed in Prohibition-era America just before the Great Depression. What is even more frightening is that nobody is safe from deliberate cyberattacks – no government, corporate entity or individual. Under most social contracts of the modern age, people trusted their states with what sociologist Max Weber called the “monopoly on the legitimate use of physical force” in times of peace because they expected the state to guard them, broadly in line with Hobbes’ reasoning about the state’s role and *raison d’être*.

PROTECTION

This protection was never complete. Interpersonal violence and organized crime were the troubling exceptions to the state’s power of protection. But now, in the digital age, it seems that disruptive forces – whether cybercrime-syndicates, terrorist organizations or even hostile states – are punching many holes in the protective ability of nation states over our digital lives, which are increasing in importance as the new dimension that is being added to human existence in the internet age.

Even in full awareness of the many challenges that Lebanon’s (almost) elected parliamentarians face in this time, *EXECUTIVE* calls for urgent implementation of the long overdue legislation on our digital rights and the best possible protection by the Lebanese state in the digital world to its citizens and residents. In the long run, digital rights may very well be as important as the voting rights, on whose timely implementation this year *EXECUTIVE* insists in the sharpest form possible. For Lebanese citizens and the economy, the state’s contribution to protection against cybercrime through appropriate legal frameworks with stiff penalties

will be vital, and so will be the implementation of best defense capabilities through a national Computer Emergency Response Team (CERT).

The world today is full of global dangers and policy challenges, from weapons of mass destruction and ever present dictatorial or totalitarian tendencies to technologically generated scourges. Lebanon, in addition, has its specific political plagues and worries. But let’s not forget that the greatest challenge to social contracts is the challenge to keep the lid on the human capacity for evil and that the noblest challenge for the state in this regard is to protect its people in their freedom. This makes it important for Lebanon to ward off cybercrime and cyberwarfare in the best possible and most globally integrated way. And there is much to do.

LACKLUSTER CYBERSECURITY

Lebanon is presently two decades overdue with its law on digital signatures. The public sector is short of cybersecurity experts in many ministries (see interview page 40). Private sector financial players, namely our banks, are leading in awareness of the importance of cybersecurity, but there are still many issues to be solved in cyber protection of financial institutions (see story page 24), and of the still under-aware and under-concerned companies in other industries.

We are lacking legal penalties that can deter cybercriminals and need the legislative framework, budget and skilled experts to develop a national CERT (computer emergency response teams) as a core element in our cyber defenses. By all expectations, cybersecurity will be one of the most important issues globally in 2017 and beyond. We thus encourage the security agencies to speed up the development of national preparedness for cyberattacks. Most importantly, we call on the Lebanese Parliament and the executive branch to pass and implement necessary cybersecurity legislation now.

THE END OF THE MONTH DOESN'T HAVE TO BE THE END OF THE WORLD

Spread your expenses with BONIFIKA LBP CARD

BONIFIKA LBP TITANIUM, an international credit card in LBP, tailored to fit your needs and lifestyle.

Don't limit yourself to your income. Fulfill your wishes today and pay later. Benefit from various types of insurance coverage and much more with SGBL.



BONIFIKA LBP TITANIUM ☎ 1274

CREDIT CARD



LEADERS

ACCESS TO INFORMATION

Rare opportunity

People now have the right to request information from government entities

Lebanon just got a new tool to promote government transparency and accountability, as well as prevent and fight corruption. Entering into force in February 2017, a new access to information law allows anyone to request specific information from virtually all government entities. From doctors needing public health data, researchers looking for economic and social indicators, bankers, industrialists, retailers and other business owners needing figures to make long-term investments, to journalists investigating government expenditures – anyone can make use of the law, and everyone should. All one has to do is send a request describ-


ing the information sought to the office(s) that might hold it. The access to information law also requires government entities to publish key documents on their websites, including an annual report (see special report pages 52 - 56).

The law is a tool to help battle corruption, anti-corruption activists say, because it would increase the level of transparency between the government and the public. That, by itself, helps mitigate corruption, and information requests can provide the evidence in cases of government fraud, fault and other mistakes.

But to make the law truly effective requires auxiliary legislation. The law prescribes that the government can either deny or ignore information requests, and refusals (or tacit refusals) can be appealed. The body specified to hear appeals, the anti-

corruption commission (ACC), does not yet exist. Legislation to create this institution is in advanced stages, says lawmaker Ghassan Moukheiber (see Q&A page 53). The ACC is urgently needed, and Parliament must make every effort to ratify its legislation before the end of this parliamentary session scheduled to conclude at the end of March. Without the ACC there is still a judicial recourse to hear appeals, but that may be open to interpretation. For appeals, courts might argue that the access to information law specifically states the ACC as the appropriate body to hear these cases and could decline to make a ruling. That would effectively render access to information dead in the water, if the ACC is not established quickly. If the ACC legislation is ratified, forming its board could take time, and the government does not have a great track record in appointing or renewing the mandates of the board of directors of public agencies, or in filling senior administration positions, EXECUTIVE reported last month.

Access to information is also a fundamental right and a necessary condition for significant reductions of government corruption, the United Nations states in its justification for goal 16 of its Sustainable Development Goals (SDGs) initiative for 2030. Passing the legislation is an early public relations win for the government and a positive step toward achieving the UN's SDGs.

EXECUTIVE calls on the public now to exercise its right to information, demand the law's full implementation, the quick ratification of ACC legislation and timely appointment of its board. If the public fails to hold the government to account by mobilizing on these points then the people will lose their right to complain about the never ending maelstrom of incompetence and corruption that passes for governance in Lebanon. 



The right to access information could be hampered by that information never being collected in the first instance.

You see a family recreating art.



At Fidus,
we see a USD 57 million
Van Gogh masterpiece.



We know a good investment when we see one
Private Wealth Management • Trading and Capital Markets • Funds & Structured Products Advisory
+961.1.990600 • www.fidus.com.lb

fidus
WEALTH MANAGEMENT



THE BATTLE BETWEEN GOOD AND EVIL GOES VIRTUAL

Online threats continue to proliferate

The serpent's tale is a powerful narrative that has captured man's attention over millennia. The contemporary version of the story goes something like this: the digital garden at first was created as a lush world filled with smart gadgets, useful computer programs, fun games, social networks and great business opportunities. People were delighted with these gadgets and used them freely to their hearts' content. But then a snake entered this garden and hid in the undergrowth.

This serpent was more cunning than all of the gadgets and programs in the garden. It told people that they could partake in superior knowledge, if they just clicked on its emails and attachments that promised innocent fun and untold riches. But when the people listened to the snake and clicked, viruses and Trojan horses were unleashed and infested the digital garden. Thus, evil was released and proved impossible to eliminate.

In 2017, this ancient serpent is only too real. It is called malware and has reached a proliferation rate that is mind boggling and difficult to comprehend. What does it mean for individuals in the digital world that more than 1 million new malware tools come into existence every three days and that their number keeps growing? Or that more than 500 million personal records were stolen or lost in 2015, according to the 2016 Internet Security Threat Report?



Cybersecurity

■ Spam email increased from 500 spam messages per second in 2012 to 3,500 spam emails per second in 2016

How can an average user visualize, in front of their inner eye, that according to the Cisco Cybersecurity Report 2017, spam email increased from 500 spam messages per second in 2012 to 3,500 spam emails per second in 2016? Moreover, what can one do to protect their mobile phone? At the world's largest congress for innovation and products in this sector – the Mobile World Congress (MWC) last month in Barcelona – security companies like Intel took this opportunity to turn our attention to the vulnerability of our beloved smartphones and pushed their various solutions, such as multi-factor authentication and home security platforms.

Numbers concerning the impact of breaches on businesses are just as bad. According to Cisco's report, which was released at the end of January, of the organizations that experienced cyber breaches, more than one-fifth lost customers after a breach, almost one-third lost revenues, and close to one-



quarter lost business opportunities. Serious damages – more than 20 percent losses of customers, revenue or opportunities – struck about 9 percent, 11 percent and 10 percent of breached organizations, respectively. There are reports by the bucket, which all have in common that they generally document the steady increase of cybercrime and also show that average costs per breach can be life-threatening for small, medium and large businesses.

A GROWING THREAT

Actually, whichever source one checks, all numbers about malware are bad, as malware is growing rapidly. But it is not only mass that matters. The student hackers of before, who did their hacks simply because they could, are still around, as are ideological hacktivists and small-time crooks. Yet the really malignant cyberactors today can be crime syndicates, terrorist organizations and even states. Cyberattacks are no longer like aiming a shotgun on a flock of small birds in the indiscriminate expectation to hit any one of them. They can be as surgical as a remote-controlled scalpel, hitting deliberately sought-out targets that can be a specific bank, government agency, any large corporation, small company, or even a single family or an individual.

With improved organizational skills on top of the high rate of proliferation and the increased sophistication of attack instruments, it is estimated that cybercrime will expand exponentially for years to come. Given a growth rate of internet viruses that would make any ethical company blush with shame for expanding so fast because it would be a sign of being either unsustainable or exploitative, the economic infestation of the digital world with cybercrime is predicted to grow eight-fold in impact by the year 2020.

It can hardly come as a surprise, therefore, that there is an increase in cy-

bersecurity conferences in the Middle East this year (the EXECUTIVE calendar of regional conferences last month listed four conference headers containing the word “cyber” for the period between February and April 2017, up from one event in the same timeframe in 2015 and two in 2016). It is also unsurprising to see the internationally growing flood of alarming reports from the cyberfront, which generally mix dreadful warnings about cybercrime damages, with a pitch for selling this or

■ The really malignant cyberactors today can be crime syndicates, terrorist organizations and even states

that cybersecurity service. But, it nonetheless bears repeating (see leader page 12) that cybercrime is projected to reach \$4 trillion in four years time – *nota bene* about the same magnitude as the GDP of Germany.

Clearly, it has not escaped companies around the world that the only thing we can safely say about our digital lives is that they are not safe. Banks are the biggest prize for many cybercrime syndicates where 2016 and the still young 2017 saw some spectacular international breaches. One large recently reported case involved Lloyds Banking Group in the United Kingdom. Claiming in an overview of its business to be the UK's largest digital bank with 12.5 million online customers, Lloyds Banking Group has 818 billion pounds in assets (2016) and includes Lloyds Bank, Halifax Bank and Bank of Scotland. It was attacked in a distributed denial-of-service (DDoS) assault in January 2017 and for two days was under heavy data fire.

This breach also got a lot of attention because it had been preceded only months before by another successful cyberattack against a UK bank. In that incident it was TESCO Bank that suffered online thefts amounting to about 2.5 million pounds in total. The bank, which has more than 7 million customers, reported that roughly 9,000 customers each had as much as 600 pounds (approximately \$750) siphoned from their accounts and pledged to refund those losses within 24 working hours. But, last year's biggest incident in the financial markets was the criminal exploitation of the SWIFT interbank messaging network via an intrusion into Bangladesh Bank, the country's central bank.

According to a December 2016 statement by security company Kaspersky Lab, this incident constituted “the [world's] biggest financial heist” and used SWIFT-enabled transfers to steal \$100 million, of which many millions appear to have not yet been recovered. According to reports, SWIFT has since updated its network through a global payments innovation (GPI) messaging platform and is asking member banks to take better cybersecurity measures.

Banks in Lebanon are clearly awakening to the challenges they face in the digital realm, or they are at least more aware than they were some years ago, said several Beirut-based cybersecurity experts. Moreover, every local cybersecurity consultant or company that EXECUTIVE talked to said that banks constitute between half and 80 percent of their clientele. However, it seems that there is much room for improvement in the cyberdefense strategies of Lebanon's banking industry (see story page 24), and

Cybersecurity

there are open questions about the statuses of their cybersecurity measures. Some experts said that they found holes in the protection of some banks, and a surprising number of Lebanese banks told EXECUTIVE that they preferred not to give interviews about cybersecurity issues, citing their “sensitive nature”.

The state of Lebanese cybersecurity is much foggier when it comes to the private sector economy outside of banking and the public administration in this country. From missing experts to non-existing budgets and weak awareness, the picture of cybersecurity in civilian government agencies is, politely said, dim and very different from developed countries.

In the United States, for example, the federal authorities are major cybersecurity customers. There is even a specific assessment of this market that estimates annual federal investments into cybersecurity with a recent forecast for spending to grow from \$18 billion in 2017 to \$22 billion by 2022, at a steady compound annual growth rate of 4.4 percent. In the European Union, regulatory cyberframeworks of international consequence have been adopted in 2016 and the EU's General Data Protection Regulation – with steep fees for violators of privacy – will come into force in 14 months, in May 2018. In the UK, the new National Cyber Security Centre (NCSC) – operating since October 2016 – was inaugurated last month by Queen Elizabeth. The NCSC was created as an authority on cybersecurity, with a mission to improve cyber resilience.

Lebanon seems to be nowhere near similar levels of readiness found in the public sectors of the developed world. This is problematic for a number of reasons. There is no doubt that Lebanon has its share of state-level enemies which have a vested interest in creating any sort of impairment for the country's development or obtaining sensitive information from public administration units. In addition, 2016 made it clear that age-old hostile behaviors of states (reminiscent for example of the Cold War era) have gone digital, such as seeking to influence a country with propaganda or manipulating elections with fake news (see story page 38).

Government agencies in the Middle East had a very recent reminder about the danger of targeted

cyberattacks against them, attacks that were very damaging and possibly involved state sponsors. The Shamoon 2 virus made a repeat appearance in Saudi Arabia in January, after viruses from this family have hit the country twice in the past. Shamoon 2 targeted and disrupted at least 22 institutions, Al-Arabiya reported, including several ministries. Remarks made by government officials from several GCC countries at a cybersecurity conference held last month in Saudi Arabia said that there was an increase in attacks on their countries. Moreover, there are numerous initiatives in Gulf countries to embellish cyberdefenses and legal frameworks (see story page 44).

THE DEFENSIVE WALL

In a broader picture, the global landscape of cyberthreats and defenders (see infographic) has its villains that are growing more powerful and sophisticated from year to year. The malware arsenals of villainy are stocked with a wide variety of tools: viruses, their variants, such as worms which are self-contained malware and Trojans which disguise malware as innocent or useful programs, and further sub-variants from rootkits that give illicit administrator-level access to a computer or network to ransomware that blocks the legitimate owners' access to a computer.

Across from these cyberattackers and their arsenals stand the other stakeholders in the digital world. They use perimeter defenses such as firewalls, preventive approaches such as assumed-breach policy, early detection instruments such as threat monitoring, forensic tools and skilled defense centers such as SOCs and CERTs, and most of all try to fortify the entities most vulnerable to falling for cyberattacks – the human being in the digital world – through training and awareness building (see our guide story on how to secure emails on page 48).

All non-villainous stakeholders in the digital world are in one of two general categories: those that are primarily targets, like financial companies, utilities, the industrial sector, education institutions etc., and those that are defenders against cyberattacks, like specialized software companies and cybersecurity consultants. The borders between stakeholders that are targets and those that are defenders importantly are fluid: cybersecurity and defense is everybody's affair and some of the leading contributors to the protection of the digital world against evil attacks are the large software and systems multinationals, network operators, integrators, device manufacturers and all companies with large IT departments.

■ The state of Lebanese cybersecurity is much foggier when it comes to the private sector

**Build It
Green
Lebanon**

ANNUAL SUSTAINABILITY SOLUTIONS CONFERENCE

8

OUR CITIES, OUR HEALTH

22 MARCH 2017 | MONROE HOTEL, BEIRUT

Platinum Sponsor

Waterfront City
DBAYEH



Organized by

eecosolutions

in Partnership with

ECO
CONSULTING

Gold Sponsor

Tinol

Community Business
Partner

[executive]

Strategic Media
Partner

EKARUNA

Digital Partner

Beiruting
www.beiruting.com

Media Partner

WORLDENVIRONMENT.TV
we
MAGAZINE

REGISTER ON: WWW.BIGLEB.COM

Cybersecurity

CYBER THREAT & DEFENSE LANDSCAPE

1 THREAT ORIGINATORS

- State sponsors
- Terrorist organizations
- Cybercriminals (small states)
- Criminal hackers
- Criminals
- Hackers
- Insiders

2 CYBERATTACK ARSENAL

- Trojan Horses
- Botnets
- DDoS attacks
- Ransomware
- Malware
- Spyware
- Scareware
- Mobile threats
- Browser hijackers
- Viruses
- Worms
- Backdoors
- Keyloggers
- Rootkits
- Phishing
- Drive-by
- Spam



3 CYBERDEFENSE TOOLS

- Firewall
- Threat monitoring
- Encryption
- ✦ Malware detection
- ✦ Certificates
- ✦ Security plans
- ✦ Physical isolation
- ✦ Counterintelligence
- ✦ Threat audits
- ✦ Anti-virus software
- ✦ Regular software updates

4 DEDICATED DEFENDERS

- Network operators
- Cybersecurity consultants
- Cyber SOC's & CERTs
- ✦ ICI companies
- ✦ Software developers
- ✦ Mobile insurers
- ✦ Governments
- ✦ Insurers

5 TARGETS

- State organs
- Banks & financial companies
- IT companies
- ✦ US firms
- ✦ Education providers
- ✦ Hospitals
- ✦ Manufacturers
- ✦ Retailers
- ✦ Travel & tourism businesses
- ✦ Civil society organizations
- ✦ Events
- ✦ Individuals

By Thomas Schellen

Cybersecurity

Cyber(in)securities

Fresh thinking needed to protect the banking system

At the center of the cybersecurity issue in Lebanon resides, as with many issues in this country, an unfortunate and seemingly unmovable constellation. In one corner towers the banking sector as the primary force and primary concern for all things economic and also all things digital. The banking industry, as all the expert voices in conversations with EXECUTIVE about the cybersecurity issue acknowledged, is the biggest target for cyberattacks and the most advanced in awareness, preparedness and spending on cybersecurity in Lebanon.

Crouching in the opposite corner is the public sector. It is limited by severe lack of information technology (IT) spending budgets in general, and cyberdefense in specific. Many ministries are not equipped with a single cybersecurity specialist in their IT departments. In the perception of experts on Lebanon's cybersecurity, the public sector is in a worse state than the private sector and moreover gives the appearance of being engulfed in complete ignorance of advanced methods to maintain safety and simultaneously be on the cutting edge of internet usage.

Banks have undergone an evolution from a few years ago when they used to rely on having just one individual staff member with security responsibility who reported to the IT department. This was done to comply with a Banque du Liban (BDL), Lebanon's central bank, requirement that mandated banks to have this security representative. Overall, in the experience of Iskandar Aoun, head of the security department at Banque Libano-Française (BLF), "it was a marginal function".

According to him, this has changed in recent years as cybersecurity advanced from a marginal matter to the biggest threat for all banks and a major concern to their boards of directors. "This evolution occurred on different levels: the organizational level, the regulatory level, the media level

■ Many ministries are not equipped with a single cybersecurity specialist

and, of course, the technological level," he says. On the important organizational level it is common, at least in the sector's alpha group banks, that the security entity nowadays "is a complete entity with a minimum of five or six staff and reports directly to upper management," Aoun explains.

THE GAUSS MALWARE

Deputy General Manager Sleiman Maaraoui, head of Systems, Division Projects and Infrastructure at Société Générale de Banque au Liban (SGBL), tells EXECUTIVE, via an emailed response, that maintaining first-class cybersecurity capabilities requires a "relatively significant percentage of IT spending" and quantifies the share of cybersecurity measures at around 10 percent of the IT budget. "At SGBL, we have a dedicated team [within Information Technology Security Evaluation Criteria (ITSEC)] to monitor cyberactivity and track any suspicious behavior using cutting edge tools. Alongside, IT teams have dedicated resources to support and maintain this infrastructure," he says.

Maaraoui confirms that cybersecurity investments have gone up due to the necessity of implementing the latest tech tools and are expected to increase further. "This cost will increase over the coming years to meet targets set by top management and add new functionalities that will provide a seamless integration and an easier adoption by our customers," he says, citing as an example biometric tools such as fingerprints, voice identification and face recognition.

It seems that the crunch moment in banks' elevation of cybersecurity to the top in their list of priorities came after the 2012 discovery of the so-called Gauss malware, which had penetrated over 1,600 computers in Lebanon at several of the country's top banks according to global security company Kaspersky Lab's count. According to a Kaspersky Lab statement from August 2012, Gauss malware was a "nation-state sponsored cyberespionage toolkit designed to steal sensitive data," specifically targeting online banking credentials and browser passwords. The malware was said to have been active for more than nine months before it



Cybersecurity



was discovered on some 2,500 machines. According to Aoun at BLF, which was one of six major Lebanese banks which the statement mentioned by name. Several banks that were infected by the malware even refused to declare this fact.

HUMBLE HACKING PAST GIVES WAY TO RISK LADEN PRESENT

As Aoun tells EXECUTIVE, the risk associated with cybersecurity breaches some 10 years ago was “relatively low” and this low risk was reflected in “humble topologies,” meaning simple physical or logical layouts of the computer networks at every bank. Hacking attacks were slow, often involving days of hackers poking around to find system vulnerabilities, and damage was of the kind that even successful breaches were hardly mentioned, i.e. any damage was below the cost of reputation loss if the breach was disclosed.

“Until now, we did not have a major breach in the area, especially in banks. We have the small [incidents] of fraud where an email sent by a customer asked to transfer money somewhere, and then the bank discovered that it was fake and the request was for a transfer to an unknown account. We did not have major breaches, touch wood,” he says.

In the 2017 environment, however, hacking tools are far more advanced. “All the hacker has to do is

send a nice-looking email that contains an attachment or malicious URL link, and all that the end user needs to [do] is double click on the attachment or the URL with the result that malware is installed on the system, and the hacking job is done. The whole environment is infected,” he says, adding that the great increase in risk is reflected in banks having deployed advanced topologies to deal with this risk.

The adjustment to greater cyber risks on the technological level was mirrored in regulatory developments. According to Aoun, every bank has been obliged by the central bank to declare any incident that occurs on its premises, and the central bank evaluates all this information and incorporates it in updates of circulars related to security. He says, “Whether it is physical, a downtime of the system, a cyberattack, data theft, fraud, operational risk or anything [else], you are obliged to declare it to the central bank. We have to declare, and we also have to have a policy to inform our customers about an attack. I can also say that it is better for the bank to inform its customers rather than them finding it out over the internet or through media reports.”

According to SGBL’s Maaraoui, the rising importance of cyber risk has led to its embedding in the bank’s thinking, in addition to all other requirements that occupied the attention of banks, such as anti-money laundering regulations and recent rules on

financial standards. “Cybercrime is no less important than compliance pressures or local and international regulatory tightening. This importance has been growing year after year thanks to digitalization,” he says.

In Maaraoui’s words, cybersecurity may not be on the agenda of every board meeting at the bank, but he confirms, “board members are fully aware of threats and challenges faced with cybersecurity.” Moreover, he implies that amidst a whole array of measures to enhance customer protection in contemporary banking, the issue of protection against theft of their banking data and other forms of cybercrime is possibly the most sensitive one. “If sensitive information is stolen or otherwise misused, the public will not see that the financial institution is a victim of a malicious actor, only that it did not properly protect that which was entrusted to it. Regulations enforce severe penalties for non-compliance, while the organization’s public image can be irreparably damaged,” he says.

BANKING ROADS TO BETTER SECURITY

By the perception of perhaps the most potent company that Lebanese can turn to as a global powerhouse and authority in IT and cyberdefense, Microsoft, Lebanese banks have taken the national lead in cybersecurity measures, but often did so in ways that do not allow them to be on the forefront of digital innovation, warns Microsoft Country Manager for Lebanon Hoda Younan.

“Organizations in Lebanon, even in industries that we believe are advanced, like financial services, are very conservative and do not build on innovation because of fear [of being connected]. They sometimes cut off their people from the internet to protect themselves. We saw this as a reaction to the attack that three or four years ago that reached all banks. If you disconnect, this will definitely protect [you in one way], but it prevents you from innovating. Speaking from the perspective of a Lebanese person who feels responsible, I see that we have a lot to do. We need to build on the experience that the multinationals are giving us when they come into the country, so that we can be more aware and more protective,” Younan says.

According to Microsoft experts, local organizations face challenges that relate to a mindset of plac-

ing trust in static concepts of perimeter defense. In choosing a physical gap approach for their cybersecurity, they tend to bet their fortunes, and their lives, on erecting huge walls – in a way that resembles the approach of medieval castellans who build ramparts that were seemingly impenetrable. That approach worked only until trebuchets were invented (as the Microsoft-published game Age of Empires 2 already taught its addicts some 18 years ago).

For Nasser Kettani, Microsoft’s chief technology officer in the Middle East and Africa, to have online banking today is not enough for a bank to be innovative. For them to be able to innovate, he advises banks to develop a mindset for cybersecurity that is adapted to the current time, meaning to focus not on perimeter defense of their networks, but on technology and intelligence that can be obtained from the cloud. Moreover, perimeter defenses can be ineffective against internal hacks, he adds, citing the example of the National Security Agency (NSA) in the United States.

“The ability of banks to innovate in terms of Artificial Intelligence, Internet of Things, blockchain and a lot of things that you can do [is limited] because they have not changed their security posture. What we are finding is that you can expose yourself to the internet and be safe, but you have to change your way of doing things,” Kettani tells EXECUTIVE. This requires a new security posture, he says, citing gains in security that companies and entire countries can achieve through collaboration.

In the case of Microsoft, the company – which at all times in digital history was a target of hackers – is now more than ever subject to cyberattacks since it moved a few years ago to become a major provider of services on the cloud. It responded to the threat with huge investments in cybersecurity – in 2016 it spent over \$1 billion purely on cybersecurity according to Kettani – and also leveraged the data insights it obtained from operating about 200 cloud-based services with 100 billion user logins per month.

“Data collection gives you more insights than you can get otherwise. This volume of data that we see from around the world helps us to get intelligence that nobody else can,” he says. Microsoft uses these insights for building new security tools to protect itself and its customers through different units inside the Microsoft organization and also partners with other IT companies and law enforcement operatives in many countries – for example through national Computer Emergency Response Teams, or CERTs – to extend the umbrella for protection against cybercrime.

Under the common perception of most crime choosing the road of least resistance, the best defense

■ Organizations in Lebanon, even in industries that we believe are advanced, are very conservative and do not build on innovation because of fear [of being connected]

Cybersecurity

will be one that elevates the criminals' risk of detection and punishment when caught. Implementing such a strategy in Lebanon, however, transcends the capabilities of banks and other private sector entities. It necessitates legal measures and organized cybersecurity collaboration of private sector players with the state and with one another.

CALLS FOR MORE GOVERNMENT ACTIONS

This important need for interaction is reflected in the views of the cybersecurity specialists at BFL and SGBL. Of the important measures that the government should undertake in Aoun's perspective, one prudent initiative would be to give companies tax incentives on investments into cybersecurity systems to make it as affordable as possible and help smaller players beef up their defenses. According to Aoun, "the government should not impose any tax [on cybersecurity systems]. This will reduce the equipment cost and encourage the banks to invest in security products." In parallel to incentivizing cybersecurity investments, he advocates secondly, that the government should enforce cyber insurance as mandatory for banks, and thirdly that it should develop national cybersecurity infrastructure. Specifically, Aoun advocates for the creation of a CERT for Lebanon.

"A CERT will issue guidelines, monitor risks and inform banks of attacks. This has become an urgent matter for Lebanon," Aoun reasons, adding that having a national team will also provide faster information on attacks that happen elsewhere because CERTs communicate with one another across countries. "If there is a threat in one country, they will communicate the information to all countries and every local CERT will communicate with the companies in its jurisdiction to take precautions – this needs government action to legislate. A CERT team will also minimize the phenomenon by which everybody refuses to say what is going on," he says.

Regarding collaboration among cybersecurity officers of Lebanese banks, Aoun maintains that this issue was raised by BLF in the drafting of a let-

■ A CERT will issue guidelines, monitor risks and inform banks of attacks. This has become an urgent matter for Lebanon.



ter to the Association of Banks in Lebanon and was also mentioned in discussions with the Banking Control Commission. The call is for regular meetings or a convention of CIOs (chief information officer) so that these professionals may share their experiences and exchange information with one another, meaning that all stakeholders are provided with immediate information on new risks and incidents.

Also in Maaraoui's view, there is urgent need for government action on comprehensive legislation. He says, "The Lebanese government is urged to pass a new law that facilitates online transactions, yet ensures its security and authenticity by enabling [the] digital signature and extending it to full digital identity."

He also recommends that laws to fight cybercriminals should be put in place and that legislative actions in those two regards should be coupled with other laws and central bank circulars to guide banks forward toward "true secure omni-channel experience. The guidance of banks toward ever-increasing cybersecurity should furthermore be accompanied by actions of the Banking Control Commission of Lebanon (BCCL)," Maaraoui opines.

"BCCL should mandate an external, internal and overall 'security assessment' to be performed by third-party companies with expertise and certification in cybersecurity, [similar to that of a financial auditor], the results of which are then sent to the bank, but also directly to BCCL," he argues, citing a similar practice in Luxembourg as an example before adding that not only banks, but the entire enterprise-level environment in Lebanon needs directing toward measures that will prevent or at least minimize "potential financial, but more importantly reputational damage."

SCENARIOS FACED BY INSURERS

While banks face the dual need to embellish their security – at the same time constantly enhance and evolve their online accessibility and digital services in order to respond to changing customer expectations – and also remain competitive in the face of disruptive fintech startup companies, insurers need to approach digitization and cybersecurity under a somewhat different paradigm. On one hand, they are, just as banks are, financial companies, and thus, attractive targets for cybercrime-syndicates and individual hackers. They therefore must adapt to the digital world in their distribution strategies. On the other hand, they have the mandate to harness cybercrime as an opportunity for providing new insurance services. Moreover, their function extends to demanding that insured parties comply with preconditions for insurability, whether in the form of fire doors in a building or firewalls in a data center.

In the multi-faceted context of being stakeholders in their own cybersecurity and insuring risks of others, Lebanese insurers could find a new boom in cyber insurance premiums, says Max Zaccar, chairman of Commercial Insurance and president of the Lebanese Insurance Association. “In future, cybersecurity could be a huge portion of overall business for insurance, with estimates going as high as 50 percent of premiums to be generated by cybersecurity,” he declares.

Zaccar concedes that there is yet limited understanding of insurance for cyber risks in Middle East. He points, however, to a factor that should make cyber insurance a welcome addition to the product offerings of local insurers. “Most of the cyber insurance risk, if underwritten by local companies, will be reinsured abroad, so companies will not face too much risk of having to pay out of their own pocket,” he explains.

Lebanese insurance companies have some demand from banks for cyber insurance policies, says Fateh Bekdache, general manager of BLOM-Bank affiliated Arope Insurance. “Cybercrime is a delicate subject that is becoming very important. A lot of insurers were reluctant to consider cyber coverage because it is very complicated,” Bekdache tells EXECUTIVE.

He adds that it is a complex and challenging task to draft standard cyber insurance policies, which will stipulate the coverage terms of such contracts. This is a development in the domain of international reinsurance giants that local insurers observe from the sidelines. “There is a race among reinsurers as to who will draft a contract that is more advanced

than that of the other. We are sitting and watching,” Bekdache says.

Another challenging issue is the fact that many companies are reluctant to declare if they have experienced a breach or quantify losses from intrusions, which makes claims management even more delicate. As Zaccar and Bekdache concur, the reported growth of breaches in Lebanon is high, but it is only the tip of the iceberg and statistics suggest that local organizations, just as companies everywhere, in their vast majority do not report their breaches.

Numerous recent reports by international consultants, banks and insurance players have highlighted cybersecurity as a growing area of business and insurance. Bank of America Merrill Lynch was quoted as estimating the cybersecurity business to represent on average 6 percent of IT expenditures, which was worth \$75-77 billion in 2015 and projected to reach \$170 billion by 2020. A 2015 report by PricewaterhouseCoopers sees cyber insurance as a “potentially huge but untapped opportunity for insurers and reinsurers,” estimating worldwide annual gross written premiums as set to grow from \$2.5 billion in 2014 to \$7.5 billion at the end of the decade.

Lloyds of London said in a 2016 report that over 90 percent of large European businesses surveyed had experienced a data breach, and 51 percent were worried about being hacked by cybercriminals for financial gain. However, only about 50 percent were aware that cyber insurance coverage for a data breach is available and many were equally unaware that cyber insurance not only provides a pay-out after a cyberattack, but also helps with expert consultancy during a crisis.

Moreover, most of the market, up to 90 percent, is currently in selling cyber insurance to companies in the United States. Given that cyber risk is a globally universal growth phenomenon, the estimates for future cyber insurance needs seemingly cannot be overstated.

To take the discussion of cyber insurance in Arab countries forward, the Lebanese Insurance Association and the General Arab Insurance Federation are collaborating to convene a digitization conference this May in Beirut. According to Zaccar, the first day of the two-day event will be dedicated to new digital distribution channels and the related issue of digitizing insurance services, while the second day will be dedicated to cyber insurance and the Lebanese law enforcement perspective on cybercrime.



Securing the entrepreneurship ecosystem



Protecting startups from the get-go

It's 3 a.m. Despite your family's "no Internet after dinner" rule, your smart, web-connected refrigerator is rebelling, repeatedly attempting to load the same site. The mustard is not trying to catch up on the news, your ice box has become a zombie in a hacker's army – a botnet, in industry lingo. While the so-called "Internet of Things" allows for the connectivity of an increasing number of previously "dumb" devices and appliances, their link to the global internet presents a vulnerability hackers have already begun exploiting.

With the exponential growth of online risk, of course, comes both an opportunity for consultants and companies specialized in providing cyberdefense, and the need for companies large and small to increase security spending. In the last six years, venture capitalists have grown more keen to cash in on the flourishing cybersecurity market. Startups focused on data protection attracted \$3.48 billion in investments in 2016, down slightly from \$3.9 billion in 2015, but 76 percent above the \$833 million poured into young data defenders in 2010, according to research company CB Insights. The company also reports that in 2015, four cybersecurity startups attained so-called "unicorn" status (meaning their value was in excess of \$1 billion), with one more of the mythical beasts joining the stable in 2016. Tech news websites feature lists with

the 20 hottest cybersecurity startups to watch. A quick view of such lists reveals that career moves by specialists in this field from protecting the state to the private sector is a potentially lucrative choice – a number of newer ventures boast former Israeli or US digital warriors at the helm or among the top brass.

While niche specializations are beginning to develop in the Lebanese entrepreneurship ecosystem, such as fintech, cybersecurity is not one of them.

A SHORT LIST

Since Lebanon's entrepreneurship ecosystem first began buzzing around 2001, it has produced a few cybersecurity companies – consultancy seems more popular than solutions-provision, although exact numbers are difficult to come by – but according to EXECUTIVE's research, since 2013 there have only been two start-ups with incorporated cybersecurity focus. The first, Myki, has been profiled in the magazine before but was not available for an interview. The password-management company is now listed as a portfolio company on the site of local VC Leap Ventures, and – according to an unsourced announcement on Crunchbase.com – raised \$1.2 million in a third funding round at the end of January. Myki founder Priscilla Elora Sharuk told EXECUTIVE in March 2016 that the company had raised \$600,000 up to that point.

Early last year, Universant Technology Corporation became the newest local entrant to the cybersecurity market, founder Joe Hage tells EXECUTIVE. Hage has a background as both a successful entrepreneur and a security specialist. He explains that his rapidly growing company – which has doubled its workforce in the last 12 months – was born primarily to leverage Hage's network of contacts. Along with an angel investor providing the company with an initial capital boost, Hage had "seed clients," i.e., "contracts in hand pending incorporation." He has bold ambitions hoping to identify and nurture local talent

to win big-ticket contracts in the Gulf, and has secured one so far. To this end, Hage says Univer-sant partnered with the American University of Science and Technology (AUST) and has created an informal group of security researchers, which he describes as “almost an R&D staff.” He lists acquisition as an exit strategy but talks with a passion that suggests he may shed a few tears if ever asked to hand his baby off to new parents.

AWARE OF THE RISKS

While Lebanon’s ecosystem is not pumping out cybersecurity startups, data protection is on everyone’s mind. Jana El Husseini, project co-ordinator at Smart ESA, says the new incubator and accelerator run by the Ecole Supérieure des Affaires – a local business university established in 1996 – will teach the startups it hosts security basics. Ramy Boujawdeh, deputy general manager of Berytech, explains that security is taught as a module in the education program that the Berytech incubator provides to all startups there.

Fares Samara, the chief technology officer at the accelerator Speed@BDD, teaches young companies security basics, but notes that as Speed works with idea-stage companies that have yet to develop minimum-viable products, few students under their tutelage have advanced security needs. He points to the growth of what he called “infrastructure as a service,” an evolution of software as a service made possible by cloud platforms from companies like Microsoft, Amazon and Google, he half-jokes that IT staff in early-stage companies don’t even need to understand how to setup a secure server (as the Microsofts, Amazons and Googles are doing that for them nowadays). As startups grow, managing the increasing amounts of data they collect becomes more complex, requiring either customization of back-end infrastructure offered by third-party providers or the design of an in-house back-end, which is where most vulnerabilities can surface, Samara explains. Once a startup begins to expand, its internal security needs grow, he says.

■ It is easier and cheaper to build securely from the beginning

SECURITY BY DESIGN

Online advice for startups thinking of their own security frequently note that it is easier and cheaper to build securely from the beginning (even if this includes upfront costs like penetra-

tion testing and causes some delay in bringing a new product to market) than trying to patch vulnerabilities after intruders have gotten in. It was with this advice in mind that the local carpooling app, Carpolo, opted to build its own back-end early on instead of relying on a third-party, company co-founder Ralph Kheirallah tells EXECUTIVE. Kheirallah echoes Samara in noting this infrastructure will add the most value to the company as it grows, but argues it was worthwhile to invest from day one. Carpolo is using a business-to-business model – pitching itself to employers, a shift from the initial B2C model – and currently finding interest among local banks, clients with very strict security requirements.

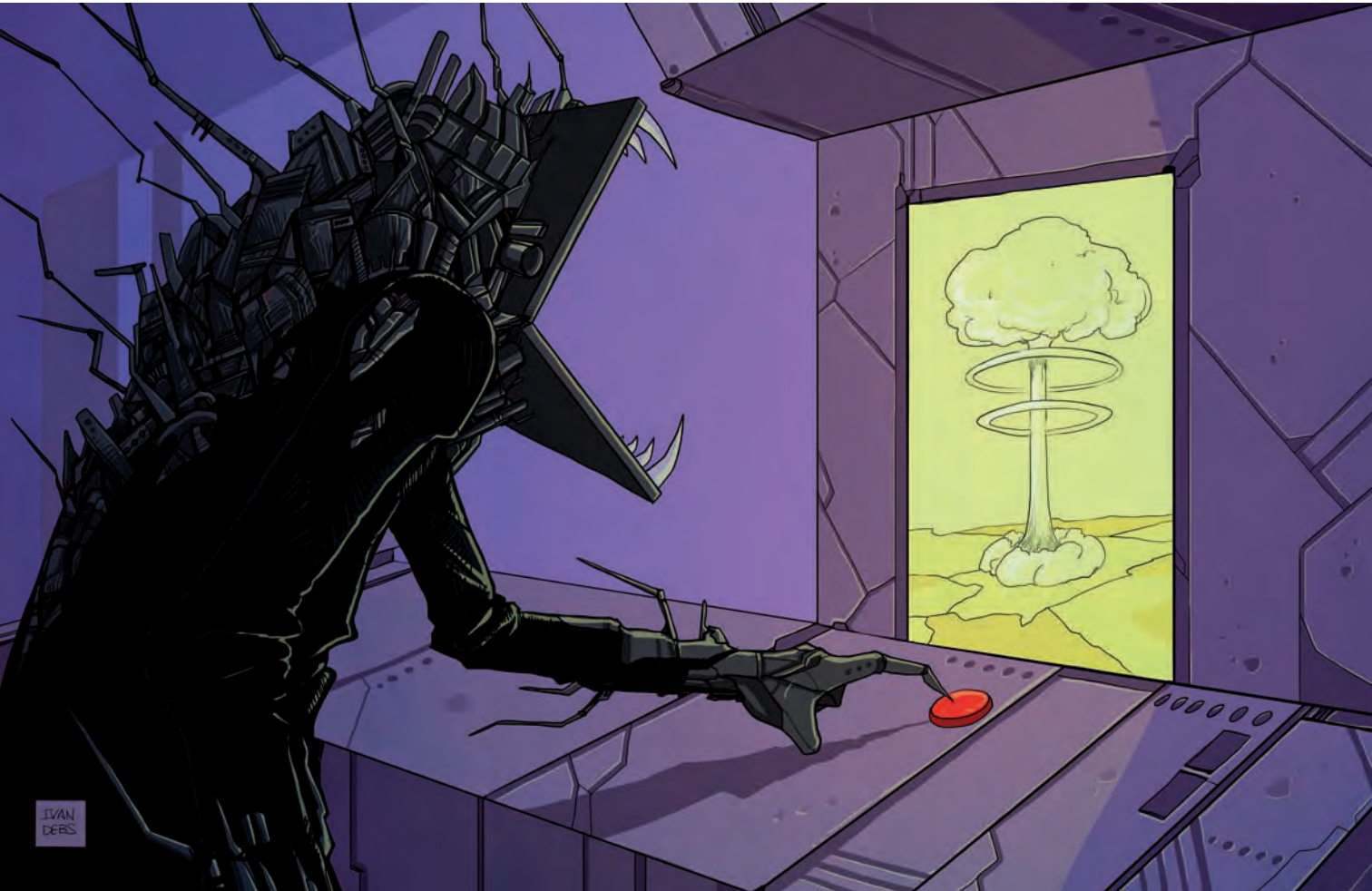
Locally and globally, banks are high-priority targets for cybercriminals (see overview page 16) and security is a top concern for startups looking to enter the financial sector. Saeb Nahas – a manager at Phoenician Funds, a local VC with a fintech, e-government and health care focus – explains that portfolio fintech companies go through extra screening to ensure their systems are secure. “We have experts who go in and do fake attacks” to “pinpoint problems” early on for portfolio companies, Nahas says. Additionally, security evaluations are part of Phoenician Funds’ due diligence when evaluating an opportunity, he notes.

NEVER TOO SMALL

With the increased sophistication of cybercriminals, and the ease with which they can attack, small companies today have to be far more aware of threats – and better prepared for attempted intrusions – than they did even five years ago. Mario Gaudet, chief technical officer for Economena Analytics, talks of a war being fought by the minute. The company is a platform for economic data for the Middle East and North Africa region. Gaudet says his network analytics reveal attempted attacks almost 24-hours per day, with “at least” 20 attempts per hour. Hacking, he says, “has become a business.” Defending against increasingly savvy criminals, therefore, is a need that will only grow for companies of all sizes.

By all accounts, Lebanon’s entrepreneurship ecosystem understands the security threat, but as safe and secure as a system can be, everyone interviewed for this article reiterated some version of a joke security professionals are rumored to frequently make, “there’s no patch for human stupidity.” Whether it is reusing weak passwords for every account or sending sensitive data over an unsecure WiFi connection, people remain the weakest link in the cybersecurity chain. ■

The Lebanese cybersecurity landscape



Providers and markets

Overall, it is not clear what the local share of the global cybersecurity market – estimated by Gardner at \$81 billion in 2016 – is or might be. Estimates and anecdotal evidence suggest, however, that the local market is still small. Salah Rustum, president of local firm Commercial & Industrial Enterprises of Lebanon (CIEL) and a veteran in the data protection business here as partner with electronic signatures authentication services company GlobalSign, estimates the market at currently “around \$10 million” when queried by EXECUTIVE. Other decision makers in Lebanese cybersecurity consultancies and net-

work operating companies say they prefer not to make any estimate about the current size of the cybersecurity market, citing the known dearth of reliable statistics in the country.

Beirut-based cybersecurity stakeholders also have only vague estimates on the number of qualified competitors that they face in the Lebanese market or on the number of highly skilled analysts with the required expertise to staff a Security Operations Center (SOC) – not currently existing in the country – as top-level forensic experts. General agreement, however, among stakeholders is that this specialist subsector of the information

technology (IT) industry is set for substantive growth – at least double-digit year-on-year – over the coming years and that the biggest challenge is not to find new customers but to obtain qualified engineers that either already have or can obtain cybersecurity skills.

One example for this dichotomy between expected demand growth and missing manpower is Crystal Networks, a Beirut-based regional IT company of 75 employees, which according to co-founder and general manager Esper Choueiri does 40 to 45 percent of its business domestically and the remainder in the Arab region, with Saudi Arabia as the main business driver there.

Choueiri tells EXECUTIVE that his company filled five new engineer positions in 2017 that were all in the security department of the venture, which has five departments. “In many cases, experienced engineers cannot be found and new engineers need to be trained in-house for cybersecurity. My biggest challenge is finding the right people, and at the same for all my customers,” he says.

LACK OF LOCAL EXPERTISE

To operate a high-grade Security Operations Center, or SOC, requires teams of engineers with three levels of expertise. Engineers need between a minimum of one year of experience to perform well on the first level and at least five years on the top level, Choueiri says. By his estimate only one fifth of needs for top-level SOC experts are currently filled in Lebanon.

Also in the view of Jens Muecke, senior partner in the roughly four-year old IT security consultancy Krypton Securities in Beirut, a shortage of local experts is holding back cybersecurity development in Lebanon. “From my opinion and what we have seen in our team, many banks and companies over here are way behind. One reason is missing expertise – it is really hard to find good people here, given the instability of [this country] and the whole region. Everyone who is acquiring the skill [of a cybersecurity expert] and a reputation for having such, is getting out of here to take

■ In many cases, experienced engineers cannot be found and new engineers need to be trained in-house for cybersecurity

up a well-paid job in Europe or the US,” he says.

German-born Muecke joined Krypton after having worked with leading consultancies and international internet and software providers in the United States. The company, which has a team of seven employees in Beirut and its nominal home in Dubai, according to him has half the major banks in Lebanon among its clients, as well as some smaller companies. Krypton does about 80 percent of its business here as its expansion in other markets such as Jordan, Cyprus, and Saudi Arabia is still in the early days. It will take a few more shocks for markets in this region to fully awaken to cybersecurity. “What I think is that this region needs a few more bad examples when things happen tragically and somebody has to pay the price before they all realize what they need,” he says.

Judging from his observations, local companies to this day tend to approach cybersecurity with the same mindset with which in earlier years they entered in other quality certification procedures. With such a mindset, companies emphasize assurance of their compliance with regulations. After they are promised cybersecurity on the cheap, they become compliant on paper but don’t achieve the knowledge transfer that they should get, Muecke says: “They have a paper saying ‘it is compliant’ but it is not. They don’t have the process and don’t do updates regularly. They don’t evaluate all reports as they should. They live day to day and hope nothing is going to happen.”

The notion that risks extend far beyond the financial sector in also the view of Tony Feghali, general manager of Potech Consulting, based at Berytech. His security company does not have exact numbers and statistics on the extent of internet-related damages at Lebanese companies but he says that in their experience, banks are not the only targets here. “They are definitely a very interesting target because that’s where the money resides, but today we’re seeing a lot of cyberattacks – especially ransomware or other type of attacks – targeting every type of business,” he says.

HUGE GROWTH POTENTIAL

The growing likelihood of being targeted does not mean that local companies radiate universal awareness of their risks. According to Choueiri, awareness levels are extremely unequal. “To be realistic the banking sector is most advanced when it comes to cybersecurity and most aware among

Cybersecurity

the Lebanese enterprise sector. Any company that is not IT-related is in my personal opinion totally unaware of security risks," he says. Along with other experts he notes that besides missing awareness, it is often difficult to assess the real number and magnitude of cyber breaches and security damages in Lebanon because of widespread reluctance of breached companies to come forward and disclose their misfortune, mostly due to fear of reputation loss.

This phenomenon, however, is global and not particular to this country or region, experts agree. The phenomenon also does not deter cybersecurity companies from expecting double-digit business growth, or better, for the next few years.

Choueiri expects demand to increase between 35 and 40 percent year-on-year and has important expectations for 2017. "I have [a] feeling that this year will be the year of cybersecurity. Everybody is talking about it," he says.

CIEL's Rustum sees year-on-year growth as upwards of 10 percent and even believes that more is in the cards. "[Growth] will be exponential in Lebanon, because the more people know about it, the more they are going to use cybersecurity," he says. He moreover is not worried that there could be too much competition for the market to carry but on the contrary believes that there is room for more cybersecurity players. "There is enough cheese for everybody. The idea is to stir up the people and tell them that if they want to go on the internet, they have to protect themselves," he elaborates.

Rustum's main worry is bringing the legal framework in Lebanon up to speed. When his

15 TOP CYBER SECURITY COMPANIES BY END FEB IN MARKET CAP

From a market cap perspective, headline evidence confirms cybersecurity as a growth segment. A fact sheet by US based venture capital multi-national Bessemer Venture Partners lists 17 sector companies which each have of \$1 billion or equivalent in market capitalization. The list grew by seven names since it was first released in the first half of 2016. By Bessemer's tally, the average cybersecurity focused Behemoth is a Silicon Valley-based software company that is listed on the NASDAQ. Tracking the companies on the list by their Feb 27, 2017 market cap, Executive got the following snapshot of the largest players:*

Name	Base	Exchange	Market Cap
Symantec	Silicon Valley	Nasdaq	\$18 billion
Checkpoint	Tel Aviv, Israel	Nasdaq	\$17.3 billion
Palo Alto Networks	Silicon Valley	NYSE	\$14 billion
Verisign	Preston, USA	Nasdaq	\$8.5 billion
Splunk	San Francisco, USA	Nasdaq	\$8.5 billion
Fortinet	Silicon Valley	Nasdaq	\$6.4 billion
Trend Micro	Shibuya, Tokyo, Japan	Tokyo Stock Exchange	690 billion yen (\$6.1B)
Gemalto	Amsterdam, NL	Euronext Amsterdam	5 billion euros (\$5.3B)
Proofpoint	Silicon Valley	Nasdaq	\$3.3 billion
FireEye	Silicon Valley	Nasdaq	\$1.9 billion
Cyber Ark	Israel	Nasdaq	\$1.7 billion
Sophos	London, UK	LSE	1.3 billion GBP (\$1.6B)
Imperva	Silicon Valley	Nasdaq	\$1.4 billion
Qualys	Silicon Valley	Nasdaq	\$1.3 billion
Barracuda Networks	Silicon Valley	Nasdaq	\$1.3 billion
*AVG Technologies	Amsterdam, NL		\$1.25 billion

*Two of the 17 companies were acquired in and no market cap information update is available.

US-based Lifelock was acquired by Symantec and Dutch AVG Technologies was acquired by Czech firm AVAST.

Source: Bessemer Venture Partners, Bloomberg, Reuters, Stock Exchanges, Executive calculations

■ What I think is that this region needs a few more bad examples when things happen tragically and somebody has to pay the price



JOIN THE LARGEST CORPORATE EVENT IN THE MIDDLE EAST
45 GAMES OF SPORTS, CULTURE, FUN & SKILLS IN 2 DAYS

Mini - Football | Basketball | Athletics | Tug of War | Ping Pong | Swimming | Badminton
Bag Race | 3 Legged Race | Wall Climbing | Tennis | The Fitness Course | Archery | FIFA 17
Dodge Ball | Arm Wrestling | Baby Foot | Quiz | Sports Quiz | Driving Quiz | Travel Quiz
IQ Test | Sudoku | Song Quiz | Squash | Bicycle Challenge | Backgammon | Chess
Grass Volley | Best Company Slogan | Best Cheering Company...

| www.beirutcorporategames.com |     **| ☎ 05.956614 | ✉ INFO@SPORTEVASIONME.COM |**

SPORTEVASION



Cybersecurity

business working with digital signatures was established in the 1990s, the country was praised as one of the first in the world where the technology was introduced, but thereafter it slipped every year down in rankings for technology adaptation as the draft law on digital signatures was put to rest in government drawers. "Time is really passing us by. What I am afraid of is that by the time Parliament approves the law, it is already obsolete," he laments.

As EXECUTIVE did not find any comprehensive study on security market data in the country, it seems difficult to assess realistically, with or without legislative innovation, what chance local companies might have for rising through international ranks, whether by expertise or by business volume related to cybersecurity. However, there can be no doubt about the growing role of cybersecurity companies in global markets, which is documented by the rise and overall growing valuations of international specialist companies. The largest firms globally in the sector are based in Silicon Valley but a few are not far from our geography in physical terms (see box).

WORK OPERATORS SEE THREAT

Local companies that are active stakeholders in the market involve not only security consultancies but also network operators. A rising hub of cybersecurity activity seems to reside in the Holcom Group of companies where EXECUTIVE encountered not only Crystal Networks but also ICT company and network operator GlobalCom, which confesses to the aim of developing its own cyber SOC in partnership with global player, British Telecom (BT).

"We first have a duty to protect our networks and then we have a duty to help our customers protect themselves," says Habib Torbey, GlobalCom Holding's chief executive officer and general manager of its data carrier unit GlobalCom Data Services (GDS). Torbey tells EXECUTIVE that the investment into the cyber SOC will be in the multi-million dollars. Although Lebanon by his observation so far

■ We don't need to wait for a disaster before we start protecting ourselves. No one in this field can fight the battle alone

has mainly seen attacks from small-time hackers, he reasons that the investment into a cyber SOC is warranted because attacks are getting more and more sophisticated, affecting more and more markets.

"We don't need to wait for a disaster before we start protecting ourselves. No one in this field can fight the battle alone, and in the same way that pirates are cooperating to make their attacks more sophisticated and more successful, the good guys need to cooperate," he reasons, explaining that GlobalCom partnered in this task with BT because there is a long-standing collaboration between the companies since the 1990s and because BT "is one of the best in cyberdefense."

According to Torbey, GlobalCom has a network that comprises backbones and over 150 sites; it carries 70 percent of corporate traffic in Lebanon through GDS. The holding also entails the Internet Services Providers IDM and Cyberia. According to BT representatives who came to Beirut for an event last month, Lebanon is regarded as one of several priority countries in Middle Eastern new markets. The multinational company has started to address the local cybersecurity market in 2016 in partnership with GlobalCom and wants to serve the country's 20 to 30 largest entities with cybersecurity services.

OUTSOURCING SECURITY

Outsourcing cybersecurity to specialist companies would be legally feasible for local banks, although compliance with banking secrecy laws requires that they would use a cyber SOC that is located in Lebanon, asserts Torbey. "Some customers who do not understand how cybersecurity works may have a tendency to think that we can see the content of their traffic and their trade secrets. No, we don't look at the content and we don't want to look at the content. We just want to look at the technical specs of the traffic in order to see if there is an attack or not and how to defend against it if there is an attack," he explains.

While operation of a cyber SOC will require running investments, Torbey says this is a necessary cost and expresses the hope to additionally turn it into revenue opportunity by selling its services. Coming from a low base in cybersecurity revenues, he expects double-digit growth of revenues and is not afraid that cyberattacks would create digital disasters for operators who know what they are up against in facing cybercrime. He says, "Once you become aware of the risk and help your customer become aware of the risk, the future is not scary. You can do something about it." ■

Just Another Day of Being *Inspiring*



Happy
Mother's Day

PRESENT THIS COUPON AT ANY VIRGIN MEGASTORE BRANCH BENEFIT FROM

10% DISCOUNT

ON YOUR MOTHER'S DAY GIFT

- TERMS & CONDITIONS APPLY -



Propaganda goes viral

Communication continues to morph in the digital age

"I don't believe what I read in the papers, they're just out to capture my dime."

Paul Simon, Have a good time

While propaganda is as old as time and political stakeholders have used the internet to spread their messages since the web's early days, in 2016 propaganda went viral. It was also monetized in an arguably new way, further highlighting the need for readers to check their sources – and the motivations behind those sources – before making decisions.


Fake news isn't new, but it was a lucrative business during last year's US Presidential election. EXECUTIVE hasn't found an exact figure for how much revenue the operators of fake news websites earned, but one US "publisher" claimed in an November 2016 interview with the Washington Post that, "right now I make like \$10,000 a month from [Google] AdSense." No shortage of US news outlets traveled to Macedonia late last year to interview teenagers who claimed to be pulling in \$1,000 or more per month operating "news" websites consisting of mostly plagiarized content with the occasional "viral" report (typically a story either made up entirely or given a wild and misleading headline) that drove up hits and ad revenues.

While Facebook and Google have both pledged to crack down on fake news by attempting to keep it off the platform and starving sites hosting it of revenues, respectively, it certainly won't go away. Efforts by these powerful gatekeepers may kill the business model that seemed to do so well last year, but they certainly can't eliminate "clickbait" and poor journalistic practice all together. Sensationalism and outright falsehood have always been the "dark side" of journalism, seductive because it sells, but ultimately corrosive (hurting the credibility of both publishers and the wider industry, and providing a disservice to readers). Stopping the profiteers masquerading as publishers pushing fake news in recent years may make fake news less voluminous, but won't eliminate the phenomenon entirely.

DIRTY TRICKS

In the past two years, Western countries have been decrying what they insist are Russian online propaganda efforts aimed at discrediting liberal democracy, but misinformation has been used as a state tool for manipulating public opinion for centuries. It is neither recent nor surprising that governments have turned to the web to promote their interests. While the West today is accusing Russia of outright lies in its propaganda efforts, governments and politicians "spin" news all the time in an effort to "manage" public perceptions of an event or issue both on and offline. The US created an Arabic-language satellite news network – *Al Hurra* – to win hearts and minds following its 2003 invasion of Iraq. Avoiding the moral debate about the differences between "spin" and outright falsehood, one shared consequence of both activities is the need for readers to be discerning when consuming information, which is also not new.

An under-reported aspect of two of 2016's most surprising election results is just how much more aware readers need to be of not only what they read, but the personal information they willingly share that will increasingly influence what they read. According to both UK-based daily *The Guardian* and the Swiss news website *Das Magazin*, a company called Cambridge Analytica used big data to craft micro-targeted messages for Donald Trump and a group called *Leave.EU*, which promoted Britain's exit from the European Union. Cambridge denies any use of fake news, but, the *Guardian* reports, the company proudly claims to have "psychological profiles based on 5,000 separate pieces of data on 220 million American voters." Our digital footprints tell a lot about us, and how we may react to certain well-crafted messages, meaning seemingly innocuous ads on the side of whatever website you're reading could actually be designed specifically to elicit a certain reaction from you individually (whether that's voting a certain way or buying a certain product).

Despite all the huffing and puffing about information manipulation online in the past few months, the internet hasn't reinvented the wheel. The web has made information more easy to publish, disseminate and access, and Big Data gives propaganda a frightening, Big Brother feel, but the web hasn't changed the fundamental fact that readers simply must be discerning in order to avoid being duped. 



Cybersecurity

The public sector's vulnerability to a cyberattack



A Q&A with OMSAR's IT security expert, Ihab Chaaban

In Lebanon, the speed at which the government is moving and the speed at which cyberthreats are developing are totally different. Cyberdefense planning, it appears, is not much of a priority for the Lebanese government. The country does not have legislation to protect digital rights, lacks legal penalties to deter criminal cyberattacks and has only patchwork solutions in place for cyberdefense. In simple terms, plans to beef up the government's cybersecurity capabilities are moving forward at a snail's pace.

Cybersecurity firms point to an uptick in attacks on Lebanon when compared to global averages. Due to the state's slow moving apparatuses and the high cost of investment, the best cyberdefense solution for Lebanon to protect its public sector, its private sector and online individuals, may be to migrate to the cloud - a debate which is still ongoing. EXECUTIVE met with Ihab Chaaban, Information and Communication Technologies (ICT) security officer at the Office of the Minister of State for Administrative Reform (OMSAR), to learn more about Lebanon's cyberdefense capabilities.

E OMSAR's first foray into cybersecurity was in hosting government websites in the mid-2000s. How has OMSAR's role in cyberdefense since evolved?

Historically, OMSAR began in its hosting environment with informs.gov.lb, [today is dawlati.gov.lb, the official e-governmental portal] and over

the years other websites were added. Suddenly, we found ourselves stuck in an unusual situation, hosting around 90 government websites without proper planning. In addition, we didn't have technical, networking or security staff on board. With the attacks on government websites, OMSAR recruited a security officer and created a cybersecurity committee in order to share all security measures, concerns and responsibilities with all Lebanese administrations. As such, we started working on a national cybersecurity policy guidelines to be adopted and implemented by all public agencies. Furthermore, OMSAR is planning awareness workshops directed at Lebanese employees in order to raise their awareness on [cyber]security.

E About six years ago, government websites were the target of cyberattacks. Were the attacks a catalyst for the government to improve cybersecurity capabilities?

There were many attacks hitting OMSAR servers and many websites were going down. The attacks began in 2011, targeting our web servers, hitting many websites, especially the websites of the Ministry of Interior and the Internal Security Forces. Because we had only one web server for all the websites, all the attacks affected the other government websites. [In response], the Council of Ministers decided to create a National Cyber Security Committee [NCSC]. The committee came out

with recommendations to secure our [online] environment immediately, [but these were] short-term security measures. We also decided to create a new web-hosting environment

and to build it based on international standards and security measures that define all the aspects of the web-hosting environment - [in order] to be a state-of-the-art national web-hosting environment. This needs a lot of work and funding.

E OMSAR is drafting a cybersecurity policy. Is there any update?

We are working on it right now while simultaneously improving the security measures of the

■ The country does not have legislation to protect digital rights

current hosting environment. Each administration doesn't have [its own] cybersecurity officers – the IT departments do the whole job. If we found a hole, we'd fix it, and if we found another then we'd fix it as well; we didn't have a strategy, it was more like patchwork. We published a cybersecurity policy to guide the directors of the administrations on how they should create their security policies. We came up with a brief document, like a pamphlet, to make it easy to use and follow.

E *How did OMSAR assess public agencies' readiness to adopt the recommendations of the cybersecurity policy?*

Even before publishing we were wondering how to get the administrations started, so we created a checklist. This helped [departments to self-assess] where they were on cybersecurity. We published the checklist in 2015.

■ The attacks began in 2011, targeting our web servers, hitting the websites of the Ministry of Interior and the Internal Security Forces

E *Did public agencies check it again in 2016?*

It's an internal process for the public agencies. OMSAR doesn't have a mandate to supervise [the other administrations] – if they request help we are always ready to assist and provide them with the needed help.

E *In terms of measuring the assessment, is there any indication at a government-wide level of cyberdefense capabilities?*

I don't have any accurate information. In 2015, before publishing, we thought of putting the checklist online – so we could fill our database with the respective [administration's] information. But after negotiating with decision makers, it was decided against that because of privacy and security [concerns].

E *If the oil and gas industry, for example, goes active then there will be seismic data, exploration data and many other valuable datasets. This vital data could probably be one of the more attractive hacking targets in Lebanon because of its actual money relevance. Is*

FOLLOW EXECUTIVE ON FACEBOOK AND TWITTER



www.twitter.com/executivemag



www.facebook.com/ExecutiveMagazine

Executive

Cybersecurity

protecting such data part of the mindset in the ministries or at the government level?

One of the recommendations of the [NCSC] was to build a national data center for the whole government. We need more time because this issue requires critical decisions by the cabinet to identify who will take responsibility for the data center, securing it and transferring data between administrations. In addition, if we want to create a national data center, all the data for the government will be residing in it and, as such, it's a critical issue.

E *What is being done to prepare a national data center?*

In OMSAR's e-government unit we have an interoperability sub-unit. Now we are working on creating a specific design to be implemented by the government, connecting and transferring data between administrations [in a secure way]. Maybe this will lead us to the next step of creating the centralized data center.

E *Cybersecurity breaches, cyberwarfare and criminal hacks have increased tremendously, especially in the last couple of years. Some companies are claiming a 4,000 percent increase in the rate of cyberattacks in the last five years.*

Yes, for sure.

E *That seems to be a cause for concern.*

There have been many voices raising this issue, especially from the Internal Security Forces, who have a cybercrime unit. They've requested the Ministry of Justice, and maybe the cabinet, to work on such a law. If I attack your server and steal your data, the criminal code has no text defining such cybercrimes and their penalties. For now, they're applying the standard criminal code and adopting it to cybercrimes.

■ ***If I attack your server and steal your data, the criminal code has no text defining such cybercrimes and their penalties.***

E *An individual from a cybersecurity firm said that state-sponsored hackers are sent on training missions to attack another country just so they know how to attack better. So they can attack Lebanon, and even if they get caught, there is very little danger of repercussion from the state because there is no legal framework. Another*

individual said because internet bandwidth in Lebanon is so limited a distributed denial of service (DDOS) attack is very easy, and it takes very little effort to shut down a website.

And this is why one of the recommendations is migrating to the cloud. Estonia, for example, is a completely electronic government – they are totally digitized. Because of the very high risks of cyberattack, they've migrated the government to the cloud.


E *Will the government migrate to the cloud?*

In 2015 we had many [consultations] from companies to advise the government on how to build a secure cyberenvironment. Those companies advised the government to move to the cloud. We came up with a terms of reference (TOR) – all our needs and requirements for securing networks – and we took it to the previous cabinet to get approval for the funds because it is quite costly, and it was signed. Now, there's still a debate of whether to go to public clouds, such as Amazon, Google or Microsoft, or have a private cloud since data cannot go outside Lebanon. There is a decision from the Council of Ministers in 2014 about a partnership between OSMAR and OGERO to build a private cloud for the Lebanese government, in addition to a redundant data center for the e-government portal.

E *Will it be implemented?*

Currently, our minister is working with the Ministry of Telecom and in collaboration with OGERO on setting a Lebanese National Cloud Computing Policy, in addition to executing a private cloud for the Lebanese administration and a secure government network for interoperability.

E *The CTO of Microsoft Middle East says their data suggests Lebanon experiences more cyberattacks than the global average, and if there was a Computer Emergency Response Team (CERT) in Lebanon, they could collaborate with Microsoft to reduce attacks to the global average.*

The national cyber security committee recommends the creation of a CERT. A year ago, we had a meeting in the [prime minister's offices] with the Telecommunications Regulatory Authority [TRA] and they mentioned that they started creating a CERT for Lebanon. But the TRA doesn't have any mandate to create and manage the CERT I think they took it as an initiative. Currently, I don't know of any update on the subject. 

Children cannot live without a Heart



Donate before it's too late

Congenital Heart Disease is the number one killer in the first year of life. One in 100 babies is born with Congenital Heart Disease.



REPUBLIC OF LEBANON
MINISTRY OF PUBLIC HEALTH

71 483 248

  braveheartfund

Cyberthreats in the GCC and Middle East



"We are vulnerable in the military and in our governments, but I think we are most vulnerable to cyberattacks commercially. This challenge is going to significantly increase."

Michael Mullen, former chairman of the joint chiefs of staff, United States Department of Defense

Building legislative defense shields

Cyberattacks present themselves in a multitude of facets, although there is no absolute single definition for cybercrime in existence. From a general perspective, cybercrime can be defined as "illegal activities, internet mediated, that occur in the context of global economic networks". The main categories of attacks are hacktivism, financial theft, data theft, ransomware, cyberespionage, cyberterrorism and cyberwarfare.

Last year shed light on new dimensions of cyberthreats in the political arena, as diplomatic confrontations erupted between the United States and Russia over allegations of Russian hacking aimed at influencing the US election. But cybercrimes are materializing globally and growing exponentially. The damages being caused by cybercrime vary from financial to reputational, as well as political and military. Cyberattacks are capable of penetrating highly sensitive and protected sectors, such as defense and national security.

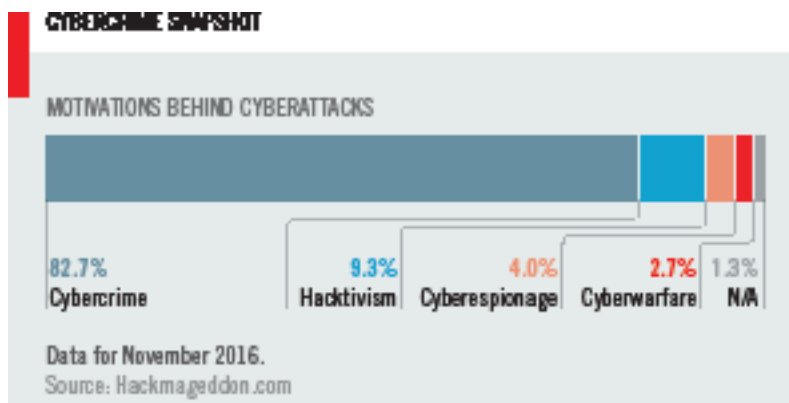
What is causing the rapidly evolving categories of attacks is the augmentation of internet traffic and usage, combined with the development of new platforms for internet delivery such as tablets and

smartphones, to name a few. One can affirm with conviction: wherever there is the internet, cybercrime will follow. The statistics are staggering – in 2016, there were 2,871,965 globally registered notifications about attempted malware infections that aimed to steal money via the illegal online accessing of bank accounts, according to the Kaspersky Security Bulletin. The bulletin derives its statistics from the Kaspersky Security Network – meaning the real number could be higher. "In February 2016, hackers used the SWIFT credentials of Bangladesh Central Bank employees to send fraudulent transaction requests to the Federal Reserve Bank of New York, asking it to transfer millions of dollars to various bank accounts in Asia. The hackers aimed to seize \$81 million transferred to the Rizal Commercial Banking Corporation in the Philippines and an additional \$20 million destined for Pan Asia Banking." Fortunately, according to internet security firm Kaspersky, the ploy was discovered in time, when a typo was detected in one of the transfer requests.

In one of the first cyberattacks with huge cross-national security implications, the Stuxnet com-

puter worm targeted Iran's Natanz nuclear facility back in 2010. The malicious computer program differed from a virus in not needing to attach itself to an existing program, and in its ability to control electromechanical processes, such as those used to control machinery on factory assembly lines and centrifuges in nuclear reactors. Stuxnet destroyed one-fifth of Iran's centrifuges by attacking all control systems in industrial installations.

These incidents exemplify the level of damage that a cyberattack is capable of causing. A large-scale cyberattack against either systemic financial infrastructure (a major clearing house or two or three stock markets simultaneously) or critical military infrastructure has not yet happened, but both are deemed as realistic threats by security experts. Countries of the Gulf Cooperation Council (GCC) and in the wider Middle East are exceptionally vulnerable to cybercrime due to their exposure to interests of foreign parties, including states and activist groups as well as financial criminals, their geographical location and the political structure of the region. GCC governments are on the alert and have in recent years introduced legislative remedial actions that seek to address the cybercrime tsunami.



LEGISLATIVE OVERVIEW OF COMBATING CYBERCRIME IN THE GCC

Cybercrime cannot be limited to a single jurisdiction. It is transnational and fluid, and this has challenged legislators in developing and developed countries alike, as the current domestic and international laws and enforcement protocols are simply not designed to fit the current legislative models. Cybercriminals know this and the com-

plexities make it more difficult for the authorities to battle against this form of crime. Cooperation and harmonization across borders is key in order to ensure the development of gold standards of legislation and enforcement. In the past, the GCC relied on traditional laws, emergency codes and criminal codes to address cybercrime. The current position is that cybercrime legislation in the Middle East is under development, with some specific laws passed and the United Arab Emirates (UAE) leading in this field.

Cybersecurity in the UAE has been a priority for some time due to the growing number of cyberattacks. According to Kaspersky Security, an average of 17.4 percent of users in the Middle East encountered cyberthreats in the third quarter of 2016. Adding to the urgency is the fact that the UAE is the second biggest target for cyberattacks in the world, after the US, according to cybersecurity company Norse. As Rabih Dabbousi of UAE cybersecurity firm DarkMatter pointed out in 2016: "The exponential adoption of technology increases the UAE's attack surface which is becoming larger every second."

According to Dabbousi, the volume of financial transactions in the UAE and the country's attractiveness for investors are just some of the reasons why banks and other financial institutions are constantly being attacked. Faced with an intensive onslaught, the UAE has created arguably the most effective and comprehensive cybercrime law in the GCC. The first cybercrime law was introduced in 2006 (Federal Law No. 2 of 2006) and was replaced by a more expansive cybercrime law in 2012 (UAE Federal Decree-Law No. 5 of 2012), designed to combat information technology crimes and codify the relevant offenses such as the transmitting, publishing or promotion of pornographic material, gambling activities and indecent acts.

The law was later expanded to cover new offenses and to ensure alignment between the UAE legislation and relevant international treaties, such as the Budapest Convention on Cybercrime (signed November 23, 2001).

As a deterrent, the UAE cybercrime law in 2012 detailed severe punishments that include prison time up to a life sentence and fines ranging between \$13,614 and \$81,688 depending on the level of the

Cybersecurity

cybercrime. The law addresses specifically social media and any misuses that can be derived from it, such as fraud, identity theft and impersonation. The law categorizes cybercriminals as hackers who hack into other individual's accounts, criminals who are highly knowledgeable of the cyberworld and exploit it for financial gains, and individuals who threaten and commit malevolent acts such as impersonation, threats and solicitation.

Similarly, Saudi Arabia introduced cybercrime legislation in 2007, but definitional foundations such as privacy and confidentiality should be made more expansive. In Bahrain, the electronic transactions law (Federal Decree No 28 of 2002) was being utilized to tackle cybercrime, but it lacked specificity. After much debate, the country introduced a new cybercrime law in 2015, designed to counter illegal access to IT systems. Anyone convicted of entering, damaging, disrupting, canceling, deleting, destroying, changing, modifying, distorting or concealing IT device data concerning any government body will face a maximum of ten years in jail. From the perspective of fighting cyberthreats in this region, this is a very positive development as it indicates that GCC governments are realizing the urgent need to modernize cybercrime legislation.

Turning to other Middle Eastern countries, Egypt has relied on the intellectual property law (Law No. 82 of 2002), the telecommunications regulation law (Law No. 10 of 2003) and the electronic signature law (Law No. 15 of 2004) to tackle cyberattacks. However, these

laws contain fundamental issues related to identifying cybercrime, as they do not always offer an extensive definition of cybercrime so as to capture all parameters, and with procedural limitations in the prosecution of cybercriminals, especially the ones operating from overseas. Transnational cybercrime requires a far more sophisticated set of laws to tackle these type of crimes. A new Egyptian cybercrime law is imminent in 2017 and will likely seek to address several of the gaps in previous legislation.


Jordan can rely on the electronic transactions law (Law No 85 of 2001) and the cybercrime law (Law No 30 of 2010). From the perspective of a

legal expert, these pieces of legislation can act as a starting point but should be reviewed and expanded as the relevant investigative procedures require beefing up. Oman adopted a cybercrime law in 2011 (Royal Decree No. 12 of 2011), and it addresses a wide range of illegal actions involving the internet and computer devices. It is focused on defining crimes committed in cyberspace such as cyberbullying and cyberterrorism. This can also be considered as a good starting point, as the initial approach was the extrapolation of existing criminal laws and telecommunications laws to combat crime, which lacked realism.

The Qatari government has passed a cybercrime prevention law (Law No. 14 of 2014), another very welcome development in a drive to combat online and cybercrimes. The law imposes many sanctions and several penalties for offenses committed through IT networks, the internet and computers, and it safeguards the cybersecurity within Qatar, as well as the country's internet infrastructure.

GREATER COLLABORATION TO SHIELD AGAINST CYBERCRIME

The field of internet communication is expanding continuously and cybercrime is evolving and adapting to the changing information landscape. The current legislative platform in the GCC has improved considerably in the last few years by providing legislative harmonization, as specific legislation has been passed in most countries. However, cyberattacks are becoming more bold, unpredictable and mainly transnational. The domestic laws require constant updating, and in order to prevent and shield countries from attacks, greater international collaboration is also required.

International and regional conventions for the fight against cybercrimes such as the Arab Convention on Combating Information Technology Offenses (2010) and the African Union Convention on Cyber Security and Personal Data Protection (2014) are encouraging, but remain limited in their reach and scope when measured against the global severity of cybercrime. It is believed that a new international convention on cybercrime is required to address transnational attacks more effectively and will involve the global community as a whole. 

NICOLE PURIN is a legal expert working in the GCC banking sector. The views expressed in this article are the author's personal views on the topic.

Under the High Patronage of the President of the Republic of Lebanon

General Michel AOUN

Children's Cancer Center of Lebanon First Childhood Cancer Conference

A one-day public conference to know more about childhood cancer
to commemorate the CCCL's **15 years anniversary**.

Friday April 7, 2017

At Issam Fares Hall, AUBMC
Starting 8:30 am

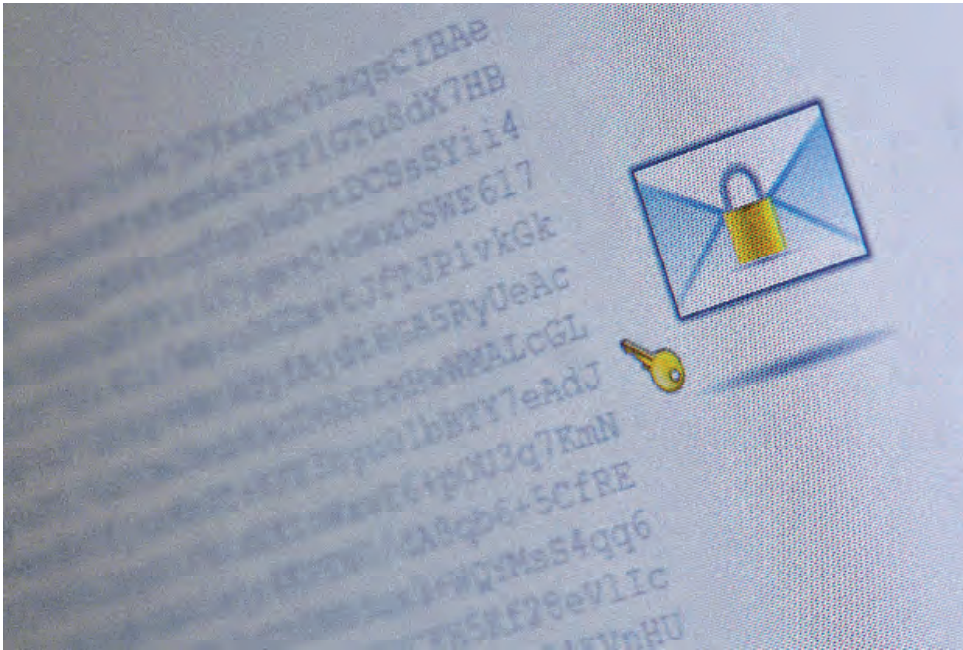
Free registration:
www.cccl.org.lb

For more information:

+961 1 35 15 15 or
+961 70 35 15 15



How to protect your email from cyberattacks



A step by step guide

The numbers are overwhelming. Ten million malicious emails are prevented by Google every 60 seconds. Hold Security discovered a cache of 272.3 million hacked email accounts last year from major providers around the world, and more than half a billion personal records were stolen or lost in 2015, an increase of 23 percent from previous years, according to the 2016 Internet Security Threat Report (ISTR).

The increase in cybersecurity threats is alarming, and given the statistics, it is difficult to feel assured that our digital lives are secure. Cybersecurity should no longer be only a concern for states, businesses and public figures. It should be a major concern for every single person.

STEP ONE: ACKNOWLEDGE THE THREAT

Alarmingly, too many people are neither concerned with nor aware of the seriousness of the problem. They adopt the attitude that it will never happen to them as they have nothing to hide. There is no need to be harboring state secrets, however, to exersize a minimum level of

privacy, protection and security. Internet users should start to actively look for ways to protect themselves. The internet's reach and scope are increasing exponentially, and organized criminal activity on the dark web is constantly on the lookout for new techniques to hack their targets, while by and large our security threshold remains the same.

The consequences of this could be devastating. John McAfee, founder of Intel Security Group, a global computer security company, has warned: "An email hack can destroy our digital world, and we won't see it coming." Estimates from various hacking groups say that passwords for 75 percent of the world's email accounts are available for purchase on the dark web. Beyond that, there are thousands of videos, tutorials and softwares online on how to hack into emails, social media accounts, smartphones and others.

STEP TWO: SECURE YOUR PASSWORD AND DEVICES

It goes without saying that the first step is to have a strong password that is a mixture of uppercase and

lowercase letters, numbers and symbols. Security experts warn against reusing the same password over separate accounts, and some suggest changing passwords often to add an extra layer of protection.

Other safety steps include: installing a well known antivirus, performing constant software updates, avoiding public PCs, being cautious of public Wi-Fi at airports, coffee shops and other locations, and opting for Secure Sockets Layer (SSL)/Transport Layer Security (TLS) when available. Also, it is best to use two-factor authentication when possible.

Regarding email addresses, avoid easy to guess emails, i.e. john.smith@gmail.com. Instead, add random numbers and characters, and avoid posting your email over the internet on blogs, websites and social media. Any hacker who knows an email address can click on the forgot password link in the webmail and try to guess the answers to the security questions, so make sure to give obscure answers.

If you do want people to contact you online, one trick is to post your email as a picture instead of having it written as text; spam software are not able to decode images. Avoid replacing the @ with (at) or .com with (dot) com in an email address; while people think this tricks spambots it is in fact very easy to decode.

STEP THREE: SECURE YOUR EMAIL

The hack of Democratic Party officials during the United States presidential elections were global news, not just for their political impact, but also because of cybersecurity concerns. If those emails had the latest level of encryption, hackers would not have been able to get their content.

The two most commonly used encryption protocols are Pretty Good Privacy (PGP) and its newer successor Secure/Multipurpose Internet Mail Extensions (S/MIME).

Although you can use the older PGP protocol, cybersecurity experts advise using S/MIME protocol if possible, as it is much more secure and offers authenticity (explained below), which you do not find with PGP.

S/MIME consists of two security services: digital signature and encryption. These two services combined offer a high level of email security. A digital signature is a unique code added to your email that proves authorship and assures the receiver that it didn't come from someone pretending to be you, and that the email has not been edited or changed during its transit.

Using a digital signature alone is not enough, however, as your email will be traveling servers in

plain text, making it very easy for hackers to intercept and read. Here, the role of encryption in S/MIME comes into play. Encryption makes your email unreadable to everyone except the intended recipient.

Setting up email encryption can be a laborious process, however. Below is EXECUTIVE's guide to securing Outlook, Hotmail and Gmail email accounts.

MICROSOFT OUTLOOK DESKTOP APPLICATION FOR WINDOWS

1. Click on the **File** tab in Microsoft Outlook, then select **Options** -> **Trust Center** -> **Trust Center Settings** -> **Email Security**.
2. Under **Digital IDs (Certificates)** click on **Get a Digital ID**, Outlook then opens up a page with a list of some of the certificate authorities (CAs) that are qualified to issue digital certificates. (Some CAs offer free Digital ID like COMODO and StartSSL, others you will have to pay for. The price ranges between \$5 per user a month to around \$10 per user a month).
3. Assuming you get your Digital ID from StartSSL, all you have to do is to go to their website using Mozilla browser, sign up for the free package and your digital ID is ready to install. If it doesn't install automatically make sure to click on the **Install** button.
4. From Mozilla menu tab, click on **Tools** -> **Options** -> **Advanced** -> **View Certificates** -> select **Your Certificates** tab.
5. Locate your certificate under "SmartCom Ltd" and click on the **backup** button.
6. It will then prompt you to add a password in order to protect your certificate. (Make sure to remember the password as there is no recovery option for it, and your certificate won't work if you don't provide the password. It's also advisable to make a copy of the certificate file you have just downloaded and store it on a USB drive). After you complete all the instructions below, delete the file from your computer, otherwise any person accessing your computer can take it and start sending emails on your behalf.
7. Going back to Outlook, Click the **Import/Export Digital ID** button located under **Digital IDs (Certificates)** (see step two).
8. Under **Import/Export Digital ID from a file** click on **Browse** and select the digital signature file that you just downloaded on your desktop.
9. Enter the same password that you just used for backing up your digital signature in step six. Press **Ok** and you will be redirected to the **Email Security** -> Press the **Settings** located under **Encrypted E-mail**.
10. Click on the **Choose** button located in the **Change Security Settings** window to select the

■ More than half a billion personal records were stolen or lost in 2015

Cybersecurity

signing certificate. It might get selected automatically by Outlook, if not then browse and select it.

11. Press **Ok** and then **Ok** again.

12. Go back to **Email Security** -> under **Encrypted E-mail**, check the **Add digital signature to outgoing messages** and then **Send clear text signed messages when sending signed messages**.

Now you can start sending digitally signed emails, and users can differentiate them through a small red certificate icon at the right of your email if the receiver happens to use Outlook. Double-clicking on that icon will show whether the certification is valid and trusted or not.

After setting up your digital signature, the next stage is encryption. Provided you have followed the steps above, this is a simple process: click to enable encryption in your Outlook. Encryption is a two-way process, meaning that the sender and the receiver should exchange their digital signatures by email and save these in their contacts. When digital signatures are exchanged between the sender and the receiver, only then can they start exchanging encrypted emails.

■ Using a digital signature alone is not enough, however, as your email will be traveling servers in plain text, making it very easy for hackers to intercept and read

HOTMAIL WEBMAIL CLIENT

Outlook Web Access, which runs Hotmail, only supports S/MIME on Microsoft Windows® 2000 and Internet Explorer 6 or higher. This is provided you already have a digital ID, explained in steps above. Only then can you install the S/MIME control.

Once installed, you can use the **gear menu > S/MIME settings** to encrypt all messages. Simply select **Encrypt contents and attachment of all messages I send** and **Add a digital signature to all messages I send**.

EMAIL WEBMAIL CLIENT

Gmail supports TLS connection, which means that the connection is secure and encrypted, but not the email itself. For the TLS connection to persist when an email travels to data servers other than Google's, then those servers need to support TLS as well. It's important to note that Gmail emails are stored as plaintext on Google's servers, without any encryption. Back in 2010, a Google employee was

fired after being caught using information from a teenagers' emails accounts to stalk them. Since then, Google has taken some measures to increase its security locally, although Gmail emails are still stored as plaintext on their servers.

Currently S/MIME is only active for Gmail Enterprise and not solo users, so EXECUTIVE searched for an S/MIME add-on that would work on Gmail but found none. Gmail users can, however, make use of PGP encryption. As stated earlier, PGP protocol is older than S/MIME. One of the drawbacks is that it doesn't encrypt email headers, allowing a hacker to see who an email is addressed to, though its content stays encrypted. However, when a PGP-encrypted message is additionally encrypted by a TLS connection, the sender and receiver will become encrypted as well. This solution ends up very secure, as emails are not only safely encrypted during transit, but are also stored encrypted on Google's servers as well.

PGP relies on something called public-key and private-key, which a user must own in order for them to receive encrypted emails. Those keys are generated by third party companies that support PGP encryption. The public-key encrypts the message while the private-key decrypts it. Once a user has those keys, they must share their public-key with other users, either by uploading it to special servers or by sending it via email. Let's say that A wants to send an encrypted email to B. A has to encode his email using B's public-key. When the encrypted email reaches B, he can decrypt it using his private-key.

There are many free PGP add-ons available online, and they make the process very easy for anyone to use; you just have to follow their instructions. EXECUTIVE has tested Mailvelope and Enlocked add-ons for webmail clients (Gmail and Hotmail), and they proved very user friendly.

However, if you don't want to bother with add-ons, browser compatibility and so forth, you can always switch to a webmail client such as ProtonMail, as their server can't be decrypted (though ProtonMail has become so popular you might find yourself on a waiting list), or you can use a third-party company like DocuSign where you can digitally sign and S/MIME encrypt your email before sending.

In order to be secure, you constantly need to stay up to date on the latest security releases, performing regular updates of your software, and encrypting not only your emails, but your computer, laptop and mobile as well. Act now, before you become the next victim. Stay secure, and stay safe. ■

PROJECT LEBANON



16 - 19
MAY 2017

BIEL - BEIRUT

Concurrent with:



7th Edition

BUILDING INTERNATIONAL NETWORKS

Construction Material & Equipment

22nd Edition

Book Your Space Now

+961 5 959 111
projectlebanon@ifpexpo.com

projectlebanon.com



Official Insurer:



Official Hotel:



Official TV:



Official Freight
Forwarder:



Official Air
Express:



A step toward transparency

Obstacles, benefits and the need for anti-corruption commission

After nearly a decade of preparation and debate, Lebanon's Parliament finally ratified an access to information law in January. The country is consistently perceived as corrupt, according to global watchdog Transparency International, and Lebanon does not rate highly on the World Bank's ease of doing business index. Enforcement of this new law might, over time, help improve those rankings, as well as the business investment environment and the quality of services the government provides to the public – all while coercing Lebanese authorities to be more transparent and accountable to the citizens. The law came into effect in February but, while this magazine has not yet put it to the test, its implementation could face some obstacles, and another law is still required to establish a key body crucial to define what information actually is accessible.

OBSTACLES

The law prescribes that virtually all government entities publish key documents showing indicators of each office's performance, such as an annual report, orders and decisions, and office expenditures. Government offices are required by law to publish these documents online, but a number of these entities do not have websites, so it is unclear how soon they would be able to comply with this particular aspect.

The law also outlines a process by which specific information can be requested from the government (see EXECUTIVE's explainer page 54, and accompanying infographic page 56), detailing what is to be published and laying out the stages accompanying any request. The law is a welcome and positive step toward improving transparency and public accountability, civil society stakeholders tell EXECUTIVE, but there will be challenges in requesting information and in appealing requests that are denied.

The law calls for the establishment of an anti-corruption commission (ACC) that would serve three primary roles. First, it would act as a watchdog by investigating allegations of corruption. Second,



Ghassan Moukheiber consults with other MP's.

as an educational entity guiding public servants in filling requests and informing citizens' awareness of their right to information. Third, it would serve as an advisory body consulting authorities on whether information should be disclosed or remain confidential. Establishing the ACC requires additional legislation that is still in subcommittee at the Parliament, according to Ghassan Moukheiber (see Q&A with Moukheiber page 53).

The fact that the ACC is not established as the access to information law goes into effect is a concern at multiple levels. Administrative records could be hard to track down because, based on observational evidence, they're neither regularly digitized nor systematically archived.

Public officials, innocently or not, might not include pertinent information in the required documents to be published automatically on their offices' websites, or they might deny requests simply because there is no culture of disclosure within the government, says Dany Haddad, a former consultant for the Lebanese Transparency Association, the local chapter of Transparency International. The law is "asking them to be like the private sector, where you have to report about your work, but the public sector has never done this," Haddad says. The ACC would be instrumental in defining what information is disclosed, and without it in place there is no central authority deciding how narrowly to interpret information that is exempted from

disclosure. The law lists broad categories where information would not be accessible, including: professional and trade secrets; private information relating to individuals and open court cases; minutes of confidential government meetings; opinions issued by the State Council; and state secrets relating to security, foreign relations or the economy. So, hypothetically, Banque du Liban (BDL), Lebanon's central bank, could cite banking secrecy in a refusal to deny figures on its stimulus packages.

The ACC would also be the authority ruling on appeals to denied or ignored requests. But it is just one of several avenues of appeal, Moukheiber says. While the law prescribes that the State Council will rule on appeals of ACC decisions, it does not clearly outline where appeals should be heard in the absence of the ACC. "You always have to ask, what if we don't establish the anti-corruption commission? Will this law be null and void? The answer is no," Moukheiber says, adding that Lebanon's common law of administration allows appeals of denied requests to be heard by the State Council and other courts. But, he admits, this could be open to interpretation. "I'd say you have three appeals possible: you can go to court; you can pursue disciplinary prosecution of administrative recourse to force the administration to give the document; or, after it's established, appeal to the anti-corruption commission."

That is worrisome, says Ayman Mhanna, executive director of the Samir Kassir Foundation. "My concern is that the law specifically says where the appeal should go," a risk, he says, that could push the courts, or the State Council, to back away from ruling on appeals. "They could say 'the law states the appeal should go to the [anti-corruption commission], therefore we cannot look into it,'" Mhanna adds.

HOW IS IT USEFUL?

Access to information is not just about digging up the government's dirt or exposing corrupt practices. "There is a very strong role for journalists," Mhanna says, "very often people look at access to information only from a confrontational point of view. I think this approach is needed, but it's not the only way to get results." Access to information can be used in a very constructive and non-confrontational way to improve the quality of journalism, especially investigative journalism. Government-produced reports and statistics can inform long-term planning on public health issues, for example, by international donors and on-the-ground non-profits providing health care access. Data measuring the sectors of the economy can also help foreign and local investors make decisions about where to put their money.

Q&A WITH GHASSAN MOUKHEIBER

ON THE ACC, ITS TASKS AND POTENTIAL FORMATION

E *What will be the role of the Anti-Corruption Commission (ACC)?*

The Anti-Corruption Commission is responsible for a number of tasks, in addition to hearing appeals [if access to information requests are denied]. It receives complaints related to the implementation of this law, investigates and issues decisions. It advises competent authorities on every issue. So if you're an administration, and you're uncertain whether [a piece of] information has to be disclosed or is confidential, it acts as an advisor. It publishes annual reports about the implementation of the law. So it's a watchdog on the law, and it contributes in education and raising citizens' awareness on their rights to access information. It's a watchdog, it's an education entity, it's an appeal [body] and it's an advisor.

E *Who might be selected to sit on the ACC's board?*

The members will be nominated by third parties such as the courts, the bar associations, the auditors' association and the banking association. So the Council of Ministers will appoint members from the ones that are nominated by third parties, and its operations will be totally independent.

E *What is the status on forming the ACC?*

It's in subcommittee and is going to justice committee. So it's in an advanced phase of drafting. In the absence of the anti-corruption commission, it is the role of the prime minister to oversee the proper implementation [of this law] by all ministries because the prime minister is the coordinator of all ministries. You always have to ask, what if we don't establish the ACC? Will this law be null and void? The answer is no. Because you always have judicial recourse.

E *Do you feel that now there is an appetite for reform?*

It is necessary to complete our institutional build up for fighting and preventing corruption. [The ACC] is a tool to prevent corruption. And it's only a tool, a necessary condition, but it is not a sufficient condition for fighting corruption. It is necessary to have transparency but that does not fight corruption all by itself. [The ACC] is not sufficient. It's a piece in the puzzle, but an important [one].

E *Is there other legislation that would complement access to information?*

There's the whistleblower protection, which is ready. I was surprised to notice that it was sent to another committee, but we are trying to get it through as quickly as possible. We are also in the last phases of drafting a new bill, a modification of a current bill on tacit declarations and illicit wealth. That's also almost completed and will be sent to the justice committee.

Overview

Access to information law

That information might take the form of up-to-date statistics, reports or internal government correspondence that could help business executives make decisions that impact their companies' bottom lines long into the future. One of the complaints often voiced in EXECUTIVE's interviews with business owners, executives and managers is a lack of economic data (often because the government has neglected its collection or dispersion) across a number of indicators.

The law could help attract foreign investment and enhance the business environment by improving market transparency. Lebanon is ranked 126th out of 189 countries in the latest edition of the World Bank's Doing Business report, a ranking of great concern, the minister of economy said in comments published last month in EXECUTIVE. That the law requires government offices to publish annual reports, expenditures, decisions and reasons for making those decisions is, to the business community, less about corruption and more about indications of how those offices are governing and how they will in the future. More information could encourage investors to put their money to work in Lebanon.

While Transparency International measures the perceived levels of corruption, an index that consistently ranks Lebanon as a very corrupt country, there are no overall figures on the cost of corruption to the Lebanese economy. What is available are self-reported bribery payments by individuals seeking help in processing paperwork or securing other government services. Those bribes are tallied by *Sakker el Dekkene*, a local watchdog. The 2,543 self-reported cases of bribery since the organization began its tallies in 2014 totaled nearly \$2.6 million. But that data gives only a limited picture of the scale of bribery and is only a first indicator of the total cost of corruption.

Then again, access to information and the substantial reduction of corruption are major tenets of goal 16 of the United Nations Sustainable Development Goals. "National and local institutions must be accountable and need to be in place to deliver basic services to families and communities equitably and without the need for bribes," the UN says in response to why goal 16 matters. How does one do that? By exercising the right that Lebanon's law now grants: to request information and hold public officials to account.

"The challenge of this law is implementation,"

Moukheiber says. "But it is also a challenge for people to use it. For people who ask if it's going to be enforced or not, I say that the proof is in the pudding, as the saying goes. You have to use your right, even if you're denied. It is resilience that'll lead us to the fulfillment of our rights."

EXPLAINER

The access to information law prescribes that virtually all government entities - including public administrations, judicial authorities (civil and religious), municipalities, state-owned enterprises, private companies managing public assets and government concessions such as Electricite du Zahle - are required to automatically publish: an annual report and the laws, decrees or decisions they issue and the rationale behind issuance; and expenditures on their websites. A number of these entities currently do not have websites, so it is unclear how soon those offices could comply with this aspect of the law.

The law also allows for specific requests of information held by the government. Any individual or organization can request access to view and receive copies of the requested information, paying only the cost of printing. Requesting information is a relatively straightforward process. The requester simply sends a letter describing the documents or data sought to the office(s) that might have the information. The office(s) must immediately acknowledge receipt of the request and has 15 days to deliver, but can extend the deadline for another 15 days to track the information down.

Accessing this information however, could be problematic on both ends. While the government is slowly scaling up digitization of administrative records and some public entities do already have records accessible online, they have not always been consistent with the physical documents.

Information requests relating to national security, foreign relations, financial and economic interests of the state and safety of the national currency, individuals' private information, including mental and physical health records, and trade secrets can be denied under this new legislation. Following a maximum of 30 working days after submission the requester should either receive the information or be given a reason why the information was not available.

There are procedures for requests that are denied. An appeal can be filed within two months from the date of the request's denial or after the 30 day period if the request has been ignored. The body responsible for hearing appeals of denied requests, the Anti-Corruption Commission (ACC), is not yet established (see Q&A with Ghassan Moukheiber). In lieu of the ACC appeals can be directed to the judiciary, but there are questions as to whether judicial authorities would hear appeals that the law specifically states should go to the ACC. The infographic on page 56 illustrates the request and appeal process.

24TH EDITION



4 to 7 April 2017
3-9 pm, BIEL - Lebanon

NETWORK AND STAY ONE STEP AHEAD WITH

+ 350 suppliers + 350 exhibitors + 2,500 local and international brands + 20 international celebrity chefs
+ 30 top international food, drink & hospitality experts + 500 participants in + 25 daily competitions and workshops



STAY AHEAD WITH THE
HORECA LEBANON APP!



GET YOUR ONLINE BADGE
horecashow.com

GOLD SPONSORS

Boecker®

Prunelle

SUPPORTING HOTELS

ROYAL
HOTELS & RESORTS - BEIRUT

PHOENICIA
BEIRUT

OFFICIAL MAGAZINES

Hospitalitynews
MIDDLE EAST

Taste
& FLAVORS

OFFICIAL CARRIER

MEA

SUPPORTED BY



ihra



AN EVENT BY

Hospitality
SERVICES

hospitalityservices.com.lb

Access to information law

ACCESS TO INFORMATION LAW

1

WHAT DOES THE LAW MEAN?

In principle, the law increases the transparency and accountability of public institutions:

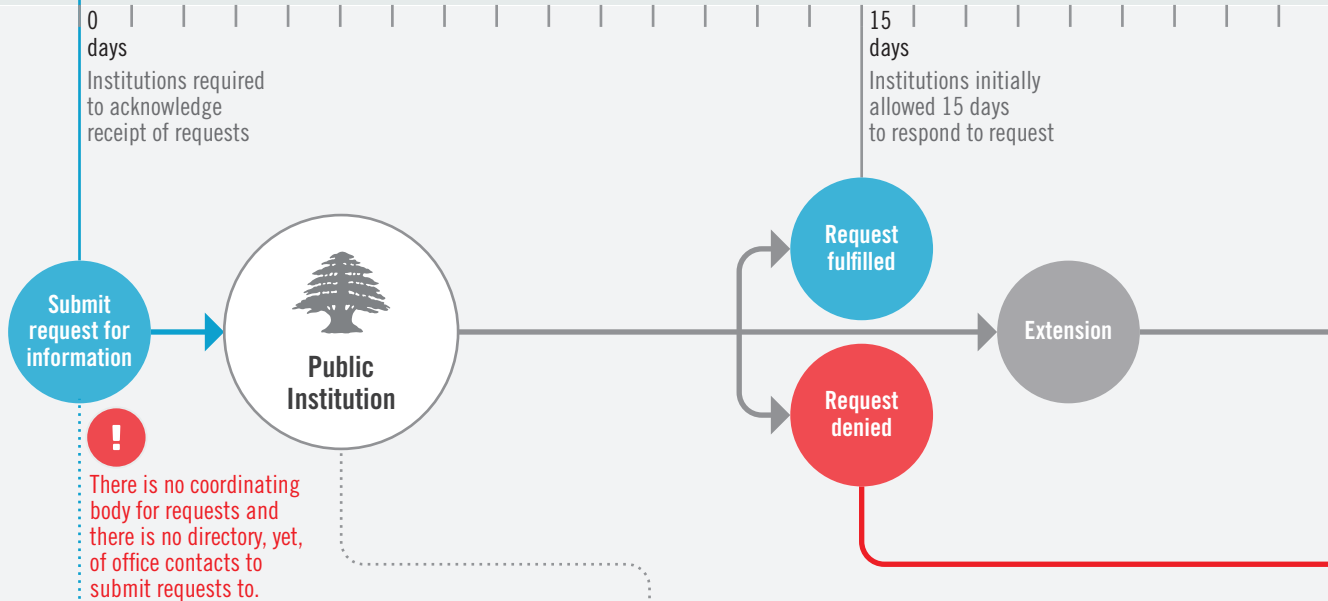
A

Institutions required to fulfill requests for information from the public

B

Institutions required to automatically publish certain types of information related to their operations on their websites

0 days
Institutions required to acknowledge receipt of requests



4

WHAT TYPES OF INFORMATION CAN BE REQUESTED?

- Administrative documents
- Statistics, reports & studies
- Internal & external correspondence
- Concluded contracts
- Archives

5

WHICH INSTITUTIONS ARE INCLUDED IN THE LAW?

- Public administrations
- Public institutions
- Judicial, administrative & religious courts
- Municipalities & federations
- Private companies managing public assets
- State-owned enterprises
- Companies operating government concessions

2 WHAT MUST BE AUTOMATICALLY PUBLISHED?



Annual reports



Decrees & decisions



Rationale for decisions



Expenditures

3 WHERE IS INFORMATION PUBLISHED?



Website of institution



Many institutions including government agencies, judicial authorities and municipalities do not have websites.

30 days

Institutions can take a total of 30 days to fulfill or deny request

Request fulfilled

Request ignored

Request denied

+60 days

Applicants have up to 2 months from the date the request was denied to appeal.

(If request ignored, 2 month appeal period starts 30 days after initial request submitted).

Appeal denial

6 WHAT INFORMATION CANNOT BE ACCESSED?



State secrets relating to security, foreign relations & economy



Professional & trade secrets



Private information relating to individuals and open court cases



Minutes of confidential government meetings



Opinions issued by State Council

The ACC would advise authorities on disclosure and would clarify appeals on denied requests.



Without the ACC, exemptions will be open to interpretation (e.g. the central bank might cite banking secrecy for data on stimulus money).

7 HOW DO APPEALS WORK?

Anti-Corruption Commission



The law requires appeals to be submitted to the Anti-Corruption Commission (ACC), an institution that does not yet exist.

Possible interim routes for appeals may include civil courts and the administrative court (State Council), the body that will rule on appeals of ACC decisions.

Roundup of numbers and sentiments

Rise of financial optimists

After a long and depressing dry spell that made local markets yearn for fresh investments, the Lebanese investment climate is looking up, says Jamil Koudim, the head of the asset management team at Beirut-based Banque Libano-Française (BLF). He presides over a family whose offspring has just doubled from a single fund to two. After the BLF Total Return Fund, which saw its inception in September 2012, the team put to effect the BLF Income Fund in November of last year. This new fund is open-ended, denominated in dollars and focused on fixed-income instruments. “We have mainly government bonds, central bank [certificates of deposit], maybe preferred shares of banks [in the portfolio] and any other fixed-income securities by institutions or corporations, and securitized products. Any fixed-income security is our market for this fund,” Koudim explains.

Though Koudim concedes that funds of this type are already offered by several Lebanese banks, the more significant part of the story surrounding the new product is its international attractiveness. He says that this rise in appeal is evidenced in the fact that financial entities outside of Lebanon have shown interest in this fund, and other local investment products. Koudim goes on by stating that what makes the new Income Fund (I.F.) alluring is the extra earnings potential that is encased in the possibility of Lebanese economic performance improving beyond expectations, which would enable the I.F. to provide returns in excess of its normal target. “If you offer an investment product, you have to be satisfied with the market

that you are looking at. This is where the story is. We really think there is upside to [the Lebanese market] following what we have been through. We view last year as worsening of the economy, but the swap transactions [by Banque du Liban] put a floor to that,” Koudim tells EXECUTIVE.

ATTRACTIVE STABILITY

He adds that he met with several representatives of international funds during a recent trip to London and that these funds, as well as some banks in the Gulf region looking for country-focused funds to recommend to their clients, are all showing an increased interest in financial investment opportunities in Lebanon. International funds were aware of the 2016 financial engineering measures adopted by Banque du Liban (BDL), Lebanon’s central bank, but their resurging interest was mainly based on political factors. “Their focus was more on the political outlook and political stability, both domestically and regionally. Syria is very important and the war of the past years is [now supplanted by rising stability].

All this is positive,” Koudim says.

His message of upside potential and optimism correlates with other recent local mood indicators for the economy in both soft and hard data. A January 2017 Economena survey of 17 economists working at Lebanese banks, universities, corporations and institutions found that the median expectation of the surveyed economists is for 2.5 percent growth of GDP in

2017, Economena referred to this as a “particularly bullish sign,” which was yet above the International Monetary Fund’s (upwards revised) projection of 2 percent growth. No economist in the survey expected growth of less than 1 percent for the Lebanese economy this year. Some even estimated growth to exceed the 3 percent real GDP growth projected by the International Institute of Finance for 2017.

According to the monthly EcoNews publication of bank SGBL, a consumer confidence indicator for Lebanon by regionally active ARA Marketing Research reached 161 points in the fourth quarter of 2016, which represents a 66.5 percent year-on-year increase, signaling the highest confidence level since 2011. EcoNews also pointed to economic upside potentials from oil and gas prospects, tourism, real estate, exports, external political relations and what it called a “rare domestic politi-

■ No economist in the survey expected growth of less than 1 percent for the Lebanese economy this year

cal breakthrough in late 2016.”

Optimistic views were also reported from a recent roundtable by the Lebanese Institute of Strategic Affairs (directed by economist Sami Nader), which said that the “enterprise landscape in the region is booming” and that Lebanon – albeit slow in embracing entrepreneurship as a drive for economic growth, and thus, not yet having developed to its full poten-

SOLICET

PRESENTS

Slava's

SNOWSHOW

STARTING 14 MARCH 2017
PALAIS DES CONGRÈS



INFO + 961 1 999 666

ORGANIZED BY

SOLICET

SUPPORTED BY



Mondanité



النمى
WWW.ANNAHAIR.COM



Executive

Investment Roundup

tial in this regard – “has gone a long way in developing its environment for entrepreneurs.”

As far as hard indicators from the banking sector, the Lebanon This Week (LTW) publication of Byblos Bank reported from Beirut Stock Exchange filings of six listed banks, that the aggregate net profits of these six banks rose 12 percent year-on-year to \$1.36 billion in 2016.

RICH DEPOSITS

Alone, the country's largest bank, Bank Audi, published headline numbers of \$44.4 billion in assets, \$36 billion in customer deposits, \$17.3 billion in loans and \$3.8 billion in shareholder equity. Its net profits came in at \$470 million, representing a 17 percent year-to-year increase, accounting for about 35 percent of the aggregate profits reported by listed banks, and, *nota bene*, a new record profit in line with the expectation noted in the year-end issue of EXECUTIVE.

While assets grew moderately, and net loan portfolio dropped 2.9 percent in year-to-year comparisons, Bank Audi noted that these dents in its figures were connected to currency depreciation in its largest two markets outside of Lebanon, Egypt and Turkey. When calculated on a constant exchange rate, the growth rates of consolidated deposits and loans both would have been 10 percent in 2016, the bank said, marking a difference in spirit to the opening sentence of its statement on its consolidated activity highlights in 2016, which read: “The year 2016 was difficult for the entire Middle East and North Africa region.”

Consolidated figures for the performance of Lebanon's 14 largest banks were not yet available from specialized consultancy Bankdata at time of this writing, but total assets of banks operating in the country grew 9.9 percent to 204.3 billion at the end of 2016, according to central bank numbers. Based on Bank Au-

di's publication in Lebanon Weekly Monitor (LWM), the growth of activity was higher than in 2015, and also higher than in the average of the past five years, by 78 and 61 percent respectively.

Customer deposits accounted for almost 80 percent of sector balance sheets and grew by \$10.9 billion in year-to-year terms, or 7.2 percent. Of this total deposits growth, \$8.6 billion, or 79 percent was in foreign currency deposits. Deposits in Lebanese lira (LL) increased by the equivalent of \$2.3 billion. Deposit growth more than doubled from \$3.1 billion in the first half of 2016 to \$7.8 billion in the second half. Growth of resident deposits and non-resident deposits both showed uptrends from one quarter to the next throughout 2016, with the rise of resident deposits being more pronounced between the two.

Whereas Lebanese Lira deposit growth was lower than in 2015, the growth of deposits in foreign currency exceeded that of 2015 by about 153 percent. The composition of deposit growth reflected the influence of BDL's financial engineering operation in the May to October period and related offers by banks seeking to attract foreign currency deposits in the course of the QE exercise. The dollarization rate of deposits increased by 90 basis points to 65.8 percent.

Lending growth in 2016 was of \$3 billion, a drop from the \$3.3 billion seen in 2015. Two-thirds of the loan growth in 2016 was a result of an increase in the Lebanese Lira denominated loan portfolio, which was driven up by the central bank's financial engineering, as intended. Foreign currency denominated loans rose by less than \$1 billion. “Lending activity growth yet rose by a healthy 5.4 per-

cent,” the LWM said.

Byblos Bank's LTW noted that total banking sector assets and deposits at the end of 2016 were equivalent, respectively, to 393 percent and 312.7 percent of GDP and that these rates-to-GDP were higher than in 2015. Loan-to-deposit ratios were 38.8 percent in foreign currency and 28.2 percent in Lebanese liras. According to LTW, gross foreign currency reserves by the end of 2016 stood at

■ Not all the signs for the Lebanese economy have switched from red to green, yet the mood indicators are more positive than in recent periods

\$34.03 billion, having dropped by some 0.71 billion since the end of October last year. The year-on-year rate of increase, however, was up to 11.06 percent.

Not all signs for the Lebanese economy have switched from red to green, yet the mood indicators are broadly more positive than in recent periods. But while BLF's Koudim highlights the good story for Lebanon that is entailed in regional scenarios of more stability, and domestic scenarios of budget and reforms for taking Lebanon in a more bullish direction, he makes a point that the known domestic downside scenarios of high risk and large public debts could be exacerbated “if the political hopes do not materialize.”

He elaborates: “We have seen that international investors, which normally are underweight on Lebanon, are now all interested and want to allocate a certain amount of money to trading Lebanon. What could turn things [back into negative sentiment] would be disappointment in terms of reforms, [and] in terms of political stability.” ■

HR Lebanon summit

March 30-31 | 8:00 am - 6:00 pm
April 1 | 8:00 am - 2:00 pm **2017**
Hilton Beirut, Metropolitan Palace

The ideal opportunity for senior thinkers and practitioners in the HR community to come together, share experiences and ensure corporate growth at the Levant's largest HR platform



■ WHY ATTEND

- 1 **Hear** from renowned international & local speakers and HR leaders
- 2 **Get** updates on the latest HR Industry's trends and initiatives
- 3 **Gain** tools to maximize performance and productivity at your workplace
- 4 **Learn** the best practices from some of the world's leading organizations / Exclusive case studies
- 5 **Benchmark** your HR practices against recognized employers of choice
- 6 **Network** with key leaders and international experts

■ KEY TOPICS

- A Survival Guide For the Age of Disruption: HR's Role in Lowering Stress & Boosting Shared Energy
- Building a Passionate Work Culture
- HardTalk: Difficult Conversations in the Workplace
- "Intelligent Organizations ... Only they will Survive", 7 Secrets to Thrive in the Future!
- Happiness at Work - The Ultimate Success Factor
- Designing Succession Planning
- Positive Leadership, Achieving Positive Deviant Performance
- Retention of High Potential Employees - Case Study
- An Incentive Scheme - Case Study

- Reinventing the Organization, the Collaborative Approach
- Performance Management: Is it Obsolete?
- Levers for Better Employee Engagement
- Benefits & Limitations of Psychometric Testing
- Culture as Competitive Advantage
- Creating an HR Analytics Capability to Deliver Actionable Insight

■ MASTERCLASSES

- HR Business Partners: Enhancing Your Strategic Contributions
- Behavioral Interviewing: Practices for Hiring Smart

REGISTRATION FEE 1000 USD for 3 days

Including access to 15 sessions & workshops, a half-day Certified SHRM Masterclass, an Attendance Certificate, unparalleled networking opportunities, exquisite coffee breaks & lunches.

For Registration
www.careerslb.com/lhrs

Tel: +961 - 5 - 45 67 45

E-mail:
lhrs@careerslb.com

**Seats are very limited & attendance is upon prior registration.*

A grand hotel plots a new course

Phoenicia Beirut's GM talks upcoming plans and her vision for 2017

The Phoenicia Hotel is one of Lebanon's most renowned five star hotels. Built in 1961, it catered to the era's most glamorous crowd, with Omar Sharif and Brigitte Bardot among its famous guests. After being destroyed during Lebanon's civil war, it reopened in March of the year 2000, and has managed to survive the various ups and downs of the Lebanese hospitality sector ever since.

Dagmar Symes was recently hired as the latest general manager, making her the first woman to serve as Phoenicia's GM.

EXECUTIVE sat down with Symes to talk about her plans for Phoenicia and her ideas for bringing the hotel's vintage glamour and appeal to 21st century guests' needs and lifestyles.

E What motivated you to accept the post of general manager at Phoenicia Hotel?

First of all, the Phoenicia is the Phoenicia: it's the landmark in Beirut. I believe it has grown the hospitality roots in Lebanon, and is a fascinating hotel as such. The Phoenicia is a "Grand Hotel," and a lot of my experience is very much linked to a refined environment; the grand hotel flair is really something I feel very comfortable in.

It's also an amazing challenge. The Phoenicia never had a woman GM before, and not to discriminate against anybody, but we [women] have a different way of seeing teams and refinement, and we are maybe more communicative in that regard. I think this is exactly what the hotel needs right now. This is how things fell into place from all parties.

E In your role as a GM of a grand hotel, what added value do you intend to bring to the table?

General managers are general, so we are a little bit everywhere, and this is how I perceive my role.

I'm the main cheerleader of the crowd, with a lot of specialists to ideally do the task. I see the true duty of a GM as leading the team, true leadership: management is here and leadership is here (gestures higher), and if you embrace the culture and embrace the people, you will get amazing results.

So, to align the team to go in the right direction with you is the key role to play, aside from the strategic part.

E Would you say the job is 80 percent heart and 20 percent brain? Or 40 percent heart and 60 percent brain?

If I say 80 percent heart and 20 percent brain then InterContinental and the owners would have a problem with me! (laughs)

I would say 50/50, knowing that right now I am more on the brain side rather than the heart side because the team deserves it, and also because of these difficult times in Lebanon.

Hospitality has lost, to a certain extent, its sparkle. If you lose the spark, and you're demotivated, you have a tendency to become maybe less quality driven. So I think to re-boost [morale] you have to spread the positive energy and pull everybody up again.

This is how I perceive the role of the GM: the first part is team-related and then of course it's business-related and number crunching. At the end I am judged by the numbers, but if you have the right team, you get the numbers right as well because it is all filtering down properly.

E What is your vision for Phoenicia, and how will you align it with the existing



vision of the owning family, given that the hotel has been in operation for a long time?

We want to use the hotel's very historical and well-established institutional roots to bring it to the modern world.

Why now? Because things are changing a lot. Beirut is very much into arts, into fashion, into clubbing, into a huge diversification of its culinary scene. This is why we have to be far more integrated to bring all that to a grand hotel, while still looking at the luxury and refinement appeal we have as an international platform.

The other part is the integration in the local market, which is through F&B primarily, and also through weddings. This is basically how we would like to move forward.

The third pillar is HR because Phoenicia has always been, and is, the breeding ground for the hospitality industry in Lebanon. So we want to also continue our duties by giving

the youngsters in hospitality a good base to grow or to start their career because the education system is so amazing here.

E *Does that mean that you are investing in your HR and training with a new kind of capital expenditure, or is it only more activity?*

What we need to do is to make people aware that it is an international company supporting the Phoenicia spirit, and I think honestly we have enough tools within the company that we largely exploit in a very healthy way.

Many people believe this is linked to a training manager. I don't believe so because on-the-job training now is far more important – and takes up literally 70 percent of your training – than the theoretical classroom-style approach.

We use that style of training in certain things because you have to, but the real training is with the right leaders and right managers on the spot. We have departmental trainers in every department, and a quality manager following up on that. It does not need to have an extra capital expenditure.

However for the talented, or in other words, those that have the right aptitude and attitude, and want to, we have put aside a budget to go beyond the classics. For example, I can send a pastry chef to France for four weeks to work with a Michelin chef. We have done this in the past and we will do it again.

E *You have a budget for it, but the system is not...*

We have the budget and the system is in place, but it is a matter of where we focus on first. Pure gut feeling and where we stand today would be the F&B team.

This is because the F&B is selling to the local community. It doesn't matter in which sense, if it's à la carte or banqueting, or a wedding, it is all F&B linked. Usually, hotels have a challenge with F&B outlets, and the community has a challenge with them; because for you, you're going into a hotel, and you think it's not really a restaurant.

Here our competitors are the freestanding restaurants out there;

we are not talking about hotels only anymore. In our vicinity there are 40 restaurants that I have to take into consideration.

E *Does that mean you are planning to redefine your F&B offerings?*

Definitely.

Given what I just said, we are redefining all the concepts to be quite honest. Eau De Vie – which is our fine dining outlet – has a huge potential from the setting alone and will have a new touch. Café Mondo was less frequented in the recent past because of the huge security barrier that blocked off the scenery for some time, but now it's accessible again, so we need to use the terrace and get this "living" spirit into the space.

Then you have the classics that need to be implemented. A grand hotel usually has an afternoon tea for example: does it need to be the afternoon tea of yesteryear? Clearly not! But I think we have been very creative in that sense and we will revive that as well, although maybe not on a daily basis.

E *In the past, the Salha group seemed a little wary when they said they've moved from making most of their money with accommodations to F&B as the main driver of their revenue. What is your view on that?*

This is absolutely true. Even last year's strategy was rooms oriented, because profitability in the rooms' part is far higher than F&B, and in different markets I would fully support this vision.

Having had a very challenging economic environment, you had to go with certain profitability rules to be able to have funds to invest in the hotel and everything else.

But again I believe Lebanon without food is the wrong approach, and we have to have fine balance. The food part always eats most of your share, but on the other hand, as I always tell the owning company, you wouldn't have all those restaurateurs out there if they didn't have a profitable operation.

E *When Phoenicia reopened, it was the only venture available for a certain class of events. Now you have had a number of competitors and halls in other places in Beirut, as far as Dbayeh, and as near as The Four Seasons and The Yacht Club. So the landscape is different, and your ambition is still to be the landmark within that landscape: how do you plan to do that with other capable operators, with international backing of their own, sprouting around you?*

Phoenicia has survived extremely well in a very difficult market context, and, yes, there are competitors, but you have certain market shares toward competitors.

If I compare myself with the Four Seasons, then it is the maybe more the business client and weddings rather than anything else. If I go Le Gray, it is the upscale international travelers; if I go Hilton, it's banqueting. So you know you grab a little bit of everything, whereas I understand that the cake is getting smaller and smaller with every new competitor in the local market.

Internationally, I think you have to be smart to focus on the right markets. Here, I think Phoenicia has always been extremely international. We are making huge sales throughout the globe, starting with the European market, our region as well as going down to South America, where there is a huge Lebanese diaspora.

When there are difficult times, we are more locally focused, so we are all somehow sharing the same cake. But we have a very strong wedding segment, and this was always one of the key segments which sustained the business in tough times. Competitors also help to position you properly, and this is what I would use for our repositioning.

E *But in your repositioning, do you aim to be known as the hotel that has a little bit of everything, or the wedding hotel or the meetings, incentives, conferences, exhibitions hotel etc.?*

I think we have to be part of everything by nature of the market. We

Q&A



are international, we are aiming at the corporate and leisure segment, we have a kids club for families and we have a beautiful spa. Overall, we have to grab onto everything.

However, the fact remains that Lebanon as a country is extremely attractive for tourists from the Gulf region. Phoenicia was always known as one of the hotels attracting these clientele and that will come back, but it was never our main focus to attract only, and exclusively, this market. I think it is a mistake that Lebanon does, in that we all focus on this market only, because if the ban comes, or if it collapses – this is the reality – everything collapses.

But, you know, we have never lost our position as such, as a landmark. It is a matter of getting back into a certain society, and having maybe had a shift there. I think also it is natural because [we are dealing] with the new generation, which is different.

E *Regarding this element, Generation Y's preferences and tastes are probably not the same as their grandparents'. How do you see yourself positioning the hotel vis à vis generation Y customers?*

First of all, this rejuvenation part plays a big role because Generation Y in my humble opinion is extremely visual in a way, so we will work on visual impact. We work a lot on social media; we are reaching out differently

through the Facebook approach, being younger and trendier.

When I say visual it's also everything related to images: photography and linking to old values – if you look back to traditional values such as fashion and art, most of the time you would link it to Europe – but reintroducing this in a very humble way will also automatically attract the youngsters.

E *Speaking of art, you have one of the largest presences of art in your overall hotel environment, but sometimes it feels as though it is one of the most understated with regards to awareness and visibility. Are you planning on attracting more of the art crowd to the Phoenicia?*

We definitely do. It's part of our program for this year. But I think you also have to be very careful with these things, because everybody is jumping on these kind of “new trends,” and art has a certain value which you should not use and abuse in a wrong way. Phoenicia indeed has a lot of art pieces in a very discreet way – we never made something fancy out of it.

E *Will this stay the same?*
Definitely.

E *The other thing you refer to is that feeling of Phoenicia being the most secure place for a traveler to come to. But on the other hand, of course, this total openness and accessibility was lost. What is your*

vision on hotel security?


I think you have to have a really fine balance. Personally, I wasn't in Phoenicia in the old times, and I'm not even sure we needed this total security environment; I don't believe so. We have a very well established and big security team, you cannot access the hotel through any funny backdoor. If we have delegations, fair enough, we get additional support from the local authorities.

For me, security has to have the right measure of prevention while maintaining guest contentment. If somebody really wants [to do harm] I think they are creative and smart enough to make it, but this you don't stop through getting a third barrier around your building.

E *What about the hard targets, the numbers? Do you have goals for 2017: annual year-on-year growth, anything that you can disclose? Will you be judged by how much increase in the year you can achieve?*

It's not necessarily increase only, but of course everything, at the end of the day, is based on numbers, on GOP, on profitability. That's the nature of the business. I think, however, that we went into our budget in a very positive way, because we believe that this year will set a new chapter with the new president and the first signs that confirmed this. We feel it also in the booking situation. If nothing really upsets this year's environment, we will definitely have a very, very positive year.

E *Any year-on-year comparison you can give us in terms of January actual, or Q1 bookings, 2017 versus 2016 ratios?*

All I can really say is that we have now already well succeeded and well passed our general forecast for January. To the extent that we revised the entire forecast again for the remaining year with the main focus on the summer months, because this is where we believe the bulk will start coming back in. And then we will see. 



مصرف لبنان
BANQUE DU LIBAN

Under the Patronage of
H.E. Riad Salame'
Governor of Banque Du Liban

De-Risking & Sanctions: From Awareness to Aversion Role of Financial Regulator and Banks



April 28th, 2017
Four Seasons Hotel
Beirut - Lebanon

Organized by
Al-Bank Wal-Mustathmer Group

Tel: +961 1 985411 / 2 / 3 / 4 - Mobile: +961 3 747431 - +961 81 606085 / 7

BLIND DATE AT SFEIR-SEMLER GALLERY

ART EXHIBITION OPENS SPACE FOR SEVEN NEW ARTISTS

Words by **Olga Habre**

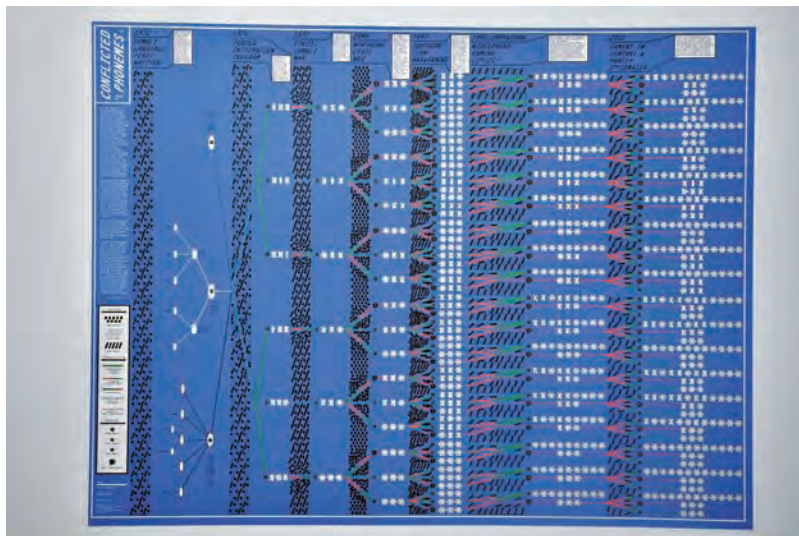
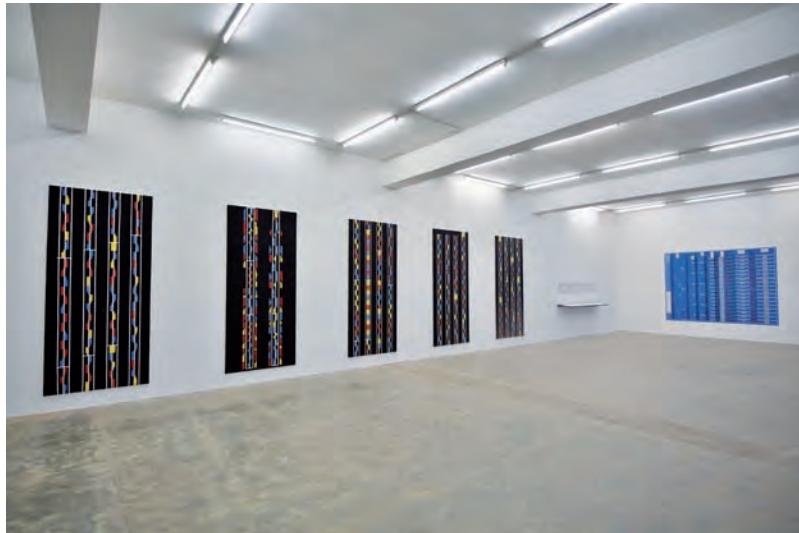


An eclectic exhibition titled "Blind Date" at the Sfeir-Semler Gallery in Karantina gave way to introductions for seven artists who had never before exhibited at the art space. Gallery Director Rana Nasser-Eddin explains, "These are artists that caught our eye. It's our blind date with the artists and their blind date with the space." Making their debut, the exhibitors (who hail from various backgrounds including Lebanese, Palestinian, Egyptian, South African and American) each brought a unique energy to the gallery. While the mostly abstract artworks could be ambiguous at first, Nasser-Eddin diligently walks visitors through the exhibition to reveal the depths of each piece and processes of the artists.

Two of the works on display are highly political. Like many contemporary artists, Lebanon's Lawrence Abu Hamdan strongly believes art and politics can't be separated, and his piece "Conflicted Phonemes" appears more like a linguistic analysis

than the traditional notion of art. Abu Hamdan uses scientific data from Dutch immigration to analyze how Somali refugees' dialects essentially determine whether their applications for asylum are accepted or rejected. In the controversial practice, refugee speech is analyzed to determine what part of their country they are from. Applicants stand a higher chance of being denied asylum if they seem to come from areas not immediately affected by conflict. The artist extracts, conceptualizes and maps language sounds, looking at their inherent politics and exploring the nature of accents. "It's a reflection of how a sound can essentially deny a right for someone," explains Nasser-Eddin.

While Abu Hamdan's work looks at science from a political perspective, Palestinian artists Basel Abbas and Ruanne Abou-Rahme, who work as a pair, consider a more psychological aspect of politics. They address their trauma as Palestinians through



their installation, which includes various elements hung on walls and others scattered on the floor as well as a documentary film. The story behind "And Yet My Mask is Powerful" is powerful indeed. It follows the pair's research journey to understand the world's oldest Neolithic masks, found on Palestinian land and seized by the Israeli state, which the artists are now reclaiming as Palestinian. The historic masks were appropriated and exhibited at The Israel Museum and around the world, although they actually come from Palestinian villages. For the installation, Abbas and Abou-Rahme use photos, plants, replicas of the masks, a poem by Adrienne Rich and even cement – symbolic in its recalling of Israeli settlements, the West Bank wall, Palestinian building customs and more. Meanwhile, the documentary looks at the towns from which the masks originate. The project thus creates a counter-narrative that reclaims these historical relics as Palestinian by sharing their story.

Storytelling is also present in emerging Egyptian artist Mohamed Monaiseer's art, which pays tribute to traditional fables, revisited in a contemporary context. A series of artworks first painted on fabric from an old bed and then embroidered replicate a traditional way of illustrating stories, evoking myths like those of Calila e Dimna. His other artwork in the exhibition features a suspended shroud-like piece that's covered in what Nasser-Eddin describes as "heightened calligraphy," a calligraphy-like script that doesn't actually have any words.

On the other hand, the work of Ania Soliman, who was born in Poland and grew up between Iraq, Egypt, Europe and the U.S, is very scientific, mostly



focusing on how the digital world is incorporated into our lives. Her piece titled "Explaining Dance to a Machine" depicts a digitized dance notation from the 1920s. To a trained dancer, the notations are recognizable patterns one follows during a dance routine, similar to how a musician reads musical notes. Her large, geometric paintings, mostly in primary colors, turn the back and forths of human movement in dance into something that is computerized and structured. Yet because the painting was done by hand it retains its humanness through its flaws.

Dineo Seshee Bopape from South Africa works across various themes in her art, including politics, race, spirituality, gender and sexuality. The elaborate structures in her installation, "Sedibeng (It Comes With the Rain)," include abstract figures and charms, as well as herbs traditionally associated with healing female health problems and a plethora of flowers found in South Africa. She manipulates the space using mirrors, light and shadows, and uses sounds and a slideshow to affect the viewer with an onslaught of sensory data.

Also looking at nature, American filmmaker and animator Joshua Mosley's work looks at the human relationship with nature through a film and bronze sculptures replicating those used in the film. Using the difficult and time-consuming stop-motion animation technique, the film stars models of French philosophers Jean-Jacque Rousseau and Blaise Pascal, as well as several animals, who discuss the human condition in a forest.

The exhibition is ongoing until March 25 at Sfeir-Semler Gallery, Karantina.



Technology... does NOT wait.



SmartEx

11-14 May 2017 / Forum de Beyrouth
www.smartexlebanon.com

Lebanon's ONLY
exhibition solely
dedicated to
TECHNOLOGY.

Book Your Space Now

+961 3 287 837

| lara@micellebanon.com

Organized By:



Media Sponsors:



In Collaboration With By:



Strategic Partner:



NADA ABOU FARHAT DELIVERS IN TAILOR-MADE "*HEBLE, EN CINQ*"

GABRIEL YAMMINE'S DARK COMEDY AT METRO AL MADINA

Words by **Olga Habre**



Lebanon's theater darling Nada Abou Farhat is pregnant in real life and on stage. When she revealed she was expecting to her longtime friend and theater veteran Gabriel Yammine a few months ago, he decided to write and direct a piece just for her. She stars in the dark comedy titled "*Heble, En Cinq*," currently on at Metro Al Madina, alongside Zeinab Assaf, Oussama El Ali and Joyce Abou Jaoude.

In the play, Abou Farhat's character, Claire, is a pregnant woman in her late 30s reflecting on her life and anxious about the future of her child. Raised around floundering marriages in a home with a combative mother and feeble father, Claire talks to the audience about her hilarious and miserable efforts to find love, and the personal struggles she's encountered in the confines of Lebanese traditions. Meanwhile, each of the other actors plays multiple

characters, switching effortlessly between the roles of Claire's family, friends, teachers and others. Ultimately, the play is an intricate, witty look at the pressures exerted by Lebanese society, especially on women.

One might find it strange that a man is so accurately writing from the perspective of a pregnant woman, and Yammine, who has written over 90 adaptations and original plays and directed close to 30, reveals that the script is entirely based on stories from real life. "I had to put myself in [a woman's] shoes and feel what she feels. I talked to Nada [Abou Farhat], my wife and friends. Life has more absurdities than people imagine. When you start expressing those ideas they become theater, and sometimes people don't even believe it," he explains.



Indeed, truth can be stranger than fiction. The play is peppered with amusing anecdotes about awkward dates and strange home remedies related to pregnancy. Perhaps it is these unusual incidents and hyperbolic characters that make the play refreshingly non-cliche, while still relatable.

Though viewers might take away messages from the story, the playwright maintains he is just using his artform to illustrate ideas, and there are no messages he wants to prescribe. "Artists use their tools, whether it's a paintbrush or a guitar, to express pain, happiness and other emotions. If [viewers] see messages, that's good, but they might see messages that we didn't even see when we were [creating the piece]," he explains.


To Yammine, art in general and theater specifically, especially when introduced at a young age, foster dreams and give rise to better, more peaceful citizens.

That's why to him, theater is a need, and he laments that the Lebanese aren't very appreciative of the art-form. Theater advocates are active in Lebanon and Yammine's own life is dedicated to it. "Theater is my life, not my work. I feel dead if I don't do this and that's why I keep going," he says, but admits it's virtually impossible to profit locally. The market is so small that even if a large percentage of the population came to see a stage production, the actual amount wouldn't add up to much. The same applies to the local film industry, although he points out a major distinction between theater and the big screen; being in the same room with actors during a live show and feeling their breath and energy connects actors and audiences in ways screens cannot.

To Yammine, it's people in positions of authority, headmasters, teachers, as well as the government that need to do more – but first they must believe that theater is important. The government could help financially, especially by opening more theatrical spaces, giving a wider range of people exposure and access to plays. But he acknowledges the government has other priorities and sadly the arts are not seen as a necessity.

Another major problem is one of perception. In Lebanon people often see arts as high-brow and classy – not for everyone, only for the educated. "This is totally wrong and that is what leads to the demise of art," Yammine says, explaining that the very people who consider themselves cultured are actually contributing to art's failure because they are making it exclusive and not giving access to the public. In order to make "*Heble, En Cinq*" more accessible, Yammine – a passionate advocate for the Arabic language – insisted on having the actors use traditional dialects from all over the country in the dialogue.

Yammine is convinced that performance art and other art forms can be a key to improving any society. "What I know is when people start to [appreciate] theater and art, things will change. And this change can happen quickly. I believe this," he states, adding, "People need to start believing that [art] is a need, like water. No one believes this yet and this is sad. I can't do more, just continue my work."

"*Heble, En Cinq*" is showing at Metro Al Madina until March 7. 

BUSINESS ESSENTIALS

Company Bulletin

The outstanding performance of **T. Gargour & Fils** in 2016 was honored at the **Mercedes-Benz Commercial Vehicles Regional Award Night** held in Dubai, UAE, on January 31, 2017.

GROHE is proud to announce that it has received the Best of the Best Iconic Award for **GROHE Blue® Home**, its innovative water system that delivers filtered and carbonated water directly from the tap.

HMD Global, the home of **Nokia** phones, unveiled a new generation of Nokia smartphones, setting a new standard in design, quality and user experience throughout the range. The highly anticipated global portfolio features three new smartphones.

Booz Allen Hamilton has been named on **Fortune Magazine's** prestigious list of "The World's Most Admired Companies" for the sixth consecutive year.

The **Brave Heart Fund** launched its annual Congenital Heart Disease Awareness Campaign in line with World Congenital Heart Disease week during a press conference at the **Le Vendôme Beirut Hotel**.

G.A. Bazerji & Sons, the official dealer of **Maserati** in Lebanon, has reported an increase in demand for the Levante following its debut in summer 2016. The model has quickly become a preferred vehicle of choice in the luxury SUV segment.

As the biggest and most versatile model in the **MINI** range and featuring the brand's most powerful engine to date, the new **MINI John Cooper Works Countryman** combines a race track feeling and useful versatility on and off the road.

Bassoul Heneiné sal, official importer of **Renault, Dacia, BMW, MINI** and **Rolls Royce** vehicles to Lebanon,

has established a long-lasting partnership with **Jouzour Loubnan**. In an active endeavour to maintain a sustainable relationship with the environment, Bassoul Heneiné has been planting a cedar tree for every vehicle sold.

HORECA Lebanon, the country's premier B2B hospitality and foodservice event, returns to Beirut for its 24th edition from April 4-7. As the key meeting place for trade professionals from across the region, the event has become a destination for firms looking to explore fresh markets, pursue new business opportunities and keep up with innovations and trends.

Flat6Labs Beirut, a partnership between **Flat6Labs** and **ArabNet**, announced the launch of **Lebanon Seed Fund**, a \$20 million early stage fund aiming to support 100 Lebanese startups over the next five years.

Officine Panerai continues its extraordinary commitment to promoting classic sailing with the 13th edition of the leading international circuit for the grandes dames of the sea, the **Panerai Classic Yachts Challenge**.

Continually catering to eclectic customers in Lebanon, **Bassoul Heneiné sal**, the official **BMW Group** importer in Lebanon, has welcomed the eagerly anticipated **BMW 5 Series** to its showroom.

Arabia Insurance Company has signed a three-year partnership agreement with **Harley Davidson®-Lebanon**, in cooperation with **Atlantis Financials** as portfolio managers, who have consulted for years on the design and evolution of the exclusive Harley-Davidson Motorcycle Insurance Policy.

The **Contemporary Art Show** showcases sculptures, paintings and

wall sculptures crafted by well-renowned international artists. The exhibition opened its doors at **Le Yacht Club Beirut** on February 16 and will stay open until March 12.

Samsung Electronics Middle East and North Africa unveiled how it is building on its heritage of innovation to reach higher for consumers during its seventh annual MENA Forum in Singapore.

Kempinski Summerland Hotel & Resort is pleased to announce the appointment of Daniele Vastolo as head of the hotel's current and future ventures. Vastolo joins Kempinski from his most recent role as group director of operations in **Nikki Beach Hotels & Resorts EMEA Ltd.**

Huawei was ranked as the world's eighth-largest company in terms of research and development spending in 2016, according to **EU Industrial R&D Investment Scoreboard**.

According to data released by leading analyst firms **Strategy Analytics** and **Counterpoint Research**, **Huawei Consumer Business Group** became the third largest smartphone manufacturer by market share, commanding 10 percent of the total global market.

International funding for Lebanon in 2016 amounted to \$1.9 billion, as shown by the funding update released by the **Office of the United Nations Resident and Humanitarian Coordinator for Lebanon**.

LGB Bank participated in the **Lebanese Architect Awards** festival dedicated to exposing leading projects executed after the year 2000.

Zain, a leading mobile and data services operator in the Middle East and Africa and **iflix**, the world's leading internet TV service for emerging

markets, announced the establishment of their joint venture, **iflix Arabia** to bring iflix's world class service to the MENA.

■ The **INSEAD Alumni Association in Lebanon** elected a new executive committee for a three-year mandate, following a general assembly held in Beirut on January 19.

■ **LUSH Lebanon**, a leading retailer of fresh handmade cosmetics, in collaboration with **Creative Space Beirut**, a fashion design school offering free creative education, jointly launched a design competition.

■ As part of its ambitious strategy to engage citizens in public affairs and refuse dynasty and corruption, **Sabaa**, the new transformative political platform in Lebanon, held a non-traditional meeting on February 19 at the Forum de Beyrouth.

■ **Nokia** won the **UAE Drones for Good Award** in the international category for showcasing the use of drones to facilitate efficient rescue operations for first responders.

■ Between February 11-14 a unique exhibition was held at the **Gstaad Palace's** Baccarat Room where selected clients could admire **de GRISOGONO** High Jewelry Collections.

■ On February 11 and 14, **Grand Hills** organized two special nights, where Valentine's Day was celebrated in style, elegance and finesse at the ballroom of the hotel, and Chez Alain, the French brasserie restaurant.

■ After 13 years of defining luxury, **Phantom VII** leaves the stage with a fittingly artful tribute to the skills of the craftspeople at the House of **Rolls-Royce**.

■ **Lions Health, Cannes Lions'** dedicated stream focused on life-changing creativity, announced June Laffey of McCann Health as the 2017 Pharma Lions Jury President and Serviceplan Health & Life's Mike Rogers as the Health & Wellness Lions Jury President.

■ In a first for Lebanon's telecommunications sector, **Alfa** has embarked on another digital transformation process in partnership with **Oracle** whereby the operator deploys the **Exadata** solutions within its systems.

■ An **Alliance for Youth**, launched by **Nestlé Middle East** last year to bring together companies and other entities that can help young people in the region enhance their skills and develop their careers, is now partnering with the UAE's **General Authority of Youth and Sports** and expanding to include several other corporations.

■ The popular Smurfs characters are encouraging children, young people and adults to make the world happier, more peaceful, equitable and healthy with a campaign launched by the **United Nations, UNICEF** and the **United Nations Foundation**.

■ The **United Nations World Food Programme** has honored Ajay Banga, president and chief executive officer of **Mastercard**, in recognition of outstanding contributions toward achieving zero hunger.

■ As part of World Class 2017 training program, **Diageo** held a seminar about the art of crafting conceptual cocktails and ingredients. The Masterclass was held at **Caprice** on February 8, and was hosted by Nikos Bakoulis & Vasilis Kyritsis from **The Clumsies**.

■ The **BMW** brand's international **Instagram** channel has broken through the 10 million followers mark, making it the most successful automotive brand on Instagram worldwide.

■ **Volvo Cars** has reported a robust 66 percent increase in operating profit in 2016 to \$1.24 billion compared to \$7.45 million in 2015, as global sales hit a new record of 534,332 cars.

■ **Ericsson, SK Telecom** and **BMW Group Korea** have broken a world

record for 5G speeds in a follow-up to the 5G trials announced in November 2016.

■ **Careem**, the region's leading car hailing app, is collaborating with **UNHCR** to support and raise awareness for programs to benefit refugees, asylum seekers and the stateless, as well as returnee and internally displaced persons in the MENA region.

■ **flydubai** has announced its Full-Year Results for 2016, reporting a profit of \$8.6 million. It has reported total revenue of \$1.37 billion, an increase of 2.4 percent compared to the same period last year.

■ Committed to providing the elderly with the care and attention they require to live their golden years comfortably, **Beit Rafqa**, a non-profit organization, has established a home for the elderly, managed by a specialized team of professionals, aiming to revolutionize elderly care services in Lebanon and the Middle East.

■ **SGBL** and **Mastercard** signed a partnership agreement with **La Sagesse Beirut Sports Club**. The signing took place in the Veterans Building of Collège La Sagesse in Achrafieh, in the presence of SGBL's executive management, Mastercard senior representatives, the management and teams of La Sagesse Club, the school and university directors, alumni and parents, as well as the media.

■ Following the success of its first branch in Hamra, **Curli-Q** opens on Bayada's main road. The opening took place on February 7, as media members, online influencers and pastry lovers gathered to witness spit baking at its finest.

■ **ICICI Securities Ltd**, a subsidiary of **ICICI Bank** and India's leading integrated financial services firm and **Saxo Bank**, the online multi-asset trading and investment specialist, announced a strategic partnership to offer Saxo's trading and investment capabilities via a digital platform to Indian investors.

BUSINESS ESSENTIALS

Company Bulletin

■ **Spinneys**, the leading supermarket retailer in the Middle East and North Africa, launched its newest initiative dedicated to distributing unsold and excess fruits and vegetables available in its stores to charities on a daily basis.

■ In line with its craftsmanship of developing premium smartphone devices that set the industry standard for elegance and performance, **Huawei Consumer Business Group** kicked off 2017 with the launch of **Huawei GR5 2017** and **Huawei GR3 2017** in Lebanon.

■ On the occasion of his 80th birthday, Mr. Jacques Saadé announced the appointment of his son Rodolphe Saadé as chief executive officer of the **CMA CGM Group**. Jacques Saadé remains chairman of the board of directors.

■ **Ericsson** opened **Mobile World Congress 2017** with three stand-out announcements featuring partners and major customers. These included network evolution toward 5G, an innovative new business model between content owners and operators to bring media to people more conveniently, and industry transformation in the transport sector.

■ **AbbVie**, a global biopharmaceutical company, held a media roundtable discussion to launch **TANGO**, a new initiative on adherence, in the presence of Professor Weinman from the UK, Professor Raymond Sayegh, the president of the **Lebanese Order of Physicians** and Dr. Jad Okais, the head of the national adherence working group.

■ Despite the depreciation of the Egyptian Pound and the Turkish Lira versus the US Dollar, **Bank Audi** recorded a strong performance in 2016. Consolidated net profits reached \$470 million, rising by 17 percent relative to 2015. Net profit growth was supported by a corol-

lary increase in consolidated assets, reaching \$44.4 billion at year end.

■ As main partner of **Photomed Lebanon**, **Byblos Bank** inaugurated a collective exhibition at its headquarters in Ashrafieh titled "Le Cinéma Italien" by renowned French photographers Richard Dumas and Alain Fleischer, and Italian photographer Sergio Strizzi.

■ At the 2017 **Geneva International Motor Show**, **BMW** will be presenting current highlights from its range of models as well as the latest advances in the field of sustainable mobility with all-electric and plug-in hybrid vehicles.

■ **BLOM Bank** PMI rose again in the first month of 2017, reflecting the slowest pace in economic contraction seen in a year.

■ **Jaguar Land Rover's** world-leading **Virtual Reality Experience** packs are now available in the Land Rover showrooms in Lebanon for customers to immerse in each new vehicle the company launches.

■ **Byblos Bank** issued the results of the **Byblos Bank Real Estate Demand Index** for the fourth quarter of 2016. The results show that the index posted a monthly average of 46.5 points, constituting an increase of 17.5 percent from 39.5 points in the third quarter of 2016 and a decline of 4.3 percent from 48.5 points in the fourth quarter of 2015.

■ **FORM Hotel**, the upscale hotel brand in **Smartotels Hospitality International's** portfolio, launched at **Gulf & Indian Ocean Hotel Investors' Summit** in the UAE.

■ **Nissan Motor Co., Ltd.** announced financial results for the nine-month period to December 31, 2016. "In the first nine months of the fiscal year, Nissan generated an operating profit of 503.2 billion yen, which represents a 6.1 percent margin on net revenues of 8.26 trillion

yen," said Carlos Ghosn, chairman and chief executive officer.

■ The **INFINITI Q60** is a premium sports coupe that combines expressive design with exhilarating performance and dynamics. Following the arrival of the 2.0T that is currently available at INFINITI partners across the region, the Middle East now counts down to the arrival of the all-new powerful **Q60 Red Sport 400**.


■ **INFINITI** recently concluded an exciting campaign that provided eight lucky motorists from the Middle East the opportunity to get behind the wheel of a real **Formula One** car in Valencia, Spain.

■ Five Lebanese non-governmental organizations received donations amounting to a total of \$53,000 from **Byblos Bank** and the suppliers of its Commercial Banking Division's 2016 end-year gifts, during a ceremony held at Byblos Bank Headquarters in Ashrafieh.

■ **Economena Analytics**, a specialized economic data provider, released its Lebanese Economic Outlook for 2017. The consensus among Lebanese economists is for growth to reach 2.5 percent in 2017, ahead of the IMF's forecast of 2 percent.

■ The **Renault-Nissan Alliance** delivered significant growth in 2016, with global sales of 9.96 million vehicles. The car group also reinforced its leadership in zero-emission vehicles with cumulative sales of nearly 425,000 electric vehicles since the introduction of the **Nissan LEAF** in 2010, followed by the **Renault ZOE**.

■ British Ambassador to Lebanon Hugo Shorter has announced £2.5 million toward a new **International Research Centre** in Lebanon.

■ **Boehringer Ingelheim**, one of the world's leading pharmaceutical companies, recently held its second **Cardio Metabolic Summit** in Lebanon. 



"UNLEASH YOUR CREATIVITY" CONTEST

VERSION 2

FERNAND HOSRI
GROUP

URMET | GROUP

urmet

Aprimatic
the convergence of innovation

ELKRON
Security for all environments

Yokis

FDI

CASTEL

simon
urmet



VOTE FOR YOUR BEST TEAM:  UNLEASH YOUR CREATIVITY CONTEST

PARTNERS:



Global Compact
Network Lebanon



sacotel
Your supplier of choice in Telecom, Security & Automation

J. WALTER THOMPSON
BEIRUT



IMPACT BBDO

SPONSORS:



MEDIA PARTNERS:

Executiv

Beirutings
www.beirutings.com

Moms & to be

PARTICIPATING UNIVERSITIES:



BUSINESS ESSENTIALS

Events

CONFERENCES

	ORGANIZERS	CONTACT	WEBSITE
LEBANON			
9-10 Mar	THE COMMON REPORTING STANDARDS FOR AUTOMATIC EXCHANGE OF INFORMATION FOR TAX PURPOSES Union of Arab Banks	+961 1 377800; a.majed@uabonline.net	www.uabonline.org
22 Mar	BUILD IT GREEN e-Ecosolutions	+961 9 856 565; gtegho@eecosolutions.com	www.eecosolutions.com
27-31 Mar	THE THIRTY SECOND ACM SYMPOSIUM ON APPLIED COMPUTING LAU	+961 1 786461; hhaddad@kennesaw.edu	www.lau.edu.lb
28 Apr	DE – RISKING & SANCTIONS : FROM AWARENESS TO AVERSION - ROLE OF FINANCIAL REGULATOR AND BANKS Al Bank Wal Mustathmer Group	+961 1 985 411; conference@magagroup.com	www.magagroup.com
9-10 May	OIL & GAS SUMMIT Global Event Partners	+ 44 1737 784956; -	athompsett@gep-events.com
12-14 May	BEIRUT INTERNATIONAL PROPERTY FAIR Promoteam	+961 1 339 050; promoteam-ltd.com	www.promoteam-ltd.com
23-24 May	FINANCING AND DEVELOPMENT OF REAL ESTATE IN THE ARAB COUNTRIES Union of Arab Banks	+961 1 377 800; a.majed@uabonline.net	www.uabonline.org
DUBAI			
20-21 Mar	THIRD ANNUAL RETROFITTECH UAE Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
27-28 Mar	2ND STARCH WORLD DUBAI ADM	+65 6345 7322; cynthia@cmtsp.com.sg	www.cmtevents.com
3-4 Apr	ATD MIDDLE EAST CONFERENCE AND EXHIBITION Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
4-5 Apr	TWELFTH MIDDLE EAST RETAIL BANKING CONFEX Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
10-11 Apr	THE FAHR INTERNATIONAL CONFERENCE Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
11-12 Apr	TWELFTH ANNUAL WORLD TAKAFUL CONFERENCE Middle East Global Advisors	+971 4 343 1200; info@megaevents.net	www.meglobaladvisors.com
18-19 Apr	DISTRICT COOLING STAKEHOLDERS SUMMIT Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
19-20 Apr	NEXTGEN PARKING MANAGEMENT SUMMIT Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
25-26 Apr	SUPPLY CHAIN ME STRATEGY SUMMIT Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
25-27 Apr	ARABIAN HOTEL INVESTMENT Meed Events	+971 4818 0200; events@meed.com	www.meed.com
30 Apr - 1 May	TWELFTH HUMAN CAPITAL FORUM MENA Naseba	+971 4 367 1376; prachid@naseba.com	www.naseba.com
30 Apr - 2 May	5G MENA Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
1-2 May	CLOUD MENA Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
7-11 May	STRATEGY EXECUTION AND PERFORMANCE FORUM Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
15-16 May	DIGITAL TRANSFORMATION TELECOMS SUMMIT Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
19-21 May	WORLD ECONOMIC FORUM ON THE MIDDLE EAST AND NORTH AFRICA World Economic Forum	+41 22 869 1212; contact@weforum.org	www.weforum.org
22-23 May	MIDDLE EAST INVESTMENT SUMMIT Terrapinn Middle East	+971 0 444 2500; enquiry.me@terrapinn.com	www.terrapinn.com
ABU DHABI			
20-21 Mar	GLOBAL FORUM FOR INNOVATIONS IN AGRICULTURE Media Generations Exhibitions	+44 14 23 524 545; info@mediageneration.co.uk	www.mediageneration.co.uk
1-2 May	FUTURE DRAINAGE AND STORMWATER NETWORKS Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
3-5 May	FIELD SERVICE MANAGEMENT & WORKFORCE MOBILITY Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events

	ORGANIZERS	CONTACT	WEBSITE
QATAR			
12-20 Mar	FUTURE BIM IMPLEMENTATION Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
27-28 Mar	EDEX QATAR Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
10-11 Apr	SECOND ANNUAL SMART PARKING QATAR Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
8-9 May	FOURTH ANNUAL LIGHTINGTECH QATAR Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
15-16 May	INDUSTRIAL CONTROL SYSTEMS Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
SAUDI ARABIA			
6-7 Mar	KINGDOM EDUCATION INNOVATION 2017 Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
13-14 Mar	SMART PARKING Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
14-15 Mar	KINGDOM HUMAN ASSET MANAGEMENT Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
9-11 Apr	ROTATING EQUIPMENT RELIABILITY & MAINTENANCE Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
18-19 Apr	KINGDOM CYBER SECURITY Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
24-26 Apr	KINGDOM PROCESS SAFETY 2017 Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
8-9 May	EIGHTH KINGDOM SMART MEETING Naseba	+971 4 367 1376; prachid@naseba.com	www.naseba.com
8-11 May	THE KINGDOM CUSTOMER EXPERIENCE Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
15-17 May	PLANT SHUTDOWN AND TURNAROUND 2017 Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
BAHRAIN			
6-9 Mar	MIDDLE EAST OIL SHOW Arabian Exhibition Management	+973 17550033; fawzi@aeminfo.com.bh	www.aemallworld.com
11-12 Apr	MIDDLE EAST HEAVY OIL CONGRESS dmg World Media Dubai	+971 4 331 9688; dmga@emirates.net.ae	www.dmgeventsme.com
26-27 Apr	KINGDOM WASTE MANAGEMENT AND RECYCLING Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
EGYPT			
25-27 Mar	THE ARAB BANKING CONFERENCE FOR 2017 Union of Arab Banks	+ 961 1 377800; a.majed@uabonline.net	www.uabonline.org
8-9 Apr	THIRD EGYPT INVESTMENT FORUM Al Iktissad Wal Aamal	+961 1 780 200; forums@iktissad.com	www.iktissadevents.com
26-27 Apr	CYBER SECURITY NORTH AFRICA SUMMIT Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events
KUWAIT			
4-5 Apr	KUWAIT FINANCIAL FORUM Al Iktissad Wal Aamal	+961 1 780 200; forums@iktissad.com	www.iktissadevents.com
JORDAN			
15-18 May	THE FOURTEENTH INTERNATIONAL MACHINES AND ELECTRO-MECHANICAL EXHIBITION Golden Gate	+962 565 8501; goldgate@go.com.jo	www.jordan-fairs.com
19-21 May	WORLD ECONOMIC FORUM ON THE MIDDLE EAST AND NORTH AFRICA 2017 World Economic Forum	+41 22 869 1449; contact@weforum.org	www.weforum.org
OMAN			
4-6 Apr	OMAN DOWNSTREAM EXHIBITION AND CONFERENCE Golden Gate	+971 4 327 7733; hazel.nocellado@omanexpo.com omanexpo@omantel.net	
15-17 May	BUSINESS CONTINUITY & EMERGENCY RESPONSE Fleming Gulf	+971 4 609 1555; info@fleminggulf.com	www.fleming.events

BUSINESS ESSENTIALS

Events

EXHIBITIONS

	ORGANIZERS	CONTACT	WEBSITE
LEBANON			
4-7 Apr	HORECA LEBANON Hospitality Services	+961 1 480081; info@hospitalityservices.com.lb	www.hospitalityservices.com.lb
11-14 May	SMARTX INFORMATION TECHNOLOGY AND MICE	+961 1 384791; lara@miclebanon.com	www.smartxlebanon.com
12-14 May	BEIRUT INTERNATIONAL PROPERTY FAIR Promoteam	+961 1 339 050; sm@promoteam-ltd.com	www.promoteam-ltd.com
16-19 May	PROJECT LEBANON IFP	+961 5 959 111; info@ifpexpo.com	www.ifpexpo.com
23-27 May	GARDEN SHOW AND SPRING FESTIVAL Hospitality Services	+961 1 480081; info@hospitalityservices.com.lb	www.hospitalityservices.com.lb
23-28 May	BEIRUT BOAT IFP	+961 5 959 111; info@ifpexpo.com	www.ifpexpo.com
DUBAI			
7-8 Mar	MIDDLE EAST RAIL 2017 Terrapinn Middle East	+971 14440 2500; enquiry.me@terrapinn.com	www.terrapinn.com
13-15 Apr	GULF EDUCATION AND TRAINING EXHIBITION International Conferences and Exhibitions	+971 4 335 5001; info@icedxb.com	www.icedxb.com
1-2 May	SEAMLESS MIDDLE EAST 2017 Terrapinn Middle East	+971 14440 2500; enquiry.me@terrapinn.com	www.terrapinn.com
22-25 May	INDEX DESIGN SERIES dmg World Media Dubai	+971 4 331 9688; dmg@emirates.net.ae	www.dmgeventsme.com
ABU DHABI			
18-20 Apr	CITYSCAPE ABU DHABI Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
SAUDI ARABIA			
6-7 Mar	LIGHTING TECH Advanced Conferences and Meetings	+971 4 361 4001; opportunities@acm-events.com	www.acm-events.com
27-30 Mar	THE BIG 5 SAUDI dmg World Media Dubai	+971 4 331 9688; dmg@emirates.net.ae	www.dmgeventsme.com
4-6 Apr	THE HOTEL SHOW SAUDI ARABIA dmg World Media Dubai	+971 4 331 9688; dmg@emirates.net.ae	www.dmgeventsme.com
25-26 Apr	FUTURE LANDSCAPE AND PUBLIC REALM IFP	+961 5 959 111; info@ifpexpo.com	www.ifpexpo.com
BAHRAIN			
7-9 Mar	MIDDLE EAST OIL SHOW Arabian Exhibition Management	+973 17550033; fawzi@aeminfo.com.bh	www.aemallworld.com
11-12 Apr	MIDDLE EAST HEAVY OIL CONGRESS dmg World Media Dubai	+971 4 331 9688; dmg@emirates.net.ae	www.dmgeventsme.com
25-27 Apr	GULF PROPERTY SHOW Hilal Conferences and Exhibitions	+973 17 299123; info@hilalce.com	www.hilalce.com
EGYPT			
9-11 Mar	PROJECT EGYPT IFP	+961 5 959 111; info@ifpexpo.com	www.ifpexpo.com
15-19 Mar	HEAVY DUTY - CAIRO INTERNATIONAL MOTOR SHOW ACG - ITF	+202 7538 401; info@acg-itf.com	www.acg-itf.com
31 Mar - 3 Apr	CITYSCAPE EGYPT Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com

	ORGANIZERS	CONTACT	WEBSITE
18-19 Apr	ARWADEX Exicon	+961 1 821 421; ghada@exicon-intl.com	www.exicon-intl.com
22-24 Apr	FOOD AFRICA IFP	+961 5 959 111; info@ifpexpo.com	www.ifpexpo.com
11-14 May	USED MACHINERY EXPO USED	-; usedexpo-eg.com	www.ifg-eg.com
QATAR			
13-15 Mar	CITYSCAPE QATAR Informa Middle East	+971 4 336 5161; info-mea@informa.com	www.informa-mea.com
22-25 Mar	AGRITEQ IFP	+961 5 959 111; info@ifpexpo.com	www.ifpexpo.com
2-4 Apr	FOODEX QATAR Al Fajer Information and Services	+971 50 640 3275; rupa@alfajer.net	www.alfajer.net
8-11 May	PROJECT QATAR IFP	+961 5 959 111; info@ifpexpo.com	www.ifpexpo.com
KUWAIT			
19-22 Apr	JEWELLERY ARABIA KUWAIT 2017 Arabian Exhibition Management	+973 17550033; fawzi@aeminfo.com.bh	www.aemallworld.com
OMAN			
1-28 Apr	COMEX-IT,TELECOM & TECHNOLOGY EXHIBITION Oman Convention, Muscat	-; info@oite.com	www.oite.com
18-20 Apr	OMPEX 2017 Oman Convention, Muscat	-; info@oite.com	www.oite.com

www.executive-bulletin.com

Your daily update on all corporate news and
announcements from all the region's countries and sectors

Executive

LAST WORD

By Talal F. Salman

Lebanon's national budget

A strategic instrument for adequate policymaking

Lebanon has been operating for the last 12 years without an approved budget.

Now that there is a real opportunity for an agreement at the Council of Ministers over the accounts pending since 2005, the 2017 budget proposed by the finance minister and potentially the salary scale with its commensurate revenue measures, it would be good to remind ourselves of the importance of having a budget in the first place.

The fact that we don't have an approved budget by the Council of Ministers and subsequently, by the Parliament, does not mean that the ministers of finance have not done their job over the years. On the contrary, Ali Hassan Khalil, the current minister of finance, has produced a national budget in each of the past three years within the legal deadlines. However, any budget, if not approved, will remain idle and spending will

occur based on ad-hoc needs as opposed to following a strategic vision.


For instance, the three major expenditure items for the Lebanese government are: wages, interest on debt and transfers to cover the deficit of the electricity company. Any attempts to improve productivity of public servants and the collection of revenues would require policy adjustment to the structure of wages, which in turn would need to be part of an approved budget.

Any strategic plan to reverse the trend of debt and reduce interest costs would require new revenue and expenditure measures to improve the primary fiscal surplus. In addition, any serious reform to the electricity sector would require capital expenditures to revamp and expand the asset base, both of which would again need to be part of an approved budget.

National budgets play two major

roles. The first is to act as a policy tool for governments to design their tax policies, expenditure plans and funding needs according to a clear mid-term economic strategy. The second is to serve as an accounting tool to be used by the central government to guide, compile and oversee spending plans of ministries and government agencies, and ensure they fit within the general government policy framework.

Most developed countries and some developing ones now draft their annual budgets with a multi-year perspective, through the preparation of a medium-term revenue and expenditure framework that takes borrowing constraints into consideration. A comprehensive budget would take into account: the needs of different sectors in the economy, the sustainability of spending in the medium-term and macroeconomic constraints such as inflation, borrowing costs and limits, outstanding government debt and expected growth. The budget also needs to be realistic and achievable so that the government would be able to use it as a building block year after year toward a medium-term vision of the economy, public finances and public debt.

The multi-year approach has been pioneered by countries such as Australia, Denmark and the Netherlands. A combination of expenditure ceilings, a comprehensive budget approach, quality information and technical capabilities have resulted in improved fiscal discipline and understanding of revenue constraints, a better working relationship amongst ministries and government agencies, and the efficient allocation of resources for development purposes. 

Talal F. Salman, Director of UNDP Fiscal Reform Project

THE MAJOR BENEFITS OF LEBANON GETTING ITS NATIONAL BUDGET BACK ON TRACK ARE:

- A clear government strategy that guides policymakers across all ministries and government agencies, resulting in improved policymaking with objectives that target the most pressing economic, social and infrastructural needs.
- Improved visibility on fiscal and economic performance to better anticipate the policy requirements of future years.
- Decreased discretionary expenditures and less need for large extra-budgetary funds, which results in better control and transparency of overall spending.
- Improved perception of credit rating agencies, multilateral stakeholders and international investors in Lebanese assets, leading to more credibility, cheaper borrowing, and increased investment in the economy and in government bonds.
- Support for the government's mission to reach fiscal consolidation and a reversal of the trends in chronic deficits and high debt.
- Normalization of the policymaking function of the treasury in anticipation of major changes in the structure of the Lebanese economy ahead of the exploration of petroleum resources.

DOWNTOWN HAS ITS **BOARDROOM** NOW

LE GRAY
BEIRUT



Tel +961 1 971111

Martyrs' Square

Beirut, Lebanon

legray.com

A CAMPBELLGRAY HOTEL


THE LEADING HOTELS
OF THE WORLD®



2 in 1 **COMBO CARD**

Dual Use for you to Choose

Choosing between your credit and debit accounts is now easier with the new 2 in 1 Combo Card by Mastercard. Combining credit and debit in a single card, you simply select the account of your choice at points of sale and ATMs. Protected by a unified PIN code, the Combo Card comes with exclusive benefits: a complimentary Priority Pass membership card offering access to over 950 airport lounges worldwide, a free supplementary card for the first year, free online and mobile banking allowing cardholders to access their accounts on-the-go with free enrollment in Creditbank loyalty program and a welcome gift of 50 points.

*Credit & Debit
combined for your convenience*