
اتحاد المصارف العربية
Union of Arab Banks
بالتعاون مع:
مصرف قطر المركزي
Qatar Central Bank
ينظم ورشة عمل مصرفية متخصّصة حول موضوع:
CYBER SECURITY
القرصنة الإلكترونية وأمن المعلوماتية في المصارف
6 - 8 تشرين الثاني / نوفمبر 2016
الدوحة / دولة قطر

## الـخـلـفـيـة

يعتبر أمن المعلوماتية عنصراً حيوياً من عناصر سلامة العمل المصرفي. ولقد باتت هذه المسألة تشكل هاجساً مقلقاً للمهتمين بسلامة العمليات المصرفية نتيجة للتطور الهائل في التقنيات الإلكترونية الحديثة والإختراعات والإبتكارات المرافقة لها والتي غزت عالم الأعمال في العقود القليلة الماضية وما رافقها من تطبيقات في الصناعة المصرفية، الأمر الذي أفسح المجال أمام إبتكار أساليب جديدة من عمليات الغش والتزوير والاحتيال تعتمد بشكل أساسي على إستخدام تكنولوجيا المعلوماتية (IT)، وبات على العاملين في هذا الحقل من حقول المهنة المصرفية إبتكار أساليب الكشف والمواجهة اللازمة والتي تتماشى مع هذا التطور التكنولوجي غير المسبوق.

إن نجاح القطاع المالي في قطر يظهر جلياً في كافة المحافل الإقليمية والدولية، وقد تمكن هذا القطاع من التغلب على الكثير من المصاعب مما نتج عن ذلك نمو ملحوظ في المصارف القطرية مقارنةً مع الدول الأخرى. ولكن من الناحية الأمنية، تساهم حالة الإزدهار التي يعيشها القطاع المصرفي القطري في جذب المجرمين اللذين يسعون إلى إستغلال هذا النمو في حجم هذا القطاع للقيام بعملياتهم الإجرامية.

إنطلاقاً من هذا الواقع، ونظراً لأهمية هذا الموضوع بالنسبة للعاملين في أمن المعلوماتية في المصارف ينظم إتحاد المصارف العربية هذه الورشة بالتعاون مع مصرف قطر المركزي التي سوف تتناول أحدث التكنولوجيات والاجراءات والوسائل التي يجب إتخاذها لحماية نظم المعلومات في المؤسسات المالية والمصرفية والإقتصادية، وضمان سير التعاملات الإلكترونية وإستمراريتها في بيئة تكنولوجية آمنة، ورفع كفاءة المؤسسة في مواجهة التحديات والأخطار التي يمكن أن تواجهها - في حال إغفال توفير التقنيات الوقائية، وسبل تأمين الحماية اللازمة ضد القرصنة ومحاولات الإختراق الإلكتروني- والتي تهدد الإستقرار الأمني المعلوماتي للمؤسسة وما يترتب على ذلك من خسائر فادحة سواء مالية أو معنوية.

## الاهداف :

**سوف يتمكن المشارك في هذه الورشة من التعرف بعمق على:**

- التهديدات الإلكترونية الجديدة وتأثيرها على قطاع المصارف.
- أهمية المخاطر التي قد تنجم عن الحوادث الأمنية أو القرصنة الإلكترونية أو جرائم الحاسوب التي تستهدف أمن تكنولوجيا المعلومات في سائر المؤسسات المصرفية والمالية، لتبقى هدفاً للعاملين عليها والتنبه والوعي لمثل هذه المخاطر.
- ضمان تحسين كفاءة وفعالية عمليات المؤسسة المرتبطة بتكنولوجيا المعلومات.
- خلق وإدارة نظام عمليات أمنية ووقائية بهدف حماية تكنولوجيا المعلومات وكيفية الدفاع والردع ضد الهجمات الإلكترونية.
- التعرف على مدى كفاية الضوابط وكفاءتها للعمليات المالية والمصرفية لمعرفة مدى قوة الاجراءات الأمنية المتبعة ومعرفة نقاط الضعف والتهديدات وأنواع الهجمات وأساليبها التقنية ومعرفة الجهات التي تسعى لذلك ومصادرها.
- التوافق مع القوانين والتشريعات، ومتطلبات البنوك المركزية العربية، والتوجيهات المختصة بالقواعد التنظيمية لأمان تكنولوجيا المعلومات في المصارف والمؤسسات المالية ومؤسسات الوساطة المالية.

## المشاركون المستهدفون :

- مدراء وكوادر دوائر التشغيل وخدمة العملاء والإمتثال والتدقيق الداخلي.
- العاملون في إدارات تكنولوجيا المعلومات في المصارف.
- العاملون في إدارات أمن المعلوماتية في المصارف.
- العاملون في الإدارات القانونية في المصارف والمؤسسات المالية ومؤسسات الوساطة المالية.

## المواضيع الرئيسية والبرنامج الزمني:

### اليوم الأول:

**الحقيقة المرّة**

- الأخبار الأمنية
- المخاطر الجديدة ونقاط الضعف:
  - » عصر القراصنة الإلكترونيين
  - » البيئة المعقدة
  - » التكنولوجيا الجديدة
  - » التركيز المحدود
  - » الخبرة المحدودة
  - » وكلاء التهديد
- تحليل الهجوم الإلكتروني

### اليوم الثاني:

**الضوابط الإدارية التشغيلية**

- معيار أمن المعلومات ISO 27001:2013
  - » تعريف ISO 27001/27002
  - » المقاربة
  - » تعريف ISMS
  - » التوثيق
  - » الأهداف الرقابية
  - » العملية اللازمة للإستحصال على الشهادة

**PCI-DSS**

- تعريف PCI DSS
- المتطلبات
- ISO 27005 إدارة مخاطر أمن المعلومات
  - » تعريف
  - » الأهداف
  - » العملية اللازمة لإجراء تقييم للمخاطر

### اليوم الثالث:

**التحكم التقني والأدوات الأمنية**

- جدار الحماية
- نظام منع الإختراق
- البرامج المضادة للفيروسات
- Sandboxing
- منع فقدان البيانات
- SIEM
- المسح: الشبكة، النظام وقاعدة البيانات
- إدارة التعديلات

**سوف تعرض حالات عملية وتطبيقية خلال الورشة**

## المحاضر:

### الأستاذ طوني شبلي:

**• مدير إدارة تكنولوجيا المعلومات وأمن المعلوماتية لدى مجموعة الإعتماد اللبناني - لبنان. إنضم للمجموعة في عام 2008 حيث حقق عدداً من النجاحات في مجال أمن المعلومات وقام بتصميم برنامج أمني مبني على مبادىء ISO 27001 and PCI-DSS والذي ساعد من خلاله المصرف في الإمتثال لتعاميم لجنة الرقابة على المصارف وحقق العديد من النجاحات في مجال أمن المعلوماتية، حيث أنجز مشاريع Compliance PCI – DSS و CCM Netcommerce، وكذلك IPN لبنك الإعتماد اللبناني والشركات الشقيقة .**

**• السيد شبلي حائز على الشهادات التالية:**

CISSP (since 2001) - PECB ISO/IEC 27001 Lead Auditor - PECB ISO/IEC 27005 Risk Manager - PECB Certified Trainer –

**• لفترة عقد من الزمن، قدم السيد شبلي خدمات في أمن المعلومات كجزء من Deloitte و Secor/Computel Group في منطقة الشرق الأوسط (الإمارات العربية المتحدة، لبنان، الأردن، تركيا والمملكة العربية السعودية).**

**• قام السيد طوني أيضاً بتطوير العديد من السياسات والإجراءات الأمنية لمنظمات كبرى في منطقة الشرق الأوسط بالإضافة إلى التطبيق الشامل لتلك الإجراءات. وشارك أيضاً كمتحدث في العديد من المؤتمرات والنشاطات التدريبية وساهم في تطوير التوعية الأمنية في السوق الشرق أوسطي.**

**• متحدث ومحاضر / مدرب في العديد من المؤتمرات الدولية، ومحاضر معتمد لدى إتحاد المصارف العربية وبعض المنظمات الدولية.**

## رسم الإشتراك

1100 $ للمصارف الأعضاء .
1350 $ للمصارف غير الأعضاء .
يتضمن رسم الإشتراك حضور أعمال الورشة واستلام أوراق العمل، والضيافة وغداء يومي للسادة المشاركين.

## البرنامج الزمني ولغة الورشة

التسجيل: في اليوم الأول من 8:00 - 9:00 صباحاً.
البرنامج الزمني: من الساعة 9:00 - 15:00.
لغة الورشة: **اللغة العربية والإنكليزيّة**

## طريقة الدفع

بشيك مصرفي مسحوب على نيويورك لأمر إتحاد المصارف العربية، أو بحوالة لحساب الإتحاد رقم 0331-082305/510-8 طرف البنك العربي، فرع رياض الصلح بيروت/لبنان، أو نقداً عند حضوركم الورشة.
للإشتراك والدفع بواسطة بطاقة الإئتمان يرجى زيارة موقعنا على شبكة الإنترنت: www.uabonline.org

Or by transfer to our account at: Arab Bank - Beirut - Lebanon Swift code (ARABLBBX)
Riyad El solh Br. Account No:0331-082305-510
Through Wells Fargo - Sanfrancisco – USA Swift code (PNBP US 3N NYC)
Iban: LB42 0005 0000 0000 3310 8230 5510

يرجى إرسال أسماء السادة المشاركين إلى العناوين المبينة أدناه:


**إتحاد المصارف العربية**

**المركز الرئيسي:**

- **بيروت - الجمهورية اللبنانية : ص.ب.** 11-2416 **رياض الصلح** 1107 2110
- **هاتف:** 7/5/881364-1-961+ 377800-1-961+
- **فاكس:** 364955-1-961+ 364952-1-961+
e-mails: training@uabonline.org Booking online: www.uabonline.org

**المكاتب الإقليمية:**

- **الخرطوم - جمهورية السودان: ص.ب.** (12597) - **هاتف وفاكس:** 249-183-781742+
- **عمّان - المملكة الأردنية الهاشمية : ص.ب.** (942100) **عمّان** (11194) **الأردن** - **هاتف:** 962-6-5677234/5+
- **فاكس:** 962-6-5688854+
- **القاهرة - جمهورية مصر العربية:** 19 **شارع البطل أحمد عبد العزيز -الدور الثاني، شقة** (11) **- المهندسين - الجيزة**
- **هاتف:** 202-33034442+ 202-33023762+ - **فاكس:** 202-33440297+
- **تونس - الجمهورية التونسية: شارع خير الدين باشا- حي النسيم – ص.ب.** 1002/45 **تونس البلفيدير - مبنى البيت المصرفي**
- **هاتف:** 216-71-908083+ - **فاكس:** 216-71-951419+

## PARTICIPATION FEES:

1100 $ for UAB members
1350 $ for Non-UAB members
fees include attending the workshop, receiving the material, refreshments and a daily lunch,

## SCHEDULE AND LANGUAGE:

Registration: the first day from 8am to 9 am.
Schedule : from 9:00 am to 15:00 pm daily.
Workshop languages: Arabic and English.

## MEANS OF PAYMENT

A Bankers check shall be drawn at New York to the order of the Union of Arab Banks, or by transfer to the account of the UAB No: 82305-510/8 Arab Bank - Beirut Lebanon.
For online registration & payment, please visit our website :www.uabonline.org

Or by transfer to our account at: Arab Bank - Beirut - Lebanon Swift code (ARABLBBX)
Riyad El solh Br. Account No:0331-082305-510
Through Wells Fargo - Sanfrancisco – USA Swift code (PNBP US 3N NYC)
Iban: LB42 0005 0000 0000 3310 8230 5510
Beneficiary: Union of Arab Banks

For any additional information or inquiries regarding this event, please contact us at the following addresses:

**Union of Arab Banks**
**Headquarters:**
**Beirut - Lebanon:** P.O. Box: 11-2416 Riad El-Solh 1107 2210
Tel: +961-1-377800 - +961-1-364881 - 5 - 7 Fax: +961-1-364952 - +961-1-364955
Email: uab@uabonline.org
e–mails: training@uabonline.org Booking online: www.uabonline.org

**Regional Offices:**
**Cairo - Egypt :** 19 Al-Batal Ahmed Abdelaziz Str. 2nd Floor - Apt (11) - Mohandissine - Giza
Tel: +202-33023762/+202-33034442 Fax: +202-33440297
Email: uab-egypt@uabonline.org

**Amman - Jordan:** P.O. Box: (942100) Amman (11194) Jordan
Tel: +962-6-5677234/5 Fax: +962-6-5688854
Email:uab-jordan@uabonline.org

**Khartoum - Sudan:** P.O. Box: (12597) Khartoum Telefax: +249-183-781742

**Tunisia:** P.O.BOX:1002/45 Tunis Tel: +216 71 908083 Fax: +216 71 951 419

## TOPICS AND AGENDA

### DAY 1:

**UGLY TRUTH**

- Security News
- New threats and vulnerabilities
  - » Hackers age
  - » Environmetal complexity
  - » New technology
  - » Limited focus
  - » Limited expertise
  - » Threat agents
- Anatomy of an attack

### DAY 2:

**MANAGEMENT OPERATIONAL CONTROLS**

- Information Security Standard ISO 27001:2013
  - » Introduction to ISO 27001/27002
  - » Approach
  - » Introduction to ISMS
  - » Documentation
  - » Clause & Control Objectives
  - » Process needed to achieve certfication

**PCI-DSS**

- Introduction to PCI DSS
- 12 Requirements

### DAY 3:

**ISO 27005 INFORMATION SECURITY RISK MANAGEMENT**

- Introduction
- Objectives
- Process to conduct risk assessment

**TECHNICAL CONTROL SECURITY TOOLS**

- Firewalls
- Intrusion Prevention Systems
- Anti-virus
- Sandboxing
- Data Loss Prevention
- SIEM
- Scanner: network, system and database
- Patch Management
- And others.

**CASE STUDIES WILL BE APPLIED DURING THE COURSE**

## THE TARGETED ATTENDEES

**THIS WORKSHOP IS INTENDED TO:**

- Managers and cadres operating departments, customer service , compliance and internal audit.
- IT and Security staff members at any position who wish to enrich their knowledge in information security and increase the protection of their information assets.
- Workers in the legal departments of banks and financial institutions and financial intermediaries.

## SPEAKERS:

## MR. TONY CHEBLY

Tony presently is heading the Information Security Department at Credit Libanais Group. He joined the group since September 2008 where he accomplished several success stories .
He designed a security program based on ISO 27001 and PCI-DSS standards which helped the Bank complying to Banking Control Commission circulars.
He accomplished several success stories among them achieving PCI – DSS compliance for Credit Libanais sister companies: CCM, Netcommerce and IPN.
He designed a security program based on ISO 27001 and PCI – DSS standards which helped the Bank complying to banking Control Commission circulars (222, 272 and others) and satisfying the external and internal IT auditors requirements.
Tony has achieved the following certifications:

- CISSP (since 2001) - PECB ISO/IEC 27001 Lead Auditor - PECB ISO/IEC 27005 Risk Manager - PECB Certified Trainer

For a decade, Mr. Tony performed many information security services, as part of Deloitte and Secor/Computel group, in the Middle East region (UAE, Lebanon, Jordan, Turkey, and KSA).
He developed security policies and procedures (based on BS7799) for large organisations in the Middle East and backed that up with full implementations of the standard.
He is featured as speaker at several conferences, contributed in developing the security awareness for the Middle East market.
Mrs. Chebly is an accredited speaker / trainer at the Union of Arab Banks, and speaker in many international conferences and forums.

## BACKGROUND:

IT security is a vital component of the banking safety elements. The issue has become a major concern for those interested in the safety of banking operations as a result of the tremendous development of modern electronic technologies and inventions and innovations associated with them, which invaded the business world in the past few decades and the accompanying applications in the banking industry, which has opened the way to create new methods of cheating and fraud the fraud relies primarily on the use of information technology (IT), and a pat on the workers in this field from the fields of banking business innovation disclosure necessary and which are in line with this technological development is unprecedented and confrontational methods.

The success of the Qatary financial industry is constantly appearing in the international media and events- in fact the banking industry beat the odds since Qatary banks are still growing strongly compared to other countries; unfortunately, for the security profession all this good news turns into bad news because Qatary's prosperity acts as a magnet for criminals who previously ignored us. Indeed when businesses are booming and flourishing, criminal's interest will be raised simply for the following reasons: money, information, competition and the list goes on. As you may know, the best approach to achieve the criminals' goal is simply through Cyber threats.

With this in mind, the Union of Arab Banks is pleased to conduct a workshop in Doha in collaboration with Central Bank of Qatar, entitled: "Cyber Security in Banks".

This workshop is addressed to the latest technologies and procedures and the means to be taken to protect the information systems in the financial, banking and economic institutions, and to ensure that the conduct of electronic transactions and continuity in a safe technological environment, and raising enterprise efficiency in the face of the challenges and dangers that can be encountered - in the event of the omission of the provision of preventive techniques, and repel securing the necessary protection against piracy and attempts to hack electronics that the security and stability of the institution and the consequent heavy losses both financial and moral.

## OBJECTIVES

### The objectives of this workshop are to acquaint the attendees to:

- Highlighting the importance of risk that may result from security incidents or electronic hacking or computer crime aimed at IT security in the rest of the banking and financial institutions, to keep the target for the workers and pay attention and awareness of such risks.
- The recent cyber threats against the banking industry
- Learn about the techniques used by Hackers
- Ensure improved efficiency and effectiveness of the institution's operations related to information technology.
- Create and conduct preventive security operations in order to protect information technology and how to defense and deterrence against cyber attacks.
- Identify how efficient controls and efficiency of the financial and banking operations to see how strong security measures in place and know the weaknesses and threats and the types of attacks and technical methods and knowledge of those who seek for it and their sources.
- Compliance with laws and regulations, and the requirements of Arab central banks, competent regulatory rules and guidelines for information security working in banks and financial institutions and financial intermediaries' technology.

اتحاد المصارف العربية
Union of Arab Banks

in collaboration with:

مصرف قطر المركزي
Qatar Central Bank

**ORGANIZES A SPECIALIZED BANKING WORKSHOP ENTITLED:**


# CYBER & IT SECURITY IN BANKS

**6 - 8 NOVEMBER 2016**

**DOHA / QATAR**