الجرائم الالكترونية من خلال مؤشرات عالمية وآثارها على المؤسسات

Electronic crimes through global indicators and their impact on institutions

د. وهيبة عبد الرحيم
أستاذ محاضر صنف "أ"
معهد العلوم الاقتصادية
المركز الجامعي بتمنراست،
الجزائر
wahibawahiba80@yahoo.fr

د. أمين بن سعيد[1]
أستاذ محاضر صنف "أ"
كلية العلوم الاقتصادية والتجارية
وعلوم التسيير
جامعة الجزائر 3، الجزائر
Benamineee@hotmail.fr

د. نادية عبد الرحيم
أستاذ محاضر صنف "أ"
كلية العلوم الاقتصادية
والتجارية وعلوم التسيير
جامعة الجزائر 3، الجزائر
nadia.abd16@yahoo.com

تاريخ الاستلام: 2018/06/09
تاريخ القبول: 2018/11/01

ملخص:

للجرائم الالكترونية آثارا سلبية على الاقتصاد وبشكل مباشر على الشركات خاصة المؤسسات المصرفية حيث أنها الأكثر عرضة لهذا النوع من الجرائم، ويرجع ذلك كون النقود هي السلعة التي تتعامل بها هذه المؤسسات، وقد سببت الجرائم الالكترونية خسائر مالية فادحة سنويا لهذه الشركات بالإضافة إلى خسارة الثقة التي يضعها فيها الزبائن. وهكذا أصبحت الجرائم الالكترونية حجر عقبة أمام نمو وازدهار المؤسسات وجذب أكبر عدد ممكن من الزبائن وكسب ثقتهم، وتفاقمت المشكلة أكثر فأكثر على الرغم من الأساليب الأمنية المتطورة وأحدث التقنيات المستخدمة، والتقارير العالمية التي تصدرها الهيئات المتخصصة توضح حجم المشكلة في مختلف أنحاء العالم وتؤكد أن الولايات المتحدة هي الأكثر تضررا بشكل مستمر.

كلمات مفتاحية: الجرائم الالكترونية؛ آثار الجرائم الالكترونية؛ أرقام وإحصائيات

تصنيف JEL: L86, M15, O32

Abstract:

The electronic crimes have a negative impact on the economy and directly on companies, especially banking institutions, as they are the most vulnerable to this type of crime. This is because money is the commodity that these institutions deal with. Electronic crimes have caused huge financial losses for these companies in addition to the loss of confidence Where customers. Electronic crime has become a hurdle to the growth and prosperity of institutions, attracting as many customers as possible and gaining their confidence. The problem is further compounded by sophisticated security techniques and the latest technologies used. The global reports issued by specialized agencies illustrate the magnitude of the problem worldwide and confirm that the United States Are the most consistently affected.

Keywords: Electronic Crimes; Effects of Electronic Crimes; Figures and Statistics.

JEL Classification Codes: L86, M15, O32

[1] المرسل: **أمين بن سعيد**، البريد الإلكتروني: ***Benamineee@hotmail.fr***

مقدمة:

أصبحت الجرائم الالكترونية اليوم تهدد المؤسسات الاقتصادية الكبيرة منها والصغيرة فتقلل من ربحيتها وتستهدف نظامها المالي، فالمؤسسة ذات نظام حماية ضعيف تعتبر هدفا سهلا للقراصنة ومجرمي الانترنت الذين يسلطون الضوء على البرامج التكنولوجية والقيود المالية للمؤسسات سواء من أجل سرقة الأموال أو فقط من أجل تدمير وتخريب البرامج لإلحاق الضرر بهذه المؤسسات.

فالتكنولوجيا سلاح ذو حدين، بالرغم من المزايا المستفاد منها في جميع مناحي الحياة إلا أنها أصبحت عائقا أمام التقدم التجاري والاقتصادي والفضل في ذالك يعود للجرائم الالكترونية التي كبدت المؤسسات خاصة البنكية خسائر مالية فادحة، حيث تكشف التقارير العالمية باستخدام الإحصائيات والأرقام في كل دول العالم عن حجم وخطورة هذه الجرائم التي يصعب في الكثير من الحالات الكشف عن مرتكبيها لارتكازها على العالم الافتراضي وهي الميزة التي يستغلها هؤلاء المجرمون لارتكاب جرائمهم والإفلات من يد العدالة.

فأصبح الشغل الشاغل للمؤسسة حماية برامجها من القرصنة ولذلك تقوم بتسخير أموال ضخمة من أجل هذه الحماية، فالجرائم الالكترونية تلحق الضرر من بابين الأول عندما تتعرض المؤسسة للقرصنة والثاني عند تثبيت نظام الحماية، وذلك يكلف المؤسسات أموالا ضخمة ترفع من تكاليفها وتكبدها خسائر مضاعفة.

منهجية الدراسة:

ضمن هذا الإطار العلمي والفكري المتداخل وأمام العرض السابق تبرز ملامح إشكالية هذا البحث والأهداف التي يرمي إلى تحقيقها على النحو التالي:

أهداف الدراسة:

ترمي هذه الدراسة إلى تحقيق جملة من الأهداف نذكر منها ما يلي:

- تسليط الضوء على ما يعرف بالجريمة الالكترونية والتي تعتبر أهم العوائق المدمرة لنجاح المؤسسات التي تعتمد بشكل كبير على التقدم التقني؛
- التطرق لمختلف وأهم الأساليب التي تستخدم في الجرائم الالكترونية؛
- التعرف وبالإحصائيات على حجم وخطورة هذه الجرائم عن طريق الكشف عن آثارها المدمرة للمؤسسات؛
- معرفة حجم الأضرار التي تتكبده المؤسسات بسبب آفة الجريمة الالكترونية؛
- دراسة الإحصائيات على مستوى عدة مناطق للحكم على مدى انتشار الظاهرة عالميا.

أهمية الدراسة:

تتمثل أهمية الدراسة في محاولة الكشف عن تعرض المؤسسات للضرر بسبب آفة الجريمة الالكترونية وما يكبدها ذلك من خسائر مالية، وذلك بالرغم من تطور طرق الحماية التقنية والتكنولوجية فبدل تسخير أموال الحماية للإنتاج والصالح العام توجه نحو الوقاية من القرصنة والسرقة الالكترونية.

مشكلة الدراسة:

ومن خلال ما سبق ذكره نطرح التساؤل التالي: **ما هي الآثار السلبية التي تتسبب فيها الجرائم الالكترونية للمؤسسات وكيف تتفادى هذه الأخيرة ذلك؟**

منهج الدراسة والأدوات المستخدمة:

قمنا باختيار المنهج التحليلي من خلال التطرق للظاهرة محل الدراسة بتحليل المعطيات والإحصائيات المتحصل عليها، أما الأدوات المستخدمة فهي التقارير الصادرة عن هيئات عالمية والتي تتناول الظاهرة محل الدراسة.

المحور الأول: أهم الإحصائيات المتعلقة بالجرائم الالكترونية

من الناحية الفنية، تعرف الجرائم الالكترونية على أنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[1]، وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الالكترونية، حيث أنه لارتكاب الجريمة يتطلب وجود أجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة.

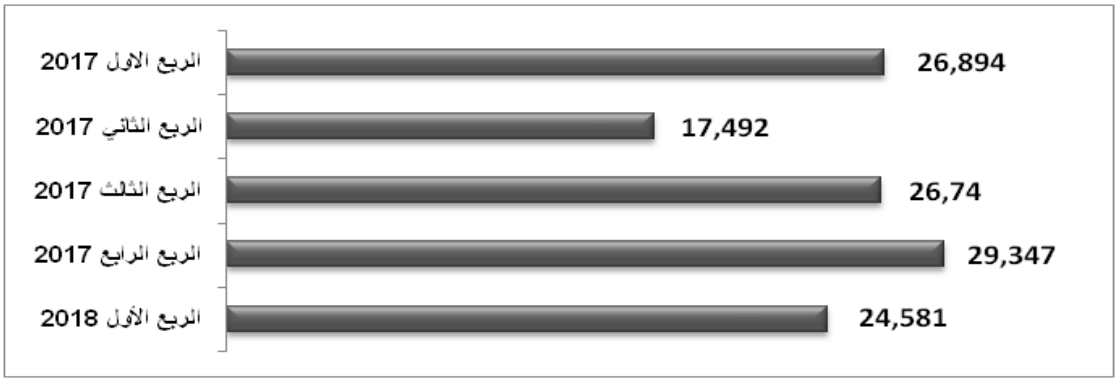
أما من الناحية القانونية تعرف بأنها: "مجموعة من الأفعال والأنشطة المعاقب عليها قانوناً والتي تربط بين الفعل الإجرامي والثورة التكنولوجية" وبمعنى آخر هي: "نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي"[2].

إذن هي: "الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بشكل غير قانوني".

أولا: أكثر الدول عرضة للجرائم الالكترونية

حسب تقرير أعدته RSA العالمية لأمن المعلومات، فإن الربع الرابع من سنة 2017 سجل أكبر فترة تمت فيها هجمات التصيد الالكتروني بحوالي 29.347 هجمة أما الربع الأول لسنة 2018 يشهد هو الأخر حوالي 24.581 هجمة الكترونية، فعدد الهجمات الالكترونية تحافظ على استقرار نسبي لها مما يدل على استمرا الظاهرة بشكل مكثف حتى سنة 2018.

شكل رقم (1) مجموع هجمات التصيد الالكتروني التي تم اكتشافها (الربع الأول 2017–الربع الأول 2018)



Source: RSA, « **RSA QUARTERLY FRAUD REPORT** », Volume 1, Issue 1, Q1 2018, Date of view: 30/19/2018, P 5, online: https://www.nu.co.za/images/docs/rsa-fraud-report-q1-2018.pdf

وحسب نفس التقرير للربع الأول والثاني من سنة 2018 فإن الدول الأكثر استهدافا لهجمات صيد المعلومات هي الولايات المتحدة الأمريكية وكندا، أما الدول الأكثر استضافة للهجمات هي الولايات المتحدة، كما شهدت هولندا واسبانيا زيادة في هجمات التصيد في الربع الثاني من 2018، مما دفعهما للوصول إلى أكثر خمس بلدان استهدافا، فرنسا هي الوافدة الجديدة لقائمة أفضل 10 بلدان استهدافا.

جدول رقم (01): الدول المستهدفة والمستضيفة للهجمات الالكترونية للربع الأول والثاني 2018

الدول المستضيفة للهجمات الالكترونية (الربع الأول 2018)		الدول المستهدفة من قبل الهجمات الالكترونية (الربع الأول 2018)		الدول المستضيفة للهجمات الالكترونية (الربع الثاني 2018)		الدول المستهدفة من قبل الهجمات الالكترونية (الربع الثاني 2018)	
.1	الو.م.أ	.1	كندا	.1	الو.م.أ	.1	كندا
.2	روسيا	.2	الو.م.أ	.2	الهند	.2	الو.م.أ
.3	الهند	.3	الهند	.3	كندا	.3	هولندا
.4	أستراليا	.4	البرازيل	.4	روسيا	.4	الهند
.5	كندا	.5	هولندا	.5	ألمانيا	.5	اسبانيا
.6	فرنسا	.6	كولومبيا	.6	هولندا	.6	البرازيل
.7	لوكسمبورغ	.7	إسبانيا	.7	استراليا	.7	كولومبيا
.8	ألمانيا	.8	المكسيك	.8	ماليزيا	.8	فرنسا
.9	الصين	.9	ألمانيا	.9	ايطاليا	.9	البيرو
10	إيطاليا	10	جنوب إفريقيا	.10	فرنسا	.10	المكسيك

Source: - RSA, « **RSA QUARTERLY FRAUD REPORT** », Volume 1, Issue 1, Q1 2018, Date of view : 30/19/2018, P 5, online: https://www.nu.co.za/images/docs/rsa-fraud-report-q1-2018.pdf
- RSA, « **RSA QUARTERLY FRAUD REPORT** », Volume 1, Issue 2, Q2 2018, Date of view : 30/19/2018, P 6, online: https://www.arame.com.mx/wp-content/uploads/2018/08/rsa-fraud-report-q218.pdf

فالربع الثاني لسنة 2018 شهد تغييرات مثيرة للاهتمام يشمل وافدون جدد لقائمة البلدان المستضيفة كهولندا واستراليا وماليزيا، كما سجلت روسيا انخفاض طفيف في عدد الهجمات التي استضافتها، أيضا

سجلنا سقوط كل من الصين ولوكسمبورغ من القائمة للربع الثاني مما يدل على انخفاض محسوس للهجمات التي تعرضت لها هذا الربع.

وحسب تقرير [3] آخر لسنة 2015 صادر عن الأمم المتحدة للتجارة والتنمية حول الاقتصاد المعلوماتي فإن الكثير من المستهلكين والشركات من قدموا شكاوي بخصوص تعرضهم للجرائم الالكترونية، أين تحتل الولايات المتحدة المركز الأول من حيث تلقي شكاوي المستهلكين وشكاوي المؤسسات لتعرضهم لجرائم الكترونية، وتحتل الصين المركز الثاني وبريطانيا المركز الثالث لتلقي شكاوي المؤسسات، فعدد الشكاوي تقرب الصورة نحو حجم الجرائم في كل دولة والضرر الذي يلحق من جرائها بالفرد والمؤسسة، والإحصائيات موضحة في الجدول التالي:

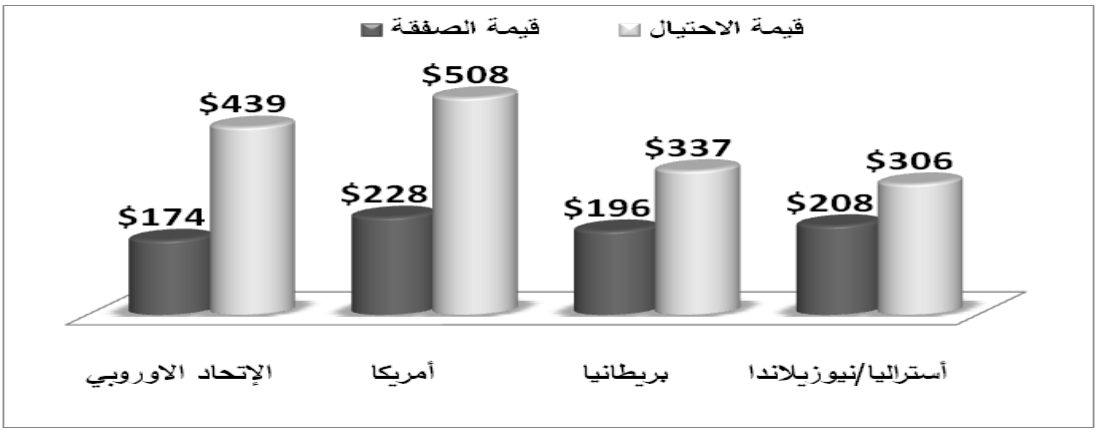
جدول رقم (02): عدد الشكاوى المقدمة من طرف المستهلكين والشركات لتعرضهم لجرائم الكترونية

موقع المستهلك	عدد الشكاوى	موقع الشركات	عدد الشكاوى
الولايات المتحدة	13445	**الولايات المتحدة**	4731
استراليا	1914	**الصين**	3996
فرنسا	1100	**بريطانيا**	1213
بريطانيا	767	**الهند**	469
كندا	694	**كندا**	285
البرازيل	555	**استراليا**	264
اسرائيل	448	**فرنسا**	246
الأرجنتين	341	**ألمانيا**	220
الهند	311	**المكسيك**	158
اسبانيا	295	**اسبانيا**	144

Source: UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, **"INFORMATION ECONOMY REPORT 2015"**, op.cit.

وإذا ما أخذنا على سبيل المثال قيمة عملية الاحتيال على بطاقات الائتمان المتعامل بها في التجارة الالكترونية حسب مناطق عالمية، سنجد حسب تقرير [4] RSA أن متوسط قيمة أي عملية احتيالية دائما أعلى من قيمة المعاملة الحقيقية، وقد لوحظ أن الاختلاف الأكثر حدة بين قيمة المعاملة الحقيقة وعمليات الاحتيال في أوروبا (غير متضمنة بريطانيا) حيث بلغ متوسط قيمة الصفقة الاحتيالية 439 دولار أي أعلى بنسبة 152% من متوسط قيمة المعاملة الحقيقية، تليها الولايات المتحدة الأمريكية التي بلغ فيها متوسط قيمة الصفقة الاحتيالية في هذا الربع الأول من سنة 2018 بحوالي 508 دولار أي أعلى بنسبة 144%.

شكل رقم (02): متوسط قيمة صفقات البطاقات الائتمانية ومتوسط قيمة الاحتيال فيها في الربع الأول من 2018

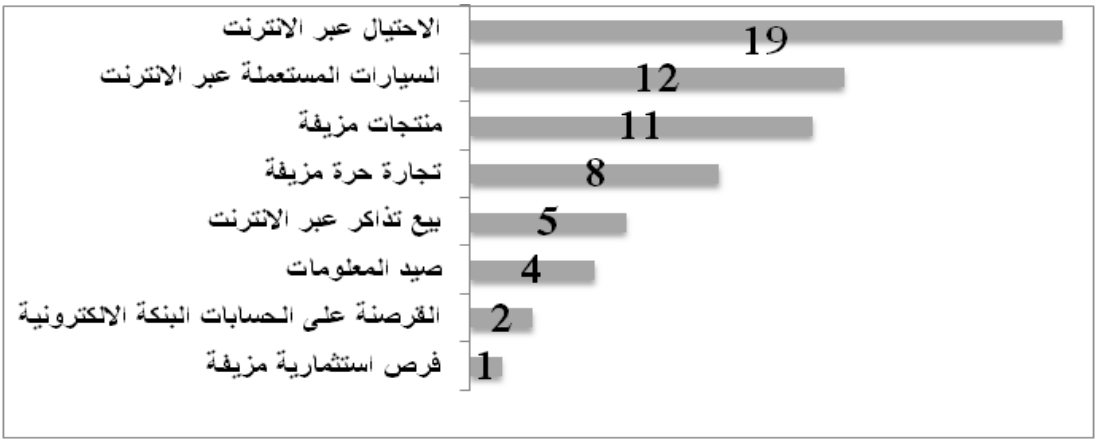


Source : RSA, « **RSA QUARTERLY FRAUD REPORT** », Volume 1, Issue 1, op.cit, p 9.

ثانيا: أكثر الجرائم الالكترونية شيوعا والتي تتعرض لها المؤسسات

أما عن نوع الجرائم المرتكبة باستخدام التقنية أو الحاسب الآلي أو شبكة الانترنت فهناك إحصائية على سبيل المثال تمت من قبل المركز الأوروبي للاستهلاك عبر شبكة الانترنت حيث قامت باستبيان ملخصة نتائجه في الشكل التالي:

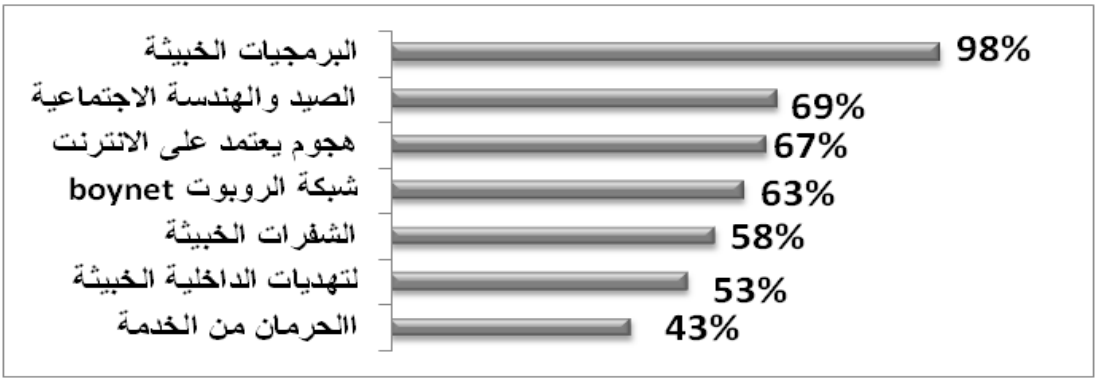
شكل رقم (03): نوع الجرائم الالكترونية المرتكبة في أوروبا



Source: UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, op.cit.

أما أنواع الهجمات الأكثر شيوعا على الشركات خلال مسح لسنة 2017 مس حوالي 254 شركة عالمية والتي تبين أن 98% منهم كانوا قد تعرضوا لهجمات ببرامج ضارة، 69% تعرضوا للاحتيال عن طريق الصيد باستخدام الهندسة الاجتماعية التي تعتمد على التحايل على العقول للإفصاح عن معلومات سرية،67% منهم تعرضوا للصيد عن طريق الانترنت.

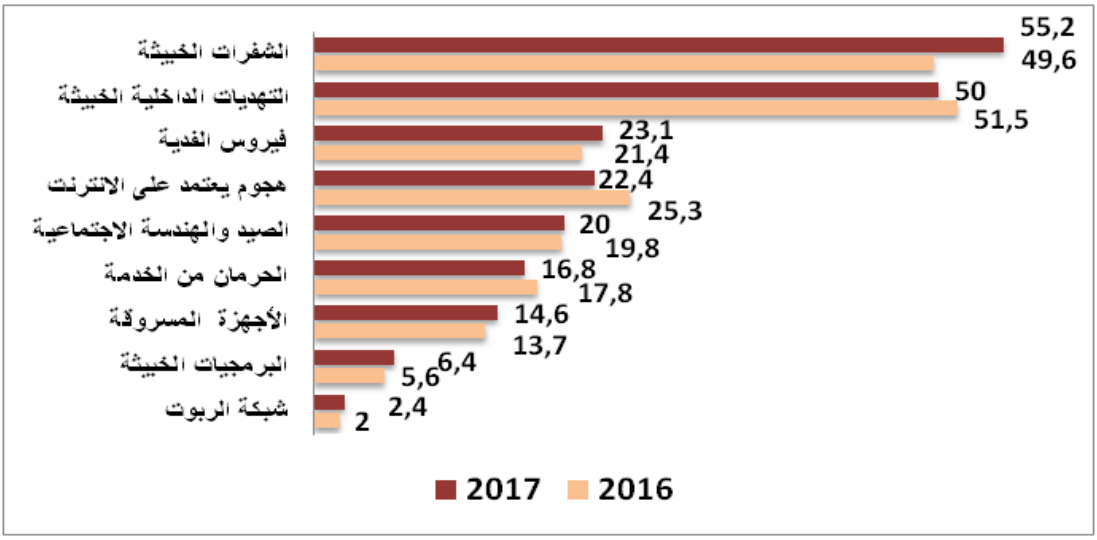
شكل رقم (04): نوع الجرائم الالكترونية التي تمس أغلب الشركات العالمية (أوت 2017)



Source: The Statistics Portal, "**Types of cyber crime attacks experienced by companies in the worldwide as of August 2017**", Date of view: 30/09/2018, online: https://www.statista.com/statistics/474937/cyber-crime-attacks-experienced-by-global-companies/

وفي دراسة من معهد Ponemon (يقوم بأبحاث مستقلة حول الخصوصية وحماية البيانات وأمن المعلومات) تمت في أوت 2017، حيث تشمل الدراسة 254 مؤسسة في سبعة دول مستقلة هي: الولايات المتحدة، المملكة المتحدة، ألمانيا، استراليا، اليابان، فرنسا وألمانيا، تبين أن بعض أنواع الجرائم تستغرق لحلها وقت أطول من غيرها لذلك هي أكثر تكلفة، والشكل الموالي يوضح الوقت المستغرق مقدر بمتوسط عدد الأيام التي يتم فيها حل مشكل نوع الهجوم الالكتروني.

شكل رقم (05): بعض الهجمات تتطلب وقتا أطول للحل



Source: Ponemo Institute, "**2017 Cost of Cyber Crime Study**", Date of view, 30/09/2018, online: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf

يتضح من الشكل أن متوسط أيام حل ومعالجة هجمات الشفرات الخبيثة، التهديدات الداخلية الخبيثة وفيروس الفدية (المخترقين) مرتفع لأنه يستغرق معظم الوقت، بينما يتم حل الهجومات المعتمدة على شبكة الانترنت والبرمجيات الخبيثة والفيروسات والروبوتات بشكل أسرع نسبيا (أي في غضون أيام قليلة)، كذلك

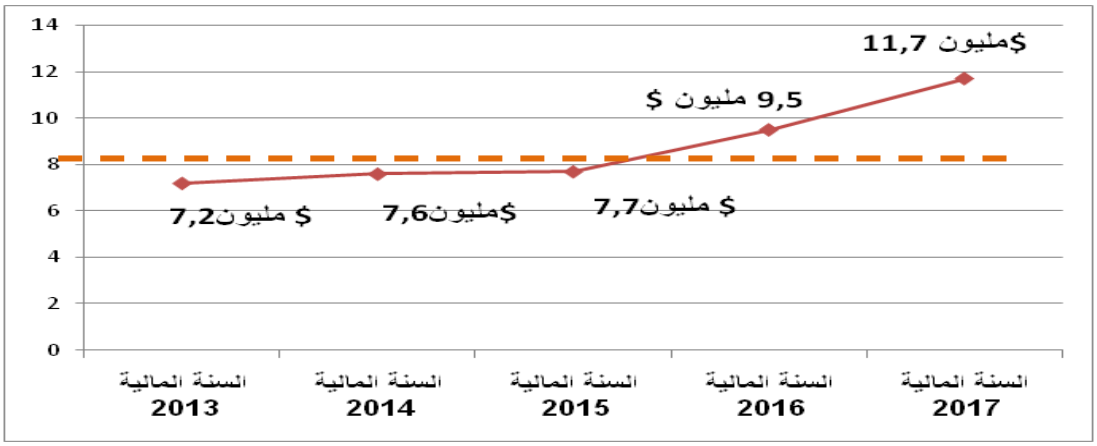
بمقارنة سنة 2016 مع سنة 2017 يتضح أن الشركات تتفق مزيدا من الوقت للتعامل مع الهجومات الالكترونية فمثلا الشفرات الخبيثة استغرقت بين 49.6 يوم سنة 2016 و55.2 يوم سنة 2017.

المحور الثاني: الآثار الناجمة عن الجرائم الالكترونية على الشركات

إن أهم أثرين للجرائم الالكترونية على الشركات هما الخسائر المالية الفادحة التي تلحق بهذه الشركات من جراء مثل هذه الجرائم، كذلك الخسائر التي تتكبدها الشركات لاقتناء وسائل الحماية والأمن ضد الهجمات والجرائم الالكترونية وخير دليل على ذلك الإحصائيات والأرقام التي تبين حجم هذه الخسائر.

فحسب تقرير[5] Ponemo Institute لسنة 2017 شهد متوسط التكلفة العالمية للجريمة الالكترونية على مدار الخمس السنوات الماضية (2013 إلى غاية 2017) زيادة ثابتة في السنوات الثلاث الأولى، ثم زيادة كبيرة قدرها 27.4 % مقارنة بالعام الماضي، حيث وصل متوسط التكلفة العالمية للجريمة الالكترونية سنة 2017 ذروته بـ11.7 مليون دولار.

شكل رقم (06): متوسط التكلفة العالمية للجريمة الالكترونية على مدار خمس سنوات (2013-2017)

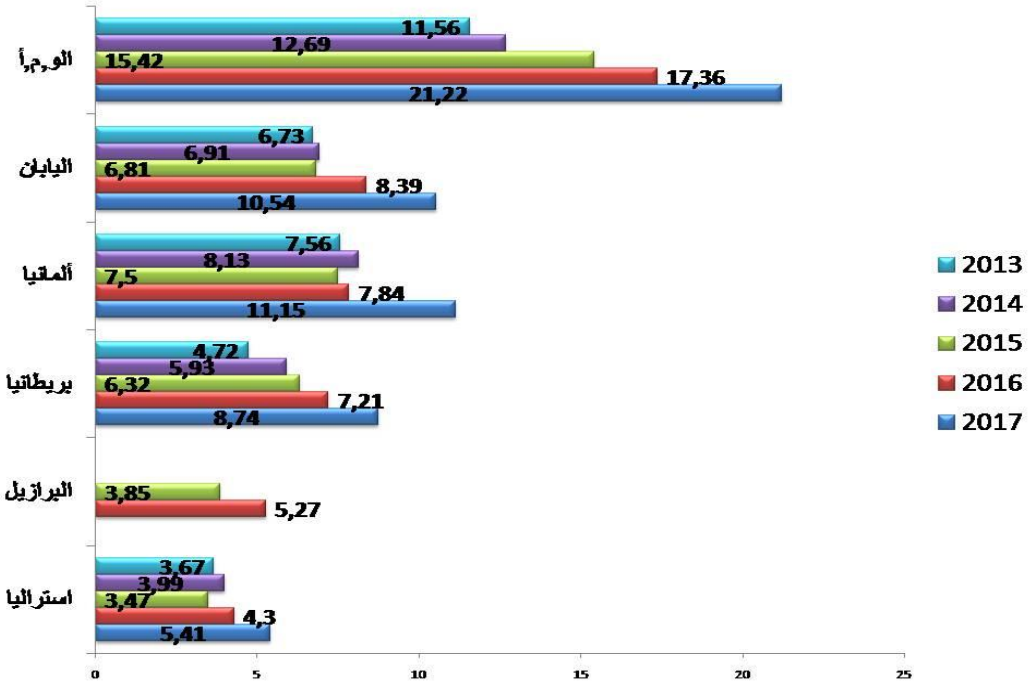


source: Ponemo Institute, "**2017 Cost of Cyber Crime Study**", op.cit, p 12

كما سنحاول تتبع حجم الجرائم الالكترونية زمنيا لأكثر الدول تعرضا لها من خلال إحصائيات عبر مسار زمني، مما سيمكننا من معرفة مدى تزايد أو تناقص هذه الظاهرة وعليه يمكن الحكم على فعالية وسائل الحماية والأمن المسخرة للتصدي ضد الجرائم الالكترونية، وذلك حسب نفس التقرير[6] لسنة 2016 وآخر سنة 2017 الصادر عن Ponemon Institute.

شكل رقم (07): تطور حجم خسائر الجرائم الالكترونية لستة دول خلال خمسة سنوات

(مليون دولار أمريكي)

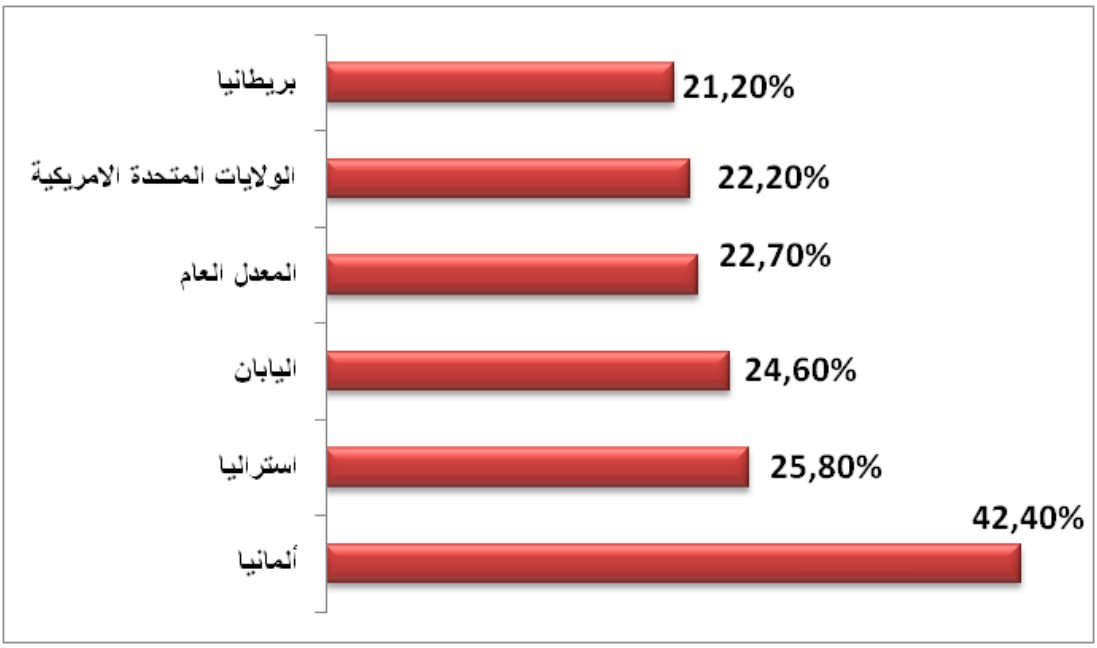


Source: - Ponemon Institute, "2016 Cost of Cyber Crime Study & the Risk of Business Innovation", p4, op.cit.
- Ponemon Institute,**"2017 cost of cyber crime study",** p13, op.cit.

عند مراقبة اتجاهات التكلفة مع مرور الوقت لحوالي 237 شركة منفصلة، نلاحظ أن أعلى تكلفة على مدار الخمس سنوات تسجل دائما بالولايات المتحدة الأمريكية وأدناها باستراليا، على العموم تم تسجيل زيادة مستمرة في تكاليف الجريمة مع مرور الوقت فالولايات المتحدة الأمريكية تطورت تكاليفها من11.56 مليون دولار سنة 2013 إلى 21.22 مليون دولار سنة 2017 أي بزيادة تقدر حوالي 9.66 مليون دولار، في حين الزيادة في تكاليف وخسائر الجريمة باستراليا مقارنة بين سنتي 2013 و2017 تقدر فقط بحوالي 1.74 مليون دولار فقط.

وحسب الشكل الموالي فإن أعلى نسبة ارتفاع لتكاليف الجريمة الالكترونية سجلت بين سنتي 2016 و2017 في ألمانيا بحوالي 42.2%، تليها استراليا بحوالي 25.8% ثم اليابان 24.6%، وأدناها سجلت في بريطانيا 21.2%.

شكل رقم (08): نسبة الزيادة في تكلفة الجريمة الالكترونية لمدة سنة واحدة (2016-20017)



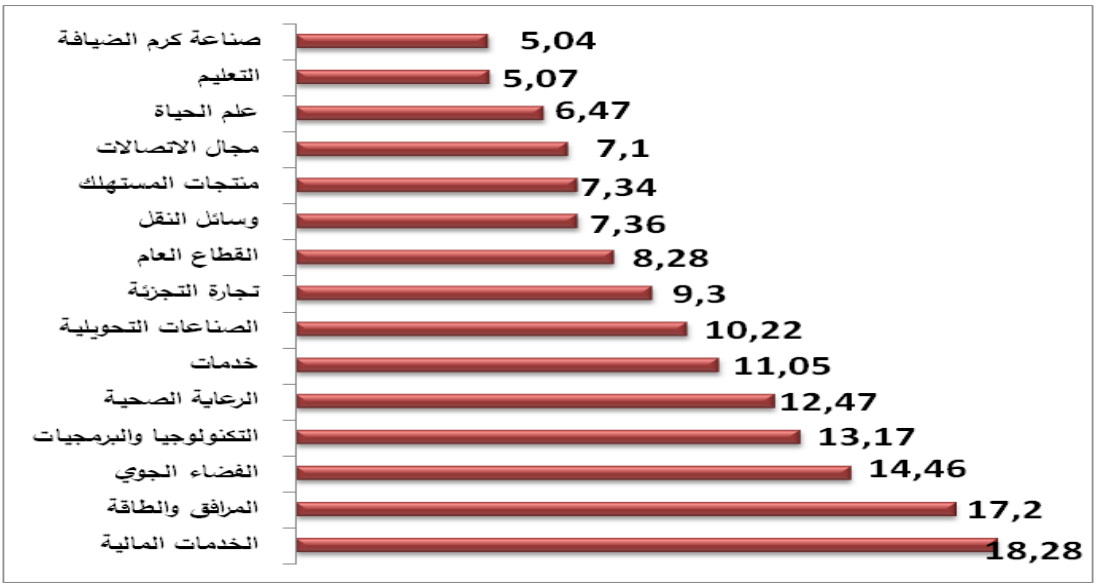
Source: Ponemon Institute,"**2017 cost of cyber crime study",** p14, op.cit.

وحسب نفس التقرير فإن الشركات التي تتبنى أجهزة أمنية مشددة ومبتكرة ضد الجريمة الالكترونية يبلغ متوسط تكلفة الجريمة 7.9 مليون دولار بينما الشركات التي تتبنى أجهزة أمنية منخفضة فإن متوسط التكلفة يرتفع عندها إلى 11.1 مليون دولار.

أما في تقريرها[7] لعام 2017 أصبح قطاع الخدمات المالية الأكثر تكلفة بسبب الجرائم الالكترونية أين كلف القطاع 18.28 مليون دولار من الخسائر جراء الجرائم الالكترونية، لأنه الأكثر استهدافا بالإضافة لقطاع المرافق والطاقة الذي تكبد خسائر قدرها 17.2 مليون دولار، هذا مقارنة بالقطاعات الأخرى كالشركات في علوم الحياة وقطاع النقل والاتصالات، وأقل قطاع تكبد خسائر بسبب الجرائم الالكترونية هو قطاع التعليم وقطاع حسن الضيافة (صناعة تعتمد على تعليم الشعوب كرم وحسن الضيافة لتشجيع السياحة) والشكل الموالي يبين تكلفة الجريمة الالكترونية حسب القطاعات لسنة 2017.

شكل رقم (09): متوسط التكلفة السنوية للجرائم الالكترونية حسب القطاع لسنة 2017

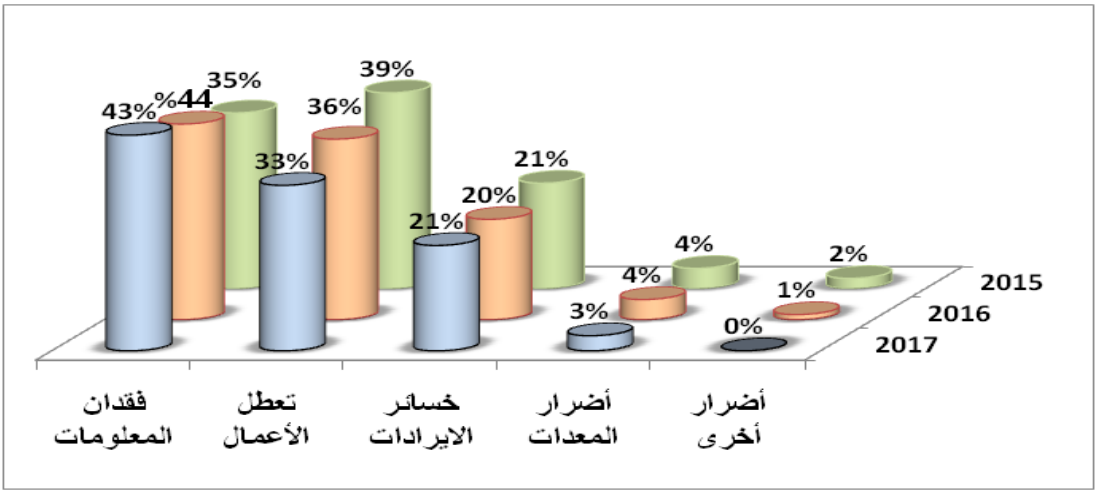
(مليون دولار)



Source: Ponemon Institute, "**2017 cost of cyber crime study**", op.cit, p20.

وفي نفس الدراسة تبين كنتيجة للجرائم الالكترونية خسارة الشركات للمعلومات هو أكبر الأضرار التي قد تلحق بها، حيث تبقى هذه الخسارة الأكبر من نوعها عند مقارنة كل من سنة 2015 و2016 2017، ثم تليها بنفس المقارنة الزمنية وبنسب قريبة منها تعطل أعمال الشركة كأكبر أنواع الخسائر التي تلحق بها بعد تعرضها للجريمة الالكترونية، وفي نفس العينة قيد الدراسة يتضح أنواع الخسائر التي تلحق بالشركة كأضرار تنتج عن هذا النوع من الجرائم مبينة في الشكل الموالي.

شكل رقم (10): النسبة المئوية للأضرار الخارجية الناتجة عن الجرائم الالكترونية لثلاثة سنوات

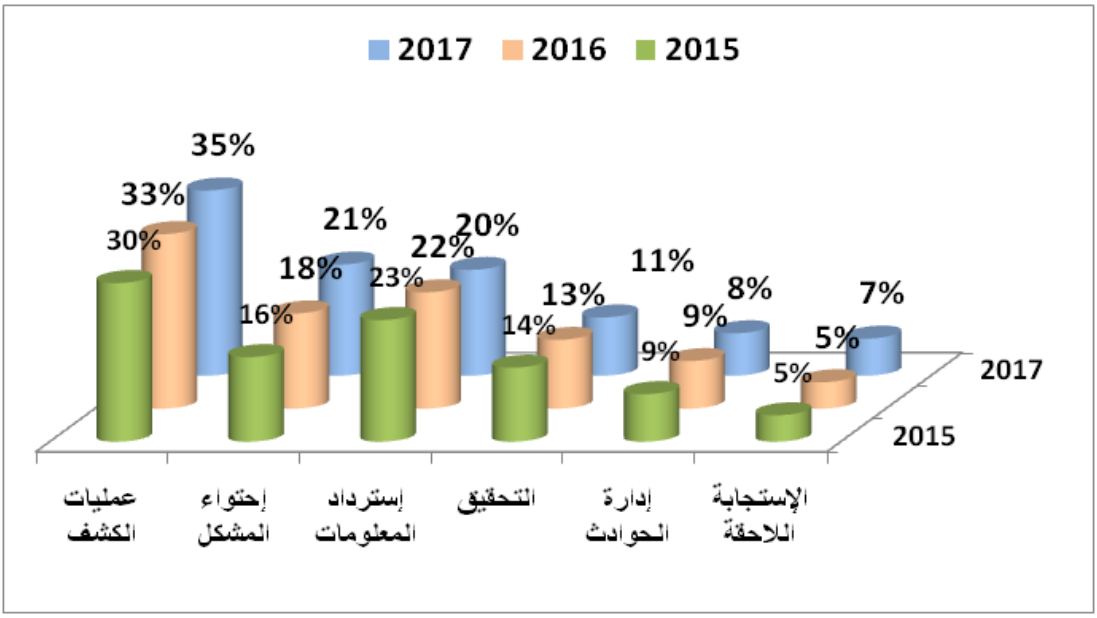


Source: Ponemon Institute, "**2017 cost of cyber crime study**", op.cit, p29.

ومما يزيد من خسائر المؤسسة طرق الكشف عن الجرائم وتقديم الحلول حيث تمثل هذه الأنشطة 55% من إجمالي تكلفة النشاط الداخلي، حيث تعتبر عمليات الكشف عن الجرائم الالكترونية

الأغلى والأكثر تكلفة إذ تكلف 35% من إجمالي تكاليف النشاط الداخلي كما سجلت ارتفاعا طفيفا منذ سنة 2015، كما هو مبين في الشكل الموالي حيث يشمل تكاليف الاحتواء والتحقيق والاستجابة للحوادث.

شكل رقم (11): نسبة الخسائر من تكلفة النشاط الداخلي

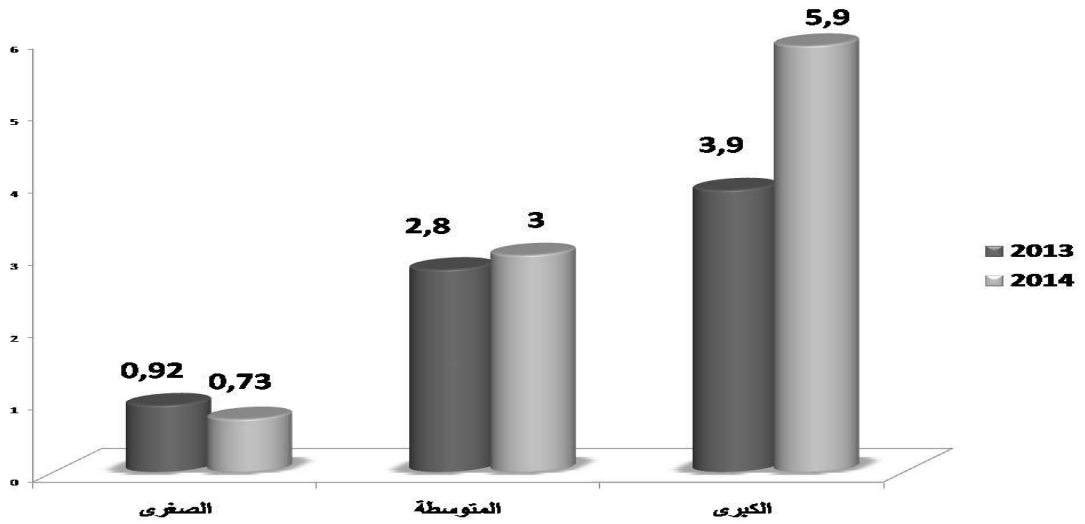


Source: Ponemon Institute, "**2017 cost of cyber crime study**", op.cit, p30.

كما جاء في تقرير [8] لشركة pwc بعنوان "إدارة المخاطر الالكترونية في عالم مترابط"، في 30 سبتمبر 2014 أن الشركات الكبرى ذات رأس مال يفوق البليون دولار تكشف في هذه السنة عن قدرتها على الكشف عن الجرائم الالكترونية بنسبة 44% أكبر من السنة الماضية (2013) والسبب يعود لكون هذه الشركات هي الأكثر عرضة لهذه الجرائم بسبب وفرة المعلومات التجارية لديها، وثائق الإستراتيجية، حجم كبير من العملاء الأوفياء.....الخ، لذلك هذه الشركات تتوفر على تقنيات تكنولوجية عالية مما يسمح لها الكشف عن هذه الجرائم. وهي تستمر في اقتناء وسائل الحماية والأمن، أما الشركات الصغرى (رأس مال أقل من 100 مليون دولار) سجلت نسبة 5% من حوادث الجرائم الالكترونية وتفسير ذلك كونها لا تستثمر كثيرا في تكنولوجيا الأمن مما يجعلها غير قادرة على الكشف عن الجرائم الالكترونية وأكثر عرضة لها.

شكل رقم (12): متوسط الخسائر المالية لقاء الأمن الالكتروني حسب حجم الشركة (2013-2014)

(مليون دولار)

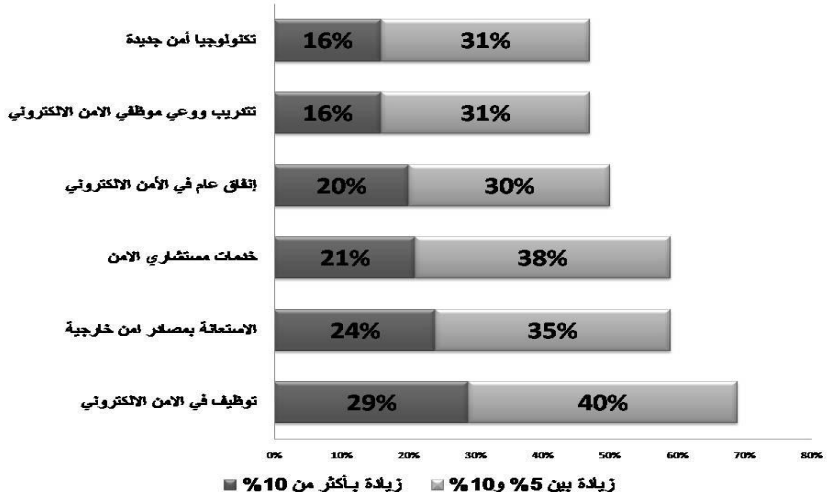


Source: pwc, « **managing cyber risks in an interconnected world** », op.cit.

يبدو أن الشركات الصغرى لا توفر ميزانية كافية للأمن الالكتروني مقارنة مع الشركات الكبرى والسؤال المطروح هل استسلمت هذه الشركات للجرائم الالكترونية؟ لكن بعد بعض الاستطلاعات يبدو أن الشركات الصغرى تعتقد بأنها لا تجذب انتباه القراصنة ولا تدخل في مجال اهتماماتهم مثل الشركات الكبرى، أيضا قد يعود السبب كون هذه الشركات لا تمتلك موظفين ذوي المهارات الكافية في التسيير.

بينت دراسة صدرت في مارس[9] 2017 توقع ازدياد 59% من غالبية ميزانيات الشركات المخصصة لمكافحة الجريمة الالكترونية خلال 12 شهرا القادمة بنسبة تفوق 5%، وواحد من خمس شركات ستقوم بمضاعفة ميزانية مكافحة الجريمة الالكترونية، وتتصدر هذه الشركات بحوالي 65% منهم تابعة لصناعة النقل والتوزيع

شكل رقم (13): مشروع الإنفاق على الأمن الالكتروني للأشهر 12 القادمة



Source: Hiscox, "**The Hiscox Cyber Readiness Report**", p8, op.cit.

وحسب دراسة معهد Ponemon لسنة 2014 (257 شركة من سبع دول) من بين أكثر التدابير فعالية ما قامت به أنشطة إدارة المؤسسات الأمنية التابعة للشركات من أجل مكافحة الجريمة الالكترونية عام 2014 بتعيين قائد أمني رفيع المستوى، شهادة المعايير الرائدة في الصناعة مثلISO27001 وتوظيف موظفي أمن ذوي خبرة...الخ، هذه الشركات تشهد انخفاض تكاليف الجريمة الالكترونية مقارنة بالشركات التي لم تطبق هذه الممارسات.

جدول رقم (03): تنفيذ الشركات لسبع أنشطة إدارة حكم الأمن

نوع الإجراء الأمني	نسبة الشركات التي تبنت الإجراء
شهادة للمعايير الرائدة في الصناعة مثلISO27001	%57
تعيين قائد أمني على مستوى رفيع	%52
توظيف خبراء في الأمن	%51
تخصيص ميزانية ذات موارد كافية	%50
تشكيل مجلس أمني على مستوى رفيع	%46
أنشطة التدريب والتوعية	%42
الاستخدام المكثف لمقاييس الأمن	%36

Source: Ponemo Institute, « **2014 Cost of Cyber Crime Study: United States** », October 2014, Date of view: 17/09/2015, online:
http://resources.idgenterprise.com/original/AST-0134059_2014_GLOBAL_CCC_FINAL_3.pdf

حيث يمكن لتنفيذ السبع أنشطة الأمنية داخل المؤسسات أن يقلل بشكل كبير من تكلفة الجرائم الالكترونية حيث يمكن تحقيق وفرات في التكاليف في المتوسط بقيمة 1131997 دولار لكل شركة من خلال استخدام شهادة للمعايير الرائدة في الصناعة أو قيمة 1267619 دولار عند توظيف أصحاب الخبرة في الأمن والجدول الموالي يوضح وفرات التكاليف التي حققتها المؤسسات محل الدراسة.

جدول رقم (04): وفرات في التكاليف عند تطبيق سبع أنشطة أمن إدارية داخل المؤسسات

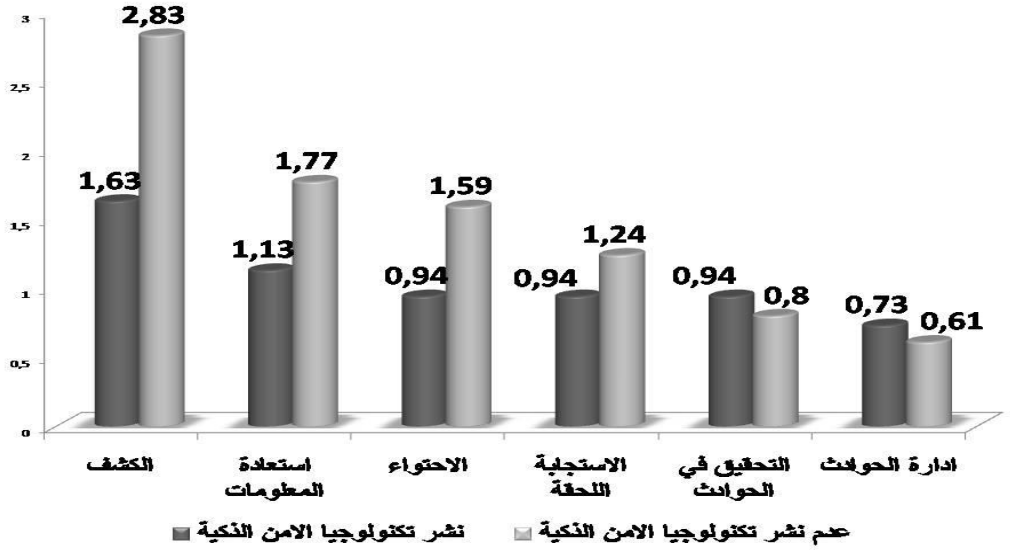
نوع الإجراء الأمني	قيمة التكلفة التي تم توفيرها
توظيف خبراء في الأمن	1.267.619 دولار
شهادة للمعايير الرائدة في الصناعة مثلISO27001	1.131.997 دولار
تعيين قائد أمني على مستوى رفيع	1.118.942 دولار
تخصيص ميزانية ذات موارد كافية	1.061.809 دولار
أنشطة التدريب والتوعية	712.603 دولار
الاستخدام المكثف لمقاييس الأمن	652.112 دولار
تشكيل مجلس أمني على مستوى رفيع	436.630 دولار

Source: Ponemo Institute, « **2014 Cost of Cyber Crime Study: United States** » .OPCIT

وحسب نفس الدراسة فإنه بالإضافة إلى تدابير الأمن الإدارية لابد من تنفيذ التدابير التقنية التي تعتمد على التكنولوجيات المتطورة، فتبني وسائل الأمن المتطورة مثل (أمن المعلومات وإدارة الأحداث SEIM) وحلول أنظمة منع الاختراق (IPS) وأنظمة شبكة المخابرات يساعد المؤسسات على كشف واحتواء الهجمات الالكترونية مما يؤدي إلى تخفيضات كبيرة في التكلفة السنوية لجرائم الانترنت، والشكل الموالي يوضح ما توصلت له الدراسة.

شكل رقم (14): مقارنة تكلفة النشاط والاستخدام لتكنولوجيات الأمن الذكية

(بالدولار)



Source: Ponemo Institute, « **2014 Cost of Cyber Crime Study: United States** », op.cit.

وحسب الدراسة هناك سبع تقنيات يجب تطبيقها لتوفير الأمن وتوفير تكاليف الجريمة الالكترونية وهذه التقنيات هي: ضوابط المحيط المتقدمة وتكنولوجيا الجدران النارية، مشاريع تكنولوجيا التشفير، نظم الأمن الذكية، الاستخدام المكثف لأدوات منع فقدان البيانات، أدوات وصول الحكم، نشر المشاريع من أدوات GRC (الحكم، أدارة المخاطر والامتثال)، أدوات إدارة السياسة الآلية.

ويمكن إنقاذ أموال الشركات بتطبيق التقنيات الأمان السبعة على سبيل المثال عند تطبيق نظم الأمن الذكية، في المتوسط، ستتمكن من توفير 2.6 مليون دولار أما عند تطبيق تقنية أدوات وصول الحكم ستوفر 1.4 مليون دولار، والجدول الموالي يوضح نتائج الدراسة.

جدول رقم (05): وفرات في التكاليف عند تطبيق سبع تقنيات تكنولوجية

تقنية الأمن	تكلفة الوفرة
أدوات إدارة السياسة الآلية	**429,173 دولار**
الاستخدام المكثف لأدوات منع فقدان البيانات	**1,134,374 دولار**
أدوات GRC	**1,335,730 دولار**
تكنولوجيا التشفير	**1,376,514 دولار**

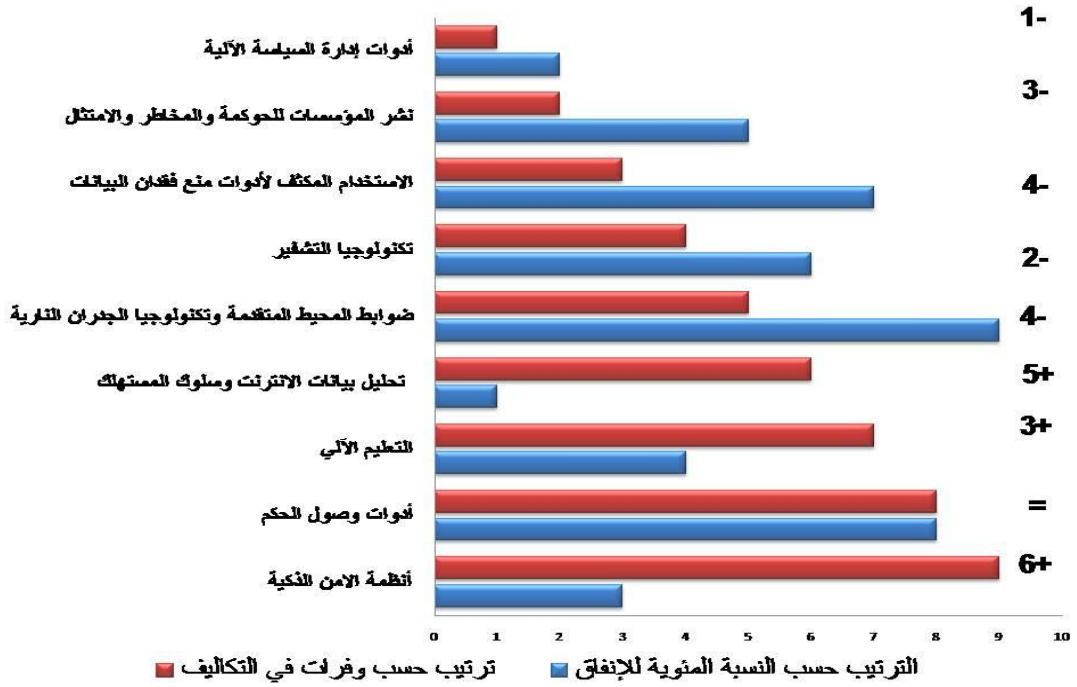
ضوابط المحيط المتقدمة وتكنولوجيا الجدران النارية	**1,397,186 دولار**
أدوات وصول الحكم	**1,403,261 دولار**
أنظمة الأمن الذكية	**2,575,405 دولار**

Source: Ponemo Institute, « **2014 Cost of Cyber Crime Study: United States** » .OPCIT

وحسب تقرير 2017 فإن تقنية الأنظمة الأمنية هي الأكثر فعالية والتي ينصح باستخدامها مقارنة مع التقنيات الأمنية الأخرى لأنه عند مقارنة تكلفة استخدام التقنية مع الوفرات في التكاليف عن استخدامها تعطينا أعلى نسبة كما يوضحه الشكل التالي.

حيث استخدمت الدراسة تقنية الرتب فمثلت قيمة 9 هي أعلى رتبة وقيمة 1 هي أدنى رتبة، فاتضح أن أنظمة الأمن الذكية ستوفر 6 رتب، بالإضافة لتقنية تحليل بيانات الانترنت وتقنية التعليم الآلي ستوفر في التكاليف بينما باقي التقنيات فهي تعود بالخسائر على الشركات.

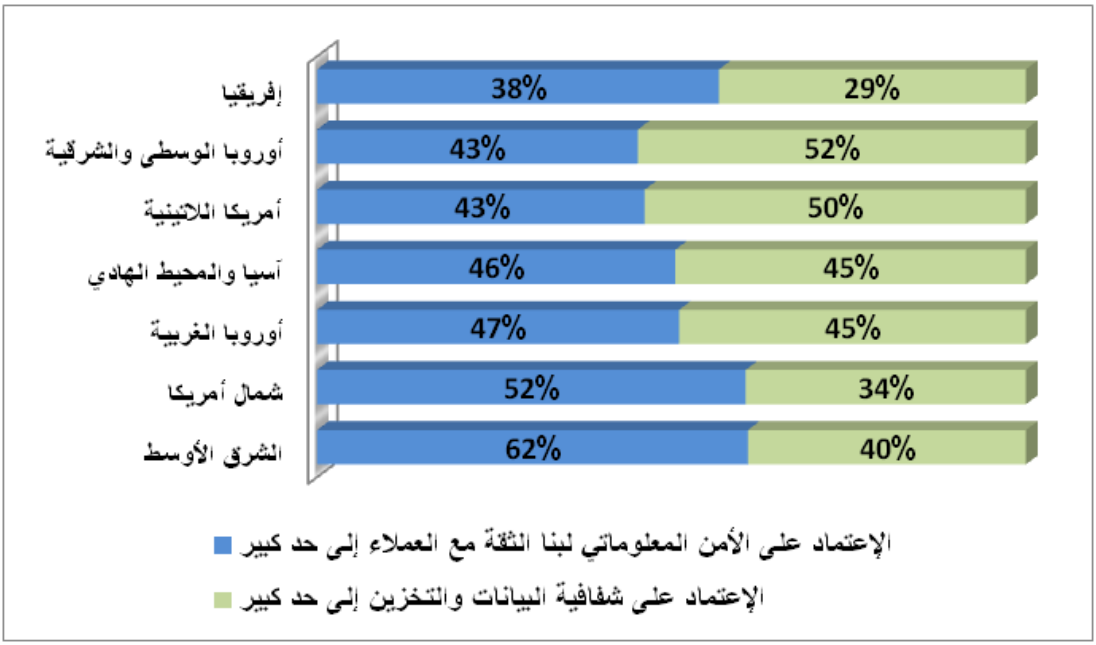
شكل رقم (15): مقارنة نظام الأمن من حيث مستويات الإنفاق ووفرات في التكاليف



Source*:* Ponemon Institute, **"2017 cost of cyber crime study**", op.cit, p 42.

في الأخير يعتبر توفير الأمن المعلوماتي والاستثمار فيه من قبل الشركات من أهم عوامل بناء الثقة بينها وبين العملاء في وقتنا الحالي، حيث أصبح من المهم للعميل التعامل مع الشركات ذات الأجهزة الأمنية العالية الجودة أكثر من أي عامل آخر حتى عامل الشفافية في الاستخدام، فقد جاء في تقرير[10] PWC لسنة 2018 التي مست 1293 مدير تنفيذي لشركات عبر مختلف العالم، التي بينت أن أغلب المديرين التنفيذيين للشركات يعتمدون على الاستثمار في تأمين المعلومات إلى حد كبير من اجل بناء الثقة بينهم وبين عملائهم، مقارنة بعامل الاعتماد على الشفافية في البيانات وتخزين المعلومات.

شكل رقم (16): المديرين التنفيذيين في جميع أنحاء العالم لديهم مجال للنمو في الأمن الالكتروني والخصوصية



Source: pwc," **Revitalizing privacy and trust in a data-driven world**", Survey 2018, p4, op.cit.

الخاتمة:

أصبحت البيئات الافتراضية أراضي خصبة لجرائم الإنترنت، مع عدد الجرائم التي تتصاعد سنويا جنبا إلى جنب مع شدة حجم الخسائر، ولذلك تأثير سلبي كبير على قطاعات لها علاقة مباشرة بالتقنيات التكنولوجية كالمؤسسات التي تعتمد على الأنظمة والشبكات الالكترونية وقطاع التجارة الالكترونية والمصارف...الخ، فعلى سبيل المثال لا الحصر حسب تقرير عام 2014 أن كل من إندونيسيا (حوالي 35% من معاملات التجارة الالكترونية مزورة) وفنزويلا (33%) وجنوب إفريقيا (25%) والبرازيل (11%) ورومانيا (10%) صنفت كأكبر دول منتجة للمعاملات الاحتيالية على الانترنت مما جعل تجار التجزئة الأمريكية يرفضون التعامل مع هذه البلدان والتركيز فقط على المعاملات المحلية.

فللجرائم الالكترونية آثار لا تعد ولا تحصى وقد لا تدرك الشركة أصلا بأنها كانت ضحية للجريمة الالكترونية لذا لا يمكن حصر الخسائر التي لا تكون دائما مادية فقد تكون أيضا معنوية، فقد تخسر الشركة عملائها الأوفياء لحظة إدراكهم أن هذه الشركة كانت ضحية لجريمة الكترونية وبذلك تخسر أيضا سمعتها مما يُكبدها خسائر أكثر.

نتائج الدراسة:

- للجريمة الالكترونية آثار مدمرة على الشركات خاصة في خضم الأزمات الاقتصادية، ما يجعل من الصعب على هذه الشركات تحقيق أرباح عندما تجد نفسها بين خسائر الجرائم الالكترونية وبين تكاليف تقنيات الأمن؛
- يمكن تلخيص آثار الجريمة الالكترونية على المؤسسات في النقاط التالية:
  - تكلفة الحماية من توظيف ذوي الخبرة واقتناء الوسائل التقنية للأمن؛
  - فقدان ثقة العملاء؛
  - الدفع للمستهلكين المتضررين؛
  - خسائر المبيعات (انخفاض المصاريف وارتفاع الإيرادات)؛
  - تغيير أساليب ممارسة الأعمال.

التوصيات:

- على المؤسسات التي تعمل في محيط معرض للجرائم الالكترونية كالبلدان المتقدمة، اقتناء برامج حماية متطورة منذ بداية تأسيسها حتى تحافظ على سمعتها؛
- يجب إنشاء مكاتب خاصة داخل كل مؤسسة متخصصة في برامج الحماية من الجرائم الالكترونية وكيفية معالجة القضايا في حال حدوثها؛
- على المؤسسة المتضررة من الجرائم الالكترونية بناء أسلوب صارم للخروج من الأزمة بأقل الخسائر الممكنة، كتعويض الخسائر من أموالها الخاصة للعملاء المتضررين دون إخطارهم بتعرضها للقرصنة في سبيل حماية سمعتها المستقبلية؛
- لابد على كل مؤسسة التفكير في احتمالية تعرضها للجرائم الالكترونية، وعدم الثقة بأنها بعيدة كل البعد عن ذلك فهي جريمة عابرة للقارات وتحدث دون إشعار مسبق.

الهوامش والمراجع:

1. محمد الأمين البشرى وإبراهيم محمد الهنائي، "**الجرائم الالكترونية وسبل مواجهتها** "، مركز البحوث والدراسات الأمنية، القيادة العامة لشرطة أبو ظبي، الإمارات العربية المتحدة، 2008، ص 29.

2. عبد الفتاح بيومي حجازي، "**الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**"، دار الكتب القانونية، مصر، 2002، ص 01.

3. *UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, "**INFORMATION ECONOMY REPORT 2015**", Date of view: 14/09/2015, online: http ://unctad.org/en/PublicationsLibrary/ier2015_en.pdf*

4 . *RSA, « **RSA QUARTERLY FRAUD REPORT** », Volume 1, Issue 1, op.cit, p 9.*

5 . *Ponemo Institute, "**2017 Cost of Cyber Crime Study**", op.cit, p 12.*

6 .- *Ponemon Institute,"**2016 Cost of Cyber Crime Study & the Risk of Business Innovation**", October 2016, Date of view: 01/10/2018 , p4, online: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf*

*- Ponemon Institute, **"2017 cost of cyber crime study**", p13, op.cit.*

7. *Ponemon Institute, "**2017 cost of cyber crime study**", p13, op.cit.*

8 *. pwc, "**managing cyber risks in an interconnected world**", Date of view: 17/09/2015, online: http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf*

9 . *Hiscox, "**The Hiscox Cyber Readiness Report**", 2017, p8, Date of view: 01/10/2018, online : https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf*

*10 – pwc," **Revitalizing privacy and trust in a data-driven world**", Survey 2018, p4, Date of view: 1/10/2018, online:*

https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf