Pricing cyber risks: Challenges and solutions



Tel Aviv, December 5 Simon Dejung, Senior Underwriter sdejung@scor.com



The opinions expressed in this presentation represents the views and interpretations of the author and do not necessarily represent the official position of SCOR.

Third-party sources are quoted as appropriate.

This publication is intended for information purposes only.

Topics discussed are of a qualitative nature such as the impact of new legislation and complying with Anti-Trust laws & regulations.



ertieren 🝷 🚮 Auswählen



How Israel Became a Cybersecurity Superpower

by TheTower.org Staff | 05.16.16 11:11 am

Israel's rise as one of the world's leaders in cybersecurity has been cooperation between the military, government, education, and priva partnership unmatched in the Western world, The Washington Pos

Israel's cybersecurity sector is now worth half a billion dollars annu⁰

FINANCIAL TIMES \equiv Q

HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Cyber Security	+ Add to myFT		Read next
Surge in	launche	es of Israeli cyber security	Fast FT Deutsche
compani	es		possible c
10 2 2	186		2 HOURS 4GO

Founders of country's start-ups are no longer just former veterans of elite military units



🎒 http://www.darkreading.com/analytics/meet-some-of-th 🔎 🔻 🖒 🚺 🚛 🔀 🚛 🕞

vertieren 🔹 💦 Auswählen

YTICS

Directly

MENTS

NOW

Meet Some Of The Emerging Israeli **Cybersecurity Firms**

Many are borne out of the entrepreneurial spirit of the Israel Defense Force's Cyber Intelligence Unit 8200. Could any other nation keep up?



If it seems to you like a hot new cybersecurity company springs out of Israel every week, you're not far off. Israel is now the world's second-largest exporter of cybersecurity products and services--second only to the US--with exports that grew from \$3 billion to \$6 billion in just a few years. The secret to its success: military experience. While the technology varies, many if not most of the newest companies have one thing in common: they were founded by veterans of the Israel Defense Force's (IDF) elite cyberintelligence Unit 8200.

"Last year, there were 16 Israeli companies on the Cybersecurity 500 list of the world's hottest and most innovative cybersecurity companies. This year there are 26, and we are expecting more in 2017," says Steve Morgan, founder and 1 CEO at Cybersecurity Ventures. "VC firms and corporate investors have put around a half-billion dollars into Israel cybersecurity startups over the past few vears."

Why Israel dominates in cyber security

by Peter Suciu SEPTEMBER 1, 2015, 6:00 AM EST

 \times

< 1 of 38 🕨

٧.

in



Historical, political, and societal factors have turned Israel an epicenter of security innovation, attracting companies like Microsoft

In recent months, and especially since the nuclear deal with Iran, there has been a strain between the U.S. and Israel. Despite this, one area where the ties remain close is cyber security, with the two parties even cosigning a statement committing continued cooperation on that front last

Steve Mills, senior vice president and group executive of IBM Software and Systems, speaks during the opening of the "CyberTech 2014" international conference on January 27, 2014 in the Mediterranean coastal city of Tel-Aviv.

Photograph by Jack Guez — AFP/Getty Images

SPONSOR CENTER

Israel's cyber security frontier

Warwick Ashford

G+ in 💌

The Israeli city of Beer Sheva is quickly becoming a global centre of cyber security technology



The southern Israeli city of Beer Sheva is used to protecting the frontier. During Roman times, it was a dusty outpost that formed part of the Limes Arabicus, a series of desert fortresses defending the empire from raiding tribes, Earlier, the Bible repeatedly cited Beer Sheva as the southern civilised limit of the Israelite kingdoms.



Cyber insurance – Available covers

- Data recovery
- Crisis management
- Forensics
- Monitoring
- Customer Notification
- Public relation (reputation)
- BI/LOP + extra expenses
- Extortion (ransom)
- Legal costs, fines, penalties
- TPL harm done by your incident to 3rd parties
- All risk
- → Cyber Insurance is a mechanism to transfer, share and pool IT security related risks
- → Cyber Insurance requires partnership with IT industry
- → Cyber Insurance is one of several IT Risk management mechanism



IoT & Interconnectivity in our everyday's life





Friday's Massive DDoS Attack Came from Just 100,000 Hacked IoT Devices

🛗 Wednesday, October 26, 2016 🛛 🛔 Swati Khandelwal

G+1 45 F Share 1114 Tweet 292 in Share 129 Share 1600



Future DDoS Attacks Could Reach 10 Tbps





EU / US / Israel - Protection of personal data



Home * Enforcement * Statutes * Federal Trade Commission Act

Federal Trade Commission Act

TAGS: Competition | Consumer Protection | Alcohol | Appliances | Automobiles | Clothing and Textiles | Finance | Franchises, Business Opportunities, and Investments | Funerals | Jewelry | Real Estate and Mortgages | Tobacco | Advertising and Marketing | Advertising and Marketing Basics | Children | Endorsements | Environmental Marketing | Health Claims | Made in USA | Online Advertising and Marketing | Telemarketing | Credit and Finance | Credit and Loans | Debt | Debt Collection | Mortgages | Payments and Billing | Privacy and Security | Children's Privacy | Consumer Privacy | Credit Reporting | Data Security | Gramm-Leach-Bliley Act | Red Flags Rule



· HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

· HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans) · The Enforcement Rule provides standards for the enforcement of all the Administrative

Simplification Rules

· HHS enacted a final Omnibus rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA



The documents here are unofficial translations to English of Israeli legislation and other relevant documents.

Information and Technology The only official version of Israeli legislation is the Hebrew version as it was accepted by the Knesset (the Israeli parliament) and published in the public Register. Organizational Chart

Legislation

ILITA The Israel Law,

Authority

- Basic Law: Human Dignity and Liberty
- Protection of Privacy Law, 5741-1981 unofficial translation
- Protection of Privacy (Transfer of Data Abroad) Regulations unofficial translation

Other documents

Legislation

- The Schoffman Report Report of the Committee for the Examination of Legislation Relating to Databases
- A Guide to Data Protection in Israel
- WP165 Opinion 6/2009 on the level of protection of personal data in Israel, adopted on 1 December 2009 by the Article 29 Data Protection Working Party
- · Yoram Hacohen, Data protection in Israel towards a new policy, Data Protection Review.eu (digital magazine published by the Data Protection Agency of the Community of Madrid)



Patient Safety

Associates

Covered Entities & Business

Training & Resources

FAQs for Professionals

Other Administrative

Simplification Rules

+

From hardwired "island operation" to a interconnected ICS networks

THE PAST: HARDWIRED INTERFACES

- A collection of dry contact inputs/outputs were used to fulfill a correlation matrix to meet a specific project integration objective
- Relay Logic was used to design complex interfaces
- Systems were poorly documented if at all and <u>nearly impossible to</u> <u>maintain or extend</u>









IRAM Industrial Risk Assessment Map by SCADACS www scadacs org

www scadacs org







NIS Directive & ExO 13636 – Recommendations & incentives for cyber insurance



Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Department of Homeland Security Integrated Task Force

Incentives Study Analytic Report

June 12, 2013



Homeland Security

					CIERCE ALL ECAD ALL	DUILL ECAD LUGIII	ADOUL CONTACL				
0		DIG	TAL SI	NGLE MARK	ET						
European Commission		Digital	Economy	& Society							
uropean Commission >	Network a	nd Information	Security Directiv	e: co-legislators agree on	the first EU-wide legis	lation on cybersecurity					
The strate	gy	Economy	Society	Access & connectivity	Research & innovation	DG CONNECT					
ociety			Netwo	ork and Info	ormation S	Security Dir	rective:				
kills & Jobs			co-legislators agree on the first EU-wide legislation on cybersecurity								
Health and Ageing											
mart living			Published on 09/12/2015								
igital Inclusion			On 7th December 2015, the European Parliament and the Council reached an agreement on the Commission's proposed measures to increase online security in								
ublic Services											
ybersecurity and pr	ivacy	+	the EU. The <u>Network and Information Security (NIS)</u> Directive is the first piece of European legislation on cybersecurity. Its provisions aim to make the online environment more trustworthy and, thus, to support the smooth functioning of the								
Cybersecurity		-									
Cybersecurity ind	ustry		EU Digital	Single Market.							
Online privacy			The proposal for a Directive concerning								
EU Funded Projects			network a	to ensure a high com nd information securi	ty across the						
nline trust			Union was put forward by the European								
ontent and media			a set of m	easures to boost the	overall level of cyb	persecurity in the EL	J.				
mergency and supp	ort lines		The new r	ules will:							
 improve cybersecurity capabilities in Member States improve Member States' cooperation on cybersecurity require operators of essential services in the energy, transport, banking healthcare sectors, and providers of key digital services like search engines cloud computing, to take appropriate security measures and report incidents to the national authorities, 											

9



Reliability issues with cyber loss data

Potential attributes can also be added



Cyber Scenarios (columns) and affected covers (rows)

IMIA Working Group Paper 98 (16)

Cyber Pricing Cyber Scenarios with Effects to Indemnification types	Malicious Act /Targeted Virus Target: PD frequency estimate events per year freq.estimate per outsourcing provider events per year				Computer Malware, widespread Virus frequency estimate events per year freq.estimate per outsourcing provider events per year			Human Error frequency estimate events per year freq.estimate per outsourcing provider events per year			System Failure frequency estimate events per year freq.estimate per outsourcing provider events per year					
		Prob	ability	1	Probability			1	Probability			Probability				
+ Privacy Breach: Pll data affected											<i>\\\\\\</i>					
+ Data Breach: non-Pll data affected																
+ Data Insurance: Loss of own data																
+ Property Damage	100															
+ PD costs																
+ BI following PD																
+ Loss of Profit		¥														
+Increased cost of working		¥//////														
+ Extortion due to PD threat								<u></u>				¥				
+ Payment of Extortion Ransom		¥														
+ Chisis management Fees																
+ Extortion due to unknown threat		t									ŧ					
+ other target affected through insured's network											ŧ					
+ Media Liability Issue		VIII					V				ŧ////					
											V					

- Loss severity distribution: NLE PML MFL
- Frequency estimation
- *Multiple coverage triggers*



Data Comparison of Cyber incidents & claims publications – predominantly US



Highlights from NetDiligence® 2016 Cyber Claims Study



2016 Cost of Data Breach Study Global Analysis



Journal of Cybersecurity, 2016, 1–15 doi: 10.1093/cybsec/tyw001 Research paper

Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC June 2016



Research paper

Examining the costs and causes of cyber incidents

Sasha Romanosky*

RAND Corporation, 1200 South Hayes St, Arlington, VA 22202, USA

*Corresponding author: E-mail: sromanos@rand.org.

Received 23 January 2016; revised 24 May 2016; accepted 20 June 2016



Cause of claim (event)

Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach

Consolidated view (n=383)



Figure 5. Rates of malicious events.





Ø cost / event: insurance claim & incident - not the same!!

Figure 2. The average total organizational cost of a data breach over three years Grand average for FY 2016=\$4.0, FY 2015=\$3.8, FY 20|14=\$3.50 *Historical data is not available in all years (FY 2016=383, FY 2015=350, FY 2014=315) Measured in US\$ (millions)



Table 2. Cost by event type (in millions)

Event type	Ν	Mean	SD	Median	Min ^a	Max
Data Breach	602	5.87	35.70	0.17	0.00	572
Security Incident	36	9.17	27.02	0.33	0.00	100
Privacy Violation	234	10.14	55.41	1.34	0.00	750
Phishing	49	19.99	105.93	0.15	0.01	710
Total	921	7.84	47.28	0.25	0.00	750

while the largest was \$15 million (note that some claims are still open). The **average breach** cost was \$665K, down slightly compared to last year's study. The median breach cost was \$60K.





Claims cost per cause of loss

TOTAL COSTS (including SIR)											
	Cases	Min	Median	Mean	Max						
Hacker	41	2,500	210,856	1,863,419	15,000,000						
Lost/Stolen Laptop/Device	21	290	55,000	140,784	1,650,000						
Malware/Virus	36	1,190	99,380	468,788	3,952,626						
Other	20	1,789	14,940	44,447	287,000						
Paper Records	11	1,000	12,634	22,987	60,000						
Rogue Employee	12	8,914	80,338	1 ,023,595	11,491,000						
Staff Mistake	16	1,234	9,871	133,609	1,603,800						
System Glitch	10	1,825	25,878	207,867	779,293						
Theft of Hardware	1	110,000	110,000	110,000	110,000						
Theft of Money	4	23,755	49,250	94,314	255,000						
Total	172										



Ø cost / **record**: insurance claim & incident - not the same!!

Figure 1. The average per capita cost of data breach over three years

Grand average for FY 2016=\$158, FY 2015=\$154, FY 2014=\$145 *Historical data is not available in all years (FY 2016=383, FY 2015=350, FY 2014=315) Measured in US\$



\$307

\$3.94

66% of the claims in the dataset reported both the number of records lost and the total breach



US (64)



The Art & Science of Risk

\$1.36

10.000

5,000



\$250

\$201

\$194

\$189

\$183 \$186 \$196

\$200

\$148

\$141 \$146 \$156

\$140 \$134 \$133 \$131

\$150

Š\$163 159

\$217 \$221

\$211 \$213

\$211

Ø cost / record per industry sector

Figure 4. Per capita cost by industry classification

Consolidated view (n=383), measured in US\$





Cost split of a cyber claim

Figure 16. Coverage provided by the insurance company More than one response permitted



SCOR The Art & Science of Risk

Crisis cost / event







Notification costs were the highest in US. Notification-related include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication set-up. By far, notification costs for US organizations were the highest (\$0.59), as shown in Figure 14.





Cyber claim (event) by data type



Figure 4. Cyber events by type of information compromised.



Claim (event) frequency by industry sector





Privacy Violations ----- Security Incide



PERCENTAGE OF RECORDS EXPOSED BY BUSINESS SECTOR (N = 120)

Figure 2. Four types of cyber events.







NUMBER OF CLAIMS BY BUSINESS SECTOR (N = 176)

Figure 3. Cyber incidents, and rates, by industry.

The Art & Science of Ris

D.B.: disclosure of PII, theft of computers, identity theft, fraud

S.I.: computers/network disruption, DoS, intellectual prop. theft, hack, extortion, BI

P.V.: collection, use, sharing of personal information

Correlation of claims (losses) & company revenue





Figure 15. Loss as a percentage of revenues.



IT SOLUTIONS INTEGRATOR Revenue: \$1.7 million Revenue: \$200 million Limit: \$1 million Exempels from the US market Limit: \$5 million Premium: \$1800 Premium: \$41,500 PHARMACY BENEFITS MANAGEMENT COMP SAAS PROVIDER SAAS PROVIDER Revenue: \$4 billion Limit: \$5 million Revenue: \$750,000 Revenue: \$3 million Premium: \$84,000 Limit: \$10 million Limit: \$2 million Premium: \$29,800 Premium: \$6000 **INDUSTRY: HEALTHCARE** Revenue: \$25 million IT CONSULTING & DATA HOSTING PROVIDER Limit: \$1 million FAST FOOD Premium: \$12,900 Revenue: \$1.5 million Limit: \$2 million Revenue: \$15 million Premium: \$3,643 Limit: \$1 million **INDUSTRY: HEALTHCARE, SOCIAL WORKER** Premium: \$9000 Revenue: \$120,000 Limit: \$1 million HEALTHCARE SAAS PROVIDER Premium: \$859 Revenue: \$2 million HOSPITAL Limit: \$2 million Revenue: \$170 million **INDUSTRY: EDUCATION** Premium: \$9398 Limit: \$5 million Revenue: \$25 million Premium: \$42,000 Limit: \$1 million **HEALTHCARE** Premium: \$6,000 **PROVIDER/CONSULTING/PROJECT** MANAGEMENT DATA STORAGE CENTER **INDUSTRY: FINANCIAL** Revenue: \$4.5 million Revenue: \$15 million Revenue: \$100 million Limit: \$5 million Limit: \$1 million Limit: \$20 million Premium: \$34,600 Premium: \$37,000 Premium: \$120,000

https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-databreach-insurance-premiums/

The Art & Science of Ris

DOCTOR'S OFFICE

Exempels from the UK market

Options Based on the total gross revenue of the Proposer for the last financial year, tick (🗹) the box indicating the Premium for the Option required.											
Limit of Liability											
(Any one claim and in the				GBP 1,000,001		GBP 2,500,001	GBP 5,000,001				
aggregate)	U	p to GBP 1,000,000		to GBP 2,500,000		to GBP 5,000,000		to GBP 10,000,000		GBP10,000,001 to GBP20	,000,000
GBP 100,000		GBP 400		GBP 550		GBP 850		GBP 1,250		GBP 1,850	
GBP 250,000		GBP 650		GBP 800		GBP 1,050		GBP 1,500		GBP 2,220	
GBP 500,000		GBP 950		GBP 1,100		GBP 1,350		GBP 1,850		GBP 2,275	
GBP 1,000,000		GBP 1,450		GBP 1,625		GBP 1,950		GBP 2,450		GBP 3,225	
GBP 2,000,000		GBP 2,350		GBP 2,600		GBP 2,950		GBP 3,500		GBP 4,500	
GBP 3,000,000		GBP 3,250		GBP 3,500		GBP 3,800		GBP 4,750		GBP 6,000	

Premiums are excluding local taxes and are subject to change. If you require a limit of liability above the GBP 3,000,000, or the total gross revenue is above GBP 20,000,000, approach your Broker to obtain a specific alternative quote. Please note that this document does not represent a unilateral offer and that the terms herein are subject to confirmation by the Insurer.

Retentions- Applicable to all sections of	the policy, except for First	Response where no retention	applies	
Up to GBP1,000,000 Total Gross Revenue	GBP1,000			
GBP1,000,001 to GBP5,000,000 Total Gross Revenue	GBP2,500			
GBP5,000,001 to GBP10,000,000 Total Gross Revenue	GBP5,000			
GBP10,000,001 to GBP20,000,000 Total Gross Revenu	e GBP7,500			
Coverage		Sub-limit of Liability	Separate Retention	
A. Event Management		Full Limit	General policy retention	
A. 1 First Response:		Full Limit	Nil retention	
B.1 Data Protection Investigations		Full Limit	General policy retention	
B. 2 Data Protection fines		Full Limit	General policy retention	
C. Liability		Full Limit	General policy retention	
Optional Extentions		Sub-limit of Liability	Separate Retention	Additional Premium
Digital Media		Full Limit	General policy retention	10 % of original premium YES 🗖 NO 🗖
Cyber/Privacy Extortion Liability		Full Limit	General policy retention	5 % of original premium YES 🗖 NO 🗖
Outsource Service Provider		Full Limit	N/A	Refer to AIG for this cover
Network Interruption		Full Limit	Waiting period 12 hours	25 % of original premium YES 🔲 NO 🗖



Prerequisites for a healthy cyber insurance market:

- Strong IT security providers
- Legal incentives for cyber/IT risk management (see US/EU)
- Wordings must address "silent" cyber cover & manage these "new" scenarios (new exposures) by pricing it OR excluding it clearly

Due to lack of historic data, pricing is scenario-based on a case by case basis

> Actuary, underwriter & IT security specialist have to work together

Studies for cyber incident costs & cyber incident insurance claims are often inconsistent and depend on:

- Sample size
- Industry sector
- Company size
- Country & legal system







