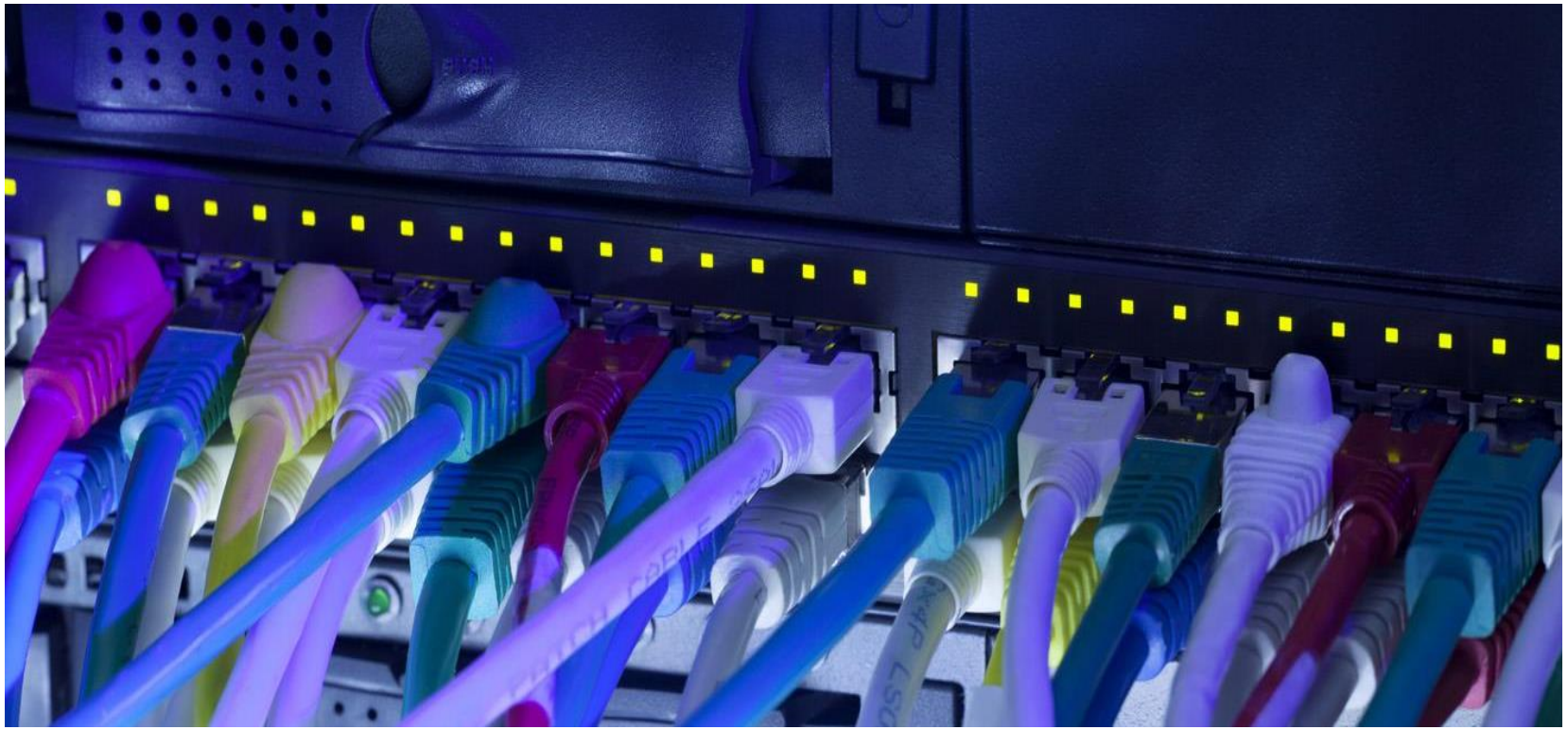
Pricing cyber risks: Challenges and solutions



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

SCOR
The Art & Science of Risk

DISCLAIMER

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.

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 priv
partnership unmatched in the Western world, *The Washington Pos*

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

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?

1 of 38

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 CEO at Cybersecurity Ventures. "VC firms and corporate investors have put around a half-billion dollars into Israel cybersecurity startups over the past few years."

FINANCIAL TIMES

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

Cyber Security + Add to myFT

Surge in launches of Israeli cyber security companies

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

Read next

Fast FT Deutsche possible c 2 HOURS AGO

Latest o

Fast FT Deutsche possible c 2 HOURS AGO

Lloyd's bo attack dat

Fast FT Vinci shar

Why Israel dominates in cyber security

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

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

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

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

SPONSOR CENTER

Israel's cyber security frontier

Warwick Ashford
Security Editor

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

THIS ARTICLE COVERS
Cybercrime

RELATED TOPICS
Antivirus
Secure Coding and

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**

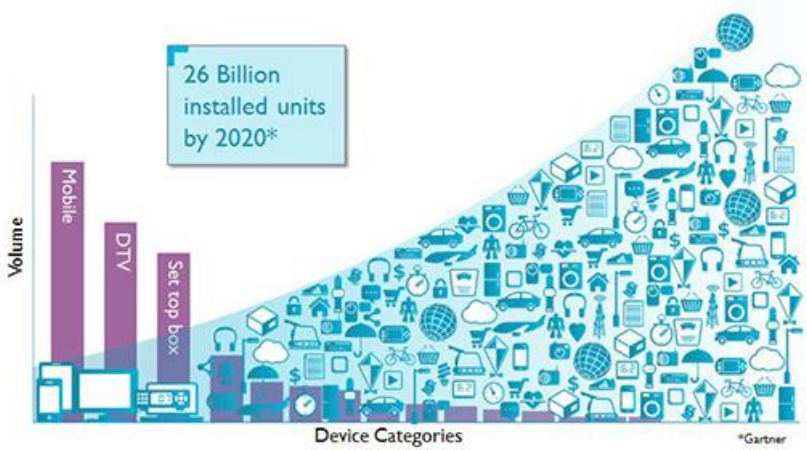
→ **Cyber Insurance is one of several IT Risk management mechanism**

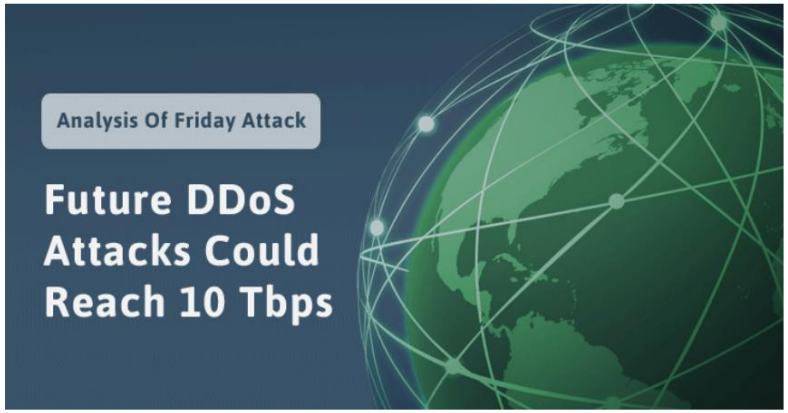
IoT & Interconnectivity in our everyday's life

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

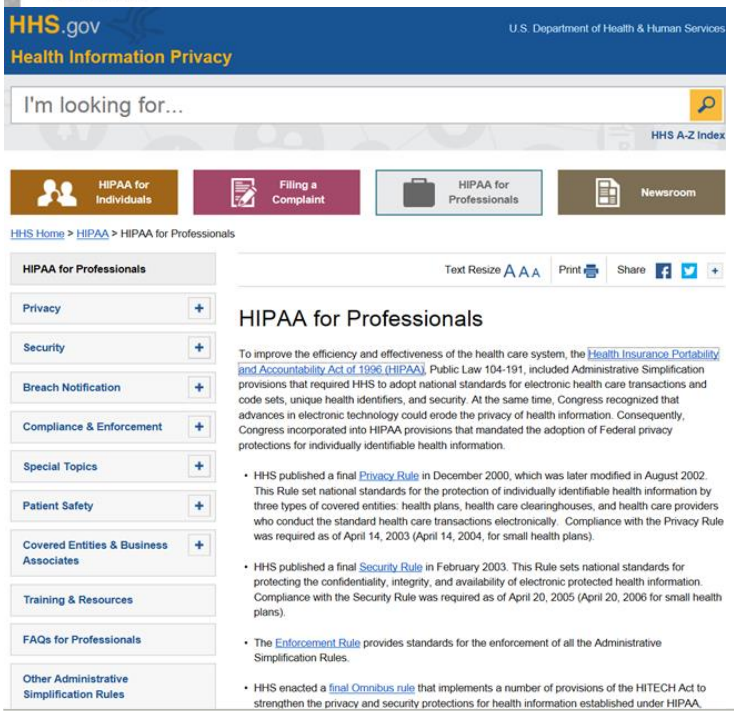
Wednesday, October 26, 2016 Swati Khandelwal

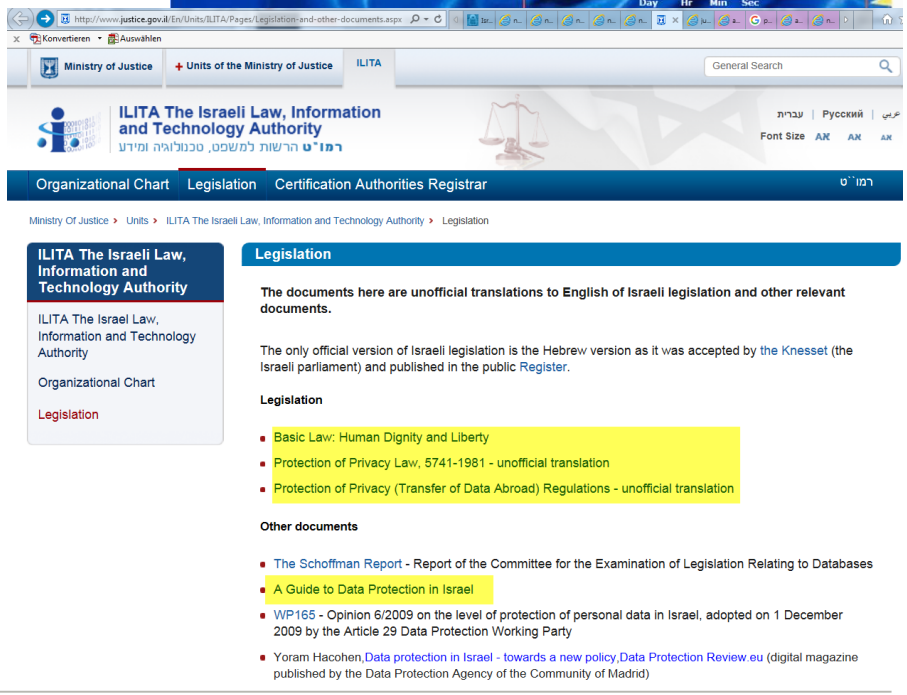
G+1 45 Share 1114 Tweet 292 Share 129 share 1600





EU / US / Israel - Protection of personal data

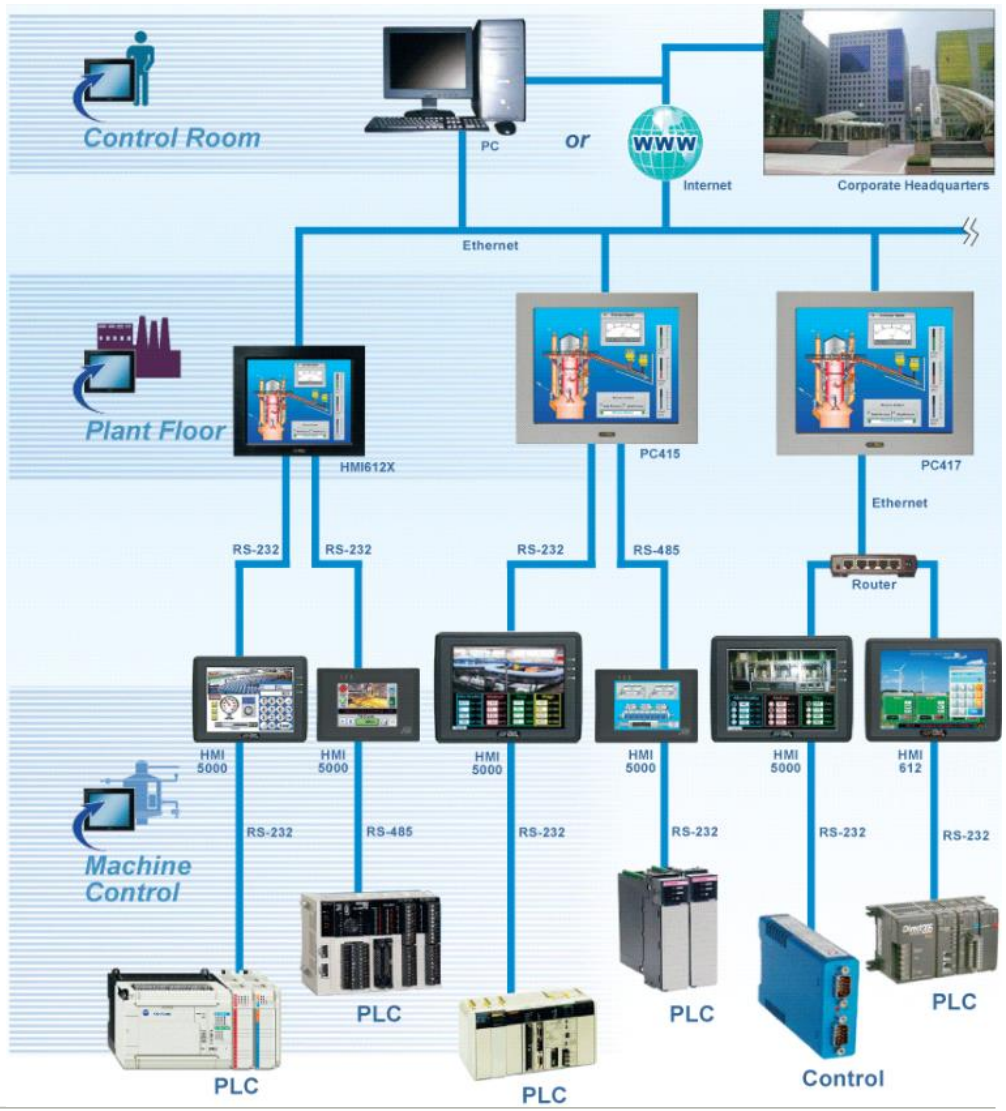




From hardwired “island operation” to a interconnected ICS networks

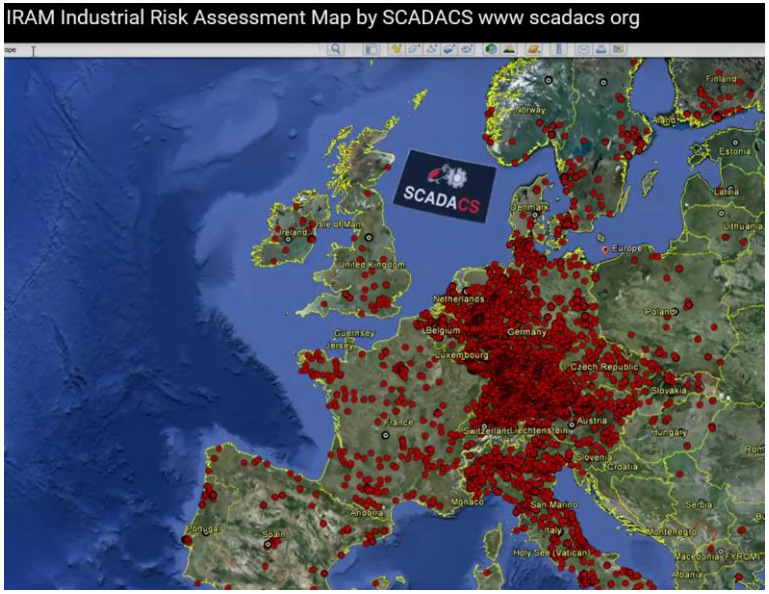
THE PAST: HARDWIRED INTERFACES

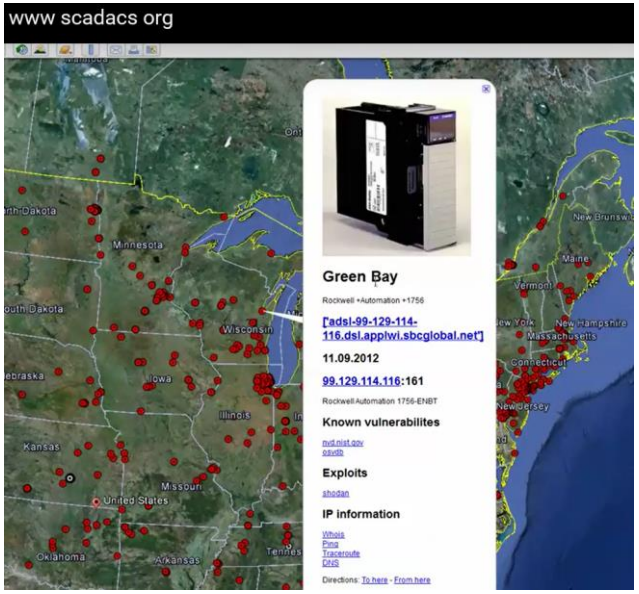
- A collection of dry contact inputs/outputs were used to fulfill a correlation matrix to meet a specific project integration objective
- Relay Logic was used to design complex interfaces
- Systems were poorly documented if at all and nearly impossible to maintain or extend



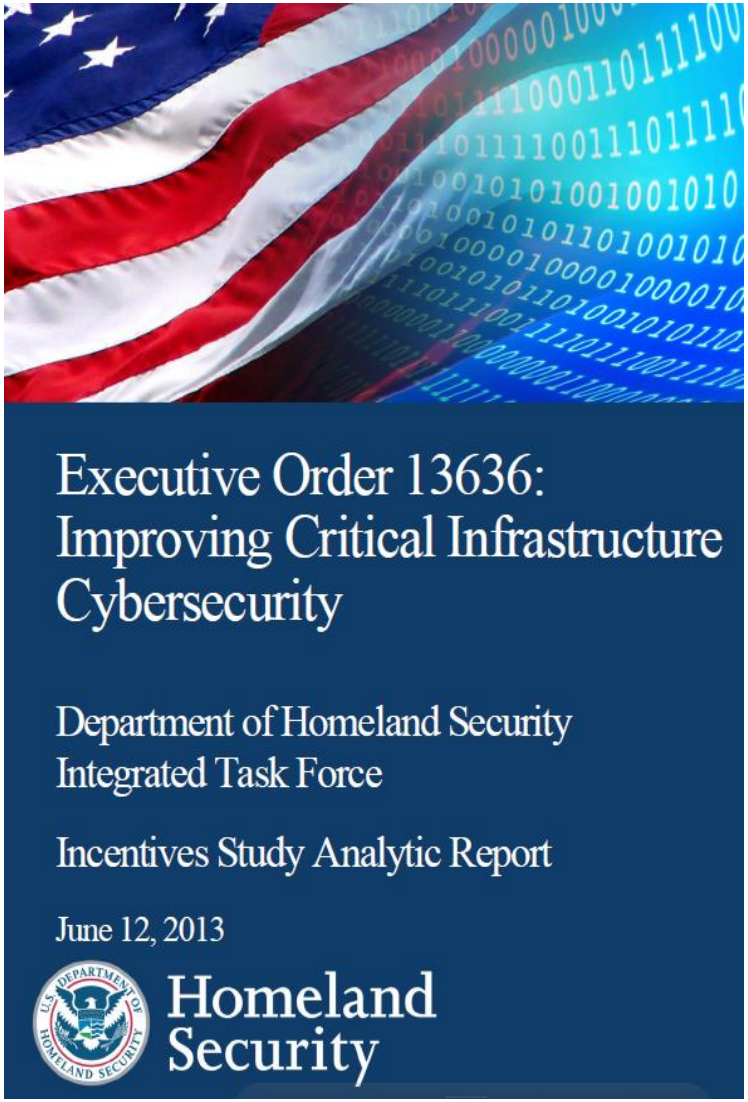
https://en.wikipedia.org/wiki/SCADA

- IoT & ICS search engines





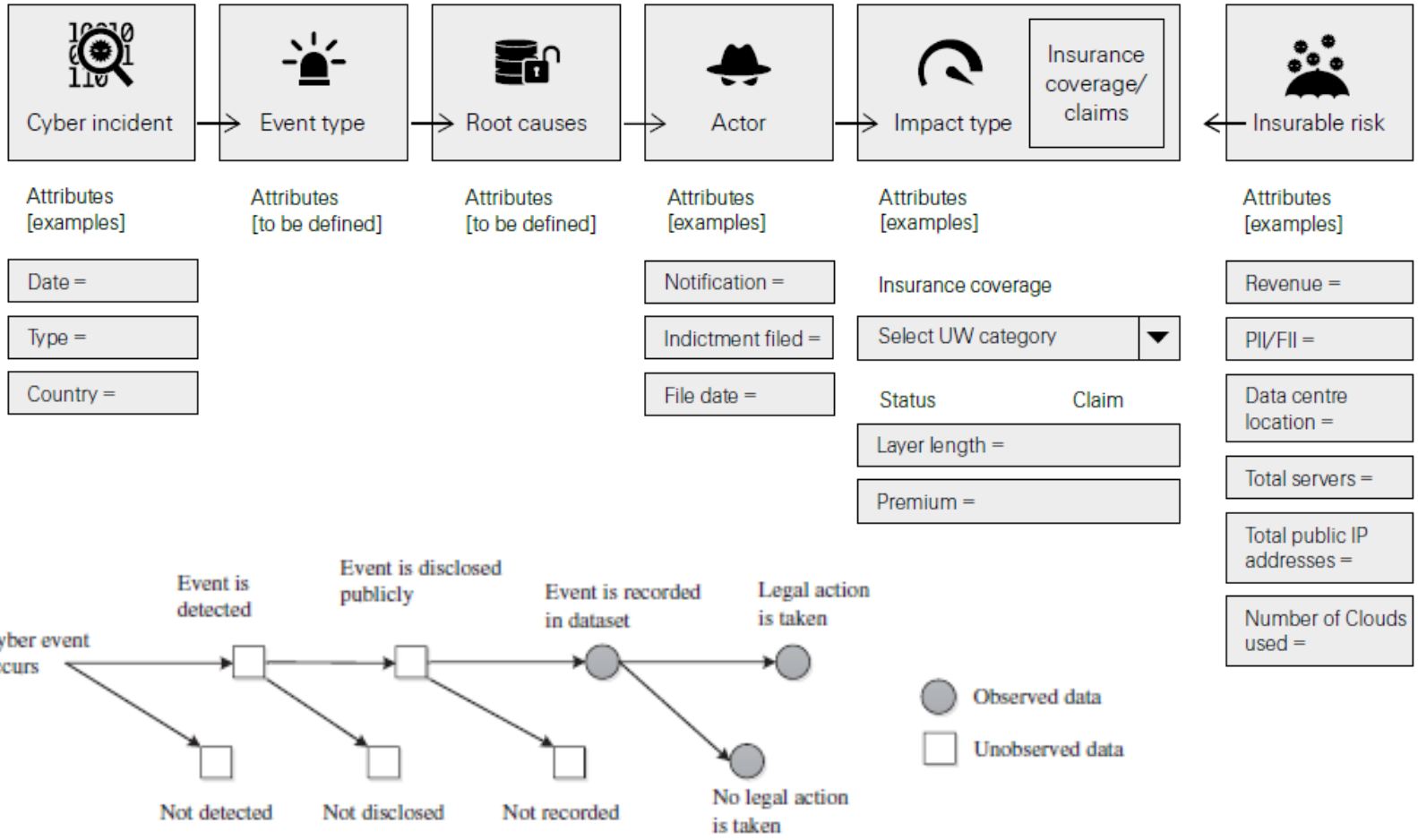
NIS Directive & ExO 13636 – Recommendations & incentives for cyber insurance



https://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Discussion_Final.pdf
https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
https://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf
http://www.bna.com/the-potential-effect-of-executive-order-13636-on-cybersecurity-insurance-coverage/
https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

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	Computer Malware, widespread Virus	Human Error	System Failure
	frequency estimate	frequency estimate	frequency estimate	frequency estimate
	events per year	events per year	events per year	events per year
	freq.estimate per outsourcing provider	freq.estimate per outsourcing provider	freq.estimate per outsourcing provider	freq.estimate per outsourcing provider
	events per year	events per year	events per year	events per year
	Probability	**Probability**	**Probability**	**Probability**
+ Privacy Breach: PII data affected				
+ Data Breach: non-PII 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				
+ Payment of Extortion Ransom				
+ Crisis management Fees				
+ other BI				
+ Extortion due to unknown threat				
+ other target affected through Insured's network				
+ Media Liability Issue				

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

Data Comparison of Cyber incidents & claims publications – predominantly US

CYBER LIABILITY
INSURANCE PAYS

Highlights from NetDiligence® 2016 Cyber Claims Study

2016 Cost of Data Breach Study
Global Analysis

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

IBM

Journal of Cybersecurity Advance Access published August 25, 2016

JOURNAL OF CYBERSECURITY

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

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)

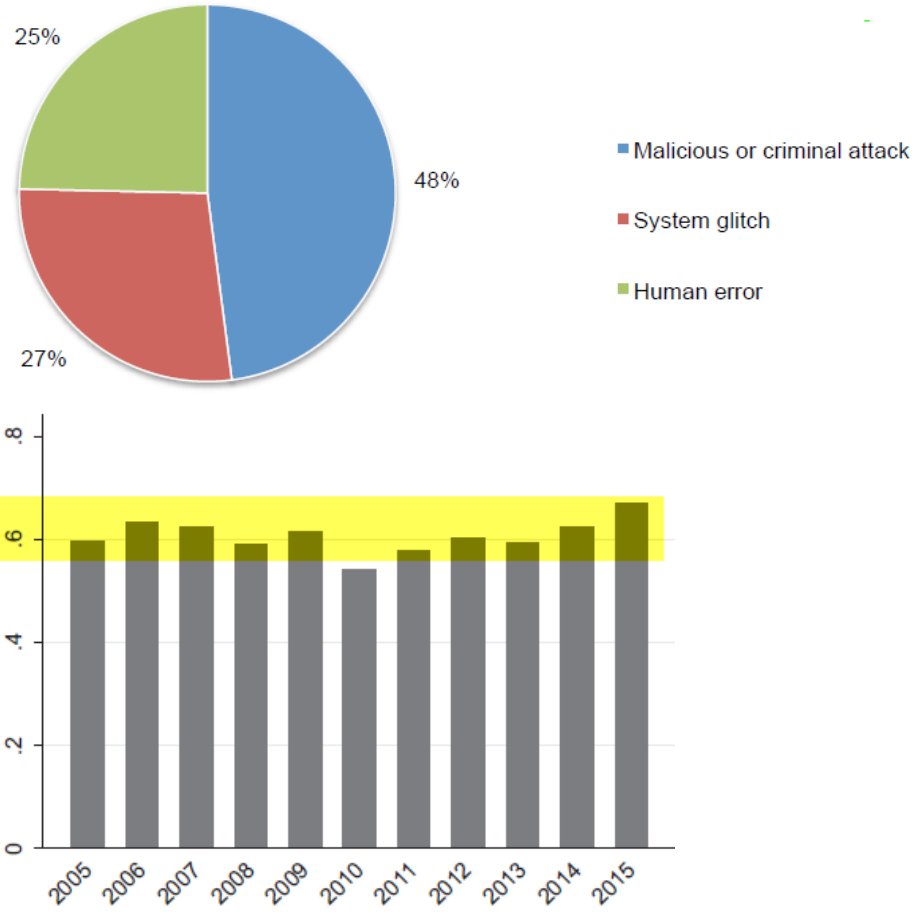
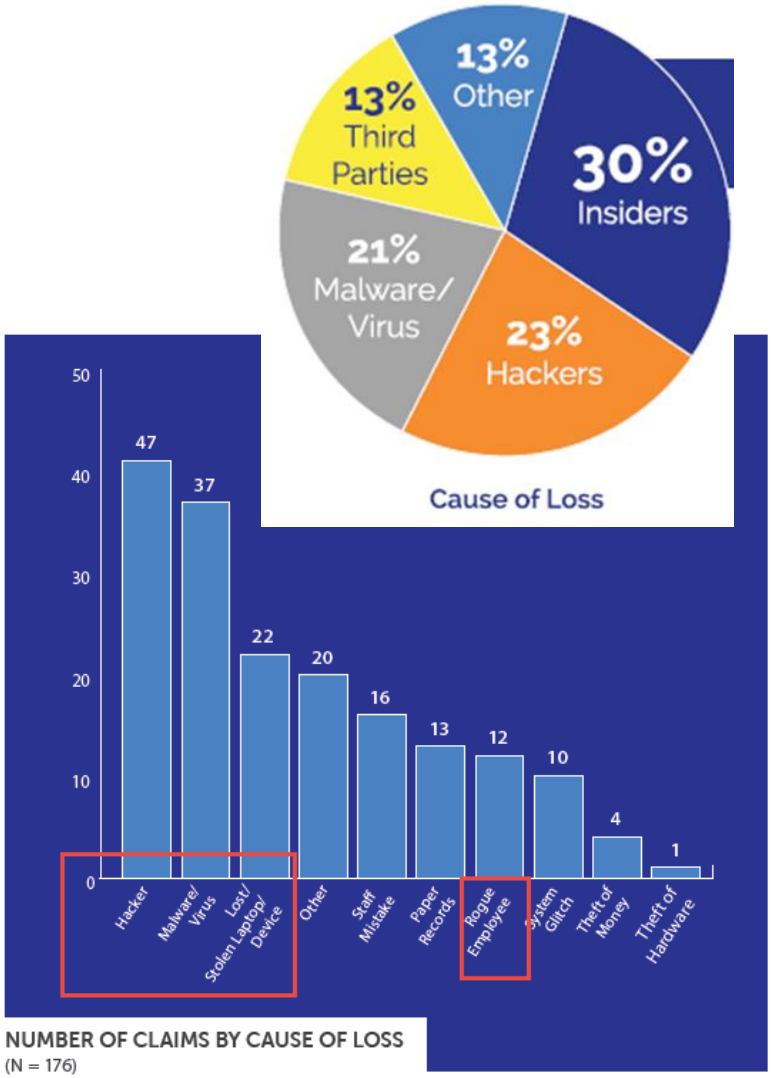


Figure 5. Rates of malicious events.



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 2014=$3.50
*Historical data is not available in all years
(FY 2016=383, FY 2015=350, FY 2014=315)
Measured in US$ (millions)

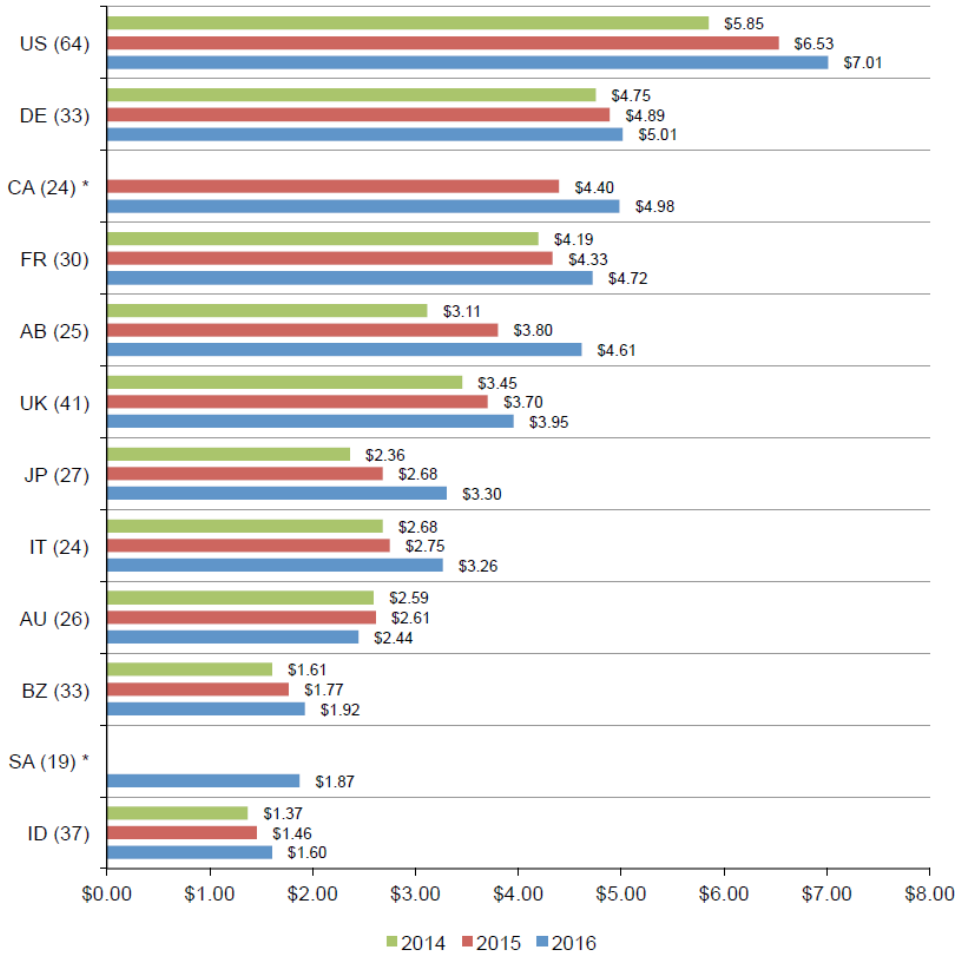
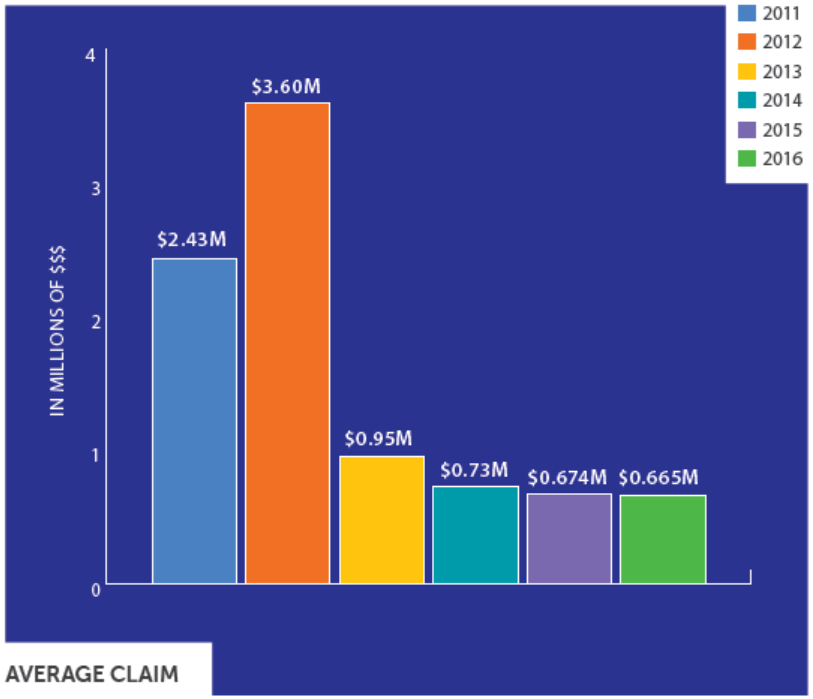


Table 2. Cost by event type (in millions)

Event type	N	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.



SCOR
The Art & Science of Risk

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!!

66% of the claims in the dataset reported both the number of records lost and the total breach cost. The minimum cost per record was $0.03 and the maximum cost per record was $1.6M. The **average cost per record was $17K,** while the median cost was $39.82.

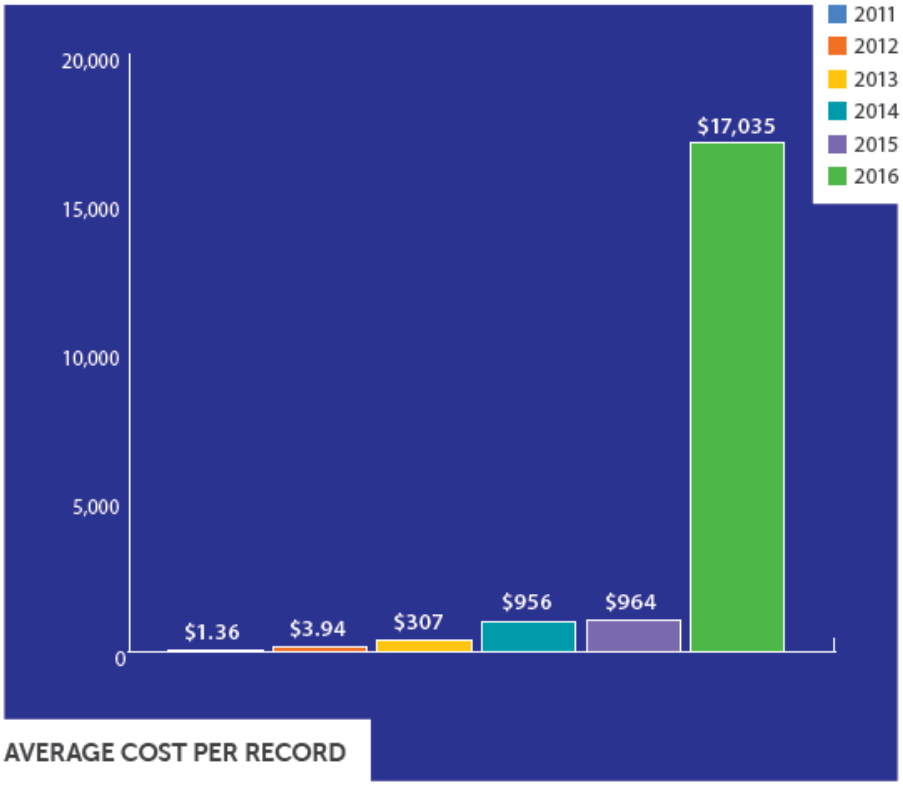
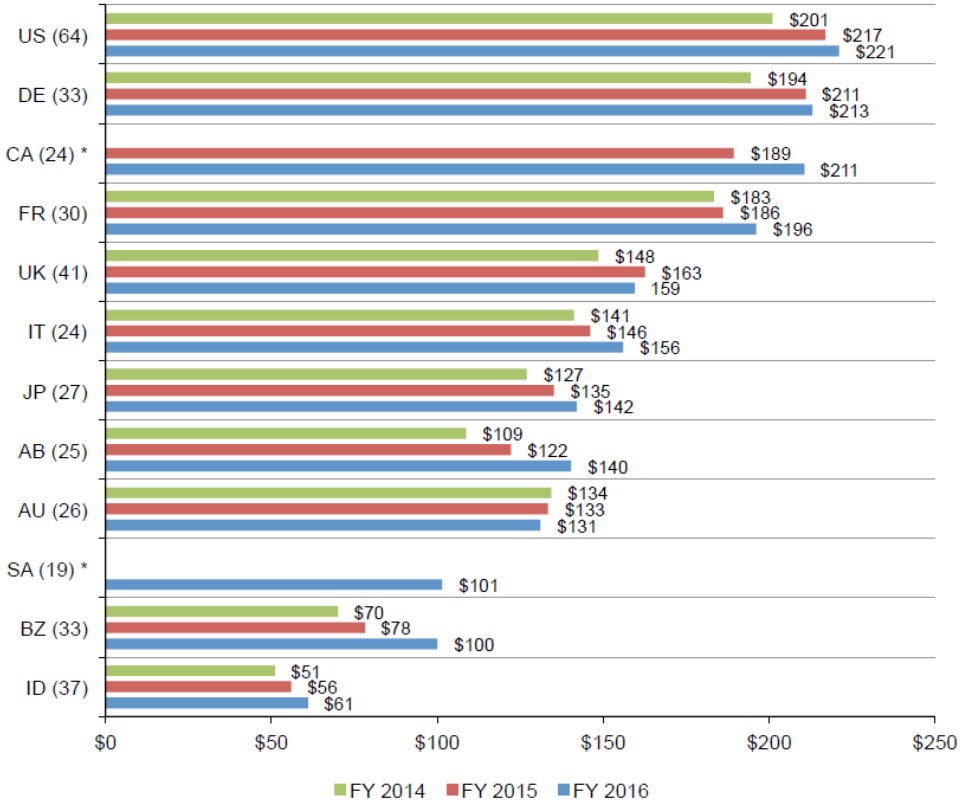
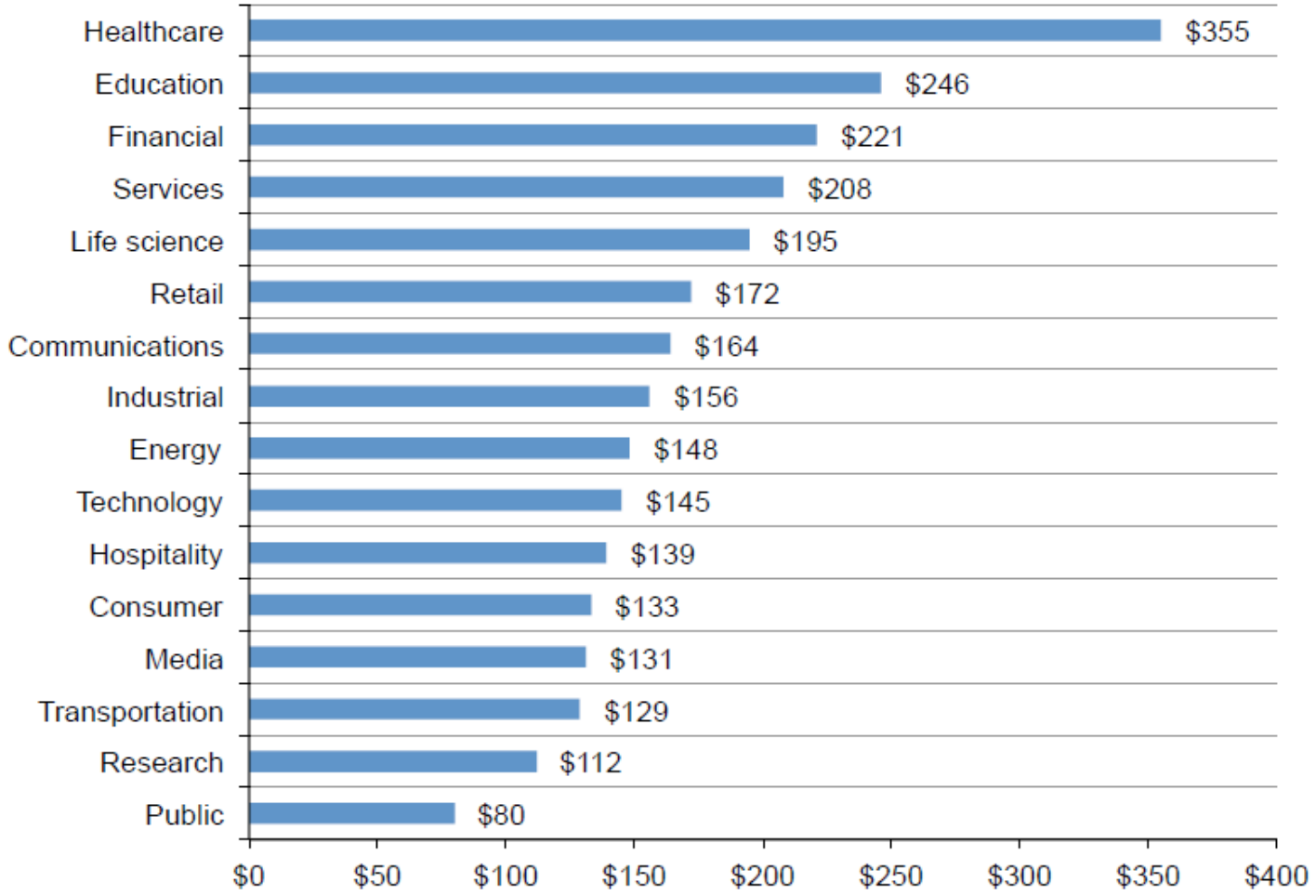


Figure 1. The average per capita cost of data breach over three years
Grand average for FY 2016=$158, FY 2015=$154, FY 2014=$145
*Historical data is not available in all years
(FY 2016=383, FY 2015=350, FY 2014=315)
Measured in US$



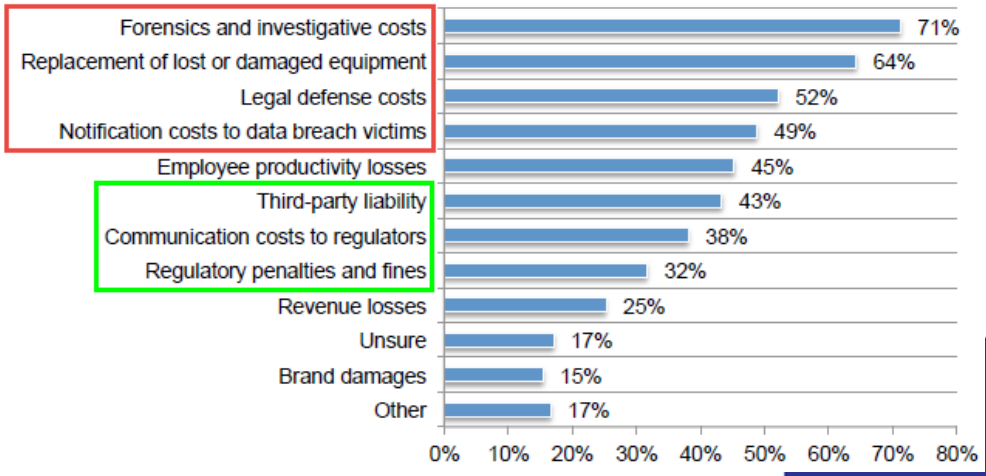
Ø cost / **record** per industry sector

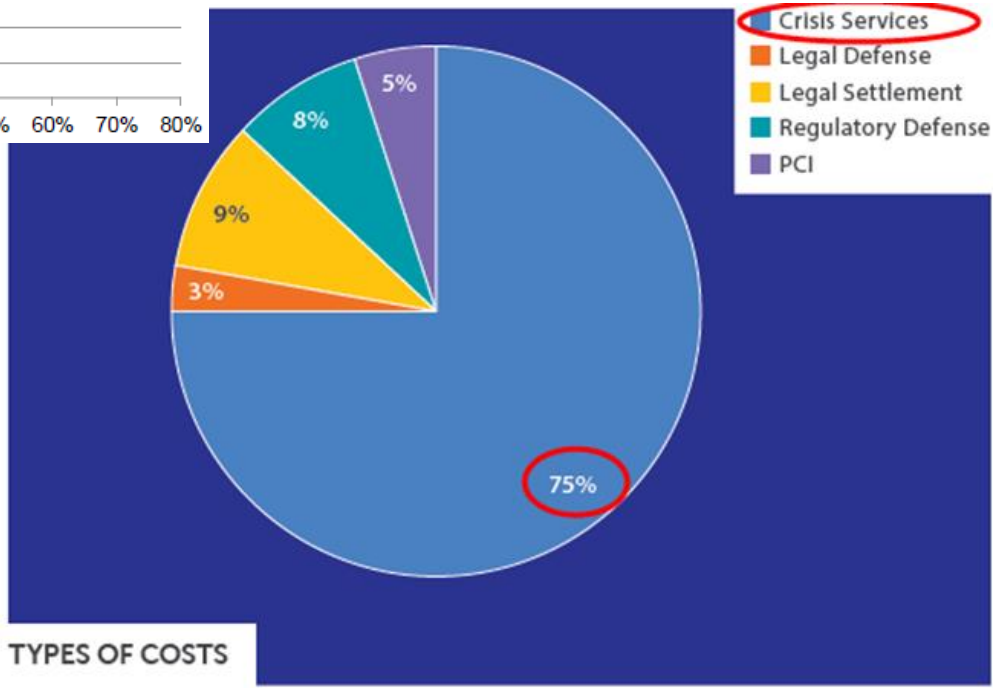
Figure 4. Per capita cost by industry classification
Consolidated view (n=383), measured in US$



Cost split of a cyber claim

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





2015 Global Cyber Impact Report

Sponsored by Aon Risk Services
Independently conducted by Ponemon Institute LLC
Publication Date: April 2015

AON Ponemon INSTITUTE

Crisis cost / event

for Crisis Services was $290, while the largest claim was $7.1M. The **average for Crisis Services was $357K.** The median was $43K.

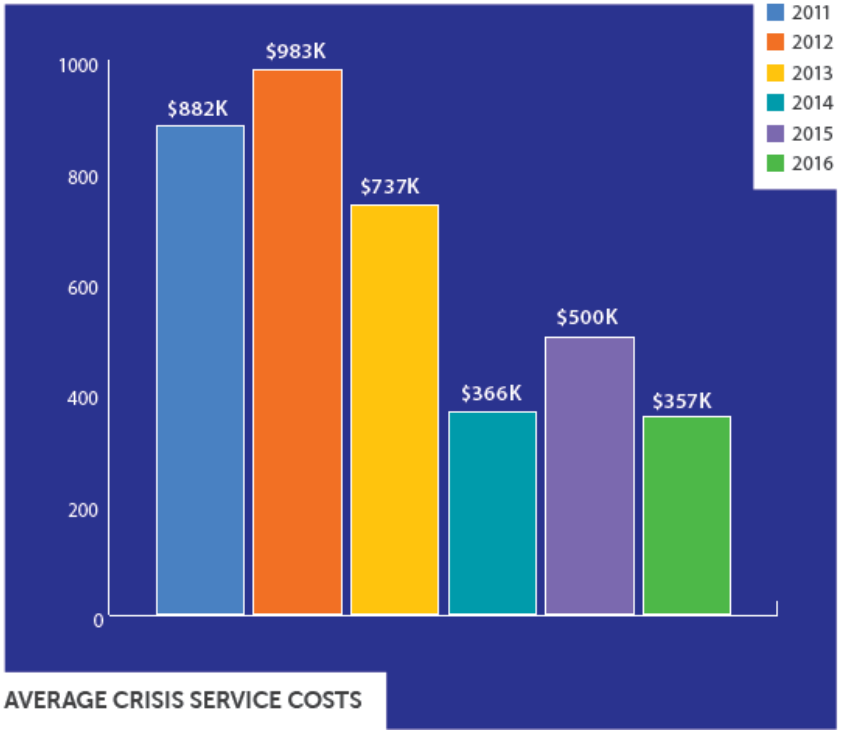
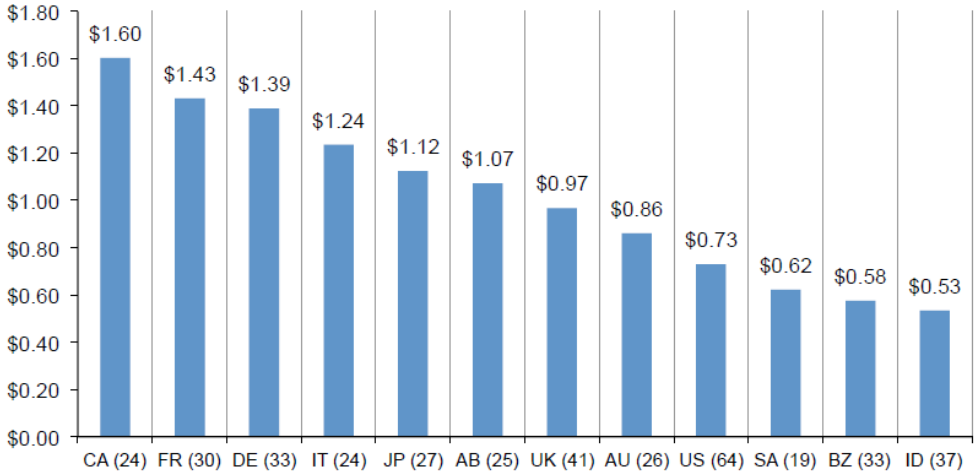
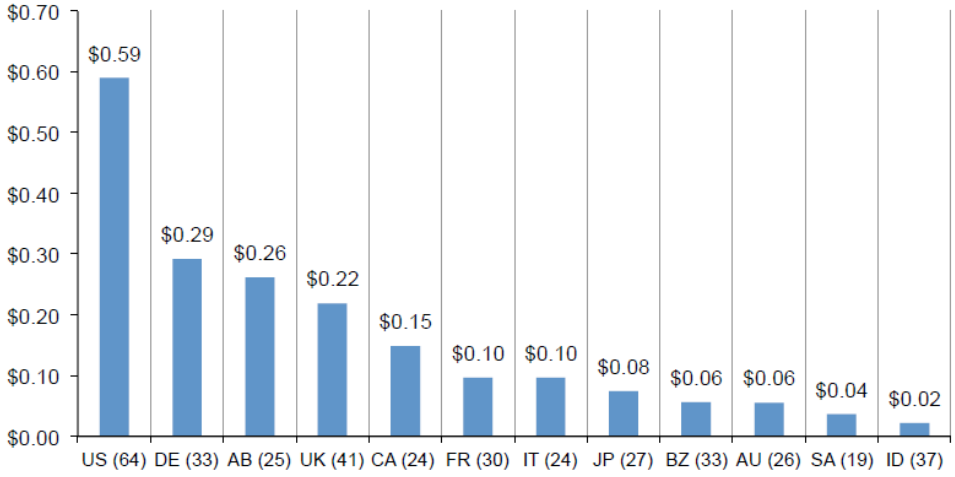


Figure 13. Detection and escalation costs
(n = 383), Measured in US$ (millions)

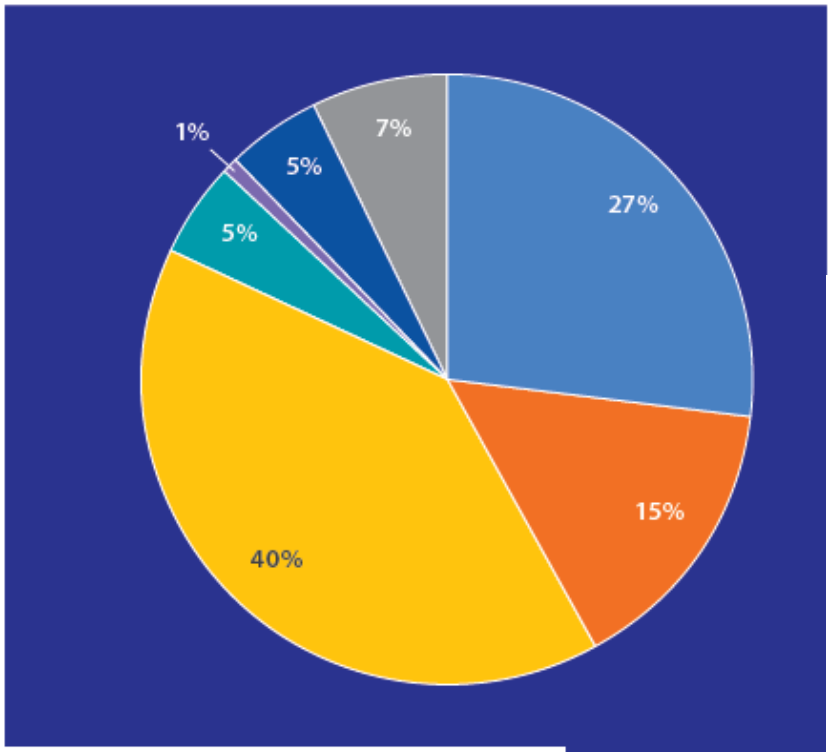


Notification costs were the highest in US. Notification-related include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication set-up. By far, notification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

Figure 14. Notification costs
(n = 383), Measured in US$ (millions)



Cyber claim (event) by data type



PERCENTAGE OF CLAIMS BY DATA TYPE
(N = 176)

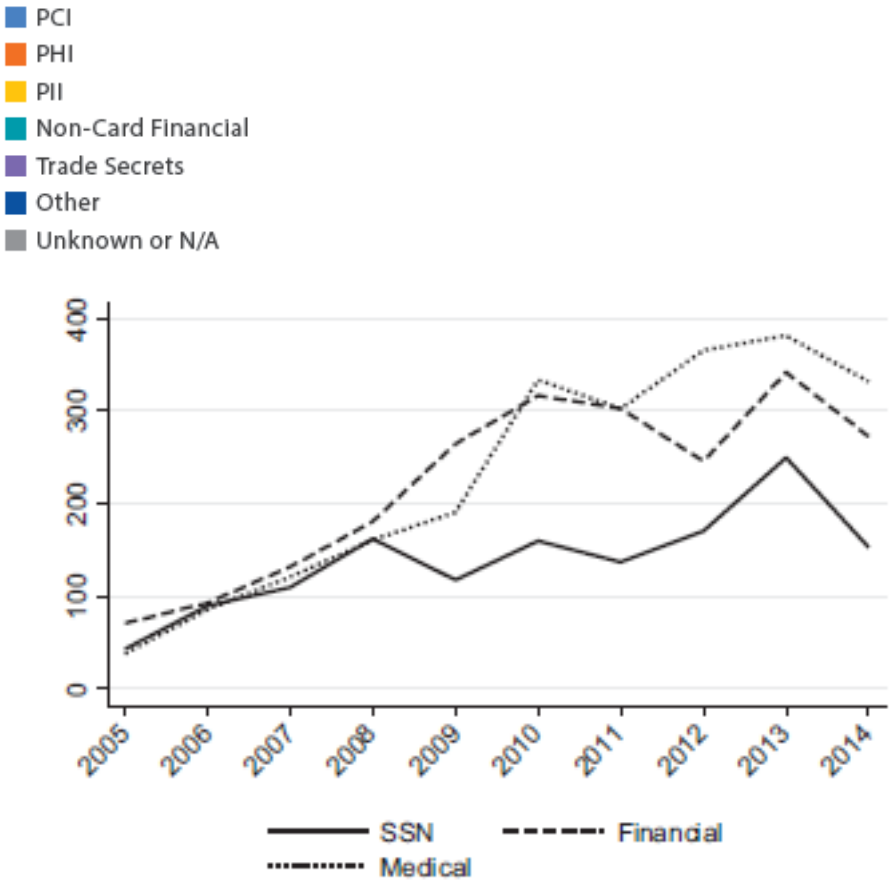


Figure 4. Cyber events by type of information compromised.

Claim (event) frequency by industry sector

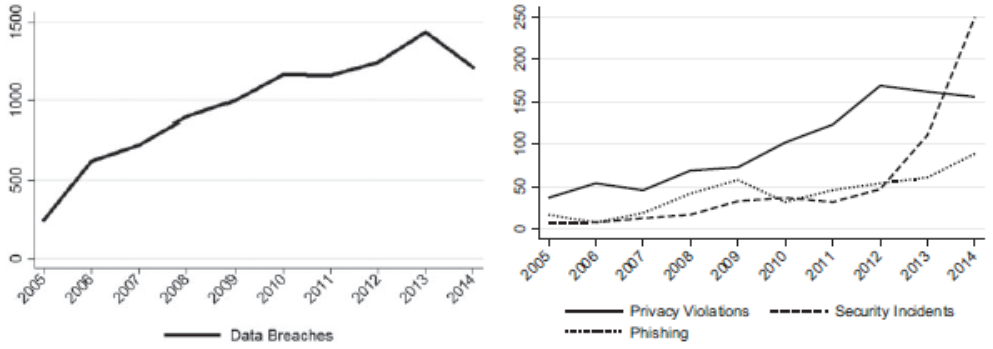


Figure 2. Four types of cyber events.

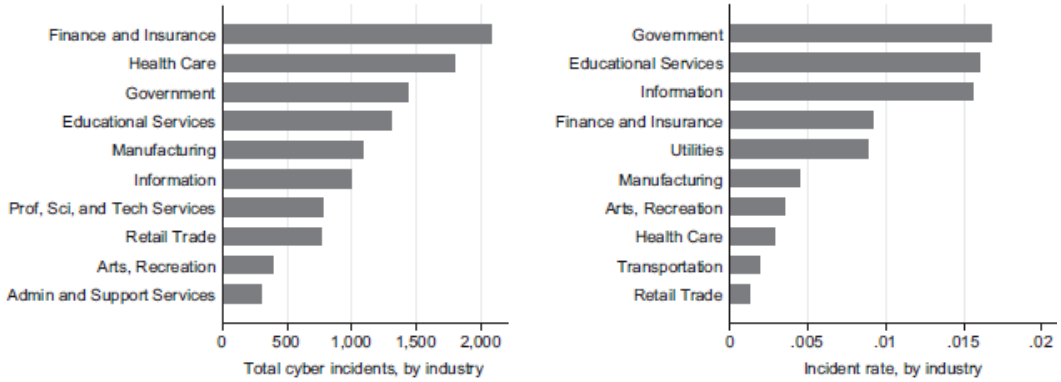
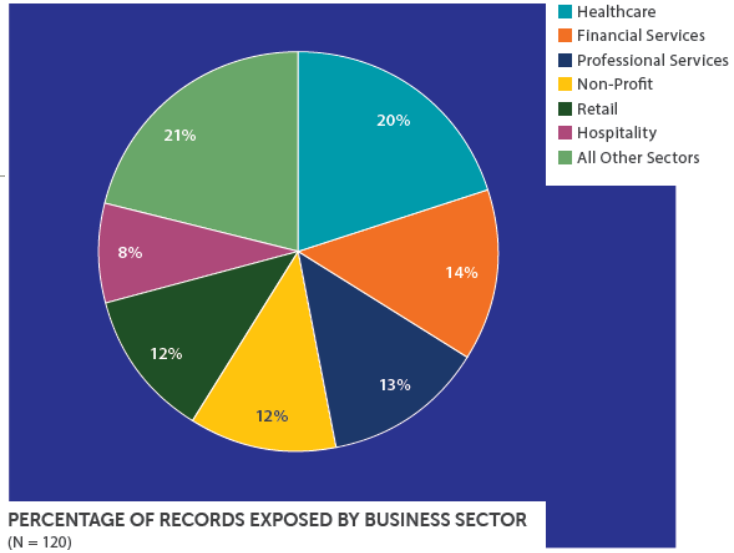
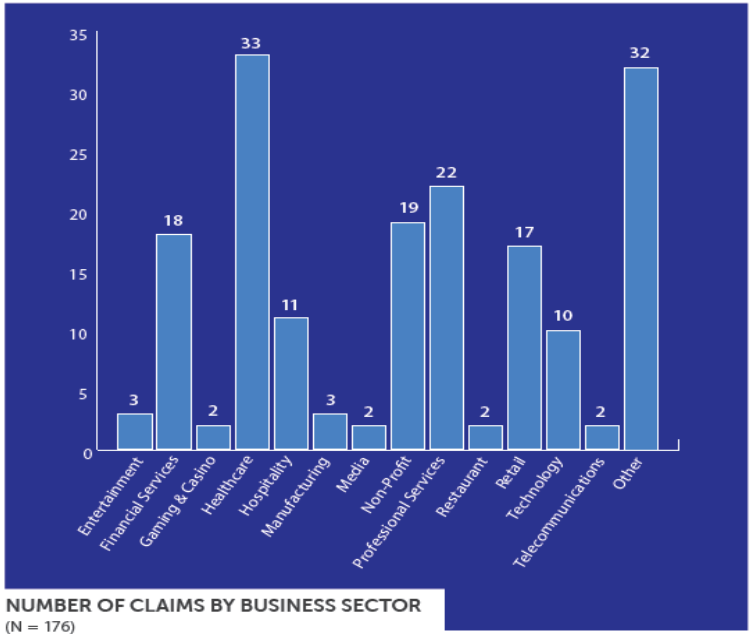


Figure 3. Cyber incidents, and rates, by industry.



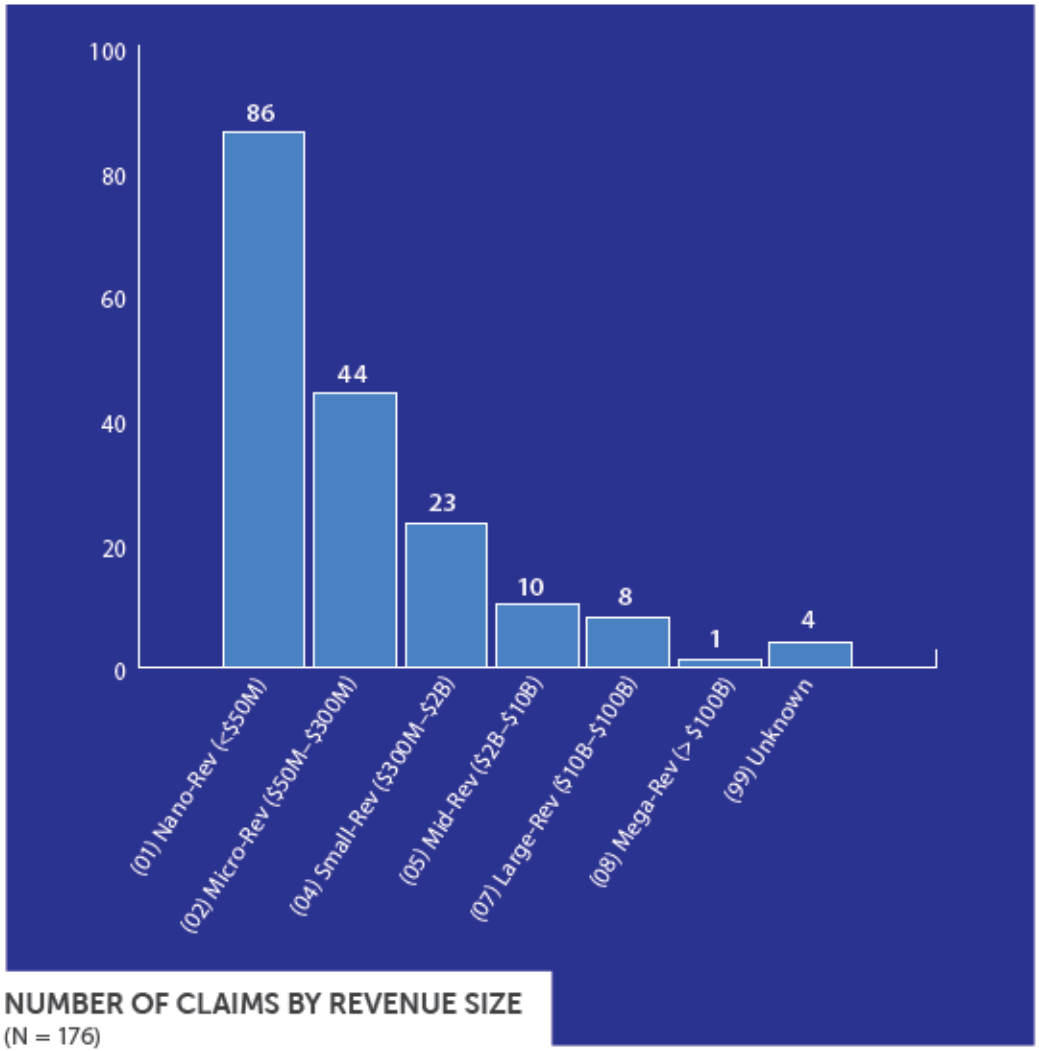


D.B.: disclosure of PII, theft of computers, identity theft, fraud

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



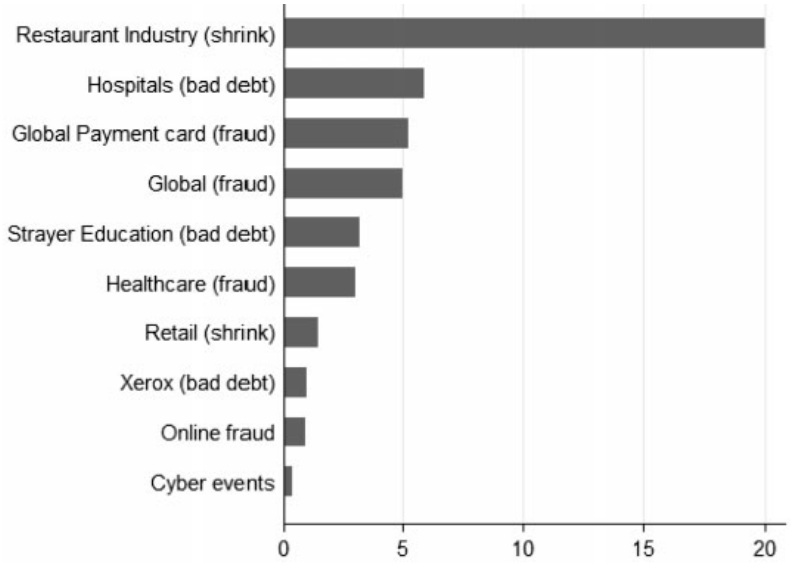


Figure 15. Loss as a percentage of revenues.

Exempels from the US market

PHARMACY BENEFITS MANAGEMENT COMP

Revenue: $4 billion
Limit: $5 million
Premium: $84,000

INDUSTRY: HEALTHCARE

Revenue: $25 million
Limit: $1 million
Premium: $12,900

INDUSTRY: HEALTHCARE, SOCIAL WORKER

Revenue: $120,000
Limit: $1 million
Premium: $859

INDUSTRY: EDUCATION

Revenue: $25 million
Limit: $1 million
Premium: $6,000

INDUSTRY: FINANCIAL

Revenue: $100 million
Limit: $1 million
Premium: $37,000

IT SOLUTIONS INTEGRATOR

Revenue: $200 million
Limit: $5 million
Premium: $41,500

SAAS PROVIDER

Revenue: $750,000
Limit: $10 million
Premium: $29,800

IT CONSULTING & DATA HOSTING PROVIDER

Revenue: $1.5 million
Limit: $2 million
Premium: $3,643

HEALTHCARE SAAS PROVIDER

Revenue: $2 million
Limit: $2 million
Premium: $9398

HEALTHCARE PROVIDER/CONSULTING/PROJECT MANAGEMENT

Revenue: $4.5 million
Limit: $5 million
Premium: $34,600

DOCTOR'S OFFICE

Revenue: $1.7 million
Limit: $1 million
Premium: $1800

SAAS PROVIDER

Revenue: $3 million
Limit: $2 million
Premium: $6000

FAST FOOD

Revenue: $15 million
Limit: $1 million
Premium: $9000

HOSPITAL

Revenue: $170 million
Limit: $5 million
Premium: $42,000

DATA STORAGE CENTER

Revenue: $15 million
Limit: $20 million
Premium: $120,000

https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/

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 aggregate)	Total Gross Revenue								
	Up to GBP 1,000,000		GBP 1,000,001 to GBP 2,500,000		GBP 2,500,001 to GBP 5,000,000		GBP 5,000,001 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 Revenue	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 ☐

https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Financial-lines/Cyber/aig-cyber-dec-2-0-brochure.pdf

Take-home message

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

Q & A ?