

ZAŠTO NAM UOPĆE TREBA INFORMACIJSKA SIGURNOST? (RAZLOZI ZA UVOĐENJE ISO 27001)

Igor Liščić
Voditelj informacijske sigurnosti
Raiffeisen Bank Austria d.d.

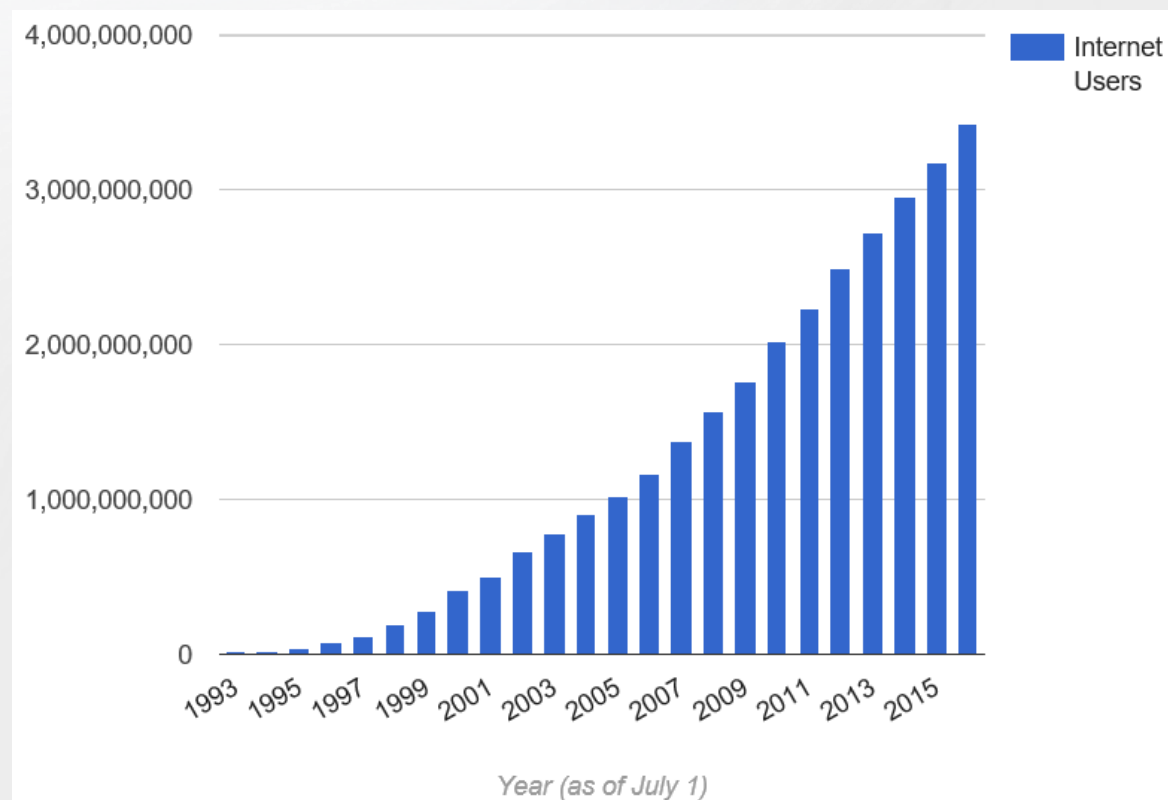
Uvod

- **Svrha** – ukazati na važnost sustavnog pristupa problematici informacijske sigurnosti u poduzeću primjenom međunarodne norme ISO 27001:2013
 - Razvoj informatičkih tehnologija
 - Prijetnje poslovanju povezane s razvojem informatičkih tehnologija
 - Posljedice realizacije prijetnji
 - Zaključak

Informatička revolucija

III Zakon termodinamike:

"U zatvorenom sustavu, entropija (mjera neuređenosti), raste ili ostaje ista, odnosno ne može padati".



Danas preko 40% svjetske populacije ima pristup internetu.

1995 je taj iznos bio manji od 1 %

Izvor:

<http://www.internetlivesstats.com/internet-users/>

Informatička revolucija

- **Krivulja udvostručenja ukupnog svjetskog znanja (Knowledge Doubling Curve)**
 - Trenutno vrijeme udvostručenja je **13** mjeseci (2013 godina)
 - Procjena je da će se ovo vrijeme smanjiti na 12 sati
- **Za primjer**
 - Oko 1900 godine – za udvostručenje količine znanja trebalo je 100 godina
 - Oko 1945 godine trebalo je **25** godina

Izvor: Industry Tap written by David Schilling, 2013

Razvoj informacijskih tehnologija i povezanih usluga

1. Umjetna inteligencija i strojno učenje
- 2. Inteligentne aplikacije**
- 3. Inteligentne naprave**
4. Virtualna stvarnost
5. Digitalni blizanci
6. "Blockchain" i distribuirane glavne knjige
7. Sustavi konverzacije
- 8. Mrežna arhitektura aplikacija i servisa**
9. Digitalne tehnološke platforme
10. Adaptivna sigurnosna arhitektura

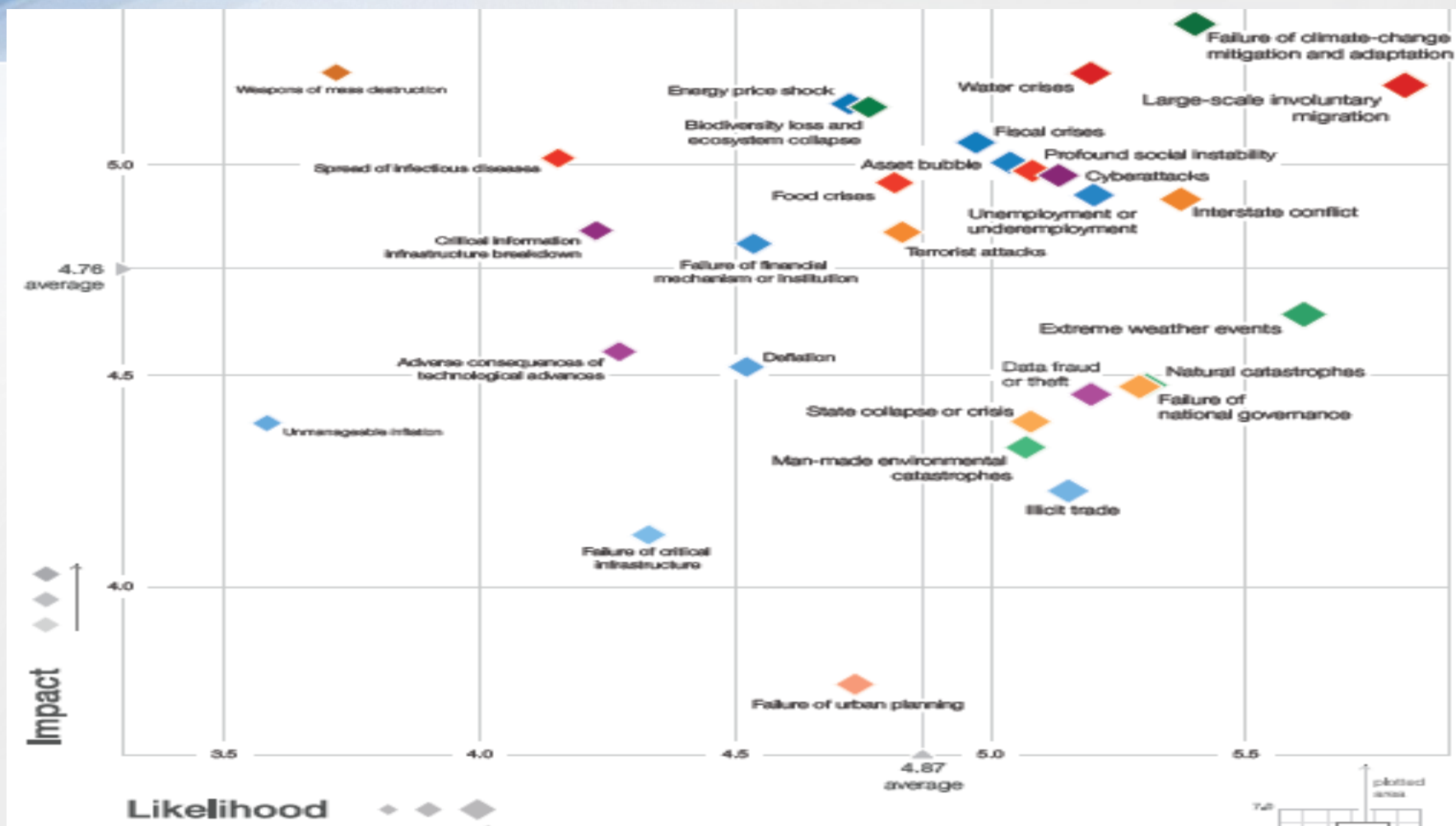
Top 10 Strategic Technology Trends for 2017, GARTNER, listopad 2016

Posljedice informatičke revolucije

- ❖ Snažan utjecaj informatizacije na svako poduzeće, neovisno o:
 - Veličini,
 - Djelatnosti,
 - Području djelovanja

- ❖ Utjecaj se odnosi na:
 - Financije,
 - Prodaju i marketing,
 - Operacije

Prijetnje poslovanju – globalni pogled



The Global Risks Report 2016, World Economic Forum

Prijetnje poslovanju – pogled poduzeća

<i>Prijetnja</i>	<i>Poredak</i>		<i>Izrazito zabrinuti (%)</i>		<i>Uopće ih ne brine (%)</i>	
	<i>2013</i>	<i>2016</i>	<i>2013</i>	<i>2016</i>	<i>2013</i>	<i>2016</i>
Neplanirani ispadi IT i telekomunikacija	1	3	27%	35%	4%	4%
Gubitak (krađa) podataka	2	2	26%	41%	8%	4%
Cyber napad	3	1	25%	48%	7%	2%
Gubitak opskrbe energijom	4	6	15%	16%	15%	10%
Vremenske nepogode (uragan, tsunami)	5	8	13%	14%	13%	15%
Sigurnosni incident	6	5	12%	17%	15%	10%
Požar	7	>10	11%	-	20%	-
Urušavanje lanca opskrbe	8	7	10%	16%	17%	18%
Terorizam	9	4	9%	19%	25%	14%
Ekolološki incident	10	10	9%	11%	22%	20%

BCI Horizon Scan - Survey Report 2013, BCI Horizon Scan - Survey Report 2016
Uzorak od 730 poduzeća iz 62 države

Prijetnje poslovanju – tehnološki pogled

BIG NUMBERS

BREACHES



Total Breaches

2013	2014	2015
253	312	318
–	+23%	+2%



Breaches With More Than 10 Million Identities Exposed

2013	2014	2015
8	4	9
–	-50%	+125%



Total Identities Exposed

2013	2014	2015
552M	348M	429M
–	-37%	+23%



Average Identities Exposed per Breach

2013	2014	2015
2.2M	1.1M	1.3M
–	-49%	+21%



Median Identities Exposed per Breach

2013	2014	2015
6,777	7,000	4,885
–	+3%	-30%

Internet Security Threat ReportInternet Report - VOLUME 21, APRIL 2016, Symantec

Prijetnje poslovanju – tehnološki pogled

EMAIL THREATS, MALWARE AND BOTS

Overall Email Spam Rate

2013	2014	2015	
66%	60%	53%	
—	-6%pts	-7%pts	

Email Phishing Rate (Not Spear Phishing)

2013	2014	2015
1 in 392	1 in 965	1 in 1,846

Email Malware Rate (Overall)

2013	2014	2015
1 in 196	1 in 244	1 in 220



Number of Bots			
2013	2014	2015	
2.3M	1.9M	1.1M	
—	-18%	-42%	

New Malware Variants (Added in Each Year)

2014	2015
317M	431M
—	+36%



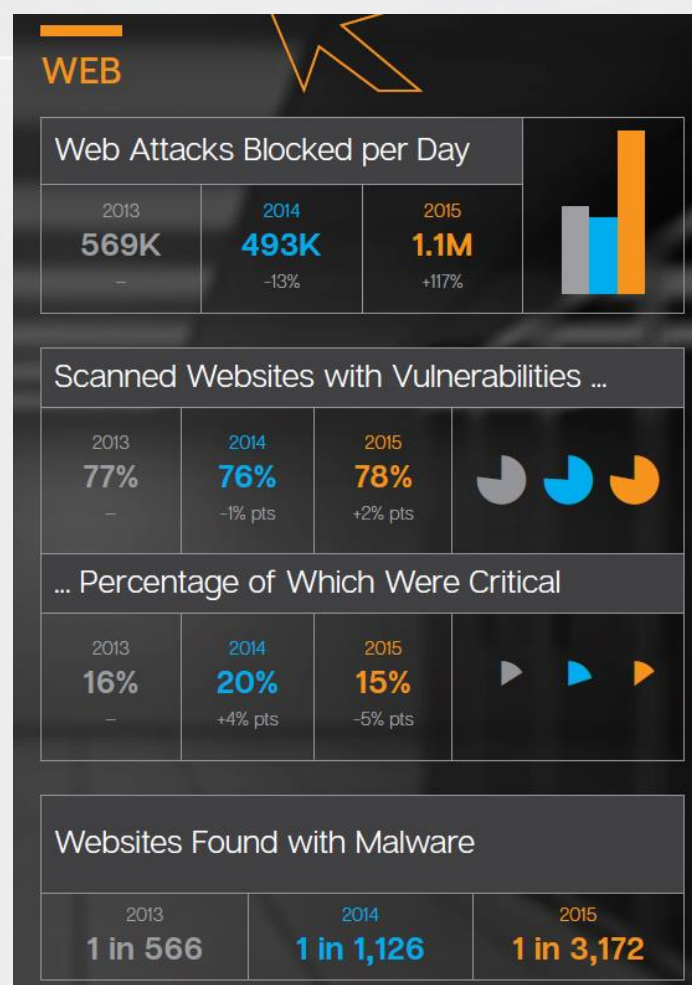
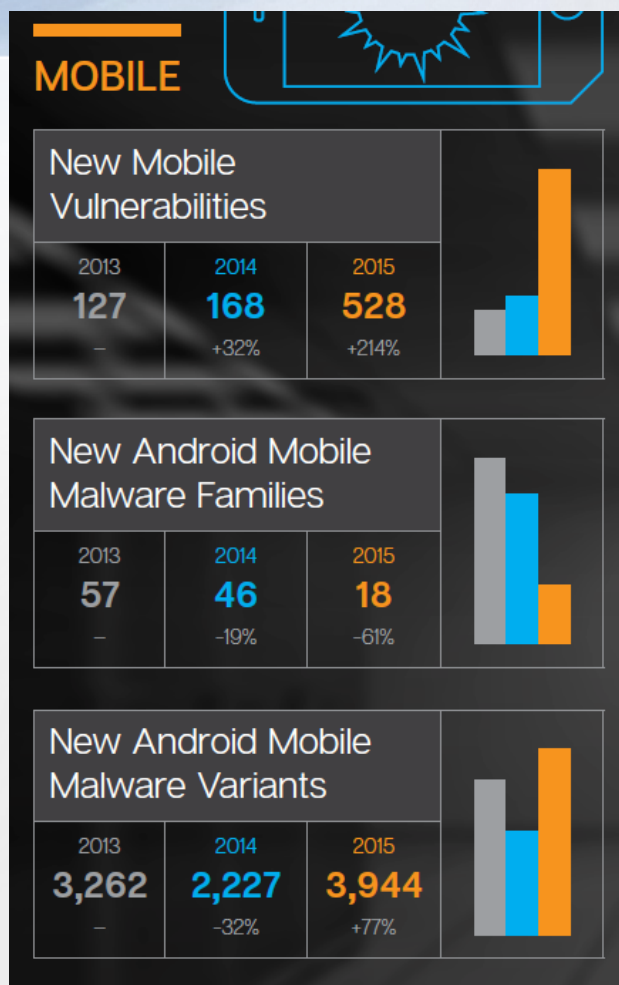
Crypto-Ransomware Total

2014	2015
269K	362K
—	+35%
Average Per Day	Average Per Day
737	992



Internet Security Threat ReportInternet Report - VOLUME 21, APRIL 2016, Symantec

Prijetnje poslovanju – tehnološki pogled



Internet Security Threat ReportInternet Report - VOLUME 21, APRIL 2016, Symantec

Prijetnje poslovanju – tehnološki pogled

VULNERABILITIES

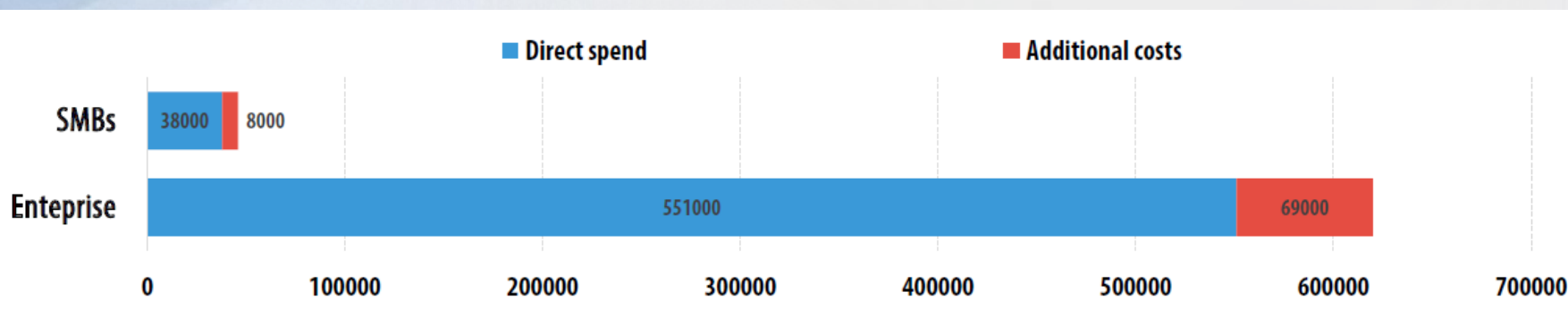


SPEAR-PHISHING (EMAIL TARGETED ATTACKS)

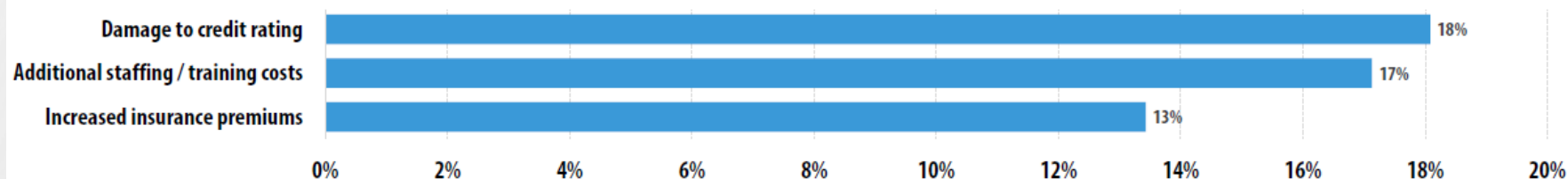


Internet Security Threat ReportInternet Report - VOLUME 21, APRIL 2016, Symantec

Gubici uslijed incidenata informacijske sigurnosti



- Top three major consequences of a breach:
 - Loss of access to business-critical information
 - Damage to company reputation
 - Temporary loss of ability to trade



*DAMAGE CONTROL: THE COST OF SECURITY BREACHES - IT SECURITY RISKS
SPECIAL REPORT SERIES, Kaspersky Lab, 2015*

Zakonski zahtjevi

- Naglasak kod poslovanja **s fizičkim osobama**:
 - Zakon o zaštiti osobnih podataka, Narodne novine" broj 106/12-pročišćeni tekst
 - DIREKTIVA (EU) 2016/680 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. (*Data Protection Directive*)
- Poslovanje s **pravnim osobama**:
 - Zakon o obveznim odnosima (NN 35/5) - *Čuvanje poslovne tajne, odgovornost za štetu....*

ZAKLJUČNO

- Posljedice incidenata informacijske sigurnosti:
 - 1) Financijski gubitak (odmah)
 - 2) Gubitak klijenata
 - 3) Gubitak ugleda
 - 4) Zakonske sankcije
- Stoga:

Potreba za sustavnim upravljanjem
informacijskom sigurnošću

Zahvaljujem na pažnji!

Pitanja?

Kontakt podaci:
Igor Liščić
igor.liscic@rba.hr
+385 99 365 93 38