CYBER OSIGURANJE – PROIZVOD ZA NOVU GENERACIJU RIZIKA

KREŠIMIR FRANČIĆ
Croatia osiguranje

IZVRSNOST UZ NOVE IZAZOVE

CYBER NAPADI SVE UČESTALIJI I „UČINKOVITIJI” – PROCJENA GODIŠNJIH IZNOSA ŠTETA, 445 MLRD. USD

Naslovna › Hrvatska › Cyber stručnjaci u HGK: 'Dnevno se bilježi i do sedam milijuna kibernetičkih...

Hrvatska

Cyber stručnjaci u HGK: 'Dnevno se bilježi i do sedam milijuna kibernetičkih napada'

11/24/2022

Pixabay

'HAKERSKI NAPAD NA INU pokrenut je iz Mađarske i zaključao je podatke o poslovanju potrebne Lazardu'

21. 03. 2020. 23:00 Autor: Sandra Carić Hercog

FOTO I PIXSELL

AVIOKOMPANIJA NA UDARU

NOVI VELIKI PROBLEMI USRED PANDEMIJE Hakerski napad na easyJet ugrozio podatke devet milijuna klijenata

Piše: Nina

Objavljeno: 19. svibanj 2020. 18:39

INSTITUCIJA NA UDARU

Izvršen kibernetički napad na HANFA-u: Ne može odgovarati na emailove, stranica joj je nedostupna

"U suradnji s nadležnim institucijama intenzivno radimo na otklanjanju posljedica napada", rekla je HANFA

Piše: B. R.

Objavljeno: 23. listopad 2014. 18:33

Crna Gora: Iza cyber napada stoji grupa Cuba Ransomware

Ministar javne uprave Maraš Dukaj kaže kako imaju potvrdu da iza napada u posljednjih 12 dana ne stoje individualci, nego prepoznata kriminalna grupa u cyber terorizmu.

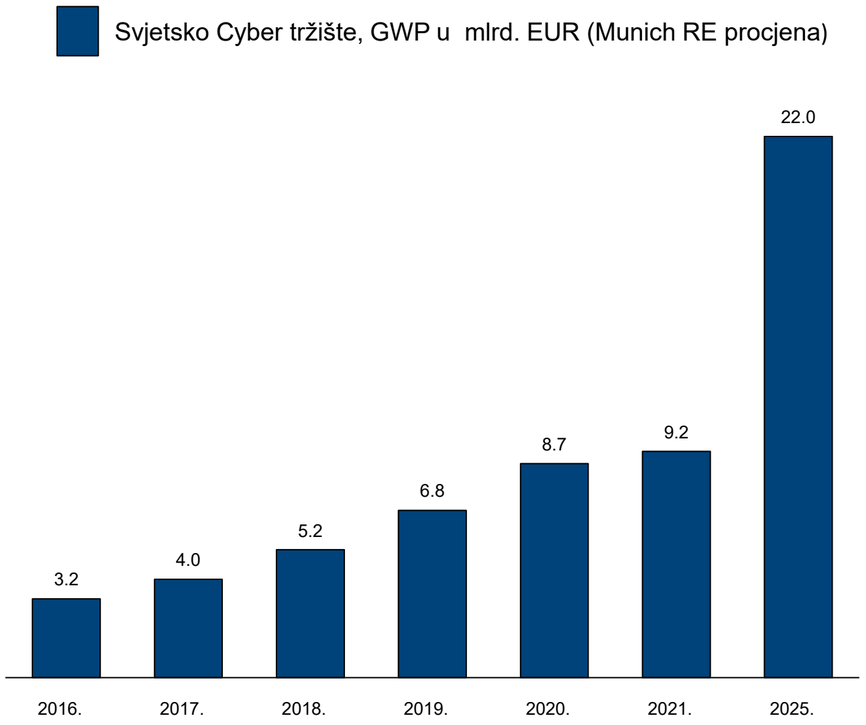
Home › Google News

Nino Krstačić · Google News, Novosti, Poslovanje · 22. srpnja 2022.

A1 dobio milijunska kaznu, zbog posljedica Cyber napada

IZVRSNOST UZ NOVE IZAZOVE

CYBER TRŽIŠTE RASTE KONTINUIRANO ZADNJA DVA DESETLJEĆA – PROCJENA CYBER TRŽIŠTA U 2022 IZNOSI 13 MLRD $



Country	Proportion of global premium income
US	62.5%
UK	9.3%
Canada	6.4%
Germany	6.1%
France	2.1%

Source: Guy Carpenter

Izvor: Munich Re / Geneva Association, AON Global Risk Management Survey 2022

IZLOŽENOST PREMA INDUSTRIJAMA I PREMA VELIČINI PRIHODA TVRTKI

Industry Sector Standard Industrial Classification (SIC)	Proportion of global premium income
Services	42.6%
Finance, Insurance and Real Estate	14.6%
Manufacturing	14.4%
Retail Trade	9.9%
Non-classifiable	8.0%

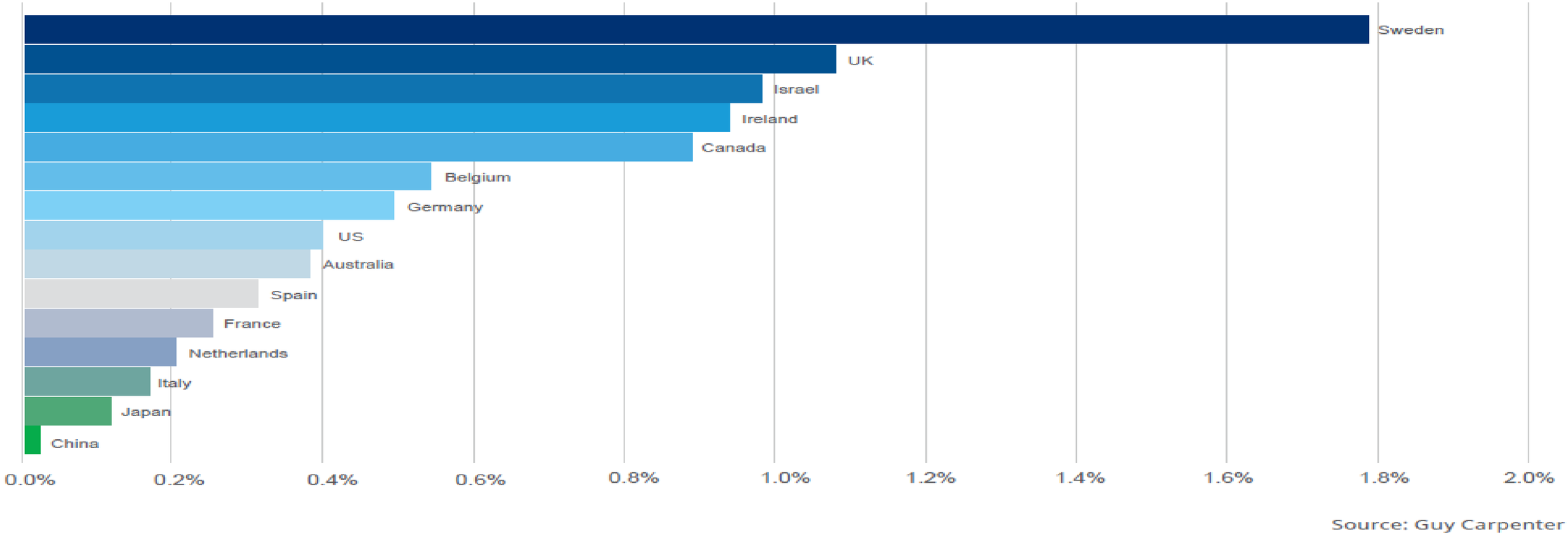
Source: Guy Carpenter

Organization Size	Proportion of global premium income	Revenue Band
Large	41.7%	USD 1 billion-plus
Medium	19.8%	USD 250 million to 1 billion
Small	26.8%	USD 10 million to 250 million
Micro	11.6%	0 to USD 10 million

Source: Guy Carpenter

✓ **Najviše se osiguravaju tvrtke iz uslužnih djelatnosti iz segmenta velikih tvrtki (prihod > 1 mlrd $)**

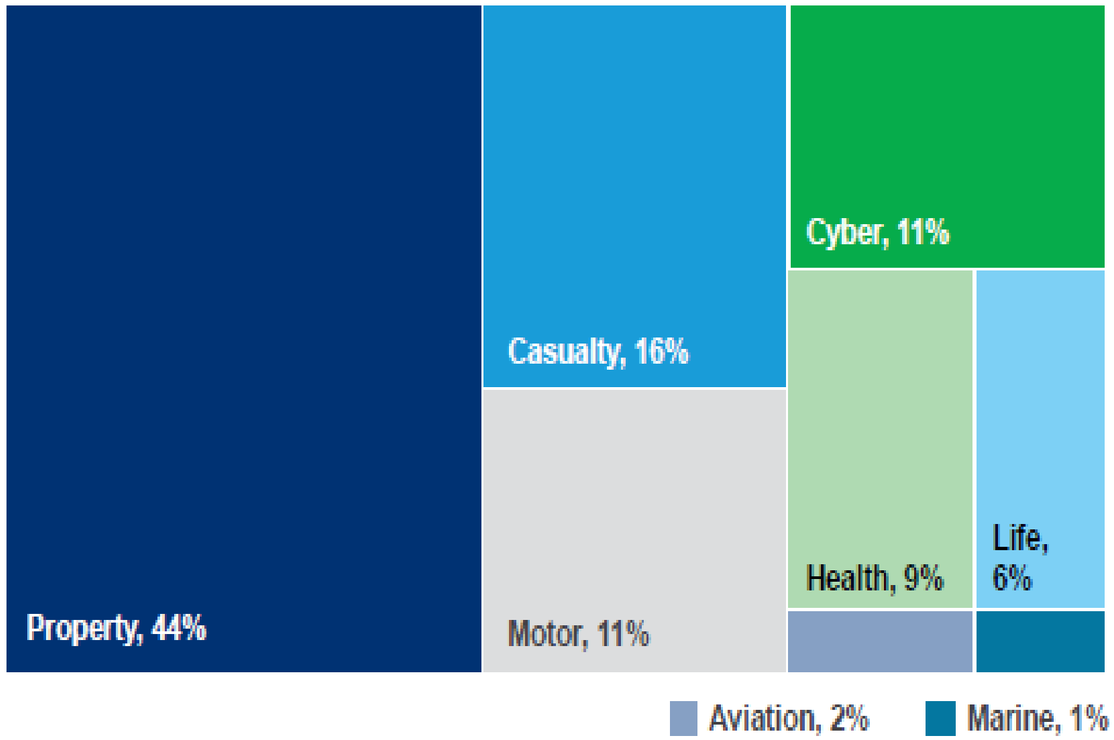
UDIO CYBER PREMIJE U UKUPNOJ NEŽIVOTNOJ PREMIJI OSIGURANJA PO POJEDINIM DRŽAVAMA



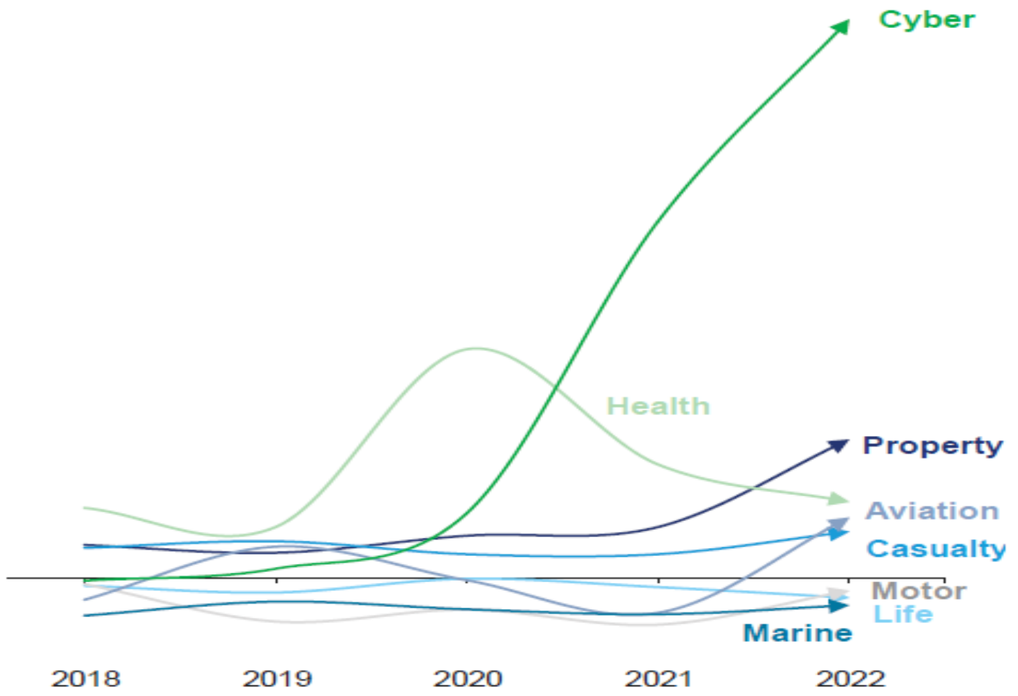
Source: Guy Carpenter

✓ **Cyber tržište preraslo „aviation” tržište, a očekuje se da će uskoro biti veće i od „marine” tržišta**

PREGLED „ZARADE” PREMA VRSTAMA OSIGURANJA



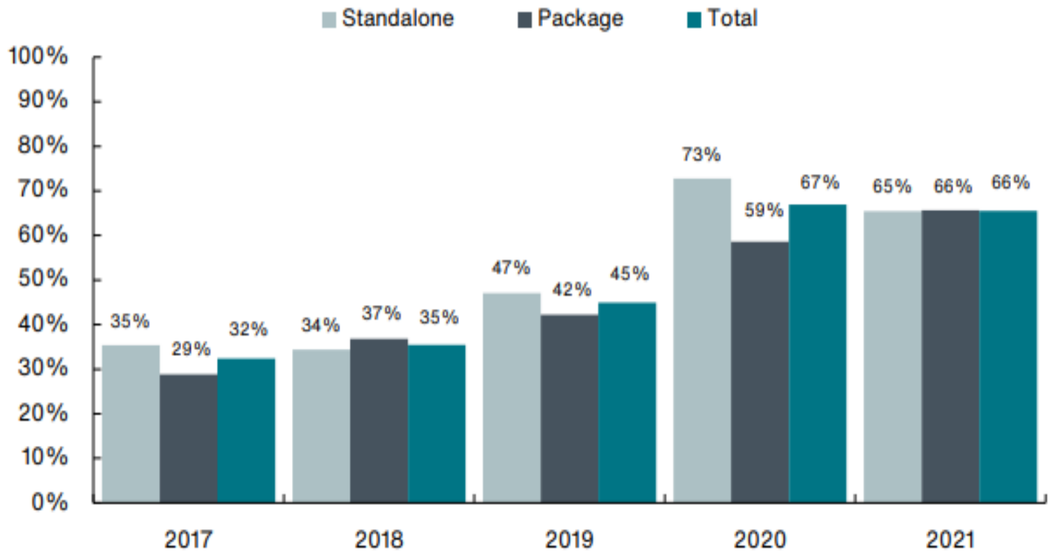
Source: Alpha Sense—Earnings conference call transcripts



Source: Alpha Sense—Earnings conference call transcripts

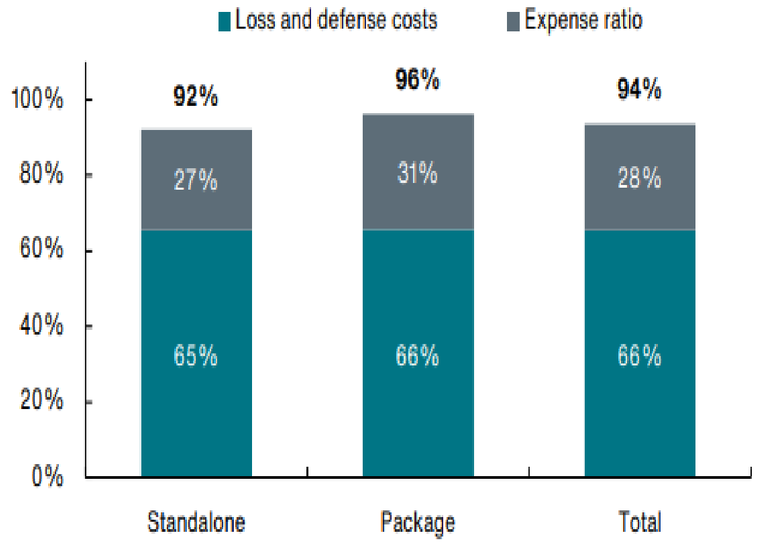
USA CYBER „LOSS RATIO”

Exhibit 4: U.S. Cyber loss ratio | 2017 – 2021



Izvor: AON (U.S. Cyber market Update)

Exhibit 7: Estimated 2021 U.S. Cyber combined ratios



Izvor: AON (U.S. Cyber market Update)

NOVA PRAVILA O CYBER SIGURNOSTI PREDSTAVLJAJU POTENCIJAL ZA DALJNJI RAST TRŽIŠTA OSIGURANJA U EU

Direktiva NIS 2, stupa na snagu u listopadu 2024.:

- ✓ **Modernizacija postojećeg pravnog okvira u svrhu odgovora na digitalizaciju i cyber prijetnje**
- ✓ **Proširenje područja primjene pravila o cyber sigurnosti na nove sektore/subjekte koji su ključni za gospodarstvo i društvo, a koji se u velikoj mjeri oslanjaju na informacijske i komunikacijske tehnologije: energetika, promet, voda, bankarstvo, zdravstvena skrb, digitalna infrastruktura, proizvodnja i dr.**
- ✓ **Obveza ključnih subjekata za ispunjenje minimalnih sigurnosnih zahtjeva u svrhu izbjegavanja cyber napada i zaštite kritične informacijske infrastrukture, poduzimanje propisanih tehničkih, operativnih i organizacijskih mjera za upravljanje rizicima**
- ✓ **Obveza država članica za donošenje nacionalnih strategija za cyber sigurnost, uspostava jedinstvenih kontaktnih točaka, timova za odgovor na računalne sigurnosne incidente (CSIRT-ovi) i dr.**

FINANCIJSKI, PROIZVODNI, IT I USLUŽNI SEKTORI NAJVIŠE SU U FOKUSU CYBER NAPADA

Najveća potreba za cyber osiguranjima dolazi iz industrija najviše pogođenima cyber napadima:

- **Financijski sektor**
- **Proizvodni sektor**
- **IT**
- **Servisne kompanije**
- **Uslužne djelatnosti**
- **Zdravstvo…**

OTKUDA DOLAZE NAJVEĆE PRIJETNJE

Unutarnje prijetnje:

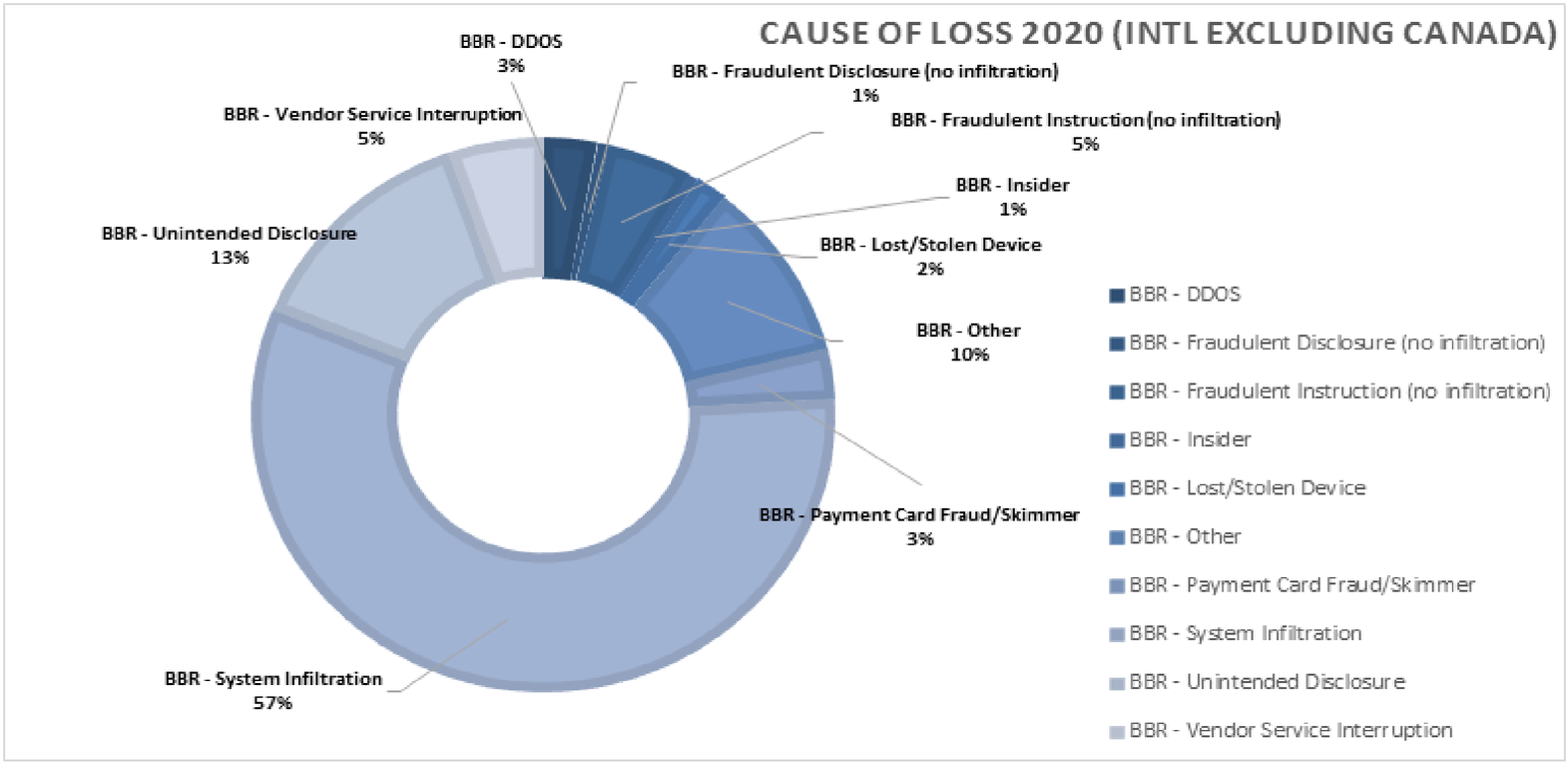
- Nemar zaposlenika:
  - Sigurnosni propusti
  - Izgubljeni prijenosni uređaji
  - Nenamjerna otkrivanja putem e pošte, telefona ili osobno
- Neuspješno šifriranje prijenosnih uređaja
- Neznanje zaposlenika
- Nepropisno odlaganje osobnih podataka
- Nedostatak obrazovanja i svijesti
- Zlonamjerni i/ili znatiželjni zaposlenici

Vanjske prijetnje:

- Hakeri:
  - Malware
  - Phishing and spear phishing
- Lopovi:
  - Alati društvenog inženjeringa
  - Ukradeni uređaji
- Dobavljači/poslovni partneri

Industry	Unintended Disclosure	Hack or Malware	Social Engineering
Healthcare	39%	19%	3%
Financial	22%	48%	12%
Education	27%	43%	9%
Retail	4%	53%	30%
Professional Services	12%	48%	21%
Hospitality	4%	74%	9%

PREGLED ŠTETA PREMA UZROKU



Izvor: Beazley 2020

OSIGURATELJNA POKRIĆA I ISKLJUČENJA U CYBER OSIGURANJU

First-party losses	▪ Troškovi prekida rada ▪ Troškovi obnove IT sustava, podataka ▪ Troškovi odnosa s javnošću ▪ Isplata iznude (extortion)…
Third-party losses-liability	▪ Naknada štete zbog povrede zaštite podataka (troškovi obrane, odšteta, kazne regulatora…)
Usluge prevencije i odgovora na incidente	▪ 24/7 podrška u slučaju cyber napada ▪ Troškovi IT forenzike…

REZULTAT ISTRAŽIVANJA TRŽIŠTA CYBER POLICA - USA TRŽIŠTE

- ✓ **Informacije u nastavku prezentacije dobivene su iz istraživanja koje je objavljeno 27.01.2019 godine u Journal of Cybersecurity, Volume 5, Issue 1, 2019, tyz002 (https://doi.org/10.1093/cybsec/tyz002)**
- ✓ **Analiza 235 dokumenata (iz New Yorka, Pennsylvanie i Kalifornije, veliki i manji osiguratelji) napravljena je u tri segmenta:**
  - **osigurateljna pokrića i isključenja,**
  - **upitnici za procjenu rizika i**
  - **način formiranja premijske stope koje se koriste za izračun premije osiguranja**
- ✓ **Napravljena je način da su se sva pokrića i isključenja kodirala i segmentirala - rezultat analize je evidentirano 17 pokrića i 58 isključenja.**

OSIGURATELJNA POKRIĆA U CYBER OSIGURANJU

„**First party“**

- ✓ **uključuje gubitke koje su se izravno dogodile osiguraniku,**
- ✓ **Primjer grupiranih pokrića s zajedničkim podlimitima**

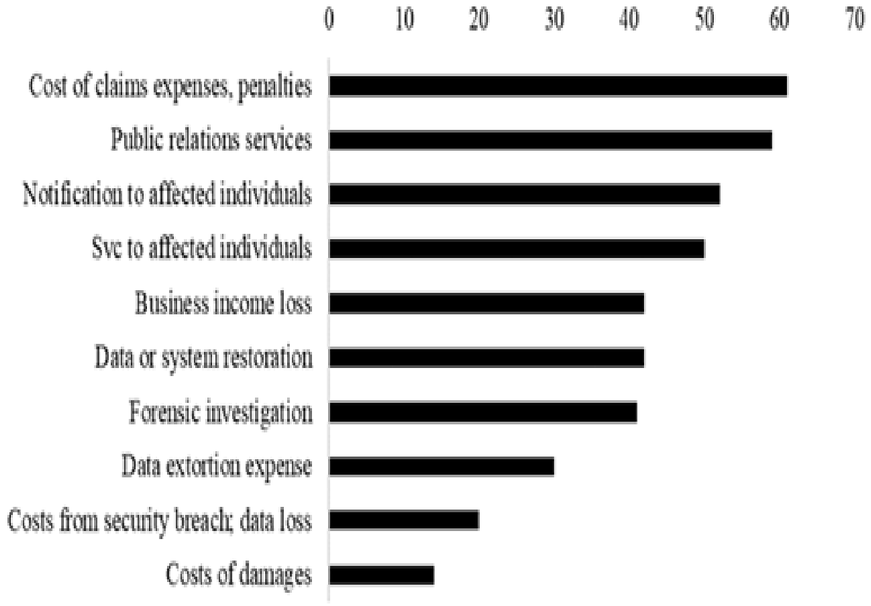
Coverage area	Description
Data Compromise Response	“Provides coverage for specified expenses arising from a personal data compromise involving personally identifying information of affected individuals. Affected individuals may be customers, clients, members, directors or employees of the insured entity.”
Identity Recovery	“Provides coverage for Identity Recovery caused by an identity theft of an identity recovery insured first discovered during the policy period.”
Computer Attack	“Provides coverage for specified expenses arising from a computer attack on the computer system.”
Cyber Extortion	“Provides coverage for the cost of an investigator retained in connection with the extortion threat and coverage for any amount paid by the insured in response to the threat.”

OSIGURATELJNA POKRIĆA U CYBER OSIGURANJU

„Third party“ pokriće

- ✓ **pokriva troškove obrane od javnih ili privatnih parnica, nagodbi, presuda, kao i novčane kazne i naknade koje proizlaze iz tužbi**
- ✓ **Primjer grupiranih pokrića s zajedničkim podlimitima i top 10 pokrića**

Liability	Description
Data Compromise	“[Provides] coverage for defense and settlement costs in the event that affected individuals or a government entity sue the insured because of a personal data compromise.”
Network Security	“Provides coverage for defense and settlement costs in the event that a third party claimant sues the insured because of: • The breach of third party business information • The unintended propagation or forwarding of malware • The unintended abetting of a denial of service attack • The inability of an authorized third party user to access the insured’s computer system.”
Electronic Media	“Provides coverage for defense and settlement costs in the event that a third party claimant sues the insured alleging that the insured’s electronic communications resulted in defamation, violation of a person’s right of privacy, interference with a person’s right of publicity or infringement of copyright or trademark.”

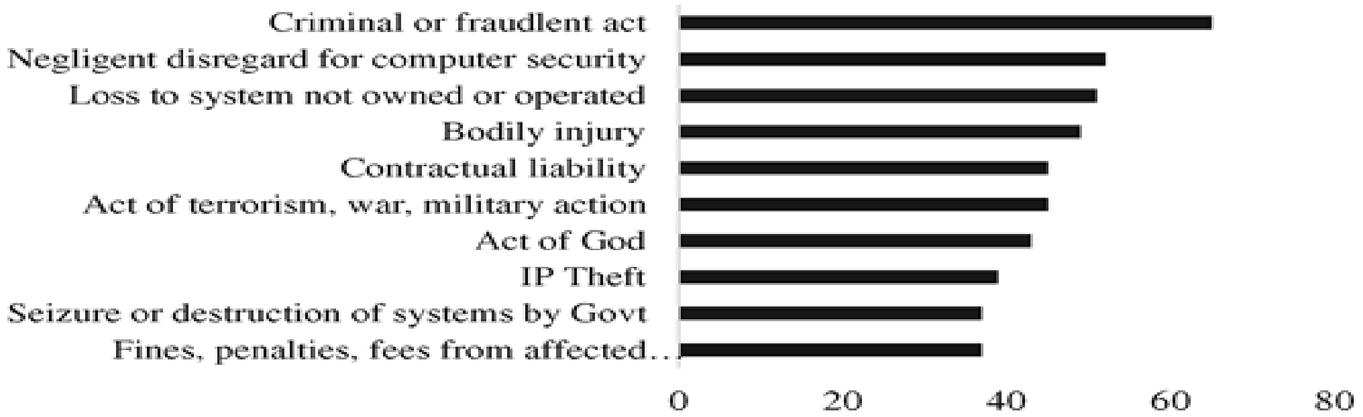


OSIGURATELJNA ISKLJUČENJA U CYBER OSIGURANJU

✓ **Najčešća isključenja nisu izravno povezana s cyber područjem nego se odnose na:**

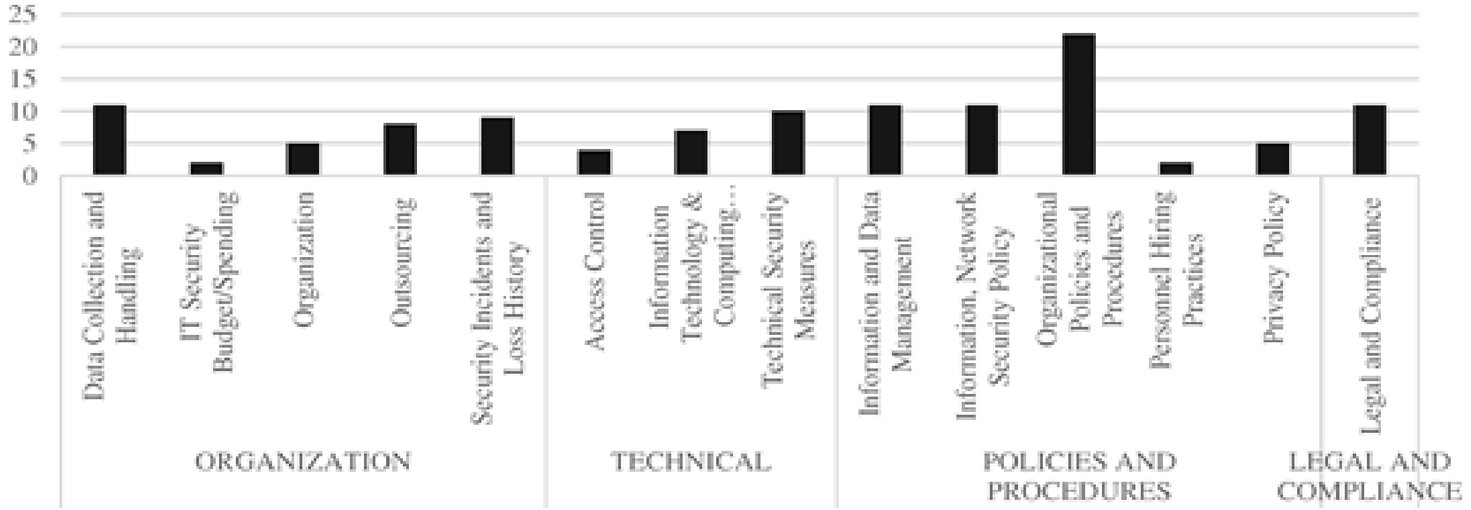
- **kaznena djela, prijevare, pogreške ili propusti,**
- **namjerno kršenje zakona, bilo koja kaznena istraga ili postupak koji je u tijeku i plaćanje novčanih kazni ili naknade,**
- **isključenja vezana za kršenja patenata,**
- **otkrivanja poslovne tajne ili povjerljivih podataka ili kršenja zakona o vrijednosnim papirima**

✓ **10 najčešćih isključenja koje se nalaze na policama osiguranja:**



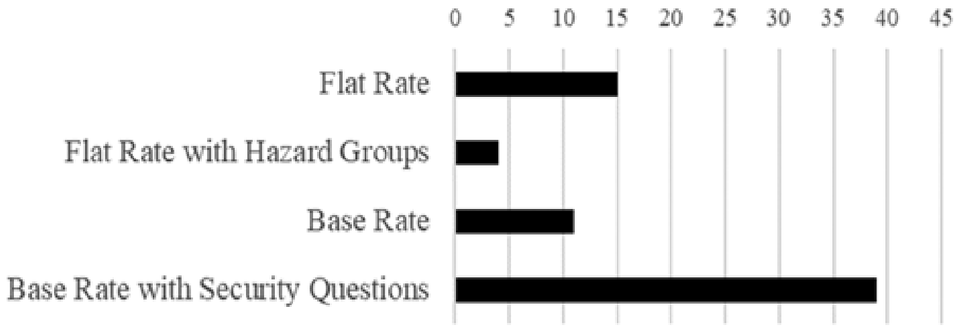
UPITNICI ZA PRIHVAT I PROCJENU CYBER RIZIKA

✓ **Analiza je rađena na uzorku od 34 upitnika - rezultat analize je evidentirano 118 pitanja koja su podijeljena u 14 područja iz kojih su segmentirane 4 glavne kategorije:**



ODREĐIVANJE PREMIJE OSIGURANJA

- ✓ **Na temelju pregleda 235 polica njih 69 imalo je pregled premijskih stopa i na temelju analize segmentirane su u 4 kategorije:**
  - **Fiksne premijske stope**
  - **Fiksne premijske stope prema grupama rizika**
  - **Osnovne premijske stope**
  - **Osnovne premijske stope zajedno s upitnicima za prihvat rizika**



ODREĐIVANJE PREMIJE OSIGURANJA

Fiksna premijska stopa

- ✓ **Najjednostavniji način određivanja premije je putem fiksnih premijskih stopa za „first and third party“ pokriće za sve tvrtke**
- ✓ **Iako je riječ o najbržem načinu određivanja premije nedostatak ovog modela je što nema razlike u premiji ovisno o specifičnostima pojedine tvrtke ili djelatnosti kojom se ista bavi (premija je ista za sve)**
- ✓ **Primjer izračuna premije:**

Coverage	Frequency	Severity	Expected loss (lost cost)	Profit load	Premium
Computer attack	0.20%	$49 800	$99.60	35%	$153
Network security liability	0.17%	$86 100	$147.23	35%	$227

ODREĐIVANJE PREMIJE OSIGURANJA

Fiksna premijska stopa prema grupama rizika

- ✓ **Radi se o modelu gdje postoji fiksna premija no postoji određeni modifikator ovisno o skupini rizika kojoj pripada određena tvrtka, npr:**
  - **“Nizak rizik“ - tvrtka ima web stranicu samo u informativne svrhe ili male količine prodaje od proizvođača čiji je glavni distribucijski kanal putem maloprodaje**
  - **„Srednji rizik“ - osiguranik posluje, barem djelomično, na svojoj web stranici i / ili zadržava brojeve kreditnih kartica kao i ostale potencijalno osjetljive podatke**
  - **„Veliki rizik“ - osigurani potencijalno velik dio svog poslovanja obavlja putem svoje web stranice ili zadržava osjetljive podatke poput brojeva socijalnog osiguranja ili ima neku kombinaciju oba.**

Primjeri tvrtki koje bi bile u kategoriji „Nizak rizik“ su auto kuće, frizeri, a u kategoriji „Veliki rizik“ trgovine elektronikom.

ODREĐIVANJE PREMIJE OSIGURANJA

Osnovna premijska stopa

- ✓ **U ovom načinu izračuna premije osiguranja postoji osnovna premija koja ovisi o veličini prihoda tvrtke ili vrijednosti imovine. Na tu osnovnu premiju mogu se onda obračunavati razni faktori ovisno o franšizama, traženim limitima i slično.**
- ✓ **Primjeri izračuna premije osiguranja:**

Revenue (in millions)	Annual gross base premiums
$0–$10	$1913.91
$10–$20	$2602.92
$20–$50	$3502.46
$50–$100	$5224.98

Limits	Factor
$500 000	0.809
$1 000 000	1.000
$2 000 000	1.132
$3 000 000	1.245
$4 000 000	1.371
$5 000 000	1.405

Industry classification factor	Weighting
Nonprofit, nonmedical	1.0
For profit, manufacturer	1.5
For profit, wholesale	1.5
For profit, nontechnical service provider	1.5
Computer consultants	2.0
System integration	2.0
Software manufacturer	2.0
Retail	3.0
Healthcare	3.0
Accountants	3.0
Financial	4.0
Large risk (over $250M revenue)	5.0
All other	3.0

ODREĐIVANJE PREMIJE OSIGURANJA

Osnovna premijska stopa zajedno s upitnicima za prihvat osiguranja

- ✓ **Najdetaljniji način određivanja premije koje je korišteno u 39 polica (57% polica iz analize) uzima u obzir kontrolu informacijske sigurnosti klijenta**
- ✓ **Prilagodba premije temeljena na stvarnom sigurnosnom položaju klijenta uvelike se razlikuju među osigurateljima, od osnovnih kategorija rizika do detaljnijih mjernih podataka**
- ✓ **Primjeri izračuna premije osiguranja:**

Category	Modification		
	Below Avg	Avg	Above Avg
Privacy controls	1.20	1.00	0.80
Network security controls	1.20	1.00	0.80
Content liability controls	1.20	1.00	0.80
Laptop and mobile device security policy	1.10	1.00	0.90
Incident response plan	1.10	1.00	0.90

Rating	Weighting
Excellent	0.75–0.85
Good	0.85–1.00
Fair	1.00–1.25
Poor	1.25–1.50

ODREĐIVANJE PREMIJE OSIGURANJA

- ✓ **Na temelju pregledanih polica (osim za police s fiksnim premijskim stopama), nakon što se utvrdi vrijednost imovine / prihoda, konačna premija izračunava se kao linearni umnožak svakog od koeficijenata sadržanih u premijskom sustavu**
- ✓ **Primjeri izračuna premije osiguranja:**

Premium = [Base Premium] x
[Loss Rating] x
[Professional Experience] x
[Longevity of Operations] x
[Use of Written Contracts] x
[Risk Characteristics] x
[Prior Acts Factor] x
[Coverage Adjustment] x
[Deductible]

Final Premium = (Third Party Liability Base Rate) +
(First Party Costs Base Rate, if elected) x
(Limit Factor) x
(Retention Factor) x
(Data Classification Factor) x
(Security Infrastructure Factor) x
(Governance, Risk and Compliance Factor) x
(Payment Card Controls Factor) x
(Media Controls Factor) x
(Computer System Interruption Loss Factor, if applicable) x
(Retroactive Coverage Factor) x
(Claims/Loss History Factor) x
(Endorsements Factor, if applicable)

ZAKLJUČAK

- ✓ Cyber osiguranje nije daleka budućnost ono je već brzo rastuća sadašnjost
- ✓ Daljnja digitalizacija poslovanja i sve „stroža direktiva” dodatno će potaknuti rast cyber osiguranja u državama EU
- ✓ Veliki izazovi prilikom uvođenja ove vrste proizvoda na nova tržišta - kompleksnost proizvoda (veliki broj rizika i isključenja, nepostojanje povijesti šteta), specifična znanja koja su potrebna za 24/7 podršku klijentima, još uvijek ograničena RE podrška, nedovoljno UW znanje i iskustvo te ne educiranost prodajne mreže i tržišta

HVALA NA PAŽNJI

THANK YOU FOR YOUR ATTENTION

Krešimir Frančić

kresimir.francic@crosig.hr