16. Seminar zavarovalnih zastopnikov in zavarovalnih posrednikov, 25. januar 2018, Gospodarska zbornica Slovenije, Ljubljana

KIBERNETSKO ZAVAROVANJE

mag. Bojana Kifnar Strmčnik

triglavRE

KIBERNETSKO ZAVAROVANJE

triglavRE

Kibernetski riziki in kibernetsko okolje

Pojem

- **Izraz "Cyber" kot predpona opredeljena kot nekaj, kar je povezano z računalniki, informacijsko tehnologijo, virtualno realnostjo** *(vir: Oxford Dictionaries)*

kibernetski rizik
Cyber-risk

kibernetsko zavarovanje
Cyber-insurance

kibernetski napad oz. varnostni incident
Cyber-attack

kibernetska varnost
Cyber-security

kibernetska grožnja oz. varnostna grožnja
Cyber-threat

kibernetski kriminal
Cyber-crime

triglavRE

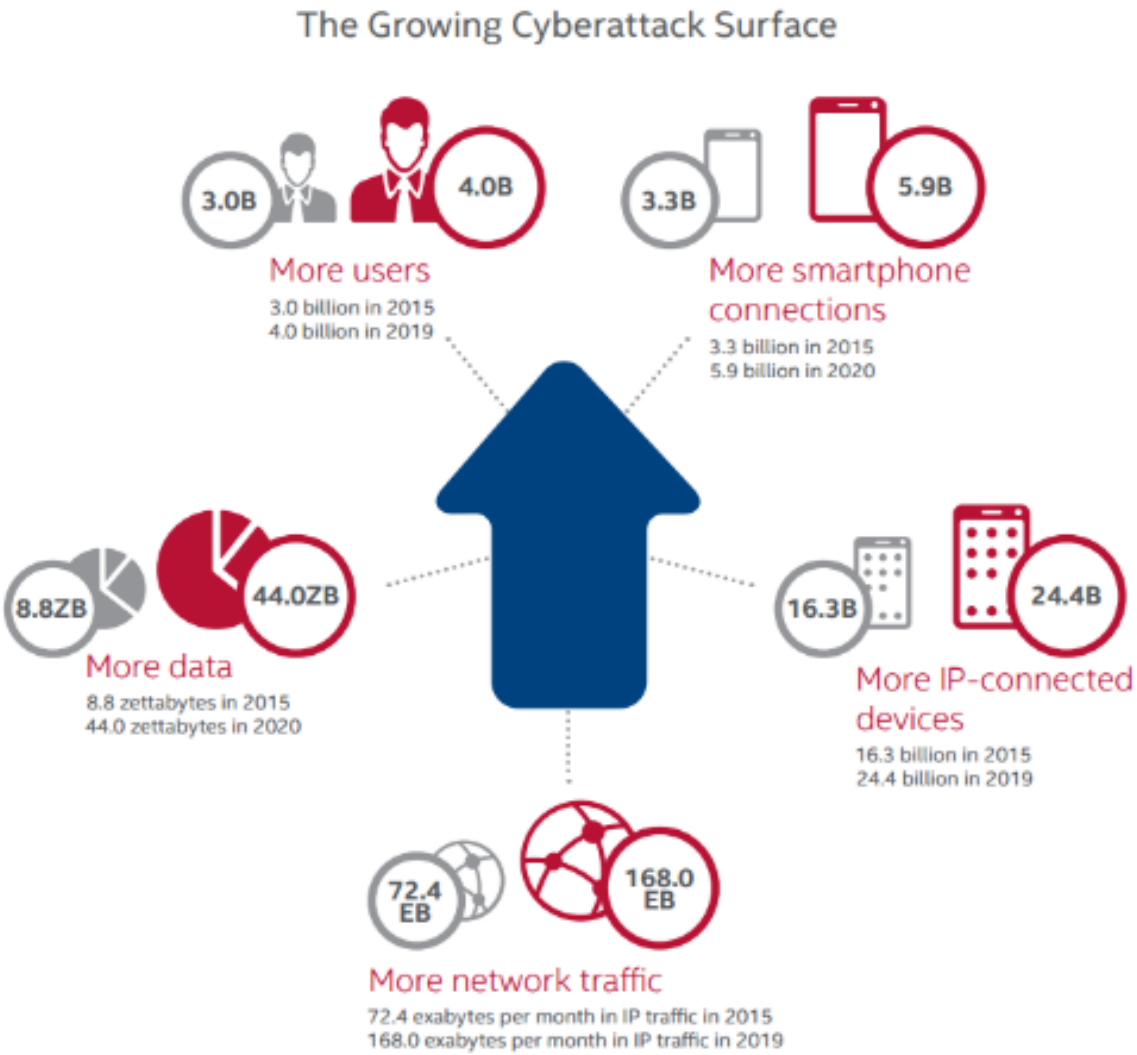
Kibernetski riziki in kibernetsko okolje

Zakaj predstavljajo kibernetski riziki nevarnost?

- **Življenje in delovanje v dobi interneta**
- **Vse večja globalna povezanost, soodvisnost**
- **Rast internetnega poslovanja, digitalizacija podatkov in procesov**
- **Razvoj novih tehnologij**

triglavRE

Kibernetski riziki in kibernetsko okolje



Source: McAfee Labs, 2015.

triglavRE

Kibernetski riziki in kibernetsko okolje

Zaposleni:
- Zlonamerna dejanja
- Nenamerna dejanja (malomarnost)

Zunanji:
- "Hacker"
- Organiziran kriminal
- tuje vlade

"Tretje osebe":
- Oblak
- Podatkovni center
- Service Provider

Socialna omrežja:
- Twitter
- Facebook
- Linkedin

Cilj: z raznolikimi pristopi na podlagi usmerjenih motivov pridobiti /razkriti /uničiti različne informacije ali onemogočiti delovanje sistema

triglavRE

Kibernetski riziki in kibernetsko okolje

Kaj je izpostavljeno nevarnosti?

Vsako delovanje oz. poslovanje, ki temelji na IT podpori /podatkih

- **Internetne strani, informacijski sistemi, tehnologija poslovanja v oblaku →** lažna internetna stran, prekinitev delovanja, kraja / oškodovanje podatkov

- **Email →** npr. vhodna točka za vnos virusa

- **Mobilne naprave, "Hardware" oprema, "IoT" →** nepravilno delovanje in povzročitev materialne / nematerialne škode

triglavRE

Kibernetski riziki in kibernetsko okolje

Ko gre narobe - kakšne so posledice?

<u>Nastanek škode</u> **- pri žrtvi incidenta** *(first-party loss)*
- pri tretjih osebah *(third-party loss)*

- **Materialna škoda**
- **Izgube ali poškodovanje podatkov → finančne posledice**
- **Nerazpoložljivost podatkov, razkritje/zloraba podatkov → odgovornost do tretjih oseb in izguba dobrega imena in ugleda**

Kibernetski riziki in kibernetsko okolje

Značilnosti kibernetskih oz. varnostnih incidentov

- **Porast števila incidentov v času**
- **Hitro se spreminjajoči načini vdora (razvoj tehnologije)**
- **Vse več namernih in ciljno usmerjenih incidentov** (motivi: finančni, doseganje konkurenčne prednosti, politični, aktivizem)
- **Sistemski vidik vdora – grožnja akumulacije**

triglavRE

KIBERNETSKO ZAVAROVANJE

1 Kibernetski riziki in kibernetsko okolje

2 Primeri kibernetskih incidentov

3 Ekonomski učinek incidentov

4 Percepcija kibernetskega rizika

5 Zavarovalno kritje

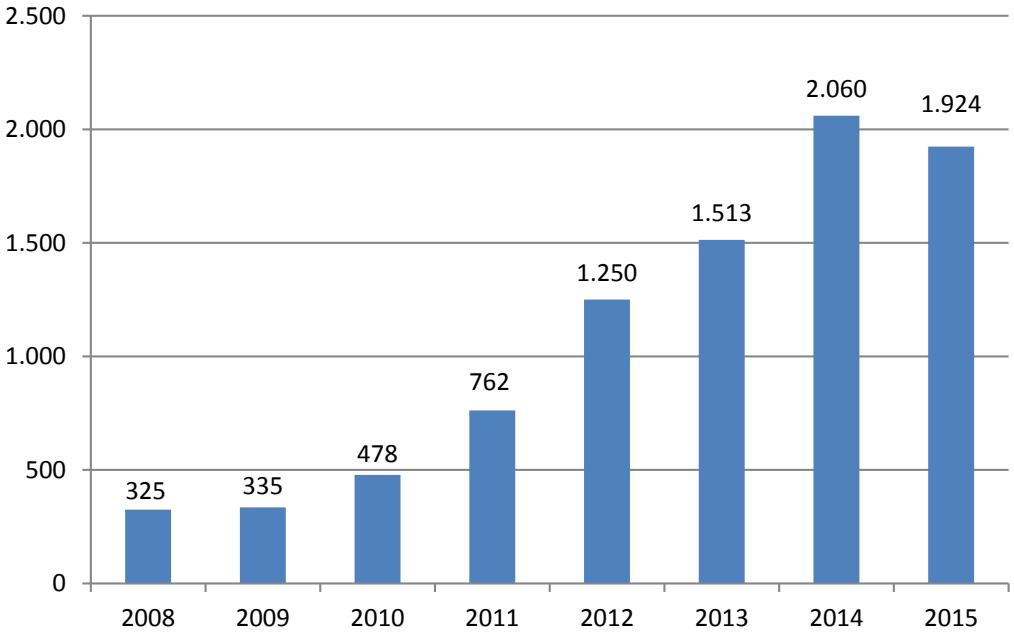
6 Priložnosti in izzivi zavarovanja kibernetskih rizikov

triglavRE

Primeri kibernetskih oz. varnostnih incidentov

Primeri kibernetskih oz. varnostnih incidentov

Število obravnavanih varnostnih incidentov v SI-CERT v letih 2008 - 2015



Vir: SI-CERT, Poročilo o omrežni varnosti

Grožnja kibernetskega napada skupine Anonymous (2012): tarča državna infrastruktura zaradi podpisa sporazuma ACTA

"Phishing" kibernetski napad na komitente 6 slovenskih bank (2015): poslanih cca 100.000 lažnih sporočil in postavljenih cca 40 lažnih kopij spletnih mest bank

si·cert

VARNI NA INTERNETU
Od mene je odvisno vse.
www.varninainternetu.si

triglavRE

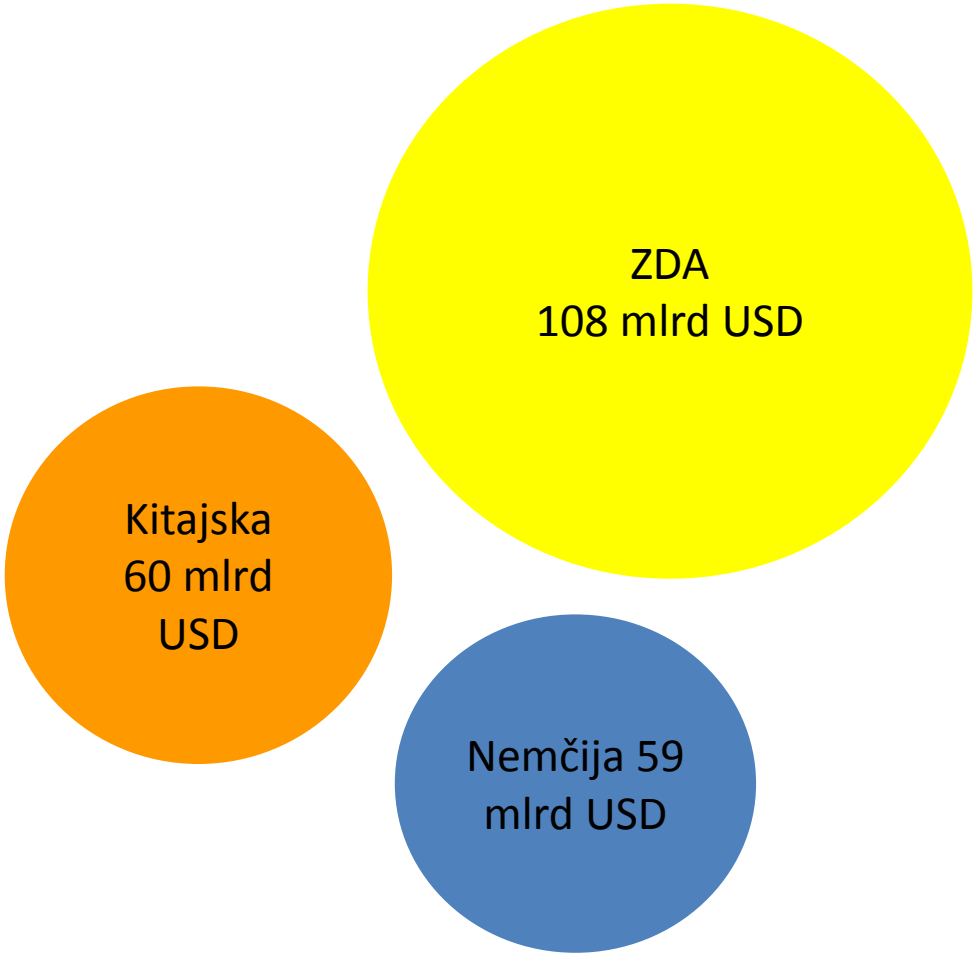
KIBERNETSKO ZAVAROVANJE

triglavRE

Ekonomski učinek incidentov

- **Letni strošek globalnega gospodarstva (ocena): 445 milijard USD** (Vir: CSIS/McAfee)

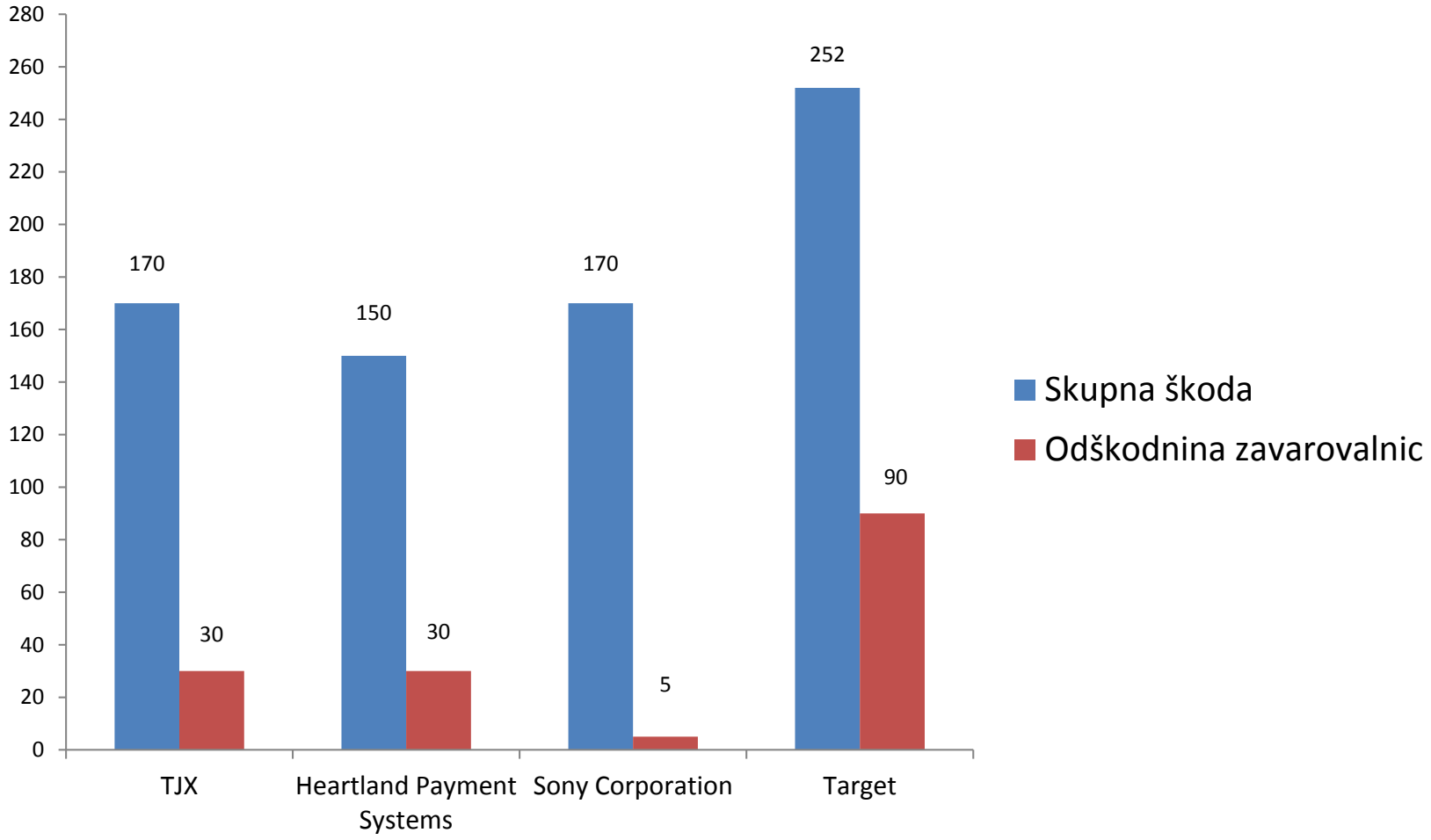
- **Letni strošek 3 največih gospodarstev (ocena) : 200+ milijard USD** (Vir:CSIS/McAfee)



Profit kibernetskega kriminala je večji od profita mednarodnega trga z drogami
(vir: C. Eckert)

triglavRE

Ekonomski učinek incidentov



Vir: A. Schlayer, Cyber insurance

triglavRE

KIBERNETSKO ZAVAROVANJE

triglavRE

Percepcija kibernetskega rizika

- **Več kot 60% targetiranih žrtev kibernetskega kriminala so SME** (vir: Aon)

- **Več kot 43% napadov je usmerjeno na družbe z manj kot 250 zaposlenimi** (vir: Symantec)

- **Samo 12% družb zavaruje svoja informacijska sredstva (neopredmetena sredstva), medtem ko opredmetena sredstva zavaruje 51% družb** (vir: Aon)

triglavRE

Percepcija kibernetskega rizika

Kibernetske nevarnosti po doseženem mestu glede na pomembnost za gospodarske družbe
(vir: Allianz Risk Barometer 2014 – 2018)

	2014	2015	2016	2017	2018
Doseženo mesto na lestvici Top 10 nevarnosti	8. mesto	5. mesto	3. mesto	3. mesto	2. mesto

2018 Allianz Risk Barometer report:

- **Kibernetski incidenti prepoznani kot "trigger", ki se ga strokovnjaki najbolj bojijo kot povzročitelja prekinitve poslovanja.**

- **Ocena vrednosti škode: 5 mio USD**

triglavRE

Percepcija kibernetskega rizika

Bruto zavarovalna premija po zavarovalnih vrstah v 2014 (mlrd USD)
(vir: M. Bundt)

Skupina zavarovanj	ZDA	Evropa	Azija	Skupaj
Avtomobilska zavarovanja	246	161	77	484
Druga premoženjska zavarovanja	169	113	28	310
Odgovornostna zavarovanja	90	41	23	154
Zavarovanje kibernetskih tveganj	2	0,2	0,1	2,3

Percepcija kibernetskega rizika

Zakaj tako nizko zavedanje o kibernetskih nevarnostnih pri potencialnih kupcih zavarovanja?

- **Premalo (še vedno) odmevnih kibernetskih incidentov –** ni zadostne publicitete in informacije o ekonomskem strošku (strah pred izgubo ugleda)

- **Prelaganje odgovornosti za upravljanje s tovrstnimi nevarnostmi na IT managerja v podjetju –** nizko zavedanje glede pomena preventive (Firewall zaščite, antivirusne zaščite, izobraževanje zaposlenih…)

- **“Ni se zgodilo meni/mojemu podjetju” – nevarnost ne obstaja!?**

triglavRE

KIBERNETSKO ZAVAROVANJE

1 Kibernetski riziki in kibernetsko okolje

2 Primeri kibernetskih incidentov

3 Ekonomski učinek incidentov

4 Percepcija kibernetskega rizika

5 Zavarovalno kritje

6 Priložnosti in izzivi zavarovanja kibernetskih rizikov

triglavRE

Zavarovalno kritje

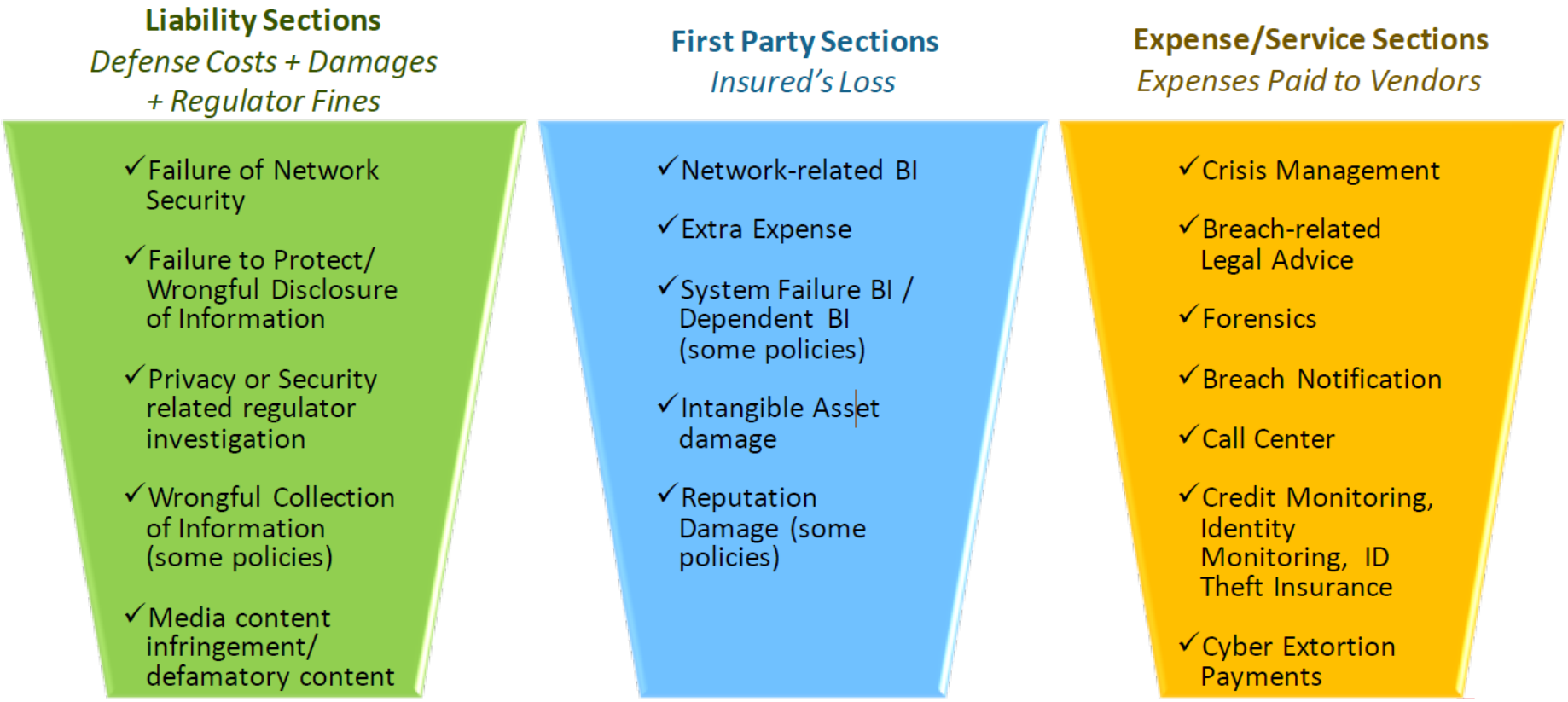
- **“Standalone” zavarovalno kritje kibernetskih rizikov:**
  - **kritje škode, nastale pri zavarovancu** (stroški povezani z obnovo IS, forenzičnega pregleda, obnove podatkov, stroški odkupnine/stroški preiskave za preprečitev izsiljevanja
  - **kritje škode, nastale pri tretjih osebah** (kritje sodnih stroškov zaradi razkritja zaupnih podatkov, stroški kazni, stroški obveščanja lastnikov podatkov o razkritju, stroški komuniciranja z javnostjo)

- **Paket zavarovalnega kritja sestavlja lahko več modulov, ki se razlikujejo glede na specifiko zavarovanca v povezavi z:**
  - velikostjo poslovanja
  - gospodarskim sektorjem
  - lokalno zakonodajo

- **“Emerging” kritje – zahtevnejše (npr. kritje telesnih poškodb tretjih oseb)**

triglavRE

Zavarovalno kritje



Vir: Aon, 2017

triglavRE

KIBERNETSKO ZAVAROVANJE

1 Kibernetski riziki in kibernetsko okolje

2 Primeri kibernetskih incidentov

3 Ekonomski učinek incidentov

4 Percepcija kibernetskega rizika

5 Zavarovalno kritje

6 Priložnosti in izzivi zavarovanja kibernetskih rizikov

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

PRILOŽNOSTI za zavarovalnice

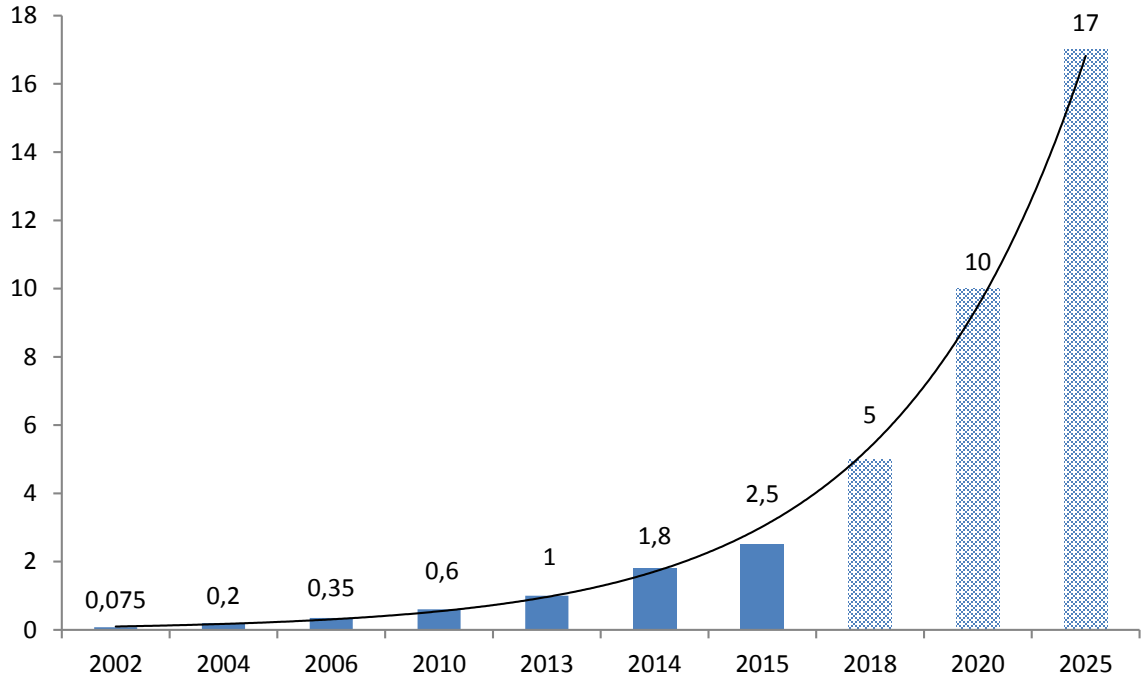
- **Raba interneta in internetno poslovanje – še naprej v vzponu**
- **Direktiva EU o varstvu osebnih podatkov – maj 2018 – pričakovan dvig zavedanja o kibernetskih rizikih, posledično vpliv na dvig povpraševanja po zavarovalnih produktih (podjetja / fizične osebe)**
- **Zavarovalnice kot pomemben element mitigacije rizika - ni popolne varnostne zaščite, obstoj zadostnih kapacitet zavarovalnega / pozavarovalnega trga**

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

PRILOŽNOSTI za zavarovalnice

- **Rast premije zavarovalnega trga – nova zavarovalna vrsta**
  Globalne premije zavarovanja kibernetskih rizikov 2002 – 2015 (v mlrd USD), ocena do 2025



(vir: Aon, M. Bundt)

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

PRILOŽNOSTI za zavarovalnice

- **Sprejem slovenske strategije kibernetske varnosti (2016) – akcije za dvig osveščenosti, obveščanje javnosti o grožnjah in svetovanje ob incidentih (SI-CERT) - pričakovan pozitivni učinek na nivo zavedanja prebivalstva in gospodarstva → več delovanja v smeri preventive**

- **Zmotno mnenje mnogih manjših družb, da niso tarča kibernetskih napadov**

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

IZZIVI za zavarovalnice

- **Nadaljevanje trenda povečevanja števila kibernetskih incidentov –** tako manjših kot tudi večjih razsežnosti
- **Manjko specifičnih informacijskih znanj –** nujno povezovanje s specializiranimi družbami (sodelovanje pri oceni rizika, ob škodi, ponovni vzpostavitvi delovanja)
- **Premalo verodostojnih podatkov o preteklih škodah (kibernetskih incidentih in ekonomskem učinku) za korektno aktuarsko obdelavo in analizo –** vpliv na stopnjo zavarovaljivosti, oceno rizika, določitev cene zavarovanja
- **Narava hitrega spreminjanja kibernetskih nevarnosti –** vrste akterjev in načini se ves čas spreminjajo; preteklo dogajanje ni nujno uporabno za napoved naprej

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

IZZIVI za zavarovalnice

- **Akumulacija rizika** – en škodni dogodek lahko doseže neslutene razsežnosti škode zaradi globalne povezanosti subjektov
- **Standardizacija procesa ocene rizika** – dogovoriti minimalne standarde ocene rizika in transparentnost pogojev zavarovanja
- **Razvoj dodatnih storitev zavarovalnic / pozavarovalnic** – pregled in ocena stanja informacijskega sistema, ocena ranljivosti, pomoč pri določitvi limita kritja, 24/7/365 asistenca ob škodi
- **Sledenje razvoju novih tehnologij** - vpliv na obstoječe rizike in nastanek novih

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

INFORMACIJE potrebne za oceno rizika

- **Opredeliti kibernetski profil družbe na podlagi sledečih informacij:**
  - **Varnostna politika družbe**
  - **Protokol rednega testiranja ranljivosti Sistema**
  - **S kakšnimi vrstami občutljivih podatkov upravljajo**
  - **Kje shranjuje družba občutljive podatke**
  - **“Incident response plan”**
  - **Število zaposlenih v IT oddelku**

- **Opredeliti in ovrednotiti kibernetskih rizike, ki jim je družba izpostavljena**

- **Obseg zahtevane informacije odvisen od obsega poslovanja, vrste rizikov, katerim je družba izpostavljena in gospodarske panoge, v kateri deluje**

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

KORISTI za zavarovance

- **Ni popolne varnostne zaščite – potreba po zavarovanju**
- **Strokovna asistenca v vseh fazah – pred sklenitvijo, pri oceni rizikov, ob nastanku incidenta in po njem (še posebej prednost pri manjših družbah)**
- **Prenos dela rizika na zavarovalnico – razbremenitev družbe za del rizika z ublažitvijo stroškov vzpostavitve v prvotno stanje pred incidentom**
- **Zavarovalno kritje "po meri", prilagojeno specifičnim potrebam družbe - običajno kombinacija različnih modulov kritja**
- **Zahteve regulative glede zaščite osebnih podatkov**

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

Kako naprej?

- **Jasna in transparentna opredelitev kritja in izključitev** – pomen izkušenj mednarodnega trga preko sodelovanja s pozavarovalnicami
  - enostavnejši produkt za fizične osebe
  - kompleksnejši produkt za pravne osebe (“po meri”)

- **Kibernetsko zavarovanje ni tipičen zavarovalni produkt** – investirati v pridobitev novih znanj (zavarovalni agentje, posredniki, UW, škodniki)

- **Ni še prepoznan produkt na trgu** – gre za t.i. **“push” produkt**; izpostaviti koristi za zavarovance ter regulatorne zahteve

- **Potrebne spremembe standardov na trgu** – npr. nivo min. varnostne zaščite, razumevanje rizika, tesno sodelovanje med zavarovancem in zavarovalnico (že v fazi preventive in ocene rizika) in sprotno prilagajanje razmeram, glede na specifiko zavarovanca

triglavRE

Priložnosti in izzivi zavarovanja kibernetskih rizikov

Kibernetski riziki so kompleksni in predstavljajo eno največjih groženj današnjemu poslovanju

Ni več vprašanje ali se bo incident zgodil, le še kdaj!

triglavRE