Težave ocenjevanja kibernetskega tveganja in upravljanja z njim

prof. dr. Sergeja Slapničar

University of Queensland Business School

Četrtek, 15. junij ob 19:00 (CET)

Ekonomska fakulteta UL (Klubska soba) | Zoom

ASEF

AMERICAN SLOVENIAN EDUCATION FOUNDATION

AUSCERT

Po treh najbolj priznanih svetovnih rangiranjih univerz v letu 2023, je Univerza v Queenslandu na drugem mestu v Avstraliji in na 42. mestu na svetovni lestvici.

UQ Cyber

Leading cyber innovation in the Asia Pacific

- **Slapničar**, Vuko, Čular, Drašček (2022). **Effectiveness of cybersecurity audit.**
- Gale, Bongiovanni, **Slapničar**, (2022). **Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead.**
- Pollmeier, Bongiovanni, **Slapničar** (2023). **Designing a financial quantification model for cyber risk: a case study in a bank.**
- **Slapničar**, Axelsen, Bongiovanni, Stockdale (2023). **A pathway model to 5 lines of accountability in cybersecurity governance**.
- **Slapničar**, Axelsen, Euelrich (2023). **Measuring and managing cyber risk.**

Storilci

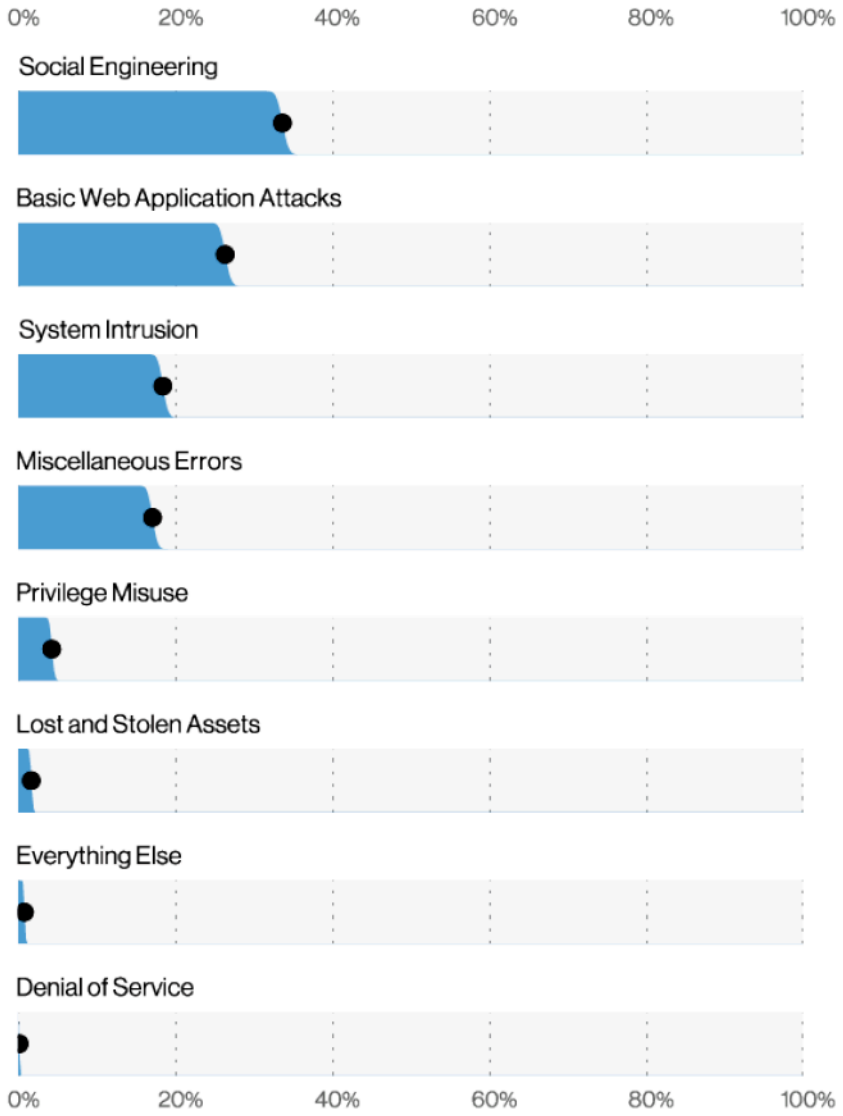


Figure 5. Patterns in breaches (n=5,275)

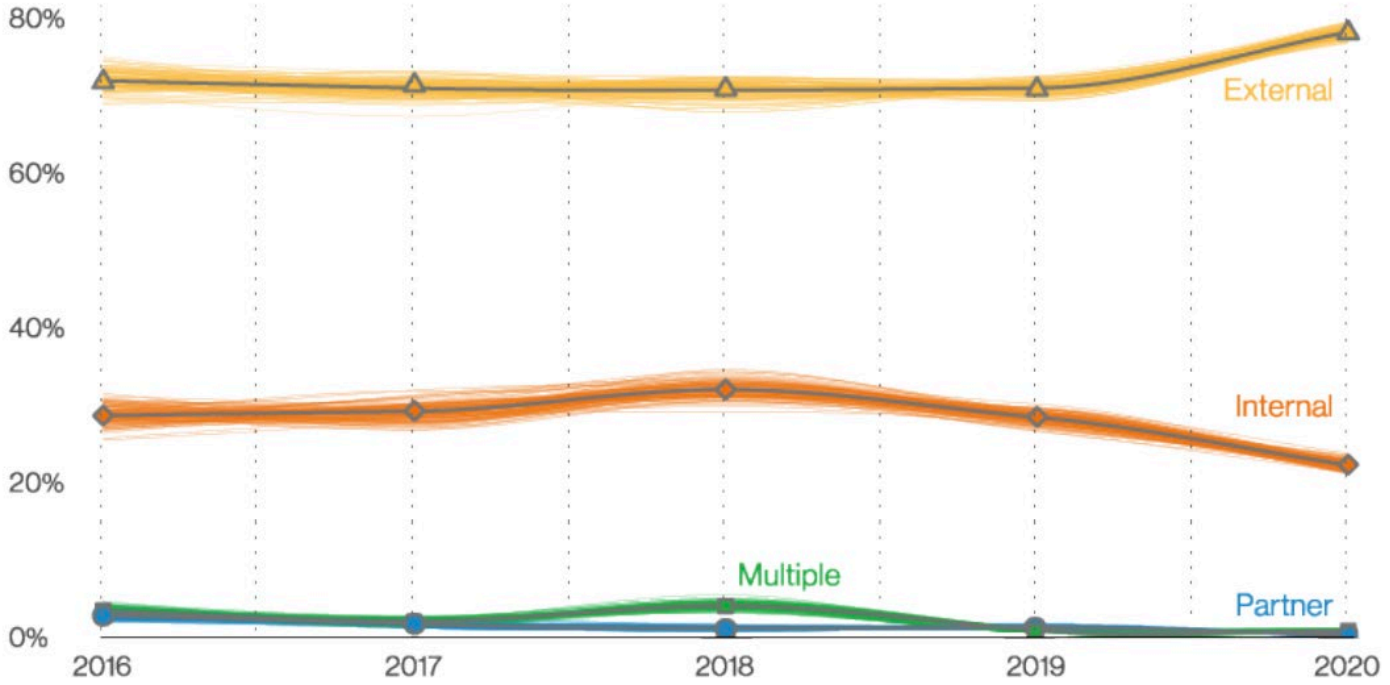


Figure 14. Threat actor over time in breaches

Verizon 2021 Data Breach Investigations Report

Motiv Št 1: finančni

organiziran kriminal

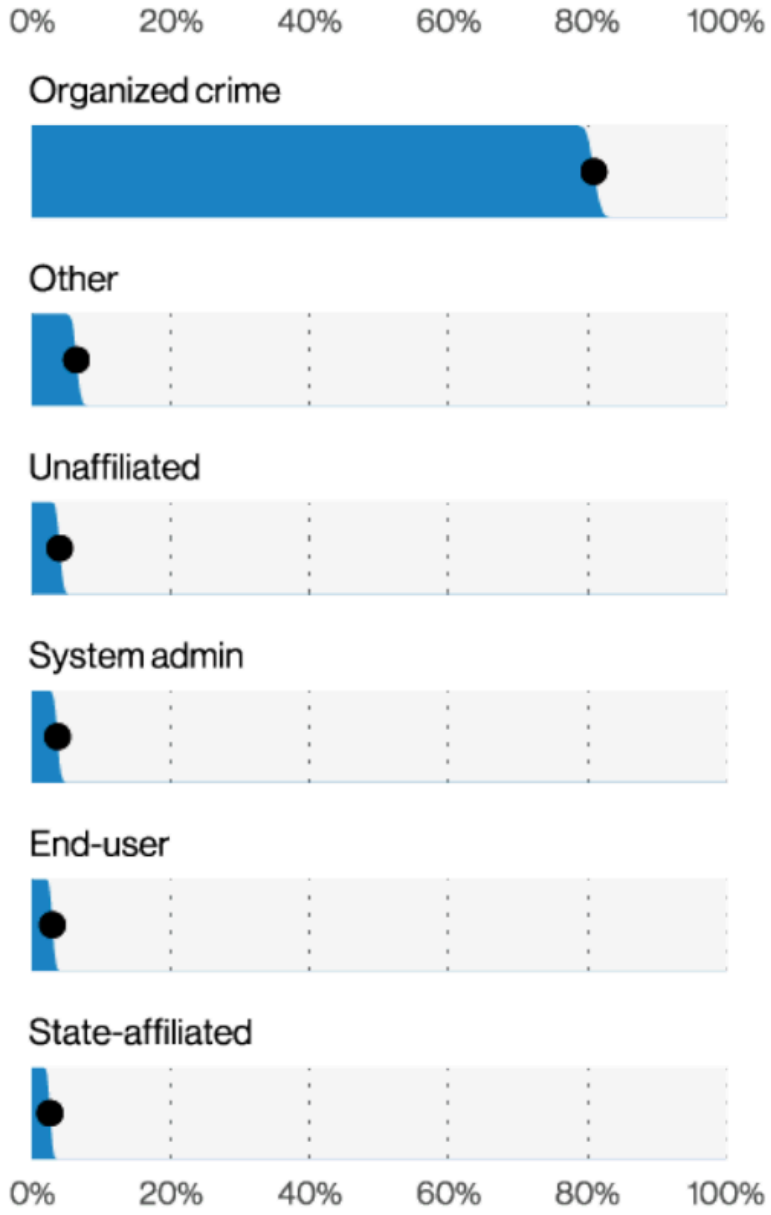


Figure 16. Top threat actor varieties in breaches (n=2,277)

Figure 14. Threat actor over time in breaches

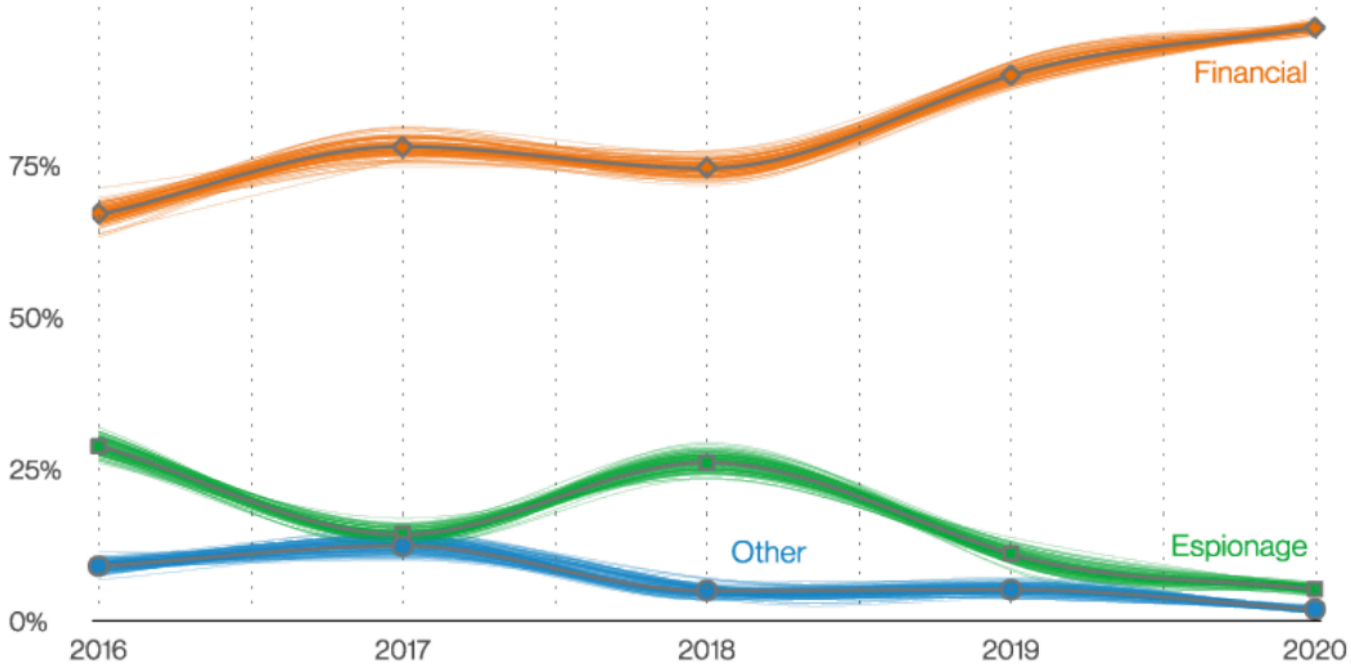


Figure 15. Top threat actor motive over time in breaches

Način

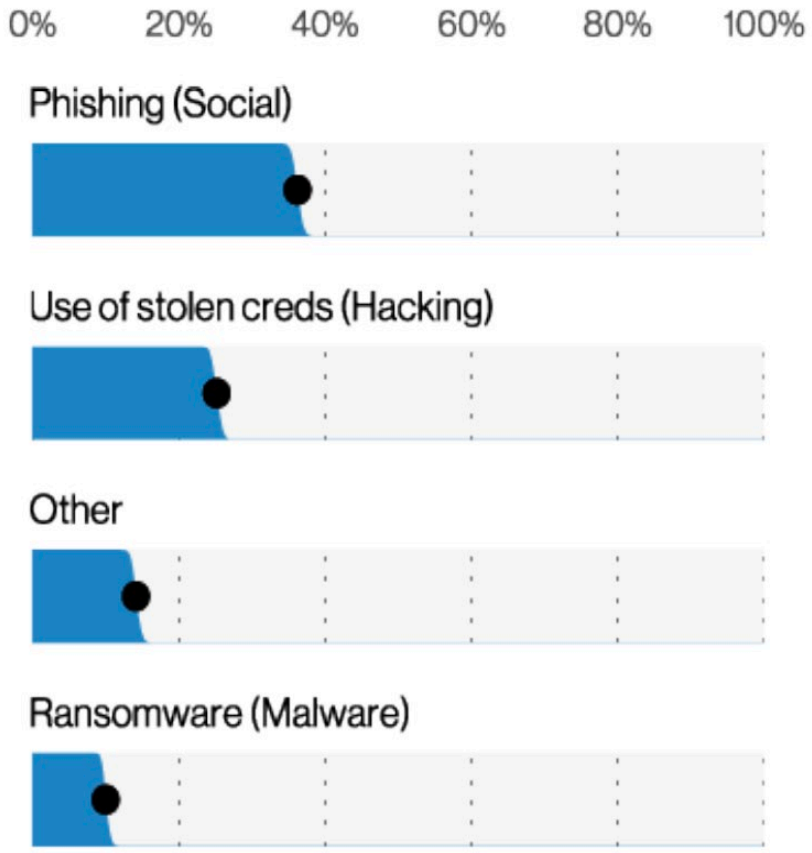


Figure 20. Top Action varieties in breaches (n=4,073)

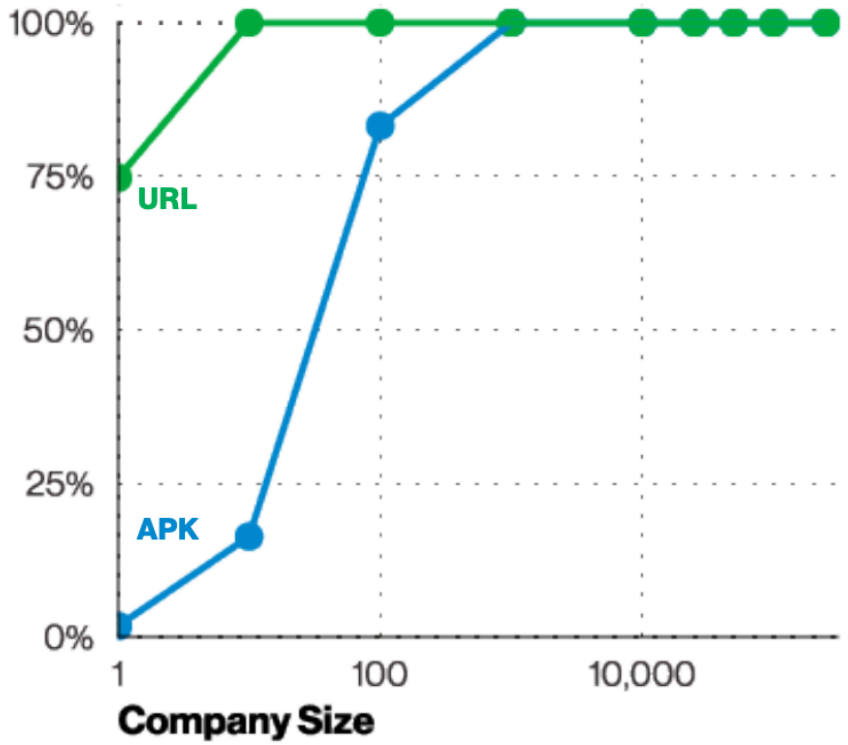


Figure 34. Probability that someone in the company will receive a malicious URL or install a malicious APK based on organization size (n=5,440,000). Blue is malicious APKs, green is malicious URLs.

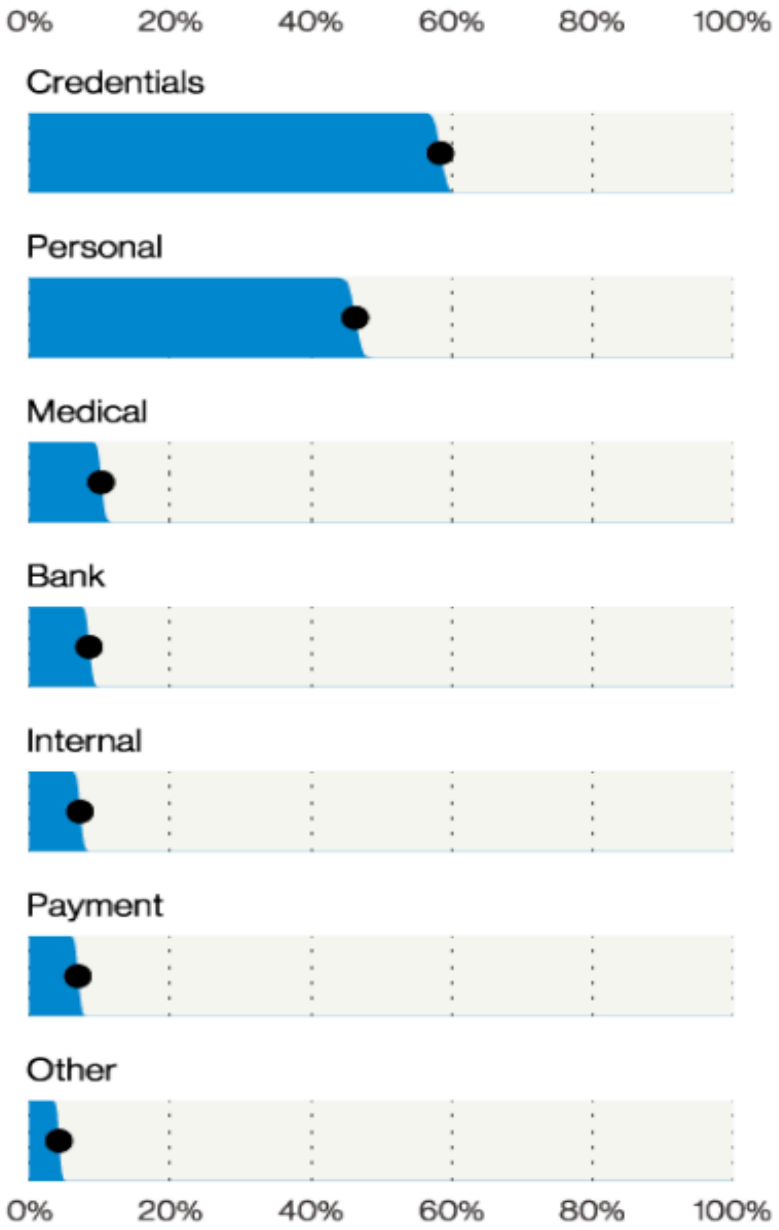
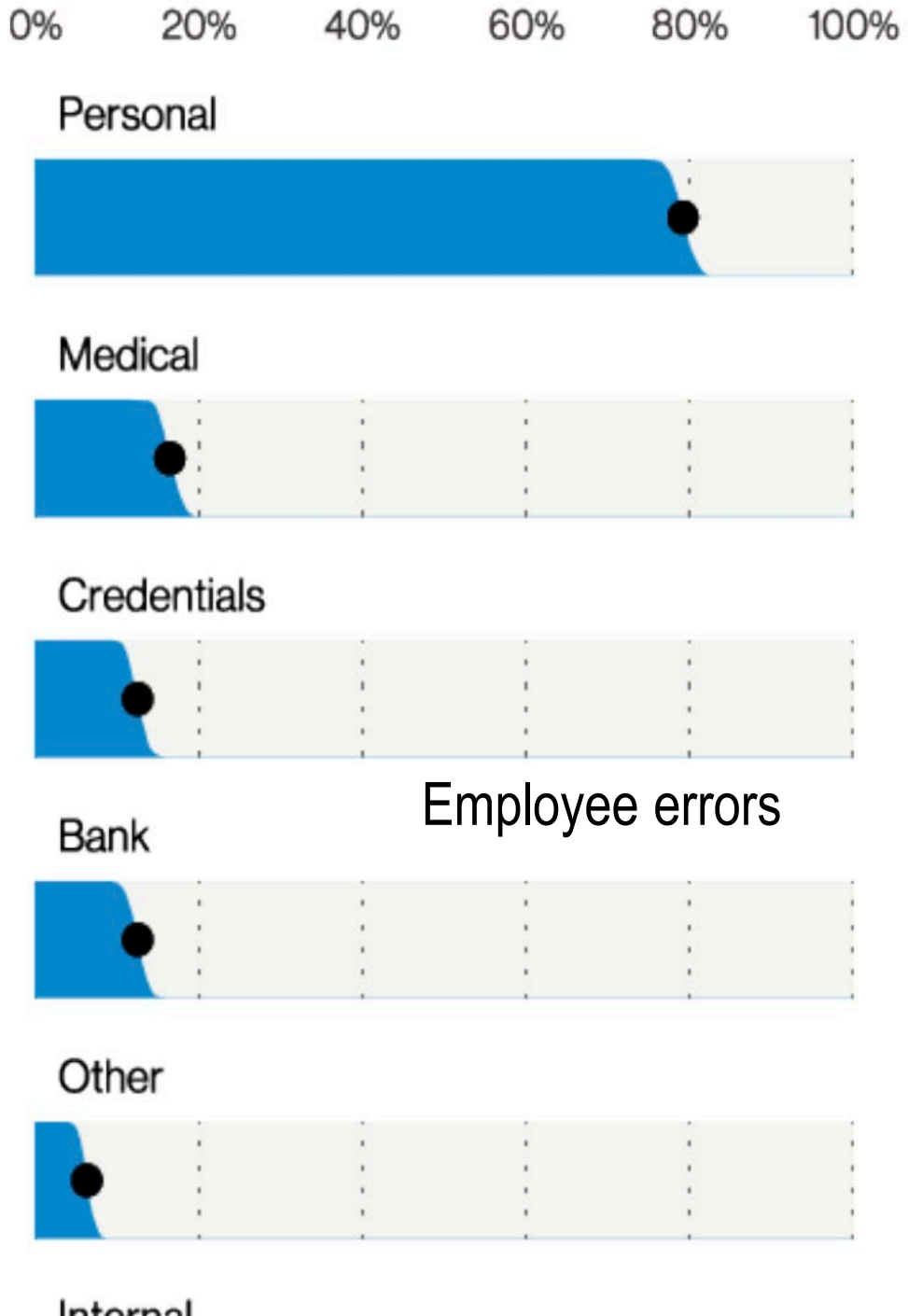


Figure 35. Top data varieties in breaches (n=4,552)

Podatki

Poverilnice so najbolj iskane



Employee errors

Verizon 2021 Data Breach Investigations Report

"Naj se IT s tem ukvarja!"

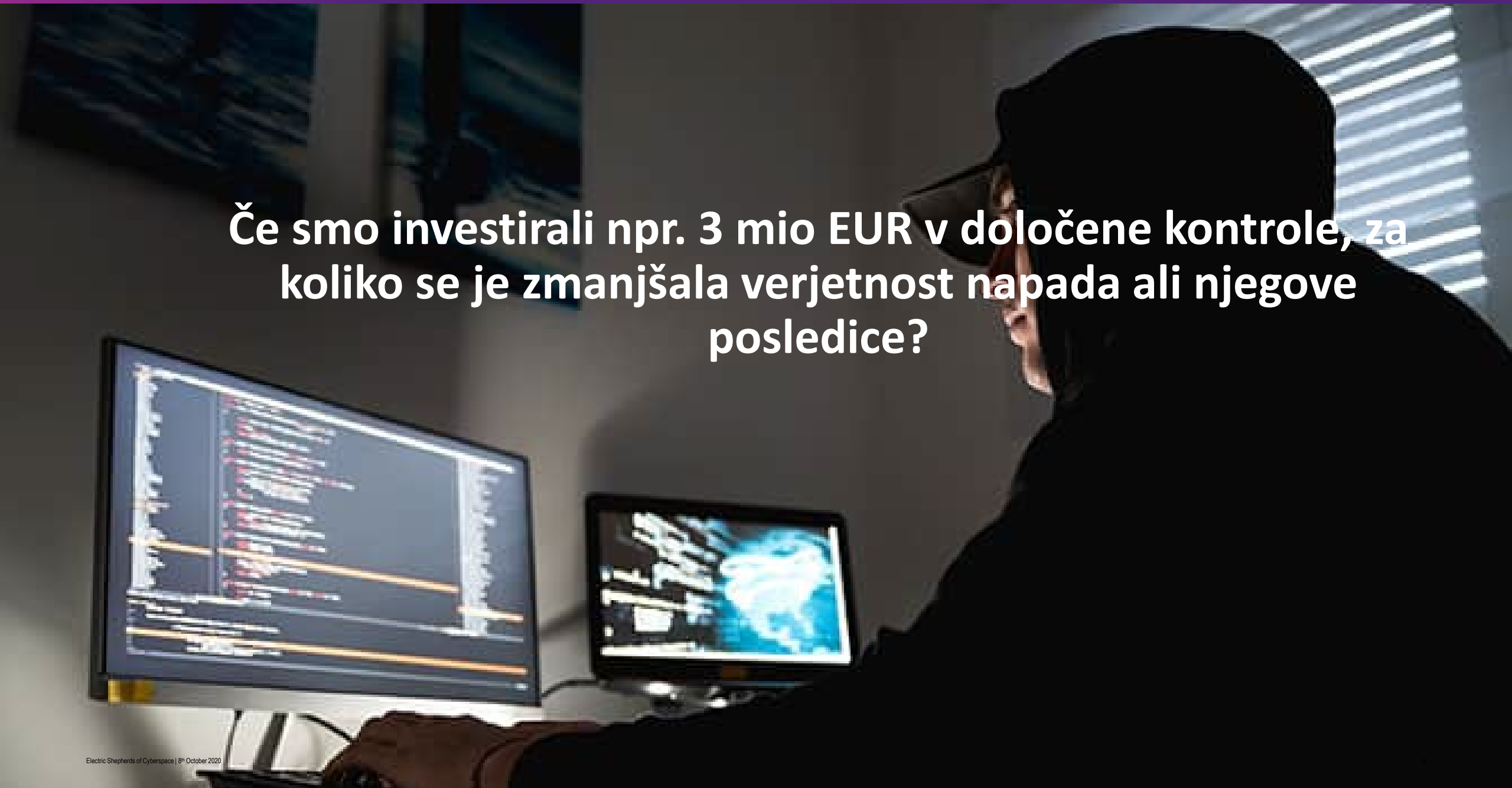
5. LINIJA: Nadzorni svet
Nadzor in strateške usmeritve

4. LINIJA: Uprava
Integrirati kibernetsko varnost v strategijo, politike in celovit sistem upravljanja s tveganji

Upravljanje s kibernetskimi tveganji
Tri linije obrambe:

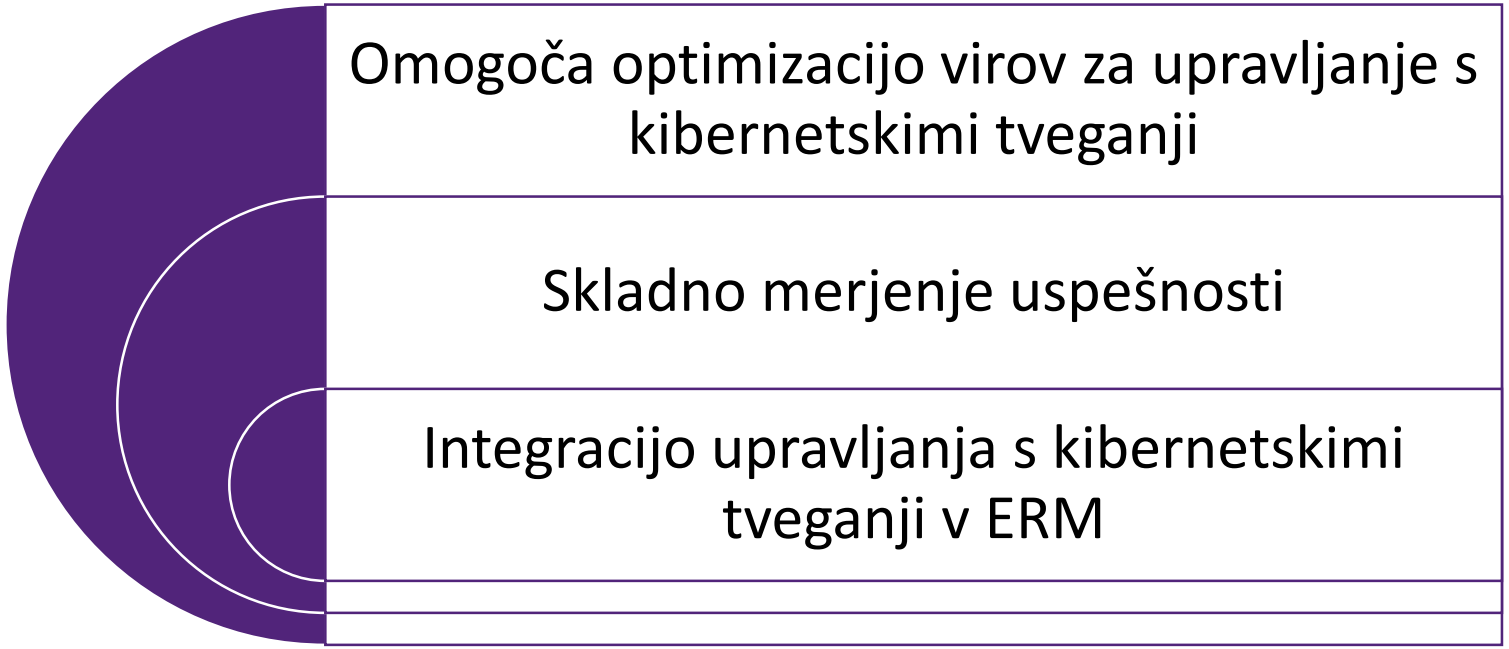
- 1. LINIJA: IT oddelek
- 2. LINIJA: manager informacijske varnosti
- 3. LINIJA: notranja revizija


Kakšnemu kibernetskemu tveganju smo izpostavljeni?
Koliko bi nas stal kibernetski incident ?
Kako verjeten je?



Če smo investirali npr. 3 mio EUR v določene kontrole, za koliko se je zmanjšala verjetnost napada ali njegove posledice?

Kvantificiranje kibernetskih tveganj je ?



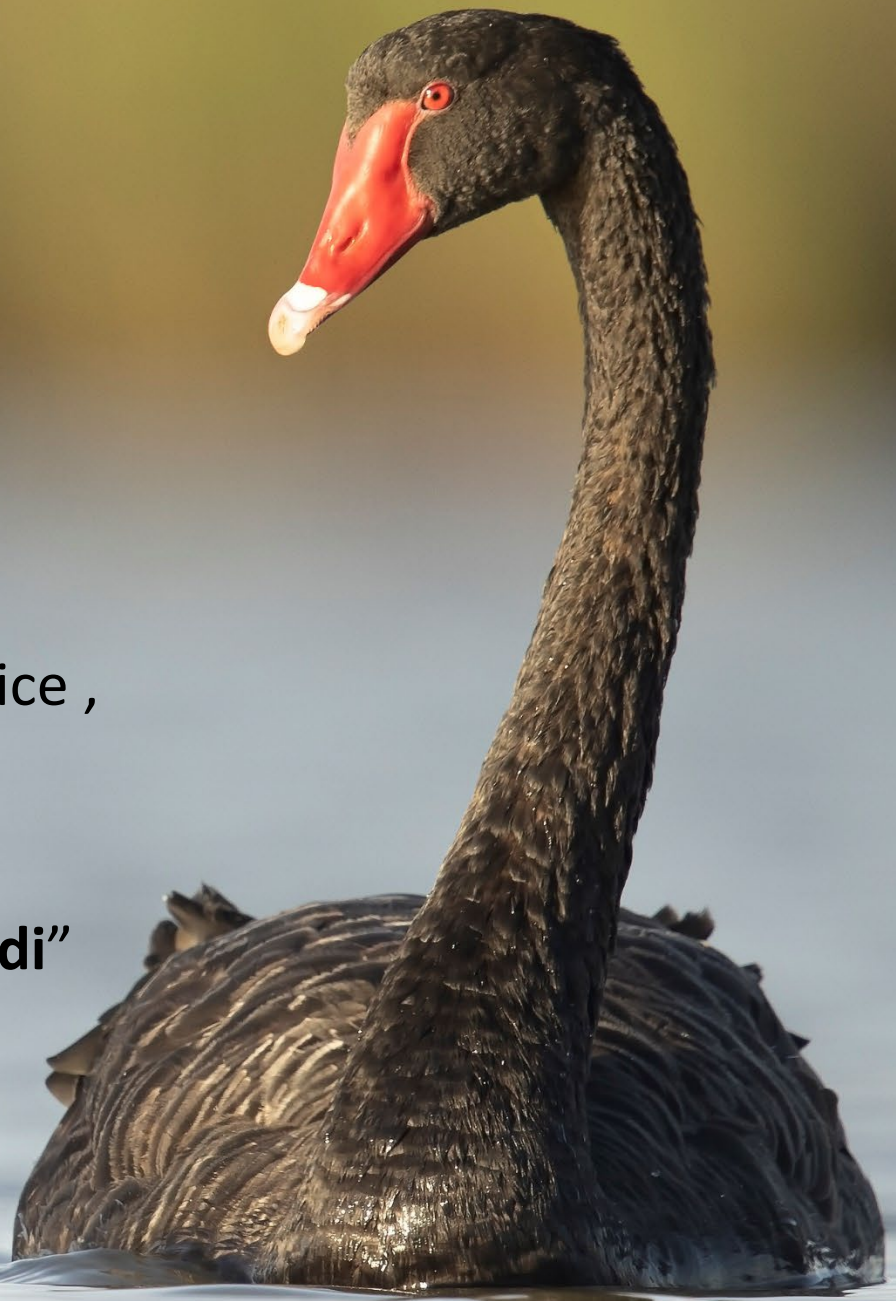
Kvantitativno merjenje kibernetskih tveganj omogoča določitev in merjenje

- Izpostavljenosti
- Tolerance (apetita) do tveganj
- Pragov kritičnosti
- Merjenje, do kakšne mere je tveganje zmanjšano

Samo kvantifikacija kibernetskih tveganj omogoča na tveganju temelječe upravljanje.

Je pa zakomplicirano…

- **Operativna tveganja** – redki dogodki; raznovrstne in vedno nove grožnje, pomanjkanje podatkov
- **Kibernetsko tveganje** – tehnološke, poslovne, pravne, zdravstvene posledice , tveganje ugleda; posledice za management
- "**Radikalna negotovost**" ali "**črni labodi**" – tveganja, ki jih ni mogoče opisati z znanimi dogodki, posledicami in distribucijo verjetnosti



Definicija kibernetskega tveganja

NIST SP 800–30: “funkcija **verjetnosti,** da bo določen vir **grožnje** izkoristil **ranljivost**, kar bo imelo **negativne posledice** za organizacijo.”

“It is better to be roughly right than precisely wrong.”
(John Maynard Keynes)

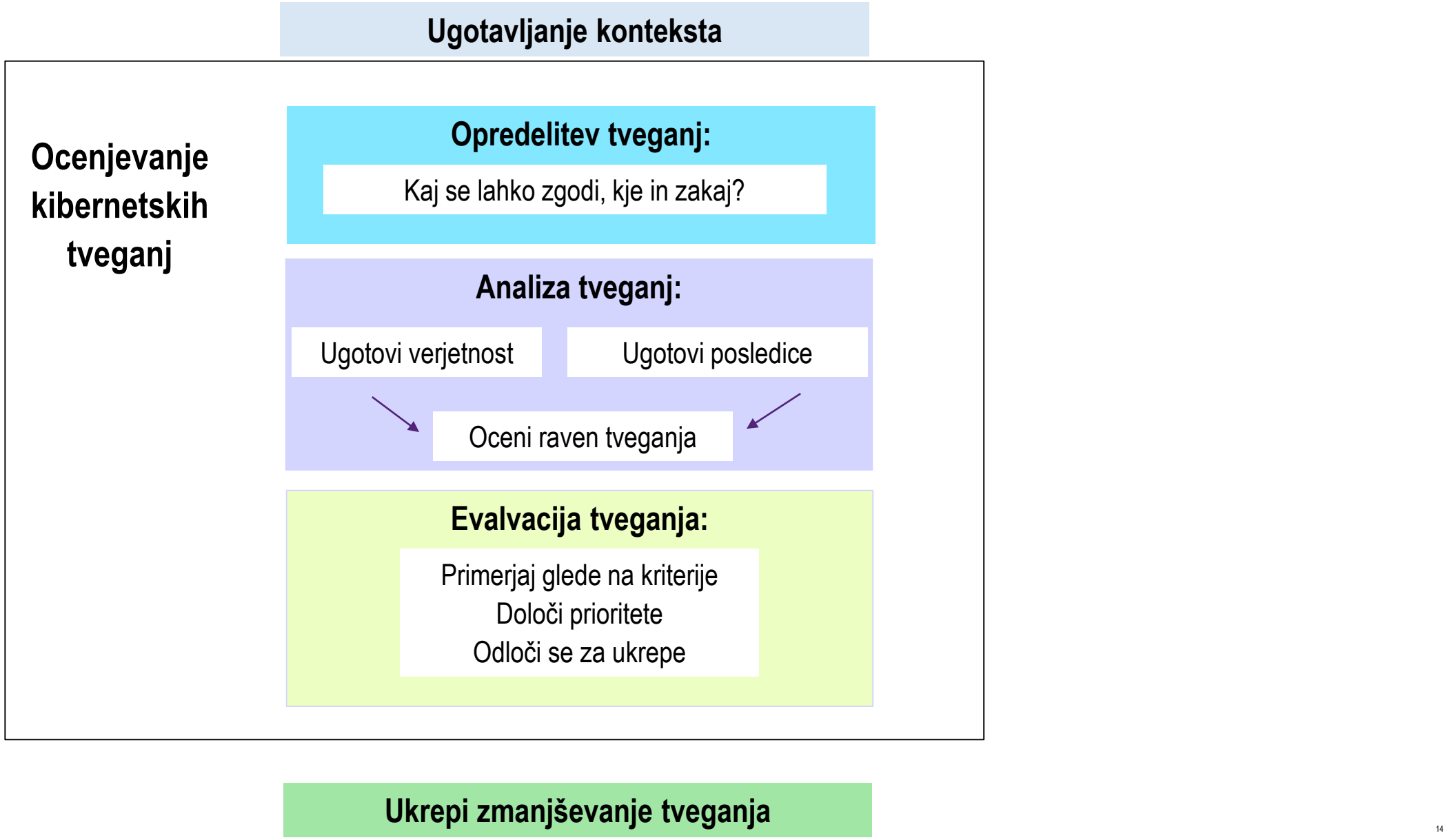
Kaj pomeni kibernetsko tveganje tistim, ki ga upravljajo?

"**Prekinitev poslovanja** in **kraja podatkov** sta dva najpomembnejša elementa tveganja" (CISO, transportna kritična panoga)

"V nasprotju z nekaterimi profitnimi organizacijami, ki jih zanimajo finančne posledice, nas ne. Zavedamo se, koliko so naši podatki vredni na črnem trgu. Vendar pa pri ocenjevanju kibernetskih tveganj poskušamo oceniti **klinična tveganja.** Če bi nam DoS napad onesposobil enega naših primarnih sistemov, bi morali v bolnišnici preiti na "ročno" upravljanje sistemov. (Direktor tehnologije, velika zdravstvena organizacija)

"Tveganje številka ena so **podatki strank**. Imamo 1,000,000 online strank. Ščitenje osebnih podatkov je naša primarna skrb – mi smo PCI Tier 1 prodajalec. Ugled je ključen za našo sposobnost poslovanja online." (managerka za varnost, veliki trgovec na drobno)

ISO/IEC 27005 2022



1. Opredelitev tveganj

Proces identificiranja in opisovanja tveganj

1. **Na dogodku temelječ pristop**: identificiraj strateške scenarije, vire tveganja, vrste napadov.

2. **Na sredstvih temelječ pristop**: identificiraj operativne scenarije, ki podrobno opredeljujejo sredstva, grožnje, ranljivosti.

Na dogodku temelječ pristop (ISO/IEC 27005:2022)

Organizacija opredeli svoje **kritične poslovne procese** in **produkte**, ki bi jih imel kibernetski incident nanje.

Npr. v banki sta taka procesa **kreditiranje** in **plačilni promet**.

"Grožnja obstaja, da kibernetski kriminalci vdrejo v sistem s pomočjo socialnega inženiringa, s katerim pridejo do poverilnic, enkriptirajo kritične podatke o strankah in transakcijah. Podajo zahtevo po odkupnini, da odklenejo podatke. "

Ta pristop se uporablja, ko ocenjujemo **resnost posledic** za določen strateški scenarij (Varela, 2022).

Na sredstvih temelječ pristop

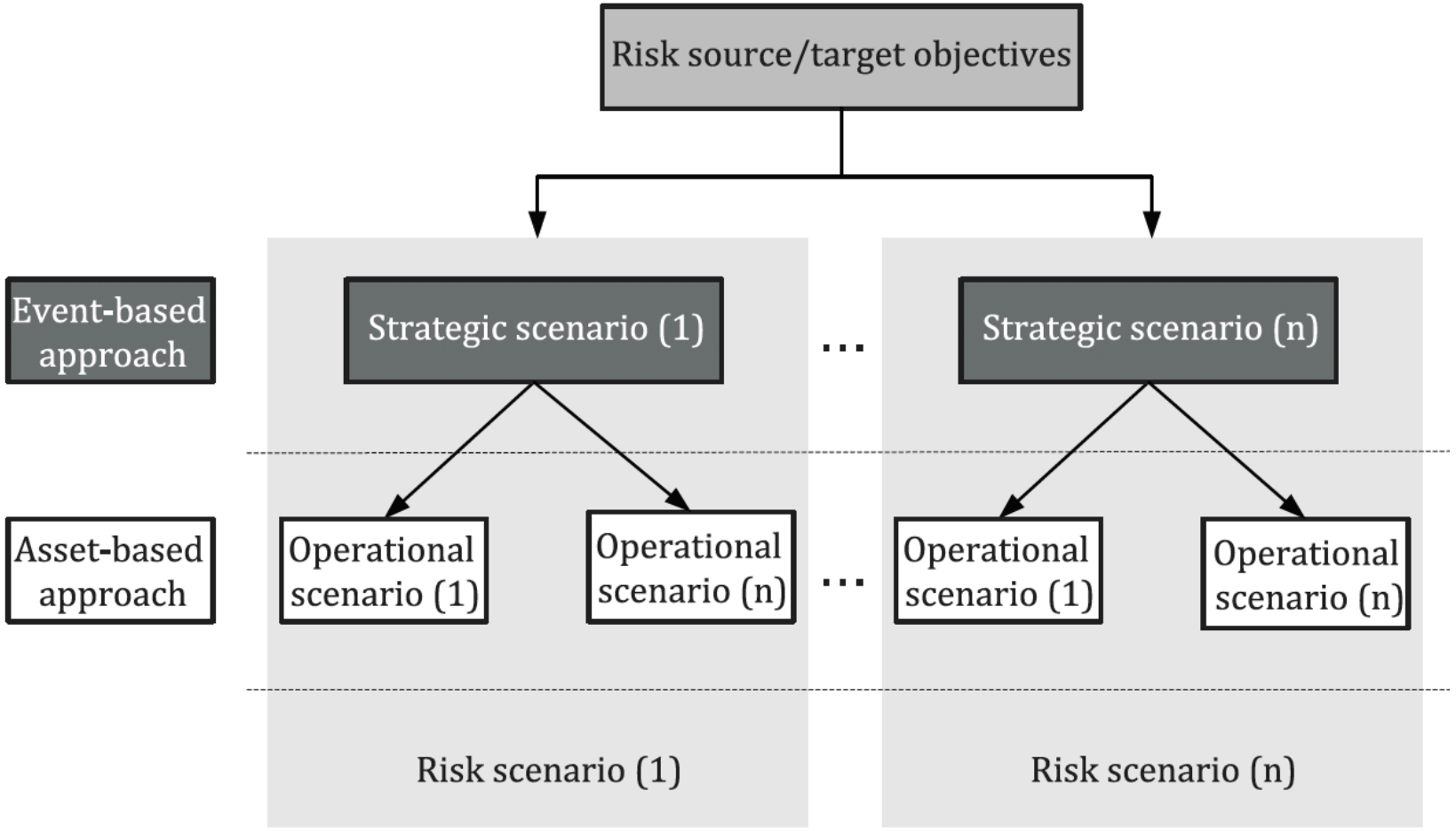
Kaj je sredstvo?

Sredstvo je vse, kar ima **vrednost za organizacijo** in zahteva **zaščito** (IS = procesi in informacije).

Seznam sredstev, ki so povezana s procesiranjem informacij, ali informacije same.

Tveganja je mogoče identificirati s pregledom sredstev, groženj in ranljivosti.

Ta pristop se uporablja, ko ocenjujemo **verjetnost** za določen strateški scenarij (Varela, 2022).



ISO/IEC 27005

Primer scenarija v zdravstveni zavarovalnici – kompromitirana zaupnost informacij

- Kibernetski kriminalec dostopi do zaupnih zdravstvenih podatkov **več milijonov strank**.
- Zagrozi, da bo objavil občutljive podatke na **dark webu** in **zahteva odkupnino več milijonov dolarjev**.

- **Način in vpletena sredstva**:
- uporaba ukradenega uporabniškega imena in gesla dobavitelja,
- nepopolno konfiguriran požarni zid v zavarovalnici, ki ni zahteval dodatnih varnostnih certifikatov

Posledice

$ 45 mio nadgradnja IT sistemov

$10 mio odkupnina

Več skupinskih tožb strank $$$?

Regulatorne kazni, ustavljeno poslovanje na borzi

Izguba $1,8 milijarde tržne kapitalizacije v enem dnevu vendar so delnice že zrasle za 9% ob objavi polletnih rezultatov (aprila 2023)

Updated: Apr 18, 2023 – 8.08am. Data is 20 mins delayed.

Glede vpliva na delnice raziskave kažejo:

- **Kratkoročni učinki**: padec vrednosti -0.14 to -4.1 %, večji za manjša podjetja
- **Dolgoročni učinki**: niso dokazani
- **Učinki okuženja**

Primer scenarijev – kompromitirana razpoložljivost informacij

"Če bi bila ena izmed naših spletnih strani onesposobljena, lahko zelo hitro ugotovimo, kakšno finančno izpostavljenost imamo. Če bi morali zapreti številne trgovine, ker bi njihova oprema bila kompromitirana, bi lahko ocenili, koliko nas to stane" (CIO, trgovina na drobno).

"V tem trenutku je še intuitivno, ampak v glavnem naš IT varnostni team, naš CISO in jaz smo skupaj brainstormali, kaj bi se lahko zgodilo v najslabšem možnem scenariju. Če nekdo prodre v naš sistem, kakšno kazen lahko pričakujemo, koliko bi nas stalo, da ponovno vzpostavimo sistem , kakšne dinamične izgube bi imeli in tako naprej […] Mislim, da smo opredelili sedem ali osem kategorij, ki bi vplivale na kumulativno maksimalno škodo" (direktor upravljanja s tveganji, velika banka).

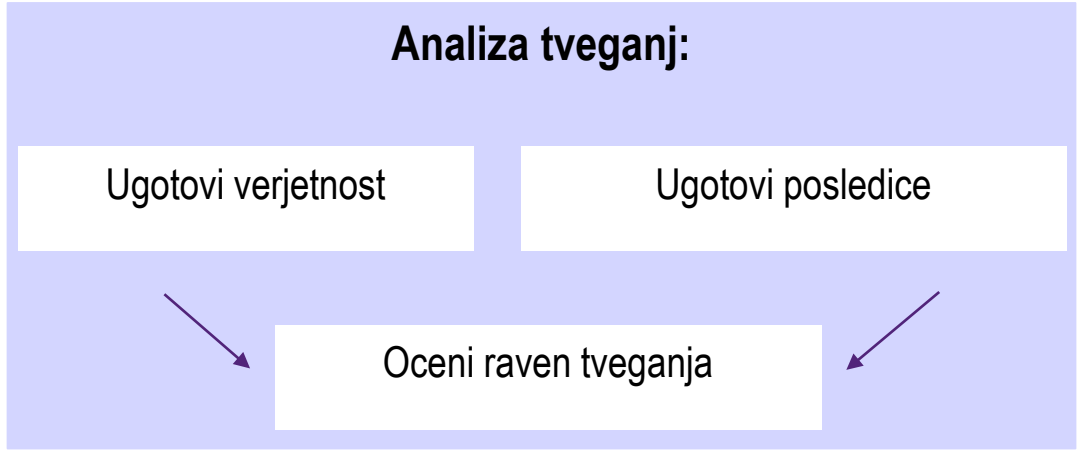
Iz naše raziskave (Measuring and managing cyber risk, Slapničar, Axelsen, Eulerich, 2023)

Primer na sredstvih temelječe opredelitve tveganj

"V registru tveganj opredeljujemo 219 kibernetskih tveganj. Razvrstimo jih glede na poslovni segment, čeprav je malo problematično razporediti kibernetska tveganja v posamični poslovni segment, ker se nanašajo na celotno organizacijo. Razvrstimo jih glede na vrsto, poslovno enoto, verjetnost, zaupnost informacij, kritičnost storitev, poslovne učinke, inherentno tveganje, rezidualno tveganje." (IT varnostni arhitekt iz visokošolskega sektorja)

Iz naše raziskave (Measuring and managing cyber risk, Slapničar, Axelsen, Eulerich, 2023)

2. Analiza tveganj



- **Ocenjevanje posledic:** Lastniki tveganj ali uporabniki, služba za upravljanje s tveganji, interni revizorji, računovodje (kontroling), vodja marketinga, vodja prodaje, pravniki
- **Ocenjevanje verjetnosti:** Strokovnjaki za varnost, IT revizorji
- **Skupne delavnice?**

2. Analiza tveganj

Tehnike analize tveganj

a) **kvalitativne**, z uporabo kvalitativnih mer (visoko, srednje, nizko)

b) **kvantitativne**, z uporabo monetarnih vrednosti za posledice in frekvence ali verjetnosti nastanka dogodka

Posledice (ISO/IEC 27005)

- a) Izguba življenja ali velika škoda posameznikom in skupinam;
- b) Izguba svobode, časti, ali pravice do zasebnosti
- c) Izgube zaposlenih in intelektualnega kapitala
- d) Prekinjeno poslovanje, naše in tretjih oseb;
- e) Realizacija planov;
- f) Finančne izgube in izgube prihodnjega poslovanja
- g) Izguba tržnega deleža
- h) Izguba ugleda in zaupanja javnosti
- i) Prekršitev pravnih in regulatornih norm
- j) Prekršitev pogodbenih zavez
- l) Negativni učinki na okolje

2. Analiza tveganj

		Posledice				
		Varnost	**Finančne**	**Ugled**	**Pravne**	**Okoljske**
Škoda	**Katstrofalna**	Več mrtvih	Stečaj	Izgubljen ugled, velik odhod kupcev	Prevzem s strani države, Zaporne kazni za vodilne	Dolgoročni izjemno visok vpliv
	Velika	En mrtev	Velike izgube	Medijska "gonja"	Intervencija države, Velike finančne kazni, Zamenjava vodstva	Velik vpliv
	Srednja	Invalidnost	Izgubljen dobiček	Neugodne novice v medijih	Denarne kazni, posebne revizije	Visok vpliv z zahtevo po resnem odzivu
	Majhna	Poškodbe	Zmeren znesek (npr. <100k)	Lokalen vpliv na ugled	Manjše kazni	Poseben odziv
	Nepomembna	Odsotnost z dela	"Drobiž"	Brez učinka	Opozorila	Običajen odziv

ISO/IEC 27005: Kriteriji ocenjevanja posledic: samo za ocenjevanje kibernetskih tveganj?

Consequences	Description
5 – Catastrophic	**Sector or regulatory consequences beyond the organization** Substantially impacted sector ecosystem(s), with consequences that can be long lasting. And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance. And/or: critical consequences on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.).
4 – Critical	**Disastrous consequences for the organization** Incapacity for the organization to ensure all or a portion of its activity, with possible serious consequences on the safety of persons and property. The organization will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences.
3 – Serious	**Substantial consequences for the organization** High degradation in the performance of the activity, with possible significant consequences on the safety of persons and property. The organization will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact.
2 – Significant	**Significant but limited consequences for the organization** Degradation in the performance of the activity with no consequences on the safety of persons and property. The organization will overcome the situation despite a few difficulties (operation in degraded mode).
1 – Minor	**Negligible consequences for the organization** No consequences on operations or the performance of the activity or on the safety of persons and property. The organization will overcome the situation without too much difficulty (margins will be consumed).

Ocenjevanje verjetnosti

1. Pridobitev informacij o aktualnih **grožnjah**
2. Ocena **ranljivosti** kontrol: NIST CSF, COBIT, lastno razviti okvirji kontrol

   Ocena kvalitete **kontrolnega okolja** z uporabo **lestvice zrelosti** ali/in

   učinkovitost kontrol, pridobljenih s storitvami dajanja zagotovil ali uporabo indikatorjev tveganj

Example NIST CSF Control Maturity Assessment

ID	Objective	Question	Rating	Response
PR.AC-1	Identities and credentials are issued, managed, verified, revoked and audited for authorized devices, users and processes.	What is the process to regularly review access to ensure users are appropriate and revoke it when no longer required?	1	None
			2	*Ad hoc* review by IT or audit
			3	Documented process rolled out to all critical systems
			4	Automated using identity access management (IAM) tools

Vohradsky 2022

Kriteriji verjetnosti pri kvalitativnem ocenjevanju

Table A.2 — Example of likelihood scale

Likelihood	Description
5 – Almost certain	The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very high.
4 – Very likely	The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is high.
3 – Likely	The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is significant.
2 – Rather unlikely	The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is low.
1 – Unlikely	The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very low.

ISO/IEC 27005

2. Analiza tveganj

Likelihood

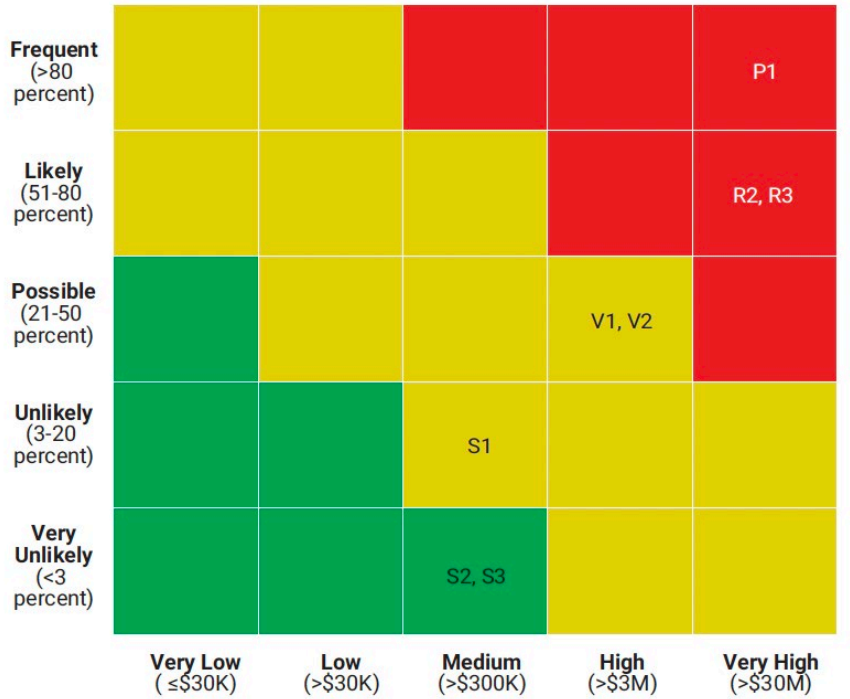
ID	Scenario	Inherent Risk	Key Controls	Control Rating	Overall Control Rating	Current Risk
P1	Cybercriminal uses phishing to gain access to the patient management system	High	Policy Framework	Marginal	Marginal	High
			Authentication	Strong		
			Access Management	Strong		
			Privileged Access Management	Weak		
			User Awareness Training	Weak		
			Email and Web Protection	Strong		
			Security Logging and Monitoring	Strong		
			Security Incident Response	Marginal		

Vohradsky 2022

Raven kibernetskega tveganja

Table A.3 — Example of qualitative approach to risk criteria

Verjetnost	Posledice				
	Catastrophic	**Critical**	**Serious**	**Significant**	**Minor**
Almost certain	Very high	Very high	High	High	Medium
Very likely	Very high	High	High	Medium	Low
Likely	High	High	Medium	Low	Low
Rather unlikely	Medium	Medium	Low	Low	Very low
Unlikely	Low	Low	Low	Very low	Very low



Kvantitativne lestvice posledic (ISO/IEC 27005)

Table A.5 — Example logarithmic consequence scale

Consequence (a loss of)	Log expression	Scale value
£1 000 000	(10^6)	6
£100 000	(10^5)	5
£10 000	(10^4)	4
£1 000	(10^3)	3
£100	(10^2)	2
Less than £100	(10^1)	1

Kvantitativne lestvice verjetnosti (ISO/IEC 27005)

Table A.4 — Example logarithmic likelihood scale

Approximate average frequency	Log expression	Scale value
Every hour	(approximately 10^5)	5
Every 8 hours	(approximately 10^4)	4
Twice a week	(approximately 10^3)	3
Once a month	(approximately 10^3)	2
Once a year	(10^1)	1
Once a decade	(10^0)	0

Še vedno subjektivno!

Podatki in metode

- **Pretekli podatki podjetja** – so relevantni?
- Podatki za **druga podjetja iz iste panoge** – so primerljivi?
- **Ekspertne ocene** – so subjektivne!
- Zunanji eksperti za informacije o grožnjah (threat intelligence)

- **Bayesovo modeliranje**, posodabljanje začetnih ocen, ko je na voljo več informacij
- **Metode strojnega učenja** – globoke nevronske mreže in avtoregresivne časovne serije zahtevajo velike količnine podatkov, na katerih se algoritmi učijo, da bi lahko predvideli verjetnost dogodka; temeljijo na notranjih podatkih, ne upoštevajo novih groženj
- **Copula** modelira strukture soodvisnosti med različnimi kibernetskimi tveganji
- **Monte Carlo** simulacije

Primer na dogodku zasnovanega pristopa (Santiago, Bongiovanni, Slapničar, 2023):

Strateški scenarij

"Kibernetski kriminalec je dostopil do občutljivih informacij strank banke in sicer do 25% strank v naši bazi. Regulator je že obveščen, medtem ko javnost še ni izvedela za kibernetski napad."

1. Opredelitev strateških scenarijev kibernetskih tveganj

Kritičnost

- Poslovnih procesov
- Podatkov strank

Scenarij 1

Scenarji 2

Scenarij 3

Digitalna sredstva, ki podpirajo najbolj pomembne procese.

Občutljivost

- Poslovnih informacij

Scenarij 4

Scenarij 5

Scenarij 6

Občutljivost je stopnja zaupnosti informacij.

2. Razčlenitev kategorij posledic kibernetskih incidentov

Učinek	
Regulatorni	Intervencija regulatorja (kazni, omejitve poslovanja, stroški odgovarjanja regulatorju)
Na stranke	Vpliv na bazo strank, na poslovanje. Stroški nadzora zlorabe informacij strank, izgube zaradi ustavitve poslovanja, izguba konkurenčne prednosti)
Na medije	Vpliv na odnose z javnostmi. Stroški upravljanja odnosov z javnostmi, komunikacije z bančnimi strankami.
Na poslovanje	Vpliv na poslovanje banke zaradi omejevanja vplivov incidenta na poslovne procese, prekinitev pogodbe z določenimi odgovornimi zaposlenimi.
Viri financiranja	Vpliv na vire financiranja in stroške kapitala. Izguba depozitov, povečanje zahtevane donosnosti kapitala.
Forenzični	Vpliv na poslovanje banke zaradi forenzičnih preiskav.

Posledice napada so različne glede na to, ali je prizadeta

Zaupnost podatkov

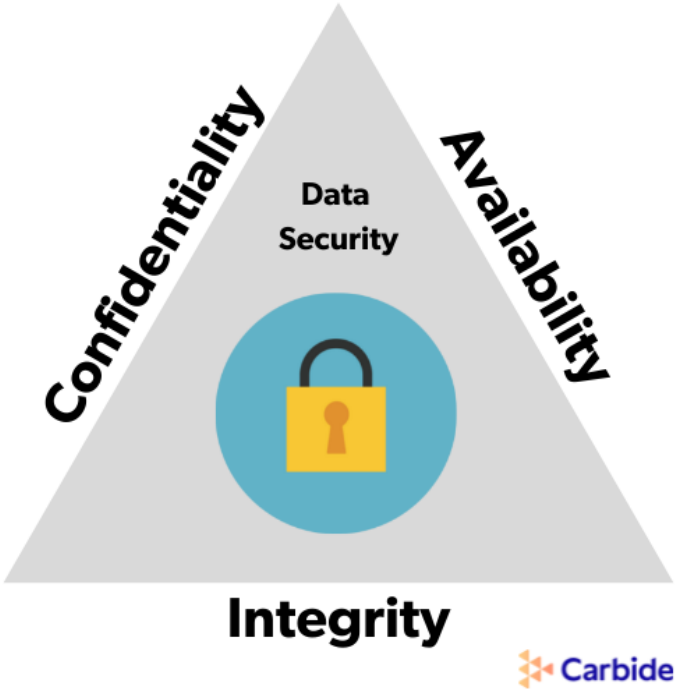
- Pravni in regulatorni stroški
- Pogodbene kazni in prekinitve pogodb
- Učinki na ugled

Neokrnjenost podatkov

- Oportunitetne izgube zaradi produktivnosti
- Učinki na ugled

Razpoložljivost podatkov

- Začasna: nadomestna vrednost, ugled, oportunitetne izgube
- Trajna: izbubljena prihodnja korist, nadomestna vrednost, ugled, oportunitetne izgube



3. Opredelitev razmerja med incidentom in posledicami

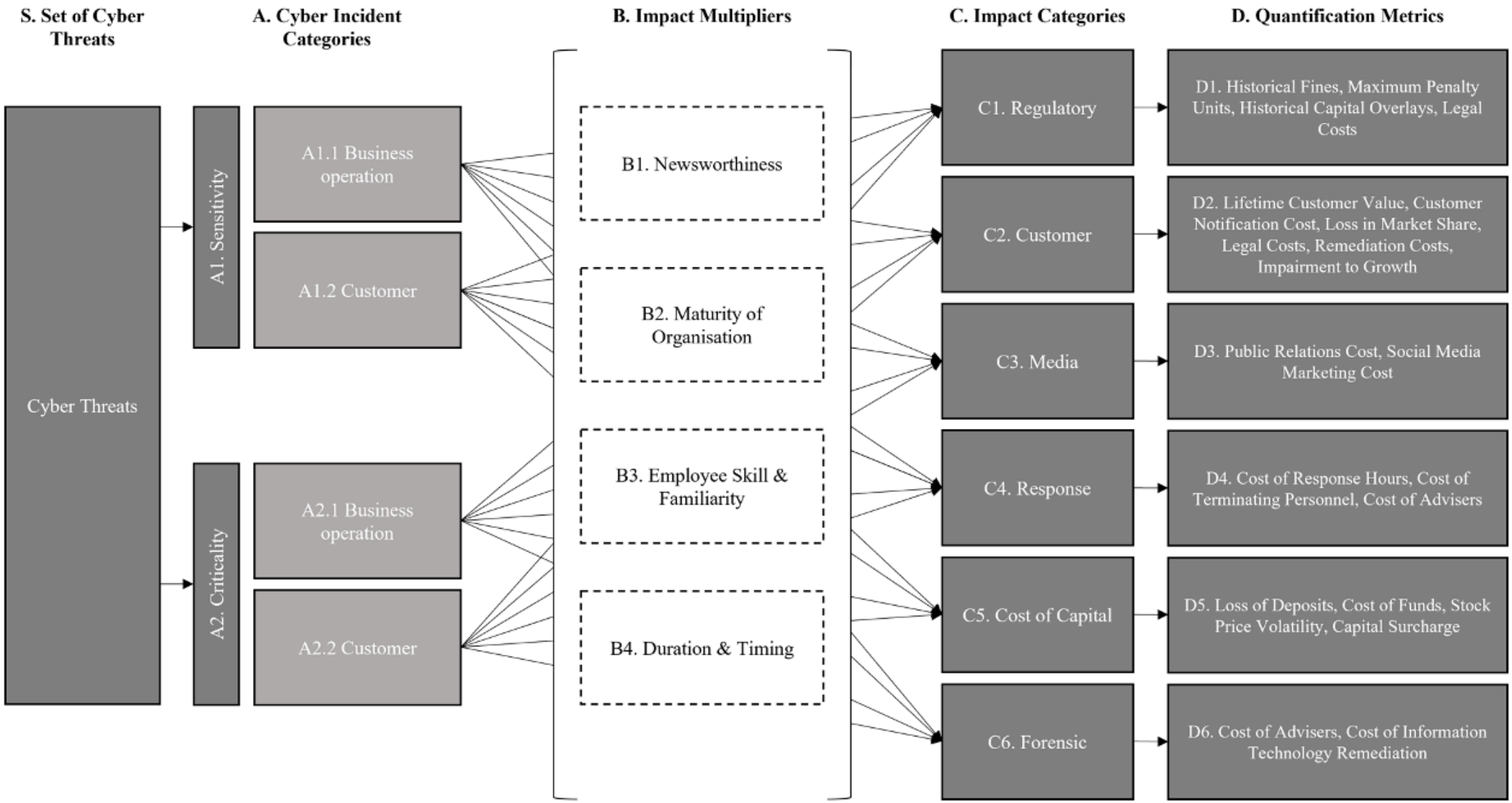
Na resnost posledic vpliva več dejavnikov

1. **Medijska pokritost dogodka**
2. **Zrelost organizacije**
3. **Veščine zaposlenih**
4. **Čas in trajanje dogodka**

4. Opredelitev finančnih kazalnikov posledic

Učinek	
Regulatorni	Kazni, Ocena stroškov odgovarjanja regulatorjem, Ocena pravnih stroškov
Na stranke	Življenjska vrednost strank, Stroški obveščanja strank, Izguba tržne vrednosti, Pravni stroški, Stroški tožb strank, Zmanjšanje rasti ali negativna rast prihodkov
Na medije	Stroški obveščanja javnosti, Trženjski stroški na socialnih medijih
Na poslovanje	Stroški ustavljenega poslovanja, Pravni stroški s prekinitvami delovnih pogodb, Stroški svetovalcev, Tehnološka posodobitev
Viri financiranja	Izguba depozitov in povečanje stroškov financiranja, Vpliv na ceno delnice, Pribitek kapitala
Forenzični	Stroški svetovalcev in ekspertov, Oportunitetni stroški lastnih zaposlenih z ukvarjanjem z incidentom

2. Analiza tveganj



3. Evalvacija tveganja

Primerjaj	rezultate analize tveganj s **kriteriji sprejemanja tveganj**
Prioritiziraj	analizirana tveganja glede na njihovo pomembnost

Donirajte del dohodnine ASEFu

- **1% dohodnine** za financiranje upravičencev do donacij.
- Donacija dela dohodnine vas **ne stane nič**.
- Zadnji rok je **31. december 2023**.

Kako oddati zahtevek:

1. **Elektronsko** prek portala eDavki.
   - Vloga “Zahteva za namenitev dela dohodnine za donacije (Doh-Don)”.
   - V vlogi vpišite naziv organizacije (Inštitut ASEF),
   - davčno številko (84740175) in
   - višino odstotka, ki ga namenjate (0,1, %, 0,2 %, … 1%).
2. Osebno ali po pošti pri pristojnem finančnem uradu z izpolnjevanjem **fizične kopije dokumenta.** Dokument lahko dobite danes pri nas.

Z vašo donacijo bo ASEF lahko še dalje omogočal nove priložnosti za mlade talente in povezoval Slovenijo s svetom.

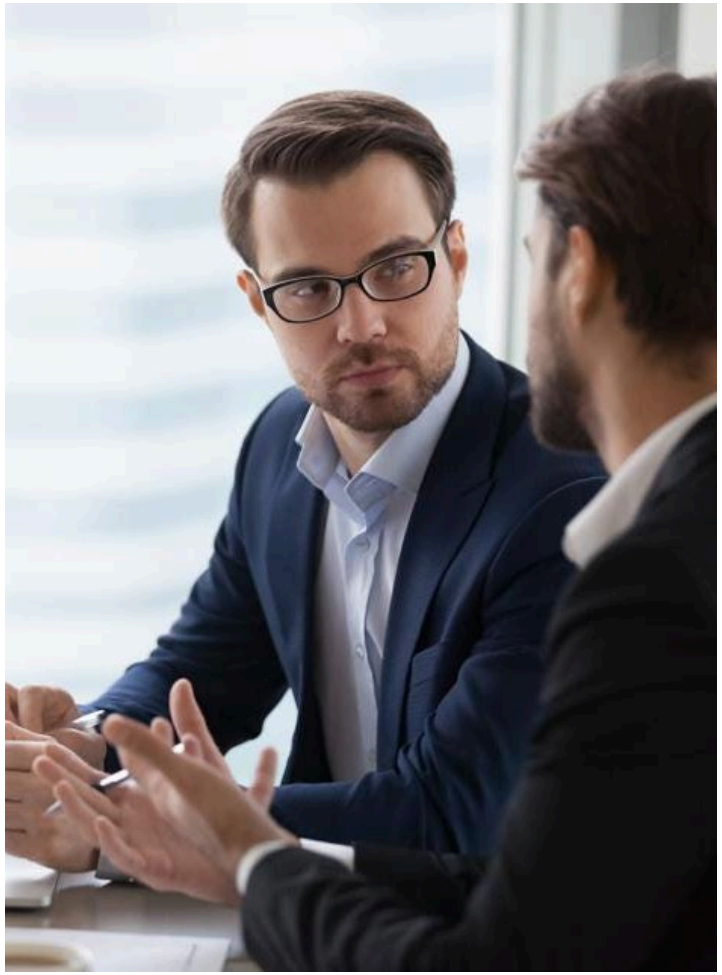
THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Hvala za pozornost!

s.slapnicar@uq.edu.au

"Če tveganje izraziš s številko, se zdi, kot da si naredil fantastično oceno. Zgleda zelo natančna. Saj ne more biti, da so jo ljudje ugibali.

Naredil sem vse, da ocenjevanje tveganj ne bi bila mehanična vaja. Vedno zahteva diskusijo in razsodnost. Ali je znanost v tem? Ne, je bolj pripoved." (Direktor upravljanja s tveganji v visokošolski instituciji)



Iz naše raziskave (Measuring and managing cyber risk, Slapničar, Axelsen, Eulerich, 2023)

Standardi na področju ocenjevanja kibernetskih tveganj

Mednarodni standardi in okviri

- ISO/IEC 27005 (2022) in ISO/IEC 31000 and 31010
- NIST
  - SP800-30: Guide for conducting risk assessment
  - SP800-37: RMF for Information Systems
  - SP800-39: Managing Information Security Risk
  - SP800-161: Managing Supply Chain Risk
  - SP800-221: Integration ICT and Corporate Risk
- ISACA Risk IT Framework (2022); Cyber risk Quantification. www.isaca.org/cyberrisk-quantification
- COBIT ali NIST CSF (za ocenjevanje zrelosti kontrol)

Strokovna literatura na področju ocenjevanja kibernetskih tveganj

- Freund and Jones, 2014: Factor Analysis of Information Risk (FAIR).
- Hubbard, Seiersen, 2016. How to measure anything in cybersecurity risk.
- Hubbard, 2020. The failure of risk management: Why it's broken and how to fix it.

Viri, citirani v tem predavanju

- Leitner-Hanetseder, S., Lehner, O. M. (2023). **AI-powered information and Big Data: current regulations and ways forward in IFRS reporting**, Journal of Applied Accounting Research 24(2), 10.1108/JAAR-01-2022-0022
- Pollmeier S., Bongiovanni I., Slapničar S. (2023). **Designing a financial quantification model for cyber risk: a case study in a bank**. Safety Science, 159 106022, doi: 10.1016/j.ssci.2022.106022
- Slapničar S., Axelsen M., Bongiovanni, I., Stockdale, D. (2022). **A pathway model to 5 lines of accountability in cybersecurity governance**. International Journal of Accounting Information Systems. Accepted for publication. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176559
- Slapničar S., Axelsen M., Euelrich M.: **Measuring and managing cyber risk**. European Accounting Association Congress, Helsinki, 24-26 May 2023
- Varela P. (2022). **ISO/IEC 27005:2022 What is new?** https://www.linkedin.com/pulse/isoiec-270052022-what-new-paul-varela/?trk=pulse-article
- Vohradsky D. (2022). **The cyberrisk quantification journey. ISACA Journal, vol. 2**