Gospodarska zbornica Slovenije

Zbornica za poslovanje z nepremičninami

Zagotavljanje kibernetske varnosti v organizaciji

Božidar Dajčman

Božidar Dajčman

- direktor varnosti v večji slovenski banki

- 25+ let v finančni industriji
- Različne vloge znotraj in zunaj IT
- CISO od 2014
- CSO od 2017
- Nepremičnine?

Agenda

- Kaj se nam lahko zgodi?
- Kako se lotimo zagotavljanja varnosti?
- Koraki upravljanja varnosti
- Vloge pri zagotavljanju varnosti
- Nekaj namigov

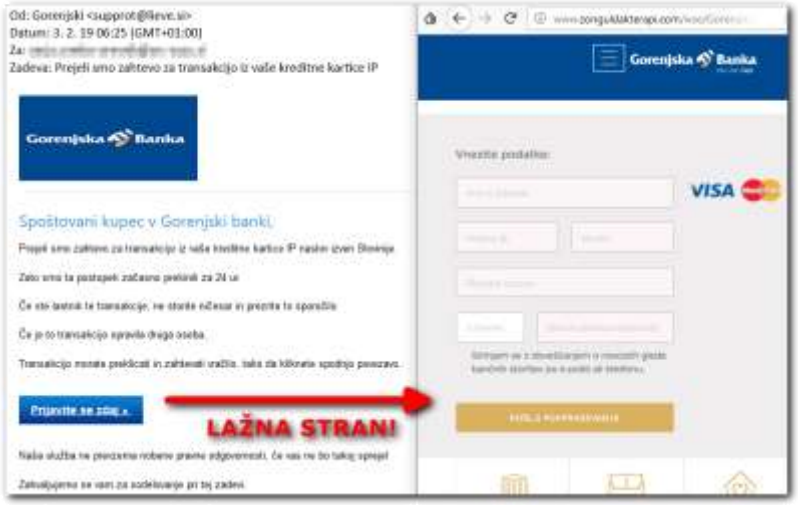
Kaj se nam lahko zgodi?

Končno na našem trgu. Naravni pripravek, ki izboljšuje sluh in je največji sovražnik tinitusa in vnetja ušes.

23-letna milijonarka iz Ljubljane pripoveduje, kako je postala bogata

Prevare „low-tech“

Prevare z uporabo nekaj tehhnologije

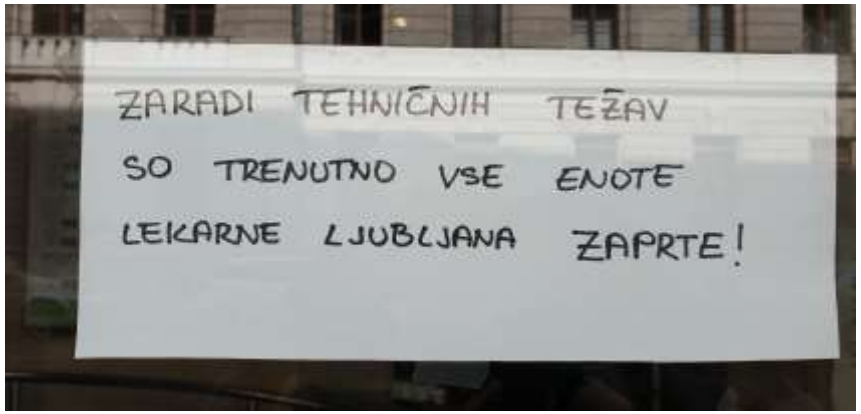


Update 9.2.2022 ob 2.30: Vzdrževalna dela so zaključili.

POP TV hekerski napad / kibernetski napad

9.2.2022 popoldne, dan po hekerskem napadu, so na POP TV / Pro Plus podali nekaj več pojasnil.

> *Celotnega obsega napada še ne moremo oceniti, trenutno smo vse svoje sile usmerili v to, da bodo naši glavni sistemi v najkrajšem času postavljeni v prvotno delovanje, kar bo omogočilo nemoteno delovanje televizijskih programov in spletnih strani.*



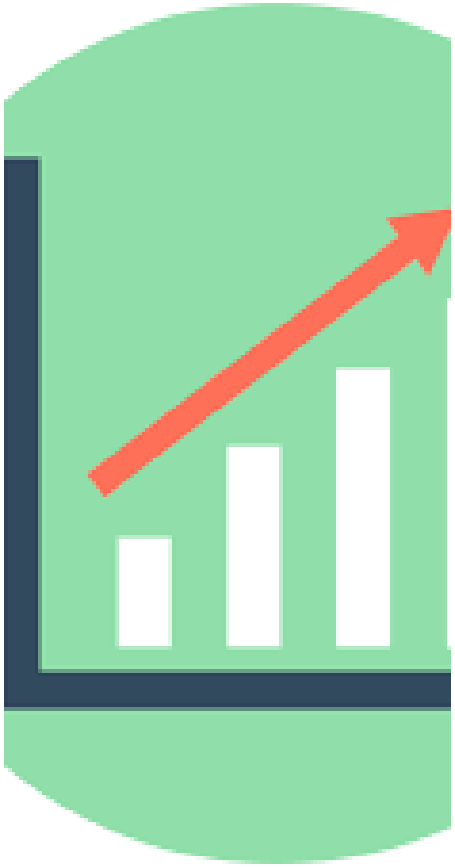
Kibernetski napadi

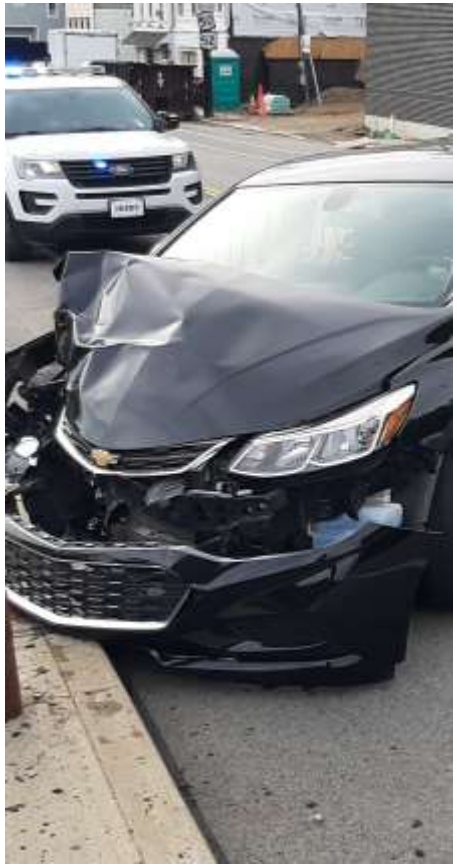
Kolikšna je škoda?

SI-CERT: Poročilo o kibernetski varnosti za leto 2022

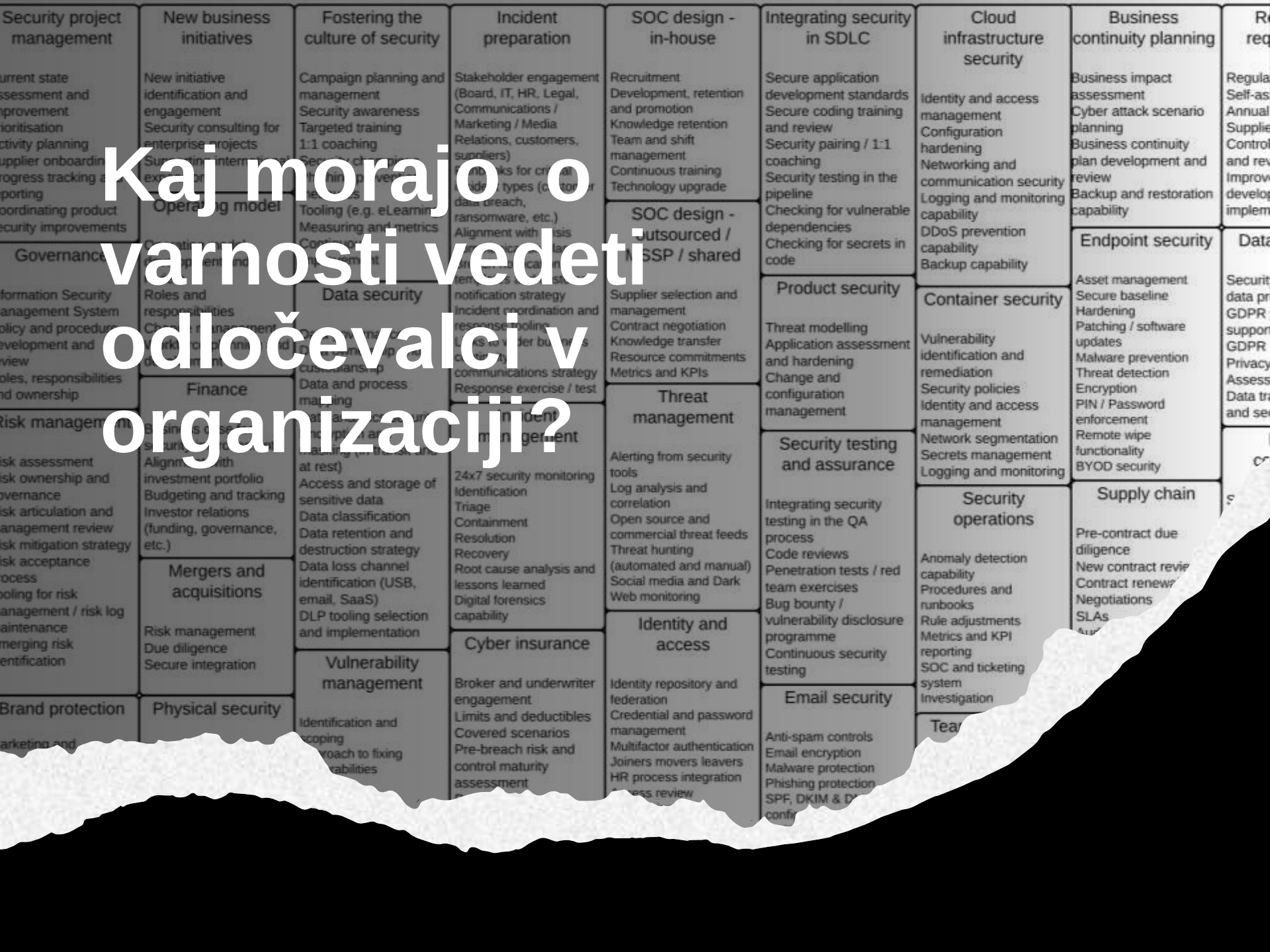
Oškodovanje	Opis
najvišja oškodovanja	
3.000.000 EUR	Najvišji znesek, na srečo neuspešnega, oškodovanja v letu 2022 (šlo je za vrivanje v poslovno komunikacijo, ang. business email compromise oz. BEC fraud) – prenos denarja je bil pravočasno zaustavljen zaradi nadzornih mehanizmov bank in Urada RS za preprečevanje pranja denarja.
400.000 EUR	Najvišje oškodovanje fizične osebe (izsiljevanje z lažnimi grožnjami o pregonu).
povprečna oškodovanja	
58.000 EUR	Povprečno oškodovanje v nigerijski prevari (vnaprejšnje plačilo).
31.000 EUR	Povprečno oškodovanje v ljubezenski prevari.
19.000 EUR	Povprečno oškodovanje zaradi lažne tehnične pomoči Microsofta.
3.400 EUR	Povprečno oškodovanje pri phishing napadu (zloraba kreditne kartice).
780 EUR	Povprečno oškodovanje pri spletnem nakupovanju.

Kako se lotimo zagotavljanja varnosti - izhodišča?





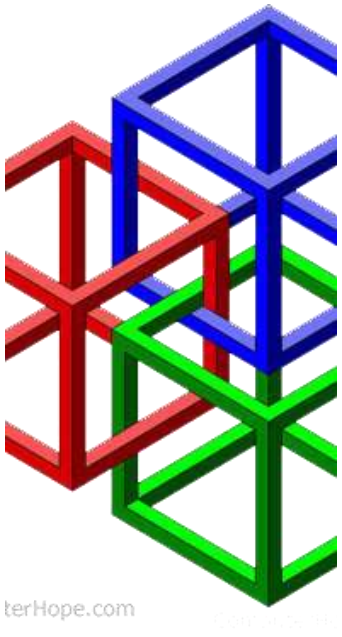
Svet okoli nas


Kaj morajo o varnosti vedeti odločevalci v organizaciji?

Odločanje na podlagi strahu?

Odločanje na podlagi nadzora tveganj!

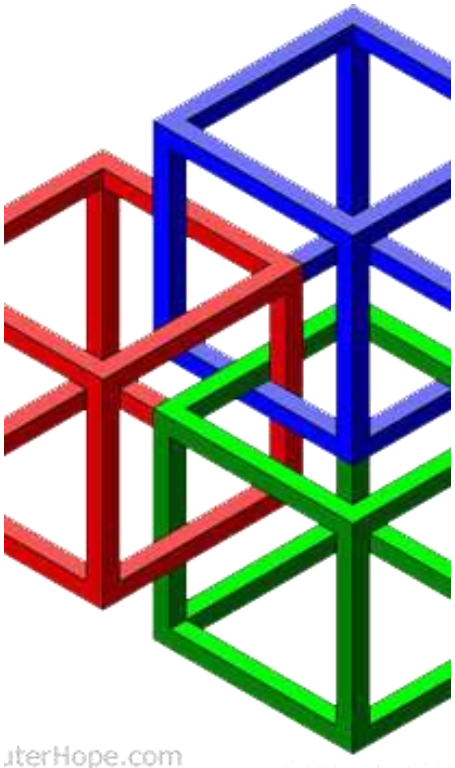
Koraki upravljanja varnosti



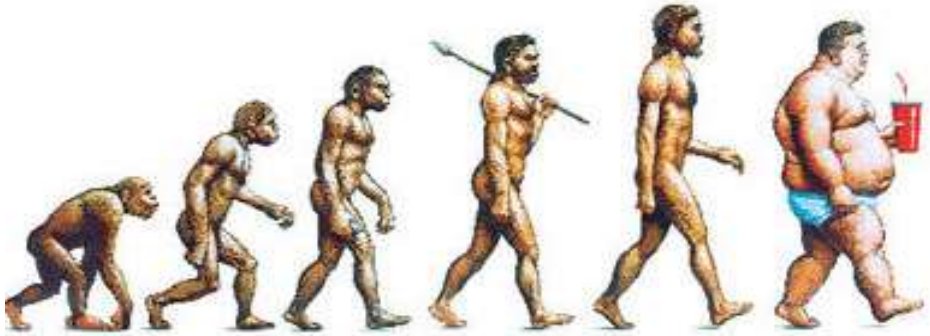
Kje smo?
Kam hočemo?

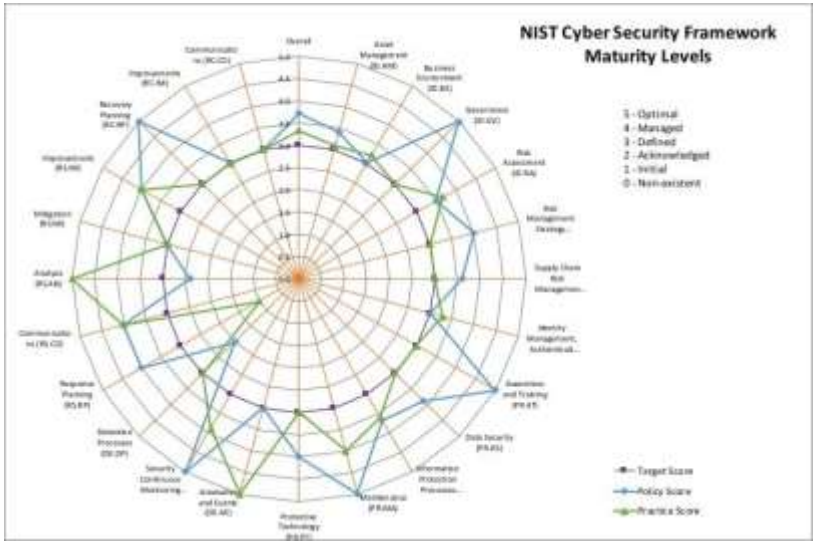
Komunikacija

Okvir upravljanja varnosti



Stopnja zrelosti



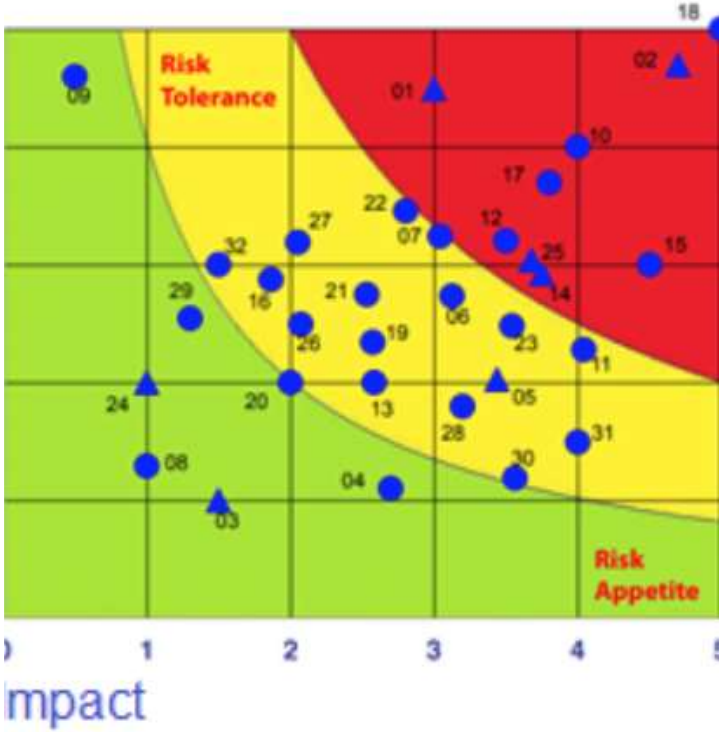


	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
People	Activities unstaffed or uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
Process	No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
Technology	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

LEVEL 1 Initial	LEVEL 2 Established	LEVEL 3 Self-Assessed	LEVEL 4 Integrated	LEVEL 5 Vanguard
• Minimal cyber awareness • Minimal cyber info sharing • Minimal cyber assessments and policy & procedure evaluations • Little inclusion of cyber into Continuity of Operations Plan (COOP)	• Leadership aware of cyber threats, issues and imperatives for cyber security and community cooperative cyber training • Informal info sharing/ communication in community; working groups established; ad-hoc analysis, little fusion or metrics; professional orgs established or engaged • No assessments, but aware of requirement; initial evaluation of policies & procedures • Aware of need to integrate cyber security into COOP	• Leaders promote org security awareness; formal community cooperative training • Formal local info sharing/cyber analysis. initial cyber-physical fusion; informal external info sharing/ cyber analysis and metrics gathering • Autonomous tabletop cyber exercises with assessments of info sharing, policies & procedures, and fusion; routine audit program; mentor externals on policies & procedures, auditing and training • Include cyber in COOP; formal cyber incident response/recovery	• Leaders and orgs promote awareness; citizens aware of cyber security issues • Formal info sharing/ analysis, internal and external to community; formal local fusion and metrics, initial external efforts • Autonomous cyber exercises with assessments of formal info sharing/local fusion; exercises involve live play/metrics assessments • Integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery	• Awareness a business imperative • Fully integrated fusion /analysis center, combining all-source physical and cyber info; create and disseminate near real world picture • Accomplish full-scale blended exercises and assess complete fusion capability; involve/ mentor other communities/entities • Continue to integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery

	Impact Rating	Likelihood Rating	Inherent Risk	Control Assessment	Residual Risk
P-DRP	M	L	M	S	L
control & governance	M	M	M	S	L
n incomplete/incorrect	H	M	H	S	M
e provider	H	M	H	S	M
utsource provider	H	L	M	S	L
	H	L	M	S	L
ersonnel / experience	H	L	H	MOD	H
	H	H	H	MOD	H
	H	L	M	MOD	M
ayment from client	L	L	L	S	L
	M	L	M	S	L
ownturn	M	M	M	S	L
olan	H	L	H	S	M
	H	M	H	MOD	H
	M	H	L	S	L
	H	L	M	S	L

m, L = Low, S = Satisfactory, MOD = Moderate, W = Weak



Ocena tveganj

Strateško in taktično načrtovanje

Vloge pri zagotavljanju varnosti

Kdo je zadolžen za kibernetsko varnost v organizaciji?

Vloge pri kibernetski varnosti

- Vse zaposleni
- Strokovne službe
- Vodstvo organizacije

Kaj namesto nas lahko naredijo drugi?

- MSSP (managed security service providers)
- **Odgovornosti ne moremo prenesti, zato je razumevanje kibernetskih tveganj potrebno znotraj organizacije.**

Nekaj namigov

Ozaveščenost zaposlenih!

SI-CERT (nacionalni odzivni center)

www.varninainternetu.si
www.varnivpisarni.si

Začnite pri začetku

- Upravljanje informacijskih sredstev
- Omejene dostopne pravice
- Požarna pregrada
- Zaščita pred zlonamernimi programi
- Nameščanje varnostnih popravkov
- Avtentikacija
- Varnostne kopije
- …

Zagotovite si neodvisno mnenje

Pripravite se na incident!

- Koga boste poklicali?
- Kdo bo sprejemal odločitve?
- Kako boste komunicirali z javnostjo in nadzornimi institucijami?
- Kako boste okrevali po napadu?

Hvala za pozornost.