HANFA

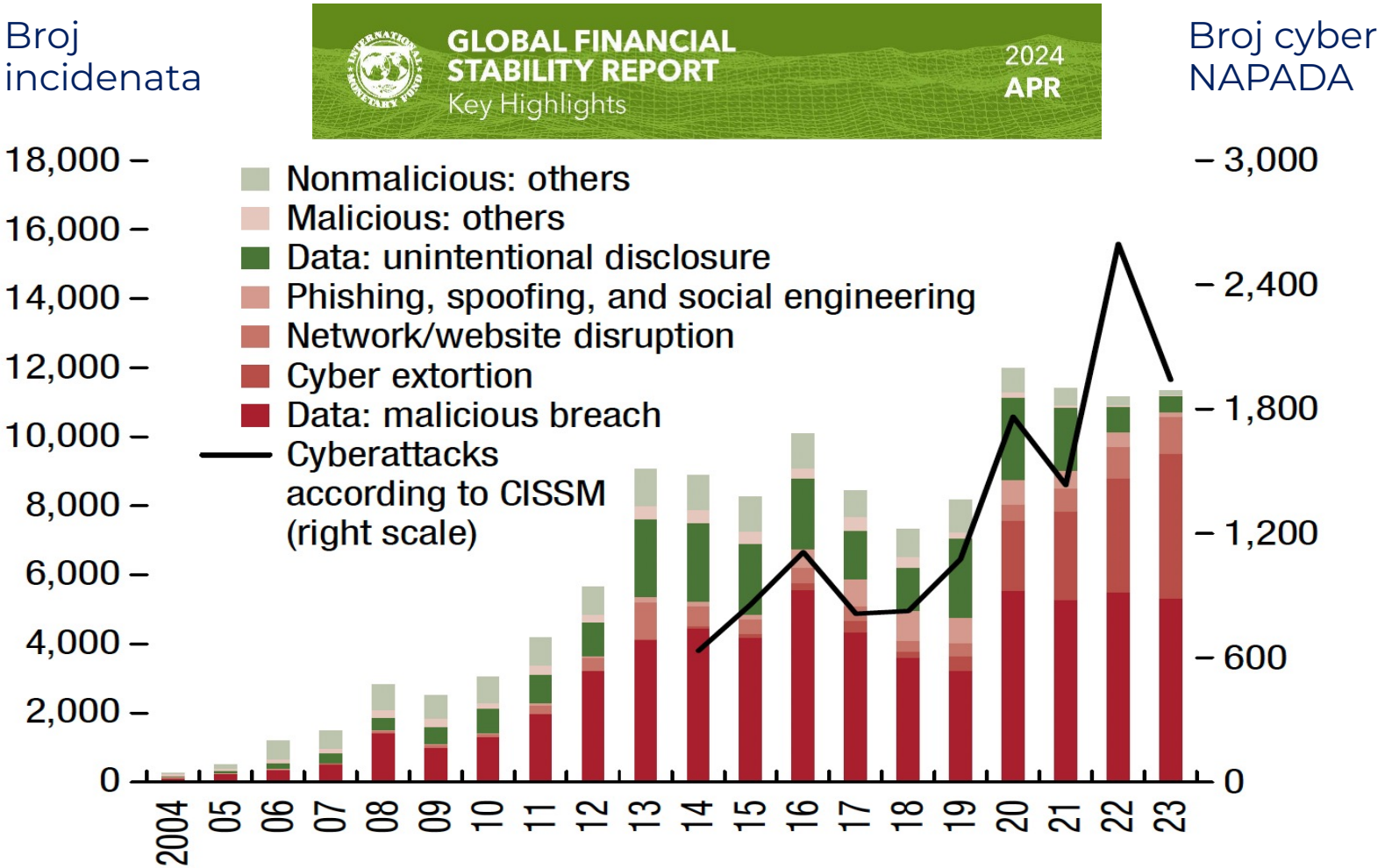
HRVATSKA AGENCIJA ZA
NADZOR FINANCIJSKIH USLUGA

Kako raditi uz kibernetičke napade?

dr.sc. Ante Žigman
Predsjednik Upravnog vijeća

25.11.2024.

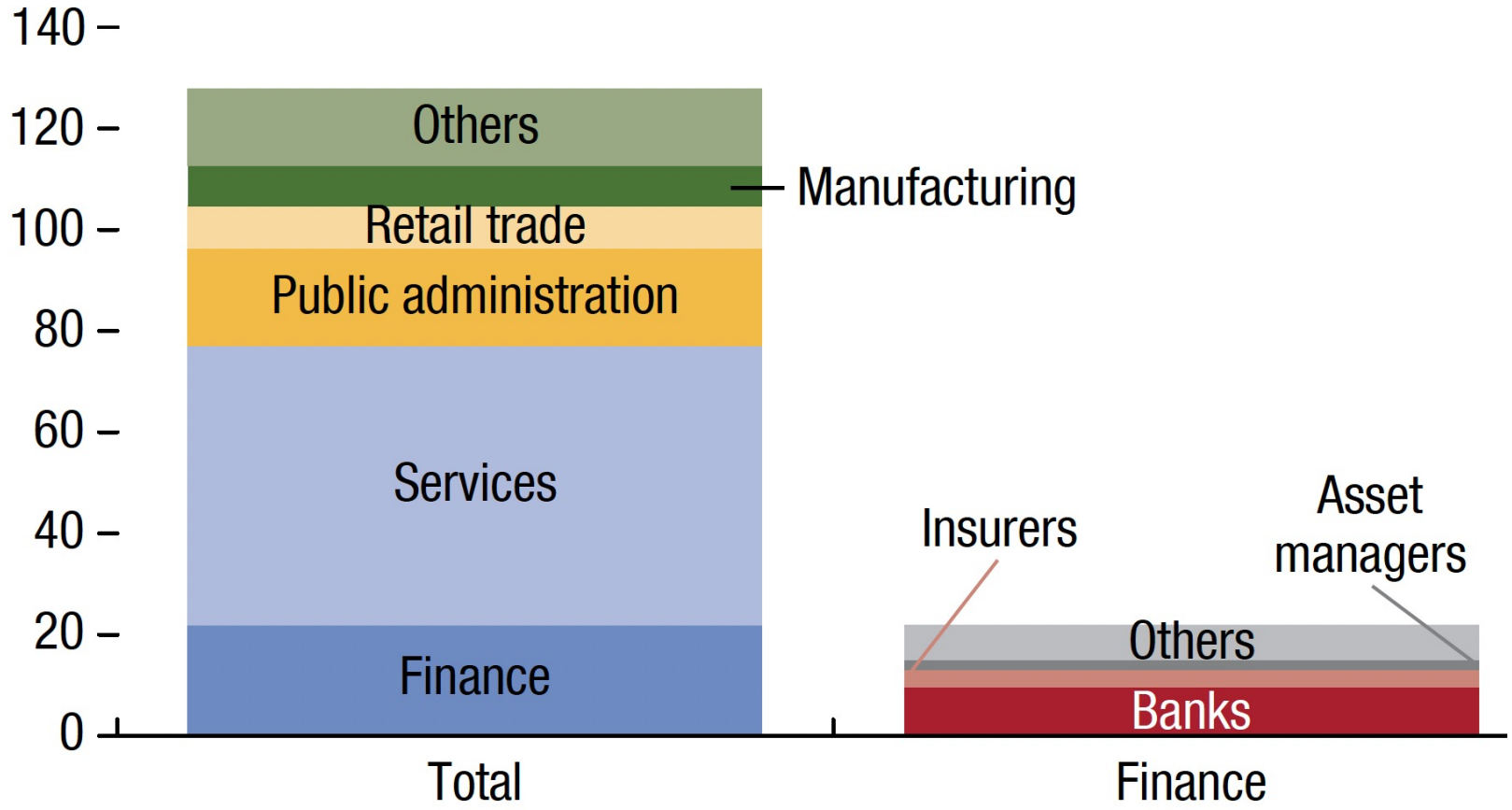
BROJ CYBER INCIDENATA GLOBALNO 2004.-2023.



IMF travanj 2024. CISSM = Center for International and Security Studies , Maryland

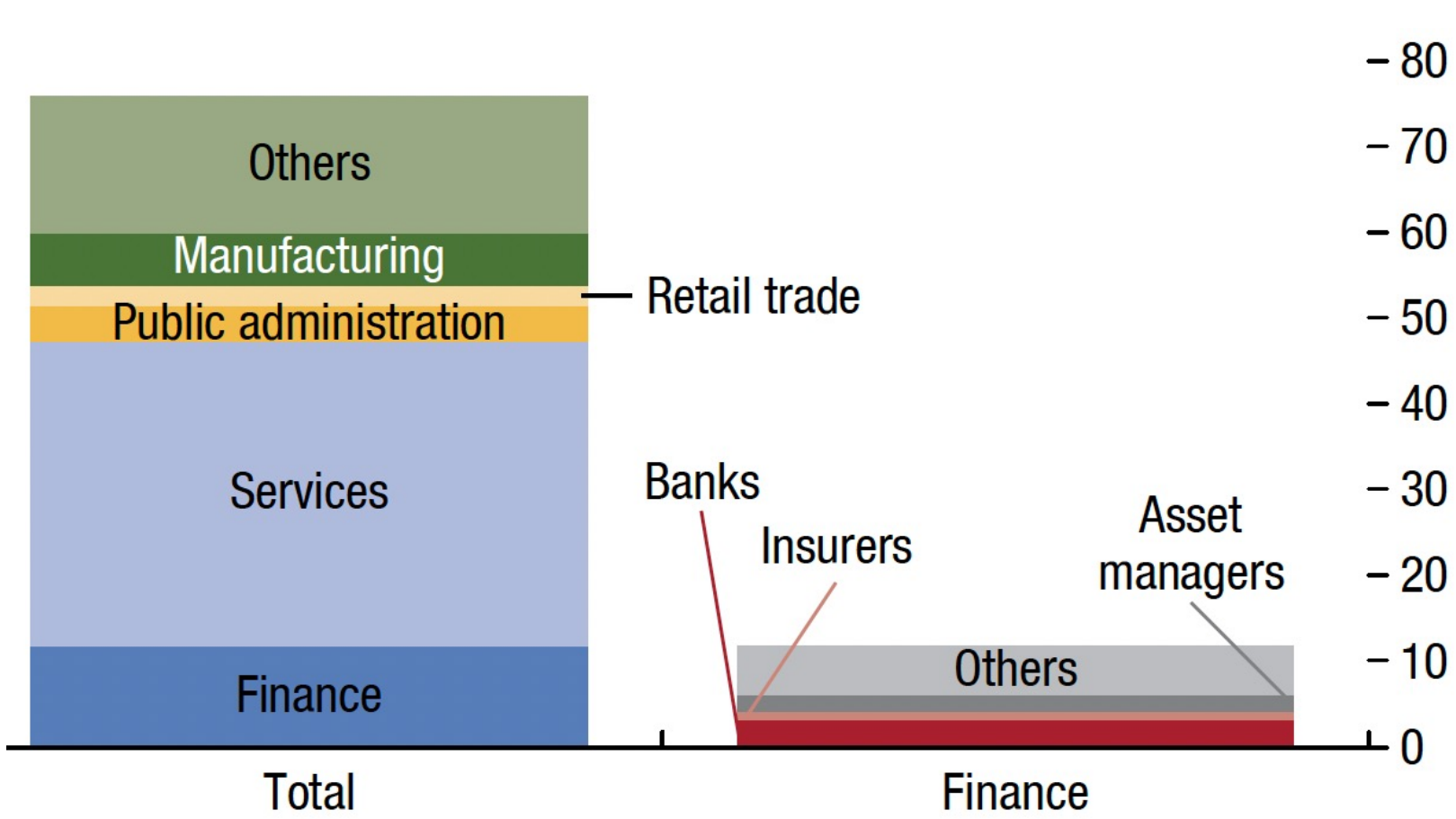
UKUPNO CYBER INCIDENTI GLOBALNO 2004.-2023.

Broj incidenata tisuće



IMF travanj 2024. CISSM = Center for International and Security Studies, Maryland

GUBICI – CYBER INCIDENTI GLOBALNO 2004.-2023.

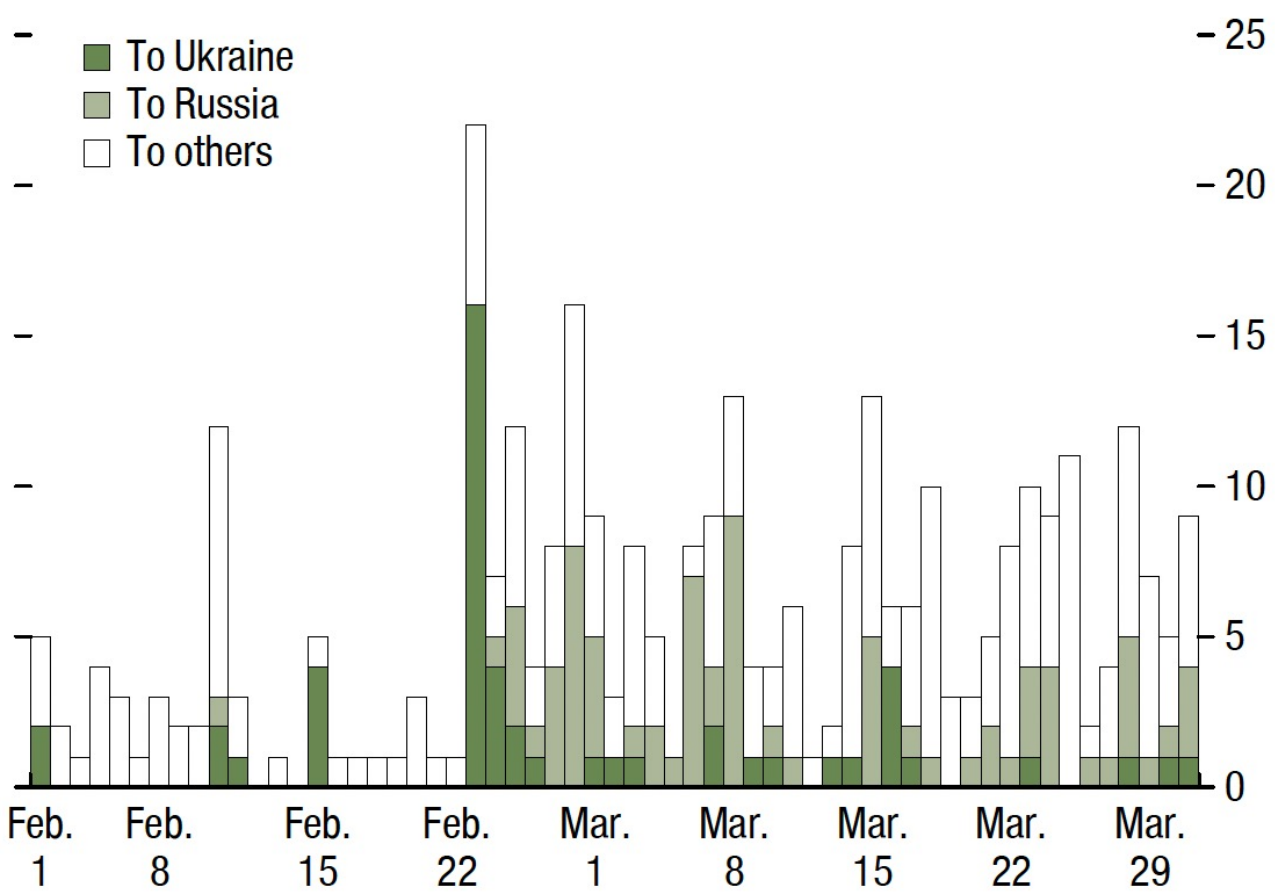


IMF travanj 2024. CISSM = Center for International and Security Studies, Maryland

GEOPOLITIČKI ODNOSI I CYBER NAPADI

Napad Rusije na Ukrajinu

Broj cyber napada Dnevno prije i poslije



Izvor: Advisen Cyber Loss Data; CISSM (Harry i Gallagher 2018.); ITU publikacija; IMF kalkulacija

MMF IZVJEŠĆE, travanj 2024. (poglavlje 3)

- Broj kibernetičkih napada je gotovo dvostruko veći u odnosu na razdoblje prije COVID-19
- Financijski sektor visoko izložen kibernetičkim rizicima – približno 20% svih napada
- Do sada kibernetički incidenti nisu bili sistemske razine ali rizik postoji
- Poremećaj u radu kritičnih sustava može dovesti do većeg incidenta zbog visoke razine povezanosti I međuovisnosti
- Nova regulativa EU kao i nacionalne razine (DORA, NIS2) će značajno unaprijediti stabilnost i umanjiti učestalost incidenata

CYBER HIGIJENA – NOVA ETAPA DRUŠTVENOG RAZVOJA

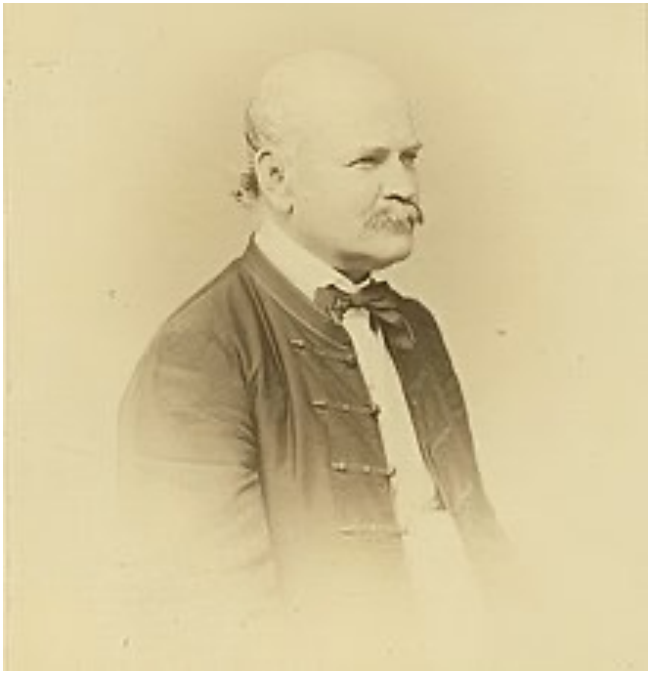
- Liječnik u Općoj bolnici u Beču
- Empirijski otkrio da se infekcije mogu značajno smanjiti mjerama HIGIJENE

pranje ruku otopinom klora i limete

- Smrtnost rodilja na jednom odjelu se smanjila s 18% na 2 %
- Objavio je 1861. knjigu o svojim saznanjima, ali ga je znanstvena javnost odbila
- Louis Pasteur je dokazao teoriju mikroba godinama kasnije i potvrdio teoretski Semmelweisova opažanja i tvrdnje

Ignaz Philipp Semmelweis

(1818 –1865)



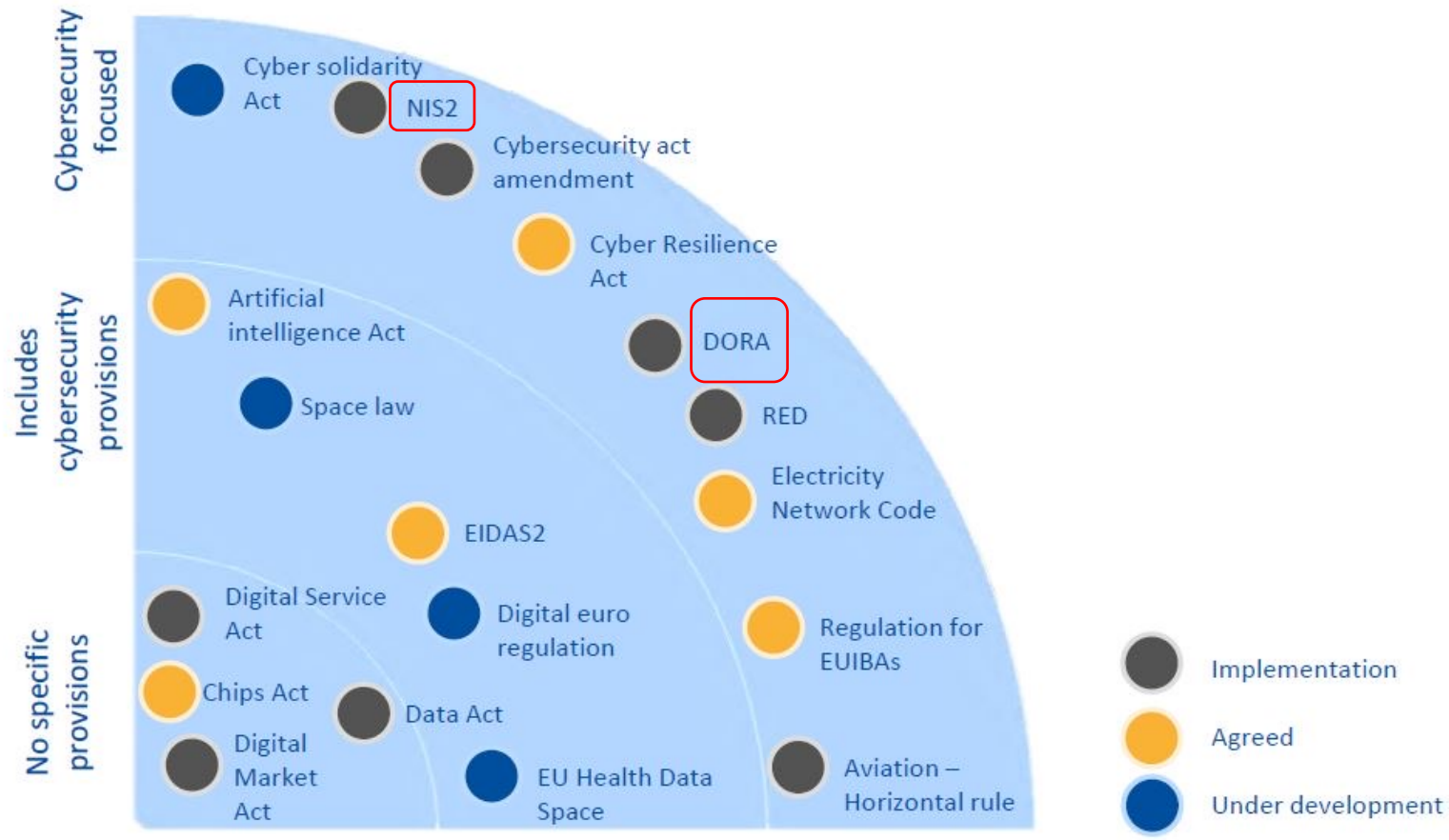
PREPORUKE: CYBER HIGIJENA

- Ne koristiti NA VIŠE MJESTA iste lozinke
- Lozinke: dugačke i složene, slučajni niz
- Pristup – **VIŠESTRUKA PROVJERA** (Multifactor Authentication)
- Provjere – redovne i neovisne: tehničke, procesne i organizacijske
- Ojačavanje – ciljano podešavanje sustava (Security Hardening)
- Threat Inteligence – pratite jeste li aktivna meta (vaša procjena rizika)

TEMELJNI ZAHTJEVI NOVE REGULATIVE: DORA I NIS2/ZKS

- Odgovor na visoku razinu ovisnosti suvremenog društva o digitalnoj tehnologiji i temelj za daljnji razvoj EU
- Organizacijski pristup kontinuitetu upravljanja kibernetičkom sigurnošću i spremnost za daljnji razvoj; Fintech, AI
- Razvoj kulture upravljanja rizikom kibernetičke sigurnosti

EU REGULATIVA – ZNAČAJAN SEGMENT KIBERNETIČKE SIGURNOSTI



* ENISA: WK 10244/2024 INIT, 17. srpnja 2024.

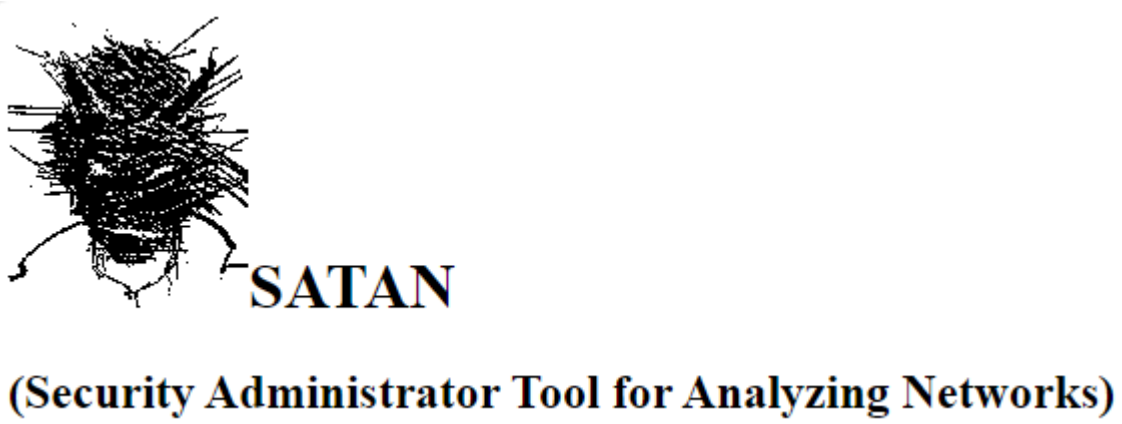
DORA : POČETAK U 2020.

- 24 rujna 2020. Europska komisija objavila je prvi draft Digital Operational Resilience Act (DORA).
- Zakonski tekst nadograđuje postojeće zahtjeve upravljanja IKT rizicima koje su već razvile pojedine EU institucije i povezuje niz inicijativa u jednu Uredbu
- DORA u 2025. uspostavlja znatno čvršću osnovu za EU nadzorna i regulatorna tijela, omogućuje proširenje fokusa nadzora financijskih institucija
- Do sada: financijska stabilnost i zaštita potrošača
- **Od 2025 : podizanje sposobnosti financijskih institucija da održe visoku razinu otpornosti u poslovanju uslijed cyber napada**

NIS2 : ISTODOBNO ZA DRUGE SEKTORE

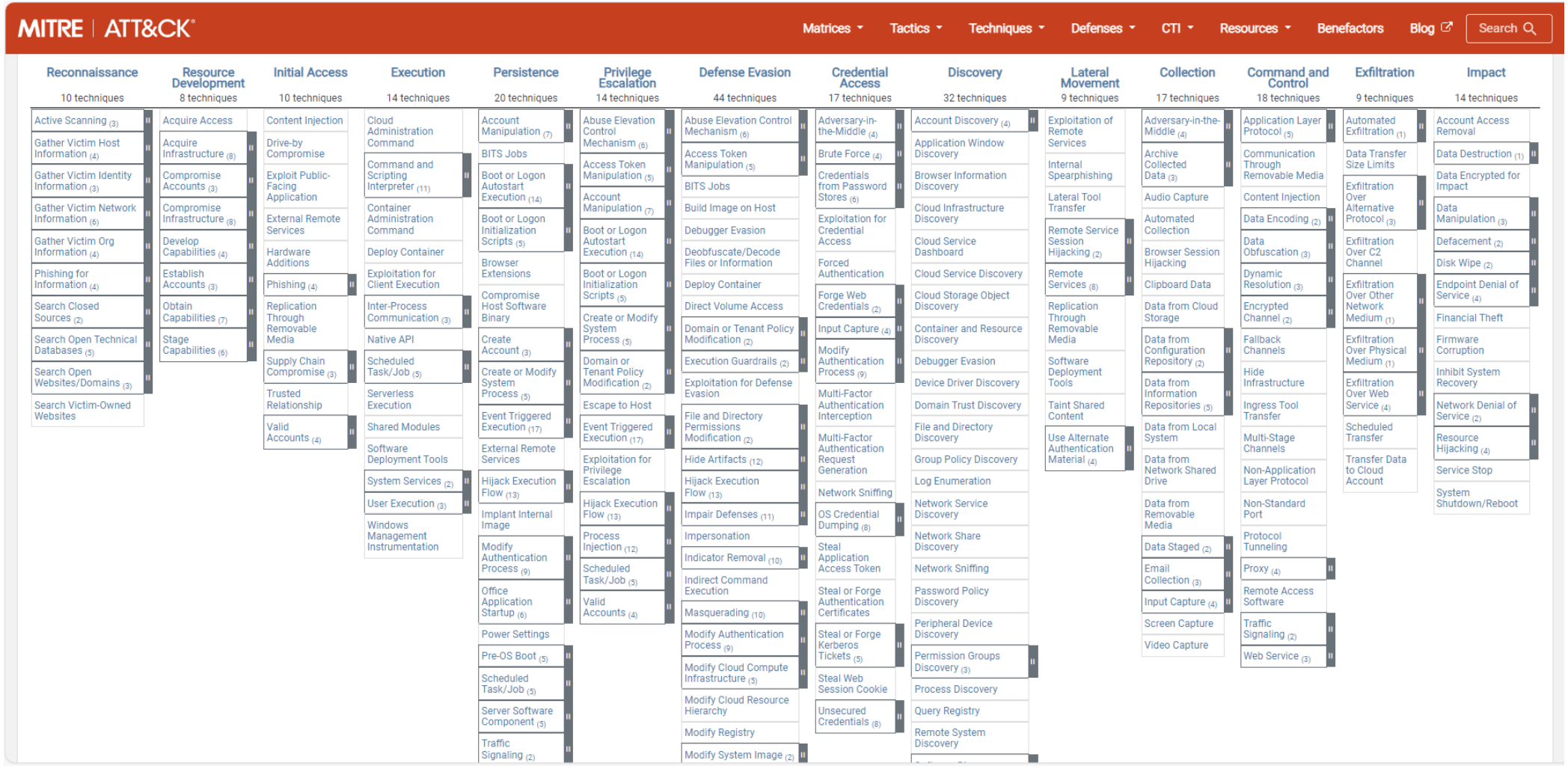
POVIJEST ANALIZE SIGURNOSTI I DRUŠTVENI ODGOVOR

- 1995. dva programera objavila su alat za provjeru sigurnosti S.A.T.A.N.
- Alat je objavljen u časopisu PC Magazine i bio je BESPLATAN
- Ministarstvo pravosuđa SAD je zaprijetilo da povuku alat iz distribucije
- Razlog : alat se može koristiti za napade na mreže i sustave



ALATI DANAS – SUSTAVNO DOSTUPNI

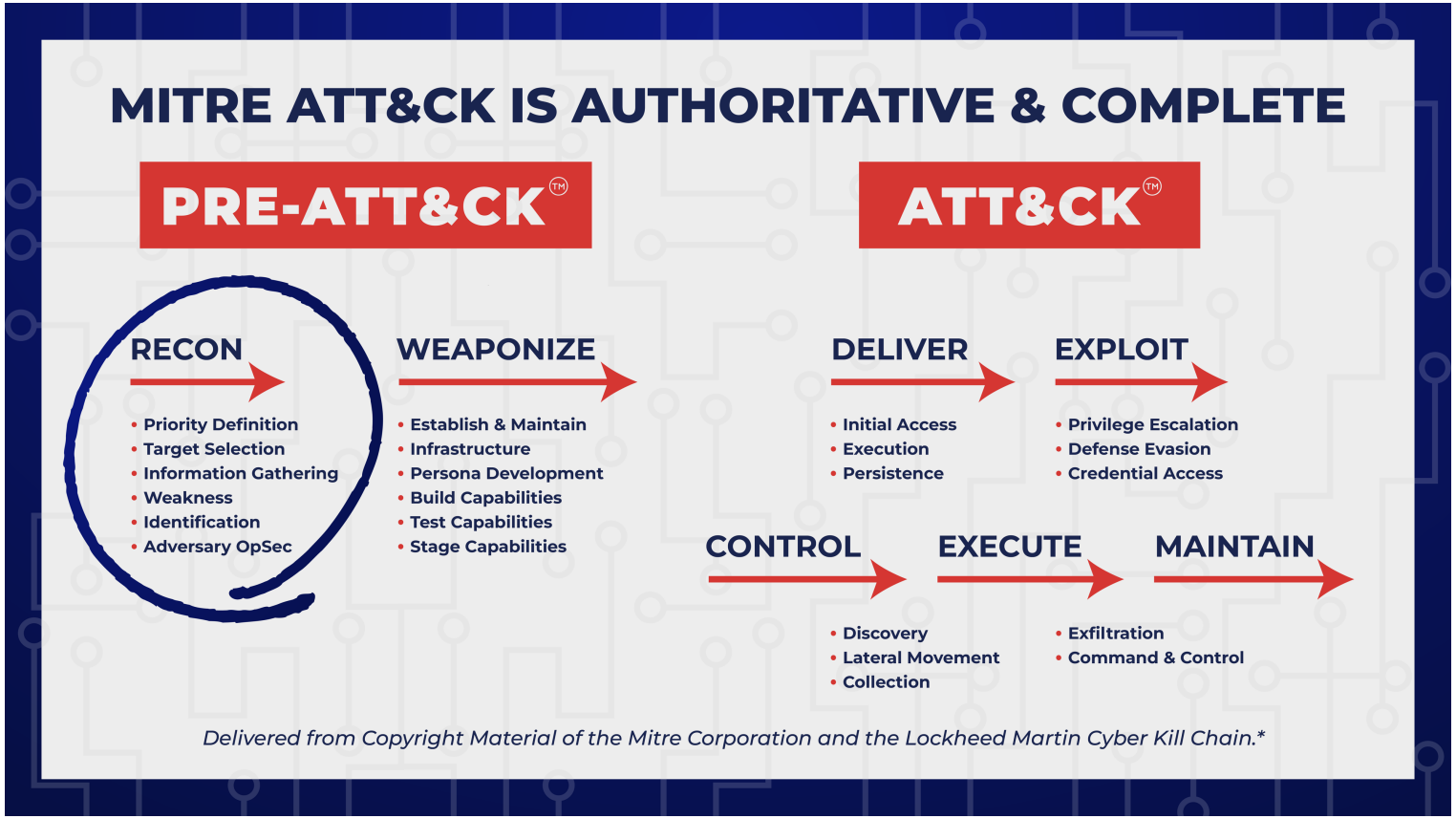
HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA



MITRE korporacija *Adversarial Tactics, Techniques, and Common Knowledge

ANALIZA - JASNO SE RAZLIKUJU FAZE NAPADA

Lockheed Martin postavio je analizu koja se danas koristi u MITRE ATT&CK* okviru



Napad uvijek počinje **izviđanjem**

kako izgledate na mreži kakve ranjivosti imate

gdje mjere nedostaju

IZVIĐANJE (JOŠ PRIMJERA)

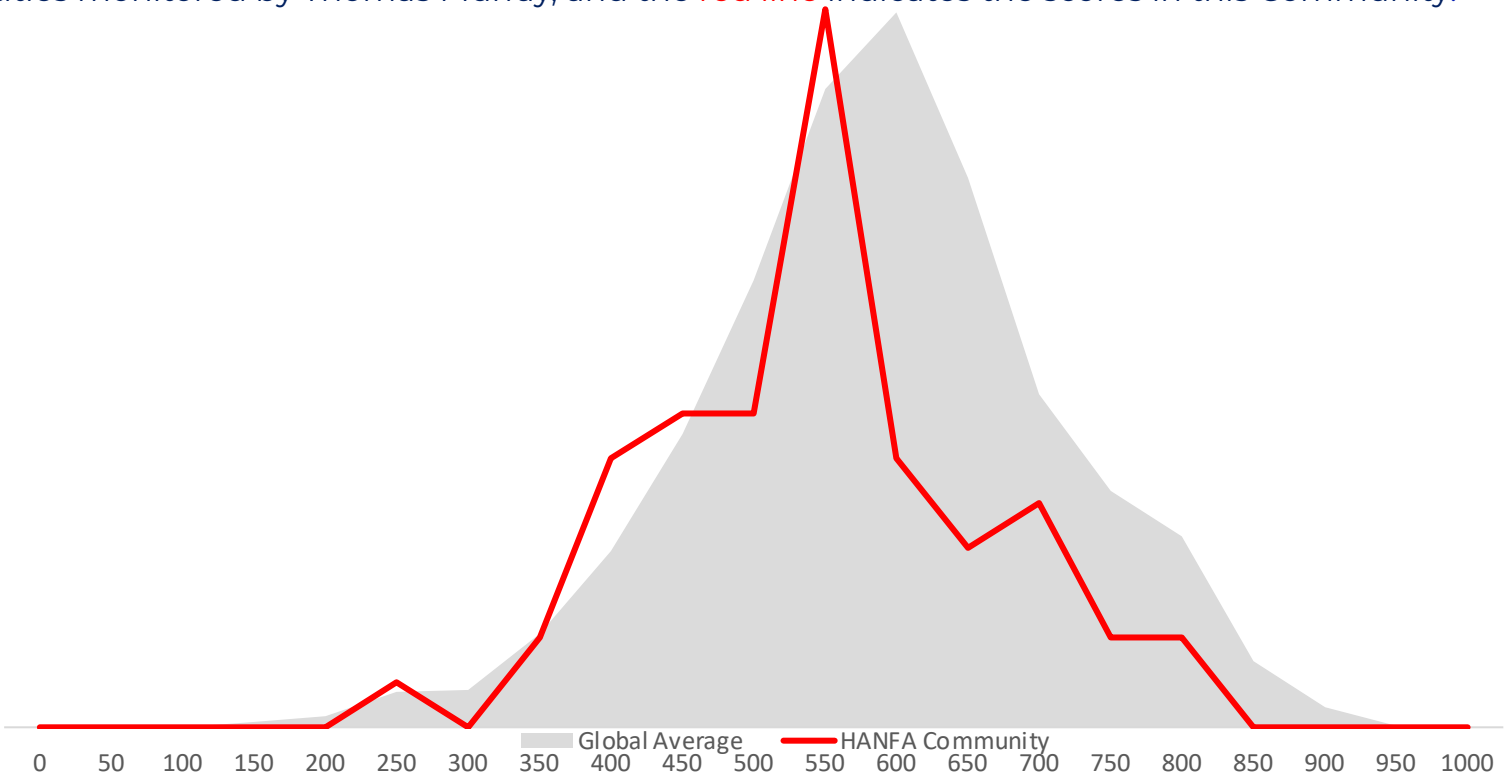
HANFA je angažirala „etičke hakere” da obave izviđanje

Thomas Murray Cyber(UK) obavio je izviđanje SVIH subjekata nadzora Hanfe

- Neinvazivno skeniranje dostupnih sustava na internetu
- Analiza otkrivenih slabosti, ranjivosti koje omogućuju prodor
- Provjera dostupnih informacija na „dark webu”
- Usporedba ukupnog profila rizičnosti s drugim subjektima
- Ne objavljujemo podatke tvrtki
- Pojedinačni podaci su dostupni za daljnju analizu

SCAN: OCTOBER SECURITY SCORES

The distribution shows the number of companies at each Orbit Risk score level. The filled area represents the Global distribution of scores across all entities monitored by Thomas Murray, and the red line indicates the scores in this Community.



Key takeaways:

- Some entities in the HANFA community fall below a score of 500.
- A few entities score less than 400.

HANFA Average	**566**
Global average	**611**

HIGH RISK ISSUES

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

xx

Open Service

Services likely to not be purposely exposed

xx

Vulnerable Service

Services out of date and may require patching

xx

Compromised Server

Servers may be port-scanning or part of a botnet – **Further investigation required**

xx

Stolen Credentials

Stolen credentials may highlight password re-use and could be used for initial access

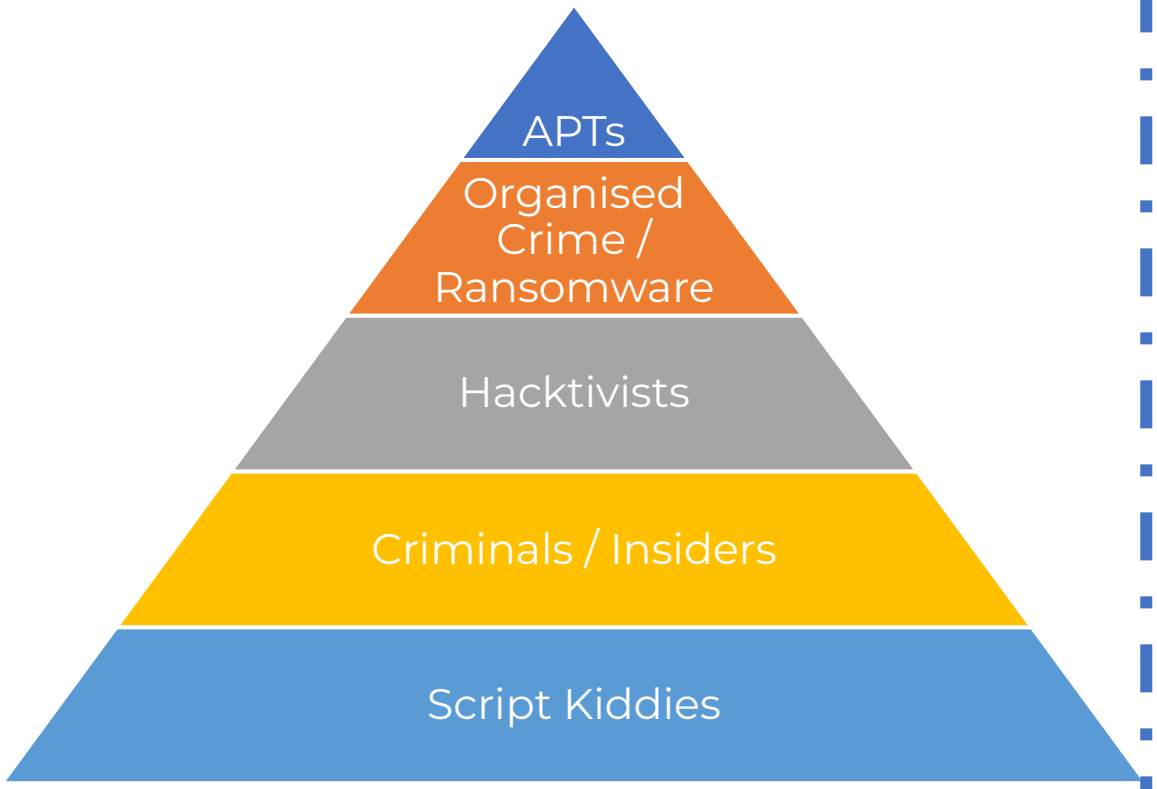
xx

Breached Emails

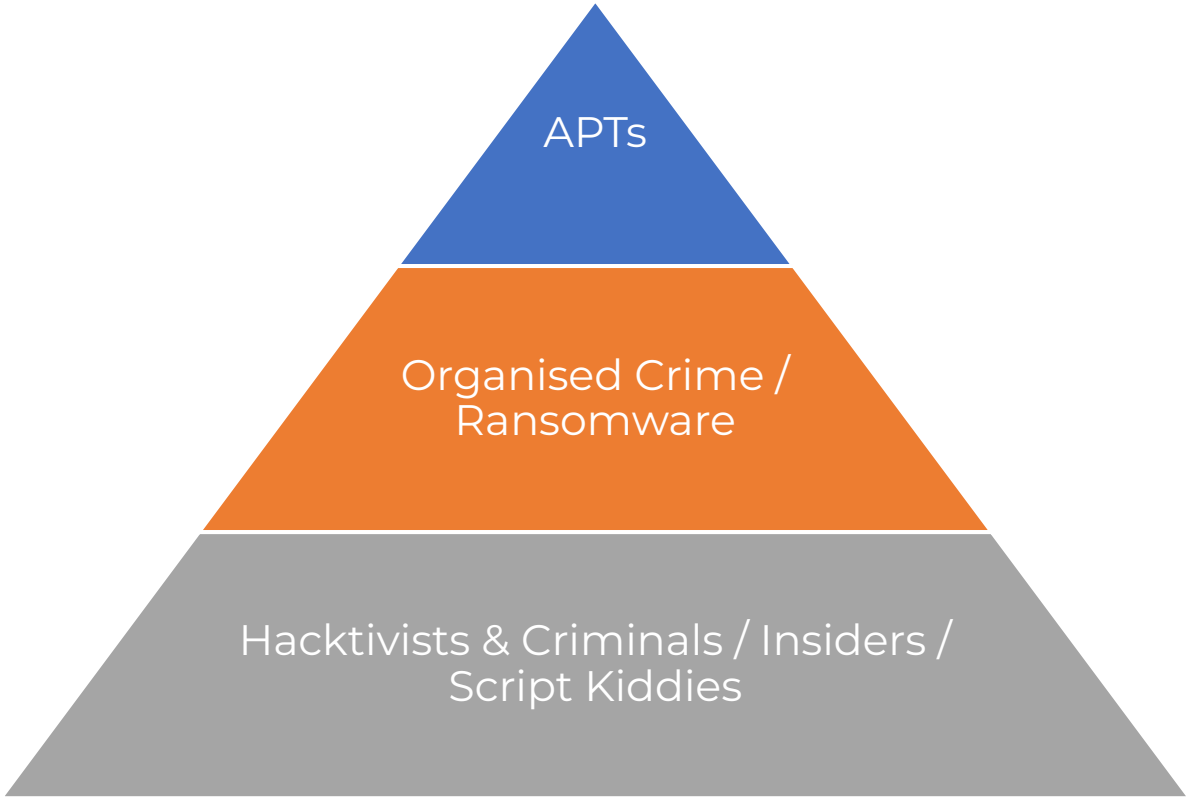
Emails identified in data dumps

Orbit Security Analsysis

NAPADAČI PO VRSTAMA



Post-ChatGPT



KAKO BITI SIGURAN I POSLOVATI

- Učinimo sve što je moguće
- Dosegnimo sigurnost!

NAŠ NOVI MINDSET – *ASSUME BREACH*

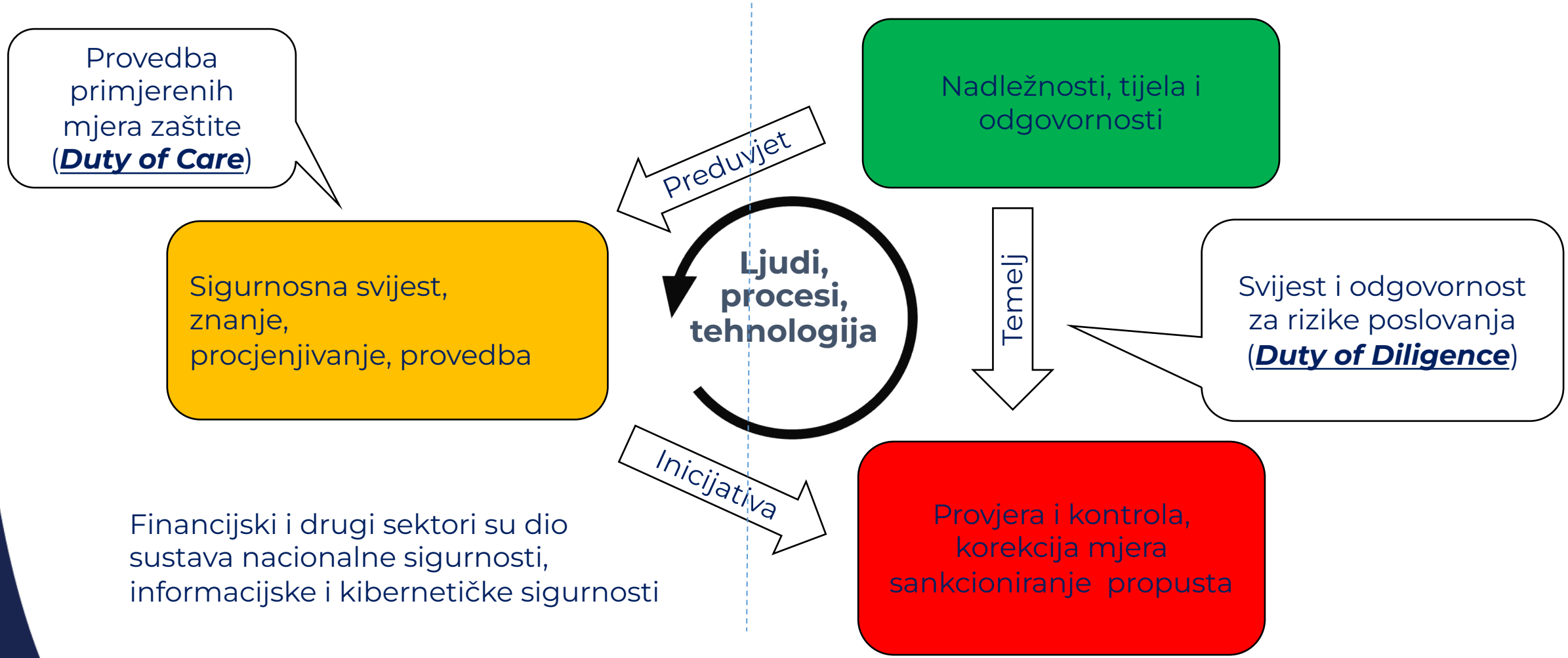
Analize i iskustvo nas uči da se incidenti ne mogu izbjeći

Jedino što nam preostaje je priprema, jer tada upravljamo incidentima

Hanfa je u listopadu 2024. provela vježbu odgovora na kibernetičke incidente s 11 društava te izvijestila tržište

Incidenti će se događati – potrebno je pripremiti se da utjecaj bude manji

KAKO NAM KORISTI REGULATIVA*



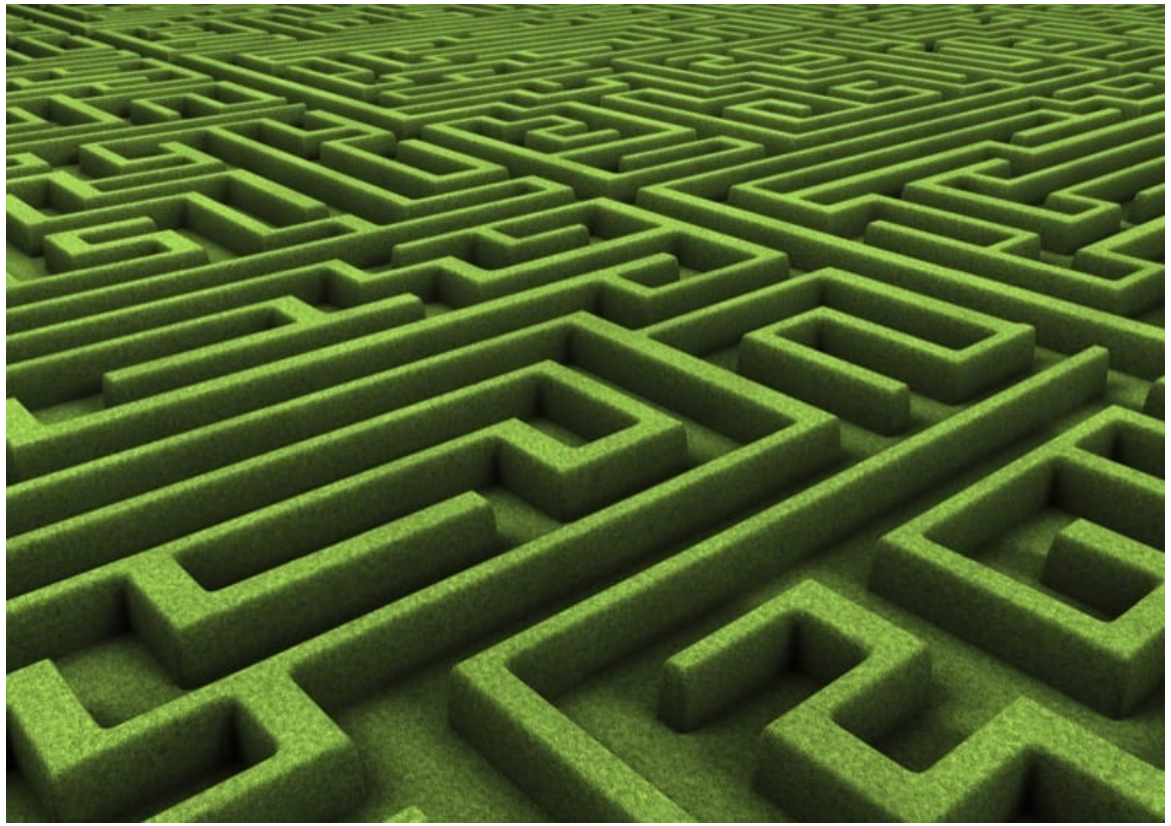
Financijski i drugi sektori su dio sustava nacionalne sigurnosti, informacijske i kibernetičke sigurnosti

* SOA; Sk@ut konferencija 2024.

HANFA
HRVATSKA AGENCIJA ZA NADZOR FINANCIJSKIH USLUGA

KAKO RADITI...

- Koliko prepreka imate?
- Jesu li složene i zahtjevne?
- Običan napadač će uvijek izabrati lakši put
- Šansa je da će umjesto vas napasti nekog drugog



HANFA

HRVATSKA AGENCIJA ZA
NADZOR FINANCIJSKIH USLUGA

HVALA NA POZORNOSTI!