A következő incidenst ma kell megelőzni: NIS2 megfelelés a gyakorlatban

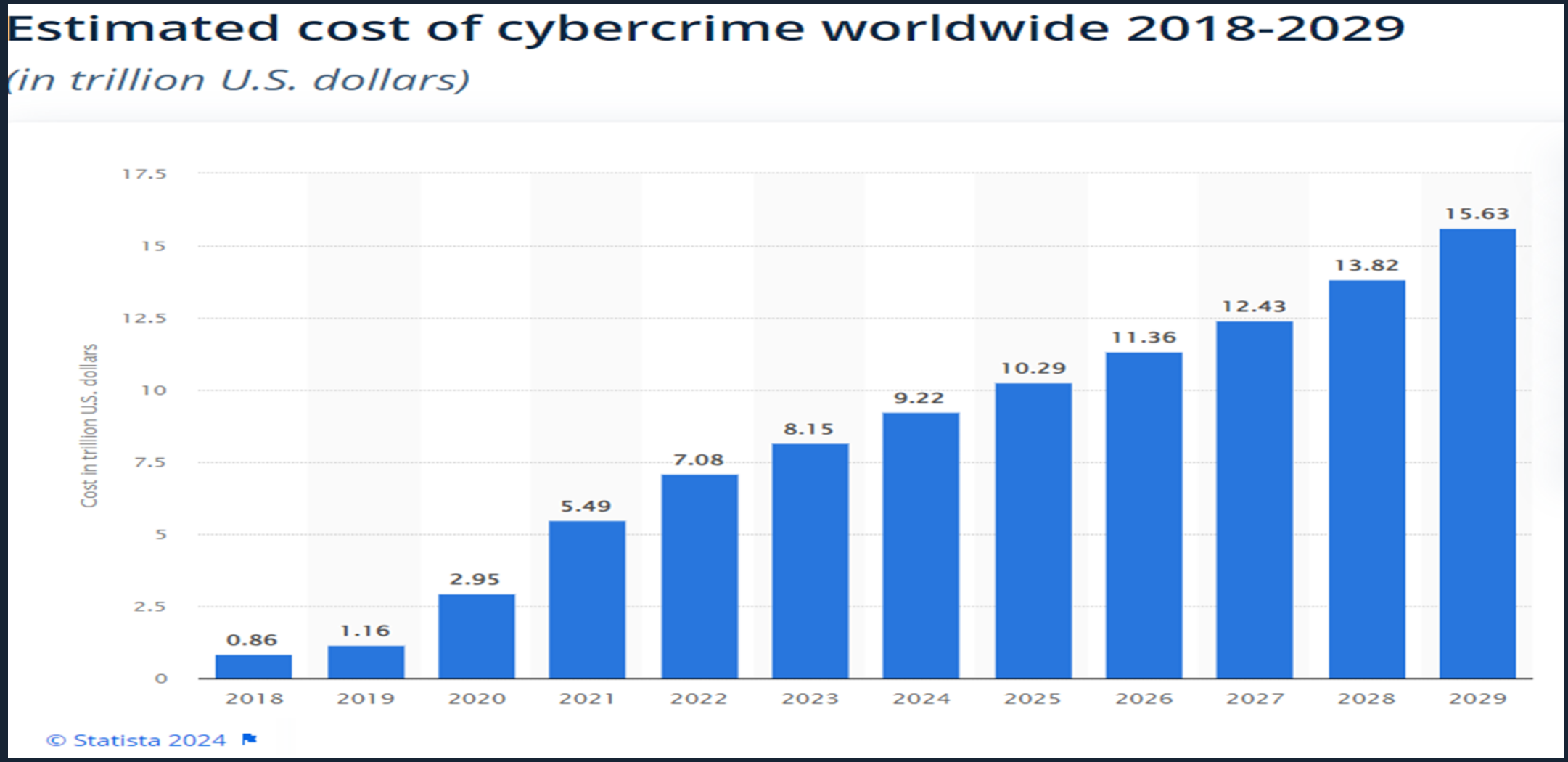
Bor Olivér
Manager | Technology Consulting and Cybersecurity

2025
Ernst & Young Tanácsadó Kft.

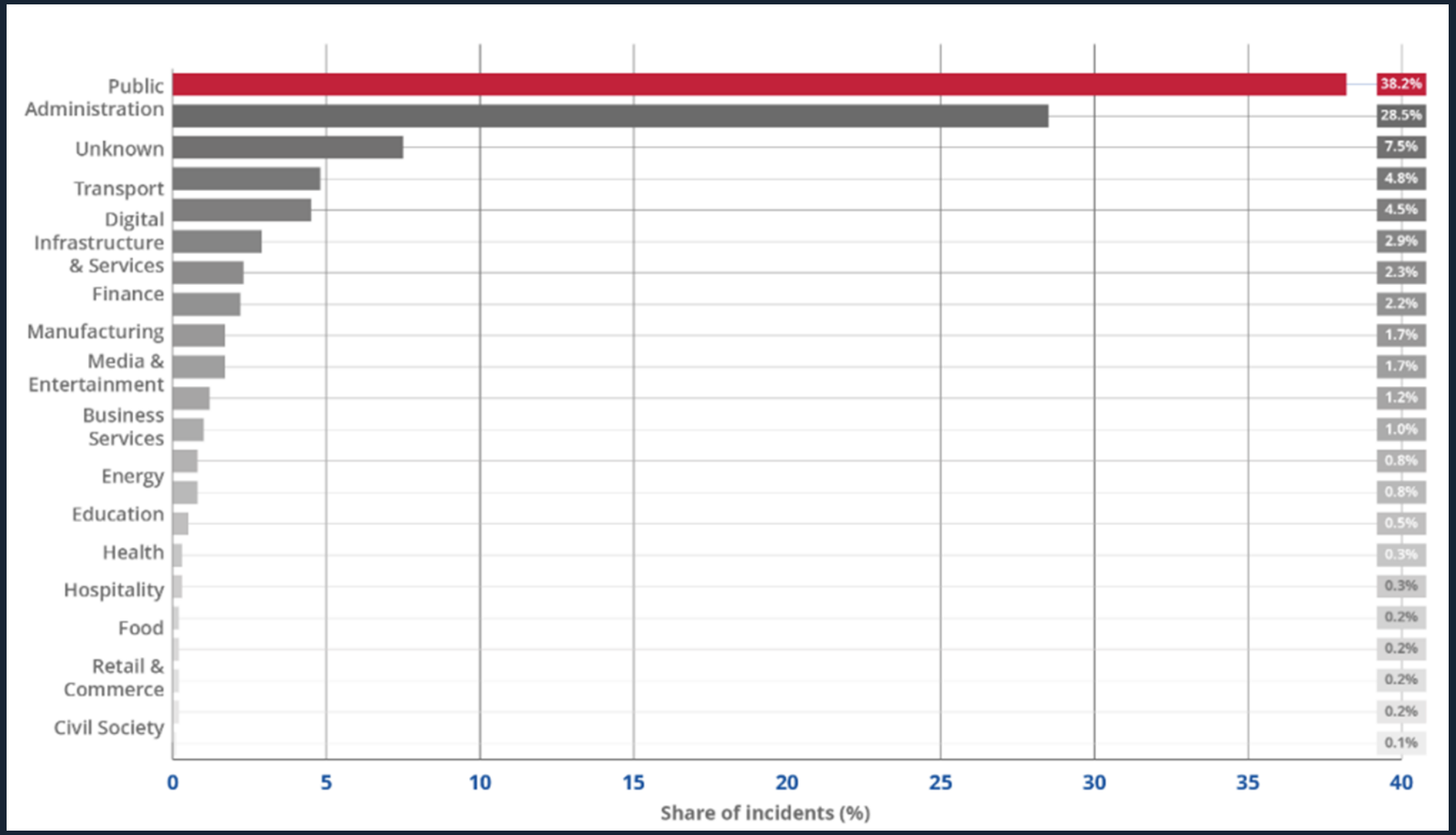
The better the question. The better the answer.
The better the world works.

Building a better working world

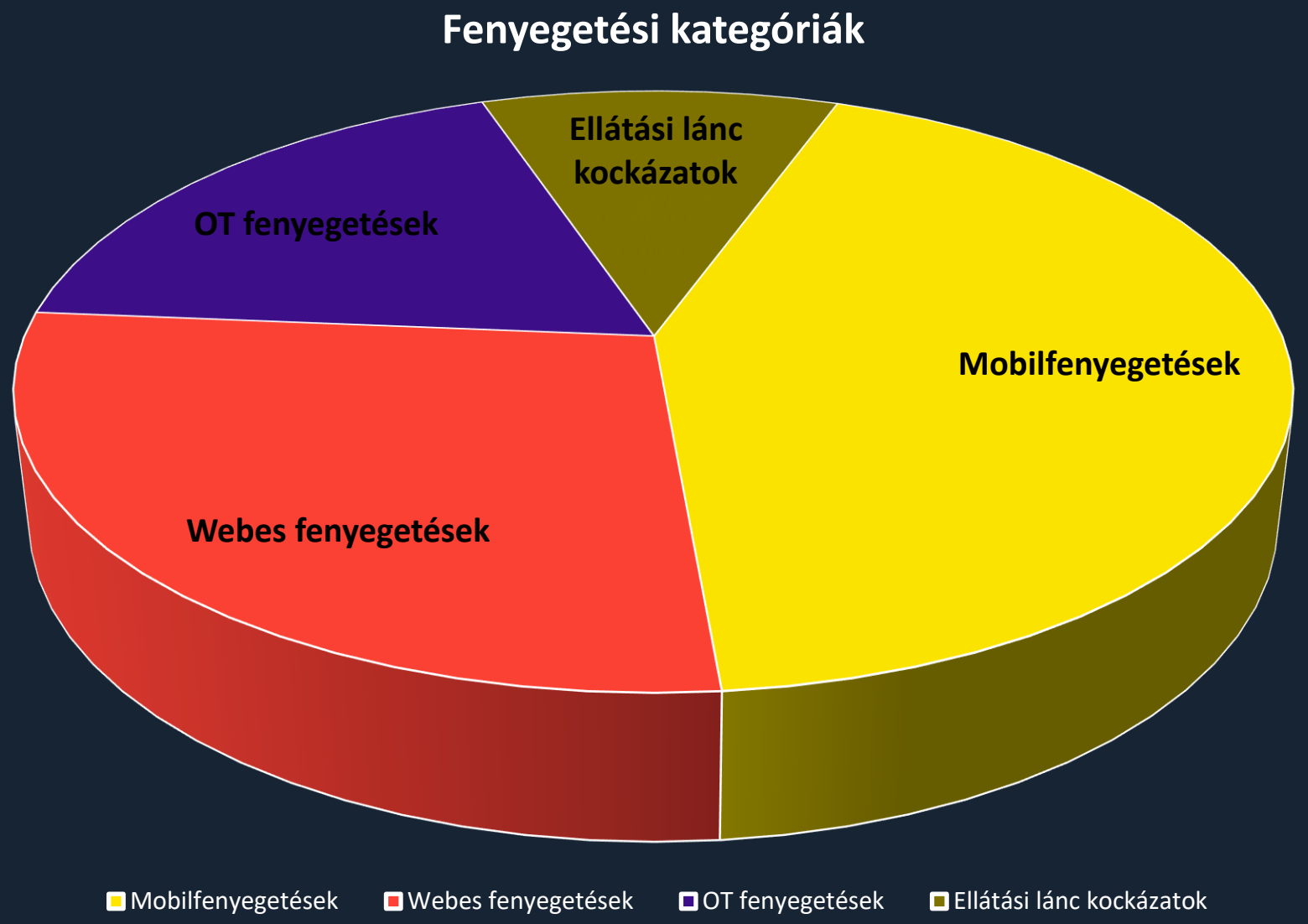
Kiberbiztonsági trendek és statisztikák



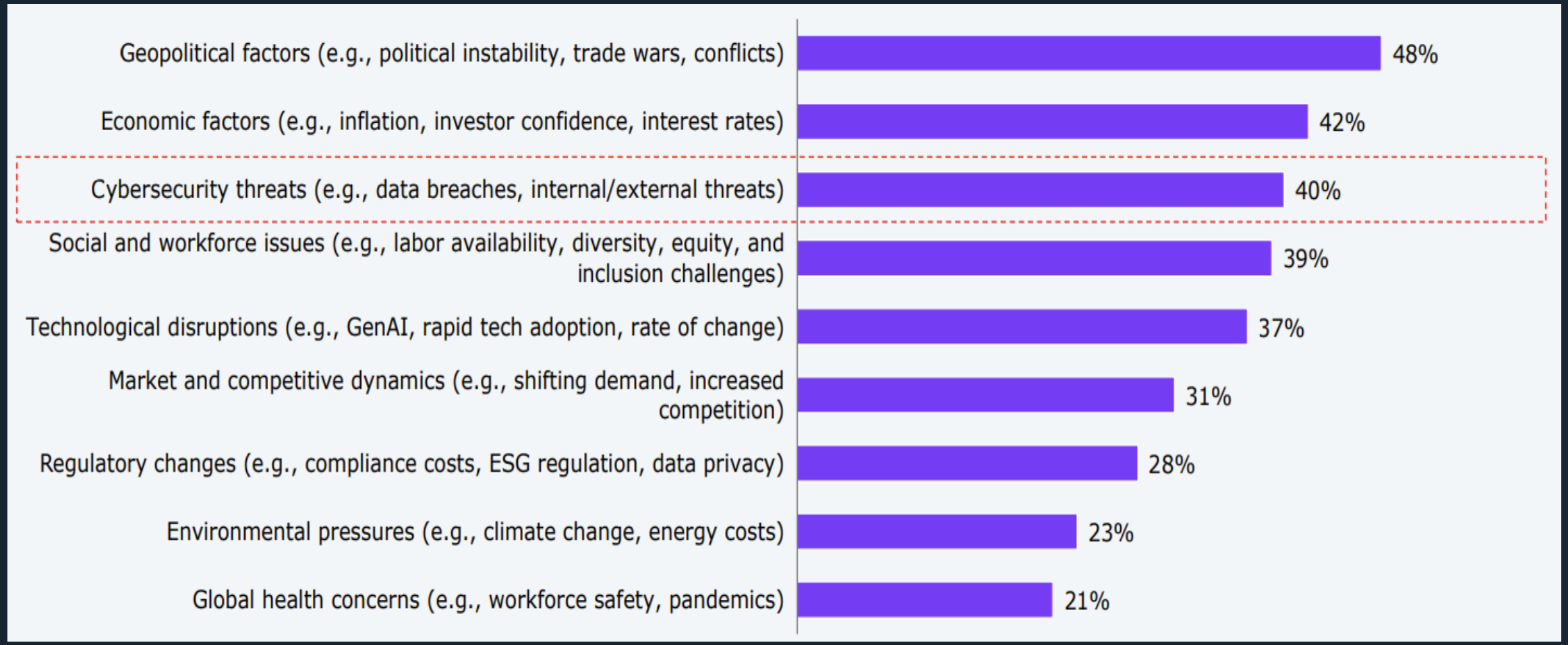
Mitől kell félnünk? (ENISA Threat Landscape 2025)



Mitől kell félnünk? (ENISA Threat Landscape 2025)



Külső tényezők, amelyek veszélyeztetik a szervezet stratégiai prioritásait



Az IBF, CISO, kiberszaki szerepe

A kiberbiztonság szemléletváltása: az értékvédelemtől az értékteremtésig

Szempont	Hagyományos megközelítés	Értékteremtő megközelítés
Megközelítés jellege	Reaktív – a problémákra utólag reagál	Proaktív – megelőző és stratégiai szemléletű
Üzleti hatás	Súrlódás forrása, gyakran akadályozza az üzleti folyamatokat	Új technológiák gyors bevezetésének elősegítője
Fókusz	Technikai fókuszú, IT-központú működés	Az üzleti stratégiához igazított, célorientált működés
Célrendszer	Megfelelés-vezérelt (compliance-driven)	Átalakulásra és innovációra összpontosító
Működési modell	Elkülönült, a többi funkciótól független	Együttműködő és keresztfunkcionális
Látókör	Belső fókuszú, az IT-rendszerek védelmére korlátozódik	Ökoszisztéma-alapú, külső partnereket és beszállítókat is integrál
Szerep	Technikai szakember a funkción belül	Stratégiai értékteremtő az egész szervezetben
Szükséges kompetenciák	IT-biztonsági tudás és megfelelési ismeretek	Mély üzleti és iparági ismeret, stratégiai szemlélet
Finanszírozási prioritás	Védekezésre, incidenskezelésre irányul	Olyan kezdeményezésekre, amelyek üzleti értéket teremtenek (pl. AI, digitális transzformáció, akvizíciók)

Valós veszély és hiányosság lehet…

- Hiányos, elavult kiberbiztonsági / információbiztonsági szabályrendszer: fontos az alvállalkozókra és a szállítmányozó partnerei is kiterjeszteni
- Elavult hálózati infrastruktúra és eszközpark
- IT és OT rendszerek nem megfelelő védelme, szegmentáció hiánya
- Alulpriorizált feladatok és vezetői elkötelezettség hiánya

Mesterséges intelligencia által generált illusztráció

Tapasztalatok a NIS2 felkészülési szakaszában

#miazazEIR

#nincsEIRem

#miazazOT

#azanyavállalatmegmondja

#nemkellfelkészülni

#nincsEIRemnemkellaudit

#beférek5alá

#beszéljmárazSZTFHval

#13bóllett3

#nincserreidőm

Tapasztalatok a NIS2 felkészülési szakaszában

Mesterséges intelligencia által generált illusztráció

Tapasztalatok a NIS2 felkészülési szakaszában

Elkerülési technikák

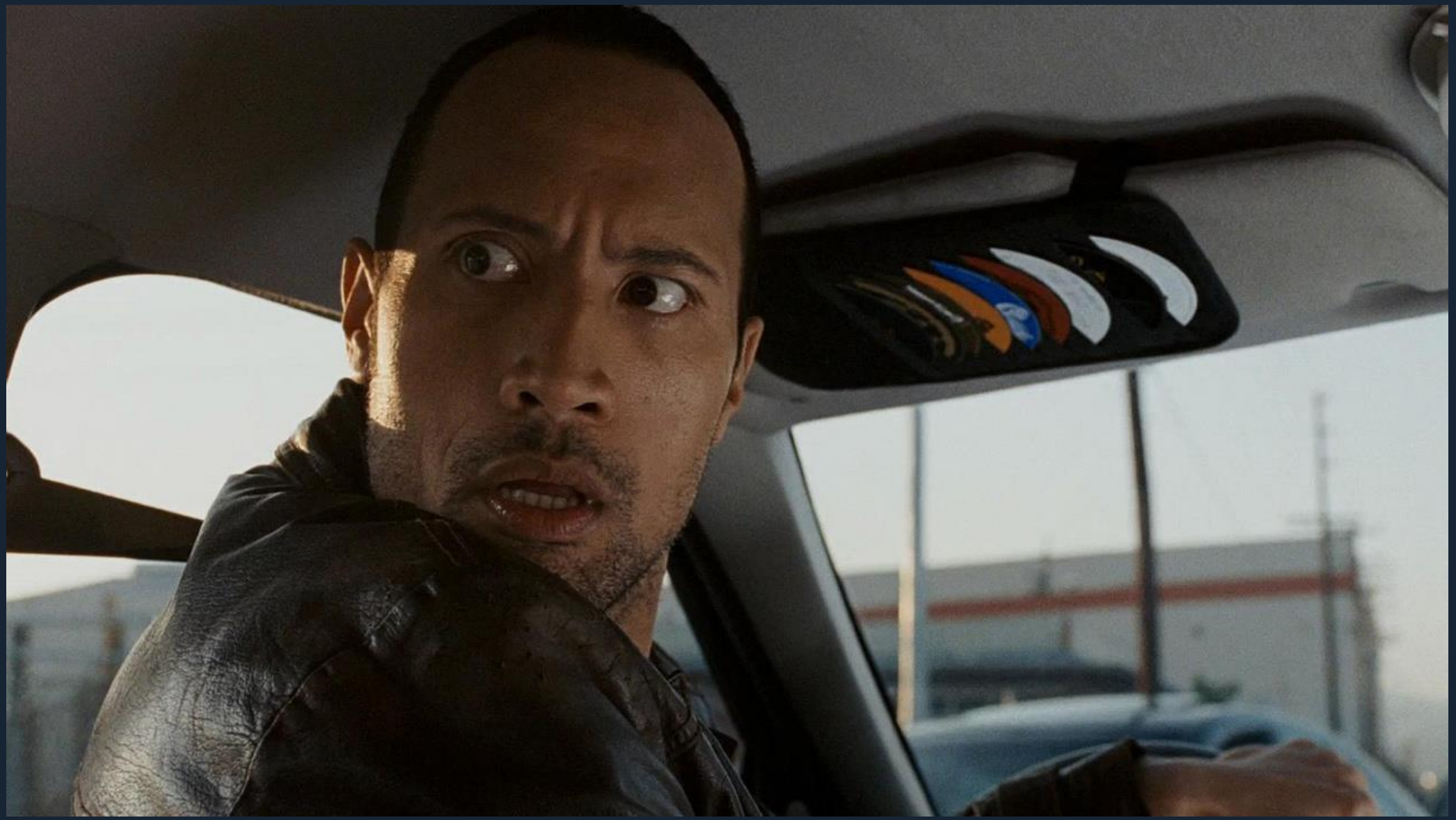
Hatósági szankciók hiánya = bizakodó vállalatok

Feladat komplexitás alábecsülése

Tapasztalat hiánya: idő, költség növekedése

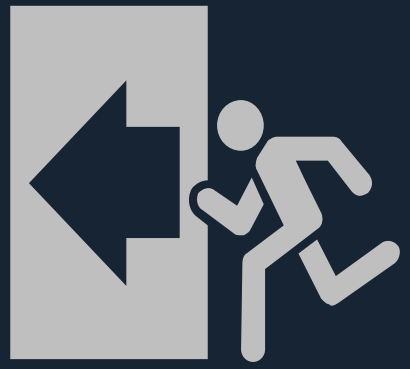
Jogszabály-értelmezési problémák

Tapasztalatok a NIS2 audit szakaszában



El tudja vinni a NIS2-őt 1 ember?

CISO-k megfelelési kényszerben



Köszönöm a figyelmet!

A kibertámadások gyors fejlődése, különösen a mesterséges intelligencia által támogatott támadások, **egyre nagyobb kihívást jelentenek** a szervezetek és a cégek számára.

Ezért **a szervezeti kiberreziliencia fenntartása érdekében**, a jogszabályoknak való megfelelés mellett **kulcsfontosságúvá válik** az ilyen típusú fenyegetések időben történő felismerése és **a hatékony felkészülés**.

Bor Olivér

Manager | Technology Consulting and Cybersecurity

Ernst & Young Tanácsadó Kft.