Kibertámadások az agrár szektor ellen

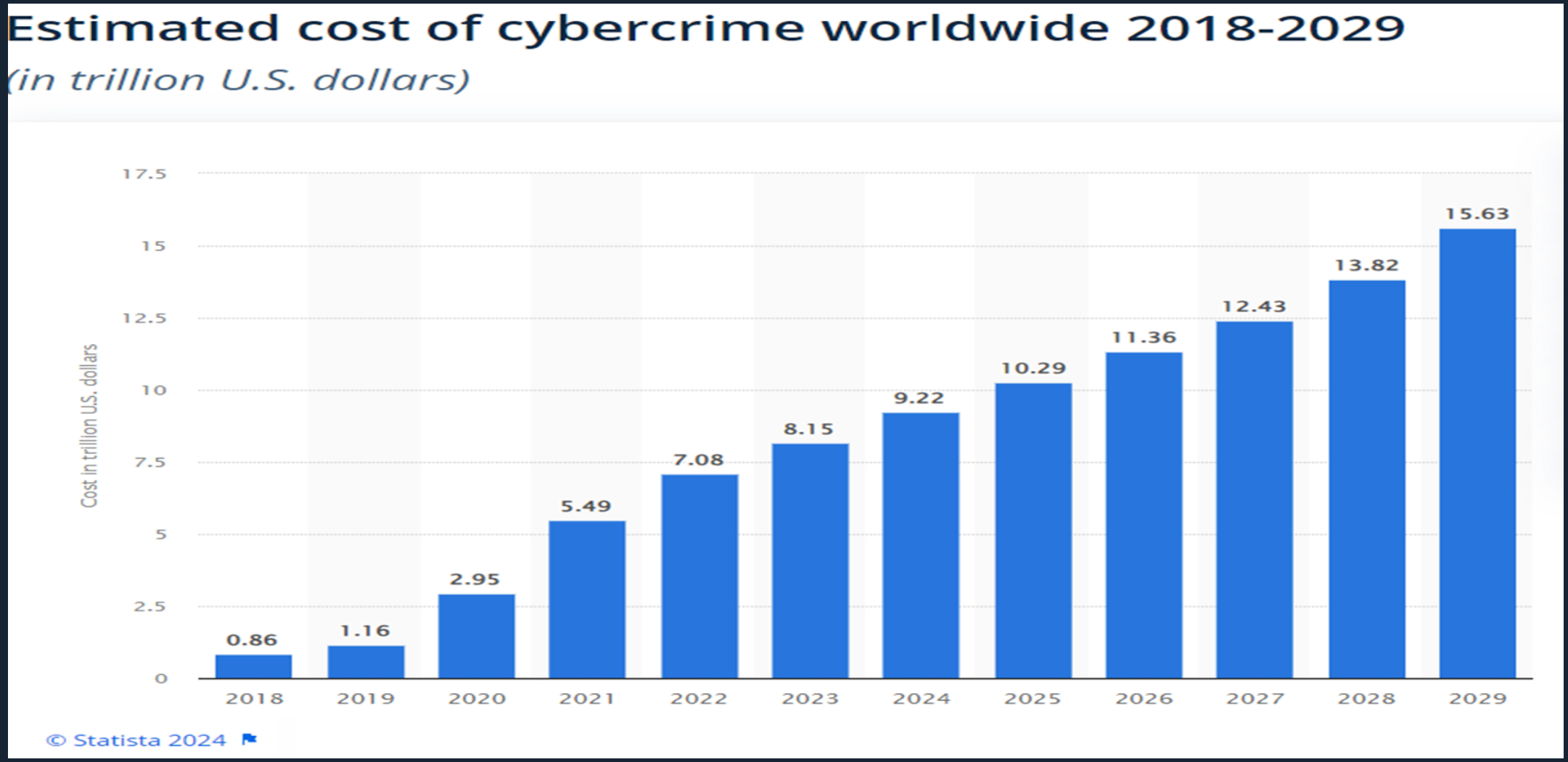
Bor Olivér
Manager | Technology Consulting and Cybersecurity

2025
Ernst & Young Tanácsadó Kft.

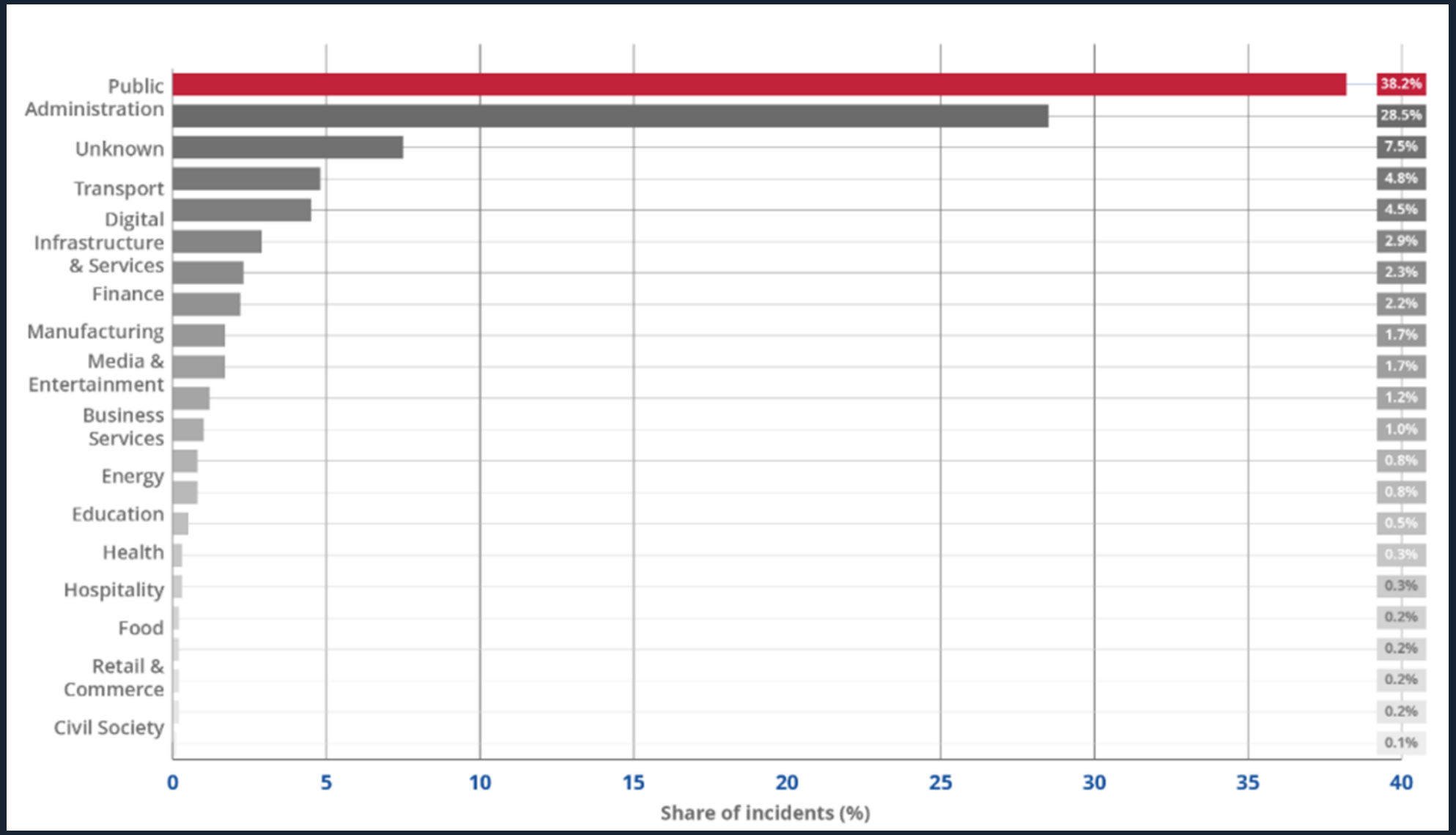
The better the question. The better the answer.
The better the world works.

Building a better working world

Kiberbiztonsági trendek és statisztikák



Mitől kell félnünk? (ENISA Threat Landscape 2025)



Mitől kell félnünk? (ENISA Threat Landscape 2025)

Támadási trendek és módszerek:

- A phishing maradt a leggyakoribb belépési pont (60%)
- A sebezhetőségek kihasználása az esetek 21%-át tette ki
- A mobil és OT rendszerek (pl. ipari vezérlők) kiemelt célpontok
- A mesterséges intelligencia mind az állami, mind a bűnözői szereplők kezében egyre inkább a hatékonyság növelésének eszköze

Mitől kell félnünk? (Everstream Analytics)

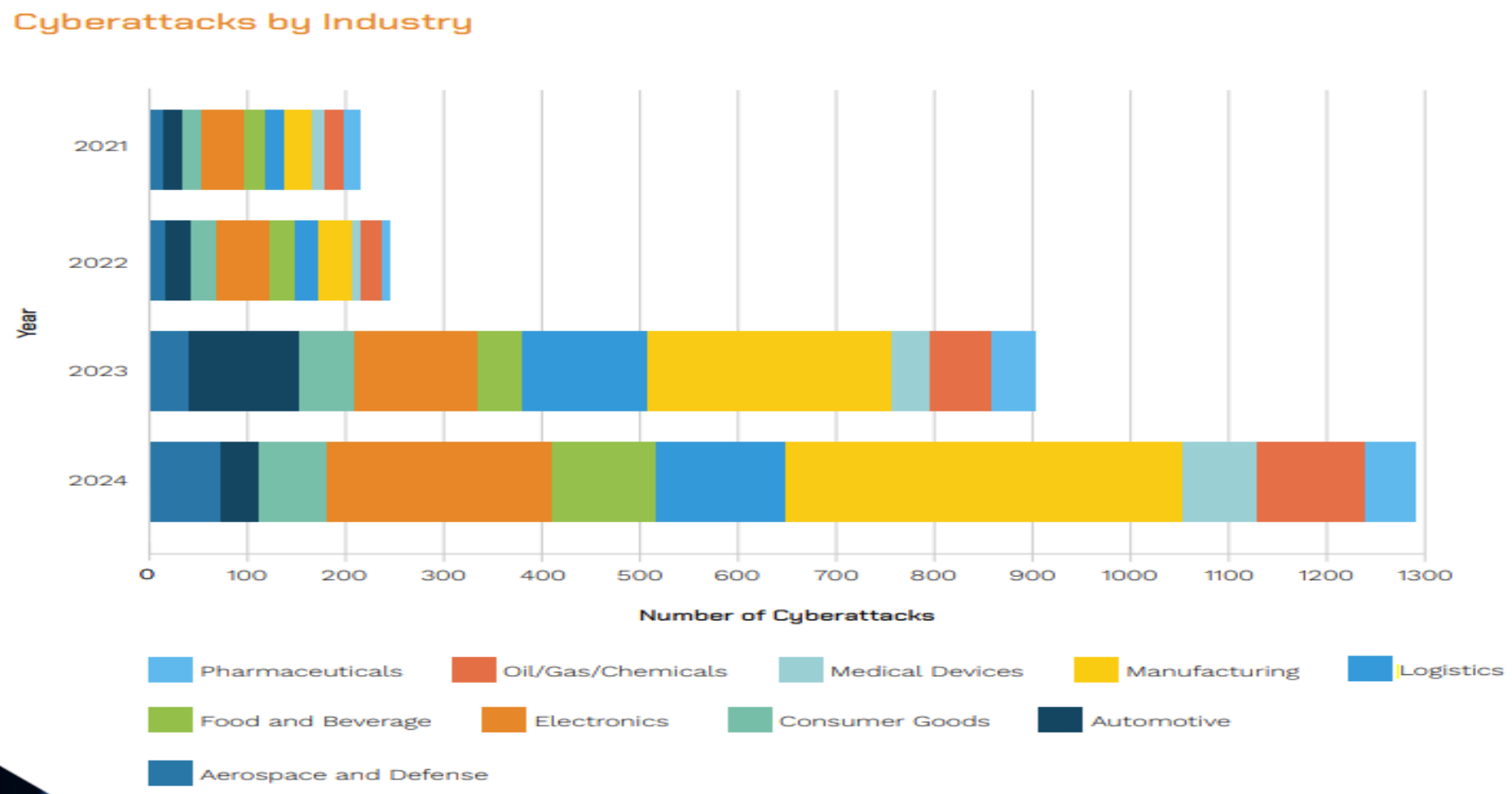
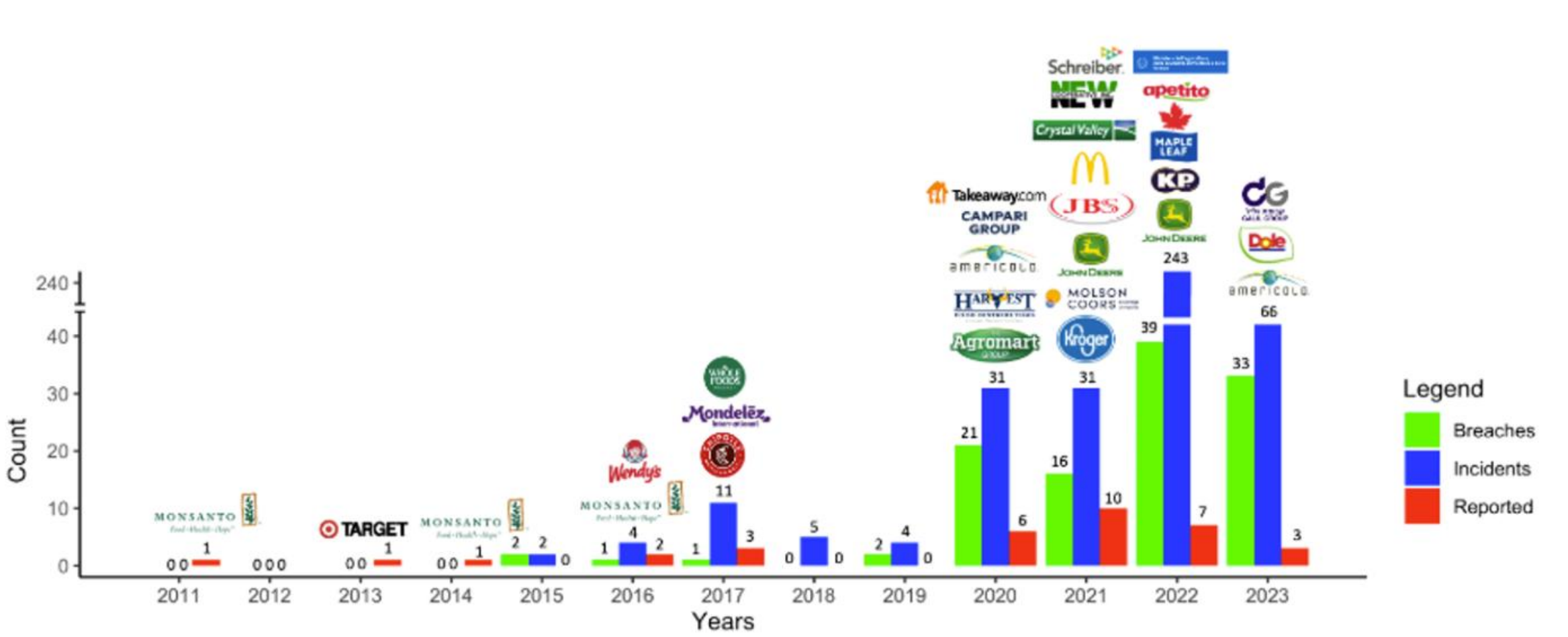


Figure 6: Manufacturing are the most impacted sectors by cyberattacks (source: Everstream Analytics)

Valós veszély és hiányosság lehet…

- A mezőgazdaság egyre inkább adatvezérelt: szenzorok, IoT, GPS-alapú gépek
- A kibertámadások fizikai hatással is járhatnak (termelés megállása, élelmiszer-ellátás)
- A hagyományos rendszerek nem készültek fel a mai fenyegetésekre: összekapcsolt rendszerek és gépek, logisztikai rendszerek
- Az agrárszektor is kritikus infrastruktúra – nem csak IT-probléma!
- A kockázat növekedése: ahogy nő az agrár-ellátási lánc digitalizáltsága, úgy válik egyre vonzóbb célponttá a kiberbűnözők számára – a termelés-leállás, ellátási zavar, adatvesztés komoly következményekkel járhat.

Valós veszély? Valós veszély…



Source: Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., & Batarseh, F. A. (2024). A Review of Cybersecurity Incidents in the Food and Agriculture Sector

Valós veszély? Valós veszély…

Az élelmiszer- és mezőgazdasági ágazatban 2025 első három hónapjában 84 zsarolóprogramos incidens történt: ez több mint kétszerese volt az előző év azonos időszakában regisztrált eseteknek.

Márciusi sűrű hónap volt:
- támadás Dél-Afrika legnagyobb csirkehústermelője ellen: több mint 1 millió dolláros kár
- támadás Dél-Szibéria legnagyobb tejfeldolgozó üzeme ellen: ismeretlen kárösszeg
- támadás Amerika egy legnagyobb élelmiszrkereskedője, elosztója ellen: kár összeg nem ismert, de majdnem egy hétig álltak a rendszerek

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

GPS rendszerek sebezhetősége: számos ilyen jellegű támadás az elmúlt 2 évben

Valós veszély és hiányosság lehet…

Just-in-time logisztika: a modern mezőgazdaság a „just-in-time” (éppen időben) típusú termelésre és szállításra épül, így minimális a hibalehetőség. Egy kibertámadás szoftverleállást vagy szállítási akadályt okozhat, ami azonnali és súlyos zavarokat eredményez.

Rosszul allokált erőforrások: human és pénz…

Incidenskezelési gyakorlat hiánya

Kiberbiztonsági tudatosítása hiánya

Tapasztalatok a NIS2 felkészülési szakaszában

Elkerülési technikák

Hatósági visszamenőleges ellenőrzés

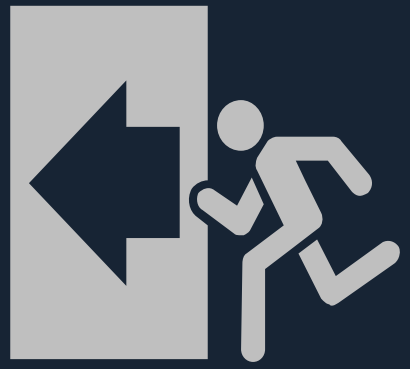
Feladat komplexitás alábecsülése

Tapasztalat hiánya: idő, költség növekedése

Konszolidált beszámoló szabályok ismeretének hiánya

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.