TGS BALTIC
VARUL GRUNTE SUTKIENE

DUOMENŲ APSAUGA IR KIBERNETINIS SAUGUMAS – KODĖL TAI TURĖTŲ RŪPĖTI PIRMIAUSIA VADOVUI?

Mindaugas Civilka

Advokatų kontoros TGS Baltic partneris,
Technologijų industrijos grupės vadovas

ESTONIA // LATVIA / LITHUANIA

1 **_NEBĖRA_ NE IT ĮMONIŲ**

*„Tai - **IT klausimas**“*

2 **KIBER SVEIKATA – _STRATEGINIS_ SPRENDIMAS**

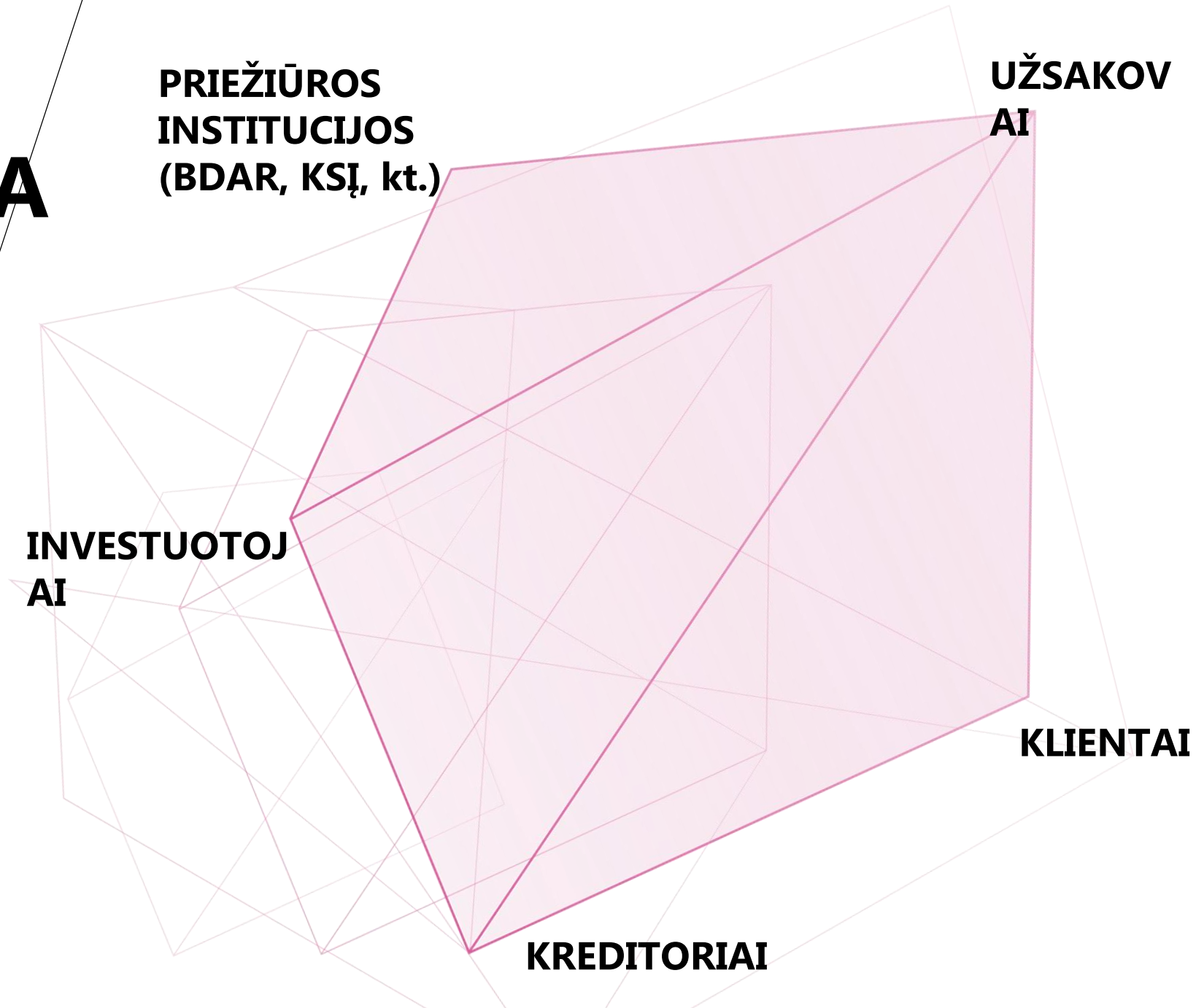
*„Žinome, kad svarbu, bet **tai palauks**, susitvarkysime vėliau“*

3 **KIBER SVEIKATA – NESUSIJUSI SU _ĮMONĖS DYDŽIU_**

*„Mes **neturime vertingų duomenų**, kad mus pultų“*

SSF Integrated Advert By Åkestam Holst: Passwords | Ads of the World™

KAS REIKALAUJA ?



KAS ATSAKINGAS?

VALDYBA

CEO

DPO, CIO, CTO

HOLISTINIS **(IT, ORGANIZACIJA, HR)**
MATYMAS

NEINVESTUOJI DABAR, SUSIMOKĖSI VĖLIAU

Tikimybė, kad spragos IT ūkyje per ateinančius **x metų** sukels **y EUR nuostolius** (baudas, negautas pajamas, reputacinę žalą, kt.), yra lygi **z%**

Siekdama išvengti minėtų nuostolių, per ateinančius x metus į saugumą privalo investuoti ne mažiau nei **y [***įvertinus pinigų laiko vertę***] z EUR**

IMUNITETO STOKOS PASEKMĖS

1 Žala įmonei ženkli – turtinė / ***neturtinė***

2 **Vadovų** civilinė atsakomybė

3 Institucijos, tyrimai, baudos

4 Grupiniai ieškiniai

5 Sutarčių nutraukimas, užtikrinimo reikalavimas, kt.

6 Kitos ***netiesioginės pasekmės***

KAIP VALDYTI KIBER-RIZIKAS

Prevencija, nustatymas, atsakas

Mokymas / švietimas

***Savęs* auditai (Self assessment)**:

Pardavėjų / teikėjų auditai (Vendor's DD):

- *Maturity assessments /* IT security auditas
- Funkcinis, organizacinis auditas
- BDAR auditas

Sutartys

- Paslaugų teikėjai (konsultacijos, developinimas, diegimas)
- Hardware, infrastruktūros pardavėjai, palaikymas
- SaaS/IaaS

Draudimas

ESTONIA / LATVIA / LITHUANIA

IT SAUGUMAS VS. IT RIZIKŲ DRAUDIMAS

Draudimas galios **tik tiek ir tik jeigu** būsite atsakingai susitvarkę savo IT ūkį (rizikos vertinimai, patikrinimai, dokumentacija, procesai) ir atitiksite BDAR bei kitus reikalavimus

Draudimas **nepakeičia** IT ūkio saugumo ir nesuteikia **papildomo IT saugumo**

Draudimas, **jeigu galioja**, padeda suvaldyti kaštus atsitikus įvykiui

5 KLAUSIMAI IT VADOVUI

Kaip samdome IT žmones?

Kaip išorės žmonėms suteikiame prieigą prie IS?

Ar daromos esminių duomenų atsarginės kopijos?
Ar bandėme jas atstatyti?

Ar taikome MFA?

Ar šifruojami duomenys? Kurie?

Duomenų migracija?

Duomenų bazių **migracija** – 1 Iš **25** faktorių - saugumo sistemos kompleksiškumas ir *cloud migration*
IBM Security. Cost of a Data Breach Report, 2020

3 KLAUSIMAI TEISĖS SKYRIUI

Sutartys su vendoriais / paslaugų teikėjais: Kaip juos tikriname? Ar galėsime į juos nukreipti išieškojimą?

Ar randate bendrą kalbą su IT žmonėmis? Ar jie susikalba su kitais / kolektyvu?

Kibernetinių rizikų draudimas: Ar yra? Ką apima – ar kompensuojamos institucijų skiriamos baudos?

ATSITIKUS: KOMUNIKACIJA

Vaidmuo ir atsakomybė įvykus kibernetiniam incidentui. **KAS ATSAKINGAS?**

Tai - nebe IT klausimas, o komunikacijos/krizės valdymas, todėl **jo negalima patikėti vien IT vadovams – [T.I.K.]**

Incidentas nėra PATS blogiausias dalykas – blogiausia tai, kas įvyksta po to.

Informacinė krizė / kartais – informacinis karas:

- Komunikacija su klientais, visuomene
- Komunikacija su valstybės institucijomis
- Komunikacija su spauda / medija
- Komunikacija su kolektyvu

Kaip **plinta informacija**, kaip ją pasigauna socialinės / tradicinės medijos, kt.

SUSISIEKIM
E

MINDAUGAS CIVILKA
Partneris, advokatas

E mindaugas.civilka@tgsbaltic.com
T +370 5 251 4444
M +370 687 32 714