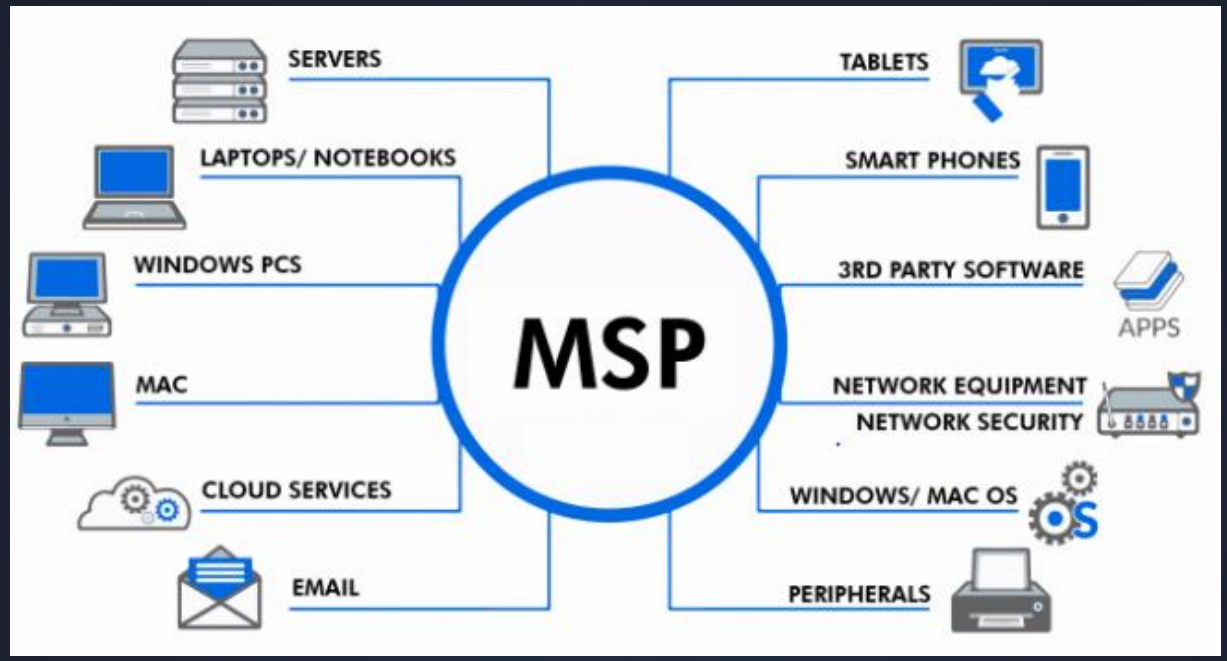
MANAGEMENTUL RISCURILOR CIBERNETICE IN RELATIA FURNIZOR - CLIENT

Otto Broker
CORPORATE INSURANCE

INTERDEPENDENTA TEHNOLOGICA NE AJUTA SA NE DEZVOLTAM DAR NE SI EXPUNE LA RISCURI DIN PARTEA FURNIZORILOR NOSTRI



- Vedem o crestere accelerata a cerintelor de asigurare din partea companiilor pentru externalizarea riscurilor cibernetice catre furnizorii lor de servicii
- Cele mai uzuale solicitari sunt pentru raspundere profesionala si raspundere cibernetica, inclusiv pentru daune de consecinta sau pierderi din intreruperea activitatii

CONCLUZIILE STUDIULUI

- **Atacurile de tip “supply chain”** au crescut accelerat in ultimii 2 ani
- **Un bun nivel de securitate cibernetica proprie nu mai este suficient pentru organizatii** atunci cand atacatorii si-au concentrat atentia pe furnizorii acesteia.
- Uzual, **un astfel de atac concertat poata dura luni pana sa se declanseze** si este fragmentat pe mai multi furnizori pana se ajunge la cel final asupra clientului
- In **66% din incidentele raportate, atacatorii s-au concentrat pe softuri/coduri proprii ale furnizorilor** – devine critic ca organizatiile sa se concentreze pe **validarea solutiilor externe inainte de implementare**
- In **58% din incidentele analizate, atacatorii au vizat datele clientilor, inclusiv date cu caracter personal, date legate de plati si proprietate intelectual**.
- In 66% din incidentele analizate, **furnizorii nu au stiut sau nu au notificat clientii** despre faptul ca sistemele lor au fost compromise
- Doar **9% din clientii atacati in astfel de incidente nu au stiut cum s-a petrecut atacul**, ceea ce spune multe despre diferente de know-how si maturitate intre furnizori si clientii finali

RECOMANDARI

PENTRU CLIENTI

- Identifica si documenteaza toti furnizorii de servicii;
- Verifica prevederile contractuale si obligatiilor furnizorilor in ceea ce priveste securitatea si asigurarile cibernetice
- Defineste criterii de risc adecvate pentru fiecare tip de furnizor, dependente critice, puncte potentiale de breach
- Monitorizeaza riscurile pe lantul de aprovizionare si urmareste amenintarile specifice industriei
- Defineste, implementeaza si urmareste respectarea procedurilor de catre furnizorii tai cu privire la date cu caracter personal
- INCHEIE O ASIGURARE DE RISC CIBERNETIC

PENTRU FURNIZORI

- Foloseste infrastructura adecvata dpdv al practicilor de securitate cibernetica
- Monitorizeaza vulnerabilitatile de securitate ce ar putea afecta serviciile livrate clientilor tai
- Inventariaza constant produsele si serviciile vandute clientilor si asigura-te ca beneficiaza de cele mai recente actualizari/patch-uri
- Limiteaza numarul angajatilor cu acces la infrastructura clientilor si/sau date sensibile
- Back-up / test restore
- INCHEIE O ASIGURARE DE RASPUNDERE PROFESIONALA SI RISC CIBERNETIC

ASIGURAREA CIBERNETICA SAU "CAND MASURILE DE PREVENTIE NU AU FUNCTIONAT"

Otto Broker
CORPORATE INSURANCE

STRATEGIC, SCADEREA PONDERII ACTIVELOR TANGIBILE IN BILANTUL COMPANIILOR AR TREBUI SA DUCA LA O REANALIZARE A RISCURILOR CU IMPACT SEVER IN ACTIVITATE

Un incendiu in spatiul inchiriat in care ne desfasuram activitatea ar trebui sa nu mai fie “cel mai rau lucru care ni se poate intampla” (daca nu lucrezi in productie)

Un atac cibernetic asupra sistemului core al companiei, pe care il blocheaza sau in care date esentiale sunt furate/criptate ar putea fi mai costisitor de rezolvat

ASIGURAT IN MOD TRADITIONAL

NEASIGURAT INTR-O PROPORTIE URIASA

SUPRAFATA DE ATAC SE INDREAPTA SPRE 100%, ATAT PENTRU INDIVIZI, CAT SI PENTRU COMPANII

Aproape totul se interconecteaza: autoritati de stat, servicii financiare, IT, servicii medicale, transporturi si distributie, e-commerce

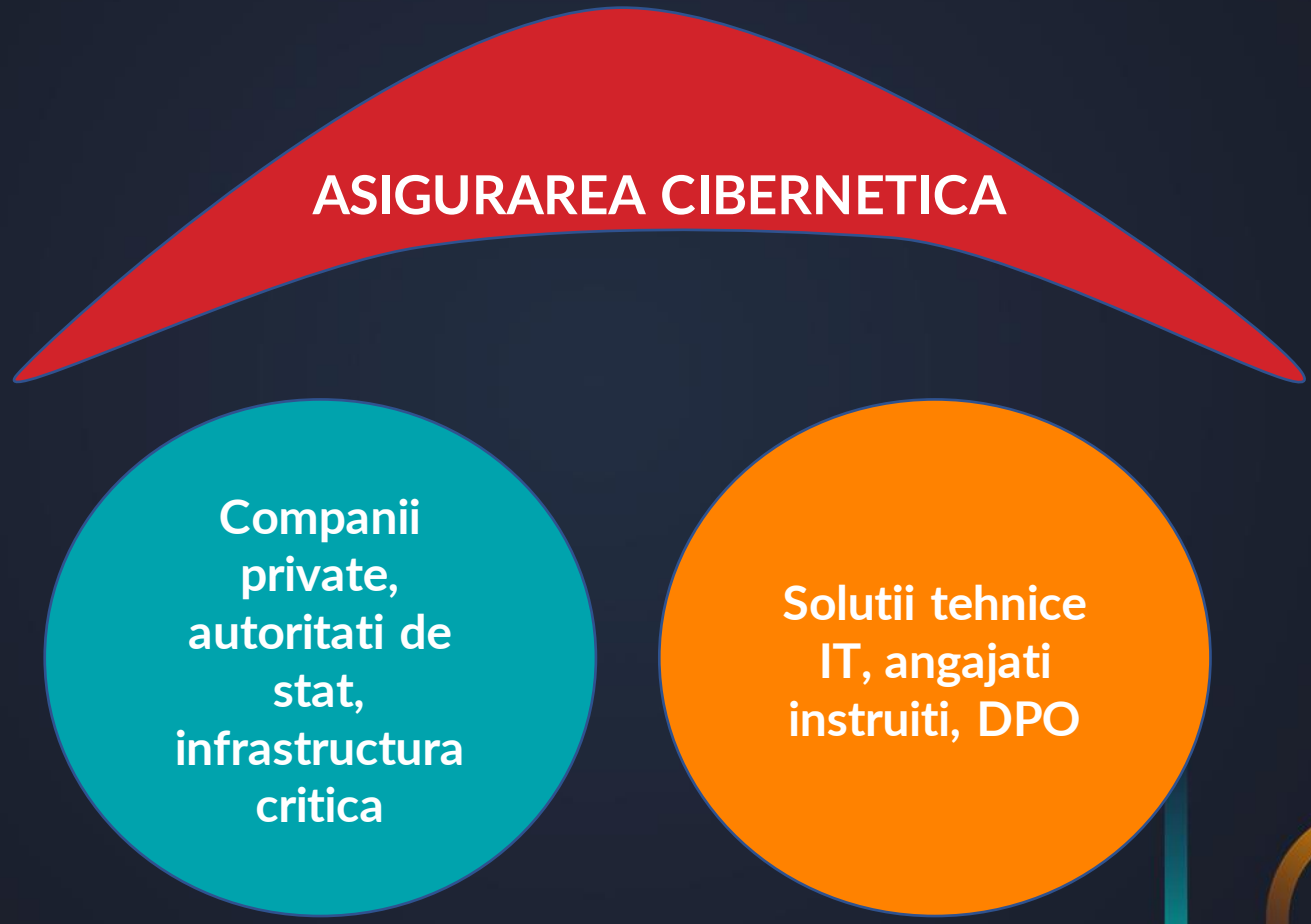
Suntem in permanenta conectati la o forma de internet, acasa si la munca

Platim din ce in ce mai des online, un trend accelerat de pandemie

Angajatii nostri primesc si citesc zilnic zeci sau sute de mesaje, mailuri, pagini web potential periculoase

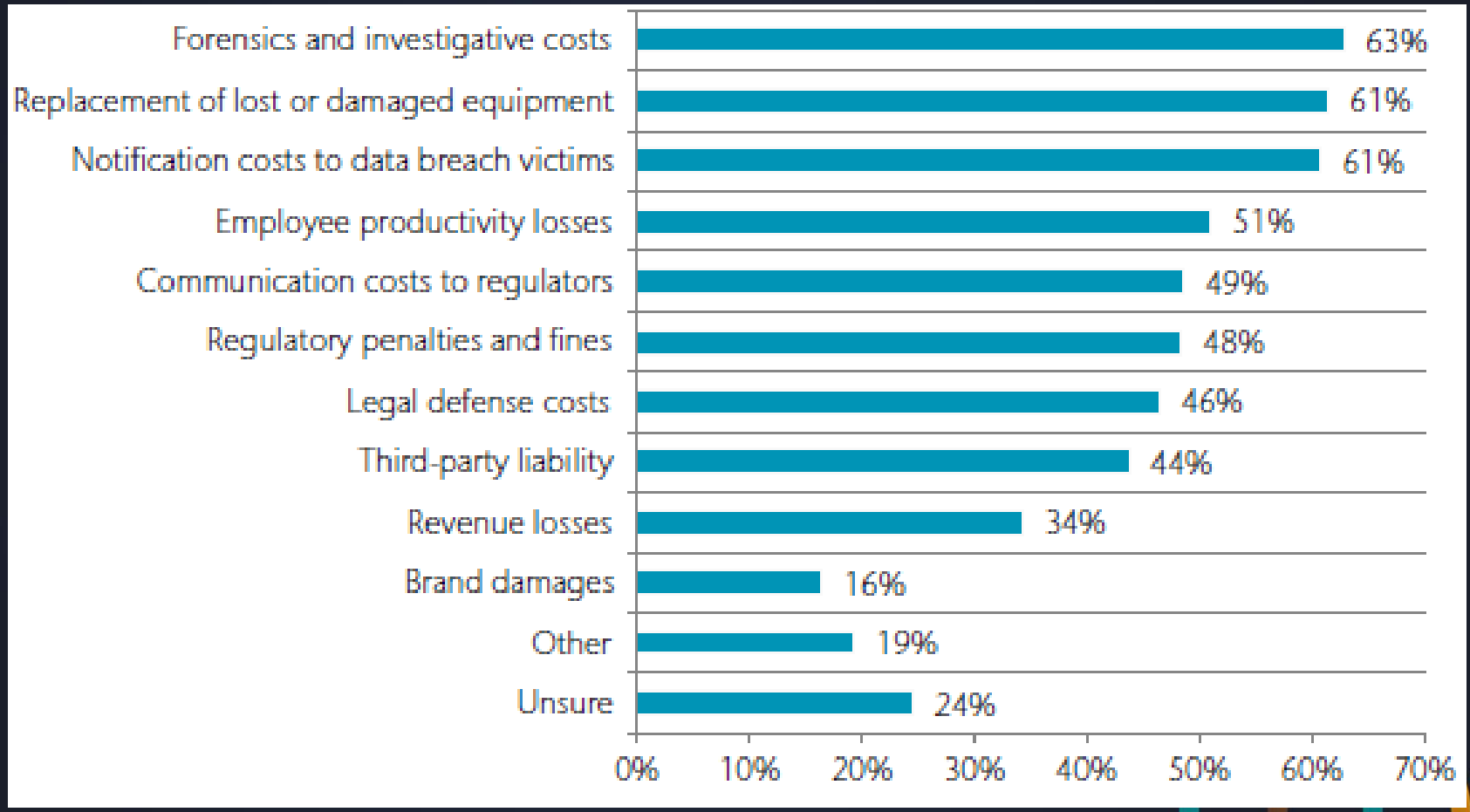
Angajatii nostri transmit si primesc date personale proprii, ale clientilor, furnizorilor, partenerilor etc

O ORGANIZATIE REZILIENTA ESTE UNA PREGATITA SA PREVINA, SA-SI URMAREASCA RISCURILE, SA-SI IMBUNATATEASCA SECURITATEA DAR SI SA SE RECUPEREZE RAPID IN URMA UNUI ATAC REUSIT



CE SE POATE ASIGURA IN MOD UZUAL PE O POLITA BUNA DE ASIGURARE CIBERNETICA

IN EXTENSO, ACEASTA INSEAMNA O SERIE DE COSTURI CU EXPERTI EXTERNI SPECIALIZATI SA TRATEZE ASTFEL DE SITUATII SI CARE SUNT DIRECT INTERESATI SA TE AJUTE SA TE REDRESEZI



SUMAR PUNCTE ESENTIALE

- [x] Asigurarea cibernetica este complementara masurilor de securitate pe care orice companie (si individ intr-o anumita masura) trebuie sa le aiba in vedere
- [x] Asigurarea acopera financiar nevoia de suport specializat in cazul unei daune: specialisti IT, avocati specializati GDPR, companii de PR de criza
- [x] Acopera prejudiciile proprii in urma unui atac dar si potentiale raspunderi fata de terti in cazul in care atacul se raspandeste dinspre sistemele proprii, inclusiv amenzi GDPR
- [x] O polita buna poate avea acoperire inclusiv pentru terorism cibernetic sau atacuri "nation-backed"
- [x] Daca tu nu poti sa te asiguri, cere-le furnizorilor tai sa o faca

MULTUMESC!

Otto Broker
CORPORATE INSURANCE