Crowe

Smart decisions. Lasting value.

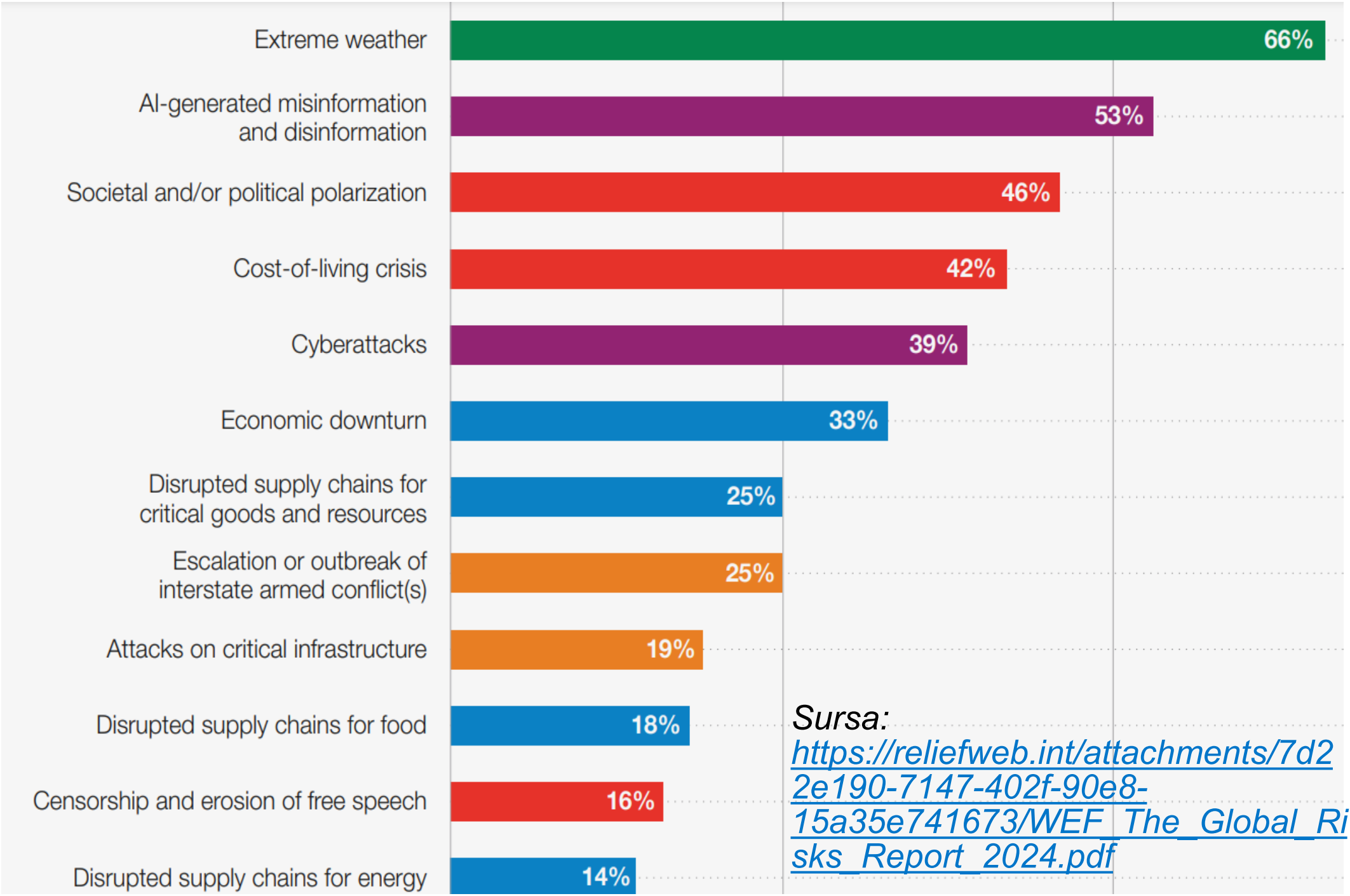
Securitatea cibernetică,

recomandări practice

WORLD ECONOMIC FORUM

Sursa:

Global Risk Report 2024



Sursa:
https://reliefweb.int/attachments/7d22e190-7147-402f-90e8-15a35e741673/WEF_The_Global_Risks_Report_2024.pdf

Securitate cibernetică?

- practica de a proteja
- nu este o problema IT
- set de procese,
- set de bune practici
- set de soluții tehnologice
- sport de echipă

Rolul securității cibernetice în raportarea financiară

- Integritatea datelor, conformitatea și încrederea utilizatorilor informației financiare
- Securitatea cibernetică a devenit un pilon esențial al raportării financiare moderne, având un impact direct asupra calității, acurateței și credibilității situațiilor financiare într-un mediu tot mai digitalizat.

Contextul actual al raportării financiare digitale

- Raportarea financiară se bazează tot mai mult pe sisteme informatice complexe pentru colectarea, procesarea și prezentarea informațiilor financiare.
- Entitățile utilizează:
  - sisteme ERP,
  - platforme de contabilitate în cloud, aplicații automatizate de raportare financiară.

  Această dependență crescută de tehnologie sporește expunerea la riscuri cibernetice care pot afecta direct integritatea și fiabilitatea informațiilor financiare.

Principalele riscuri cibernetice asupra raportării financiare

Riscurile cibernetice cu impact direct asupra raportării financiare includ:

- atacuri cibernetice și breșe de date;
- ransomware și blocarea sistemelor contabile;
- acces neautorizat la baze de date financiare;
- manipularea sau ștergerea înregistrărilor contabile;
- amenințări interne (angajați, furnizori, subcontractori).

Aceste riscuri pot genera erori semnificative și denaturări financiare materiale.

1. Ransomware

2. Phishing attacks

3. Data Leakage

4. Hacking

Impactul asupra situațiilor financiare și guvernanței

Consecințele unui incident de securitate cibernetică pot include:

- denaturarea poziției financiare și a performanței;
- pierderi financiare directe;
- sancțiuni și amenzi de reglementare;
- afectarea reputației și pierderea încrederii investitorilor;
- creșterea riscului de fraudă financiară.

Studiile arată o creștere semnificativă a cazurilor de denaturări financiare asociate incidentelor cibernetice.

Rolul tehnologiilor emergente

Pentru protejarea raportării financiare, organizațiile adoptă tehnologii avansate, precum:

- Blockchain – pentru înregistrări financiare imuabile;
- Inteligență artificială (AI) – pentru detectarea anomaliilor și a tranzacțiilor suspecte;
- Criptare avansată – pentru protejarea bazelor de date financiare;
- Monitorizare în timp real – pentru identificarea accesului neautorizat.

Aceste tehnologii cresc nivelul de siguranță, dar necesită guvernanță adecvată.

Rolul auditorilor în context cibernetic

Auditorii au un rol tot mai important în:

- evaluarea riscurilor IT și de securitate cibernetică
- înțelegerea controalelor generale IT (ITGC);
- evaluarea impactului riscurilor cibernetice asupra denaturărilor financiare;
- utilizarea analizei de date și a instrumentelor digitale.

Standardele PCAOB și IAASB încurajează integrarea riscurilor cibernetice în auditul financiar.

Politici și proceduri utile

Politica de utilizare a sistemelor

Aceasta stabilește regulile de utilizare a sistemelor IT, incluzând:

- utilizarea obligatorie a parolelor și schimbarea periodică a acestora;
- interzicerea copierii și scoaterii datelor din sediu fără aprobare;
- criptarea dispozitivelor de stocare;
- securitatea fizică a echipamentelor;
- reguli privind utilizarea în scop personal;
- autentificarea multifactor.

Politici și proceduri utile

Politica de utilizare a e-mailului

Aceasta poate include:

- interzicerea utilizării e-mailurilor personale pentru activități profesionale;
- interzicerea deschiderii atașamentelor din surse necunoscute;
- interzicerea accesului la conturile altor persoane;
- monitorizarea e-mailului de către organizație.

Politici și proceduri utile

Politica de utilizare a internetului

Aceasta poate include:

- limitarea utilizării la scopuri profesionale;
- monitorizarea traficului;
- interzicerea accesului la site-uri ofensatoare;
- descărcarea doar din surse sigure;
- interzicerea fișierelor executabile și a conținutului piratat;
- sancțiuni pentru nerespectare.

Politici și proceduri utile

Politica de acces de la distanță

Aceasta poate include:

- aprobări pentru acces extern;
- măsuri de securitate (firewall, software de protecție, MFA);
- securitatea echipamentelor;
- raportarea incidentelor;
- monitorizarea activităților utilizatorilor;
- consecințe pentru neconformitate.


Crowe
Smart decisions.
Lasting value.