კიბერ რისკების დაზღვევა

კიბერ რისკი არ არის მხოლოდ ინფორმაციული ტექნოლოგიების (IT) შიდა დეპარტამენტის გამოწვევა — ეს არის კომპლექსური საოპერაციო, ფინანსური და სტრატეგიული რისკი. კიბერ რისკები მოიცავს ნებისმიერ საფრთხეს, რომელმაც შესაძლოა დააზიანოს ორგანიზაციის ციფრული აქტივები, ჩაშალოს ბიზნესპროცესები, გამოიწვიოს ფინანსური დანაკარგი ან შელახოს კომპანიის რეპუტაცია.

<u>ვის ფარავს სადაზღვევო პოლისი:</u>

კიბერ დაზღვევის პოლისი როგორც წესი, ორ ძირითად ბლოკად იყოფა:

- **პირველი მხარის ზარალი (კომპანიის პირდაპირი დანაკარგი);**
- **მესამე მხარის პასუხისმგებლობა (კლიენტებისთვის მიღებული ზიანის ანაზღაურება).**

დაფარვები:

1. **პირველი მხარის ზარალი (First-Party Losses)**

   ეს არის ხარჯები, რომლებსაც კომპანია საკუთარი თავის გადასარჩენად და სისტემების აღსადგენად ეწევა:

   ბიზნესის შეწყვეტის ზარალი (Business Interruption): შეწყვეტილი საოპერაციო საქმიანობის შედეგად დაკარგული მოგება და ფიქსირებული საოპერაციო ხარჯები.

   მონაცემთა და სისტემების აღდგენა (Data & System Restoration): განადგურებული, დაზიანებული ან დაშიფრული მონაცემებისა და პროგრამული უზრუნველყოფის აღდგენის / ხელახლა შექმნის ხარჯები.

   კიბერ გამოძალვა (Cyber Extortion / Ransomware): გამოძალვასთან დაკავშირებული ინციდენტების მართვა, ექსპერტების ჩართულობა და კრიზისული გადაწყვეტილებების დაფინანსება.

   ინციდენტზე რეაგირების ხარჯები, კერძოდ:

   - **IT ექსპერტიზა:** შეტევის წყაროს, მასშტაბისა და მეთოდის დადგენა.
   - **იურიდიული კონსულტაცია (Breach Counsel):** მარეგულირებელთან და საკანონმდებლო მოთხოვნებთან შესაბამისობის უზრუნველყოფა.
   - **კრიზისული კომუნიკაციები და PR:** რეპუტაციული ზიანის შემცირება.

შეტყობინების ხარჯები: დაზარალებული კლიენტებისა თუ პარტნიორების ინფორმირება.

2. **მესამე მხარის პასუხისმგებლობა (Third-Party Liabilities)**

   ეს არის ფინანსური და სამართლებრივი ვალდებულება გარე პირების (კლიენტები, პარტნიორები, სახელმწიფო) წინაშე, თუ შეტევამ ისინი დააზარალა:

- **მონაცემთა კონფიდენციალურობისა და უსაფრთხოების დარღვევა:** მესამე პირების (კლიენტები, თანამშრომლები) პერსონალური ან კომერციული მონაცემთა გაჟონვით გამოწვეული სარჩელები და ზიანის ანაზღაურება.
- **მარეგულირებელი ჯარიმები და სანქციები (Regulatory Fines & Penalties):** მონაცემთა დაცვის კანონმდებლობის (მაგ. GDPR, პერსონალურ მონაცემთა დაცვის კანონი) დარღვევის გამო დაკისრებული ჯარიმები (თუ ეს კანონმდებლობით დასაშვებია).
- **მედია პასუხისმგებლობა (Media Liability)**
  ციფრული კონტენტის გავრცელებით გამოწვეული საავტორო უფლებების დარღვევის, ცილისწამების ან კონფიდენციალურობის შელახვის პრეტენზიები.

Cyber Risk Insurance

Cyber risk is not merely an internal Information Technology (IT) challenge—it is a complex operational, financial, and strategic risk. Cyber risks encompass any threat that could damage an organization's digital assets, disrupt business operations, cause financial loss, or compromise corporate reputation.

Policy Structure:

A cyber insurance policy is typically structured into two primary coverage pillars:

- **First-Party Losses** (direct financial loss incurred by the insured organization)
- **Third-Party Liabilities** (liabilities, defense costs, and compensation owed to external parties, including clients and regulators)

Coverages

1. First-Party Losses

Direct costs incurred by the organization to manage an active incident, mitigate operational impact, and restore assets:

- **Business Interruption Loss:** Coverage for loss of net operating income and continuing fixed operating expenses resulting from an operational disruption caused by a cyber event.

- **Data & System Restoration:** Expenses incurred to repair, restore, or reconstruct destroyed, corrupted, or encrypted data and software assets.
- **Cyber Extortion / Ransomware:** Costs associated with managing extortion events, engaging specialist negotiations expertise, and funding crisis response solutions.
- **Incident Response Expenses:**
    - **IT Forensics / Technical Investigation:** Independent technical investigation to determine the entry vector, scope, and methodology of the cyber-attack.
    - **Legal Counsel (Breach Counsel):** Specialized legal advice to manage regulatory compliance, statutory obligations, and mandatory disclosure requirements.
    - **Crisis Communications & PR:** Professional public relations support to protect brand integrity and mitigate reputational damage.
- **Notification Expenses:** Costs associated with notifying affected data subjects, clients, partners, and supervisory authorities.

2. Third-Party Liabilities

Legal liability and financial obligations arising from third-party losses (clients, commercial partners, employees, or regulatory bodies) resulting from a cyber event:

- **Privacy & Network Security Liability:** Coverage for legal defense costs, settlements, and court-awarded damages stemming from claims alleging failure to protect confidential corporate data, personal data exposure, or transmission of malicious code.
- **Regulatory Fines & Penalties:** Coverage for insurable administrative fines and penalties imposed by data protection authorities (e.g., GDPR or relevant local data protection legislation), to the extent permitted by law.
- **Media Liability:** Defense costs and damages arising from third-party claims alleging copyright infringement, trademark violation, libel, slander, or invasion of privacy resulting from digital content publication.