SOSEL
CORRETORES DE SEGUROS

CYBER RISK

O cyber risk significa qualquer risco de perda financeira, interrupção ou dano à reputação de uma organização resultante de algum tipo de falha dos seus sistemas de tecnologia da informação.

A fim de conhecer melhor o cyber risk vejamos como atua:
– Violações de segurança deliberadas e não autorizadas a fim de obter acesso a sistemas de informação.
– Violações não intencionais ou acidentais da segurança.
– Riscos operacionais de TI devido a fatores como baixa integridade do sistema.

É provável que se sinta seguro, contudo saiba aqui se o seu e-mail ou telemóvel foi hackeado.

Sabia que?
O volume de ataques tem crescido nos últimos anos, gerando perdas financeiras cada vez maiores. Estima-se que os prejuízos financeiros globais dos ciberataques poderão chegar a 6 triliões de dólares, até 2021. Para diminuir os riscos online e proteger economicamente o seu negócio, o seguro de cyber risk surge como uma solução eficiente para esse tipo de imprevisto.

- 25% das empresas portuguesas sofreram um ataque cibernético em 2016?
- o Ransomware wannacry afetou desde maio de 2017 mais de 230.000 sistemas informáticos?
- 70% dos executivos considera a cybersecurity uma atividade estratégica da empresa?
- um ataque cibernético pode parar por completo a atividade de uma empresa?
- Em 2021, a média semanal de ciberataques a organizações portuguesas aumentou 81%, face a 2020, com uma organização a ser atacada 881 vezes por semana, destacando-se a educação e saúde?
- Nos últimos 4 meses de 2021, Portugal registou cerca de 100 mil ameaças de cibersegurança.
- Portugal ocupa o 31º lugar dos países mais afetados por ataques de ransomware, num total de 101 países, com os Estados Unidos, Reino Unido e Canadá a liderarem a lista.

Mas que tipos de cyber risk existem?
- Bloqueio da utilização do sistema informático;
- Perda total dos dados;
- Dados Privados serem partilhados publicamente;
- Ameaça de eliminação dos dados roubados;
- Após bloqueio do sistema solicitarem um valor de resgate para poder voltar a utilizar/desbloquearem o seu sistema informático.

Afinal como se proteger?
Quer saber como funciona e as vantagens para a sua empresa? Continue a ler e veja o conteúdo que preparámos para si!

Hoje em dia, há uma grande ligação virtual entre pessoas, governos e empresas. Desta forma, são vários os riscos cibernéticos relacionados a golpes digitais, roubo de dados entre outras possibilidades de ciberataques.

No meio corporativo, além da acção de ciber-criminosos, a exposição a problemas digitais também se dá por parte de fraude de funcionários e de não conformidade com as leis (e as boas práticas) que regulam o ambiente virtual.

Um dos maiores riscos virtuais envolve a proteção de informações de pessoas físicas. Toda empresa que guarda dados, internos ou de clientes, está exposta a qualquer tipo de evento que possa implicar em uma reclamação de terceiros, conforme determina a Lei de Proteção de Dados Pessoais (RGPD).
Obviamente, alguns segmentos estão mais expostos por guardarem uma quantidade maior de dados de pessoas físicas, como os relacionados com call centers, instituições de educação, bancos, seguros, etc. No entanto, o seguro de cyber risk é indicado para todo o tipo de empresas.

Mas afinal porque é que a segurança informática é tão importante?
Pois bem, imagine que inesperadamente, sofre um ataque informático na sua empresa e perde todos os dados importantes para a sua empresa?

Entretanto e no caso de não ter qualquer backup dos ficheiros, toda a informação vai estar perdida. Além disso não vai conseguir (provavelmente) recuperar as pastas, ficheiros e dados relevantes que tinha guardados no seu computador e no dos seus colaboradores.

Acima de tudo, é importante que aposte, na prevenção, pois não existe nenhuma empresa que esteja isenta de sofrer um ataque informático.

Uma vez que quando existem problemas de segurança, podem suceder situações como fraudes bancárias, uso inadequado e ilegal de informações empresariais, falhas de sistemas, bloqueio de equipamentos, entre muitas outras questões.

Contudo, salientamos que apesar de não existir uma segurança absoluta e inabalável, é possível encontrar os pontos mais fracos da segurança da sua empresa, e realizar ações de melhoria de forma a reduzir riscos e aumentar a eficácia dos mecanismos de segurança.

Algumas situações recorrentes a evitar dos colaboradores da empresa:
- Não aceder à rede privada com os seus dispositivos pessoais.
- Não visitar sites inseguros ou desconhecidos.
- Utilizar palavras-passe seguras.
- Não abrir anexos desconhecidos ou duvidosos.

Além de tudo, é preciso ter em conta que todos os dias são criados milhares de vírus que têm diferentes diretrizes e funcionalidades, sendo por isso igualmente importante ter um sistema de segurança que esteja constantemente atualizado, de modo a dar resposta a essas ameaças.