

## **U svijetu cyber incidenti sve veća prijetnja kompanijama, u Hrvatskoj krađa i korupcija**

Potencijalni rizici s kojima se suočavaju kompanije na globalnoj razini uvelike se mijenjaju u 2016. godini. Dok su kompanije manje zabrinute zbog učinka tradicionalnih industrijskih rizika poput prirodnih katastrofa ili požara, raste njihova zabrinutost u pogledu učinka ostalih problematičnih događaja, žestoke konkurencije na njihovim tržištima te cyber incidenata.

Riječ je o ključnim zaključcima Allianzova barometra rizika za 2016. godinu, petog godišnjeg ispitivanja o korporativnim rizicima koje objavljuje Allianz Global Corporate & Specialty (AGCS), a u kojem je sudjelovalo više od 800 menadžera za upravljanje rizicima i stručnjaka za osiguranje iz više od 40 zemalja.

Prema Allianzovu barometru rizika zastoj u poslovanju i opskrbnom lancu i dalje je četvrtu godinu zaredom glavni rizik za kompanije na globalnoj razini. Međutim, brojne kompanije zabrinute su da će gubici povezani sa zastojem u poslovanju, koji su obično posljedica štete na imovini, biti u sve većoj mjeri prouzročeni cyber napadima, tehničkim kvarovima ili geopolitičkom nestabilnošću kao novim uzrocima tzv. nematerijalne štete.

Istodobno se u ovogodišnjem Allianzovu barometru rizika među prva tri korporativna rizika prvi put ističu dva rizika koja su ostvarila najveći pomak, tj. kretanja na tržištu na drugom mjestu, odnosno cyber incidenti na trećem.

Cyber incidenti također se navode kao najvažniji dugoročni rizici za kompanije u sljedećih deset godina. S druge strane, prirodne katastrofe pale su za dva mjesta, na četvrto mjesto u odnosu na prethodnu godinu, odražavajući činjenicu da su u 2015. gubici prouzročeni prirodnim katastrofama dosegli najnižu razinu od 2009. godine.

"Spektar korporativnog rizika mijenja se jer brojni industrijski sektori prolaze kroz temeljitu preobrazbu. Nove tehnologije i povećana digitalizacija mijenjaju potrošačko ponašanje, industrijsko poslovanje i poslovne modele donoseći brojne mogućnosti, ali i podižući svijest o potrebi za reakcijom na nove izazove na razini cijelog poduzeća. Kao osiguravatelji moramo surađivati sa svojim korporativnim klijentima kako bismo im pomogli suočiti se s novim oblicima stvarnosti na sveobuhvatan način", objašnjava izvršni direktor AGCS-a, Chris Fischer Hirs.

U Europi su prva tri poslovna rizika zastoj u poslovanju i opskrbnom lancu, kretanja na tržištu (nestalnost, žestoka konkurencija, stagnacija tržišta) i cyber napadi (cyber kriminal, curenje informacija, tehnički kvarovi povezani s IT tehnologijom).

Glavni rizici u Hrvatskoj

U Hrvatskoj pak uz kretanja na tržištu kao najčešće prepoznat rizik na visokom drugom mjestu liste rizika nalaze se promjene zakona i regulative te krađe, prijevare i korupcija na trećoj poziciji. Uz prirodne katastrofe među top pet rizika na hrvatskoj ljestvici nalaze se i makroekonomski trendovi (programi štednje, inflacija/deflacija).

"Ovakav redoslijed rizika u dijelu istraživanja koje se odnosi na Hrvatsku odraz je trendova i specifične ekonomske situacije na hrvatskome tržištu. I ovo istraživanje, uz ostalo, ukazuje koliko su stalne promjene zakonodavnog i regulatornog okvira rizične za poslovanje. Nestabilnost i nepredvidljivost uvjeta poslovanja, prijevare, korupcija i pravna nesigurnost destimulativni su za razvoj poslovanja i nove investicije", komentirao je Kristijan Buk, član Uprave za financije u Allianz Zagreb.

#### Izazovno tržišno okruženje

Više od trećine ispitanika (34 %) navelo je kretanja na tržištu kao što je pojačana konkurencija ili nestalno/stagnirajuće tržište kao jedan od tri najvažnija poslovna rizika za 2016. godinu, navodeći tu novu kategoriju iz ispitivanja kao drugu najvažniju opasnost na globalnoj razini.

Kretanja na tržištu posebno zabrinjavaju u području strojarstva, financijskih usluga, proizvodnje, brodogradnje i pomorstva te u sektorima farmacije i prijevoza, gdje taj rizik zauzima položaj među prva tri poslovna rizika. Nadalje, taj rizik predstavlja jedan od dva glavna razloga za zabrinutost u Europi, azijsko-pacifičkoj regiji, Africi i na Bliskom istoku.

Brojne kompanije suočavaju se s rastućim brojem izazova koji dovode u opasnost njihovu profitabilnost i potencijalno njihove poslovne modele.

"Poduzeća moraju stalno pomno pratiti situaciju, nuditi nove proizvode, usluge ili rješenja kako bi ostala relevantna kupcima i kako bi ostvarila uspjeh u promjenjivom i globalno konkurentskom okruženju", kaže Bettina Stoob, voditeljica Odjela inovacija u AGCS-u.

Dodaje kako se ciklusi inovacija ubrzano skraćuju; ruše se prepreke ulascima na tržište; potrebno je brzo usvojiti povećanu digitalizaciju i nove ometajuće tehnologije, dok potencijalno agilnije start-up tvrtke ulaze u igru. Kompanije istodobno moraju poštovati propise koji se mijenjaju ili koji se već provode, povećane zahtjeve u odnosu na sigurnost ili ograničenja u odnosu na uvoz/izvoz.

#### Povećana sofisticiranost cyber napada

Još jedno područje povećane zabrinutosti za poduzeća na globalnoj razini jesu cyber incidenti koji uključuju cyber kriminal ili curenje informacija te tehničke kvarove povezane s IT tehnologijom.

Cyber incidenti ostvarili su dodatnih 11 postotnih bodova u odnosu na prethodnu godinu te su se prvi put pomaknuli s petog mjesta među prva tri rizika (28 % odgovora). Prije pet godina cyber incidenti utvrđeni su kao rizik, ali u prvom Allianzovu barometru rizika navelo ih je samo 1 % ispitanika.

Sudeći prema odgovorima, gubitak ugleda (69 %) glavni je uzrok ekonomskog gubitka za poduzeća nakon cyber incidenta, nakon čega slijedi zastoj u poslovanju (60 %) te odštetni zahtjevi nakon povrede podataka (52 %).

Prema Allianzovu barometru rizika kompanije su sve zabrinutije zbog rastuće sofisticiranosti cyber napada.

"Hakerski napadi sve su više usmjereni na određene mete, dulje traju i uzrokuju neprestano probijanje", objašnjava Jens Krickhahn, stručnjak za računalno osiguranje u AGCS-u.

Rastu učestalost i težina računalnih napada, stoga poduzeća ne bi smjela podcijeniti učinak zastoja u radu u današnjim visoko digitalnim i povezanim industrijama.

"Jednostavan tehnički kvar ili korisnička pogreška mogu dovesti do velikog zastoja u IT sustavu te poremetiti opskrbne lance ili proizvodnju", kaže Volker Muench, AGCS-ov stručnjak za imovinsko osiguranje.

"Potrebno je implementirati sustave ranog upozoravanja i bolje sustave praćenja kako bi se spriječili veliki gubici kao posljedica zastoja u poslovanju zbog cyber napada", zaključuje Krickhahn.

Preuzeto sa: [banka.hr](http://banka.hr)