Willis Towers Watson

Press Release

Niepewność towarzyszy firmom, które decydują o przywództwie w obszarze cyberbezpieczeństwa, twierdzi Willis Towers Watson

Badanie przeprowadzone przez Global Economist Intelligence Unit, sponsorowane przez Willis Towers Watson, prezentuje różne podejścia przywództwa w zakresie bezpieczeństwa cybernetycznego w organizacjach, przy lepszej komunikacji i współpracy pomiędzy różnymi szczeblami zarządzania w organizacji, w tym przede wszystkim pomiędzy zarządem a menedżerami ds. bezpieczeństwa sieci (CISO).

Arlington, Wirginia/ Londyn, 5 września 2018 – Większość kadry zarządzającej na całym świecie ma świadomość, że staje przed dylematem "specjalista czy generalista", w kwestii tego, który z nich powinien objąć kierownictwo nad bezpieczeństwem cybernetycznym z uwagi na niebagatelne znaczenie tego tematu w organizacji, a także ze świadomością tego, że specjalizacja jest niezbędna. Jest to widoczne w wynikach globalnego badania przeprowadzonego przez The Economist Intelligence Unit (EIU) i sponsorowanego przez Willis Towers Watson. The EIU przebadał ponad 450 organizacji z całego świata pod kątem stosowanych strategii i wyzwań w obliczu których stoją, budując organizację odporną na ataki cybernetyczne. Prawie 40 procent kadry zarządzającej objętej badaniem była zdania, że to zarząd powinien nadzorować cyberbezpieczeństwo, a 24 procent kadry zarządzającej objętych badaniem uważało, że tematem tym powinien zająć się wyspecjalizowany komitet ds. cyberbezpieczeństwa. Niewielka część ankietowanych respondentów uważała, że odpowiedzialność za sprawy cyberbezpieczeństwa powinna leżeć w gestii audytu, zespołu ds. ryzyka lub innych grup.

Badanie wykazało także, że komunikacja w ramach ról przywódczych związanych z cyberbezpieczeństwem także wykazuje pewne niespójności:

- Tylko 8% kadry zarządzającej twierdzi, że menedżerowie ds. bezpieczeństwa sieci lub równorzędne osoby zajmujące się bezpieczeństwem sieci wykazują się ponad przeciętną skutecznością w komunikowaniu cyber zagrożeń i możliwych konsekwencji finansowych, personalnych lub reputacyjnych
- Mniej niż jedna czwarta kadry zarządzającej twierdzi, że wg oceny zarządu, odporność na ataki cybernetyczne w ich organizacjach plasuje się „powyżej przeciętnej"

Willis Towers Watson

Press Release

- Mniej niż 15% przyznaje menedżerom ds. bezpieczeństwa sieci lub równorzędnym osobom zajmującym się bezpieczeństwem sieci najwyższą ocenę w skali od jednego do dziesięciu.

“Nic dziwnego, że jednym z kluczowych wyzwań przed którym stają organizacje przy wdrażaniu planu ograniczenia ryzyka cybernetycznego czy planu bezpieczeństwa jest luka w komunikacji pomiędzy zarządem a menedżerami ds. bezpieczeństwa sieci.”, mówi Anthony Dagostino, globalny menedżer ds. zarządzania cyber ryzykiem w Willis Towers Watson. „Budowanie odporności cybernetycznej na ataki rozpoczyna się w zarządzie, ponieważ to zarząd w pełni rozumie ryzyko i jest w stanie wesprzeć swoje firmy w opracowaniu odpowiedniej strategii, zmierzającej do skutecznego zmniejszenia tego ryzyka. Pomimo tego, że menedżerowie ds. zarządzania bezpieczeństwem sieci są także specjalistami ds. bezpieczeństwa, to większość z nich wciąż zmaga się z problemem odpowiedniego przełożenia zagrożeń bezpieczeństwa na operacyjny i finansowy wpływ tychże na organizacje – czyli kwestie które zarząd chciałby zrozumieć. Aby zamknąć tę lukę komunikacyjną, menedżerowie ds. bezpieczeństwa sieci potrzebują odpowiednich narzędzi, które wspomogą ich w szacowaniu i interpretowaniu zagrożeń ujawnionych w trakcie badania zaawansowania i gotowości systemu do obrony przed cyber atakami. Narzędzia te pozwolą im na skuteczniejsze raportowanie ryzyka zarządowi, umożliwią określenie odpowiedniego budżetu oraz pozwolą zarządowi na przekazanie istotnych wskazówek.”

Według badania, dylemat “specjalista czy generalista” nie jest spotykany tylko i wyłącznie na poziomie zarządczym, jako że cyberbezpieczeństwo wymaga wiedzy i umiejętności specjalistycznych, a także posiadania odpowiednich i szeroko rozumianych kompetencji z zakresu biznesu, kapitału ludzkiego i przetwarzania danych. I tak na przykład, ponieważ błędy pracowników przyczyniają się do powstawania większości incydentów cybernetycznych, dwie trzecie ankietowanych organizacji uważa, że kluczową rolę odgrywa współpraca pomiędzy działem HR i działem Bezpieczeństwa Informacji. Gdy zapytano organizacje, kto przejmuje wiodącą rolę w kształtowaniu polityki cyberbezpieczeństwa związanej z pracownikami, 54% odpowiedziało że dział HR przy współpracy zespołu Bezpieczeństwa Informacji, a 28% odpowiedziało, ze to zespół Bezpieczeństwa Informacji przy współpracy działu HR. „Wyniki tych badań są optymistyczne, ponieważ sygnalizują, że coraz więcej firm angażuje działania HR w definiowaniu ryzyka cybernetycznego. Pomimo tego, organizacje ciągle jednak potrzebują usprawnienia współpracy pomiędzy zarządzającymi zasobami ludzkimi (CHRO) a menedżerami ds. zarządzania bezpieczeństwem sieci, co pomoże w dokonaniu rzetelnej oceny kultury organizacyjnej w kontekście cyber ryzyka. Szkolenie w zakresie zwiększenia świadomości cyberbezpieczeństwa nie zawsze jest jedynym rozwiązaniem. Może to być także awans w postaci powierzenia kierownictwa, stosowanie zachęt i nagród, które leżą w gestii osoby odpowiedzialnej za zarządzanie zasobami ludzkimi” dodaje Dagostino.

Willis Towers Watson

Press Release

Inne wyniki dotyczące obowiązków menedżerów odpowiedzialnych za cyberbezpieczeństwo ukazują, że:

- Trzy z czterech badanych regionów sądzi, że “zarząd jako całość” powinien nadzorować ryzyko cybernetyczne, podczas gdy Europa uważa, że do tego celu powinna zostać powołana dedykowana grupa ds. cyberbezpieczeństwa
- Tylko 30 procentu kadry zarządzającej uważa, że posiada wystarczającą liczbę dyrektorów, którzy rozumieją ryzyko cybernetyczne, oraz że tylko 23 procent aktywnie rekrutuje dyrektorów, którzy rozumieją takie ryzyka.
- We wszystkich regionach, poza Wielką Brytanią, szefowie ds. bezpieczeństwa cybernetycznego raportują bezpośrednio do prezesów. W Wielkiej Brytanii większość raportuje do zarządu.

Dokładniejsze informacje dotyczące zarządzania w zakresie korporacyjnego bezpieczeństwa cybernetycznego oraz pełny raport znajdują się pod linkiem here.

O Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) jest wiodącą, globalną firmą w branży doradztwa i pośrednictwa ubezpieczeniowego, dostarczającą rozwiązania i pomagającą klientom na całym świecie w przekształcaniu ryzyka w ścieżkę rozwoju. Korzenie Willis Towers Watson sięgają 1828 roku, firma obecnie zatrudnia 40 tysięcy pracowników w ponad 140 krajach. Opracowujemy i dostarczamy rozwiązania służące zarządzaniu ryzykiem, optymalizujące korzyści, rozwijające talenty oraz zwiększające siłę kapitału, aby chronić i wzmacniać zarówno przedsiębiorstwa, jak i osoby prywatne. Nasze unikalne podejście pozwala nam dostrzec newralgiczne punkty pomiędzy talentami, zasobami a pomysłami – to dynamiczna formuła, która prowadzi do osiągania satysfakcjonujących wyników w biznesie. Wspólnie uwalniamy potencjał. Więcej informacji pod linkiem willistowerswatson.com

O Willis Towers Watson Cyber

Wilis Towers Watson stosuje holistyczne podejście do zarządzania ryzykiem cybernetycznym oraz bezpieczeństwa cybernetycznego, mając świadomość, że kompleksowe korporacyjne rozwiązanie definiuje i obejmuje zarówno ludzi, kapitał, jak i strategie technologiczne. Nasi eksperci ds. cyberbezpieczeństwa odszyfrowali złożoność obecnego rozmieszczenia zagrożeń cybernetycznych tak, aby zagwarantować zintegrowaną perspektywę dużym przedsiębiorstwom działającym w różnych sektorach. Jako światowy lider w zakresie rozwiązań z obszaru kapitału ludzkiego, doradztwa i pośrednictwa w zakresie ryzyka, jesteśmy dobrze przygotowani do oszacowania luk cybernetycznych organizacji, zapewniając przy tym ochronę dzięki rozwiązaniom najlepszym w swojej klasie, oraz zmniejszenia zagrożenia atakami w przyszłości. Kompleksowe rozwiązania dotyczące cyberbezpieczeństwa znajdują się pod linkiem willistowerswatson.com/cyber.

Willis Towers Watson

Press
Release

Kontakt dla mediów

Diana Alickaj +1 646 395 6323
willistowerswatson@cognitomedia.com

Benjamin Theile-Long +44 (0) 20 7426 9406
willistowerswatson@cognitomedia.com