CHUBB®

Ochrona przed cyberzagrożeniami

Spis treści

Wstęp

Współdziałanie

Żadna organizacja nie może sobie pozwolić na beztroskę w kwestii cyberryzyka. Skala zagrożenia skłania do refleksji, a ataki stają się coraz częstsze i coraz bardziej finezyjne. W najnowszym badaniu przeprowadzonym przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) opisano aż 15 rodzajów zagrożeń[1]. Jego autorzy przestrzegają, że „cyberprzestępcy są zawsze o krok przed obrońcami”[2].
Nasz raport oparto na analizie opinii menedżerów wyższego szczebla w działach IT oraz zarządzania ryzykiem z ponad 250 firm z całej Europy, których roczne przychody przekraczają 500 mln euro.
W niniejszym raporcie wskazujemy na zasadnicze różnice w podejściu do cyberryzyka różnych działów tej samej organizacji i staramy się znaleźć sposób na ich pogodzenie.

Różne opinie

Nasze ustalenia pokrywają się z ostrzeżeniami ENISA. Więcej niż co czwarty ankietowany potwierdza, że przez ostatnie 12 miesięcy w jego otoczeniu miał miejsce incydent związany z cyberprzestrzenią o poważnych skutkach, lub dokonano włamania do firmowych systemów informatycznych.

Cyberryzyko szybko staje się coraz częściej poruszanym tematem w gabinetach zarządów, nie ma jednak zgody co do tego, jak najlepiej z nim walczyć. Dla wielu to dział IT powinien odpowiadać za to zagadnienie, jednak rzadko jego członkowie wiedzą, jak najlepiej minimalizować to ryzyko. Wielu innych uważa, że główną rolę powinien odgrywać dział zarządzania ryzykiem.

Mnóstwo pytań pozostaje bez odpowiedzi. Dlaczego? Często dlatego, że eksperci od IT i ich odpowiednicy zarządzający ryzykiem mają sprzeczną wizję działania. Czy lepiej założyć, że włamania nie da się uniknąć i postawić na jak najszybszą reakcję, czy może organizacja powinna skupić się na zbudowaniu zabezpieczeń nie do złamania? Czy zabezpieczenia w którymkolwiek z obszarów działalności firmy muszą być silniejsze niż w innych? Jaką rolę pełnią osoby trzecie, np. ubezpieczyciele?

Najważniejsza jest współpraca

Znalezienie odpowiedzi na powyższe pytania wymaga współpracy pomiędzy IT, ryzykiem, pozostałymi działami oraz ubezpieczycielami. Podmioty, które nie osiągną porozumienia w tej kwestii ryzykują powstanie luk w procesie zarządzania cyberryzykiem i zabezpieczeniach, które mogą zostać wykorzystane.

W walce przeciwko cyberprzestępcom najważniejsze jest współdziałanie.

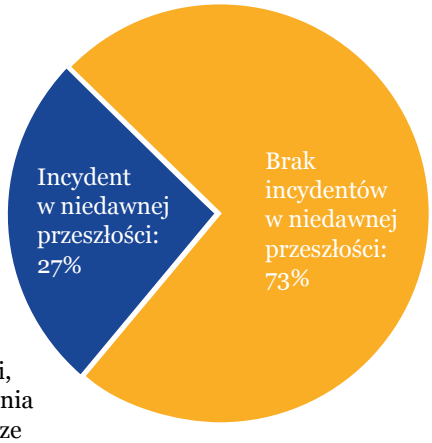
[1] Złośliwe oprogramowanie (malware), ataki sieciowe, ataki przez aplikacje internetowe, ataki typu „odmowa usługi” (DoS), botnety, phishing, spam, oprogramowanie ransomware, zagrożenia wewnętrzne, manipulacja fizyczna/uszkodzenie/kradzież/utrata, zestawy eksploitów, włamania do baz danych, kradzież tożsamości, wyciek informacji i cyberszpiegostwo.

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Istota zagrożenia

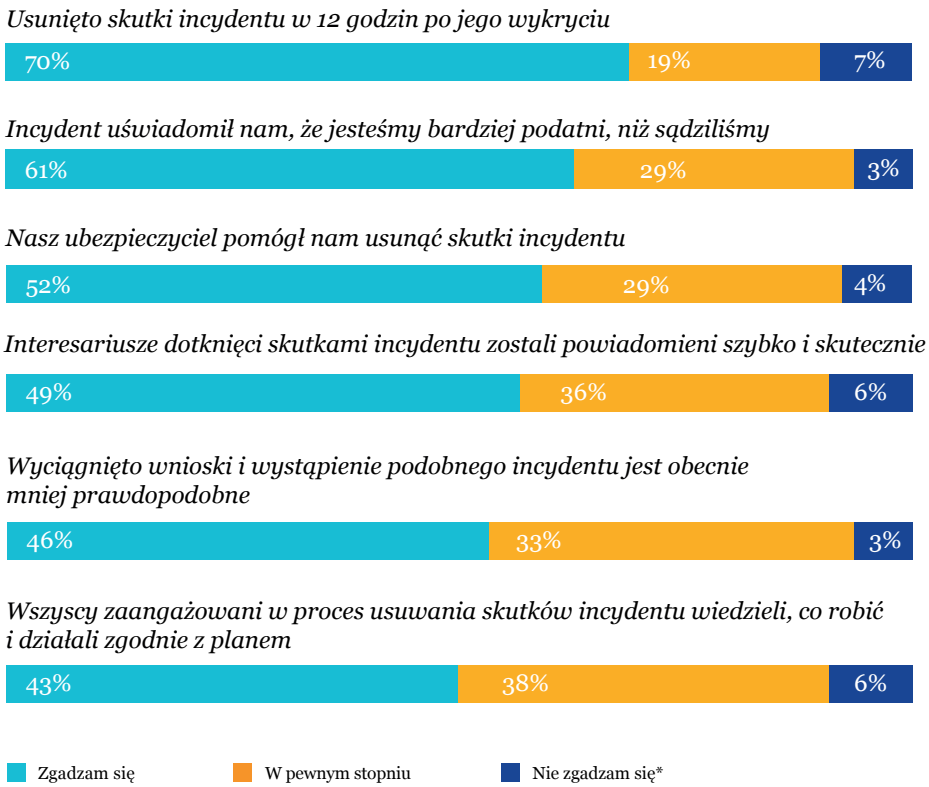
Liczba podmiotów, które w ubiegłym roku odnotowały poważny w skutkach incydent cybernetyczny lub włamanie do systemów informatycznych to dowód, że cyberryzyko jest zagrożeniem jak najbardziej realnym.

Wykres 1. Osoby ankietowane, do których systemów się włamano lub które odnotowały poważny incydent przez ostatnie 12 miesięcy.



Większość ankietowanych twierdzi, że poradziła sobie dobrze i firma powróciła do normalnego funkcjonowania w 12 godzin, pozostały jednak widoczne skutki tego zdarzenia. W wielu przypadkach incydent zwrócił uwagę na wcześniej nierozpoznane luki, a jedynie niewielu twierdzi, że ryzyko wystąpienia podobnego zdarzenia w przyszłości jest mniejsze (patrz: Wykres 2).

Wykres 2: Stopień, w jakim ankietowani zgadzają się z następującymi stwierdzeniami o włamaniu.



* Pozostałe udzielone odpowiedzi to „nie dotyczy".

„Eksperci ds. IT bardziej martwią się o przygotowanie swoich współpracowników.”

Organizacje podzielone

Przedsiębiorstwa mogą dysponować planami reagowania i stosownymi procedurami na wypadek incydentu, ale nie wszyscy pracownicy mogą być w pełni świadomi swoich obowiązków.

Mniej niż połowa osób, których pracodawcy doświadczyli włamania lub poważnego incydentu związanego z cyberprzestrzenią deklaruje, że wszyscy pracownicy wiedzieli jak się zachować i że podjęte działania były zgodne z planem. To niepokojące. Aby skutecznie usunąć skutki incydentu, wszyscy muszą działać szybko i zgodnie z opracowaną strategią działania.

– Nie wystarczy założyć, że uda się uporać ze wszelkiego rodzaju zagrożeniami – tłumaczy Lauren Webb, menedżer ds. cyberryzyka w Chubb w Londynie. – Należy przygotować plan usuwania skutków incydentu, który pozwoli zminimalizować szkody. Trzeba unikać sytuacji, w których zagrożenie rozprzestrzenia się dalej, bo nikt nie wie, co ma robić. Wszyscy muszą znać plan reagowania.

Na tego rodzaju kwestie szczególnie zwracają uwagę działy IT, gdzie tylko 29% ankietowanych deklaruje, że osoby dotknięte incydentem wiedziały dokładnie co robić. Stoi to w wyraźnej sprzeczności z opinią osób zarządzających ryzykiem, wśród których ten współczynnik wyniósł 54% i wyraźnie wskazuje, że to eksperci ds. IT bardziej martwią się o przygotowanie swoich współpracowników.

Co w tej kwestii mogą zrobić firmy? – Aby zapewnić spójność reakcji, należy zacząć od kierownictwa najwyższego szczebla – twierdzi Kyle Bryant, menedżer ds. cyberryzyka na Europę w Chubb. – Potrzebna jest wpływowa osoba, której uda się pogodzić różnice i przekonać obie strony, że ryzyko cybernetyczne jest ryzykiem całego przedsiębiorstwa.

Coraz większa świadomość, ale zdania wciąż podzielone

Świadomość istnienia cyberzagrożeń jest coraz większa, ale przed podmiotami jeszcze wiele pracy, aby na każdym szczeblu zrozumiano powagę sytuacji. Większość menedżerów najwyższego szczebla twierdzi, że przez ostatnie dwa lata więcej uwagi poświęcili temu zagadnieniu, a ponad dwie trzecie ekspertów ds. IT (69%) deklaruje, że problem cyberryzyka omawiany jest obecnie na szczeblu zarządu. Jednakże ten współczynnik jest niższy o 57% w przypadku osób zarządzających ryzykiem, a większość martwi się tym, że temat cyberzagrożeń jest postrzegany jako zmartwienie działów IT (patrz poniżej).

Udział osób ankietowanych, które zgadzają się z poniższymi stwierdzeniami:

65%

Przez ostatnie dwa lata nasza firma poświęciła więcej czasu analizie cyberzagrożeń i wzmacnianiu ochrony przed nimi.

62%

Cyberryzyko to problem omawiany na szczeblu zarządu mojej firmy.

60%

Moja firma wciąż uznaje cyberryzyko za problem IT.

54%

W mojej ocenie nie jesteśmy świadomi wszystkich cyberzagrożeń, które nas dotyczą.

50%

Nasi pracownicy generalnie nie są świadomi, jak dużym zagrożeniem dla naszej firmy są cyberryzyka.

40%

W mojej organizacji nie ma jednoznacznego zrozumienia, co niosą ze sobą cyberzagrożenia.

Działy IT i ryzyka spierają się co do stopnia przygotowania organizacji na próby włamania. Około 75% ekspertów ds. IT twierdzi, że w organizacji poświęca się czas na wzmocnienie ochrony przed cyberatakami, ale jedynie 58% osób zarządzających ryzykiem podziela ten pogląd.

Daniel Jacobs, menedżer ds. ubezpieczeń od cyberzagrożeń na kraje Beneluksu w Chubb ostrzega, że organizacje muszą położyć kres tego rodzaju sporom, jeżeli chcą chronić się skutecznie i wszechstronnie. – Osoby zajmujące się IT rozumieją, że nie da się zabezpieczyć przed wszystkim, ale menedżerowie zarządzający ryzykiem nie są jeszcze o tym przekonani – mówi menedżer.

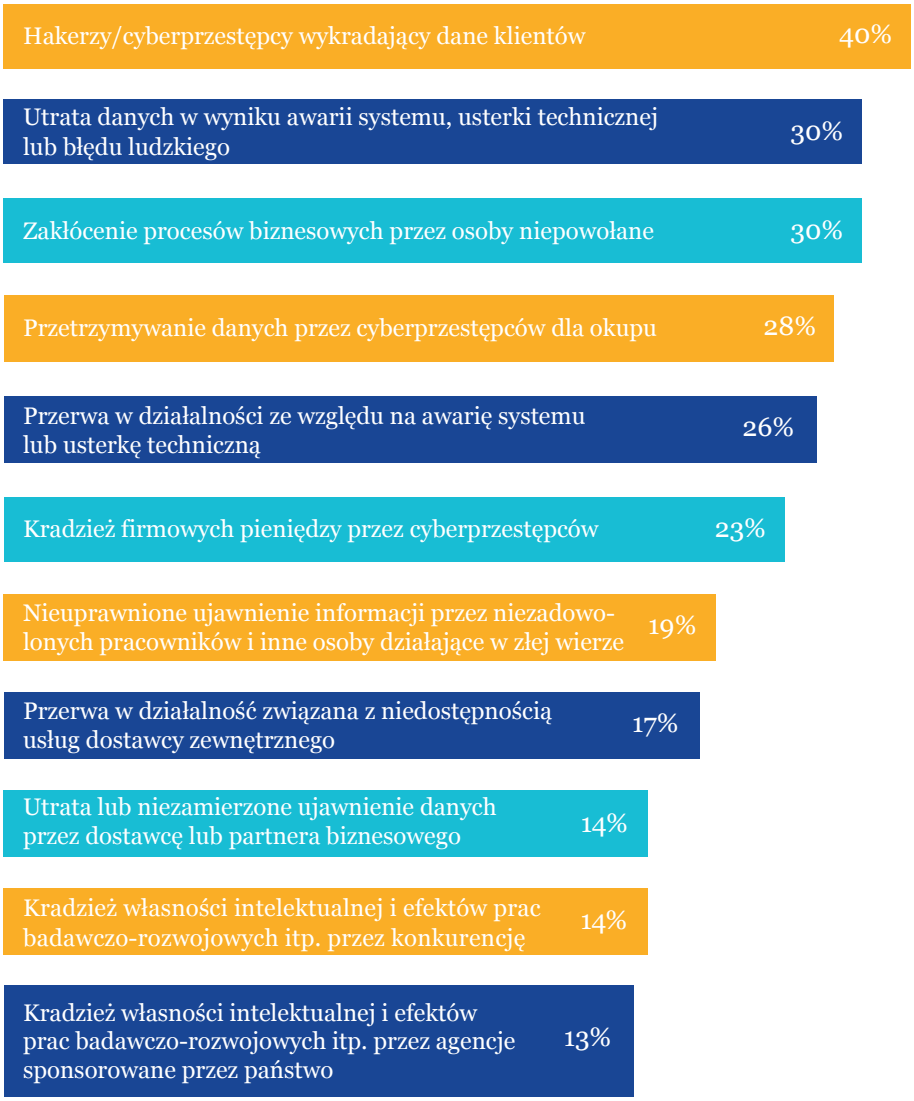
Ponad dwie trzecie ekspertów ds. IT (69%) deklaruje, że problem cyberryzyka omawiany jest obecnie na szczeblu zarządu, ale tylko 57% osób zarządzających ryzykiem jest tego samego zdania.

Zagrożenia zewsząd

Biorąc po uwagę skalę i różnorodność zagrożeń, każda luka w zabezpieczeniach nabiera kluczowego znaczenia. Każda słabość może uniemożliwić podmiotowi skuteczne ograniczenie ryzyka.

Według ankietowanych największymi zagrożeniami dla każdej organizacji są hakerzy wykradający dane klientów, jak również utrata danych spowodowana chociażby błędem pracownika, zakłócenie procesów biznesowych przez niepowołane osoby, przetrzymywanie danych przez cyberprzestępców dla okupu, czyli tzw. wymuszenie komputerowe oraz przerwa w działalności. (patrz: Wykres 3).

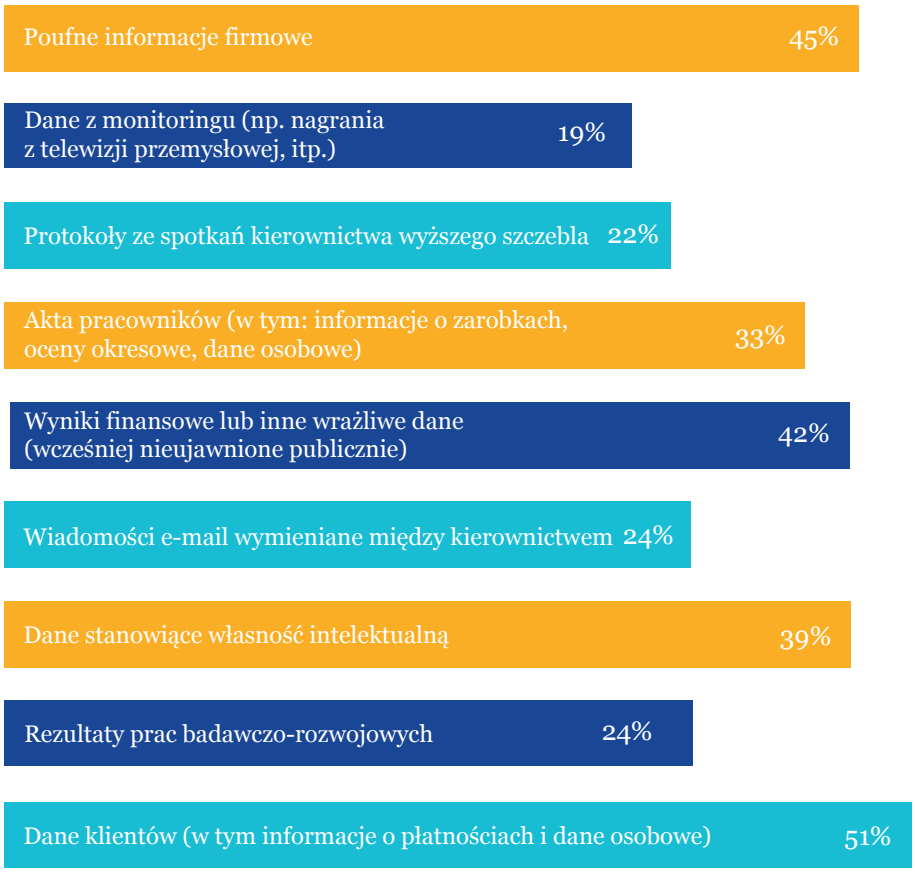
Wykres 3: Udział ankietowanych, które wskazują dane zagrożenie za najważniejsze dla ich organizacji:



W wielu przypadkach zagrożenie jest wielowymiarowe. Dobrym przykładem jest utrata danych. Ponad połowa ankietowanych (patrz: Wykres 4) twierdzi, że spośród wszystkich zgromadzonych danych, utrata danych o klientach ich firm miałaby najbardziej dotkliwe konsekwencje. Może to wynikać ze znacznej ochrony prawnej dla takich danych wprowadzonej unijnym rozporządzeniem o ochronie danych osobowych (RODO), które zaczyna obowiązywać w 2018 r. i przewiduje dotkliwe kary dla organizacji, które naruszą jego postanowienia.

Inne zagrożone dane to również poufne dane firmowe, własność intelektualna oraz wyniki prac badawczo-rozwojowych.
Aby ograniczyć ryzyko związane z cyberzagrożeniami, organizacje będą musiały chronić dane na wszystkich z powyższych frontów – i to jednocześnie.

Wykres 4: Udział ankietowanych, według których wyciek następujących rodzajów danych miałby najbardziej dotkliwe konsekwencje dla firmy.



„W rzeczywistości wielu organizacjom jest niezwykle trudno ocenić konsekwencje ewentualnego cyberincydentu lub włamania”

– Lauren Webb
Analityk ds. cyberryzyka
w Chubb w Londynie

Różnice zdań

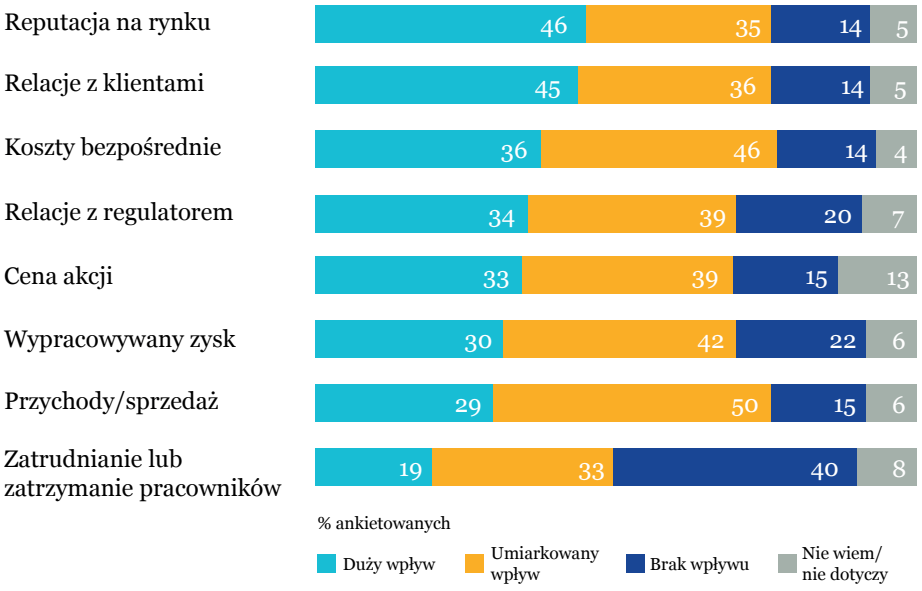
Eksperci ds. IT zakładają poważniejsze konsekwencje cyberincydentów, niż ich odpowiednicy zarządzający ryzykiem (patrz: Wykres 5). To kolejny dowód na to, że nie wszystkie organizacje w jednolity sposób postrzegają skalę zagrożenia oraz wypracowały jeden sposób obrony przed nim. Brak spójności może stanowić zagrożenie.

– W rzeczywistości wielu organizacjom jest niezwykle trudno ocenić konsekwencje ewentualnego cyberincydentu lub włamania – tłumaczy Lauren Webb z Chubb. – IT i ryzyko będą musiały współdziałać i razem analizować zagrożenia, przed jakimi staje ich organizacja oraz ocenić ewentualne konsekwencje w wymiarze finansowym.

Wykres 5: Obszary, w których incydent związany z cyberprzestrzenią miałby najbardziej dotkliwe konsekwencje według działów IT i zarządzania ryzykiem:

	Zarządzanie ryzykiem	IT
Koszty bezpośrednie	32%	41%
Cena akcji	27%	41%
Zatrudnianie lub zatrzymanie pracowników	17%	22%
Relacje z regulatorem	35%	33%
Wypracowywany zysk	23%	42%
Przychody/sprzedaż	26%	34%
Relacje z klientami	42%	50%
Reputacja na rynku	42%	53%

Wykres 6: Skutki cyberincydentu o największych konsekwencjach według osób ankietowanych:



Stan gotowości

W naszej ocenie, gotowość do błyskawicznej reakcji to najważniejszy element strategii ograniczania skutków cyberzagrożeń przez każdy podmiot. Ankietowane przez nas osoby zazwyczaj pozytywnie oceniają swoje przygotowanie, jednak są też świadome pewnych braków – pewność siebie przedstawicieli IT niekoniecznie znajduje odzwierciedlenie w opiniach ich odpowiedników zarządzających ryzykiem.

Osoby ankietowane deklarują, że ich firmy są przygotowane do obrony przed cyberryzykami. 72% przyznaje sobie ocenę 4 lub 5 w skali od 1 do 5, gdzie 5 oznacza doskonały stan zabezpieczeń, a 1 słaby.

Są jednak obszary, co do których ankietowani są bardziej pewni zabezpieczeń niż w innych. Cztery osoby na pięć (81%) uważają, że ich organizacje zdołają ochronić sieci i systemy IT w przypadku cyberataku, a 74% uważa dane wrażliwe za bezpieczne. Mają również dobre zdanie o mechanizmach tworzenia kopii zapasowych, antywirusach i firewallach oraz planach reagowania na wypadek incydentu – co najmniej 68% przyznaje sobie ocenę 4 lub 5. **Obliczenie kosztów incydentu sprawia im już większą trudność (58%)**.

Planowanie reakcji

Wiele osób ankietowanych nie jest pewnych, czy ich systemy zabezpieczeń staną na wysokości zadania. Mniej niż połowa z tych, którzy nigdy nie doświadczyli włamania twierdzi, że dysponują odpowiednim planem reagowania na wypadek cyberincydentu oraz że regularnie testują i aktualizują procedury.

Niepokoi to, że 55% z tych osób zakłada (w pewnym stopniu), że nigdy nie będą mieć do czynienia z poważnym incydentem związanym z cyberprzestrzenią.

Nasze badanie może sugerować, że w zabezpieczeniach przed cyber-zagrożeniami występują luki, a sytuację pogarsza brak spójności procesów.

– Brak jasności i koordynacji działań najczęściej dotyczy wykrywania i reagowania – powiedział Roger Francis, starszy konsultant strategiczny i kierownik ds. ubezpieczeń od cyberzagrożeń w Mandiant. Aby skutecznie zareagować na incydent, należy zawczasu zaplanować plan reakcji oraz wdrożyć odpowiednie procesy i matryce eskalacji, porządkujące różnorodne działania. Choć osoby koordynujące działania w razie wystąpienia incydentu dobrze radzą sobie z identyfikacją okoliczności włamania, potrzebują wsparcia pozostałych części organizacji, aby móc powstrzymać rozprzestrzenianie się zagrożenia i usunąć jego skutki.

Samoocena

Niemalże w każdym obszarze zarządzania cyberryzykiem ankietowani z działów IT są bardziej pewni swoich kompetencji, niż ich odpowiednicy zarządzający ryzykiem. Na Wykresie 7 przedstawiono różnice w wielu kluczowych obszarach ochrony przed cyberzagrożeniami.

Xavier Leproux, starszy analityk ds. ubezpieczeń technicznych w Chubb sugeruje, że IT mogłoby bardziej przystępnie objaśniać mechanizmy ograniczania cyberryzyka pozostałym działom organizacji.

– Osoby zarządzające ryzykiem wiedzą, że ryzyko występuje, ale ciężko im je samodzielnie ocenić – uważa. – Gdy rozmawiają z osobami z IT, zazwyczaj nie otrzymują prostych odpowiedzi, na podstawie którym mogliby wyrobić sobie własną opinię.

Wykres 7: Obszary, w których osoby zarządzające IT i ryzykiem oceniają przygotowanie organizacji jako doskonałe lub bardzo dobre

	Zarządzanie ryzykiem	IT
Opracowanie i testowanie planu reagowania na incydent	64%	74%
Opracowanie kompleksowej polityki bezpieczeństwa dotyczącej cyberzagrożeń	63%	75%
Oszacowanie łącznego kosztu incydentu związanego z cyberprzestrzenią	53%	65%
Szkolenie pracowników w zakresie najlepszych praktyk ograniczania cyberryzyka	58%	76%
Tworzenie profilów ryzyka dla poszczególnych zbiorów danych i systemów informatycznych	64%	70%
Wdrażanie oprogramowania antywirusowego i zapór ogniowych oraz uszczelnianie procedur w całej strukturze organizacji	68%	82%
Identyfikacja i zakup najbardziej odpowiedniego oprogramowania antywirusowego i zapór ogniowych oraz uszczelnień procedur dla naszej organizacji	63%	75%

Najwięcej obowiązków spoczywa na pracownikach IT, którzy walczą na froncie z atakującymi organizację hakerami. Muszą usprawnić komunikację z pozostałymi pracownikami. Bliższa współpraca pozwoli ograniczyć nieporozumienia i opracować jednolitą politykę zarządzania cyberryzykiem.

Zarządzanie i odpowie-dzialność

Skuteczne ograniczanie cyberryzyka zależy nie tylko od możliwości technicznych, ale również od sposobu zarządzania i współpracy poszczególnych działów. Te elementy umożliwiają zarządzanie zagrożeniami w ramach ściśle określonych linii odpowiedzialności.

Ryzyko przedsiębiorstwa

– Cyberryzyko jest ryzykiem całego przedsiębiorstwa i może potencjalnie wpływać na działalność, a wręcz na samo istnienie organizacji – przyznaje Saïd Dami, inżynier ds. cyberryzyka na Europę w Chubb. – Obowiązkiem zarządzających ryzykiem na najwyższym szczeblu musi być stworzenie odpowiedniej struktury ramowej, którą następnie należy wdrożyć w całej organizacji.

Przed wieloma organizacjami jeszcze wciąż sporo pracy, aby osiągnąć ten cel. Część z nich nie ufa strukturom zarządczym, a poglądy pracowników IT i zarządzających ryzykiem znacznie się różnią.

Kto jest właścicielem ryzyka?

Tylko 37% osób ankietowanych jest przekonanych, że w ich firmie jasno określono własność cyberryzyka, a nawet mniej, bo tylko 35%, deklaruje, że współpraca pomiędzy działami firmy przebiega dobrze.

Eksperci ds. IT mają generalnie bardziej optymistyczną ocenę gotowości organizacyjnej, niż osoby zarządzające ryzykiem (patrz: Wykres 9).

Osoby zarządzające ryzykiem zazwyczaj przyjmują odpowiedzialność za współpracę i organizację zarządzania w zakresie cyberryzyka w skali całej organizacji, dlatego ich względny pesymizm musi doprowadzić do trudnych rozmów z bardziej optymistycznie nastawionymi pracownikami IT.

37%

Tylko 37% osób ankietowanych jest zdecydowanie przekonanych, że w ich firmie jasno określono odpowiedzialność za zarządzanie ryzykiem cybernetycznym.

35%

Tylko 35% deklaruje, że współpraca pomiędzy działami firmy przebiega zdecydowanie dobrze.

Wykres 8: Stopień, w jakim ankietowani „zdecydowanie" lub „umiarkowanie" zgadzają się z następującymi stwierdzeniami o organizacji zarządzania

Wykres 9: Różnice zdań pracowników IT i zarządzających ryzykiem, którzy zgadzają się „zdecydowanie" lub „umiarkowanie"

	Zarządzanie ryzykiem	IT
W mojej organizacji współpraca pomiędzy działami przebiega dobrze	63%	84%
W mojej organizacji jasno określono własność cyberryzyka	64%	80%
Jeżeli chodzi o cyberbezpieczeństwo, szybka reakcja jest lepsza, niż rozbudowane i wielopoziomowe zabezpieczenia	53%	63%
Lepiej silniej zabezpieczać najważniejsze dane, niż starać się chronić wszystko równie skutecznie	60%	75%

Można spodziewać się napięć, ponieważ w kwestii odpowiedzialności za cyberryzyko występuje ostry podział: 38% ankietowanych wskazuje na dyrektora IT lub członka zarządu ds. IT (CIO), 12% na dyrektora ds. technologii lub członka zarządu ds. technologii (CTO), a 17% na dyrektora zarządzającego ryzykiem. Powyższy podział dobrze oddaje przekonania osób ankietowanych odnośnie do tego, jak powinien wyglądać podział odpowiedzialności (dane szczegółowe przedstawiono poniżej).

Opinie poszczególnych działów są podzielone. Prawie połowa (43%) osób ankietowanych z działów IT twierdzi, że za cyberryzyko odpowiedzialność powinien ponosić dyrektor IT, ale taki pogląd podziela jedynie co czwarta osoba (25%) z działu zarządzania ryzykiem. Niemniej jednak więcej ankietowanych z IT uważa, że to dyrektor zarządzający ryzykiem powinien być za nie odpowiedzialny: 23% dyrektorów IT podziela ten pogląd, podczas gdy takich osób w dziale zarządzania ryzykiem jest 19%.

Kto ponosi odpowiedzialność za zarządzanie cyberryzykiem, a kto powinien?

38% | 32%

Dyrektor IT, członek zarządu ds. IT (CIO) lub osoba o podobnym stanowisku

17% | 21%

Dyrektor zarządzający ryzykiem, członek zarządu ds. ryzyka (CRO) lub osoba o podobnym stanowisku

12% | 10%

Dyrektor ds. technologii, członek zarządu ds. technologii (CTO) lub osoba o podobnym stanowisku

11% | 18%

Dyrektor generalny/prezes zarządu, dyrektor zarządzający lub osoba o podobnym stanowisku

7% | 7%

Za cyberryzyko nie odpowiada jedna osoba

6% | 5%

Członek zarządu ds. finansowych (CFO), dyrektor finansowy lub osoba o podobnym stanowisku

5% | 4%

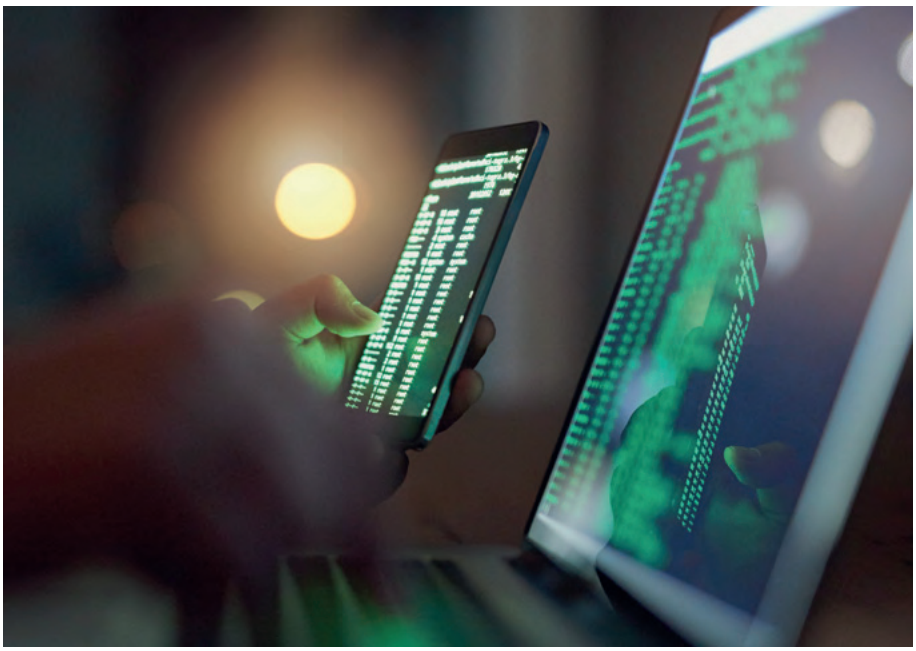
Dyrektor ds. zarządzania danymi, członek zarząd ds. zarządzania danymi (CDO) lub osoba o podobnym stanowisku

- Na kim spoczywa odpowiedzialność?
- Na kim **powinna** spoczywać odpowiedzialność?

Wygląda na to, że część menedżerów z IT chce utrzymać odpowiedzialność za cyberbezpieczeństwo, wielu ekspertów z IT (oraz ich odpowiedników zarządzających ryzykiem) patrzy obecnie szerzej na to zagadnienie.
– Był taki czas, że cyberryzyko było zagadnieniem ograniczanym wyłącznie do obszaru IT – twierdzi Saïd Dami z Chubb. – Wraz ze wzrostem znaczenia technologii i systemów cyfrowych dla całego przedsiębiorstwa, zaczyna dominować przekonanie, że cyberryzyko jest zasadniczo ryzykiem biznesowym.

„Zasadniczo bezpieczeństwo powinno być odrębnym obszarem, który doradza wszystkim jednostkom organizacyjnym przedsiębiorstwa. Jeżeli umiejscowi się je w IT, zazwyczaj nabiera wymiaru technologicznego. Jeżeli zaś w dziale prawnym – uwaga skupia się na zgodności. W przypadku zarządzania ryzykiem – na kalkulacjach ryzyka.”

– Roger Francis
starszy konsultant strategiczny
i kierownik ds. ubezpieczeń
od cyberzagrożeń w Mandiant.



Różne podejścia

Co ciekawe, osoby zarządzające ryzykiem zdecydowanie częściej niż menedżerowie z IT uważają, że organizacja może obyć się bez jednej osoby odpowiedzialnej za cyberryzyko: 11% twierdzi, że za ten rodzaj ryzyka powinna być odpowiedzialna tylko jedna osoba, a podobny pogląd podziela tylko 1% osób zarządzających IT.

Różnice opinii pogłębiają pewne założenia czynione przez przedstawicieli jednego działu o drugim. Dwie trzecie ankietowanych z IT twierdzi, że osoby zarządzające ryzykiem opuszczają tzw. strefę komfortu, zajmując się cyberryzykiem. Z kolei 56% ankietowanych z działu zarządzania ryzykiem uważa, że ich koledzy i koleżanki z IT pomijają jego „ludzki” aspekt.

Pogodzenie obu stron zajmie trochę czasu, tym bardziej, że oba działy mają różne zdania co do tego, jak należy działać. Dla przykładu, ankietowani z IT częściej narzekają, że zarząd oczekuje całkowitej odporności na ataki (66% w IT i 56% w zarządzaniu ryzykiem). Więcej z nich uważa też, że szybka reakcja jest ważniejsza, niż posiadanie rozbudowanych zabezpieczeń (63% w IT i 53% w zarządzaniu ryzykiem).

Najważniejsza może się okazać **lepsza komunikacja**, twierdzi Xavier Leproux z Chubb. – Pozostałe działy firmy muszą poczuć się pewniej, jako adresaci komunikacji płynącej z IT – uważa ekspert. – Będzie to możliwe wyłącznie wtedy, gdy prosty i przystępny przekaz dotrze do większej liczby osób, które „mówią tym samym językiem”.

Oczywiście nie ma jednego, uniwersalnego rozwiązania, ale Roger Francis z Mandiant wzywa organizacje do odłączenia cyberryzyka od jakiejkolwiek jednostki organizacyjnej i postawienie na współpracę.

– Zasadniczo bezpieczeństwo powinno być odrębnym obszarem, który doradza wszystkim jednostkom organizacyjnym przedsiębiorstwa – przekonuje. – Jeżeli umiejscowi się je w IT, zazwyczaj nabiera wymiaru technologicznego. Jeżeli zaś w dziale prawnym – uwaga skupia się na zgodności. W przypadku zarządzania ryzykiem – na kalkulacjach ryzyka.

Przeszkody i mankamenty

Osoby zarządzające cyberryzykiem – tak wywodzące się z IT, jaki i zarządzające ryzykiem – wiedzą, że aby odnieść sukces, należy stawić czoła wielu wyzwaniom.

Osoby ankietowane wymieniają kilka przeszkód, które stoją im na drodze. Jedną z nich jest ignorowanie obowiązków związanych z ochroną danych przez pracowników. Obawiają się również stale zmieniającego się charakteru zagrożenia. Ostrzegają przed coraz większą finezją przestępców.

– Nie ma zabezpieczeń nie do złamania – przestrzega Kyle Bryant z Chubb. – Nie ma panaceum, bo przed komputerem zawsze siedzi człowiek.

Zagrożenia z wewnątrz i z zewnątrz organizacji

W przeciwieństwie do zarządzających ryzykiem, eksperci ds. IT bardziej obawiają się „czarnych charakterów": **42% mówi o finezji przestępców**, gdy tylko 27% osób zarządzających ryzykiem wskazuje na to zagrożenie. Nie jest to zaskoczeniem. Przedstawiciele IT są najbardziej świadomi coraz większego wyrafinowania hakerów i zaawansowania wykorzystywanych przez nich do włamań technologii. Świadomość tego zdaje się potęgować ich niepokój.

Sytuacja jest zgoła odmienna, jeżeli chodzi o współpracowników – tylko 30% osób ankietowanych z IT obawia się zaniedbań ze strony pracowników w zakresie ochrony danych, podczas gdy podobne obawy zgłasza 45% ankietowanych zarządzających ryzykiem.

Eksperci ds. IT są lepiej zaznajomieni z technologią, dlatego rzadziej niż zarządzający ryzykiem wskazują na ten aspekt, jako na powód do niepokoju.

Niemniej jednak pracownicy powinni być priorytetem dla wielu organizacji. Nieco ponad jedna trzecia (**34%**) wszystkich ankietowanych twierdzi, że w strategii walki z cyberzagrożeniami to pracownicy są najsłabszym ogniwem (patrz: Wykres 10). Ten pogląd podzielają przedstawiciele IT i ryzyka.

Wykres 10: Jakie jest najsłabsze ogniwo zabezpieczeń przed cyberzagrożeniami?

	Zarządzanie ryzykiem	IT
Nasi pracownicy	34%	35%
Zabezpieczenia naszych dostawców i partnerów	11%	12%
Integralność naszych systemów	14%	20%
Oprogramowanie ochronne	16%	7%
Monitorowanie przez nas oprogramowania ochronnego	10%	4%
Posiadane przez nas produkty ubezpieczeniowe	3%	3%
Nasze kierownictwo wyższego szczebla	3%	0%
Nasz dział IT	3%	7%
Nasz dział zarządzania ryzykiem	1%	2%

Pułapka niezrozumienia

Przekonanie o tym, że to pracownicy są najsłabszym ogniwem wynika z obaw o ich wiedzę i brak zrozumienia istoty cyberzagrożeń. Zaskakuje to, że tylko 41% ankietowanych uważa biegłość pracowników IT w zagadnieniach związanych z cyberryzykiem za doskonałą. Tylko 32% ma taką opinię o pracownikach działu zarządzania ryzykiem. Najbardziej niepokoją jednak ograniczenia tych, których wiedza powinna być najszersza, czyli najwyższej kadry zarządzającej. Tylko 31% ankietowanych określa stopień zrozumienia istoty cyberzagrożeń przez zarząd jako doskonały.

Obawy o słabość czynnika ludzkiego znajdują wyraz w przekonaniach ponad jednej trzeciej ankietowanych, według których lepsze szkolenie wszystkich pracowników, regularne monitorowanie ich działań oraz zapewnienie bardziej klarownej komunikacji są kluczem do poprawy jakości zarządzania ryzykiem w całej organizacji.

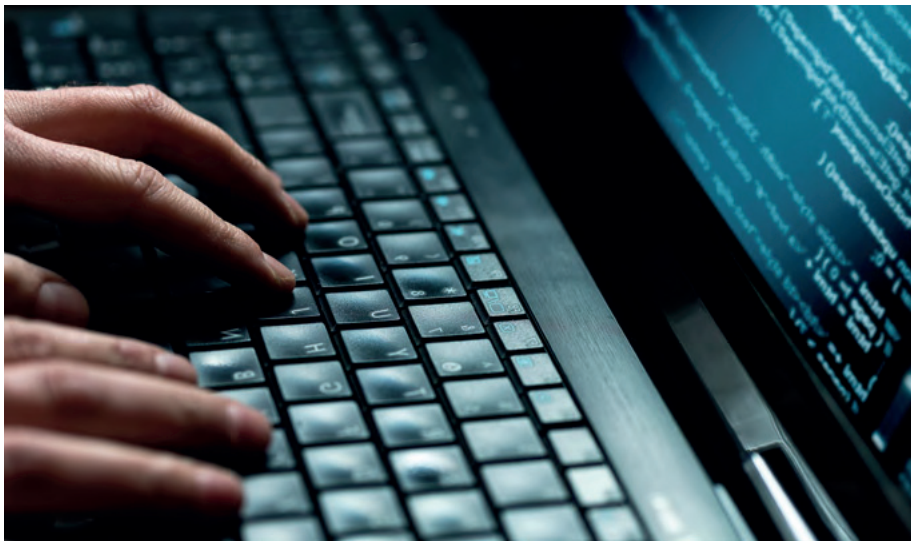
Należy podkreślić jeszcze raz, że usprawnienie komunikacji pomiędzy IT i pozostałą częścią organizacji byłoby ogromnym krokiem wprzód. – Od organizacji potrzebujemy przynajmniej powszechnego zwiększenia świadomości. Na przykład o tym, że firma przechowuje poufne dane i że może zostać zaatakowana – przekonuje Daniel Jacobs z Chubb. – Jeżeli takiej świadomość nie ma, żadne zabezpieczenia ani żadne procesy nie zapewnią ochrony.

Od systemów do ludzi

Osoby ankietowane z IT częściej skupiają się na integralności systemów danej organizacji. 20% z nich uważa ją za najsłabszą cechę cyberzabezpieczeń, a taki pogląd podziela 14% osób zarządzających ryzykiem.

– Te obawy są zrozumiałe – zauważa Kyle Bryant z Chubb. – Biorąc jednak po uwagę obawy innych działów o świadomość współpracowników, być może IT powinno skupić się na ściślejszej współpracy z innymi funkcjami. Pozwoliłoby to stworzyć spójną strategię działania i lepiej zrozumieć istotę problemu całej organizacji.

Współpraca między działami IT i zarządzania ryzykiem



Nasza analiza wskazuje na istotne różnice między działami IT i zarządzania ryzykiem co do tego, jak najlepiej ograniczać cyberryzyko. Należy dążyć do eliminacji różnic, ponieważ tylko współpraca w tym obszarze zapewni organizacjom największe szanse na skuteczną ochronę przed cyberzagrożeniami i możliwość zarządzania nimi.

– Podejście oparte na kolaboracji wymaga wytężonej i nieprzerwanej pracy, a działy zaczynają z dość kiepskiej pozycji – ostrzega Xavier Leproux.

Mniej niż połowa ankietowanych deklaruje, że IT i ryzyko współpracują w ramach sformalizowanych programów poświęconych cyberryzyku, 27% opisuje współpracę jako regularną, choć o bardziej doraźnym charakterze, a niepokojące 18% przyznaje, że współpraca ma miejsce wyłącznie w reakcji na nadchodzące zagrożenie lub dopiero po ataku.

43%

Mniej niż połowa ankietowanych deklaruje, że IT i ryzyko współpracują w ramach sformalizowanych programów poświęconych cyberryzyku.

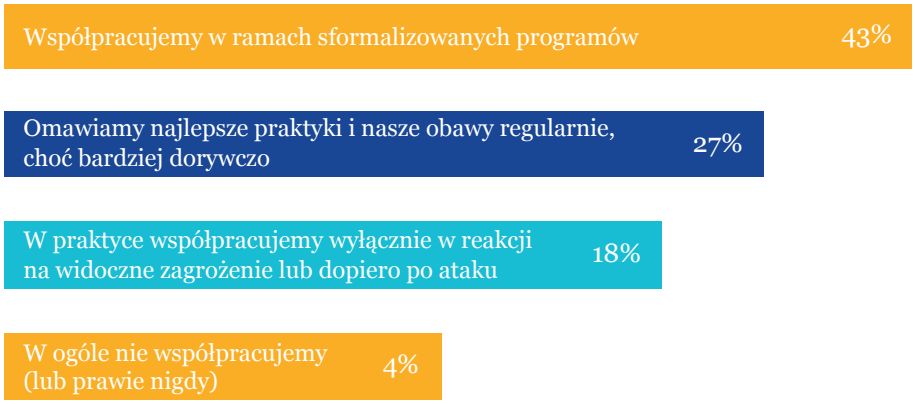
18%

Przyznaje, że współpraca ma miejsce wyłącznie w reakcji na nadchodzące zagrożenie lub dopiero po ataku.

„Postawienie na współdziałanie w zakresie zarządzania ryzykiem daje organizacji największe szanse na skuteczne ograniczenie ryzyka.”

– Lauren Webb
Analityk ds. cyberryzyka
w Chubb w Londynie

Wykres 11: Jak w praktyce wygląda współpraca pomiędzy ryzykiem i IT?



Zgodnie z odpowiedziami przedstawionymi w innych częściach niniejszego raportu, eksperci ds. IT są bardziej optymistyczni w porównaniu z ich współpracownikami zarządzającymi ryzykiem. Zazwyczaj wskazują na lepszą współpracę i chętniej przyznają, że czynione są postępy w zakresie jej usprawnienia.

Być może pracownicy działu IT powinni zastanowić się, czy nie warto nawiązać bliższej współpracy z pozostałymi częściami organizacji, a w szczególności z działem zarządzania ryzykiem.

Korzyści dla organizacji ze współpracy pomiędzy funkcjami mogą być bardzo cenne, twierdzi Lauren Webb z Chubb. – Konsekwencje cyberincydentu są daleko idące, a przecież ich eliminacja nie będzie zadaniem wyłącznie działu IT – dodaje. Postawienie na współdziałanie w zakresie zarządzania ryzykiem daje organizacji największe szanse na skuteczne ograniczenie ryzyka.

Rola ubezpieczenia

Prawie dwie trzecie osób ankietowanych przyznaje, że towarzystwa ubezpieczeniowe mogą pomóc organizacjom w zabezpieczeniu się przez cyberzagrożeniami. Spośród organizacji biorących udział w niniejszym badaniu, które deklarują, że w ciągu ostatnich 12 miesięcy miały do czynienia z cyberincydentem, ponad połowa (52%) zwróciła się do ubezpieczyciela o pomoc.

Dział IT jest świadomy potrzeb ubezpieczeniowych

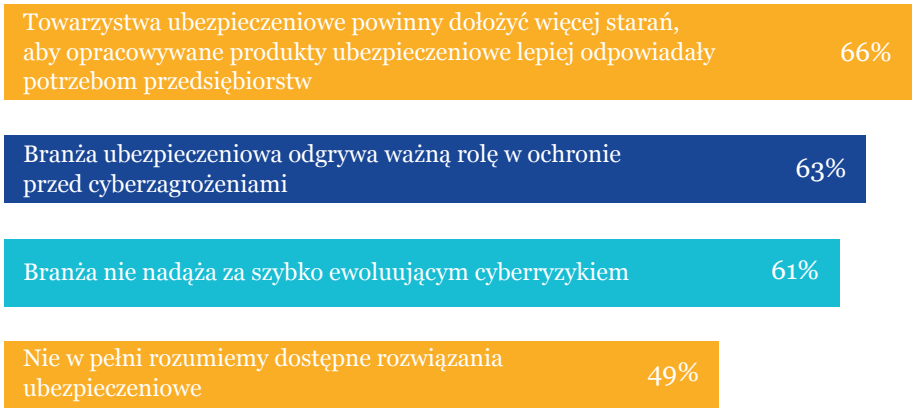
Eksperci ds. IT szczególnie intensywnie forsują wykupienie stosownej ochrony: 67% popiera ubezpieczenie jako ważną formę ochrony, a podobne zdanie ma 60% przedstawicieli działu zarządzania ryzykiem.

Zapewne odzwierciedla to przekonanie osób związanych z IT, że ochrona organizacji w każdej sytuacji jest w zasadzie niemożliwa.

Włamania będą miały miejsce, dlatego warto skorzystać z ochrony ubezpieczeniowej.

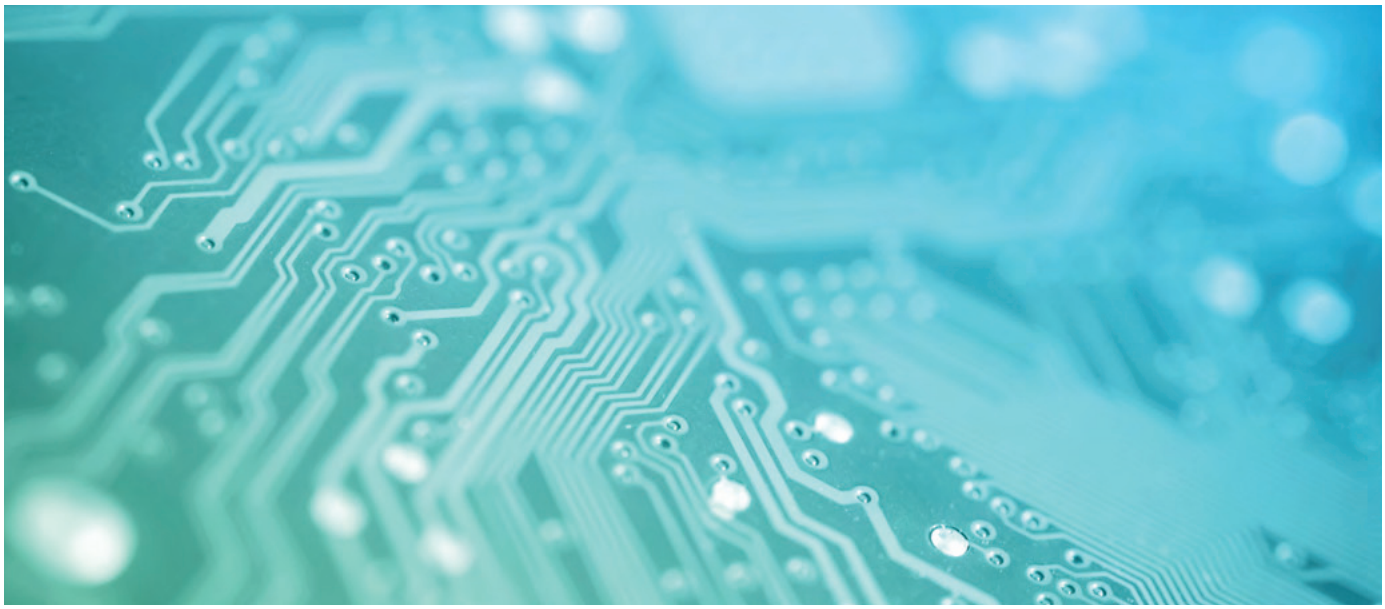
Mniej niż połowa osób ankietowanych deklaruje, że ich organizacje wykupiły ubezpieczenie od cyberzagrożeń i że dostępna oferta powoduje frustrację.

Wykres 12: Stopień, w jakim ankietowani zgadzają się z następującymi stwierdzeniami



Dwie trzecie (66%) uważa, że ubezpieczyciele muszą dołożyć więcej starań, aby ich oferta bardziej odpowiadała potrzebom przedsiębiorstw. 61% twierdzi, że ubezpieczyciele nie nadążają za szybko ewoluującym cyberryzykiem. Mniej osób podziela powyższe opinie w dziale zarządzania ryzykiem, niż w dziale IT. To zapewne odzwierciedla bliższą współpracę tej pierwszej funkcji z towarzystwami ubezpieczeniowymi oraz znajomość branżowych innowacji i świadomość postępów w tym obszarze.

Rynek ubezpieczeniowy szybko ewoluuje, twierdzi Kyle Bryant z Chubb.
– To względnie młody rynek, ale przez ostatnie 10 lat proste polisy ubezpieczeniowe na wypadek włamania i wycieku danych rozszerzyły się o ochronę w przypadku przerwania działalności, utraty i odbudowy danych oraz reagowanie na wymuszenia i żądanie okupu – mówi ekspert. – Rozwój oferty jest bardzo dynamiczny.



„Jako ubezpieczyciel staramy się pomóc ubezpieczonym zrozumieć i ocenić ryzyko oraz zwiększyć bezpieczeństwo. Pomagamy też reagować w przypadku incydentu, który miał już miejsce.”

– Saïd Dami
inżynier ds. ryzyka
w ubezpieczeniach technicznych
na Europę kontynentalną w Chubb

Szeroki zakres wsparcia

W praktyce ubezpieczyciele zapewniają wsparcie na wiele różnych sposobów. Sześciu na dziesięciu ankietowanych chwali ubezpieczycieli za rady i wsparcie merytoryczne udzielone po wystąpieniu incydentu oraz za konsultacje w zakresie najlepszych praktyk, mających na celu zapobiegnięcie incydentom w przyszłości.

Ubezpieczyciele potrafią również trafnie wycenić skutki cyberataków, co jest kwestią drażliwą we wszystkich branżach. 56% ankietowanych deklaruje, że ubezpieczyciele dobrze pomagają im oszacować skutki włamania w wymiarze finansowym. Tyle samo osób uważa, że szkody likwidowane są w sposób uczciwy.

Osoby ankietowane oczekują od ubezpieczycieli usług wysokiej jakości w wielu obszarach. Szybkość, łatwo dostępne usługi reagowania w przypadku wystąpienia incydentu, doradztwo w sprawach regulacyjnych, minimalizacja skutków i porady prawne – wszystkie powyższe elementy większość ankietowanych uważa za istotne.

– Jako ubezpieczyciel nie tylko zapewniamy ubezpieczenie od cyberryzyka – mówi Saïd Dami z Chubb. – Staramy się pomóc zrozumieć i ocenić ryzyko oraz zwiększyć bezpieczeństwo. Pomagamy też reagować w przypadku incydentu, który miał już miejsce.

Wnioski

Pracownicy działów zarządzania ryzykiem i IT obawiają się skali i różnorodności cyberryzyka, ale nie ma zgody co do tego, jak organizacje powinny monitorować zagrożenia, zarządzać nimi i chronić organizację przed ich skutkami.

Niegdyś był to problem przypisany wyłącznie do działu IT organizacji, ale dziś coraz częściej jest postrzegany jako priorytet, omawiany na szczeblu zarządów firm. Działy tak różne od siebie, jak dział zarządzania ryzykiem, prawny i zarządzania zasobami ludzkimi powinny mieć swój udział w reagowaniu na zagrożenia. Mimo coraz większej uwagi przykładanej do tego problemu, wiele organizacji wciąż bezskutecznie stara się stworzyć model zarządzania zapewniający spójną strategię.

Niekorzystna presja z góry

Sześć na dziesięć osób ankietowanych twierdzi, że kadra zarządzająca oczekuje całkowitej odporności firmy na cyberataki. To niepokojące zjawisko w czasach stale ewoluujących zagrożeń, które wywiera silną presję na działy zarządzania ryzykiem i IT, od których oczekuje się stuprocentowej skuteczności w ich eliminowaniu. Ankietowani są jednak zgodni co do tego, że nie są w stanie spełnić tych oczekiwań. 66% przyznaje, że lepiej jest silniej zabezpieczać najważniejsze dane organizacji, niż starać się chronić wszystko równie skutecznie.

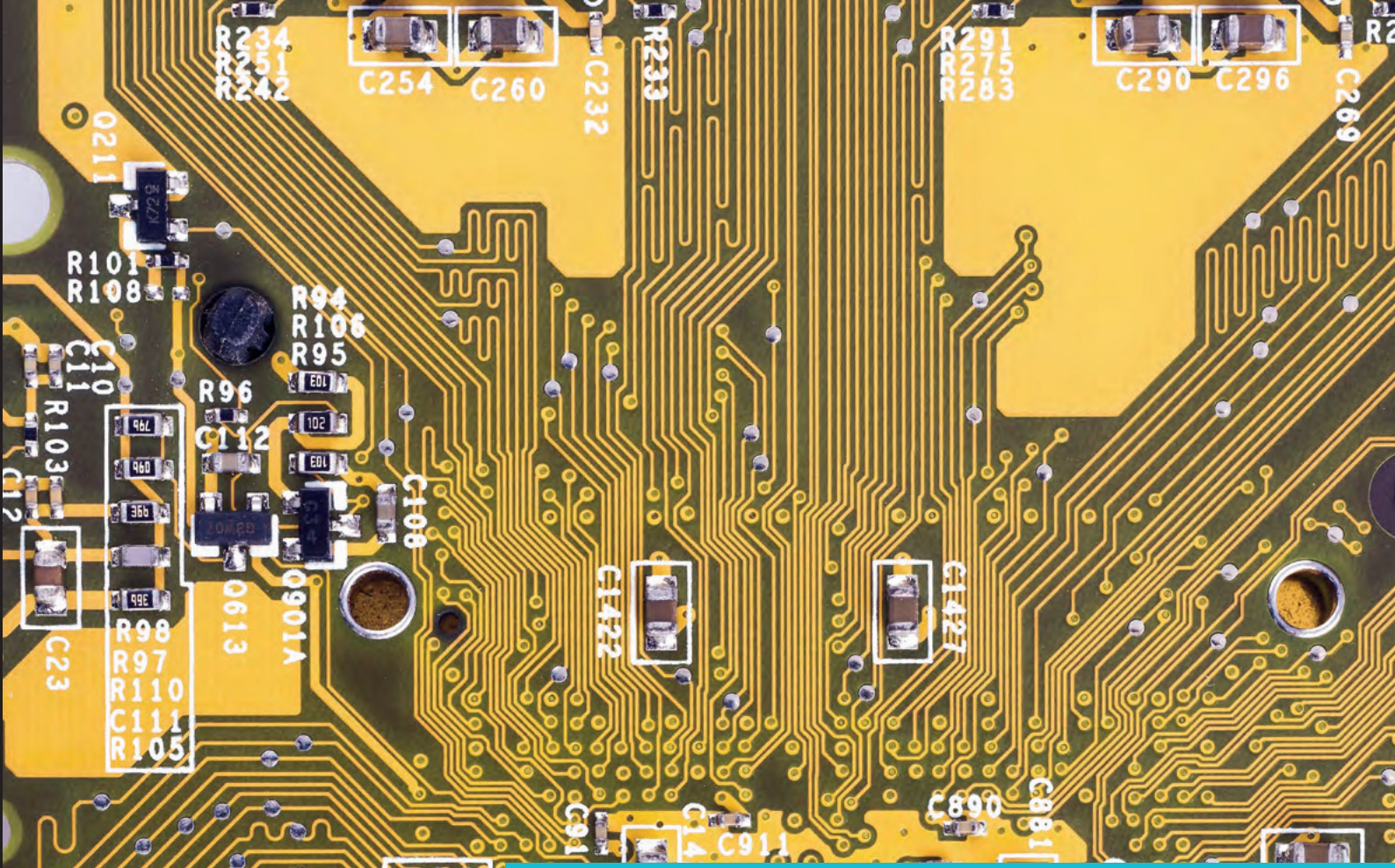
To realistyczne podejście, ale niezależnie od tego osoby zajmujące się cyberzagrożeniami muszą lepiej informować swoich współpracowników (oraz ich przełożonych) o dynamicznie ewoluującym charakterze niebezpieczeństwa. W przeciwnym wypadku będą obwiniani o włamania, gdy te będą miały miejsce. Edukowanie wymaga zacieśnienia współpracy pomiędzy działami IT, zarządzania ryzykiem oraz pozostałymi częściami organizacji.

Ponad czterech na dziesięciu ankietowanych uważa, że to dział techniczny powinien w największym stopniu ponosić odpowiedzialność związaną z cyberryzykiem. Należy jednak ponownie podkreślić, że współpraca jest podstawą – nawet gdy dział IT weźmie na siebie obowiązek opracowania i utrzymania ramowego systemu zarządzania cyberryzykiem w całej organizacji, będzie musiał znacznie ściślej współpracować z pozostałymi częściami organizacji, aby wdrożyć powyższe polityki.

Zaangażowanie podmiotów zewnętrznych

Branża ubezpieczeniowa rozumie, że musi zapewnić znacznie więcej wsparcia organizacjom zmagającym się z cyberzagrożeniami. Powyższe wsparcie obejmuje ochronę ubezpieczeniową, z której organizacje mogłyby skorzystać w przypadku wystąpienia incydentu, ale które jednocześnie obejmuje znacznie więcej różnorodnych usług. Towarzystwa ubezpieczeniowe mogą odegrać kluczową rolę w zacieśnianiu współpracy pomiędzy poszczególnymi funkcjami w organizacji w zakresie identyfikacji, wyceny i profilowania różnego rodzaju cyberryzyka, co pozwoli wzmocnić zabezpieczenia i mechanizmy obronne.

– Nic nie jest w stanie zagwarantować pełnej ochrony przez incydentami – podsumowuje Kyle Bryant. – Ubezpieczenie to dziś użyteczne rozwiązanie, które pomaga identyfikować luki w zabezpieczeniach organizacji, ograniczać skutki zagrożeń i chronić ją przed nimi.



O raporcie

Niniejszy raport został opracowany przez Chubb we współpracy z Longitude Research. Oparto go na wynikach ankiety przeprowadzonej w gronie 257 osób – 103 z działów IT i 154 z działów zarządzania ryzykiem i ubezpieczeń.

Ankietowani pracują w Belgii, Danii, Hiszpanii, Holandii, Niemczech, Norwegii, Szwecji, Wielkiej Brytani, we Francji i Włoszech. Badanie przeprowadzono przez Internet, a za udział w badaniu ankietowanym nie przysługiwało żadne wynagrodzenie. Wszystkie osoby ankietowane są zatrudnione w spółkach, których roczne przychody przekraczają 500 mln dolarów, a przychody 24% z nich przekraczają 5 miliardów dolarów.

Przeprowadziliśmy również wywiady jakościowe z wieloma starszymi ekspertami ds. cyberryzyka z Chubb. Chcielibyśmy podziękować wszystkim zaangażowanym oraz Rogerowi Francisowi, starszemu konsultantowi strategicznemu i kierownikowi ds. ubezpieczeń od cyberzagrożeń w Mandiant, za poświęcenie ich cennego czasu i podzielenie się wartościową wiedzą.

Chubb

The Chubb Building
100 Leadenhall Street
London EC3A 3BP
Wielka Brytania

Tel. +44 (0)20 7173 7000
chubb.com

Chubb. Insured.℠

UK7279-JD 10/17