Cyberbezpieczeństwo i CIO

Cyberbezpieczeństwo jest integralną częścią każdej koncepcji bezpieczeństwa korporacyjnego lub krajowego.

Wprowadzenie

Z czasem zmienia się pozycja najbardziej krytycznej osoby w przedsiębiorstwie. Dzisiaj tą najbardziej krytyczną osobą jest Chief Information Officer (CIO). Na tym samym poziomie, powyżej lub poniżej, lub ta sama osoba jest Dyrektorem ds. Technologii (CTO) i dyrektorem ds. Bezpieczeństwa informacji (CISO) w przedsiębiorstwie. Dla wszystkich praktycznych celów rozważymy CIO jako trzy w jednym. Będąc wszystkimi trzema, oczekuje się, że CIO będzie wizjonerem organizacji, doradzającym w jaki sposób wykorzystać technologię do osiągnięcia celów organizacji. CIO jest odpowiedzialny za każdy aspekt informacji w przedsiębiorstwie.

Rolę CIO w organizacji można opisać następująco:

• Członek wyższego szczebla zespołu administracyjnego / zarządzającego / planowania

• Kierownik technologii i innych zasobów informacyjnych

• Odpowiada za planowanie IT

• Odpowiedzialny za rozwój nowych systemów

• Odpowiada za opracowanie i wdrożenie polityki

Pozycja CIO wymaga pewnego spektrum osobowości, wykształcenia i doświadczenia danej osoby.

Cyberprzestrzeń to labirynt nieskończonych luk w zabezpieczeniach, których istnienie jest zwykle wykrywane przez atakujących kosztem, przynajmniej dla pierwszej ofiary. Rolą CIO jest znajomość wszystkich mechanizmów ochronnych i zdolność do opracowywania większej liczby w razie potrzeby. Można mieć na to nadzieję, jeśli dyrektorzy IT wejdą na swoje stanowisko z dużym doświadczeniem i specjalistyczną wiedzą oraz ze świadomością, że stanowisko CIO jest pracą przez całe życie.

CIO: osobowość

Spotkajmy się z CIO i zobaczmy, jakie kwalifikacje i ścieżka kariery doprowadziły tę osobę na to stanowisko.Oto kwalifikacje osobiste i zawodowe, których CIO musi potrzebować, aby skutecznie sprostać wymaganiom stanowiska.

Zaufanie i etyka

Jedną z najbardziej zaufanych pozycji w dzisiejszym przedsiębiorstwie jest stanowisko CIO. CIO jest ochroniarzem informacji organizacji. CIO musi być pewny siebie i promieniować zaufaniem i sukcesem. Zaufanie to cecha osobista, często wyczuwana podświadomie, która sprawia, że człowiek jest mile widziany w każdym otoczeniu. Szacunek dla siebie, innych, organizacji i społeczeństwa jest fundamentem zaufania. Pewność siebie i promieniowanie sukcesu są osiągane tylko poprzez szereg wcześniejszych sukcesów, małych i prawdopodobnie dużych. Nie ma absolutnie żadnego substytutu dla konsekwentnego zachowania etycznego. Będą istnieć ciągłe naciski lub satysfakcjonujące okazje do bycia nieetycznymi. Jednak CIO musi stać ponad tymi pokusami, nie podejmować ryzyka, a ponadto powstrzymywać chciwość innych, którzy sugerują skróty do prostej linii etyki.

Komunikacja i inteligencja

CIO musi być świetnym komunikatorem w organizacji. Jest to osoba, która będzie musiała przekonać innych do zdobycia zasobów, gdzie słowo zasoby nie pozostawia nic na zewnątrz. Dyrektor IT może potrzebować kapitału na nową technologię lub może potrzebować lojalności i zaufania współpracowników we wszystkich kierunkach hierarchii. Perswazja jest potrzebna do komunikacji w górę, a motywacji i inspiracji do komunikacji w dół. We współczesnej organizacji nic nie osiąga się za pomocą żelaznych pięści. CIO musi uchwycić umysł i serca wszystkich w przedsiębiorstwie, zawsze pamiętając, że język „techniczny" może być nudny dla nietechnicznych. Poza organizacją CIO dołącza do odpowiednich stowarzyszeń, bierze udział w forach, bierze udział w konferencjach i prowadzi seminaria, zyskując w ten sposób widoczność i najważniejsze umiejętności polerowania. Nie możemy wykluczyć natury z obrazu CIO. Naturalna inteligencja jest algorytmem, który przekształca obserwacje w wiedzę, a wiedza w mądrość. Mądrość połączona z doświadczeniem zwykle powoduje zdrowy osąd. Jak mówi przysłowie: mądrzy ludzie uczą się na własnych błędach, podczas gdy mądrzy ludzie uczą się na błędach innych.

Przywództwo i przedsiębiorczość

Niektórzy twierdzą, że rodzi się lider; inni uważają, że można stworzyć lidera. CIO jako lider musi znajdować się powyżej poziomu obserwujących. Ta wyższość, w pełnym tego słowa znaczeniu, musi mieć zarówno cechy osobiste, jak i umiejętności techniczne. CIO jako lider, idący korytarzami przedsiębiorstwa, jak to się mówi, musi być postrzeganym jako przewodnik z boku, a nie jako mędrzec na scenie. Aby otrzymać CIO w ten sposób, osoba ta musi być bardzo pokorna, bardzo kompetentna i doświadczona. Wszyscy w organizacji chcą zobaczyć przyjaciela w osobie CIO. Wynika to z faktu, że CIO jest wspaniałym strażnikiem, obdarzonym autorytetem, który, miejmy nadzieję, pasuje do odpowiedzialności nałożonej na ramiona tej osoby. CIO i kierownictwo przedsiębiorstwa muszą zdać sobie sprawę, że CIO jest strategiczną pozycją, która wyznacza kierunek, a CIO nie powinien być uwikłany w problemy techniczne niskiego poziomu. Jednak CIO musi mieć doświadczenie, aby wskazać kierunek rozwiązania problemów.

Dyrektor ds. Informatyki zawsze szuka okazji do poprawy pozycji biznesowej organizacji, chętny do podjęcia niekatastroficznego ryzyka. Dyrektor ds. Informatyki musi być wizjonerem , który może podważyć konwencjonalną mądrość", w stylu nadzoru, który jest dobrze wyważony między przyznaniem autonomii a stosowaniem kontroli.

Odwaga i ograniczenia

Dyrektorzy IT z powyższymi kwalifikacjami muszą być w stanie przewidzieć wykonalność proponowanego pomysłu i muszą mieć niezbędną odwagę wynikającą z bezpieczeństwa pracy i wsparcia wyższej kadry kierowniczej, aby móc swobodnie i obiektywnie wyrażać swoje opinie. Podobnie CIO powinien być w stanie porzucić projekt, który wydaje się zmierzać w złym kierunku. Przy nieprzewidywalnych postępach technologicznych dobre pomysły mogą nie być tak dobre, ponieważ nowe rozwiązania są stale dostępne. CIO, oprócz rozpoznania ograniczeń technologicznych, powinni przede wszystkim rozpoznać własne ograniczenia, czy to ludzkie, czy techniczne. Sukces CIO jest jak wchodzenie po schodach, trzeba to robić krok po kroku. Tam nie jest to plac zabaw. Bycie CIO jest misją, a nie przyjemnym zajęciem. CIO jest integralną i najbardziej krytyczną częścią przedsiębiorstwa. CIO musi mieć romans z technologią. Miliony inżynierów na całym świecie produkują nowe technologie lub nowe złośliwe oprogramowanie, a CIO nigdy nie może powiedzieć „nie wiem". Dyrektor IT może tylko powiedzieć: „W tej chwili nie wiem, ale za 48 godzin będę miał wyedukowaną opinię na ten temat".

CIO: Edukacja

Stopnie naukowe

CIO musi posiadać wykształcenie wyższe wskazujące na wykształcenie w zakresie systemów informatycznych. Stopień (stopnie) musi zawierać słowo komputer lub informacja, podczas gdy odpowiedni program nauczania musi obejmować kursy, które rozpoczęły się liczbami binarnymi i bramkami logicznymi, a zakończyły kursami zwieńczenia, które rozwinęły się w sieci. Oczekuje się, że dyrektor ds. Informatycznych będzie miał wyższe wykształcenie techniczne. Wiele uniwersytetów oferuje obecnie tytuły MBA w systemach informatycznych, które najlepiej przygotowują kandydatów na stanowisko CIO.

Certyfikaty

Poza oczekiwanym wykształceniem wyższym, CIO musi mieć certyfikaty, które pokazują walutę technologiczną. W zależności od ścieżki kariery, jaką podjął się CIO w zawodzie systemów informatycznych, oczekuje się, że na takie stanowisko będą posiadać aktualne powiązane certyfikaty. Podczas gdy stopnie uniwersyteckie sugerują szeroką wiedzę na dany temat, certyfikacja potwierdza wiedzę specjalistyczną w określonym sektorze technologii.

Ustawiczne kształcenie i nabywanie umiejętności

Korzyści płynące z tworzenia cyberprzestrzeni na świecie mają niespotykane dotąd rozmiary. Wraz z tym pojawiła się straszna zależność. Awarie internetowe przypadkowe lub złośliwe mogą spowodować niezmierzone szkody. W związku z tym przywódcy muszą mieć świadomość tej słodko-gorzkiej sytuacji. Cyberprzestrzeń stała się infrastrukturą, na której praktycznie opiera się każde działanie. Zależność ta waha się od smartfonów po zautomatyzowaną produkcję, z praktycznie każdą aktywnością człowieka pomiędzy. Nasze absolutne poleganie na cyberprzestrzeni wymaga, aby liderzy byli stale edukowani w zakresie postępów i zagrożeń, jakie Internet przynosi światu. Taka edukacja pomoże liderom zidentyfikować i zminimalizować ryzyko cybernetyczne, przygotowując społeczeństwo na nadchodzące wydarzenia , korzyści i obawy. Cyberbezpieczeństwo niewątpliwie przejmie prowadzenie, ale świadomość bezpieczeństwa cybernetycznego dla wszystkich jest niezbędna jako prawo jazdy. Wiele narodów uznało potrzebę edukacji w cyberprzestrzeni, planując odpowiednie programy edukacyjne, koncentrując się na trzech celach . Mianowicie, do

1. Zwiększenie świadomości krajowej na temat zagrożeń związanych z cyberprzestrzenią.

2. Zwiększenie grona specjalistów ds. Bezpieczeństwa cybernetycznego.

3. Utwórz globalnie współpracujące siły cyberbezpieczeństwa.

CIO: Doświadczenie

CIO musiał osiągnąć pozycję w szeregach. Sama edukacja tego nie zrobi. Oznacza to, że dana osoba musiała przez wiele lat służyć w branży IT w znaczący sposób. Być może osoba ta zaczynała jako inżynier projektu lub programista, a następnie została analitykiem, a kilka lat później przełożonym pierwszego stopnia i tak dalej. Równolegle przyszły dyrektor ds. Informatycznych poszerzał wiedzę o powiązanych kursach, seminariach i, miejmy nadzieję, uzyskał po drodze kilka certyfikatów. Mając około dziesięć do piętnastu lat doświadczenia i mając pewność co do już nabytych kwalifikacji w dziedzinie IT, przyszły CIO wkracza na rynek, próbując wody. Reszta to kwestia dopasowania nabytych umiejętności miękkich i twardych do prezentowanych możliwości. Średnio około dwunastu lat od ukończenia college'u może dostać się na stanowisko CIO, w zależności od wielkości organizacji i tego, czy karty doświadczenia i edukacji są właściwie grane. Podczas planowania kariery przyszły CIO musi pamiętać, że „rekruterzy szukają sprawdzonych historii sukcesu, a nie ludzi, którzy mogą odnieść sukces”

CIO: Obowiązki

Z czasem IT ewoluowało jako integralny i niezbędny uczestnik każdej organizacji, a potrzeba centralnej postaci, CIO, stała się oczywista. W 1996 r. osiągnął punkt, w którym w Stanach Zjednoczonych uchwalono ustawę federalną, która obejmowała nawet obowiązki CIO w różnych departamentach rządu. Określanie priorytetów jest trudne. Oczywiste jest, że obowiązki CIO obejmują całe spektrum systemów informatycznych w organizacji. W efekcie CIO jest ministrem obrony organizacji. Inne obowiązki, które nie zostały wyraźnie określone w powyższym akcie, obejmują:

*Nabycie

*Zarządzanie wydajnością i wynikami

*Architektura

*Polityka

*Ciągłości działania

*Udoskonalenie procesu

*Planowanie i inwestowanie kapitału

*Zarządzanie programem

*Relacje z klientem

*Zarządzanie ryzykiem

*Bezpieczeństwo innowacji

*Zarządzanie przywództwem

*Planowanie strategiczne

*Ocena technologii operacyjnej

Kopia zapasowa i archiwizacja danych

Dyrektor ds. Informatyki musi zaprojektować wdrożenie planów sporządzonych przez administratora danych organizacji w celu tworzenia kopii zapasowych danych operacyjnych w czasie rzeczywistym. Dzięki wprowadzeniu chmury jako możliwego miejsca docelowego kopii zapasowej, należy uwzględnić dodatkowe obawy dotyczące bezpieczeństwa z powodu niejasności co do dokładnej fizycznej lokalizacji danych.

Kultura bezpieczeństwa

Dyrektorzy IT jako dyrektorzy ds. Bezpieczeństwa informacji w organizacji ponoszą odpowiedzialność za stworzenie korporacyjnej kultury bezpieczeństwa, która posłuży jako podświadomy przewodnik w działaniach wszystkich. Podstawowymi elementami kultury bezpieczeństwa są z jednej strony świadomość istnienia zagrożeń i ich potencjalnej szkody dla organizacji, z drugiej zaś przestrzeganie zasad bezpieczeństwa. Tworzenie kultury bezpieczeństwa nie jest łatwe, ponieważ stwarza wiele niedogodności. Jednak dzięki programom szkoleniowym zrozumiałe będzie, że środki bezpieczeństwa są bardzo niską ceną, jaką należy zapłacić za to, że nie doszło do incydentów bezpieczeństwa o potencjalnie katastrofalnych skutkach. Podczas gdy faktyczny personel bezpieczeństwa CIO może być niewielki, wirtualny personel powinien obejmować każdego członka organizacji.

Szkolenie cybernetyczne

Biorąc pod uwagę, że technologia nieustannie się rozwija, szkolenie personelu IT organizacji będzie musiało być ciągłe. Dyrektor ds. Informatycznych musi mieć ścieżkę kariery dla każdego członka działu IT, a szkolenie przyczyni się do realizacji ścieżki kariery na żywo. Szkolenie może odbywać się wewnętrznie, zewnętrznie, osobiście lub online. Certyfikaty muszą stanowić integralną część filozofii szkolenia organizacji, a także szkolenia sprzedawców, tam gdzie ma to zastosowanie.

Plany awaryjne

Dyrektor ds. Informatycznych, we współpracy z kierownikami działów organizacji, opracowuje plany awaryjne na wypadek możliwie największej liczby niepożądanych zdarzeń. Dyrektor ds. Informatycznych przeszedł przez szeregi toru operacyjnego organizacji i może błędnie sądzić, że pozycja jest nadal na poziomie operacyjnym. To bardzo źle i niestety wielu CIO gubi się w szczegółach technicznych. Pozycja CIO to pozycja strategiczna, a CIO musi być wolny od kapelusza operacyjnego CIO. Aby to osiągnąć, CIO muszą się „sklonować". Oznacza to, że podobnie jak na statkach, na których pierwszy oficer prowadzi statek, a nie kapitan, CIO musi mieć pierwszego oficera, który zajmie się wszystkimi operacyjnymi aspektami informatycznymi organizacji. W ten sposób CIO będzie mógł skoncentrować się na roli strategicznej - śledzić postęp technologiczny, zabezpieczyć zasoby na potrzeby IT organizacji i upewnić się, że morale i zaufanie do kadry IT są wysokie.

Odpowiedzialność

Często zdarza się, że CIO mają ubezpieczenie od odpowiedzialności cywilnej, szczególnie jeśli pracują jako niezależni konsultanci. Istnieje wiele firm, które oferują taki zakres, często obejmujący zakres 5 mln USD

CIO: Bezpieczeństwo informacji

Istnieje wiele elementów bezpieczeństwa informacji. Najważniejsze, sklasyfikujemy jako wewnętrzne i zewnętrzne.

Wewnętrzne składniki bezpieczeństwa informacji

Kontrola dostępu - elektroniczna .Tutaj mamy trzy pytania: Kto? Co? W jaki sposób? Czasami dodaje się jeszcze jedno pytanie: Kiedy? Dzisiejsze systemy baz danych umożliwiają kontrolę dostępu aż do komórki arkusza kalkulacyjnego. Programowanie bezpieczeństwa do tego poziomu może być uciążliwe, ale są to opcje oferowane przez technologię i powinny być ważone względem znaczenia chronionych danych. Dostęp do danych można również blokować czasowo. Dane mogą być dostępne w godzinach pracy lub po konkretnym włączeniu. Ponieważ biometria wciąż nie jest głównym narzędziem kontroli dostępu, nazwa użytkownika i hasła pozostają dominującymi mechanizmami kontroli dostępu. Lukę w zabezpieczeniach hasłem można wyeliminować za pomocą uwierzytelniania dwuskładnikowego. Jest to technologia, w której po wprowadzeniu nazwy użytkownika serwer wysyła użytkownikowi jednorazowe hasło (OTP) za pośrednictwem względnie bezpiecznego medium, takiego jak e-mail lub SMS na telefon komórkowy użytkownika. Drugim czynnikiem uwierzytelnienia może być jedna z kilku opcji oprócz wyżej wymienionych. Może to być parametr biometryczny - odcisk palca lub próbka głosu - lub może to być urządzenie - bezprzewodowe lub USB - które za pośrednictwem komputera logowania wysyła do serwera rozpoznawalny i możliwy do zidentyfikowania kod.

Kontrola dostępu – fizyczna. W przedsiębiorstwie często ma to miejsce ,że dostęp jest przyznawany dla określonych obszarów obiektów. W takich przypadkach zamki szyfrowe lub urządzenia przesuwające karty umożliwiają autoryzowany dostęp. W pierwszym przypadku wadą jest możliwa

utrata lub kompromis kodu dostępu, podczas gdy w drugim przypadku wadą jest możliwa utrata samej karty. Praktycznym rozwiązaniem fizycznego dostępu mogą być mobilne blokady telefoniczne, w których tylko autoryzowane numery telefonów mogą odblokowywać i zapewniać dostęp. Takie technologie rejestrują także znacznik czasu interakcji i zapisują wszystkie nieautoryzowane próby wejścia.

Zasady cybernetyczne

Jednym z głównych obowiązków CIO jest opracowanie polityki bezpieczeństwa informacji organizacji. Ta polityka wyszczególnia reguły, na podstawie których informacje przemieszczają się w obrębie organizacji i od organizacji do innych zewnętrznych.

Cyber świadomość i szkolenie

Cyber świadomość „chroni cię dane osobowe ... i ... bezpieczeństwo twojego komputera ” . CIO promuje świadomość cyberbezpieczeństwa poprzez komunikację wewnętrzną, taką jak okazjonalne biuletyny e-mail i seminaria, podkreślając, że cyberbezpieczeństwo jest zbiorowym zadaniem i misją wewnątrz organizacji.

Cyber świadomość może być określona ilościowo za pomocą następującej listy porad:

• Zawsze miej zainstalowane niezawodne i samoaktualizujące się oprogramowanie antywirusowe.

• Zawsze używaj najnowszych wersji potrzebnego oprogramowania, w tym zainstalowanego systemu operacyjnego.

• Zainstaluj łatki, gdy tylko zostaną udostępnione.

• W środowisku Wi-Fi wyłącz transmisję SSID i zastosuj szyfrowanie WAP / WEP. Tam, gdzie to możliwe, zaprogramuj punkt dostępu do MAC dozwolonych komputerów.

• W sieciach społecznościowych zapoznaj się ze wszystkimi środkami bezpieczeństwa i ochrony prywatności i zastosuj je w celu zapewnienia maksymalnej ochrony. Nie publikuj poufnych informacji i niekompletnych zdjęć.

• Wysyłając poufne informacje, zaszyfruj je i wyślij odbiorcy hasło za pośrednictwem wspólnie uzgodnionego nośnika, takiego jak SMS, e-mail lub telefon.

• Przejrzyj opcje plików cookie w przeglądarce i wybierz tę, która będzie Ci odpowiadać w zależności od potrzeb związanych z surfowaniem. Co więcej, zaprogramuj przeglądarkę, aby wyświetlała monity przed zaakceptowaniem plików cookie.

• Zaprogramuj swoją przeglądarkę, aby automatycznie wyłączała się po X minutach bezczynności i aby usuwać tymczasowe pliki internetowe oraz ewentualnie historię i pliki cookie, jeśli to konieczne.

Trening

Szkolenia dotyczące świadomości cybernetycznej można znaleźć bezpłatnie i może zawierać następujące części:

-Wprowadzenie do Cyber Safety, obejmujące ustawienia bezpieczeństwa na komputerze osobistym i telefonie komórkowym, ustawienia ochrony przeglądarki, szyfrowanie dokumentów i wybór hasła.

-Ataki złośliwego oprogramowania, obejmujące wirusy i sposób, w jaki infekują komputery i urządzenia mobilne oraz ochronę poprzez odpowiednie ustawienia i przy użyciu oprogramowania antywirusowego.

-Ataki z wyższej półki, obejmujące rozproszone ataki typu „odmowa usługi” oraz środki ochronne.

-Cyberprzestępczość, obejmująca różne systemy przestępczości w cyberprzestrzeni oraz sposoby ich rozpoznania.

-Netykieta, obejmująca społecznie i profesjonalnie przyjętą etykietę w interakcjach przez Internet. Obejmie to czat, posty w serwisach społecznościowych i e-maile.

Ciągłości działania

CIO jest odpowiedzialny za opracowanie Planu ciągłości działania, który posiada wiedzę i aprobatę kierownictwa wyższego szczebla organizacji. Plan obejmuje „zapobieganie, łagodzenie, przygotowanie, reakcja i odzyskiwanie [z normalnych działań organizacji] z sytuacji awaryjnych ”. Szczegółowe standardy bezpieczeństwa informacji są określone w różnych opublikowanych standardach. Aby skutecznie zająć się sytuacją kryzysową, która spowoduje brak ciągłości w normalnych działaniach organizacji, dyrektor ds. Informatycznych musi wykonać co najmniej następujące dwa zadania:

1. Analiza przyczynowo-skutkowa nieciągłości biznesowej. Jest to badanie, które ocenia konsekwencje możliwej niekorzystnej sytuacji, która zmusi organizację do przerwania dostawy oczekiwanych produktów lub usług. W kontekście systemów informacyjnych niekorzystne sytuacje mogą być związane z operacjami wewnątrzorganizacyjnymi lub współpracą międzyorganizacyjną. Jak na przykład,

a. Front Office. Serwer witryny został zamknięty, a przyczyną może być niedostateczna zdolność do obsługi legalnych zadań, atak typu „odmowa usługi”, atak złośliwego oprogramowania, klęska żywiołowa lub problem personelu.

b. Zaplecze biurowe. Awaria magazynu lub obliczenia bazy danych, gdzie podobnie przyczyną może być niedostateczna pojemność, złośliwe oprogramowanie, błąd niezwiązany ze złośliwym oprogramowaniem, atak złośliwego oprogramowania, katastrofa naturalna lub problem personelu.

c. Awaria w zależności. Organizacja dodaje wartość do określonego produktu lub usługi, a dostawca zawiódł. Na przykład organizacja świadcząca usługi edukacyjne online korzysta z dzierżawionej platformy, na której występują problemy operacyjne.

d. Brak zgodności. Działania organizacji są zawieszane do momentu osiągnięcia zgodności. Straty niektórych danych mogą wymagać powiadomienia organów rządowych przed wznowieniem działalności.

Dyrektor ds. IT przeprowadza analizę dotyczącą powyższych możliwych przyczyn nieciągłości biznesowej i wiele innych, a także opracowuje Plan naprawy gospodarczej.

2. Plan naprawy gospodarczej. Jest to plan opracowany przez biuro CIO, przyjęty przez kierownictwo wyższego szczebla organizacji i gotowy do wdrożenia w razie nagłej potrzeby. Plan określa, z imienia i nazwiska lub stanowiska, osobę, która będzie kierować procesem odzyskiwania działalności, obowiązki i władzę tej osoby, a także linię dowodzenia, której należy przestrzegać, dopóki organizacja nie wyjdzie ze stanu wyjątkowego.

CIO: Zmiana roli

W miarę, jak technologia staje się coraz bardziej kluczowym kamieniem węgielnym każdej organizacji, rola CIO zmienia się „Od Stewarda technologicznego do lidera biznesu ... W tym nowym świecie transformacji opartej na technologii… CIO odgrywają coraz większą rolę”. Misją CIO nie jest już nadzorowanie codziennych działań działu przetwarzania danych, ale pomoc liderom organizacji w

wykorzystaniu informacji i technologii w celu zwiększenia wartości produkowanej i dostarczanej usługi interesariuszom. Prawdziwą miarą sukcesu organizacji jest korzyść oferowana interesariuszom w stosunku do dostępnych zasobów. Obecnie praktycznie każda organizacja wykorzystuje informacje, aby zmaksymalizować tę korzyść. Celem jest zwiększenie produktywności oferowanych produktów lub usług dla użytkownika, bardziej reagujący na potrzeby rynku, a przede wszystkim dostępne dla rynków docelowych. CIO jest rewolucyjną wizją transformacji, która chce, aby organizacja wykorzystała postęp technologiczny, aby osiągnąć nowy poziom osiągnięć. Mogą być mierzalne pod względem wydajności, świadczonych usług lub zysków. W tym zadaniu CIO znajdzie technologię jako wiernego sojusznika, a kulturę organizacyjną i biurokrację jako stałego przeciwnika. Aby jak najlepiej służyć ich organizacjom, CIO muszą uzyskać niezbędne uprawnienia zasoby, widoczność i uczestnictwo, aby nie byli narażeni problemy organizacyjne i obawy w celu przedstawienia rekomendacji opartych na technologii. Z czasem odizolowany kierownik działu IT został podniesiony z maszynowni i stał się centralną postacią w C-Suite noszącą tytuł CIO. Ponieważ technologia jest obecnie podstawą większości działań biznesowych, oczekuje się, że CIO musi „... być dobrym konsultantem biznesowym dla CEO, COO, a nawet CFO."

Zwiększanie wartości biznesowej dzięki Cyberbezpieczeństwu

Wartość większości produktów lub usług często obejmuje pewne wspólne elementy, które czynią je atrakcyjnymi. W cyberprzestrzeni tymi komponentami są prywatność, bezpieczeństwo i ochrona, zbiorowo oznaczające cyberbezpieczeństwo. Dlatego obecność cyberbezpieczeństwa dodaje wartości, a jej brak zmniejsza wartość. Im więcej „inteligentnych" produktów i usług, tym wyższe oczekiwania dotyczące cyberbezpieczeństwa. W przeszłości edukacja bez umiejętności obsługi komputera była uważana za niedostateczną. Dzisiaj umiejętności komputerowe są uważane za coś oczywistego, a edukacja bez umiejętności w zakresie cyberbezpieczeństwa jest niewystarczająca, jeśli nie niebezpieczna. Ponieważ każdy aspekt życia stara się czerpać korzyści z cyberprzestrzeni, cyberprzestępczość jedzie jak pasożyt żyjący ze zdrowych organizmów. Ponieważ wartość funkcjonalna jest wbudowywana w produkt lub usługę w fazie projektowania, podobnie cyberbezpieczeństwo musi być w niej osadzone.