WYKORZYSTANIE PSYCHOLOGII SPOŁECZNEJ DO REALIZACJI POLITYKI BEZPIECZEŃSTWA

WSTĘP

Większość pracowników ochrony współczuła kolegom z powodu trudności w nakłonieniu ludzi do zwracania uwagi na zasady bezpieczeństwa — do przestrzegania tego, co wydaje się zdrowym rozsądkiem. Kręcą głowami z niedowierzaniem, opowiadając historie o pracownikach, którzy otwierają zabezpieczone drzwi dla swoich współpracowników — lub dla zupełnie obcych osób, przez co systemy dostępu za miliony dolarów stają się bezużyteczne. W dużych organizacjach kierownicy wyższego szczebla, którzy odmawiają noszenia identyfikatorów, odkrywają, że wkrótce nikt inny też nie będzie ich nosił. Próbując wdrożyć politykę bezpieczeństwa, praktycy czasami czują, że są zaangażowani w wojny o wpływy i osobiste zemsty, a nie w racjonalny dyskurs. Problemy te odzwierciedlają społeczną naturę istot ludzkich; odzwierciedlają one jednak również fakt, że chociaż osoby zajmujące się bezpieczeństwem systemów informatycznych i zarządzaniem siecią mają różne doświadczenia, wielu z nich nie jest przeszkolonych w zakresie psychologii społecznej lub organizacyjnej. Zasady i procedury bezpieczeństwa wpływają nie tylko na to, co ludzie robią, ale także na to, jak postrzegają siebie, swoich współpracowników i swój świat. Pomimo tych problemów psychospołecznych personel ochrony zwraca niewielką lub żadną uwagę na to, co wiadomo na temat psychologii społecznej. Ustalone zasady ludzkiego zachowania społecznego mogą wiele nauczyć w przypadku wszelkich prób poprawy zapewniania informacji przez przedsiębiorstwa i instytucje (IA). Specjaliści IA są zgodni, że bezpieczeństwo zależy bardziej od ludzi niż od technologii. Innym powszechnym zjawiskiem jest to, że pracownicy są znacznie większym zagrożeniem dla IA niż osoby z zewnątrz. Z obserwacji tych wynika, że poprawa bezpieczeństwa nieuchronnie pociąga za sobą zmianę przekonań, postaw i zachowań, zarówno jednostek, jak i grup. Psychologia społeczna może pomóc nam zrozumieć, jak najlepiej pracować z ludzkimi upodobaniami i predyspozycjami, aby osiągnąć nasze cele poprawy bezpieczeństwa:

* Badania nad poznaniem społecznym dotyczą sposobu, w jaki ludzie tworzą wrażenia na temat rzeczywistości. Znając te zasady, możemy lepiej uczyć naszych współpracowników i klientów o skutecznym bezpieczeństwie.

* Praca nad kształtowaniem postaw i przekonań pomaga skutecznie prezentować informacje, a tym samym przekonać pracowników i inne osoby do współpracy na rzecz poprawy bezpieczeństwa.

* Naukowcy badający perswazję i zmianę postaw nauczyli się, jak najlepiej wpływać na umysły ludzi w przypadku niepopularnych poglądów, takich jak te dotyczące społeczności zajmującej się bezpieczeństwem.

* Badania czynników wzmacniających zachowania prospołeczne dostarczają wglądu w to, jak wspierać środowisko, w którym informacje korporacyjne są dobrowolnie chronione.

* Znajomość zjawisk leżących u podstaw konformizmu, podporządkowania się i posłuszeństwa może pomóc w zwiększeniu bezpieczeństwa poprzez zachęcanie do podporządkowania się i ochronę personelu przed presją społeczną, by naruszać zabezpieczenia.

* Badania z zakresu psychologii grup dostarczają ostrzeżeń przed patologią grupową i wskazówek dotyczących lepszej pracy z grupami w ustanawianiu i utrzymywaniu IA w obliczu zakorzenionego oporu.

W tej części dokonano przeglądu dobrze ugruntowanych zasad psychologii społecznej, które pomagają personelowi zajmującemu się bezpieczeństwem i zarządzaniem siecią efektywniej wdrażać polityki bezpieczeństwa. Każdy nowy podręcznik wprowadzający do college'u psychologii społecznej zawiera obszerne odniesienia do badań leżących u podstaw zastosowanych tutaj zasad wdrażania polityki bezpieczeństwa.

RACJONALNOŚĆ NIE WYSTARCZY

Polityki OW czasami budzą silne emocje. Ludzie mogą się bardzo złościć z powodu tego, co postrzegają jako ingerencję w ich sposób wykonywania pracy. Z perspektywy tradycyjnego specjalisty ds. bezpieczeństwa informacji, bezpieczeństwo informacji jest nadal postrzegane jako problem techniczny, ale jak pokazują ostatnie badania, jest to raczej problem zarządzania, a dominująca kultura bezpieczeństwa zapewnia wgląd w to, jak kierownictwo radzi sobie z tym problemem. Aby umieścić dyskusję w kontekście, oto definicja racjonalności autorstwa szanowanego naukowca, Jonathana Barona: Racjonalność to „rodzaj myślenia, który wszyscy byśmy chcieli, gdybyśmy byli świadomi własnego najlepszego interesu, aby osiągnąć nasze cele." Zastosowanie tej definicji do pojęcia bezpieczeństwa wydaje się sugerować, że racjonalne myślenie nakieruje nas na to, co wydaje się najlepszym kompromisem między tym, co postrzegamy jako nasze potrzeby bezpieczeństwa, a tym, co wydaje się najwygodniejszym procesem.

Schemat

Psychologowie używają słowa schemat, aby podsumować złożony obraz rzeczywistości, na którym opieramy nasze sądy. Schemat jest tym, co psychologowie społeczni nazywają sposobem, w jaki ludzie nadają sens swoim interakcjom społecznym. Praktycy IA muszą często zmieniać schematy swoich kolegów. Schematy to samospójne poglądy na rzeczywistość. Pomagają nam zwracać uwagę na to, co wydaje nam się ważne, i ignorować nieistotne dane. Pomagają nam również uporządkować nasze zachowanie. Na przykład nasz schemat relacji w biurze obejmuje uprzejme powitania, uprzejme dyskusje, komunikację pisemną i strój biznesowy. Schemat wyklucza nieprzyzwoite wrzaski, obelżywe ataki słowne, graffiti malowane sprayem i kolegów ubranych w kostiumy kąpielowe. Jest to schemat, dzięki któremu ludzie wiedzą, co jest właściwe, a co niewłaściwe w danej sytuacji. Niestety zasady i procedury bezpieczeństwa są sprzeczne ze schematami większości ludzi. Schematy pracowników biurowych obejmują dzielenie się materiałami biurowymi („Pożycz mi swój zszywacz, proszę?”), zaufanie członków zespołu do dzielenia się informacjami („Spójrz na te liczby, Sally”) oraz pozwalanie, by ich dokumenty były widoczne, gdy wychodzą ich biurka. Udostępnianie identyfikatorów użytkowników, pokazywanie poufnych informacji osobie nieposiadającej odpowiednich uprawnień oraz pozostawianie zalogowanych stacji roboczych bez ochrony to rażące naruszenia innego schematu — schematu specjalisty ds. IA. Pomyśl o kontroli dostępu: normalna uprzejmość nakazuje, że gdy kolega zbliża się do drzwi, które właśnie otworzyliśmy, przytrzymujemy drzwi otwarte dla tej osoby; kiedy widzimy gościa, uśmiechamy się uprzejmie — w końcu może to być klient. W przeciwieństwie do tego, zasady kontroli dostępu wymagają, abyśmy nie pozwolili nawet lubianym współpracownikom przejść przez system kart dostępu; zasady bezpieczeństwa nalegają, aby nieoznakowane nieznajome były kwestionowane lub zgłaszane personelowi ochrony. Zdrowy rozsądek podpowiada nam, że kiedy dyrektor naczelny (CEO) firmy czegoś chce, nie sprzeciwiamy się temu; jednak dobra IA nakazuje szkolić operatorów sal komputerowych, aby zabraniali wstępu komukolwiek bez udokumentowanego upoważnienia - w tym dyrektorowi generalnemu. Czasami ludzie podważają IA poprzez systematyczne obchodzenie zasad, ponieważ ich normalny schemat społeczny zastępuje schemat bezpieczeństwa. Nierzadko zdarza się, że naiwny personel przekazuje klucze lub kombinację zamka drzwi w celu uzyskania dostępu do zabezpieczonych obszarów, aby regularnie wyznaczać zewnętrznych dostawców i konserwatorów. Tacy dostawcy rzadko poddawani są kontrolom bezpieczeństwa, a mimo to istnieje

duże prawdopodobieństwo celowego lub nieumyślnego wyrządzenia szkody; niemniej jednak naiwni pracownicy działają bez upoważnienia, podważając normalne kontrole bezpieczeństwa i powierzając bezpieczeństwo i ochronę zasobów korporacyjnych relatywnie nieznanym: Dlaczego? Czy celowo naruszają zasady bezpieczeństwa ze złymi zamiarami? Oczywiście, że nie: pracownicy po prostu zachowują się przyjaźnie i okazują zaufanie, które może być właściwe w innych okolicznościach, ale używają niewłaściwego schematu dla środowiska korporacyjnego o wysokim poziomie bezpieczeństwa. Natomiast schemat specjalisty ds. IA w tych samych okolicznościach obejmuje wszystkich potencjalnie niegodnych zaufania przyjaciół tych outsiderów. Dopóki grupa zarządzająca bezpieczeństwem nie zmieni postrzegania przez pracowników stosowności przepisów bezpieczeństwa, konflikt między różnymi schematami będzie nadal powodował naruszenia bezpieczeństwa i podsycał niechęć wszystkich stron. Rzeczywiście, wspólna reakcja na próby egzekwowania istniejących polityk i procedur, lub do nowych zasad bezpieczeństwa, to zarzut paranoi skierowany przeciwko personelowi ochrony. Inne zarzuty obejmują autorytarne zachowanie i nieuzasadnioną ingerencję w funkcje zawodowe. Odpowiedzi te zwykle wskazują na konflikt między przyjętymi normami zachowania a potrzebą zmiany zachowania w celu dostosowania go do zasad bezpieczeństwa. Sugerują one, że przy opracowywaniu zasad nie uwzględniono potrzeb i zachowań społecznych i kulturowych. Wskazują również na potrzebę zrozumienia przez pracowników ochrony, że podstawowe łaski społeczne i przyjęte normy współżycia społecznego stoją w sprzeczności z podstawowymi potrzebami bezpieczeństwa, a pracownicy naruszający zasady bezpieczeństwa nie są z natury ludźmi złymi. Pewne przeprojektowanie może pozwolić na lepsze bezpieczeństwo, uznając, że zasady bezpieczeństwa mogą naruszać przyjęte normy społeczne. Na przykład w przypadku drzwi z zabezpieczeniem można zezwolić na względnie swobodny dostęp do wspólnych obszarów (umożliwiając w ten sposób przytrzymanie drzwi kolegom, którzy za nimi podążają), jednocześnie zabraniając takich działań w miejscach zabezpieczonych. Opublikowane wyjaśnienie zarówno przyczyn, jak i konsekwencji polityki, wyraźnie odnoszące się do różnicy między potrzebami zwykłej uprzejmości a potrzebami wysokiego bezpieczeństwa, może prowadzić do lepszego przestrzegania określonych zasad. Tekst mógłby brzmieć mniej więcej tak:

Jest to obszar o wysokim poziomie bezpieczeństwa. Uniemożliwianie komukolwiek wejścia bez przesuwania posiadanej karty dostępu nie jest niegrzeczne: to zdrowy rozsądek. Wchodzenie do obszarów chronionych bez użycia karty dostępu każdego pracownika może narazić pracowników, którzy nie używali swoich kart dostępu, na ryzyko wejścia w sytuacji awaryjnej, jeśli pracownicy ochrony nie będą wiedzieli, że nadal znajdują się w obszarach zabezpieczonych. Możesz zachować normalną uprzejmość, przytrzymując drzwi otwarte dla swoich kolegów i gości noszących identyfikatory w obszarach niezabezpieczonych.

Jeśli będziemy upierać się przy założeniu, że możemy wpłynąć na naszych kolegów, aby zmienili ich postrzeganie IA wyłącznie poprzez informowanie ich, pochlebianie, dokuczanie lub zastraszanie ich, nadal ponosimy porażkę. IA musi zostać włączona do kultury korporacyjnej poprzez zmianę schematów naszych kolegów, proces, który wymaga wykorzystania wszystkich technik, których może nas nauczyć psychologia społeczna. Prostą miarą tej rzeczywistości jest uporczywe unikanie praktykowane przez wiele agencji rządowych USA przy stosowaniu wymagań programu bezpieczeństwa informacji Federalnej ustawy o zarządzaniu bezpieczeństwem informacji z 2002 r. (FISMA). Minęło prawie pięć lat i seria niepożądanych incydentów związanych z bezpieczeństwem, zanim różne agencje uświadomiły sobie realną potrzebę wdrożenia odpowiedniej ochrony. Inną ilustracją niechęci do wdrażania zasad bezpieczeństwa jest klęska Veterans Affairs pod koniec 2000 roku, polegająca na utracie kontroli nad danymi osobowymi na niezaszyfrowanych dyskach

Teorie osobowości. Jedną z najbardziej rozpowszechnionych przeszkód we współpracy w organizacjach są konflikty międzyludzkie. Wiele konfliktów ma swoje korzenie w różnicach w stylu osobowości. Na przykład jeden powszechnie używany zestaw kategorii do opisywania osobowości ludzi wykorzystuje ten schemat:

* Ekstrawersja

* Wysoki: aktywny, asertywny, energiczny, towarzyski, rozmowny

* Niski: cichy, powściągliwy, nieśmiały, cichy, wycofany

* Ugodowość

* Wysoki: czuły, wdzięczny, miły, o miękkim sercu, współczujący

* Niski: zimny, krytykujący, nieczuły, kłótliwy, nieprzyjazny

* Sumienność

* Wysoka: wydajna, zorganizowana, planowa, odpowiedzialna, dokładna

* Niski: nieostrożny, nieporządny, niepoważny, nieodpowiedzialny, niechlujny

* Stabilność emocjonalna

* Wysoka: spokojna, zadowolona, stabilna, pozbawiona emocji

* Niski: niespokojny, nastrojowy, nerwowy, spięty, zmartwiony

* Otwartość lub kultura

* Wysoka: pomysłowość, wnikliwość, inteligencja, oryginalność, szerokie zainteresowania

* Niski: pospolity, płytki, prosty, o wąskich zainteresowaniach, nieinteligentny

Przymiotniki użyte w tym podsumowaniu są pozytywne dla wysokiej strony każdej cechy i negatywne dla niskiej strony. Jednak założenie, że różne typy osobowości można łatwo scharakteryzować jako lepsze i gorsze, poważnie przeszkadza w pełnej szacunku komunikacji między współpracownikami. Na przykład osoby o niskich parametrach mogą przeglądać poprzednie podsumowanie w następujący sposób:

* Ekstrawersja

* Wysoki: nerwowy, agresywny, pobudliwy, natarczywy, gadatliwy

* Niski: dostojny, pełen szacunku, skromny, uważny, samowystarczalny

* Ugodowość

* Wysoki: przylegający, tryskający, miękki, reagujący odruchowo, bezkrytyczny

* Niski: dostojny, analityczny, racjonalny, pryncypialny, powściągliwy

* Sumienność

* Wysoki: obsesyjny, kompulsywny, niespontaniczny, pompatyczny, niewolniczy

* Niski: wolny, spontaniczny, kreatywny, zabawny, młodzieńczy, mający perspektywę

* Stabilność emocjonalna

* Wysoki: zamrożony, bez ambicji, nudny, martwy

* Niski: żywy, romantyczny, żywy, silny, rozsądny

* Otwartość lub kultura

* Wysoka: łuszcząca się, teoretyczna, skomplikowana, nieszablonowa, dyletantka

* Niski: ziemisty, inteligentny, uziemiony, skoncentrowany, praktyczny

Omawiając zmianę kultury korporacyjnej, liderzy muszą mieć się na baczności, aby rozładować konflikty oparte na błędnym przekonaniu, że jedna konkretna reakcja lub pogląd na daną kwestię jest z konieczności dobry, a inny z konieczności zły. Konflikt może być zakorzeniony w stylach osobowości, a nie w problemach ze zrozumieniem. Jeśli grupa robocza ds. bezpieczeństwa zaproponuje, aby wszyscy pracownicy rzucili wyzwanie każdemu, kto nie nosi odznaki w chronionych obszarach, niektórzy ludzie - na przykład ci, którzy mają niską ekstrawersję - mogą mieć duże trudności z koncepcją, że powinni powiedzieć komukolwiek inaczej, co robić, zwłaszcza menedżera wyższej rangi niż ich własna. Spieranie się tylko o powody, dla których taka polityka byłaby użyteczna, pozwoliłoby ominąć podstawowy problem: wymagane zachowanie jest w bezpośrednim konflikcie z prawdopodobnie trwającymi przez całe życie i mocno zakorzenionymi poglądami na temat właściwego zachowania. Pracownicy ochrony muszą pamiętać, że nieprzestrzeganie zasad niekoniecznie wynika ze złego nastawienia. Kiedy stanie się oczywiste, że konflikty są zakorzenione w osobowości, personel ochrony będzie musiał spróbować dojść do użytecznego kompromisu. Zamiast wymagać, aby każdy osobiście skonfrontował się z osobą nieoznakowaną, polityka bezpieczeństwa mogłaby zawierać zastrzeżenie zezwalające jednostkom na natychmiastowe poinformowanie personelu ochrony. Ćwiczenia polegające na odgrywaniu ról czasami mogą rozwiązać problem z zaakceptowaniem polityki bezpieczeństwa poprzez znieczulenie opornego personelu. Przechodzenie przez ruchy tego, czego się boją lub czego nie lubi, może czasem pomóc im uświadomić sobie, że proponowana zmiana w zachowaniu nie jest tak zła, jak początkowo myśleli. Wracając do przykładu konfrontacji z naruszeniami bezpieczeństwa, wiele osób ma trudności z wyobrażeniem sobie, że mogliby powiedzieć przełożonemu w hierarchii zarządzania, aby nie jechał na barana. Termin ten, podobnie jak autostop i jazda na tylnym siedzeniu, opisuje wchodzenie przez zabezpieczone drzwi, które zostały otwarte przez kogoś innego przy użyciu ważnego kodu dostępu lub tokena. Przejście przez ćwiczenia, w których każda osoba kolejno udaje wyższego kierownika, a następnie pretendenta, pomaga przełamać opór wobec tej konkretnej polityki bezpieczeństwa. Trenerzy mogą podkreślić, że wyzwanie należy postrzegać przy użyciu innego schematu niż normalna sytuacja:

* Stosowanie polityk bezpieczeństwa w organizacji jest społecznie akceptowalne.

* Pracownicy o wyższym statusie mogą zachęcać pracowników o niższym statusie, wyrażając swoje poparcie dla polityki i pokazując, że nie czują się urażeni tą prośbą.

* Uczestnicy na wszystkich poziomach hierarchii mogą dokonać introspekcji, aby zobaczyć, czy sami nie czują się urażeni, gdy grzecznie poproszono ich o użycie odznaki podczas odgrywania ról.

Ogólnie rzecz biorąc, liderzy zespołu ds. bezpieczeństwa odpowiedzialni za wdrażanie zasad bezpieczeństwa powinni zwracać uwagę na konflikty stylów, które kolidują z głównym zadaniem zwiększania bezpieczeństwa przedsiębiorstwa. Jeśli dana osoba lubi krótkie, bezpośrednie instrukcje bez pogawędek o nieistotnych sprawach, członek zespołu ds. bezpieczeństwa powinien się dostosować i trzymać się najważniejszych rzeczy; jeśli dana osoba jest znana z tego, że lubi poznawać nieznajomego i chce spędzić kilka minut na poznawaniu pochodzenia rodzinnego, nie należy się temu sprzeciwiać. Przekazywanie pomysłów w sposób, który może być akceptowalny, jest ważniejsze niż narzucanie

innym własnych preferencji dotyczących stylu interpersonalnego. Przede wszystkim pracownicy ochrony — i kierownictwo w ogóle — powinni robić

znacznie więcej słuchania i znacznie mniej rozkazywania. Niektóre ważne kwestie psychologiczne, które liderzy bezpieczeństwa powinni wziąć pod uwagę, obejmują:

* Bezpieczeństwo cyfrowe jest niezwykle skomplikowane, a wyjaśnienia mogą być bardzo techniczne - obie te cechy nie sprzyjają skupieniu uwagi kierownictwa.

* Większość incydentów związanych z bezpieczeństwem jest spowodowana przez osoby z wewnątrz, a nie z zewnątrz, dlatego zapobieganie im wymaga konsekwentnego dokuczania — a nie czegoś, co kierownictwo lub ktokolwiek inny normalnie traktuje przychylnie.

* Sukces w bezpieczeństwie cyfrowym (w rzeczywistości w całym bezpieczeństwie) najlepiej świadczy o tym, że nic się nie dzieje, co jest trudne do zmierzenia i trudniejsze do sprzedania. Tak więc osobisty zysk z dobrze zrealizowanej strategii bezpieczeństwa jest często niewielki lub żaden — a żaden dyrektor zarządzający nie chce przedstawiać niczego jako prawdziwej miary sukcesu.

Praktyczne implikacje tych obserwacji obejmują:

* Dyskusje na temat IA powinny być rzeczowe i praktyczne, gdy tylko jest to możliwe.

* Świadomość można osiągnąć bardziej pozytywnymi środkami niż dokuczanie.

* Można tworzyć mierniki sukcesu, korzystając z gier i konkursów związanych z bezpieczeństwem, które są zabawne, a także pouczające i skuteczne w utrzymywaniu świadomości bezpieczeństwa

Oto streszczenie artykułu na temat wkładu dyrektora generalnego w bezpieczeństwo:

Niewielu menedżerów wyższego szczebla przywiązuje dużą wagę do bezpieczeństwa komputerów. Albo przekazują odpowiedzialność swoim pracownikom technicznym, albo zatrudniają konsultantów. Ale biorąc pod uwagę stawkę, podejście oparte na warunkach rynkowych jest wyjątkowo nierozsądne. Według szacunków branżowych naruszenia bezpieczeństwa dotykają co roku 90% wszystkich firm i kosztują około 17 miliardów dolarów. Na szczęście… kadra kierownicza wyższego szczebla nie musi poznawać bardziej tajemnych aspektów systemów informatycznych swojej firmy, aby zastosować praktyczne podejście. Zamiast tego powinni skupić się na znanym zadaniu, jakim jest zarządzanie ryzykiem. Ich rolą powinna być ocena wartości biznesowej ich zasobów informacyjnych, określenie prawdopodobieństwa, że te zasoby zostaną naruszone, a następnie dostosowanie zestawu procesów ograniczania ryzyka do konkretnych słabych punktów ich firmy. Podejście to, które postrzega bezpieczeństwo komputerowe jako wyzwanie operacyjne, a nie techniczne, przypomina klasyczny program zapewniania jakości, ponieważ stara się raczej unikać problemów niż je naprawiać i angażuje wszystkich pracowników, a nie tylko personel IT. Celem nie jest całkowite zabezpieczenie systemów komputerowych – to niemożliwe – ale ograniczenie ryzyka biznesowego do akceptowalnego poziomu…

Kluczowe zdanie w cytacie zaznaczyliśmy kursywą, aby podkreślić kluczową rolę zmiany kultury korporacyjnej w skutecznym zarządzaniu bezpieczeństwem.

Wyjaśnienia zachowania. W praktyce próba zmiany kultury korporacyjnej może być frustrującym i długotrwałym projektem. Jednym z aspektów tego procesu, który liderzy grup bezpieczeństwa powinni ściśle monitorować, jest interpretacja zachowań pracowników (zwana w literaturze psychologii społecznej teorią atrybucji) przez członków zespołu ds. bezpieczeństwa. Ogólnie rzecz biorąc, ludzi można postrzegać jako interpretujących (tj. wyjaśniających) zachowanie innych ludzi według dwóch niezależnych wymiarów: wewnętrznego lub zewnętrznego oraz stabilnego lub niestabilnego. Oto kilka

wyjaśnień, dlaczego Betty nie udało się wylogować z sesji po raz czwarty w tym tygodniu przed opuszczeniem biura:

* Wewnętrzny, stabilny. „Taka już jest – nigdy nie zwraca uwagi na te zasady".

* Wewnętrzny, niestabilny. „Ostatnio była przeciążona, ponieważ jej dziecko jest chore – dlatego o niej zapomniano".

* Zewnętrzne, stabilne. „System nie reaguje prawidłowo na polecenie wylogowania".

* Zewnętrzny, niestabilny. „W tym tygodniu system nie reagował prawidłowo na polecenie wylogowania".

Ta prosta czterokierunkowa klasyfikacja jest przydatna dla liderów w zrozumieniu i unikaniu klasycznych błędów atrybucji. Takie błędy atrybucji mogą powodować konflikty między pracownikami ochrony a innymi pracownikami, a nawet między pracownikami o różnym stopniu przestrzegania zasad.

Błędy atrybucji

Niektóre dobrze ugruntowane błędne interpretacje zachowań innych osób mogą kolidować z akceptacją zasad bezpieczeństwa. Takie błędy zakłócają zdolność personelu bezpieczeństwa do komunikowania wartości zasad bezpieczeństwa. Liderzy grup bezpieczeństwa powinni uwrażliwić swój personel na konsekwencje tych błędów.

Podstawowy błąd atrybucji

Najważniejszym błędem popełnianym przez ludzi podczas wyjaśniania zachowań innych ludzi jest założenie, że działania danej osoby są stałymi, wewnętrznymi cechami; typowym przykładem tego błędu jest naiwne przekonanie, że osobowość aktora jest zasadniczo tym, co osoba ta przedstawia w przedstawieniu. Każdy, kto kiedykolwiek doświadczył zaskoczenia zachowaniem i mową ulubionego aktora, z którym przeprowadzany jest wywiad, popełnił podstawowy błąd atrybucji. Niektórzy aktorzy, którzy grają złe postacie w fikcyjnych sytuacjach, byli nawet słownie i fizycznie atakowani przez widzów, którzy nie mogą oprzeć się podstawowemu błędowi przypisania i którzy naprawdę wierzą, że aktorzy są tak samo źli jak paskudni ludzie, których przedstawiają. Streszczenie a prezentacja na konferencji w 2008 roku podsumowała kilka istotnych ustaleń ilustrujących ten punkt:

W dwóch badaniach podjęto próbę udokumentowania występowania zjawiska psychologicznego znanego jako podstawowy błąd atrybucji (FAE) w medium audiowizualnym. FAE odnosi się do ludzkiej tendencji do przypisywania zachowania ludzi cechom wewnętrznym bardziej niż czynnikom zewnętrznym. W badaniu 1 wykazaliśmy, że w medium audiowizualnym widzowie mają tendencję do przypisywania zachowania aktora w dramacie telewizyjnym jego osobowości, ignorując istnienie scenariusza dyktującego zachowanie aktora. Badanie 2 powtórzyło to odkrycie, a także wykazało, że tendencja do tworzenia FAE jest związana ze stopniem, w jakim osoba zgłasza, że została przeniesiona w narrację dramatu telewizyjnego. Ponadto wykazaliśmy, że tendencja do przypisywania aktorowi cech charakteru nie zmniejsza się po wystawieniu na działanie tego samego aktora grającego dwie przeciwstawne role. Stwierdzono, że ostatnia oglądana scena determinuje ocenę cech aktora.

W pracy związanej z bezpieczeństwem wystrzeganie się podstawowego błędu atrybucji pomaga w układaniu relacji z innymi pracownikami. Na przykład, jeśli członek grupy ochrony zobaczy pracownika, Jill, który nie nosi swojej odznaki, łatwo założyć, że nigdy jej nie nosi i odmawia jej noszenia z powodu

wady charakteru. Pracownik ochrony może działać zgodnie z tymi założeniami, będąc surowym lub nieprzyjaznym w korygowaniu zachowania Jill. Surowość rodzi niechęć, a Jill może zacząć kojarzyć bezpieczeństwo z nieprzyjemnymi ludźmi, zmniejszając w ten sposób prawdopodobieństwo, że zastosuje się do zasad lub zachęci do tego innych. W rzeczywistości jednak zachowanie większości ludzi jest znacznie mniej stabilne i wewnętrzne niż niestabilne i zewnętrzne. Na przykład, jeśli pracownik ochrony po prostu się uśmiechnął i delikatnie wskazał na brak odznaki, zamiast wyciągać pochopne wnioski, mógłby odkryć, że dzisiejszy brak odznaki Jill wynikał po prostu z tego, że zdjęła kurtkę tuż przed pilnym telefonem od wiceprezydent, przerywając jej normalną procedurę przenoszenia odznaki z marynarki do kieszeni koszuli. Zatem jej brak odznaki nie byłby wcale stabilnym zachowaniem - byłby to tymczasowa aberracja bez trwałego znaczenia. Rozwiązaniem byłoby przyzwyczajenie się do przypinania plakietki do spodni lub spódnicy zamiast do marynarki lub bluzki. Podobnie wystarczy grzecznie poprosić ochroniarza, by dowiedział się, że Jill normalnie nosi odznakę, ale dzisiaj jej czteroletni syn zdjął ją z kurtki, żeby się nią pobawić, a matka nie zauważyła zmiany. W tym przykładzie zachowanie Jill jest zewnętrzne i nie ma nic wspólnego z charakterem. Życzliwe interakcje między Jill a ochroniarzem zwiększają poczucie więzi społecznej i zwiększają prawdopodobieństwo, że będzie ona pozytywnie wspominała incydent i przestrzegała polityki bezpieczeństwa w przyszłości.

Podsumowując, mając świadomość podstawowego błędu atrybucji, personel ochrony może zostać przeszkolony w przyjmowaniu mniej osądzającej lub pochopnej mentalności, która może zrazić innych pracowników i zaszkodzić programom bezpieczeństwa.

Efekt aktora-obserwatora

Efekt aktora-obserwatora polega na interpretowaniu własnego zachowania jako odpowiednich niestabilnych, motywowanych zewnętrznie reakcji

warunków środowiskowych, podczas gdy zachowanie innych ludzi postrzegane jest w świetle podstawowego błędu atrybucji jako stabilne, wewnętrznie umotywowane przejawy cech charakteru. Uświadomienie sobie tej tendencji pomaga personelowi ochrony przeciwstawić się podstawowemu błędowi atrybucji.

Stronniczość samoobsługowa

Odpowiednikiem efektu aktora-obserwatora jest samoobsługowe nastawienie, które oszukuje ludzi, aby uwierzyli, że ich własne zachowanie wynika ze stabilnych, wewnętrznych aspektów ich charakteru. Funkcjonariusze ochrony, którzy nie są świadomi tego niebezpiecznego błędu, mogą odnieść wrażenie, że są w pewnym sensie lepsi od innych osób, które nie wiedzą tak dużo o bezpieczeństwie jak oni lub które nie przestrzegają tak dokładnie polityki bezpieczeństwa jak oni. Funkcjonariusze mogli nie uwzględnić faktu, że godziny szkolenia i coachingu prowadzone przez liderów ich grup bezpieczeństwa są co najmniej tak samo odpowiedzialne za ich własną wiedzę na temat zasad bezpieczeństwa i przestrzeganie ich, jak każda wrodzona wyższość. Ujawniając tego rodzaju błędne myślenie podczas szkolenia i superwizji pracowników ochrony, menedżerowie mogą pomóc zmniejszyć konflikty, które w naturalny sposób wynikają z aury zakładanej wyższości.

Salience i uprzedzenia

Kiedy ludzie są proszeni o odgadnięcie, która osoba w grupie jest najbardziej wpływową (lub najmniej wpływową) osobą, psychologowie społeczni odkrywają, że tej osobie, która najbardziej się wyróżnia, z jakiegokolwiek powodu, częściej przypisuje się szczególne właściwości, o których mowa. Takie efekty dotyczą każdej cechy, o którą pytają psychologowie: najbardziej (lub najmniej) inteligentnej, agresywnej, sympatycznej i tak dalej. Zjawisko to znane jest jako efekt salience. Zastosowanie efektu

istotności może wystąpić, jeśli funkcjonariusze ds. bezpieczeństwa zobaczą grupę pracowników, którzy naruszają zasady bezpieczeństwa. Naturalną i nieproduktywną tendencją jest wyciąganie pochopnych wniosków, że winna jest najwyższa lub najniższa, najcieńsza lub najgrubsza, najbielsza lub najczarniejsza osoba w grupie. Ten błąd może skutkować niesprawiedliwym traktowaniem całkowicie niewinnych ludzi. Ten problem błędnej interpretacji istotności jest zaostrzony przez uprzedzenia; na przykład wyobraź sobie, że istnieje możliwa do zidentyfikowania grupa zwana Ogunianami (o ile możemy ustalić, nie ma takiej grupy), którzy tradycyjnie noszą, powiedzmy, siedmioboczny symbol swojej tożsamości. Jeśli anty-Ogunianski oficer ochrony zobaczy grupę, która nie podporządkuje się, w której jeden z członków nosi charakterystyczny siedmiokąt Oguna, oficerowi może być trudno oprzeć się obwinianiu Ogunianina za niezgodność, nawet jeśli w rzeczywistości Ogunianin czekał na używać ważnej karty dostępu w pełnej zgodzie z polityką bezpieczeństwa. Co gorsza, ludzie mogą być pod tak silnym wpływem oczekiwań — będących częścią ich schematu — że w rzeczywistości całkowicie błędnie postrzegają sytuację. Na przykład w niektórych klasycznych eksperymentach dotyczących uprzedzeń w latach pięćdziesiątych psychologowie pokazali badanym rysunek przedstawiający dwie osoby, jedną jasną, a drugą ciemną, stojące w wagonie tramwajowym. Jeden trzymał nóż. Zapytani później o zdjęcie, biali badani konsekwentnie twierdzili, że czarna postać trzymała nóż, ale w rzeczywistości to biała postać na rysunku miała nóż. Tak więc nawet sama obserwacja może zostać wypaczona przez uprzedzenia i oczekiwania; na przykład, jeśli oficer ochrony anty-Ogunian zobaczy grupę ludzi przechodzących przez otwarte drzwi do zabezpieczonego obszaru bez użycia swoich odznak, funkcjonariusz może błędnie zgłosić, że była to wina Ogunianina, nawet jeśli w pomieszczeniu nie było Ogunianina Grupa. Taki błędny raport nie tylko rozwścieczyłby niewinnych Ogunian i prawdopodobnie wywołałby ogólną niechęć lub wrogość Ogunian do wysiłków związanych z bezpieczeństwem w ogóle, ale mógłby również wprowadzić w błąd samą grupę bezpieczeństwa, aby spróbowała poprawić zachowanie niewłaściwej osoby lub osób. Podobnie każda mniejszość — niezależnie od tego, czy chodzi o płeć, orientację płciową, religię, rasę czy niepełnosprawność — może być przedmiotem winy uprzedzonego funkcjonariusza ochrony, gdy grupa nie przestrzega zasad. Liderzy ds. bezpieczeństwa powinni uświadomić swoim pracownikom niebezpieczeństwo stosowania tej błędnej metody wyjaśniania zachowań grupowych. W wielu organizacjach taka dyskryminacja stanowi naruszenie polityki korporacyjnej i może być nawet niezgodna z prawem. W każdym razie uprzedzenia nie są konstruktywne i należy je monitorować i przezwyciężać.

Różnice międzykulturowe

Wiele krajów na świecie doświadcza zmian w populacji z powodu imigracji. Zwłaszcza w obszarach, w których ludzie byli dotąd w dużej mierze jednorodni, różnorodność kulturowa, religijna i rasowa może prowadzić do konfliktów międzyludzkich i międzygrupowych. Konflikty takie mogą częściowo wynikać z uprzedzeń, ale mogą również wynikać z różnic w wartościach i założeniach. Ta definicja kultury pomaga zdefiniować dyskusję:

Kultura jako programowanie mentalne

Każdy człowiek nosi w sobie wzorce myślenia, odczuwania i potencjalnego działania, których nauczył się przez całe życie. Wiele z nich zostało nabytych we wczesnym dzieciństwie, ponieważ w tym czasie człowiek jest najbardziej podatny na uczenie się i asymilację. Gdy tylko pewne wzorce myślenia, odczuwania i działania zadomowią się w umyśle danej osoby, musi się jej oduczyć, zanim będzie mogła nauczyć się czegoś innego, a oduczenie się jest trudniejsze niż uczenie się po raz pierwszy. Posługując się analogią do sposobu, w jaki komputery są programowane, książka ta nazwie takie wzorce myślenia, odczuwania i działania programami umysłowymi, czyli...

Pracownicy ochrony zaangażowani w proces zmiany kultury korporacyjnej powinni być wyczuleni na możliwość, że ludzie z różnych rzeczywistych środowisk kulturowych mogą inaczej reagować na proponowane polityki bezpieczeństwa. Na przykład w 2001 r. fundamentalistyczni ekstremiści talibów w Afganistanie zadekretowali, że osoby niebędące muzułmanami będą musiały nosić plakietki w miejscach publicznych10. może mieć niespodziewanie emocjonalną reakcję na polecenie. Zanim zaczniesz wywierać presję (lub okazywać wrogość) komukolwiek, kto wydaje się sprzeciwiać jakiejś polityce, warto zapytać o przekonania i postawy tej osoby oraz wyjaśnić podstawy danej polityki. Zwłaszcza tam, gdzie występują różnice międzykulturowe, takie badanie i dyskusja mogą zapobiec trudnościom i niezgodom oraz złagodzić nieoczekiwany, kulturowo zakorzeniony niepokój. Specjaliści ds. bezpieczeństwa muszą być bardzo świadomi różnic kulturowych poszczególnych osób w grupie docelowej. Na przykład w niektórych kulturach (głównie nowego świata i zachodnich) rzeczywistość jest bezpośrednio związana z faktami i weryfikowalnymi obliczeniami. Inne kultury mogą kłaść większy nacisk na osobiste uczucia, intuicję i kulturowo zakorzenione przekonania w swoim rozumieniu rzeczywistości. Dlatego różni ludzie mogą nie podzielać tego samego rozumienia rzeczywistości ani wdrażać polityk według tych samych zasad, chyba że ujawnią swoje założenia i przedyskutują je z zamiarem osiągnięcia porozumienia. Rozważając kulturę, należy również uwzględnić zmieniającą się dynamikę współczesnego społeczeństwa. Każde nowoczesne miasto lub wiodąca instytucja publiczna jest dziś złożoną mieszanką ludzi z różnych środowisk kulturowych i społecznych. Wspólna praca przez dużą część ich aktywnych dni razem jako grupa prowadzi do sytuacji tygla, w której wszystkie indywidualne kultury i skłonności społeczne są dodawane do mieszanki i pojawiają się jako (w większości) inna kultura. Następnie jednostki zabierają tę nową kulturę z powrotem do domu, gdzie miesza się ona z wkładem ich rodziny i przyjaciół, co często prowadzi do większej liczby modyfikacji i odmian. Sama organizacja nieustannie się zmienia, ponieważ ludzie dołączają i odchodzą. Wszystko to sprawia, że kultura jest zjawiskiem dynamicznym, choć nie tak szybko zmieniającym się jak front technologiczny. W związku z tym każda polityka lub struktura bezpieczeństwa musi być w stanie uwzględnić i dostosować ten zmieniający się paradygmat, jeśli ma odnieść sukces w zabezpieczaniu przedsiębiorstwa.

Oprawianie rzeczywistości

Jak sprawić, by kultura korporacyjna bardziej wspierała IA? Schematy wpływają na to, co postrzegamy. Na przykład pracownik odmawia wzięcia urlopu, pracuje do późna każdej nocy, nigdy się nie spóźnia i nigdy nie jest chory. Wzorowy pracownik? Być może w jednym schemacie. Z punktu widzenia bezpieczeństwa zachowanie pracownika jest podejrzane. Zdarzały się przypadki, w których tacy ludzie byli malwersantami, którzy nie mogli odejść z pracy: nawet dzień nieobecności może skutkować odkryciem ich zbrodni. Święty czy grzesznik? Nasze oczekiwania determinują to, co widzimy. Aby zmienić ten schemat, aby ludzie poważnie traktowali IA, powinniśmy dostarczać uczestnikom szkoleń i podnoszenia świadomości bezpieczeństwa przykłady przestępstw komputerowych i naruszeń bezpieczeństwa z życia wziętych, tak aby polityki bezpieczeństwa miały oczywisty sens, a nie wydawały się arbitralne. Schematy wpływają na to, co pamiętamy. Kiedy informacje niezgodne z naszymi z góry przyjętymi założeniami mieszają się ze szczegółami, które pasują do naszych istniejących schematów, selektywnie zatrzymujemy to, co pasuje, i odrzucamy to, co jest sprzeczne. Kiedy karmiono nas dietą filmów i programów telewizyjnych ilustrujących przesłankę, że informacje są najbardziej zagrożone przez genialnych hakerów, dlaczego mielibyśmy pamiętać prawdę: że nieostrożność i niekompetencja uprawnionych użytkowników systemów informatycznych wyrządzają znacznie więcej szkód niż złe intencje i osoby z zewnątrz kiedykolwiek to robią? Instruktorzy powinni podkreślać praktyczną stronę IA, pokazując, w jaki sposób polityki chronią wszystkich pracowników przed fałszywymi oskarżeniami, zapobiegają szkodzie reputacji i zyskom organizacji, a nawet odgrywają rolę w bezpieczeństwie narodowym. Jest to szczególnie prawdziwe tam, gdzie biznes styka się z infrastrukturą techniczną, od

której wszyscy jesteśmy zależni. Co najważniejsze, nauczanie innych o IA nie może być przypadkowe i przypadkowy romans. Przed podjęciem próby wdrożenia polityk i procedur poza środkami nadzwyczajnymi, które są potrzebne natychmiast), powinniśmy upewnić się, że wśród naszych kolegów zbudowaliśmy spójny pogląd na OW. W świetle złożoności poznania społecznego, nasze zwykłe próby wdrożenia polityk i procedur bezpieczeństwa wydają się żałośnie nieudolne. Kilka godzin wykładów i film, coroczny rytuał podpisywania polityki bezpieczeństwa, która wydaje się być napisana przez Marsjan – to nie są metody, które poprawią bezpieczeństwo. Wysiłki te składają jedynie deklaracje na temat idei bezpieczeństwa. Według badań nad informacjami sprzecznymi z intuicją, sposób, w jaki informacje są prezentowane, wpływa na osąd ludzi. Na przykład nawet informacje sprzeczne z ustalonymi schematami mogą zostać przyswojone, jeśli ludzie mają wystarczająco dużo czasu, aby zintegrować nową wiedzę ze swoimi światopoglądami. Wynika z tego, że polityki bezpieczeństwa niezwiązane z sytuacjami kryzysowymi powinny być wprowadzane przez długi czas, a nie w pośpiechu. Skuteczny program OW zawiera częste przypomnienia o bezpieczeństwie. Aby zmienić kulturę korporacyjną, praktycy powinni stosować takie metody, jak kącik bezpieczeństwa w firmie publikacje korporacyjne, biuletyny bezpieczeństwa szczegółowo opisujące najnowsze przestępstwa komputerowe lub naruszenia bezpieczeństwa, które trafiły do wiadomości, konkursy na identyfikację problemów w realistycznych scenariuszach oraz kolumny do pisania, w których można odpowiadać na pytania dotyczące zasad. OW musi stać się częścią ram rzeczywistości, a nie tylko narzuconym przez kierownictwo.

W każdym kursie bezpieczeństwa lub programie uświadamiającym instruktorzy i facylitatorzy powinni wyraźnie odnieść się do kwestii kultury korporacyjnej, oczekiwań i schematów społecznych. Nie polegaj wyłącznie na dyskursie intelektualnym, gdy zajmujesz się kwestią złożonych percepcji i uczuć. Korzystaj z symulacji, filmów i ćwiczeń z odgrywaniem ról, aby wypełnić lukę między intelektem a emocjami. Zajmij się uczuciami i spostrzeżeniami wszystkich uczestników, gdy dowiadują się o sprzecznych z intuicją zachowaniach, których będzie wymagać poprawa bezpieczeństwa. Zachęć uczniów do zastanowienia się, jak mogą się czuć i reagować w różnych sytuacjach, które mogą się pojawić podczas przechodzenia do bezpieczniejszego środowiska. Na przykład poproś uczestników, aby wyobrazili sobie:

* Poproszenie współpracowników, aby nie przechodzili przez zabezpieczone wejście bez przejścia przez system kontroli dostępu z własną tożsamością

* Powiedzenie swojemu szefowi, że nie będą kopiować oprogramowania bez odpowiedniej licencji

* Przesłuchiwanie gościa lub pracownika, który nie nosi identyfikatora

Przekazywanie zasad bezpieczeństwa.

Jakie są sposoby na zmianę schematów naszych kolegów, aby stali się bardziej otwarci na politykę OW?

* Początkowa ekspozycja. Wstępne informacje mogą wpływać na reakcje ludzi na informacje prezentowane później. Na przykład samo wystawienie badanych eksperymentalnych na słowa, takie jak lekkomyślny lub żądny przygód, wpływa na ich ocenę ryzykownych zachowań w późniejszym teście. Wynika z tego, że przygotowując się do zwiększenia świadomości pracowników w kwestiach bezpieczeństwa, przedstawienie studiów przypadku może korzystnie wpłynąć na gotowość uczestników do zbadania wymagań bezpieczeństwa.

* Kontrprzykłady. Istniejące wcześniej schematy można zakwestionować za pomocą kilku kontrprzykładów, z których każdy kwestionuje składnik schematu. Na przykład uprzedzenia dotyczące grupy etnicznej są bardziej podatne na zmianę w wyniku kontaktu z kilkoma osobami, z których każda

jest sprzeczna z innym aspektem uprzedzonego schematu. Wynika z tego, że programy świadomości bezpieczeństwa powinny zawierać wiele realistycznych przykładów wymogów bezpieczeństwa i naruszeń. Jako kontrprzykład, studenci kursów IA w college'u skomentowali nierealistyczny scenariusz w pokazanym im wideo szkoleniowym: serię katastrofalnych naruszeń bezpieczeństwa, które miały miejsce w tej samej firmie. Opierając się na ustaleniach kognitywnych psychologów społecznych, film byłby bardziej skuteczny w szkoleniu, gdyby incydenty zostały udramatyzowane jako występujące w różnych firmach. W praktyce praktycy powinni być na bieżąco i aktualizować swoje materiały. Wiele publikacji dotyczących OW zawiera przydatne studia przypadków, które pomogą zwiększyć skuteczność podnoszenia świadomości i szkoleń.

* Wybór sformułowań. Postrzeganie ryzyka i korzyści jest w dużym stopniu uzależnione od sformułowań, w których przedstawiane są sytuacje i opcje. Na przykład badani eksperymentalni reagowali znacznie bardziej pozytywnie na doniesienia o leku z „50-procentowym sukcesem" niż na ten sam lek opisany jako „50-procentowy niepowodzenie".

Wynika z tego, że praktycy powinni starannie dobierać język podczas kampanii uświadamiających w zakresie bezpieczeństwa. Zamiast skupiać się na zmniejszaniu wskaźników niepowodzeń (naruszeń zasad), powinniśmy kłaść nacisk na poprawę naszych wskaźników sukcesu. Niestety, niektórych wskaźników nie da się wyrazić pozytywnie; na przykład nie jest łatwo zmierzyć wskaźnik skuteczności środków bezpieczeństwa zaprojektowanych w celu udaremnienia ataków na systemy. Osądy są łatwo zniekształcane przez tendencję do polegania na osobistych anegdotach, małych próbkach, łatwo dostępnych informacjach i błędnej interpretacji informacji statystycznych. Zasadniczo my, ludzie, nie zawsze racjonalnie przetwarzamy fakty. Jeśli programy uświadamiające dotyczące bezpieczeństwa polegają wyłącznie na przedstawianiu faktycznych informacji o zagrożeniach oraz proponowanych zasadach i procedurach, prawdopodobnie napotkają uporczywą odmowę logicznego działania. Realizacja programu bezpieczeństwa musi angażować nie tylko racjonalny umysł. Musimy również odwoływać się do wyobraźni i emocji naszych kolegów. Musimy inspirować zaangażowanie na rzecz bezpieczeństwa, a nie tylko je opisywać.

Nagroda kontra kara

Podczas egzekwowania zasad bezpieczeństwa zbyt wiele organizacji koncentruje się wyłącznie na karaniu tych, którzy łamią zasady. Jednak wszystko, co wiemy o modyfikowaniu zachowania, uczy nas stosowania nagrody, a nie kary. Karanie osób, które nie przestrzegają zasad bezpieczeństwa, często wywołuje niechęć i wrogość, które przenoszą się na przyszłe interakcje. Zamiast postrzegać zapewnienie informacji jako korzyść dla organizacji i swoich interesów, ofiary brutalnego traktowania mogą oprzeć się nawet dobrym intencjom, rozsądnym zmianom w polityce bezpieczeństwa po prostu z powodu emocjonalnej warstwy związanej z zażenowaniem i frustracją wywołaną krytyką i karami. Oprócz unikania negatywności i odpychania, nagroda może po prostu działać lepiej niż kara przy zmianie zachowania. Na przykład pracownik ochrony z dużej korporacji eksperymentował z nagrodami i karami we wdrażaniu zasad bezpieczeństwa. Pracownicy mieli wylogowywać się z terminali mainframe po wyjściu z biura, ale wskaźniki zgodności wyniosły tylko około 40 procent. W jednym dziale oficer bezpieczeństwa stosował zwykłe techniki zalecane w literaturze i powszechne wśród specjalistów ds. bezpieczeństwa; na przykład umieszczała paskudne notatki na terminalach, które nie były wylogowywane, zmieniała hasła na zaległych kontach i poniżała gwałcicieli, zmuszając ich do zgłaszania się do swoich szefów w celu uzyskania autoryzacji w celu uzyskania nowego hasła. Jednak w innym dziale po prostu zostawiła Hershey's Chocolate Kiss na klawiaturze każdego terminala, którego użytkownik faktycznie wylogował się przed wyjściem. Po miesiącu stosowania tych dwóch strategii wskaźniki zgodności w ukaranym wydziale wzrosły do około 60 procent. Zgodność w dziale

dostarczającym czekoladki osiągnęła około 80 procent — a ich stosunek do bezpieczeństwa był znacznie korzystniejszy niż norma. Ten przypadek ilustruje niektóre korzyści płynące z nagrody:

* Wskaźniki zgodności były istotnie wyższe niż w grupie ukaranej.

* Postawy są bardziej pozytywne.

* Koszty mogą być niższe, ponieważ małe nagrody dostarczane masowo mogą być znacznie tańsze i szybsze w zastosowaniu niż reklama

PRZEKONANIA I POSTAWY

Psychologowie rozróżniają przekonania i postawy. Przekonanie odnosi się do informacji poznawczych, które nie muszą mieć elementu emocjonalnego. Postawa odnosi się do oceny lub reakcji emocjonalnej. Tak więc ktoś może słusznie uważać, że kopiowanie dużej liczby pakietów oprogramowania prawnie zastrzeżonego bez zezwolenia jest przestępstwem, a mimo to mieć nastawienie, że nie ma to dla niego znaczenia. Racjonalny pracownik może sądzić, że złośliwe oprogramowanie może zostać pobrane na firmowe komputery za pośrednictwem nieautoryzowanego oprogramowania dostępnego na niezweryfikowanych stronach internetowych (a tym samym poprawnie odpowiedzieć na kwestionariusz oceniający świadomość bezpieczeństwa), ale mieć postawę, że ryzyko jest znikome – i z radością kontynuować pobieranie nieautoryzowanego oprogramowania w pracy .

Wierzenia

Przekonania mogą się zmienić, gdy prezentowane są sprzeczne informacje, ale niektóre badania sugerują, że może minąć nawet tydzień, zanim znaczące zmiany będą mierzalne. Inne badania sugerują, że kiedy ludzie mają sprzeczne przekonania, zapewnienie możliwości wyrażenia i oceny tych przekonań może prowadzić do zmian, które zmniejszają niespójność. Odkrycia te sugerują, że bezpieczeństwo korporacyjne musi zbadać obecną strukturę przekonań wśród pracowników i menedżerów. Kwestionariusze, grupy fokusowe i wywiady mogą nie tylko pomóc specjaliście ds. bezpieczeństwa, ale w rzeczywistości mogą pomóc skierować kulturę korporacyjną we właściwym kierunku. Efekt Hawthorne'a to nazwa nadana poprawie mierzonego zachowania wynikającej po prostu z reakcji pracowników na bycie badanym; przeprowadzone prawidłowo, uczciwie i bezkarnie, badanie przekonań i postaw pracowników może świadczyć o autentycznym zainteresowaniu kierownictwa poprawą polityki i praktyk bezpieczeństwa przy udziale wszystkich zaangażowanych osób.

Postawy

Postawa, w klasycznej definicji, to wyuczona reakcja oceniająca, skierowana na określone obiekty, która jest względnie trwała i wpływa na zachowanie w sposób ogólnie motywujący. Branża reklamowa wydaje rocznie ponad 50 miliardów dolarów, aby wpływać na postawy społeczne w nadziei, że te postawy doprowadzą do zmian w nawykach wydawania pieniędzy — to znaczy w zachowaniu. Badania nad warunkowaniem klasycznym sugerują, że postaw można się nauczyć nawet poprzez proste kojarzenie słów. Jeśli chcemy skłonić naszych kolegów do bardziej negatywnego spojrzenia na przestępców komputerowych, ważne jest, aby nie przedstawiać przestępstw komputerowych za pomocą pozytywnych obrazów i słów. Filmy, które pokazują hakerów jako miłych, inteligentnych, atrakcyjnych fizycznie i sympatycznych ludzi, mogą wyrządzić krzywdę, minimalizując powagę szpiegostwa przemysłowego i cyberwandalizmu. Ucząc bezpieczeństwa, powinniśmy unikać chwalenia przestępców, których opisujemy w studiach przypadków.

Badania nad rozwojem postaw konsekwentnie pokazują, że nagrody i kary są ważnymi czynnikami motywującymi zachowanie. Badania pokazują, że nawet pozornie niewielka zachęta może wpływać na

postawy. Przełożony lub instruktor powinien pochwalić każdy komentarz krytyczny wobec przestępstw komputerowych lub wspierające ustanowione zasady bezpieczeństwa. Pracownicy, którzy lekceważą kwestie bezpieczeństwa lub lekceważą przepisy, powinni być kwestionowani ze względu na ich postawę, a nie ignorowani. Takie wyzwania najlepiej przeprowadzać na osobności, aby uniknąć zawstydzenia sceptyków i potencjalnego oporu spowodowanego dumą lub poczuciem machismo.

Zmiana postaw wobec bezpieczeństwa

Perswazja — zmiana czyichś postaw — została opisana w kategoriach komunikacji. Cztery obszary badań obejmują:

1. Zmienne komunikatora. Kto próbuje przekonać?

2. Zmienne wiadomości. Co jest prezentowane?

3. Zmienne kanałowe. Jakimi środkami ma miejsce próba?

4. Zmienne odbiorców. Do kogo skierowana jest perswazja?

Zmienne komunikatora

Atrakcyjność, wiarygodność i status społeczny wywierają silny wpływ natychmiast po tym, jak mówca lub pisarz komunikuje się z docelowymi odbiorcami; jednak w okresie od tygodni do miesiąca efekty słabną, aż dominującym problemem jest treść wiadomości. Możemy wykorzystać to zjawisko, identyfikując kadrę kierowniczą wyższego szczebla, która z największym prawdopodobieństwem odniesie sukces w nadaniu pozytywnego tonu kolejnym szkoleniom w zakresie bezpieczeństwa. Powinniśmy szukać szanowanych, sympatycznych ludzi, którzy rozumieją problemy i szczerze wierzą w politykę, za którą się opowiadają. W szczególności jeden styl osobowości może zagrozić powodzeniu polityki bezpieczeństwa: osobowość autorytarna. Z wielu badań wynika, że niektórzy ludzie, często wychowani przez karzących rodziców, bardzo dbających o status społeczny, stają się sztywno oddani konwencjonalnym przekonaniom, podporządkowują się władzy, sami surowo sprawują władzę i są wrogo nastawieni do grup, które postrzegają jako niepopularne. Autorytarna osoba może być okropnym oficerem ochrony. Taki funkcjonariusz może czerpać większą satysfakcję z wydawania ludziom rozkazów i karania ich niż z długofalowych sukcesów we wdrażaniu polityki bezpieczeństwa.

Zmienne wiadomości

Strach może wpłynąć na zmianę postaw tylko wtedy, gdy jest rozsądnie zastosowany. Nadmierny nacisk na straszne skutki słabego bezpieczeństwa może przynieść odwrotny skutek, a uczestnicy programu uświadamiającego całkowicie odrzucą ten przekaz. Przerażającym konsekwencjom należy natychmiast towarzyszyć skutecznym i osiągalnym środkom bezpieczeństwa. Niektóre badania sugerują, że przedstawienie wyważonych argumentów pomaga przekonać tych, którzy początkowo nie zgadzają się z propozycją. Przedstawienie sprzeciwu wobec propozycji i przedstawienie kontrargumentów jest skuteczniejsze niż jednostronne diatryby. Popularne filmy szkoleniowe z Software & Information Industry Association wykorzystują tę technikę: pokazują ludzi, takich jak „studenci, wykładowcy i wydawcy wszelkiego rodzaju mediów, dyskutujący o prawnych i etycznych implikacjach kopiowania prac innych ludzi" i rzetelnie przedstawiają argumenty osób naruszających prawa autorskie przed ich obaleniem. Skromne powtórzenie wiadomości może pomóc w uzyskaniu bardziej pozytywnej odpowiedzi. Dlatego programy zwiększające świadomość bezpieczeństwa, które obejmują pomysłowe plakaty, kubki, specjalne biuletyny, nagrania audio i wideo oraz wykłady, z większym prawdopodobieństwem zbudują i utrzymają poparcie dla bezpieczeństwa niż okazjonalne

intensywne sesje indoktrynacji. Wykorzystanie wielu kanałów komunikacji (omówione w kolejnym punkcie) zwiększa również skuteczność przekazu.

Zmienne kanałowe

Kanał, którym się komunikujemy, ma silny wpływ na postawy i znaczenie powierzchownych atrybutów komunikatora. W nowoczesnych organizacjach większość ludzi wychodzi z założenia, że spotkanie jest idealnym sposobem na przekazanie nowych informacji. Jednak najskuteczniejszym sposobem przekonania kogoś do zwrócenia uwagi na dowolny temat jest bezpośrednia perswazja. Szkolenie w zakresie bezpieczeństwa powinno obejmować coś więcej niż tylko taśmy i książki; charyzmatyczny nauczyciel lub lider może pomóc wzbudzić entuzjazm dla – lub przynajmniej zmniejszyć opór wobec lepszego bezpieczeństwa. Ponadto edukatorzy ds. bezpieczeństwa nie powinni przedstawiać decydentom nowych pomysłów na spotkaniu. Istnieje zbyt duże niebezpieczeństwo pomieszania reakcji na politykę z kwestiami niezwiązanymi z polityką, zakorzenionymi w relacjach między uczestnikami. Nierzadko zdarza się, że jeden dyrektor sprzeciwia się nowej polityce tylko dlatego, że inny ją popiera. Dobrym sposobem na wprowadzenie polityki bezpieczeństwa są indywidualne spotkania z jednym kierownikiem w danym momencie, aby wyjaśnić problemy i propozycje oraz poprosić o wsparcie. Psychologowie badający teorię reakcji poznawczych badali wiele subtelnych aspektów perswazji. Eksperymenty wykazały, że pytania retoryczne, takie jak „Czy mamy zaakceptować inwazje na nasze systemy komputerowe?" są skuteczne, gdy argumenty są solidne, ale przynoszą efekt przeciwny do zamierzonego, gdy argumenty są słabe. Funkcjonariusze ochrony nie powinni zadawać pytań retorycznych, chyba że są pewni, że prawie wszyscy nieuchronnie uzyskają tę samą odpowiedź – tę, której szukają funkcjonariusze ochrony. Stwierdzono, że rozważanie faktów i logicznych argumentów, jako centralnej drogi perswazji, prowadzi do trwalszych postaw i zmian postaw niż peryferyjne wpływy logicznie niepowiązanych czynników, takich jak fizyczna atrakcyjność mówcy.

Zmienne odbiorców

Jak wspomniano, kwestionariusze i wywiady mogą pomóc ugruntować korzystną zmianę nastawienia, prowadząc do zaangażowania. Gdy pracownicy publicznie zadeklarują poparcie dla lepszego bezpieczeństwa, niektórzy zaczną zmieniać swoje postrzeganie siebie. Poszczególni pracownicy powinni być zachęcani do podejmowania różnych obszarów publicznej odpowiedzialności za OW w ramach swojej grupy roboczej. Role te powinny być okresowo wymieniane między pracownikami, aby dać każdemu doświadczenie publicznego zaangażowania w poprawę bezpieczeństwa. Aby utrzymać zainteresowanie bezpieczeństwem, regularne spotkania entuzjastów w celu omówienia najnowszych wiadomości dotyczących bezpieczeństwa mogą sprawić, że temat będzie świeży i interesujący. Nowe przypadki mogą pomóc funkcjonariuszom ds. bezpieczeństwa wyjaśnić zasady z aktualnymi odniesieniami, które zainteresują ich współpracowników i zmotywują kierowników do zwracania uwagi na zasady bezpieczeństwa.

ZACHĘCAMY DO INICJATYWY

Idealną sytuacją byłoby, gdyby wszyscy faktycznie pomagali egzekwować zasady bezpieczeństwa. W rzeczywistości jednak niektórzy ludzie są chętni do współpracy i pomocni, podczas gdy inni – lub nawet ci sami ludzie w różnych okolicznościach – są niechętni i podejrzliwi wobec nowych zasad. Co możemy zrobić, aby zwiększyć współpracę i zmniejszyć odrzucenie?

Zachowanie prospołeczne

Badania ludzi, którzy przybyli z pomocą innym, mogą pomóc zachęcić wszystkich w organizacji do właściwego postępowania. Niektórzy ludzie interweniują, aby powstrzymać przestępstwa; inni ignorują przestępstwa lub przyglądają się im biernie. Psychologowie społeczni opracowali schemat opisujący kroki prowadzące do zachowań prospołecznych:

1. Ludzie muszą zauważyć nagły wypadek lub przestępstwo, zanim będą mogli działać. W związku z tym szkolenie w zakresie bezpieczeństwa musi obejmować informacje o tym, jak rozpoznać, że ktoś może być zaangażowany w przestępczość komputerową.

2. Sytuację należy zdefiniować jako awaryjną – coś wymagającego działania. Szkolenie z zakresu bezpieczeństwa, które dostarcza faktów na temat wpływu przestępczości komputerowej na społeczeństwo oraz solidnych informacji o potrzebie bezpieczeństwa w organizacji, może pomóc pracownikom rozpoznać naruszenia bezpieczeństwa jako sytuacje awaryjne.

3. Każdy musi wziąć odpowiedzialność za działanie, ale im większa liczba osób w grupie dotkniętej awarią, tym wolniejszy jest średni czas reakcji. Większe grupy wydają się prowadzić do rozproszenia odpowiedzialności; każda osoba czuje, że ktoś inny jest bardziej odpowiedzialny za radzenie sobie z sytuacją kryzysową. Innym możliwym czynnikiem jest niepewność co do klimatu społecznego; ludzie boją się, że wydadzą się niemądrzy lub nadmiernie emocjonalni w oczach obecnych. Aby przezwyciężyć ten efekt, należy ustanowić kulturę korporacyjną, która nagradza odpowiedzialne indywidualne zachowania, takie jak zgłaszanie naruszeń bezpieczeństwa.

4. Po przyjęciu odpowiedzialności za rozwiązanie problemu należy podjąć odpowiednie decyzje i działania. Jasno napisane zasady i procedury bezpieczeństwa zwiększą prawdopodobieństwo, że pracownicy będą działać na rzecz poprawy bezpieczeństwa. Natomiast sprzeczne zasady, słabo udokumentowane procedury i niespójne wsparcie ze strony kierownictwa będą kolidować z decyzją o działaniu.

Inna analiza sugeruje, aby ludzie pośrednio analizowali koszty pomagania i nie pomagania przy podejmowaniu decyzji, czy działać prospołecznie. Połączenie czynników najbardziej sprzyjających prospołeczności to niski koszt pomagania i wysoki koszt nieudzielania pomocy. Procedury bezpieczeństwa powinny ułatwiać działanie zgodne z polityką bezpieczeństwa. Powinna istnieć infolinia służąca do zgłaszania naruszeń bezpieczeństwa, aw razie potrzeby należy szanować anonimowość. Poradnictwo psychologiczne i kontynuacja powinny być dostępne, jeśli ludzie czują się zdenerwowani swoim zaangażowaniem. I odwrotnie, brak odpowiedzialnego działania powinien być poważną sprawą; polityka kadrowa powinna dokumentować jasne i znaczące sankcje za brak działania w przypadku zaobserwowania naruszenia bezpieczeństwa. Kary obejmowałyby krytyczne uwagi w przeglądzie zatrudnienia, aw stosownych przypadkach nawet zwolnienie. Jedną z metod, która nie działa w celu zwiększenia zachowań prospołecznych, jest nawoływanie; zwykłe pouczanie ludzi w sposób abstrakcyjny o tym, co powinni robić, ma niewielki lub żaden pozytywny efekt. Co istotne, ogólny poziom stresu i presja skupienia się na trudnych zadaniach, których terminy wydają się niemożliwe, może znacznie zmniejszyć prawdopodobieństwo, że ludzie będą postępować zgodnie ze swoimi zasadami moralnymi i etycznymi. Bezpieczeństwo prawdopodobnie rozkwitnie w środowisku, które zapewnia wystarczającą ilość czasu i wsparcia dla pracowników do pracy zawodowej. Biura, w których wszyscy reagują na ciągłą serię oczywistych sytuacji kryzysowych, prawdopodobnie nie będą zwracać uwagi na naruszenia bezpieczeństwa. Niektóre wyniki badań potwierdzają zdrowy rozsądek. Na przykład poczucie winy motywuje wiele osób do bardziej prospołecznego działania. Efekt ten działa najlepiej, gdy ludzie są zmuszeni do przyjęcia odpowiedzialności. W ten sposób egzekwowanie standardów bezpieczeństwa za pomocą nagan i sankcji może rzeczywiście zwiększyć prawdopodobieństwo, że pracownicy będą później działać w sposób bardziej skłonny do współpracy;

jednakże, jak zasugerowano wcześniej, kara nie powinna zastępować nagrody. Ponadto nastrój wpływa na podatność na presje prospołeczne. Złe nastroje zmniejszają prawdopodobieństwo zachowań prospołecznych, podczas gdy dobre nastroje zwiększają prospołeczność. Środowisko pracy, w którym pracownicy są szanowani, bardziej sprzyja dobremu bezpieczeństwu niż taki, który ich dewaluuje i wykorzystuje. Nawet pobieżna znajomość z innymi ludźmi zwiększa prawdopodobieństwo, że im pomożemy; Dlatego sensowne jest, aby osoby nadzorujące bezpieczeństwo poznały personel, od którego potrzebują wsparcia. Zachęcanie do aktywności towarzyskiej w biurze (np. grup dyskusyjnych w porze lunchu, przyjęć okolicznościowych i projektów charytatywnych) wzmacnia relacje międzyludzkie i może poprawić klimat do skutecznego szkolenia w zakresie bezpieczeństwa. Zarządzanie przez spacerowanie to doskonała praktyka na wielu poziomach, w tym wspieranie przynajmniej pierwszego etapu relacji międzyludzkich wśród współpracowników.

Zgodność, zgodność i posłuszeństwo

Niektórzy negatywnie reagują na słowa „konformizm", „podporządkowanie się" i „posłuszeństwo", ale ignorowanie zjawisk społecznych nie pomoże praktykom bezpieczeństwa w osiągnięciu ich celów. Pomimo niepopularności tej dziedziny, warto zrozumieć, w jaki sposób ludzie mogą współpracować we wzmacnianiu polityki bezpieczeństwa. W kolejnych sekcjach przyjrzymy się, jak zwiększyć zgodność z kulturą współpracy w celu zwiększenia bezpieczeństwa, zgodność z racjonalnymi zasadami bezpieczeństwa oraz skłonność do posłuszeństwa wobec władz IA w sprawach bezpieczeństwa.

Presja społeczna i zmiana zachowania

Przekształcenie grupy w społeczność zapewnia ramy, w ramach których może działać presja społeczna w celu poprawy OW organizacji. Większość ludzi reaguje na opinie innych, przesuwając własne opinie, czasem nieświadomie, w stronę tego, co statystycy nazywają trybem – opinii najpopularniejszej. Programy bezpieczeństwa muszą dążyć do przesunięcia wartości normatywnych, sensu tego, co należy robić, w kierunku ochrony poufności, posiadania lub kontroli, integralności, autentyczności, dostępności i użyteczności danych. Według nieformalnej ankiety przeprowadzonej przez Mani Akella, współautora tego rozdziału, w trzech wiodących firmach finansowych na Wall Street, wnioski te wynikają z grupy testowej 80 respondentów:

* Starsi pracownicy wolą modelować swoje reakcje w oparciu o wspólne preferencje grupy, nawet jeśli niektóre reakcje są sprzeczne z ich własnym przeczuciem. Wydaje się, że uzasadnieniem tutaj jest to, że grupa zapewnia anonimowość, a nawet izoluje ich od reakcji kierownictwa. Młodsi pracownicy mają jednak tendencję do przeciwstawiania się grupowym trendom, gdy nie zgadzają się z proponowanymi koncepcjami.

* Przywództwo ma do odegrania dużą rolę – a grupa bardzo szybko modyfikuje swoje reakcje, aby dostosować się do zmian przywództwa. Jeśli lider lubi podążać określoną ścieżką i nie zadawać pytań, cała grupa ma tendencję do pozostawiania problemów i nie zakłócania równego tonu organizacji z obawy przed zakłóceniem liderowi, nawet kosztem ryzyka poważnych potencjalnych luk w zabezpieczeniach (zob. Sekcja 50.5.4 dotycząca myślenia grupowego). Jeśli jednak lider tworzy dynamiczne, otwarte i oparte na współpracy środowisko o wymiernej zdolności adaptacji do zmieniających się zagrożeń, grupa ożywia się dzięki innowacjom i dokłada dodatkowych starań, aby być na bieżąco (a nawet wyprzedzać) obecne zagrożenie.

* Kiedy liderzy wzywają jednostki do większych osiągnięć bez groźby karalnej reakcji, grupa reaguje pozytywnie. Przywództwo może stworzyć środowisko bezpieczeństwa, które może przekroczyć oczekiwania przedsiębiorstwa w zakresie bezpieczeństwa, zachęcając jednostki do zwiększania produktywności i nagradzania się większą satysfakcją z pracy. Bezpieczeństwo, podobnie jak większość

innych wysiłków związanych z zarządzaniem organizacją, dotyczy ludzi. Odpowiedzialny, zadowolony i świadomy personel w naturalny sposób prowadzi do lepszego ogólnego bezpieczeństwa organizacji.

Zmieniające się oczekiwania

Jak pokazały kampanie społeczne mające na celu eliminację jazdy pod wpływem alkoholu, zmiana trybu jest możliwa. W Stanach Zjednoczonych w połowie XX wieku wielu ludzi wierzyło, że prowadzenie pojazdu pod wpływem alkoholu jest zabawne; dziś pijany kierowca jest społecznym pariasem. Licealiści masowo popełniali samobójstwa w noce balów maturalnych; dziś wiele dzieci spontanicznie organizuje bezpieczne przejażdżki do domu. W podobny sposób musimy dążyć do uczynienia przestępstw komputerowych tak niesmacznymi jak publiczne pijaństwo. Tendencja do podobnych zachowań wzrasta, gdy ludzie w grupie lubią się lub podziwiają. Ponadto status społeczny jednostki w grupie wpływa na gotowość tej jednostki do dostosowania się do standardów grupy. Osoby o wysokim statusie (lubiane przez większość osób w grupie) i osoby o niskim statusie (nielubiane przez grupę) są bardziej utonomiczne i mniej uległe niż osoby lubiane przez jednych i nielubiane przez innych. Dlatego funkcjonariusze ochrony powinni zwracać szczególną uwagę na te wartości odstające podczas programów instruktażowych. Menedżerowie powinni dokładniej monitorować zgodność na obu końcach przedziału popularności. Jeśli praktyki w zakresie bezpieczeństwa są obecnie słabe, a do zmiany normy potrzebni są sojusznicy, najskuteczniejszym podejściem może być współpraca z osobami odstającymi w celu przeciwstawienia się uprzedzeniom większości wobec bezpieczeństwa. Najbardziej popularni ludzie mogą stać się niszczycielskimi agentami buntu, jeśli nie zapiszą się do programu bezpieczeństwa; paradoksalnie, najbardziej niepopularni ludzie mogą być pomocni, jeśli uda się ich przekonać do posłuszeństwa.

Norma wzajemności

Według psychologów społecznych norma wzajemności wskazuje, że w relacjach społecznych przysługi są zwykle odwzajemniane. Nawet niewielki, nieoczekiwany, nieoczekiwany lub nawet niechciany prezent zwiększa prawdopodobieństwo, że odpowiemy na prośby. Na przykład członkowie różnych kultów religijnych często rozdają kwiaty lub książki na lotniskach, wiedząc, że norma wzajemności zwiększy częstotliwość i ilość darowizn od w zasadzie niezainteresowanych przechodniów. Program podnoszenia świadomości w zakresie bezpieczeństwa obejmujący drobne upominki, takie jak atrakcyjny kubek z napisem „BEZPIECZEŃSTWO TO SPRAWA KAŻDEGO" lub niedroga, ale przydatna broszura podsumowująca zasady bezpieczeństwa, może pomóc zaangażować ludzi w kwestie bezpieczeństwa. Połączenie takich programów z nagrodami za zgodność może być potężnym narzędziem poprawy bezpieczeństwa. Połączenie wyrazu uznania z bezpośrednim kontaktem osobistym, zaczynającym się od stwierdzenia „Potrzebuję twojej pomocy", po którym następuje szczere przedstawienie sytuacji w zakresie bezpieczeństwa, może być pozytywne na wszystkich poziomach. Podejście to działa na wielu poziomach – nawiązywania relacji osobistych, budowania na normie wzajemności, zmiany schematu.

Przyrostowe zmiany.

Technika „stopa w drzwiach" sugeruje, że po małej początkowej prośbie powinna nastąpić druga, jeszcze większa. Na przykład politycy pracujący w terenie wiedzą, że mogą zacząć od drobnych pytań, prosząc ludzi o pozwolenie na umieszczenie naklejek kandydatów w ich oknie; następnie proszą o umieszczenie plakatu kandydata na swoim trawniku; w końcu mogą poprosić o czas lub pieniądze jako wolontariusze. Każde spełnienie prośby zwiększa prawdopodobieństwo, że dana osoba zgodzi się na następny krok w rosnącej serii. To tak, jakby zgoda na jeden krok pomogła zmienić samoświadomość celów. Aby zmniejszyć dyskomfort związany ze swoimi przekonaniami i zachowaniem (co psychologowie nazywają dysonansem poznawczym), ludzie zmieniają swoje przekonania, aby były

zgodne z ich zachowaniem. Pracownicy mogą zostać osobiście poproszeni o dawanie dobrego przykładu poprzez wygaszanie ekranów i blokowanie terminali przy opuszczaniu biurka. Później, gdy już rozpoczną proces redefinicji siebie („Jestem osobą, której zależy na bezpieczeństwie komputera"), można ich poprosić o coś bardziej intensywnego, na przykład o udział w szkoleniu dotyczącym bezpieczeństwa poprzez poproszenie innych o wygaszenie ekranów i zablokowanie terminali — lub nagradzanie tych, którzy to robią, słynnym czekoladowym smakołykiem. Stosując te same metody do różnych zadań, kultura korporacyjna może się zmienić w taki sposób, że większość ludzi poczuje się osobiście zaangażowana w dobre praktyki bezpieczeństwa. Niektórzy specjaliści ds. bezpieczeństwa zaproponowali, że nie powinniśmy prosić słuchaczy o zastanowienie. Rozumowanie jest takie, że każdy stopniowy krok polityki nie powinien wymagać od docelowych odbiorców uzasadnienia lub wyjaśnienia zachowania. Zamiast tego skup się na budowaniu odruchów warunkowych na określone czynniki środowiskowe i użytkowe. Organizacja i zespół ds. bezpieczeństwa powinni mieć większą pewność co do wspólnej i przewidywalnej reakcji na każde zagrożenie bezpieczeństwa ze strony każdej indywidualnej osoby wewnętrznej. Jednak przeciwny pogląd jest taki, że każde zachowanie proponowane w celu poprawy bezpieczeństwa musi być oparte na zrozumiałym schemacie. Innymi słowy, chociaż nie trzeba zmuszać słuchaczy do wyartykułowania uzasadnienia, zasady muszą mieć sens, jeśli mają być zintegrowane, zapamiętane i stosowane w dłuższej perspektywie.

ZACHOWANIE GRUPOWE

Niektóre grupy ludzi nazywane są zespołami, podczas gdy inne nazywane są gangami. Społeczno-psychologiczny wgląd w zachowania grupowe może poprawić wskaźniki sukcesu polityk dotyczących OW.

Pobudzenie społeczne

Badania nad behawioralnymi skutkami przebywania w grupach dały sprzeczne wyniki; czasami ludzie wykonywali swoje zadania lepiej, gdy w pobliżu byli inni ludzie, a czasami gorzej. W końcu psychologowie zdali sobie sprawę, że obecność innych ludzi jest podniecająca społecznie; to znaczy ludzie stają się bardziej świadomi zarówno własnego zachowania, jak i norm społecznych, gdy są w grupie. Pobudzenie społeczne ułatwia dobrze wyuczone nawyki, ale hamuje słabo wyuczone nawyki. Dlatego próbując nauczyć pracowników nowych nawyków w celu poprawy bezpieczeństwa, umieszczanie ich w dużych grupach przynosi efekt przeciwny do zamierzonego. Zindywidualizowane uczenie się (np. za pomocą szkoleń komputerowych i nagrań wideo) może przezwyciężyć hamujący wpływ grup na wczesnych etapach zmiany zachowania.

Umiejscowienie kontroli

Innym czynnikiem zakłócającym wdrażanie polityk bezpieczeństwa jest umiejscowienie kontroli. Ludzie nie lubią poczucia, że nie mają kontroli nad swoim otoczeniem. Na przykład w klasycznym eksperymencie opisanym w podręcznikach psychologii społecznej dwa równoważne zespoły ludzi zostały poddane głośnemu i uciążliwemu hałasowi dochodzącemu z głośnika w ich miejscu pracy. Jedna grupa nie miała żadnej kontroli nad hałasem, podczas gdy druga miała duży przycisk, za pomocą którego mogła natychmiast zatrzymać hałas. Grupa z przyciskiem stop radziła sobie zauważalnie lepiej ze złożonym zadaniem niż druga grupa – jednak w żadnym przypadku nikt nie nacisnął przycisku. Po prostu poczucie, że mogliby sprawować kontrolę, gdyby chcieli, znacząco zmieniło wydajność badanych eksperymentalnych.

Podobnie w badaniach nad gojeniem się starszych pacjentów zdefiniowano trzy grupy: (1) grupa kontrolna, (2) osoby, którym podano roślinę w doniczce, oraz (3) osoby, którym podano roślinę w doniczce oraz instrukcje dotyczące jej regularnego podlewania. Trzecia grupa radziła sobie znacznie

lepiej niż druga w odzyskiwaniu. Po raz kolejny okazało się, że poczucie kontroli nad otoczeniem wpływa na wyniki. We wdrażaniu polityki bezpieczeństwa doświadczenie potwierdza, że organizacje o największym udziale i zaangażowaniu wszystkich sektorów najlepiej radzą sobie z opracowywaniem i wdrażaniem planów ochrony informacji. Częstym zwrotem odnoszącym się do tego zjawiska jest „kupowanie", na przykład: „Przedstawiciele różnych departamentów uważali, że mogą naprawdę wkupić się w nowe zasady, ponieważ w pełni uczestniczyli w ich kształtowaniu"

Polaryzacja grupowa

Inna gałąź badań psychologii grup zajmuje się polaryzacją grupową. Grupy mają tendencję do podejmowania bardziej ekstremalnych decyzji niż pojedyncze osoby w grupie. W dyskusjach grupowych na temat potrzeby bezpieczeństwa polaryzacja może oznaczać podejmowanie decyzji o podjęciu większego ryzyka — poprzez ograniczenie lub zignorowanie kwestii związanych z bezpieczeństwem — niż jakakolwiek jednostka uznałaby za rozsądne. Ponownie, indywidualne dyskusje na temat potrzeby bezpieczeństwa będą generalnie bardziej skuteczne w budowaniu konsensusu, który wspiera opłacalne przepisy bezpieczeństwa, niż duże spotkania.

Myślenie grupowe

W skrajnych przypadkach grupa może wykazywać myślenie grupowe, w którym osiąga się konsensus z powodu silnego pragnienia spójności społecznej. Kiedy przeważa myślenie grupowe, odrzuca się dowody sprzeczne z przyjętym poglądem; opozycja jest postrzegana jako nielojalna; dysydenci są dyskredytowani. Szczególnie niepokojące dla specjalistów ds. bezpieczeństwa jest to, że osoby będące w uścisku myślenia grupowego mają tendencję do ignorowania ryzyka i nieprzewidzianych okoliczności. Aby zapobiec takim odchyleniom, lider musi pozostać bezstronny i zachęcać do otwartej debaty. Szanowani konsultanci ds. bezpieczeństwa z zewnątrz mogą zostać zaproszeni do przemówienia do grupy, wnosząc własne doświadczenia w celu uwzględnienia wymagań grupy. Po osiągnięciu konsensusu – a nie narzucaniu opinii osoby dominującej – grupa powinna spotkać się ponownie i skupić na zabawie w adwokata diabła, aby spróbować wymyślić dodatkowe wyzwania i alternatywy. Podsumowując, eksperci ds. bezpieczeństwa powinni zwracać uwagę na dynamikę grupy i być przygotowanym na przeciwdziałanie możliwym dysfunkcyjnym reakcjom, które kolidują z akceptacją zasad IA.

LUKI W POKONANIU TECHNOLOGICZNYM

W naszym społeczeństwie rosną przepaści społeczne między grupami społecznymi, które dorastały w interakcjach w rzeczywistych społecznościach (nieokablowane), grupami, które dorastały z Internetem (przewodowe), a najnowszą grupą dorastającą z zawsze dostępną technologią naszego złożone i bogate w treści bezprzewodowe sieci społecznościowe.

* Generacja bezprzewodowa. W dzisiejszym świecie wszechobecnej komunikacji bezprzewodowej czasami zapominamy o pokoleniu bezprzewodowym, urodzonym na początku lat 60. lub wcześniej, które dorastało, bawiąc się na świeżym powietrzu z przyjaciółmi i komunikując się twarzą w twarz. W przypadku tych starszych pracowników grupy dyskusyjne online, strumieniowe szkolenia wideo, blogi i poczta e-mail mogą nie być tak skuteczne, jak w przypadku innych, bardziej technologicznych grup. Pokolenie bez okablowania może postrzegać wykorzystanie bezosobowej technologii w szkoleniach jako wskaźnik apatii kierownictwa wobec tematu, któremu nie warto poświęcać czasu na interakcję w świecie rzeczywistym. Dla tego pokolenia, jeśli szkolenie w zakresie bezpieczeństwa jest ważne, ktoś powinien poświęcić czas, aby przeprowadzić je twarzą w twarz. Pokolenie pozbawione okablowania jest również najbardziej podatne na wiele technik i pułapek psychologii społecznej.

* Pokolenie przewodowe. Osoby urodzone od początku lat 60. do późnych lat 70. to pokolenie przewodowe. To pokolenie przejściowe dorastało u zarania Internetu, od dostępu dial-up o szybkości 300 bodów do ISDN. Od MS DOS do Windows 98 i od Cobola do C++, ta generacja jest pomostem między światem rzeczywistym a cyberświatem. To pokolenie jest również pokoleniem, które obecnie dochodzi do władzy zarówno w biznesie, jak iw rządzie. Pokolenie przewodowe, choć przyzwyczajone do spotkań twarzą w twarz w ważnych sprawach, żyje z poczty elektronicznej i telefonów komórkowych, tolerując zarówno przewodowe, jak i bezprzewodowe metody komunikacji i uczenia się.

* Generacja zawsze dostępna. Osoby urodzone po 1980 roku to pokolenie zawsze aktywne. To pokolenie dorastało z szybkim Internetem, telefonami komórkowymi, grami wideo, przenośną elektroniką i wirtualnymi społecznościami online. To jest połączona, połączona w sieć, Facebook, generacja gier wideo. Wydaje się, że to właśnie ta generacja zakłóca tradycyjną kontrolę bezpieczeństwa i politykę wdrażania.

Chociaż generacje przewodowe i bezprzewodowe mają wspólne psychologiczne korzenie w prawdziwym świecie, pokolenie zawsze aktywne ma dwa domy: świat rzeczywisty i cyberświat. Dzięki wiadomościom błyskawicznym (IM), wiadomościom tekstowym (Short Message Service lub SMS) i komórkowej łączności bezprzewodowej, to pokolenie porusza się w cyberprzestrzeni i poza nią, tak jak poprzednie pokolenie poruszało się między światem pracy i domu. Co więcej, podobnie jak poprzednie pokolenia, pokolenie „zawsze aktywne" ma inne ramy psychologiczne i socjologiczne dla swoich światów, co stanowi poważny problem w zakresie zapewniania informacji. Dla pokoleń bez i przewodowych komunikacja osobista oznaczała twarzą w twarz. Dla nieustannego pokolenia osobistego komunikacja oznacza komunikatory internetowe, pocztę e-mail i smartfony. Ponadto interakcje społeczne często oznaczają sieci społecznościowe, blogi, strony internetowe, fora dyskusyjne i wiki. Dodaj do tego fakt, że pokolenie, które jest zawsze aktywne, ma zdolność szybkiego przesyłania informacji między ich ściśle zintegrowanymi światami, a otrzymasz składniki koszmaru oficera ochrony. Rozpoznanie tych różnic i odpowiednie reagowanie może przynieść znaczne korzyści zarówno pod względem przestrzegania zasad bezpieczeństwa, jak i ogólnego sukcesu w zarządzaniu. Pierwszym krokiem może być upewnienie się, że zespoły ds. bezpieczeństwa obejmują członków z więcej niż najstarszego pokolenia w przedsiębiorstwie; młodsi ludzie mogą być w stanie działać jako pośrednicy lub tłumacze między coraz bardziej odmiennymi kulturami.

PODSUMOWANIE ZALECEŃ

Tu dokonano przeglądu głównych odkryć psychologii społecznej, które mogą pomóc w ulepszeniu programów OW. Te pomysły mogą okazać się przydatne dla czytelników, którzy myślą o psychologii społecznej podczas pracy nad wdrażaniem zasad bezpieczeństwa:

* Uznaj, że zasady IA często stoją w konflikcie ze schematem ufnego, uprzejmego zachowania w sytuacjach poza miejscem pracy.

* Przeszkol personel IA w rozpoznawaniu, że nieprzestrzeganie zasad bezpieczeństwa może wynikać z wielu innych czynników niż zwykłe złe nastawienie.

* Słuchaj więcej niż rozkazujesz.

* Naucz pracowników ochrony, aby unikali klasycznych błędów atrybucji, próbując zrozumieć motywacje swoich kolegów.

* Otwarcie dyskutuj i przeciwstawiaj się uprzedzeniom, zanim spowodują one konflikty.

* Weź pod uwagę różnice międzykulturowe przy ustalaniu i wdrażaniu zasad bezpieczeństwa.

* Przed przystąpieniem do wdrażania zasad i procedur należy zapewnić spójny pogląd na temat OW wśród współpracowników.

* O ile to możliwe, polityki bezpieczeństwa powinny być wprowadzane przez długi czas, a nie w pośpiechu.

* Przedstawienie studiów przypadku może mieć korzystny wpływ na gotowość uczestników do zbadania wymagań bezpieczeństwa.

* Programy uświadamiające w zakresie bezpieczeństwa powinny zawierać wiele realistycznych przykładów wymagań i naruszeń bezpieczeństwa.

* Spróbuj zainspirować zaangażowanie w bezpieczeństwo, a nie tylko je opisywać.

* Kładź nacisk na poprawę, a nie na zmniejszenie liczby niepowodzeń.

* Stwórz nową troskę o bezpieczeństwo korporacyjne, badając obecną strukturę przekonań wśród pracowników i menedżerów.

* Nigdy nie przedstawiaj przestępstw komputerowych za pomocą pozytywnych obrazów i słów.

* Chwal wszelkie komentarze, które są krytyczne wobec przestępstw komputerowych lub wspierają ustanowione zasady bezpieczeństwa.

* Pracownicy, którzy lekceważą obawy związane z bezpieczeństwem lub lekceważą przepisy, powinni być kwestionowani ze względu na ich postawę, a nie ignorowani.

* Zidentyfikuj kadrę kierowniczą wyższego szczebla, która z największym prawdopodobieństwem odniesie sukces w nadaniu pozytywnego tonu kolejnym szkoleniom w zakresie bezpieczeństwa i zaangażuj ich do współpracy, aby stanowili wzór do naśladowania.

* Przykłady przerażających konsekwencji użyte w materiałach informacyjnych i szkoleniowych należy natychmiast połączyć z opisami skutecznych i możliwych do osiągnięcia środków bezpieczeństwa, aby zapobiec takim konsekwencjom.

* Przedstawianie zastrzeżeń do propozycji i oferowanie kontrargumentów jest skuteczniejsze niż jednostronne diatryby.

* Programy uświadamiające o bezpieczeństwie powinny zawierać wiele częstych, a najlepiej nowatorskich i zabawnych przypomnień o kwestiach bezpieczeństwa.

* Oprócz taśm i książek polegaj na charyzmatycznym nauczycielu lub przywódcy, który pomoże wzbudzić entuzjazm dla lepszego bezpieczeństwa.

* Zachęcaj określonych pracowników do wzięcia publicznej odpowiedzialności za IA w swoich grupach roboczych.

* Okresowo zmieniaj role zabezpieczeń.

* Szkolenie w zakresie bezpieczeństwa powinno obejmować informacje o tym, jak stwierdzić, że ktoś może być zaangażowany w przestępstwo komputerowe.

* Zbuduj kulturę korporacyjną, która nagradza odpowiedzialne zachowanie, takie jak zgłaszanie naruszeń bezpieczeństwa.

* Opracuj jasno napisane zasady i procedury bezpieczeństwa.

* Procedury bezpieczeństwa powinny ułatwiać działanie zgodne z polityką bezpieczeństwa.

* Traktuj nieprzestrzeganie zasad i procedur bezpieczeństwa jako bardzo poważne sprawy.

* Egzekwowanie standardów bezpieczeństwa może zwiększyć prawdopodobieństwo, że pracownicy będą później działać w sposób bardziej skoordynowany.

* Środowisko pracy, w którym pracownicy są szanowani, bardziej sprzyja dobremu bezpieczeństwu niż takie, które ich dewaluuje i wykorzystuje.

* Poznaj personel, od którego potrzebujesz wsparcia.

* Zachęcaj do działań społecznych w biurze.

* Zwracaj szczególną uwagę na społeczne wartości odstające podczas programów instruktażowych.

* Dokładniej monitoruj zgodność na obu końcach zakresu popularności.

* Współpracuj z wartościami odstającymi, aby przeciwstawić się stronniczości grupy związanej z bezpieczeństwem.

* Uwzględnij drobne upominki w swoim programie uświadamiającym na temat bezpieczeństwa.

* Zacznij stopniowo poprawiać bezpieczeństwo i pracuj nad bardziej inwazyjnymi procedurami.

* Przed omówieniem kwestii bezpieczeństwa na spotkaniu przeprowadź indywidualną dyskusję z uczestnikami.

* Zachowaj bezstronność i zachęcaj do otwartej debaty na spotkaniach poświęconych bezpieczeństwu.

* Sprowadź ekspertów z zewnątrz w obliczu myślenia grupowego.

* Spotkaj się ponownie po zbudowaniu konsensusu i pobaw się w adwokata diabła.

* Rozpoznaj pokoleniowe luki technologiczne w naszej kulturze i odpowiednio się komunikuj; dlatego włącz osoby z różnych pokoleń do swoich zespołów ds. bezpieczeństwa.

Żadna z tych sugestii nie jest niezbędna; żaden z nich nie jest odpowiedni we wszystkich sytuacjach. Jednak budowanie na zgromadzonym doświadczeniu i mądrości psychologów społecznych ułatwi płynną integrację zapewniania informacji z każdą kulturą korporacyjną. Mamy nadzieję, że czytelnicy zapoznają się z literaturą z zakresu psychologii społecznej i organizacyjnej oraz wypróbują nowe pomysły, które w nadchodzących latach wzbogacą dziedzinę zapewniania informacji.