Ochrona przed przestępczością

Gdy przedsiębiorstwo biznesowe jest potencjalną ofiarą przestępstwa komputerowego, istnieje szereg środków, które można zastosować w celu ochrony firmy. W ankiecie Hagen i inni zajęli się zarówno oddechem, jak i głębokością w strategiach obronnych. Głębokość dotyczy zarówno środków technologicznych, jak i organizacyjnych, podczas gdy głębia dotyczy wymiarów zapobiegania, gotowości na wypadek sytuacji kryzysowych i wykrywania. Ankieta dotyczyła stosowania szerokiego zakresu technicznych środków bezpieczeństwa związanych z kontrolą dostępu i ochroną danych. Techniczne środki bezpieczeństwa obejmują zapobieganie (hasło, strefy fizyczne, uwierzytelnianie biometryczne i aktualizacja oprogramowania), awaryjne (kopia zapasowa) i wykrywanie (wykrywanie włamań i oprogramowanie antywirusowe). Organizacyjne środki bezpieczeństwa obejmują prewencję (prawa dostępu i wytyczne dla użytkowników), sytuacje awaryjne (plany zarządzania), wykrywanie (przeglądy dzienników) i reagowanie na incydenty (raporty z zarządzania). Badanie wykazało, że używanie haseł osobistych jest powszechne wśród wszystkich przedsiębiorstw, nawet tych najmniejszych:

Trend jest taki, że wraz z wielkością przedsiębiorstwa wzrasta wykorzystanie różnych mechanizmów kontroli dostępu. Istnieje również wyraźna tendencja, że duże przedsiębiorstwa wdrażają więcej i szerszy zakres środków gotowości i wykrywania sytuacji kryzysowych. Wyniki pokazują, że małe przedsiębiorstwa powinny wzmocnić kontrolę dostępu i środki ochrony danych, oprócz procedur bezpieczeństwa.

Hagen i inni uznali za zaskakujące, że duże przedsiębiorstwa nie radzą sobie lepiej niż małe przedsiębiorstwa, jeśli chodzi o podnoszenie świadomości i edukację użytkowników jako organizacyjne środki bezpieczeństwa.

Profilowanie kryminalne

Profilowanie przestępców opiera się na założeniu, że osoba popełniająca przestępstwo w cyberprzestrzeni przy użyciu komputera może pasować do określonego zarysu lub profilu. Profil składa się z cech przestępcy, które reprezentują założenia dotyczące osobowości i zachowania przestępcy. Cechy mogą obejmować budowę fizyczną, płeć przestępcy, etykę pracy, środek transportu, historię kryminalną, poziom umiejętności, rasę, stan cywilny, pasywność/agresywność, historię medyczną i miejsce zamieszkania przestępcy w związku z przestępstwem. Nykodym i inni rozróżniają cztery główne kategorie cyberprzestępczości: szpiegostwo, kradzież, sabotaż i osobiste nadużycia w sieci organizacyjnej:

W przeciwieństwie do sabotażystów i szpiegów złodziej kieruje się wyłącznie pobudkami kupieckimi dla własnej korzyści. Jedynym celem stojącym przed cyberzłodziejem jest kradzież cennych informacji z organizacji, a następnie ich wykorzystanie lub sprzedaż za pieniądze.

W zakresie profilowania kryminalnego Nykodym i inni odkryli, że wiek tych cyber-rabusiów jest silny. Jeśli przestępstwo opłaci się za mniej niż sto tysięcy dolarów, najprawdopodobniej napastnikiem jest młody mężczyzna lub kobieta w wieku 20-25 lat, wciąż na niskim poziomie hierarchii organizacji. Jeśli przestępstwo wiąże się z większymi pieniędzmi, sprawcą jest prawdopodobnie starszy mężczyzna z kierownictwa w organizacji. Jego zbrodnią nie jest nienawiść czy zemsta, ale chciwość i głód pieniędzy.

Przestępcy w białych kołnierzykach

Przestępstwo komputerowe jest definiowane jako przestępstwo finansowe. „Białe kołnierzyki" popełniają przestępstwa finansowe. Cechy charakterystyczne przestępców w „białych kołnierzykach" obejmują:

• Zamożna, ale chciwa osoba

• Wysoce wykształcona, ale praktyczna osoba

• Osoba powiązana społecznie, ale aspołeczna

• Mówi o etyce, ale działa niemoralnie

• Zatrudniony przez i w legalnej organizacji

• Osoba szanowana o wysokim statusie społecznym

• Członek uprzywilejowanej klasy społeczno-ekonomicznej

• Popełniać przestępstwo w zawodzie na podstawie kompetencji

• Na śliskim zboczu od zachowania zgodnego z prawem do niedozwolonego

• Często charyzmatyczny, przekonujący i posiadający umiejętności społeczne

• Tak zdesperowani, by odnieść sukces, że są gotowi użyć środków przestępczych

• Czasami podekscytowany dreszczem związanym z nieodkryciem

• Często w sytuacji, gdy policja niechętnie rozpoczyna dochodzenie

• Wykorzystuje zasoby, aby ukryć ślady i wyniki przestępstw

• Zachowuje się w sądzie w sposób wywołujący sympatię i zrozumienie

Tego rodzaju cechy są uporządkowane według kryteriów profilowania kryminalnego. Na przykład niektóre z nich są czynnikami indywidualnymi zakorzenionymi w psychologii, podczas gdy inne są czynnikami środowiskowymi zakorzenionymi w socjologii. W zakresie czynników psychologicznych profilowanie kryminalne może stawiać pytania takie jak:

• Jakie typy osobowości łatwiej stają się przestępcami w białych kołnierzykach?

• Jakie są ich typowe pochodzenie, styl życia i rozwój?

• Jakie są ich wartości, pomysły i ambicje?

W zakresie czynników socjologicznych profilowanie kryminalne może wiązać się z pytaniami takimi jak:

• Jak przestępcy umysłowi patrzą na społeczeństwo i swoją rolę w społeczeństwie?

• Jak postrzegają prawo i co uważają za przestępstwo i przestępców?

• W jaki sposób uczestniczą w sieciach i co jest związane ze statusem i władzą?

Nie wszyscy przestępcy komputerowi są przestępcami „białymi kołnierzykami", ale większość z nich popełnia przestępstwo dla zysku finansowego. Cyberprzestępcy mogą mieć szerszy zakres cech społecznych, a przypadki włamań i innych przestępstw związanych z Internetem, które zostały zgłoszone w mediach, sugerowałyby, że prawdopodobnie są to młode, mądre i dość samotne osoby, które są w średnim wieku. pochodzenie klasowe, często bez wcześniejszych rejestrów karnych, często przetwarzające wiedzę ekspercką i często motywowane różnymi celami finansowymi i niefinansowymi. Do popełnienia wielu rodzajów przestępstw komputerowych wymagany jest pewien stopień kompetencji technicznych

Teoria odstraszania

Niektórzy teoretycy uważają, że przestępczość można zmniejszyć, stosując środki odstraszające. Cel odstraszania, zapobiegania przestępczości, opiera się na założeniu, że przestępcy lub potencjalni przestępcy dokładnie zastanowią się przed popełnieniem przestępstwa, jeśli istnieje prawdopodobieństwo złapania i/lub obawa przed szybką i surową karą. Opierając się na takim przekonaniu, ogólna teoria odstraszania utrzymuje, że przestępstwo można udaremnić groźbą kary, podczas gdy specjalna teoria odstraszania głosi, że kary za czyny przestępcze powinny być wystarczająco surowe, aby skazani przestępcy nigdy nie powtórzyli swoich czynów. Zagrożenie to bodziec zewnętrzny, który istnieje niezależnie od tego, czy osoba je dostrzega. Jeśli dana osoba dostrzega zagrożenie, ma potencjał odstraszający. Teoria odstraszania postuluje, że ludzie popełniają takie przestępstwa na podstawie racjonalnych kalkulacji postrzeganych korzyści osobistych, a groźba sankcji prawnych będzie odstraszać ludzi z obawy przed karą. W ostatnich latach, kiedy dyrektorzy byli aresztowani i skuwani kajdankami w celu publicznego poniżenia, wprowadza to odstraszający model zapobiegania przestępczości lub przynajmniej politykę zawstydzania. Cele tych publicznych aresztowań są często symboliczne i mówią więcej o agencjach regulacyjnych, które muszą wyglądać, jakby legalnie ścigały korporacyjnych przestępców. W związku z tym, przy regulacjach tak ściśle powiązanych z klimatem politycznym, nie ma spójności w ściganiu przestępców korporacyjnych w porównaniu z polityką wojny narkotykowej z ostatnich kilku dekad. Odstraszający model zapobiegania przestępczości opiera się na założeniu, że potencjalni sprawcy odpowiadają na koszty i korzyści przestępstwa. Osoby podejmujące decyzję o popełnieniu przestępstwa ważą koszty i korzyści, a następnie wybierają przestępstwo, gdy jest ono opłacalne. W modelu przestępca racjonalnie maksymalizuje swoją oczekiwaną użyteczność. Czyn przestępczy z całą pewnością wyrządza szkodę osobom trzecim, a sprawcy grozi niepewna kara. Decyzja o zaangażowaniu się w działalność przestępczą zależy od wielkości oczekiwanego zysku z popełnienia czynu w stosunku do oczekiwanej kary. Jeżeli oczekiwana użyteczność przekracza oczekiwaną sankcję, jednostka popełnia czyn przestępczy. Norweski Krajowy Urząd Śledczy i Ścigania Przestępstw Gospodarczych i Środowiskowych (Økokrim) jest centrum zasobów dla policji i prokuratury w zwalczaniu tego rodzaju przestępstw. Økokrim została założona w 1989 roku i jest zarówno wyspecjalizowaną agencją policyjną, jak i prokuraturą z władzą krajową. Większość zasobów Økokrim poświęcona jest pracy nad konkretnymi sprawami karnymi. Formalne zasady dotyczące Økokrim można znaleźć w rozdziale 35 Instrukcji Prokuratury. Głównym celem Økokrim jest zwalczanie przestępczości gospodarczej, przestępczości przeciwko środowisku i praniu dochodów z przestępstwa. Økokrim zatrudnia około 136 pracowników. Jednym z ich celów jest odstraszanie. Chociaż pracują nad konkretnymi sprawami karnymi, starają się pokazać opinii publicznej, że każdy, kto łamie przepisy w obszarze jurysdykcji finansowej i informatycznej, będzie podlegał karom. Yusuf i Babalola zastosowali teorię odstraszania, aby zaproponować strategię kontroli oszustw ubezpieczeniowych. Teoria odstraszania postuluje, że ludzie popełniają przestępstwa finansowe na podstawie racjonalnych kalkulacji postrzeganych korzyści osobistych, a groźba sankcji prawnych (wraz z, jak wspomniano, surowością i szybkością kary sprawcy) będzie odstraszać ludzi z obawy przed karą. W literaturze teoretycznej na temat oszustw ubezpieczeniowych zidentyfikowano dwa strategiczne podejścia odstraszania: kontraktowanie i audyt. Dlatego strategia powinna koncentrować się na tych dwóch elementach:

• Odstraszanie poprzez projektowanie umowy. Po pierwsze, umowa powinna być zaprojektowana w taki sposób, aby mówienie prawdy wszystkim aktorom było optymalne. Ponieważ składka płacona przez osobę fizyczną jest bezpośrednio związana z cechami wybranej umowy, optymalna ochrona ubezpieczeniowa polega na zbilansowaniu skutków składki dodatkowej z efektem dodatkowej ochrony. Następnie umowa powinna być zaprojektowana w sposób minimalizujący koszty audytu. Po trzecie, projekt umowy powinien kryminalizować nieuczciwe zachowania i wiązać się z nałożeniem kary na nieuczciwą stronę. Wreszcie, podejście pokusy nadużycia/przestępstwa proponuje projekt umowy,

który pociąga za sobą karę za angażowanie się w oszukańcze roszczenia wobec ubezpieczonego oportunistycznie.

• Odstraszanie poprzez audyt. Roszczenia ubezpieczeniowe, które mają obserwowalne cechy, które wiążą się z możliwością oszustwa, powinny być dokładnie zbadane. Następnie te roszczenia ubezpieczeniowe, które okażą się nieważne, powinny zostać odrzucone. W przeciwnym razie kontrola może być nieskuteczna jako środek odstraszający. Na tym etapie należy wprowadzić zarządzanie wiedzą w postaci hybrydowego systemu opartego na wiedzy i statystyce, wykorzystującego techniki odkrywania wiedzy. Po pierwsze, system integruje wiedzę ekspercką z oceną informacji statystycznych w celu identyfikacji przypadków nietypowego zachowania dostawcy. Następnie system wykorzystuje uczenie maszynowe do opracowywania nowych reguł i usprawniania procesów identyfikacji.

Naruszenia bezpieczeństwa systemów informatycznych pracowników i przestępczość to poważny problem, który został zbadany przez teorię odstraszania. Zakłada się, że wykrywanie i karanie sprawców ogranicza nadużycia komputerowe. Oczekuje się, że stosowanie środków odstraszających związanych z bezpieczeństwem systemów informatycznych spowoduje zmniejszenie liczby przestępstw komputerowych wśród pracowników

Teoria neutralizacji

Potencjalni przestępcy stosują pięć technik neutralizacji: zaprzeczenie odpowiedzialności, zaprzeczenie zranienia, zaprzeczenie ofierze, potępienie skazańców i odwołanie się do wyższej lojalności. To jest oryginalne sformułowanie teorii neutralizacji. Później dodano metaforę księgi i technikę niezbędnej obrony. Metafora księgi wykorzystuje ideę kompensowania złych czynów dobrymi czynami. Według Heatha, przestępcy umysłowi mają tendencję do stosowania technik neutralizacji stosowanych przez przestępców, aby zaprzeczać przestępczości swoich działań. Przykładami technik neutralizacji są (a) odmowa odpowiedzialności, (b) odmowa zranienia, (c) odmowa ofierze, (d) potępienie skazań, (e) odwołanie się do wyższej lojalności, (f) wszyscy inni robią i (g) roszczenie o uprawnienie. Sprawca może domagać się prawa do postępowania tak, jak to zrobił, albo dlatego, że podlegał moralnemu obowiązkowi, albo z powodu jakiegoś występku popełnionego przez ofiarę. Te wymówki są stosowane zarówno w przypadku przestępczości zawodowej, jak i przestępczości korporacyjnej, zarówno na poziomie zgniłych jabłek, jak i na poziomie zgniłych beczek. Siponen i Vance opisują pięć podstawowych technik w następujący sposób:

1. Odmowa odpowiedzialności oznacza, że osoba popełniająca dewiacyjny czyn określa się jako pozbawiona odpowiedzialności za swoje czyny. Osoba uzasadnia, że dane działanie jest poza jego kontrolą. Dewiant postrzega siebie jako piłkę bezradnie kopaną w różnych sytuacjach.

2. Odmowa zranienia oznacza, że dana osoba usprawiedliwia działanie, minimalizując szkody, jakie powoduje. Osoby, które dopuszczają się przestępstw komputerowych, mogą zaprzeczać krzywdzie ofiarom, twierdząc, że atak na komputer nie wyrządza żadnej szkody ludziom.

3. Obrona przed koniecznością zakłada, że łamanie zasad jest postrzegane jako konieczne, a zatem nie należy czuć się winnym popełniając czyny. W ten sposób sprawca może odłożyć na bok poczucie winy, wierząc, że czyn był konieczny i nie miał innego wyboru. W przypadku przestępczości komputerowej pracownicy mogą twierdzić, że nie mają czasu na przestrzeganie zasad ze względu na napięte terminy.

4. Potępienie skazańców oznacza, że neutralizację osiąga się przez obwinianie tych, którzy są celem czynu. Na przykład można łamać prawo, ponieważ prawo jest nierozsądne, lub można złamać zasady bezpieczeństwa systemów informatycznych, które są nieuzasadnione. Sprawcy przestępstw komputerowych mogą twierdzić, że prawo jest niesprawiedliwe.

5. Odwołanie się do większej lojalności oznacza dylemat, który musi zostać rozwiązany kosztem naruszenia prawa lub polityki. W kontekście organizacyjnym pracownik może odwoływać się do wartości lub hierarchii organizacyjnych. Na przykład pracownik może argumentować, że musi naruszyć zasady, aby wykonać swoją pracę.

Ochrona przed przestępczością komputerową jest kwestionowana przez teorię neutralizacji. Potrzebne są techniki, które mogą hamować neutralizację. Siponen i Vance sugerują, że odpowiednie wyjaśnienie uzasadniające politykę organizacyjną poprzez seminaria, mediację ofiara-przestępca i przekonującą dyskusję może być użytecznym sposobem zmiany zachowania. W odniesieniu do zaprzeczenia kontuzji, mediacje ofiara-przestępca lub przekonująca dyskusja uświadamiają przestępcom, że doszło do urazu. W odniesieniu do odmowy odpowiedzialności przełożeni w kontaktach jeden na jeden i prelegenci na seminariach firmowych muszą podkreślać, że nie ma usprawiedliwienia dla przestępstw komputerowych. Jeśli chodzi o obronę konieczności, menedżerowie powinni podkreślać pracownikom, że nawet pod presją napiętego terminu nie ma usprawiedliwienia dla karnego skrótu. W odniesieniu do apelu o większą lojalność, menedżerowie ds. bezpieczeństwa w organizacjach muszą zapewnić, aby liderzy zespołów i kierownicy liniowi nie wspierali swoich podwładnych w łamaniu zasad bezpieczeństwa systemów informatycznych w celu wykonania ich pracy. Techniki neutralizacji można znaleźć we wszystkich rodzajach przestępstw komputerowych, w tym w internetowym uwodzeniu dzieci. Na przykład D'Ovidio i inni badali techniki neutralizacji, które są wykorzystywane do promowania, popierania i przekazywania informacji wspierających relacje seksualne między dorosłymi a dziećmi. Techniki neutralizacji obejmowały odwoływanie się do większej lojalności, potępianie skazańców i zaprzeczanie krzywdy. Wiele z przebadanych stron internetowych dla dorosłych i dzieci odwoływało się do większej lojalności, aby uzyskać akceptację dla swoich działań poprzez linki do stron ruchów społecznych niezwiązanych z aktywizmem pedofilii lub przyczynami wspierania relacji seksualnych między dorosłymi a dziećmi. W badaniu piractwa muzycznego Higgins i inni stwierdzili powiązanie między zasięgiem piractwa a zasięgiem neutralizacji. Stwierdzono, że poziom i zmiany w neutralizacji przez jednostkę mają bezpośredni wpływ na poziom i zmianę piractwa muzycznego przez tę osobę w czasie. Silniejsza neutralizacja spowodowała więcej piractwa muzycznego. Aby zmniejszyć liczbę przypadków piractwa muzycznego, sposób, w jaki jednostki postrzegają swoje zachowanie, jest kluczem do zmniejszenia liczby przypadków. Jeśli nielegalność takiego zachowania zostanie wzmocniona wśród młodzieży przed uczestnictwem w tym zachowaniu, prawdopodobieństwo, że będą oni uczestniczyć w piractwu muzycznym, zwłaszcza w sposób częsty i regularny, powinno zostać zmniejszone. W badaniu Moore'a i McMullan'a dodano jeszcze pięć technik neutralizacji:

1. Techniki księgi używa się, gdy osoba twierdzi, że jej nieodpowiednie zachowanie jest czasami akceptowalne, ponieważ spędza większość czasu na wykonywaniu dobrych i zgodnych z prawem uczynków. Osoba rozwija rezerwę dobrych uczynków, które przysłaniają jeden zły uczynek.

2. Zaprzeczenie konieczności prawa dowodzi, że prawo było wynikiem prób uregulowania zachowań przez szersze społeczeństwo, które nie miały nic wspólnego z wyższym dobrem ludzi. W rezultacie prawo zostało uznane za niewłaściwe i niewarte posłuszeństwa.

3. Robią to wszyscy inni, co oznacza, że jednostka czuje, że istnieje tak duży brak szacunku dla prawa, że ogólny konsensus jest taki, że prawo jest unieważnione lub uznane za nieważne.

4. Technika uprawniająca jest stosowana przez osoby, które czują, że są uprawnione do angażowania się w działalność z powodu pewnych względów w ich życiu.

5. Obrona konieczności jest stosowana, gdy jednostka uważa, że czyn jest konieczny, aby zapobiec jeszcze większemu czynu karalnemu.

Osoba stosuje techniki neutralizacji, gdy istnieje wątpliwość, czy coś jest nie tak z jej zachowaniem. Jeśli nie ma winy do zneutralizowania, to jest zrozumiałe, że nie ma potrzeby stosowania technik neutralizacji.

Regulacja i reakcja

Przestępczość komputerowa nie jest tak widoczna jak przestępczość konwencjonalna, a jej wykrycie jest trudne. Na przykład w sprawie o zabójstwo na ogół istnieje ciało i dowody sądowe. W przypadku przestępstw finansowych Hansen przekonuje, że rachunkowość i informatyka śledcza są obecnie najlepszymi narzędziami wykrywania i wdrożonymi w większości dochodzeń prowadzonych w ostatnich latach w białych kołnierzykach. Wzrasta zastosowanie nauki i technologii w sprawach dotyczących przestępczości białych kołnierzyków, a postęp technologiczny doprowadził do większego uzależnienia od zeznań biegłych w sprawach dotyczących przestępczości białych kołnierzyków, pamiętając, że opinii biegłych nie można wydać z absolutną pewnością. Być może, argumentuje Hansen, ze względu na środki finansowe na obronę swoich spraw, jakimi dysponują elitarne osoby i korporacje, które zostają postawione przed wymiarem sprawiedliwości, a także niechęć do negatywnego rozgłosu, negocjowanie zarzutów przed postawieniem zarzutów jest bardziej intensywne w porównaniu z konwencjonalnymi sprawami kryminalnymi. Formalne oskarżenie jest bardziej prawdopodobne, że prokuratorzy uznają je za niepowodzenie ze względu na większą liczbę zasobów, które prokuratorzy muszą przeznaczyć na ściganie spraw dotyczących przestępstw białych kołnierzyków. Również ze względu na większe piętno związane z więzieniem lub więzieniem dla elit, mogą one niechętnie negocjować ugodę, jeśli w umowie uwzględniono uwięzienie. Z drugiej strony nie jest niczym niezwykłym, że skazani oskarżeni nagle decydują się na współpracę w dochodzeniu w celu uzyskania złagodzenia kary.

Reakcja wymiaru sprawiedliwości w sprawach karnych

Ścigając korupcję i zorganizowane grupy przestępcze zajmujące się wymuszeniami na rynku pracy, Departament Sprawiedliwości Stanów Zjednoczonych poszukuje nowych sposobów myślenia o starych przestępstwach. Toner opisuje, w jaki sposób prokuratorzy kryminalni w USA rozszerzyli zakres ustaw federalnych karających oszustwa i wymuszenia w celu zwalczania wpływów zorganizowanych grup przestępczych w niektórych amerykańskich związkach zawodowych i programach świadczeń pracowniczych. Prokuratorzy wykorzystywali przestępstwa oszustwa i wyłudzeń w nowatorski sposób, na podstawie indywidualnych przypadków, w celu ścigania korupcji w sektorze pracy w USA. Uważnie przekonując sędziów procesowych, sądy apelacyjne i Kongres USA o zaletach spojrzenia na oszustwa i wymuszenia w nowy sposób, prokuratorzy federalni zrealizowali intencję ustaw, które Kongres uchwalił w celu zwalczania korupcji w rządzie, biznesie, i związki zawodowe. Przestępstwa finansowe, takie jak oszustwa podatkowe, mogą być popełniane poprzez ukrywanie dochodów w krajach o niskich podatkach. Amerykańskie prawo dotyczące podatku dochodowego jest jednak takie, że ma czelność nakładać podatki na obywateli i rezydentów USA od ich światowych dochodów. Skutkuje to umiędzynarodowieniem amerykańskiego podatku dochodowego i stanowi swoiste wyzwanie dla osób odpowiedzialnych za egzekwowanie prawa, w szczególności w zakresie pozyskiwania informacji o zagranicznych rachunkach bankowych. Cihlar stwierdził, że sądy USA w odpowiednich okolicznościach nie są niechętne nakazaniu zagranicznemu bankowi mającemu siedzibę w USA przedstawienia informacji o kontach i innych rejestrach prowadzonych za granicą. Podobne kwestie, o których mówił Cihlar w USA, pojawiły się w Wielkiej Brytanii. Pytanie brzmi, czy iw jaki sposób należy prowadzić ściganie przestępstw finansowych w wielu jurysdykcjach w erze elektronicznej. Historycznie, sądy brytyjskie zdecydowanie opowiadały się za zasadą terytorialności, aby ściśle ograniczyć założenie jurysdykcji karnej do przestępstw, które miały miejsce w całości w ramach jurysdykcji. Wraz z szybkim postępem technologii informacyjno-komunikacyjnych, a także przestępczością międzynarodową, tak

wąskie podejście do jurysdykcji stało się niewykonalne, ponieważ coraz więcej przestępstw finansowych ma aspekty wielosądowe. Hodgson twierdzi, że jeśli nie zostanie przyjęty spójny i racjonalny sposób ustalania priorytetów roszczeń konkurujących jurysdykcji dotyczących tego samego postępowania przestępczego, istnieje ryzyko, że pierwsza jurysdykcja, która może dokonać aresztowania, niekoniecznie musi być właściwa lub najwłaściwsza. jeden. Twierdzi, że zajmując się przestępstwami międzynarodowymi, organy ścigania powinny starać się koordynować między sobą wysiłki, aby zapewnić wszczynanie postępowań karnych w różnych jurysdykcjach w najkorzystniejszej kolejności lub kolejności. Reakcja wymiaru sprawiedliwości w sprawach karnych na cyberprzestępczość obejmuje jednostki policyjne zajmujące się cyberprzestępczością. Hinduja określiła ilościowo liczbę takich jednostek amerykańskich, które znajdują się w sieci WWW i opisała sposób, w jaki się reprezentują. Odkrycia sugerują, że chociaż jednostki ds. cyberprzestępczości w USA zazwyczaj mają podobne misje (np. reagowanie na jedną lub więcej form przestępczości komputerowej), korzystały one ze swojej samodzielnej witryny internetowej na różne sposoby, aby przekazywać informacje swoim wyborcom. Pierwsza wyspecjalizowana jednostka Komisji Europejskiej ds. zwalczania nadużyć finansowych została utworzona w 1988 r. Quirke zbadał, w jaki sposób nowsza jednostka ds. zwalczania nadużyć finansowych w UE współpracuje z państwami członkowskimi i jak rozliczała się ze swoich działań. Badanie wykazało, że walka z nadużyciami finansowymi została śmiertelnie osłabiona przez wysoki stopień rozdrobnienia ze względu na mnogość zaangażowanych agencji krajowych i unijnych.

Rozporządzenie

Fletcher zbadał wyzwania związane z regulacją oszustw finansowych w cyberprzestrzeni. Badał osoby odpowiedzialne za oszustwo, możliwości ścigania oraz sytuację cyberprzestrzeni w świetle jurysdykcji i kontroli. Zagadnienia takie jak; kto jest odpowiedzialny za oszustwa internetowe, czy można zebrać wystarczające dowody, aby ścigać osoby popełniające oszustwa finansowe w cyberprzestrzeni, czy cyberprzestrzeń podlega własnej jurysdykcji i kto ją kontroluje; to są ważne perspektywy. Fletcher stwierdził, że wprowadzenie regulacji dotyczących internetu będzie przydatne w zwalczaniu oszustw w cyberprzestrzeni. Potrzebny jest konkretny ponadnarodowy program walki z cyberprzestępczością oparty na jego cechach charakterystycznych i ograniczony do kroków niezbędnych do usunięcia zidentyfikowanych uchybień. Larsson badał rozwój sytuacji w zakresie regulacji przestępczości gospodarczej w Norwegii. Metodologią jego badań były jakościowe wywiady eksperckie oraz analiza szerokiego zakresu publikacji dotyczących pracy tych urzędów. Odkrył, że w ciągu ostatnich dwóch dekad w Norwegii nastąpił znaczny wzrost zasobów, przepisów i regulacji dotyczących regulacji przestępczości gospodarczej. Nastąpiło przesunięcie regulacji z ogólnych porozumień i zachęt ze strony państwa w kierunku regulacji rynkowej, wspartej groźbą sankcji karnych i cywilnych. Segmenty gospodarki przeszły od postrzegania ich jako wytwórca wartości do miejsca przestępstwa. Regulacja i zapobieganie elitarnej przestępczości korporacyjnej ma zazwyczaj charakter reaktywny, a nie profilaktyczny. Ponadto, wraz ze spadkiem regulacji, pojawiają się szanse na przestępczość. Po skandalach związanych z wykorzystywaniem informacji poufnych w latach 80. Komisja Papierów Wartościowych i Giełd (SEC) przyjęła zasadę zakazującą oferentom i spółkom docelowym ujawniania informacji lub handlu w oparciu o fuzje i przejęcia lub negocjacje arbitrażowe. Podobnie ustawa Sarbanesa-Oxleya z 2002 roku powstała po klęsce Enronu i WorldComu. W ostatnich latach, kiedy dyrektorzy byli aresztowani i skuwani kajdankami w celu publicznego poniżenia, wprowadza to odstraszający model zapobiegania przestępczości lub przynajmniej politykę zawstydzania. Cele tych publicznych aresztowań są często symboliczne i mówią więcej o agencjach regulacyjnych, które muszą wyglądać, jakby legalnie ścigały korporacyjnych przestępców. W związku z tym, przy regulacjach tak ściśle powiązanych z klimatem politycznym, nie ma spójności w ściganiu przestępców korporacyjnych w porównaniu z polityką wojny narkotykowej z ostatnich kilku dekad. Odstraszający model zapobiegania przestępczości opiera się na założeniu, że potencjalni sprawcy odpowiadają na koszty i

korzyści przestępstwa. W modelu przestępca racjonalnie maksymalizuje swoją oczekiwaną użyteczność. Czyn przestępczy z całą pewnością wyrządza szkodę osobom trzecim, a sprawcy grozi niepewna kara. Decyzja o zaangażowaniu się w działalność przestępczą zależy od wielkości oczekiwanej korzyści z popełnienia czynu w stosunku do oczekiwanej kary. Jeżeli oczekiwana użyteczność przekracza oczekiwaną sankcję, jednostka popełnia czyn przestępczy. Araujo opracował model do badania opartego na zachętach podejścia do zapobiegania oszustwom w firmach. Teoria bodźców została wykorzystana do zaprojektowania mechanizmu, który sprawia, że pracownicy ujawniają swój prawdziwy typ, czyli chęć lub zdolność do walki z korupcją. Zastosowane w badaniu podejście do projektowania mechanizmów zakłada powierzenie kierownikowi lub zleceniodawcy uprawnienia do uczynienia pracowników agentami. Regulacje odegrały ważną rolę w falach przestępczości białych kołnierzyków, które dotknęły wiele rozwiniętych gospodarek. W latach 80. deregulacja w wielu krajach doprowadziła do powstania kreatywnych planów finansowych, niektórych legalnych, ale innych wyraźnie przestępczych. Handel informacjami poufnymi rzadko był badany lub ścigany przez agencje regulacyjne, mimo że był i jest nielegalny. Deregulacja jest postrzegana jako winowajca dopuszczający złe praktyki księgowe, w tym ukrywanie strat lub długów, jak w przypadku Enronu, a także zawyżanie zysków i aktywów. Zmiana regulacji w odpowiedzi na poważne przestępstwa korporacyjne jest jak zamykanie drzwi stodoły po ucieczce wszystkich owiec. Trudno jest powstrzymać nadużycia, zwłaszcza jeśli nagroda pieniężna nadal przeważa nad sankcjami. Według Hansena samoregulacja również nie wydaje się być rozwiązaniem. Wiele ocen, czy to dokonywanych przez grupy zewnętrzne, czy też wewnętrznie, ma charakter ceremonialny. Na przykład menedżerowie w firmie technologicznej mogą mieć tylko podstawową wiedzę z zakresu chemii, biologii lub komputerów, ale zatrudniać ekspertów technologicznych do wykonywania podstawowej pracy firmy. W innych przykładach istnieje konflikt interesów, jak w przypadku Arthura Andersena, który był zarówno audytorem, jak i płatnym konsultantem Enronu. Ponadto certyfikowane standardy nie okazały się skuteczne. Jednym z powodów jest częsty rozdźwięk między certyfikacją a stałą zgodnością.

Samoregulacja w zakresie prywatnej ochrony przestępczości gospodarczej również nie wydaje się być rozwiązaniem dla Williamsa. Zidentyfikował pięć barier dla tego rodzaju podejścia do zarządzania:

1. Tajemnica, słaba widoczność i uznaniowa sprawiedliwość prowadzą do nieformalnych negocjacji, łatwego zakończenia, luźnego łączenia dochodzeń z formalnymi ramami prawnymi oraz potencjalnych przywilejów dla niektórych osób, ale nie dla innych.

2. Wiele standardów prawnych i forum shopping prowadzi do standardów prawnych i proceduralnych, które zwykle różnią się w poszczególnych przypadkach, w zależności od wybranej drogi lub forum prawnego.

3. Wiele podmiotów prawnych o różnych referencjach i kwalifikacjach stosuje różnorodne kodeksy, standardy i obowiązki zawodowe i quasi-zawodowe.

4. Wielu interesariuszy i grupy interesu mają tendencję do występowania konfliktów interesów. Jednakże, aby mówić o rozliczalności i zarządzaniu, nieuchronnie konieczne jest przyjęcie określonego punktu widzenia.

5. Dychotomia publiczno-prywatna prowadzi do liberalnej tradycji prawnej, w której rozróżnienie na publiczne i prywatne pozostaje trwałym elementem myśli prawnej. Opiera się na dwóch powiązanych ze sobą zasadach, które mają bezpośredni wpływ na działalność śledczych wewnętrznych. Po pierwsze, korporacje mają takie same prawa jak osoby fizyczne, a zatem są definiowane jako prywatne podmioty prawne. Po drugie, istnieją fundamentalne ograniczenia władzy i jurysdykcji państwa, które uniemożliwiają niepotrzebne interwencje i wtargnięcia w sferę prywatną.

Podobnie jak Hansen i Williams, Schneider badał prywatyzację egzekwowania przestępstw gospodarczych, badając rolę agencji śledczych sektora prywatnego. Agencja dochodzeń finansowych odnosi się do organizacji sektora prywatnego działającej w oparciu o rachunkowość, która świadczy usługi dochodzeniowe, zarządzania ryzykiem, doradztwa i wsparcia w prowadzeniu postępowań sądowych w zakresie przestępczości gospodarczej. Szczególnym rodzajem samoregulacji jest samoobrona, w przypadku której ochronę potencjalnie osiąga się poprzez edukację aktorów. Przykładem jest ochrona inwestorów przez słabości pierwszych ofert publicznych (IPO). Solaiman argumentuje, że powszechnie wiadomo, że wiedza inwestycyjna umożliwia inwestorom ochronę przed winą emitentów, ich specjalistów i pośredników, zwanych strażnikami. Zdolność inwestorów do dokonywania ostrożnych osądów inwestycyjnych pod kątem alokacji zasobów jest uważana za ważny element w każdej gospodarce rynkowej. Solaiman argumentuje, że oprócz samoobrony istnieje potrzeba ochrony inwestorów przez organy regulacyjne. Ochronę inwestorów przez organy nadzoru papierów wartościowych można podzielić na dwie: ochronę pośrednią i bezpośrednią. Pierwszy odnosi się do upoważnienia inwestorów do ochrony siebie, podczas gdy drugi dotyczy ochrony przez regulatora poprzez tworzenie, administrowanie i egzekwowanie.

Prywatne działania policyjne związane z przestępczością finansową będą musiały opierać się na sprawiedliwości organizacyjnej postrzeganej przez członków organizacji. Scott i inni przekonali się, że ćwierć wieku badań nad sprawiedliwością organizacyjną ujawniło wiele na temat tego, jak pracownicy reagują na przestrzeganie i łamanie zasad sprawiedliwości przez ich menedżerów. Pracownicy oceniają sprawiedliwość w wielu wymiarach: sprawiedliwość wyników decyzji, sprawiedliwość procesów decyzyjnych, adekwatność wyjaśnień i postrzegana wrażliwość komunikacji interpersonalnej. Te wymiary są częścią tego, co Rodell i Colquitt nazywają sprawiedliwością antycypacyjną: sprawiedliwością dystrybutywną, sprawiedliwością proceduralną, sprawiedliwością informacyjną i sprawiedliwością interpersonalną. Skutki sprawiedliwości antycypacyjnej zostały zbadane w kontekście zmian organizacyjnych. Zmiana jest naturalnym elementem życia zawodowego pracowników, a pracownicy mogą doświadczać różnych zmian w trakcie swojej kadencji organizacyjnej, od zmian na dużą skalę, takich jak przenoszenie organizacji lub fuzje, po nowe zasady, takie jak zakazy świadczeń dodatkowych. W ramach sprawiedliwości antycypacyjnej Zapata-Phelan i inni badali sprawiedliwość proceduralną i wewnętrzną motywację wśród pracowników. To, co najbardziej wyróżnia się na tle wyników ich badań, to istotny związek między sprawiedliwością proceduralną a motywacją wewnętrzną. Relację wspierano za pomocą miernika samoopisowego oraz motywacji odniesienia zarówno do konkretnych zadań, jak i wieloaspektowych zadań w zakresie całokształtu obowiązków zawodowych. Takie relacje będą miały tendencję do wpływania na rolę i wydajność finansowych agencji śledczych. Schneider zaleca opracowanie polityk i programów publicznych, które pielęgnują zwiększoną i bardziej formalną rolę finansowych agencji śledczych w kontekście partnerstwa z agencjami rządowymi. W Norwegii publiczna debata w mediach wskazywała, że rola finansowych agencji śledczych powinna zostać zmniejszona, a więcej środków należy udostępnić policji . Hansen twierdzi, że zapobieganie przestępczości korporacyjnej nie powinno być jedynie przedmiotem troski organów regulacyjnych i organów ścigania. Korporacje mogą stracić więcej niż reputację, gdy pojawiają się skandale finansowe. Nawet jeśli przestępczość w białych kołnierzykach nie osiąga proporcji Royal Bank of Scotland, Enron czy WorldCom, korporacje są poszkodowane. Szacuje się, że przestępczość białych kołnierzyków może kosztować firmy średnio sześć procent rocznej sprzedaży. Podjęto kilka prób zapobiegania przestępczości korporacyjnej poprzez ponowne uregulowanie przepisów, a ustawa Sarbanesa-Oxleya z 2002 r. w Stanach Zjednoczonych była jedną z prób naprawienia niektórych problemów dotyczących ładu korporacyjnego, które wyszły na światło dzienne w przypadku Enronu. Prawo wymaga bardziej rygorystycznej rachunkowości wobec SEC, a

także uniemożliwia najwyższemu kierownictwu (dyrektorom generalnym, prezesom itp.) twierdzenie, że można zaprzeczyć, z powodu nieznajomości praktyk księgowych w ich firmach. Niestety, nie zapobiega to oszukańczemu raportowaniu do SEC lub akcjonariuszy, ale pociąga menedżerów bezpośrednio do odpowiedzialności za wykroczenia swoich pracowników księgowych, jeśli zostaną przyłapani. Ponadto zapobieganie przestępczości korporacyjnej i elitarnej jest skazane na niepowodzenie, jeśli jedynym zastosowanym rozwiązaniem będzie regulacja. Praktyki biznesowe nie mają miejsca w środowisku ścisłych regulacji. Są raczej niechlujne i nieuregulowane, a wyniki są mniej przewidywalne. Jednak branże skarżą się, że są nadmiernie regulowane, a rząd interweniuje (ma ograniczone zasoby i wsparcie) tylko wtedy, gdy kwestionuje się sytuację finansową i bezpieczeństwo pracowników, konsumentów i społeczeństwa. Ponadto, badając dewiacje samych organizacji, a nie osób, często istnieje cienka granica między tym, co jest przestępcze, a tym, co nie jest. Hansen stwierdza, że nawet przy zwiększonych przepisach i ściganiu przestępstw korporacyjnych, takich jak uchylanie się od podatku dochodowego i fałszywe wartości zapasów, a także surowych kar za naruszenie praw pracowniczych i bezpieczeństwa, nie jest zaskoczeniem, że osoby w organizacjach mają trudności z rozróżnieniem między nieetyczne i nielegalne. Wiele wykroczeń indywidualnych i korporacyjnych wymaga lat, aby zostać wykrytym, czego dowodzą skandale związane z handlem poufnymi informacjami na Wall Street w latach 80., a także skandal z Enronem. Kiedy demaskatorzy się zgłaszają, jest to wielokrotnie długo po fakcie, kiedy opuścili organizację i osiedlili się w innych korporacjach lub karierach. Przestępstwa korporacyjne są trudne do wykrycia z powodu skomplikowanych spisków w formie sieci społecznościowych. Osoby w organizacjach niekoniecznie działają w pojedynkę, popełniając przestępstwa. Podobnie jak działalność przestępcza, taka jak handel narkotykami, haraczy, prostytucja i hazard, prowadzona jest w ramach sieci przestępczych, tak elitarna przestępczość gospodarcza występuje w ramach złożonych relacji społecznych. Te elitarne sieci nie ograniczają się do członków społeczności biznesowej, ale obejmują także polityków i funkcjonariuszy organów ścigania. Niektórzy biznesmeni, którzy prowadzą przypuszczalnie legalne i całkowicie legalne przedsiębiorstwo, biorą udział jawnie lub potajemnie w działalność przestępczą. Niektórzy biznesmeni są finansistami operacji przestępczych. Egzekwowanie przepisów i sankcje stają się problematyczne, gdy politycy i agencje regulacyjne albo aktywnie współspisują, albo przymykają oko na nielegalną działalność. Kiedy korporacje i osoby fizyczne zostają „przyłapane na gorącym uczynku" i muszą rozliczać się ze swojego przestępczego zachowania, mają większe środki finansowe na zwalczanie zarzutów o wykroczenia i przestępczość niż pospolity przestępca. Karanie nie jest zgodne z przewidywalnym schematem zemsty lub rehabilitacji. Nawet ugody cywilne są dalekie od rzeczywistego zwrotu kosztów. Według Hansena wynika to w dużej mierze z nierówności istniejących w samym społeczeństwie, gdzie regulacje społeczne zarówno odzwierciedlają, jak i odtwarzają nierówności w ekonomii politycznej w ogóle, a zwłaszcza w strukturze społecznej organizacji biznesowych. Sugeruje to, że pozwani przedsiębiorcy generalnie doświadczają korzyści prawnych, które nie są dostępne dla oskarżonych o przestępstwa konwencjonalne. Nazywa się to czasem „brudną tajemnicą przestępczości": przeciętnego obywatela najbardziej niepokoi brutalne przestępstwa uliczne, które są wynikiem biedy, bezrobocia itp., podczas gdy korporacje ze świtą prawników, księgowych i ekspertów od public relations negocjują przepisy i prawo ponieważ funkcjonariusze organów ścigania, śledczy, sędziowie i prokuratorzy są łagodni wobec przestępstw popełnianych przez elity. Trzy rozwiązania do kontrolowania przestępczości korporacyjnej i białych kołnierzyków

1. Dobrowolna zmiana zarówno postaw korporacyjnych, jak i struktury. Specjaliści powinni być odpowiedzialni przed różnymi grupami zawodowymi, takimi jak lekarze, prawnicy i inne zawody. Innym czynnikiem odstraszającym przestępczość korporacyjną są społeczne, a nie prawne konsekwencje działalności przestępczej. Ponieważ elitarni przestępcy są właśnie tym - elitą - ich tożsamość społeczna jest zinstytucjonalizowana w zajmowanych przez nich warstwach społecznych, a wpływ kary

pozbawienia wolności jest zintensyfikowany. Innymi słowy, im są większe, tym mocniej spadają. Istnieje przekonanie, że nieformalne sankcje (tj. wydalenie ze społeczności zawodowej) w połączeniu z obawą przed formalną karą uniemożliwiają większości osób popełnianie przestępstw. Jednak w przeciwieństwie do swoich odpowiedników z przestępczości ulicznej, przestępcy umysłowi rzadko otrzymują długie wyroki pozbawienia wolności.

2. Silna interwencja państwa politycznego w celu wymuszenia zmian w strukturze korporacyjnej

3. Środki prawne mające na celu powstrzymanie lub ukaranie lub działania konsumenckie (szkodzenie korporacji w portfelu może być jedynym sposobem na zwrócenie ich uwagi).

Organizacje międzynarodowe, takie jak MFW i Bank Światowy, podchodzą do korupcji i innych przestępstw gospodarczych, zwracając uwagę na darczyńców, organizacje pozarządowe oraz rządy i obywateli, zwłaszcza w krajach rozwijających się, gdzie korupcja grozi osłabieniem oddolnego wsparcia dla pomocy zagranicznej. Podejście to ma cztery cele: zapobieganie nadużyciom finansowym i korupcji w ramach projektów finansowanych przez banki, pomoc krajom, które proszą o wsparcie bankowe w ich wysiłkach na rzecz ograniczenia korupcji, wyraźniejsze uwzględnianie korupcji w strategiach pomocy dla krajów oraz wspieranie międzynarodowych wysiłków na rzecz ograniczenia korupcji. Kayrak przekonuje, że do korupcji należy podejść kompleksowo, angażując wszelkie wysiłki, aby ją odstraszyć, ponieważ jest to zjawisko wielowymiarowe. Przedstawia teoretyczne ramy zaangażowania najwyższych organów kontroli (NOK w walkę z korupcją i ich wkład w praktykę. NOK to agencje nadzorujące, które przeprowadzają zewnętrzną kontrolę wydatków, dochodów i aktywów wszystkich instytucji rządowych). prominentnych osobistości w celu zapewnienia przejrzystości i odpowiedzialności sektora publicznego. Button i Brooks zbadali postępy w opracowywaniu strategii zwalczania nadużyć finansowych w organach rządu centralnego Wielkiej Brytanii. Odkryli szereg centralnych organów publicznych o ograniczonych strategiach kultury zwalczania nadużyć finansowych. Główne elementy odstraszania i zapobieganie oszustwom zgodnie z taką strategią polega na: (i) stworzeniu kultury przeciwdziałania oszustwom, (ii) uzyskaniu poparcia opinii publicznej, (iii) przekazaniu oszustom wiadomości, że zostaną złapani, (iv) zabezpieczeniu przed oszustwami. programów, (v) są zgodne z istniejącymi kontrolami oraz (vi) wzmacniają kontrole w odpowiedzi na pojawiające się zagrożenia.Michel twierdzi, że istnieje ciągłe wyzwanie polegające na skuteczne rozwiązania zapobiegające przestępczości finansowej. Podobnie Jayasuriya stwierdza, że sukcesy były bardzo nieliczne. Sukces w walce z przestępstwami finansowymi musi obejmować partnerstwo, szkolenia, edukację, właściwe projektowanie rynku i świadomość społeczną. Aby odnieść sukces w audycie, Dion sugeruje, że audytor musi rozumieć kulturę organizacyjną. Jeśli audytor rozumie kulturę, może lepiej zrozumieć, gdzie, kiedy, jak i dlaczego popełniono oszustwo lub inne przestępstwo finansowe. Nowy paradygmat audytu obejmuje cztery kroki:

1. Analiza kultury organizacyjnej: konkurencja kontra współpraca, zamknięta kontra otwarta, rotacja personelu i jej motywy, kontrola lub upodmiotowienie zarządzania itp.

2. Analiza branży: przedsiębiorstwa dochodowe lub nierentowne, wzrost lub nasycenie rynku, wizerunek moralny branży itp.

3. Doświadczenie konsultanta w zakresie zachowań organizacyjnych: słabości i zagrożenia w organizacji, które zachęcają do oszustw i innych rodzajów przestępstw finansowych.

4. Analiza systemu kontroli ryzyka: biurokracja czy organizacja wiedzy.

Na strukturę kosztów firmy mają wpływ zarówno konkurenci, jak i klienci. Definiowanie i reagowanie na potrzeby klientów, dążenie do zysków i reagowanie na konkurencję to etyczne decyzje i działania korporacyjne, o ile postrzegamy przedsiębiorstwo jako podmiot moralny.

Regulacje finansowe

Spalek zgłosił kilka ważnych obaw dotyczących charakteru regulacji finansowych w Wielkiej Brytanii i ich wpływ na inwestorów i ofiary przestępstw finansowych:

Zasadniczo działa system aktuarialny, w ramach którego ryzyko związane z przestępstwami finansowymi i złym zarządzaniem jest narzucane na barki indywidualnych konsumentów. Pojęcie „wolnego wyboru" i mit ofiary jako „inwestora oszukanego" są utrwalane przez Financial Services Authority.

Oznacza to, że w ramach regulacyjnych inwestorzy mogą swobodnie decydować o tym, czy zainwestować w określony produkt i instytucję, a ponadto osoby, które padły ofiarą przestępstwa finansowego, zostały oszukane w wyniku niedostatecznej wiedzy o systemie finansowym i związanych z nim ryzykach. Jednostka ds. Przestępczości Zorganizowanej i Finansowej w Wielkiej Brytanii jest odpowiedzialna za opracowanie rządowej strategii przeciwko przestępczości zorganizowanej. Jednostka ta nadzoruje również odzyskiwanie mienia pochodzącego z przestępstwa oraz wykrywanie i skazanie osób zajmujących się praniem pieniędzy. Cele jednostki to:

• poprawa strategicznego obrazu zagrożenia przestępczością zorganizowaną

• współpraca z Grupą Strategii ds. Przestępczości Zorganizowanej, opracowanie strategii walki z przestępczością zorganizowaną

• zapewnienie agencjom i siłom jasnego sterowania priorytetami w zakresie zwalczania przestępczości zorganizowanej oraz opracowywanie skutecznych strategii

• zapewnienie, że agencje i siły są w stanie skutecznie generować, udostępniać i oceniać dane wywiadowcze taktyczne

• zapewnienie siłom i agencjom narzędzi potrzebnych do prowadzenia skutecznych operacji przeciwko przestępczości zorganizowanej;

• sponsoring Agencji ds. Poważnej Przestępczości Zorganizowanej (SOCA)

Zespół ds. Przestępstw Finansowych jest częścią działań rządu na rzecz poprawy zdolności systemu wymiaru sprawiedliwości w sprawach karnych do śledzenia i odzyskiwania dochodów z przestępstwa, a także do zapobiegania, wykrywania i karania osób zajmujących się praniem brudnych pieniędzy. Do jego kluczowych zadań należą:

• wdrożenie ustawy o dochodach z przestępstwa z 2002 r.

• wdrażanie Strategii Odzyskiwania Mienia i monitorowanie jej przez Komitet ds. Odzyskiwania Mienia

• prowadzenie Funduszu Środków Odzyskiwanych

W dochodzeniach dotyczących odzyskiwania mienia często surowcem są dane osobowe związane z finansami. Dlatego Kennedy twierdzi, że zbieranie, udostępnianie i analizowanie informacji w dochodzeniach dotyczących odzyskiwania mienia polega na wygraniu wojen informacyjnych. Przestępcy wykorzystają słabości, umieszczając mienie pochodzące z przestępstwa, w przypadku gdy informacje dotyczące tego majątku nie mogą być łatwo uzyskane przez prokuratorów. Jeśli odzyskiwanie mienia ma się powieść, ważne jest, aby badacze byli w stanie zebrać krytyczne informacje

z niedostępnych źródeł, a nie nieistotne informacje z dostępnych źródeł. Może to być częścią strategii antykorupcyjnej. Sektor finansowy ma kluczowe znaczenie dla skuteczności walki z przestępczością zorganizowaną, korupcją i finansowaniem terroryzmu. Hardouin zaproponował zasady zarządzania sektorem w dwóch kanałach. Jednym z nich jest ogólna organizacja i regulacja sektora. Zarządzanie zależy od ram określonych przez regulatora. Drugim kanałem jest odpowiedzialność biznesu. Również sektor prawny ma kluczowe znaczenie w walce z przestępczością finansową. W Kanadzie na prawników nakłada się rygorystyczne obowiązki regulacyjne dotyczące finansów w zakresie przeciwdziałania przestępczości. Gallant twierdzi jednak, że nałożenie na kanadyjskich prawników zobowiązań w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu jest projektem obarczonym niepewnością. Dzieje się tak, ponieważ nie jest jasne, czy strategia ścigania kryminalnych finansów, leżąca u podstaw werbowania prawników do wojny z kryminalnymi finansami, działa na rzecz odstraszania przestępczości. W dochodzeniach dotyczących odzyskiwania mienia często surowcem są dane osobowe związane z finansami. Dlatego Kennedy twierdzi, że zbieranie, udostępnianie i analizowanie informacji w dochodzeniach dotyczących odzyskiwania mienia polega na wygraniu wojen informacyjnych. Przestępcy wykorzystają słabości, umieszczając mienie pochodzące z przestępstwa, w przypadku gdy informacje dotyczące tego majątku nie mogą być łatwo uzyskane przez prokuratorów. Jeśli odzyskiwanie mienia ma się powieść, ważne jest, aby badacze byli w stanie zebrać krytyczne informacje z niedostępnych źródeł, a nie nieistotne informacje z dostępnych źródeł. Może to być częścią strategii antykorupcyjnej. Sektor finansowy ma kluczowe znaczenie dla skuteczności walki z przestępczością zorganizowaną, korupcją i finansowaniem terroryzmu. Hardouin zaproponował zasady zarządzania sektorem w dwóch kanałach. Jednym z nich jest ogólna organizacja i regulacja sektora. Zarządzanie zależy od ram określonych przez regulatora. Drugim kanałem jest odpowiedzialność biznesu. Również sektor prawny ma kluczowe znaczenie w walce z przestępczością finansową. W Kanadzie na prawników nakłada się rygorystyczne obowiązki regulacyjne dotyczące finansów w zakresie przeciwdziałania przestępczości. Gallant twierdzi jednak, że nałożenie na kanadyjskich prawników zobowiązań w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu jest projektem obarczonym niepewnością. Dzieje się tak, ponieważ nie jest jasne, czy strategia ścigania kryminalnych finansów, leżąca u podstaw werbowania prawników do wojny z kryminalnymi finansami, działa na rzecz odstraszania przestępczości. Sathye oszacował koszty przestrzegania przepisów dotyczących przeciwdziałania praniu prania i stwierdził, że przepisy te nakładają znaczne obciążenia finansowe na instytucje finansowe w Australii. Zrewidowane w 2003 r. 40 zaleceń Grupy Zadaniowej ds. Przeciwdziałania Praniu Pieniędzy w Wielkiej Brytanii umożliwia regionowi lub narodowi wdrożenie podejścia opartego na ryzyku w odniesieniu do kluczowych elementów przeciwdziałania praniu pieniędzy i finansowaniu terrorystów. Podejście oparte na ryzyku obejmuje opracowanie odpowiednich środków kontroli ryzyka w oparciu o proces identyfikacji i kategoryzacji ryzyka. Koker przestudiował oparte na ryzyku wytyczne FATF dotyczące zwalczania prania pieniędzy i finansowania terroryzmu, aby określić swoje podejście do identyfikacji i zarządzania dostawcami, produktami i transakcjami niskiego ryzyka. Przeanalizował odpowiednie zalecenia FATF i zawarte w nim wytyczne oraz zastanowił się nad kluczowymi pytaniami dla regulatorów i instytucji finansowych. Doszedł do wniosku, że wydaje się wskazane, aby FATF zapewnił jaśniejsze i oparte na zasadach ramy koncepcyjne zarządzania ryzykiem, ale powstrzymał się od identyfikowania przykładów i wskaźników, zwłaszcza produktów i transakcji niskiego ryzyka, chyba że są one naprawdę uniwersalne lub właściwie ujęte w kontekście.

Regulacja oparta na ryzyku odnosi się do dostosowywania zasad, aby skoncentrować się na przypadkach podwyższonego ryzyka. Nadzór oparty na ryzyku to podejście, w którym organ nadzorczy koncentruje się na ryzyku stwarzanym i zarządzanym przez podmioty regulowane oraz alokuje zasoby nadzorcze na podstawie ich profili ryzyka:

Podejście oparte na ryzyku na ogół prowadzi nadzorców do poświęcania mniejszej uwagi podmiotom o niższym ryzyku, a raczej skupiania uwagi i zasobów na podmiotach stwarzających większe ryzyko.

Podmioty podlegające regulacji, które stosują podejście oparte na ryzyku do przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy, dostosowują swoje środki kontroli do profili ryzyka ich różnych produktów i klientów. Główną korzyścią jest odpowiednia i efektywna alokacja zasobów

Ochrona zasobów informacyjnych

Organizacje dysponują szeregiem narzędzi i technologii służących do ochrony informacji elektronicznych. Obejmują one metody zabezpieczania systemów i danych, zapewnienia kontroli systemu i jakości systemu:

• Kontrola dostępu obejmuje procedury stosowane przez organizację w celu zapobiegania niewłaściwemu dostępowi do systemów przez osoby nieupoważnione i osoby z zewnątrz. Aby uzyskać dostęp, użytkownik musi zostać autoryzowany i uwierzytelniony. Uwierzytelnianie odnosi się do zdolności do poznania, że dana osoba jest tym, za kogo się podaje.

• Firewall to połączenie sprzętu i oprogramowania, które kontroluje przepływ przychodzącego i wychodzącego ruchu sieciowego.

• System wykrywania włamań zawiera narzędzia do monitorowania w pełnym wymiarze czasu, umieszczone w najbardziej wrażliwych punktach organizacji obliczeniowej.

• Oprogramowanie antywirusowe służy do sprawdzania systemów komputerowych i napędów pod kątem obecności wirusów komputerowych.

• Szyfrowanie to proces przekształcania zwykłego tekstu lub danych na tekst zaszyfrowany, którego nie może odczytać nikt inny niż nadawca i zamierzony odbiorca.

• Certyfikat cyfrowy to plik danych używany do ustalenia tożsamości użytkowników i zasobów elektronicznych w celu ochrony transakcji online.

• Audyt systemu bada ogólne środowisko bezpieczeństwa organizacji, a także mechanizmy kontrolne rządzące poszczególnymi systemami informacyjnymi.

Oprócz wdrażania skutecznych zabezpieczeń i kontroli zarówno zewnętrznie, jak i wewnętrznie, organizacje mogą poprawić niezawodność systemu i zapobiegać kradzieży informacji, stosując wskaźniki oprogramowania i rygorystyczne testowanie oprogramowania.

Przypadek chińskiej Komisji Papierów Wartościowych

Chiny kryminalizują handel informacjami poufnymi poprzez ustawodawstwo i mają krajowy system regulacji i egzekwowania wprowadzony przez Chińską Komisję Regulacyjną ds. Papierów Wartościowych. Rynek akcji w Chinach doświadczył w ciągu ostatniej dekady ogromnego wzrostu i rozwoju. Głównym odkryciem badania przeprowadzonego przez Chenga jest niedostatek przypadków wykorzystywania informacji poufnych oraz brak wyroków skazujących za wykorzystywanie informacji poufnych jako przestępstwa w Chinach. Głównym wyzwaniem związanym z regulacjami dotyczącymi wykorzystywania informacji poufnych w Chinach jest fakt, że większość spraw dotyczących wykorzystywania informacji poufnych dotyczy wysokich rangą urzędników rządowych i partyjnych. Komisja regulacyjna nie ma uprawnień do bezpośredniego administrowania dyscypliną i karami dla urzędników państwowych i kadr partyjnych za przestępstwa związane z wykorzystywaniem informacji poufnych. Istnieją przede wszystkim trzy sposoby, za pomocą których Chińska Komisja Regulacji

Papierów Wartościowych wykrywa i dowiaduje się o działaniach związanych z wykorzystywaniem informacji poufnych:

• Pracownicy Komisji, którzy znajdują się na pierwszej linii egzekucji, szukają nielegalnych zachowań poprzez regularne inspekcje lub przeglądanie informacji finansowych w poszukiwaniu wskazówek.

• Skargi przyjmuje Biuro Skarg Cywilnych Rady Państwa, które zajmuje się różnego rodzaju skargami w kraju.

• Istnieją skierowania dochodzeń prowadzonych przez Giełdę Papierów Wartościowych w Szanghaju i Giełdę Papierów Wartościowych w Shenzhen.

Giełdy mają obowiązek monitorowania codziennych działań handlowych na swoich giełdach pod kątem naruszeń. Szanghajska Giełda Papierów Wartościowych poinformowała rok temu, że podczas ankiety przeprowadzonej wśród ponad 600 dyrektorów 54 spółek giełdowych wykryto cztery przypadki nieprawidłowości, w tym wykorzystywanie informacji poufnych.