Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 238 · 2015

Dariusz Garczyński

Uniwersytet Ekonomiczny we Wrocławiu
Wydział Zarządzania, Informatyki i Finansów
Katedra Bankowości
dariusz.garczynski@ue.wroc.pl

RYZYKO NOWYCH TECHNOLOGII W ZARZĄDZANIU RYZYKIEM OPERACYJNYM W BANKU

Streszczenie: W ostatnich latach zaobserwować można gwałtowny rozwój nowych kanałów komunikacji bank–klient, związanych przede wszystkim z technologiami informatyczno-telekomunikacyjnymi. Wprowadzanie innowacji w tym zakresie niesie ze sobą jednak szereg zagrożeń w obszarze bankowego ryzyka operacyjnego. Do jednego z najważniejszych zaliczyć tu należy zagrożenie wynikające z zastosowania różnego rodzaju technik manipulacji inżynierii socjalnej (ang. *social engineering*), przede wszystkim *phishing*. W artykule przedstawione zostaną techniki inżynierii socjalnej stosowane do ataków na bezpieczeństwo bankowych systemów informatycznych oraz analiza środków ochrony przed tym rodzajem zagrożeń.

Słowa kluczowe: ryzyko operacyjne, ryzyko informatyczne, inżynieria socjalna, *phishing*.

Wprowadzenie

Rozwój technologii informatyczno-telekomunikacyjnych, warunkujący powstanie i rozwój bankowości elektronicznej, postawił przed bankami szereg wyzwań w zakresie zapewnienia bezpieczeństwa zdalnych kontaktów bank–klient. Podstawowym problemem w chwili obecnej w tym obszarze jest (ze względu na skalę zagrożenia) stosowanie przez cyberprzestępców technik inżynierii socjalnej mających na celu przejęcie danych umożliwiających logowanie do systemu bankowości elektronicznej, przede wszystkim *phishingu*. Celem artykułu jest przedstawienie kontekstu zagrożenia *phishingiem* w bankowości elektronicznej jako elementu systemu informatycznego banku, zaprezentowanie definicji i me-

tod inżynierii socjalnej (socjotechniki) oraz krótka analiza środków zabezpieczających przed *phishingiem* po stronie banku i klienta.

1. Ryzyko informatyczne jako element ryzyka operacyjnego

Ryzyko informatyczne związane jest z możliwością wystąpienia negatywnego zjawiska powodującego określone straty w systemie informatycznym. Najczęściej wykorzystywaną definicję ryzyka informatycznego podaje Polska Norma PN-I-02000:2002 [PN-I-02000 – Technika informatyczna…]. Zgodnie z nią ryzyko informatyczne to „możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych". W odniesieniu do bankowych systemów informatycznych mogą to być na przykład próby nieautoryzowanego dostępu do systemu informatycznego lub pożar w serwerowni banku.

W ostatnich latach zaobserwować można wzrost poziomu tego rodzaju ryzyka w instytucjach bankowych. Wiąże się to nie tylko ze wzrostem skomplikowania samych bankowych systemów informatycznych, ale przede wszystkim z wprowadzeniem przez banki usług bankowości internetowej w połowie lat 90. ubiegłego stulecia. Do tego momentu systemy bankowe były w zasadzie niedostępne dla osób niebędących pracownikami banku (systemy zdalnego dostępu do rachunku bankowego – *home/office banking* wykorzystywane były przede wszystkim przez przeszkolonych pracowników dużych firm). Pojawienie się możliwości wpięcia systemu informatycznego klienta do systemu informatycznego banku poprzez przeglądarkę internetową i sieć Internet, spowodowało gwałtowny wzrost liczby użytkowników tego kanału dystrybucji usług bankowych, a co za tym idzie wzrost liczby potencjalnych zagrożeń.

Proces ten dostrzegły instytucje nadzoru finansowego, w tym przede wszystkim Bazylejski Komitet Nadzoru Bankowego, który już w 1998 r. doprowadził do powstania zespołu pod nazwą Electronic Banking Group (EBG), odpowiedzialnego za opracowywanie zaleceń i rekomendacji w zakresie praktyk nadzorczych w obszarze bankowości elektronicznej. EBG jednoznacznie stwierdza, że bankowość elektroniczna modyfikuje niektóre rodzaje ryzyka bankowego, a w szczególności wpływa na wzrost zagrożenia ryzykiem operacyjnym [Electronic Banking Group…, 2000]. Do podstawowych cech bankowości elektronicznej, które powodują konieczność nowego spojrzenia na zarządzanie ryzykiem bankowym, Komitet Bazylejski zalicza [Risk Management Principles…, s. 5]:

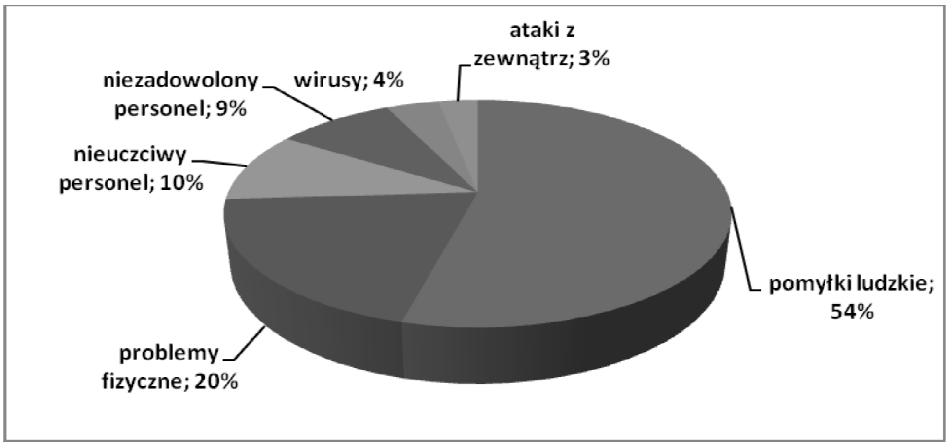
– bezprecedensową szybkość zmian w zakresie innowacji technologicznych i obsługi klienta,

- wszechobecny, globalny charakter otwartych sieci elektronicznych,
- integrację aplikacji bankowości elektronicznej z pozostałymi systemami komputerowymi,
- rosnące uzależnienie banków od stron trzecich dostarczających niezbędnej technologii informatycznej.

Reasumując powyższe wywody, należy stwierdzić, że w chwili obecnej ryzyko informatyczne banku uzależnione jest nie tylko od zagrożeń tradycyjnych, wewnętrznych informatycznych systemów bankowych, ale również od systemów bankowości elektronicznej, a przede wszystkim internetowej.

Zagrożenia systemów informatycznych w bankowości nie mają jednolitego charakteru. Istnieje wiele różnych klasyfikacji tych zagrożeń, wszystkie jednak uwzględniają źródło ich pochodzenia. Najpełniejszą analizę problematyki bezpieczeństwa bankowych systemów informatycznych podjął J. Grzywacz [2003], dzieląc zagrożenia systemów informatycznych na:

- zagrożenia ludzkie celowe (m.in. manipulacja danymi, fałszerstwa dokumentów, *hacking*, szpiegostwo przemysłowe, *social engineering*),
- zagrożenia ze strony programów komputerowych (m.in. ataki DoS, programy skanujące, wirusy),
- zagrożenia środowiskowe (m.in. woda, ogień, kurz, wilgoć, awarie zasilania itp.).



Rys. 1. Zagrożenia bezpieczeństwa systemów informatycznych w bankowości

Źródło: Grzywacz [2003, s. 14].

Na uwagę zasługują przed wszystkim zagrożenia związane z tzw. czynnikiem ludzkim, czyli użytkownikami bankowości elektronicznej, pracownikami wewnętrznymi banku lub osobami usiłującymi uzyskać dostęp do zasobów sys-

temu w sposób nieuprawniony (hakerzy). Konsekwencją gwałtownego rozwoju bankowości elektronicznej jest nie tylko wzrost liczby użytkowników tej usługi, ale przede wszystkim obniżenie poziomu świadomości istotności zagrożeń bankowego systemu informatycznego. Wiedza informatyczna klientów, którym banki oferują usługi bankowości elektronicznej, jest czasem na poziomie niezadowalającym z punktu widzenia bezpieczeństwa bankowego systemu informatycznego. Najpoważniejszym zagrożeniem jest tutaj niebezpieczeństwo kompromitacji parametrów dostępu do systemu (identyfikator, hasło, lista haseł jednorazowych, PIN itp.). Zagrożenie to jest następstwem albo podsłuchu w sieci lokalnej, albo wykorzystania oprogramowania szpiegującego czy zastosowania metod inżynierii socjalnej (*social engineering*). Ten ostatni sposób naruszenia bezpieczeństwa systemów informatycznych w bankowości wykorzystywany jest coraz powszechniej, przede wszystkim do ataków typu *phishing*.

2. Mechanizmy i narzędzia inżynierii socjalnej

Pojęcie inżynierii socjalnej (socjotechniki, inżynierii społecznej) nie doczekało się jeszcze jednej, ogólnie obowiązującej definicji. T. Trejderowski [2009] definiuje socjotechnikę jako „ogół metod, działań i środków praktycznych zmierzających do uzyskania pożądanego zachowania jednostek czy też grup ludzkich; innymi słowy, zmierzających do wywołania pożądanych przemian w postawach i zachowaniach społecznych". Podobnie pojmuje socjotechnikę A. Podgórecki [1966, s. 23], wskazując na jej praktyczny aspekt – „socjotechnika jako 'nauka praktyczna' dostarcza wiedzy, której zastosowanie, używając odpowiednich instrumentów i środków, pozwala na skłonienie jednostek bądź grupy osób do zachowań oczekiwanych przez sprawców oddziaływań".

Niekwestionowany autorytet w dziedzinie cyberprzestępstw – K. Mitnick [2003, s. 3] uwzględnia w swej definicji socjotechniki ważne z punktu widzenia technologii informatycznych aspekty – „Socjotechnika to wywieranie wpływu na ludzi i stosowanie perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji".

Robert Cialdini [2009, s. 12] podaje siedem najważniejszych reguł socjotechniki. Są to:

– reguła wzajemności, polega na potrzebie odwzajemnienia doznanego dobra; podobnie doznanie z czyjejś strony krzywdy wywołuje dokładnie taką samą reakcję,

- reguła sympatii bazuje na miłych skojarzeniach lub ciepłych uczuciach wywoływanych przez manipulatora; w tym wypadku uczucie przyjaźni wykorzystywane jest jako narzędzie służące do wywierania wpływu na innych,
- reguła niedostępności, której podstawą są sztucznie wykreowane, bezpowrotnie przemijające okazje; przekazuje, że ograniczoność dóbr, jak i czasu ich dostępności dla zainteresowanego, powoduje automatyczny i sztuczny wzrost ich wartości,
- reguła społecznego dowodu słuszności – wykorzystuje tendencję do powielania zachowań masowych,
- reguła konsekwencji, wykorzystująca ludzką cechę konsekwentnego podążania za obranym celem,
- reguła autorytetu bazuje na naszej głęboko zakorzenionej potrzebie ulegania osobom społecznie ważnym i uznanym,
- reguła wartości, zwana również regułą maksymalizacji własnego zysku, polega na utożsamianiu rzeczy (pojęć) drogich z rzeczami (pojęciami) dobrej jakości.

Wymienione wyżej reguły socjotechniki wykorzystywane są w tzw. cyklu socjotechnicznym [Mitnick 2003, s. 360], który może być stosowany wielokrotnie wobec tego samego celu.

Tabela 1. Cykl socjotechniczny

Działanie	Opis
Rozpoznanie	może się zacząć od ogólnej analizy powszechnie dostępnych informacji, jak wyniki finansowe, katalogi, zgłoszenia do urzędu patentowego, wzmianki prasowe, artykuły w prasie fachowej, zawartość strony internetowej, a także zawartości śmietników.
Budowanie więzi i zaufania	użycie wewnętrznych informacji, podawanie się za kogoś innego, wspominanie nazwisk osób znanych ofierze, zgłoszenie potrzeby pomocy lub zasugerowanie posiadania władzy.
Wykorzystanie zaufania	prośba o informację lub działanie skierowane do ofiary. Zmanipulowanie ofiary tak, aby sama poprosiła o pomoc.
Wykorzystanie informacji	jeżeli uzyskana informacja jest tylko kolejnym krokiem zbliżającym napastnika do celu, wraca on do poprzednich kroków cyklu, aż do osiągnięcia sukcesu.

Źródło: Mitnick [2003, s. 360].

Zastosowanie reguł socjotechniki zazwyczaj przeprowadzane jest na osobie reprezentującej jedną z grup:

- nieświadomi wartości informacji – pracownicy administracji, ochrony, recepcji, ale także klienci bankowości elektronicznej,

- posiadający specjalne przywileje – pomoc techniczna, administratorzy systemów komputerowych, operatorzy komputerów, administratorzy systemów telefonicznych,
- producenci sprzętu i oprogramowania,
- określone wydziały – księgowość, kadry.

Do typowych metod socjotechnicznych, wykorzystywanych w manipulacji, Mitnick zalicza:

- udawanie pracownika tej samej firmy,
- udawanie przedstawiciela dostawcy, firmy partnerskiej lub agencji rządowej,
- udawanie kogoś, kto ma władzę,
- udawanie nowego pracownika proszącego o pomoc,
- udawanie przedstawiciela producenta systemu operacyjnego zalecającego pilną aktualizację,
- oferowanie pomocy w razie wystąpienia jakiegoś problemu, sprawienie, by problem wystąpił i manipulacja ofiarą w taki sposób, aby sama zadzwoniła z prośbą o pomoc,
- wysłanie darmowego programu do aktualizacji lub zainstalowania,
- wysłanie wirusa lub konia trojańskiego w załączniku do poczty,
- użycie fałszywego okna dialogowego wyświetlającego prośbę o powtórne zalogowanie się lub wprowadzenie hasła,
- przechwytywanie naciśniętych klawiszy za pomocą specjalnego oprogramowania,
- podrzucenie w okolicach stanowiska pracy ofiary dyskietki lub płyty CD-ROM zawierającej niebezpieczny kod,
- używanie wewnętrznej terminologii i żargonu w celu zbudowania zaufania,
- oferowanie nagrody za rejestrację poprzez wprowadzenie nazwy użytkownika i hasła na stronie internetowej,
- podrzucenie dokumentu lub pliku w pomieszczeniu poczty wewnętrznej firmy, aby dotarł do miejsca przeznaczenia jako korespondencja wewnętrzna,
- zmiana ustawień nagłówka w faksie tak, aby wydawał się pochodzić z wewnątrz,
- prośba do recepcjonistki o odebranie i przesłanie faksu dalej,
- prośba o transfer pliku do lokalizacji, która wydaje się wewnętrzna,
- ustawienie skrzynki poczty głosowej w taki sposób, że w trakcie oddzwaniania napastnik jest identyfikowany jako osoba z wewnątrz,
- podawanie się za pracownika z innego oddziału i prośba o tymczasowe otwarcie konta e-mail.

Niektóre z podanych wyżej metod stosowane są wobec klientów bankowości elektronicznej w celu uzyskania haseł dostępu do rachunku. Proceder wyłudzania

haseł do zasobów systemów informatycznych nazywany jest *phishingiem* (podobno nazwa ta pochodzi od słów *password fishing* – łowienie haseł). Jak pokazuje badanie przeprowadzone w maju 2012 r. przez O+K Research na zlecenie Kaspersky Lab [www1], rozpoznanie takiej wiadomości nie zawsze jest łatwe. 50% respondentów przyznało, że nie potrafi rozpoznać wiadomości *phishingowej* lub spreparowanej strony internetowej. Z badania wynika, że cyberprzestępcy, którzy wykorzystują *phishing* jako narzędzie do kradzieży danych, są głównie zainteresowani uzyskaniem nieautoryzowanego dostępu do kont na portalach społecznościowych, kont w systemach bankowości online oraz systemach płatności, jak również sklepach internetowych. Wyniki badania stanowią bezpośredni dowód na to, że metoda wykorzystująca masowe wysyłki przynosi efekty: około połowa respondentów przyznała, że trafiła już na podejrzaną korespondencję na portalach społecznościowych i w poczcie e-mail. 47% użytkowników komputerów PC otrzymało wiadomość z podejrzanym odsyłaczem lub załącznikiem, a 29% respondentów dostało wiadomość wysłaną w imieniu banku, portalu społecznościowego lub innego portalu wyglądającego na wiarygodny. Ponadto 26% użytkowników przyznało, że ich komputery zostały zainfekowane w wyniku otwarcia załącznika do wiadomości, a 13% respondentów podało osobiste oraz finansowe dane na podejrzanych stronach.

Zwiększenie liczby ataków z wykorzystaniem *phishingu* skłoniło firmę Kaspersky Lab do przeprowadzenia badania tego zjawiska. Jak wynika z raportu „Ewolucja ataków phishingowych 2011–2013" [www2], liczba użytkowników Internetu, którzy zetknęli się z tym rodzajem zagrożenia bezpieczeństwa, zwiększyła się w tym czasie z ok. 20 mln do 37,7 mln. Najczęściej atakowanymi przez *phisherów* serwisami były portale społecznościowe (Yahoo!, Google, Facebook, Twitter), natomiast ponad 20% wszystkich ataków *phishingowych* korzystało z wizerunku banków i innych instytucji finansowych.

Tabela 2. Firmy, których wizerunek wykorzystywano najczęściej w atakach *phishingowych* w latach 2011-2013

Firma	Procent wszystkich ataków
Banki	20,64%
Yahoo!	9,85%
Facebook	9,69%
Google	6,89%
Amazon	3,86%
Inne	49,07%

Źródło: Ewolucja ataków phishingowych: 2011-2013 [2013, s. 11].

Podobne badania przeprowadza cyklicznie organizacja APWG, skupiająca ponad 2000 różnego rodzaju instytucji z całego świata, zajmująca się koordynacją działań wymierzonych przeciw przestępstwom w cyberprzestrzeni. W swoim raporcie „Phishing Activity Trends Report 2nd Quarter 2014" [www3, s. 7] wskazuje na serwisy obsługi płatności elektronicznych oraz serwisy finansowe jako główne cele ataków *phishingowych* (odpowiednio 39,80% i 20,20% wszystkich ataków).

3. Środki ochrony przed *phishingiem* w obszarze bankowości elektronicznej

Jak wspomniano w poprzednim rozdziale, podstawową metodą socjotechniczną cyberprzestępcy, który pragnie uzyskać nieautoryzowany dostęp do rachunku bankowego, jest wykorzystanie naiwności lub braku doświadczenia użytkownika bankowości elektronicznej. Firmy, które przeprowadzają testy penetracyjne systemów bezpieczeństwa, podają, że próby włamania się do systemu komputerowego klienta za pomocą metod socjotechnicznych są prawie w 100% skuteczne. Zabezpieczenia technologiczne mogą utrudnić takie ataki poprzez minimalizowanie udziału ludzi w procesie decyzyjnym. Jednak jedyną naprawdę skuteczną metodą osłabienia tego zagrożenia jest zastosowanie zabezpieczeń technologicznych w kombinacji z procedurami bezpieczeństwa, które ustalają podstawowe zasady zachowania się pracowników oraz odpowiednim teoretycznym i praktycznym ich szkoleniem.

Analizując problematykę bezpieczeństwa systemów bankowości elektronicznej pod kątem narażenia na *phishing*, wskazać należy, że środki ochrony przed zagrożeniami tego typu powinny być zastosowane w dwu obszarach – obszarze systemu wewnętrznego (serwera) kontrolowanego przez bank oraz w obszarze systemu informatycznego klienta. Oba te obszary odpowiadają bowiem za bezpieczeństwo transakcji elektronicznych, choć mają nieco odmienne obowiązki i zadania [Wawrzyniak 2012, s. 137].

Po stronie serwera do podstawowych zabezpieczeń *anty-phishingowych* zaliczyć należy:

- szyfrowanie transmisji protokołem EV SSL,
- uwierzytelnianie użytkownika na etapie logowania do systemu.

Posługiwanie się protokołem EV SSL jest w tej chwili standardem wśród instytucji finansowych. Jeśli chodzi o uwierzytelnianie logowania do systemu, to banki w chwili obecnej stosują szereg metod uwierzytelniania, takich jak:

- hasła – statyczne lub maskowane,
- wirtualne klawiatury,
- obrazki bezpieczeństwa (*personal safety seal*),
- token – sprzętowy lub jako aplikacja w telefonie komórkowym,
- sprzętowy podpis elektroniczny.

Wymienione metody (w kolejności od zapewniającej najmniej bezpieczne uwierzytelnianie) w celu podniesienia poziomu bezpieczeństwa powinny być stosowane łącznie.

Po stronie klienta podstawowym zabezpieczeniem przed atakiem z wykorzystaniem *phishingu* jest aktualna przeglądarka internetowa i aktualny program zabezpieczający z funkcją *antyphishing*, czyli modułem wykrywającym spreparowane wiadomości e-mail lub strony WWW. Niestety sam program nie wystarczy – niezbędna jest świadomość zagrożenia oraz podstawowa wiedza na temat korzystania w Internecie z usług bankowości elektronicznej. Jest to najważniejszy problem do rozwiązania dla banków, które dbając o wysoki poziom bezpieczeństwa kanału elektronicznego, muszą zapewnić klientom odpowiednią ergonomię pracy z serwisem bankowości elektronicznej.

Podsumowanie

Zaprezentowana w artykule problematyka zagrożeń bezpieczeństwa kontaktów bank–klient w bankowości elektronicznej nie wyczerpuje całości zagadnienia ze względu na bardzo szeroki jego zakres, znacznie wykraczający poza ramy publikacji. Wskazanie tzw. czynnika ludzkiego, którym w kontekście omawianej problematyki jest klient banku, jako ogniwa najbardziej podatnego na ataki, a zarazem najtrudniej definiowalnego pod względem przygotowania do korzystania z nowoczesnych technologii informatycznych, stawia banki w niezwykle trudnej sytuacji. Z jednej strony muszą bowiem zapewnić maksymalnie wysoki poziom bezpieczeństwa oferowanych usług bankowości elektronicznej, z drugiej – klienci oczekują łatwego i intuicyjnego dostępu do kanałów elektronicznych. W chwili obecnej trudno jest wskazać rozwiązanie technologiczne czy organizacyjne spełniające oba postulaty jednocześnie.

Literatura

Cialdini R.B. (2009), *Wywieranie wpływy na ludzi. Teoria i praktyka*, GWP, Gdańsk.

Electronic Banking Group Initiatives and White Papers, Oct. 2000, www.bis.org/publ/bcbs76.pdf, (dostęp: 25.10.2014).

Grzywacz J. (2003), *Bezpieczeństwo systemów informatycznych w bankach w Polsce*, SGH, Warszawa.

Mitnick K. (2003), *Sztuka podstępu*, Helion, Gliwice.

PN-I-02000 – Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia, Polski Komitet Normalizacyjny, 2002.

Podgórecki A. (1966), *Zasady socjotechniki*, Wiedza Powszechna, Warszawa.

Risk Management Principles for Electronic Banking, July 2003, www.bis.org/publ/bcbs98.pdf, (dostęp: 25.10.2014).

Wawrzyniak D. (2012), *Ryzyko informatyczne w działalności bankowej*, Wyd. Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław.

[www 1] www.kaspersky.com/downloads/pdf/kaspersky-lab_ok-consumer-survey-report_eng_final.pdf.

[www 2] http://vs.kaspersky.pl/download/analizy/klp_ewolucja_phishingu_2013_pelny_raport.pdf.

[www 3] http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf.

RISK OF NEW TECHNOLOGIES IN BANK OPERATIONAL RISK MANAGEMENT

Summary: In recent years rapid development of new bank – client communication channels, related primarily to the IT, can be observed. Innovation implementation in this area, however, brings with it number of risks in the area of bank operational risk. One of the most significant danger here is a threat resulting from the use of various types of manipulation techniques of social engineering, primarily phishing. The article presents the social engineering techniques used to attack the security of banking systems and the analysis of the means of protection against this type of threat.

Keywords: operational risk, IT risk, social engineering, phishing.