telematik 2004

KFB & TELDOK

Ny teknik som drivkraft och hjälpmedel för finansiella bedrägerier

Bengt Carlsson

telematik 2004

Denna småskrift i programmet Telematik 2004 utgör samtidigt KFB-rapport 1999:36 (ISBN 91-88371-53-0) och Via TELDOK 37 (ISSN 0283-5266).

TITEL/TITLE
Ny teknik som drivkraft och hjälpmedel för finansiella bedrägerier

FÖRFATTARE/AUTHOR
Bengt Carlsson
SERIE/SERIES
Telematik 2004
KFB-Rapport 1999:36
Via Teldok 37

ISBN KFB:
91-88371-53-0

ISSN
KFB: 1104-2621
ISSN TELDOK: 0283-5266

PUBLICERINGSDATUM/DATE PUBLISHED
December 1999

UTGIVARE/PUBLISHER
TELDOK och KFB – Kommunikationsforskningsberedningen, Stockholm

KFBs DNR
99-0350

Ny teknik som drivkraft och hjälpmedel för finansiella bedrägerier

Bengt Carlsson

Företal

KFB (Kommunikationsforskningsberedningen) och TELDOK startade våren 1999 programmet Telematik 2004 för att att finansiera och publicera studier av tidiga IT-användare och användningsområden.

Utgångspunkten för Telematik 2004 är de förändringar som sker i samband med förverkligandet av ”informationssamhället” och vad detta betyder för Sverige. Vilka blir följderna om stora grupper av människor och företag börjar använda den teknik som i nuläget ett mindre antal nyttjar? Rapporter om tidig användning – sådana som publiceras inom Telematik 2004 – kan ge vägledning.

Inom programmet finansieras två slags skrifter: småskrifter (på som mest 30-50 sidor, baserade på samtal) och rapporter (på som mest 100 sidor, som beskriver och analyserar utvecklingen inom ett visst område). Den första ”småskriften” föreligger nu: en dokumentation av den fjärde internationella konferensen om finansiell brottslighet, skriven av Bengt Carlsson. Till vardags är Bengt Carlsson journalist på Dagens Nyheter och har tidigare också bl a författat TELDOK Rapport 104 (från 1996): Utan IT stannar marknaden.

Den nya informationstekniken har i det närmaste revolutionerat den finansiella sektorn. IT verkar kostnadssänkande och effektiviserande. Dessutom används IT för att utforma nya, mer sofistikerade tjänster och nya, mer automatiserade marknadsplatser. Kommunikation kan ske direkt, utan mellanhänder och över hela världen.

Men gränslösheten kan ha baksidor. Bengt Carlsson pekar på att tekniken kan användas också för mer sofistikerade och effektivare bedrägerier, som ”kommer att utsätta alla för ökade risker, från den lilla människan till det stora, stora företaget – eller till ett helt land”. (För övrigt finns exempel på att de finansiella bedragarna hittat på fiktiva länder för att bedriva sin verksamhet!)

Därför är ”de finansiella bedrägerierna … en av de verksamheter som globaliseras fortast”: internationella finansiella bedrägerier bedöms komma att omsätta nära 300 miljarder svenska kronor i år. Å andra sidan ger den nya tekniken ”bättre möjligheter för dem som ska jaga och döma brottslingarna”, menar Bengt Carlsson. Brotts-

lingar som använt sig av IT tycks ändå vara lättare att spåra än mer konventionella förbrytare, även om det ligger i teknikens natur att användarna kan verka på avstånd, utan hänsyn till tid och rum.

Trevlig läsning önskas.

Urban Karlström
Generaldirektör KFB

Bertil Thorngren
professor, CIC, Handelshögskolan,
Telia Business and Innovation,
Ordförande TELDOK Redaktionskommitté

Innehåll

1.
Sammanfattning och utblick

Att döma av vad ett antal av talarna vid Fraud 4, en internationell konferens om finansiella bedrägerier, tror om framtiden så blir det närmast en kapplöpning mellan bedragare och polis och andra myndigheter under de kommande åren.

”Det här är bara början”, sa Nicholas Ridley från det europeiska polissamarbetet Europol apropå sina studier av hur organiserade kriminella från det forna Östeuropa nu ”globaliseras” och använder alltmer av ny teknik.

Alla kommer att bli mer utsatta

Och en värld med mer och mer finansiella bedrägerier, där den verkliga tillväxten kommer att ske där olika former av ny teknik används, kommer att utsätta alla för ökade risker, från den lilla människan till det stora, stora företaget – eller till ett helt land. För individen är det bedrägerier med hjälp av Internet som kommer att ha de största riskerna. Här är spektrat brett, från falska länder som Melchizedek (kapitel 6), via risken att någon bedragare kommer över betal- eller kreditkortsnummer till falska råd om värdepapper.

Uppfinningsrikedomen kommer att vara stor, även om nu många bedrägerier på nätet finns i annan tappning sedan länge. Men Internet gör bedragarnas arbete effektivare. Det räcker med en trovärdig hemsida istället för som tidigare personer som bearbetade tänkbara offer per telefon, eller kanske med ett prydligt kontor som fasad. En hemsida är dessutom betydligt lättare att stänga och flytta.

Och bedragarna kan finnas på något helt annat ställe än vad vi tror, via länkningar/vidarkopplingar av datatrafik och telefoner. Därmed kan bedragarna finnas på platser som är svåråtkomliga rent praktiskt, men också tack vare att lagstiftningen skiljer sig kraftigt åt mellan olika länder. De ”traditionella” skatteparadisen, som en del karibiska öar, är populära även som bas för internetbrott, precis som de varit för annat.

Så att de finansiella bedrägerierna är en av de verksamheter som globaliseras fortast är inget tvivel om.

Svårt men inte hopplöst

Men, även om läget är svårt så är det inte hopplöst. Den bilden ville bland andra amerikanska FBI förmedla. Lisa Kate Osofsky gav några exempel på hur FBI, tack vare samarbeten lyckats få fast olika typer av bedragare som använt datatekniken, antingen för att sprida datavirus via Internet, sprida falsk information via falsk hemsida för att få en aktiekurs att stiga eller gått in på bankkonto och fört över pengar.

En slutsats av hennes och andras tal var att ny informationsteknik också betyder bättre möjligheter för dem som ska jaga och döma brottslingarna. När det väl blir samarbeten mellan olika intressenter, som myndigheter, polis och privata företag så tycks snarast möjligheterna att få fast brottslingar som använt sig av datateknik och telekommunikationer vara bättre än att få tag på mer konventionella förbrytare.

Även om en databrottsling försöker sopa igen spåren efter sig, som den PairGainanställde som låg bakom falsk information som drev upp bolagets aktiekurs, eller som den amerikan som stal hemlig information om kommande produkter från den finska telekomjätten Nokia (det talade John Austin, datasäkerhetsexpert, om), så finns det spår eller rester av spår som ger ledtrådar.

På några års sikt kommer också intelligenta datasystem och program att ha utvecklats radikalt. Det pekade både holländaren Jouke van der Zee och britten Peter Bentley på. Peter Bentley arbetade med att utveckla sådana system och en trolig utvecklingsväg är att olika typer av system (som är bra på olika saker) kombineras.

Riskerna överdrivs

Men det finns en risk för att Internet målas upp som farligare och osäkrare än vad det är. Det menade till exempel konferensens inledningstalare professor Michael Levi, Cardiff University. Han påpekade att olika internetbrott visserligen ökar snabbt sett till procent, men att ökningen sker från en låg nivå (Internet är ju färskt). Medierna har dock fattat tycke för internetbrott, så uppmärksamheten blir stor. Det gäller inte minst hackers. Riskerna med 16-åringar som bryter sig in i system ska dock inte överdrivas, menade John Austin som talade om olika typer av databrott. De finns visserligen, men John Austrin hävdade att det är de professionella hackarna och brottslingarna som är farliga.

Även om bedragarna kommer att ligga långt framme, både vad gäller uppfinningsrikedom och teknik, så finns det starka krafter som kommer att driva på jakten på bedragarna. Detta utöver vad myndigheter gör, där dock resurser och juridiska skillnader mellan olika länder kan utgöra begränsningar.

Förtroende och tillit för elektroniskt överförd information

För att koppla till syftet med Telematik 2004:

Risker för finansiella bedrägerier kommer att bli en faktor att ta mer hänsyn till när alltfler gör alltmer via framförallt Internet. Det gäller både vid informationsinsamlande, rådgivning och i affärer via nätet. Men seriösa banker, säljare och kanske marknadsförare (portalägare) kommer att lägga ned mycket kraft och pengar på att alla kan lita på att identifikation och förmedling, avtal och affärer sköts pålitligt. Annars hotas hela den tillväxt i den här typen av handel som ”alla” räknar med.

Handel på nätet kanske också går i bräschen för en större kunskap om hur den elektroniska tekniken kan användas även på andra områden. Kanske behöver människor inte ens handla, mediernas rapportering kring hur och var man kan handla på nätet och vilka risker som finns bygger i sig upp kunskap. Så om många vet hur elektronisk handel fungerar och har förtroende för den så kan det ge positiva ”spin-off-effekter” till hela inställningen till tekniken. Och vice versa. Ekonomiska förluster, eller risker för sådana, är också en mycket konkret effekt – konkretare än hur andra risker med elektronisk information kan beskrivas.

Den enskilda människan måste bli mer uppmärksam på att det finns en rånrisk även på nätet och att den är betydligt mer sofistikerad än den synliga brottslighet som man är van vid, som ficktjuvar, inbrott i ens hem och så vidare. Men eftersom det finns många som trots vetskap om risken bär plånboken i bakfickan och hänger handväskan på ryggstödet på restaurangen så kommer det att finnas en bra ”marknad” för de skrupellösa som kan använda elektroniska tekniker.

Här finns sannolikt en generationsskillnad, men slutsatserna av detta är inte givna. Medan äldre sannolikt är försiktigare till internethandel, så kanske de också löper mindre risk att bli lurade. Kanske är det också så att det är äldre som reagerar mer på vad som skrivs om risker och

elektroniska brott i medierna. Yngre är vana att använda nätet även för affärer, och de flesta har sannolikt gjort det många gånger utan att något oönskat hänt. ”Det händer inte mig”-inställningen kommer säkert att leda till att en del drabbas. Här spelar det säkert in att riskerna för de mer vanliga brotten är mer synliga – som att många faktiskt har drabbats av cykelstöld eller liknande – än vad de elektroniska riskerna är. Det kan invagga i falsk säkerhet, liksom det skulle kunna leda till större rädsla än vad som egentligen är motiverat.

För säljare och mellanhänder är det av största vikt att så många risker som möjligt löses utan att det antingen gör det mer omständligt att agera via Internet eller fördyrar transaktionerna. Konkurrensmedlet är inte minst priset, och här skulle det vara ett allvarligt hot om till exempel kontokortsföretagen bestämmer sig för att ta ut en avgift på internethandel för att täcka bedrägerier och uteblivna betalningar (för det senare är det väl framförallt banker som står risken).

Fungerar Internet som tänkt så kommer transaktionskostnaderna att minska. Det gäller såväl varor och tjänster, som värdepappershandel, där vi redan ser hur elektroniska mäklare slår sig in med lågpriskoncept.

Kommersiella krafter driver på säkerheten

Se på vad det är som är hetast och mest förväntningar på i världens aktiemarknader idag? Jo, internetbolag och framförallt de som har med handel via Internet att göra. Det är en explosionsartad tillväxt för den handel som ska motivera de uppskruvade förväntningarna på alla internetrelaterade (och de som vill räkna sig som internetrelaterade) bolag runt världen.

Det skulle vara totalt förödande för dessa värderingar och förväntningar om det blir så att konsumenterna, oavsett om de är privatpersoner eller företag, inte vågar använda Internet för att säkerheten upplevs som bristfällig.

Konsekvensen av detta är att det är starka krafter som kommer att lägga ned stora resurser, långt större än vad tillsynsmyndigheter kan lägga, på att internethandeln blir säker och på att bedrägerier spåras.

Eftersom medierna dessutom så här långt gärna ägnar utrymme åt riskerna med internethandel, vilket är helt rimligt att de gör, så riskerar bedrägerier som drabbar privatpersoner snabbt att ge den här handelsformen dålig publicitet och därmed dåligt rykte.

Bedrägerierna får inte drabba de enskilda kunderna, knappast med besvär (som att få sitt kortnummer eller någon personuppgift stulen) och framförallt inte ekonomiskt. Idag är tendensen den att banker eller säljare tar den ekonomiska smällen när någon blivit lurad i internethandeln. Men det är förstås så att också kostnaderna för dessa bedrägerier läggs på kunderna, antingen påverkas räntevillkoren i banken eller också dess avgifter och vad gäller säljarna av varor och tjänster så måste förstås de förluster som görs kompenseras genom priset på övriga varor.

Att skydda internethandeln är alltså en drivkraft, den andra syntes tydligt på Fraud 4-konferensen. Många talare, ofta före detta poliser, jobbar idag som säkerhetsexperter eller -konsulter. Deras levebröd är att täppa till kryphål, avslöja bedragare och så vidare. Säkerhetsbranschen är en snabbt växande och lönsam bransch, inte minst system och program för säkerhet. Till exempel har kryptering gått från att vara en märklig konstform till att vara en standardsak även för hemdatorn, påpekade datasäkerhetskonsulten David Chaikin.

Till saken hör väl nu också att säkerhetsexperterna också måste se till att göra världen uppmärksam på de faror som finns. Det bidrar ju till att öka deras marknad.

Två typer av bedrägeririsker för individer

Bedrägerierna som kan drabba en enskild individ kan delas upp i två huvudgrupper. Den ena är stöld och missbruk av kreditkort, någon som tömmer mitt bankkonto och så vidare. Alltså någon form av konkret (om detta nu är rätt ord för databrott) tillgrepp. Här är då intrycket att det under de närmaste åren kommer att finnas starka krafter som av kommersiella skäl kommer att hjälpa den enskilde.

För den andra huvudgruppen av bedrägerier går det inte att räkna med samma skydd. Det är lurendrejeri, där jag som privatperson fastnar för ett Nigeriabrev, köper värdepapper som visar sig vara bluff, låter mig luras av en falsk bank som erbjuder fantastiska villkor för de pengar som jag sätter in (En vanlig kategori sådana är sparklubbar, som då förhoppningsvis, ur bedragarens perspektiv förväxlas med sparbanker och som erbjuder till exempel 25 procents riskfri avkastning per år). Varianterna är många, en del svåra att genomskåda, andra lättare. En gammal förnumstig tumregel som ändå stämmer är att det som ser för bra ut för att vara sant ofta är precis det, alltså för bra för att vara sant.

Men de här typerna av bedrägerier kommer ändå att skörda många, många offer. Utsikten att tjäna mer pengar lockar alltid många, pyramidspel dyker upp med jämna mellanrum – de går utmärkt att starta via Internet. Med ett större intresse än någonsin (runt världen) att placera pengar för att få en bra avkastning så kommer det att finnas många gyllene tillfällen för bedragare. En faktor som hjälper dem är globaliseringen, det blir vanligare att till exempel en svensk lockas att placera i ett börsbolag i Malaysia – och det som man inte känner till är mycket lättare att bli lurad av.

På det här området finns det inte lika starka krafter som driver på för att stoppa eller i varje fall minimera brotten. Det blir istället mer en fråga för myndigheter, som då inte har samma resurser att mobilisera.

Medier, skvaller och sunt förnuft ska skydda

Här får nog medierna bli en viktig varningskanal. Och troligen blir de gärna det, området intresserar läsare och tittare. Men det finns också andra vägar. En av besökarna (inte talarna) på konferensen representerade ett företag som försöker avslöja sådana här typer av bedragare. De hade en hemsida som listar olika typer av bedrägerier, några som finns på sidan just nu är Melchizedek, landet som inte finns, sparklubbar och Nigeriabrev. Sidan heter www.quatloos.com och är en underhållande läsning. Sannolikt kommer varningar för bedrägerier att spridas även på andra sätt via nätet, som i chatgrupper, på skvallersidor för finansiell information och så vidare. Och sådan informationsspridning kan gå snabbt, återigen, den nya tekniken gör att både bedragarna och de som vill avslöja dem kan arbeta snabbare och mer spritt än tidigare.

Men den allra viktigaste faktorn för att stoppa eller minimera finansiella lurendrejerier är sunt förnuft. Känner jag till vem som står bakom det här? Förstår jag vad jag ger mig in på? Ser det rimligt ut? Finns det någon jag kan fråga, som känner till avsändaren ? Nu kan man dock vara tämligen säker på att ambitionen att göra bra affärer i många fall kommer att vara större än det sunda förnuftet. Tyvärr.

Det gäller att stå emot trycket från vad som låter lockande och övertygande. Psykologen Raj Persaud påtalade hur svårt detta kan vara i en organisation. Den finansiella psykopaten, eller den mest troliga att begå sådana brott, var inte sällan den som sågs som underbarn. I en organisation kan det vara tufft att gå emot den som alla andra tror på. Det-

samma gäller i investeringar, om jag tycker att något ser märkligt ut men många andra har lockats med så är det kanske alldeles rätt att stå emot.

Vad händer då framöver?

Trycket på säkerhetsavdelningarna ökar, sa den holländske datasäkerhetsexperten Jouke van der Zee som en av två huvudpunkter (den andra var utvecklingen av intelligenta system).

Men även privatpersonen får tänka på sin säkerhet, i ungefär samma banor som stora som små företag och organisationer måste göra. En rad talare gav samma råd:

- Se till att de säkerhetsrutiner som finns verkligen fungerar. Testa och testa igen.
- Använd lösenord.
- Brandväggar, som håller isär interna datanätverk med externa sådana är väl mer för företag och organisationer, men det var ett mycket vanligt råd.
- Kryptera känslig information som skickas via Internet. Viss kryptering är bättre än ingen kryptering. Detsamma gäller egentligen alla säkerhetssteg, även om de inte är heltäckande så är det bättre att de finns än att de inte finns.
- Ställ klockan på datorn rätt. Det var ett märkligt enkelt råd som FBIs representant gav, men det underlättar när en bedragare ska spåras.

2. Inledning:

Bakgrund och omfattning

Internationella finansiella bedrägerier kan omsätta mer än 20 miljarder pund, runt 275 miljarder svenska kronor i år. Bland svenska börsbolag är det bara Ericsson som har ett högre börsvärde än så. Bedrägeriberäkningarna har gjorts av konsult- och redovisningsjätten PricewaterhouseCoopers.

Och enligt samma firma är det många bedrägerier som aldrig utreds på grund av att utredningarna är för svåra och komplicerade. Därför vet heller ingen säkert hur stora bedrägerierna är, inte heller PricewaterhouseCoopers.

Fraud 4 var en konferens om internationell finansiell brottslighet. Som namnet säger var det den fjärde konferensen i detta ämne. Tre av fyra konferenser har hållits i London, så även denna. Den första hölls 1995. Upphovsmannen till konferensen var engelsmannen Brendan Hewson som under många år jobbade på Scotland Yard och där utbildade poliser, bankfolk och andra från hela världen om finansiell brottslighet och hur den kan bekämpas. Brendan Hewson gick därpå från Scotland Yard till Bank of America (som numera heter NationsBank) som ansvarig för internationella undersökningar. Han och advokaten Richard Parlour vid Stephenson Harwood i London, specialiserad på finansiell brottslighet tyckte att det fanns ett behov av att så många som möjligt med erfarenheter av finansiell brottslighet kunde träffas.

Vid den första konferensen kom deltagarna från 30 länder, vid den andra från närmare 50. 1998 var 80 länder representerade och nu 1999 bröts 100-vallen. Deltagarna kommer från officiella institutioner som centralbanker, tillsynsmyndigheter och liknande samt framförallt från den finansiella världen, det vill säga banker och försäkringsbolag. Totalt hade 350 personer i år betalat den ganska saftiga konferensavgiften.

Konferensen styrs av en central idé: Bedrägerierna kan inte stoppas, men de kan minimeras. Utbildning behövs för alla finansiella institutioner, oavsett storlek och var de finns, i industriländernas finansiella centrum eller i utvecklingsländer. Konferensen arrangeras av Ifex, International Financial Exhibitions Ltd, som specialiserat sig på konferenser för den finansiella världen.

Programmet

Fraud 4 pågick i tre dagar. På konferensen framträdde närmare 50 talare. Varje dag hade ett tema, men avgränsningen var inte total, ämnen tenderar att gå in i varandra. En rad punkter handlade om vad som händer inom lagstiftning, policyutveckling, hur olika regioner eller sammanslutningar (som EU, Europarådet och FN) ser på problemen etcetera. De här mer övergripande föredragen har hoppats över i den här rapporten. Det här är i stället ett försök att sammanfatta vad som sades i frågor som mer direkt påverkar enskilda individer, som typer av bedrägerier, hur man kan skydda sig, varifrån hoten kommer och så vidare. Det är dock inte de mest konkreta svaren på sådana frågor som ges på en sådan här konferens.

De refererade talarna är indelade i tre grupper;

1. Exempel på bedrägerier.
2. Elektroniska hot och försvar.
3. Personligheten hos en bedragare.

Sist i den här rapporten finns ett sammanfattande kapitel, där jag försökt göra en koppling från vad talarna sagt (och vad som talades om vid luncher och under andra pauser) till hur detta påverkar individen. Referaten är som regel inte ordagranna, utan komprimerade versioner av vad som sades. Merparten av de talare som refererats framträdde under dag två, som hade den övergripande rubriken ”Bedrägerier på finansiella marknader utan gränser”.

Internetbedrägerierna dominerar

Det största bedrägeriområdet är Internet, som står för drygt hälften, eller runt 140 miljarder svenska kronor enligt den beräkning från PricewaterhouseCoopers som nämndes inledningsvis. I de internetrelaterade bedrägerierna dominerar bruk av stulna eller falska kontokortsnummer eller identiteter, enligt Bill Cleghorn som är chef för bedrägeriundersökningar hos PricewaterhouseCoopers och var en av talarna på konferensen Fraud 4.

På internetsidan handlar det alltså om många, många små bedrägerier – som banker, företag (som säljer varor eller tjänster som de inte får betalt för) eller privatpersoner förlorar pengar på.

För det näst största bedrägeriområdet handlar det om en bråkdel av antalet internetfall, men betydligt större belopp i de enskilda fallen. Bedrägerier mot internationella valutafonden IMF eller Världsbanken beräknas till 1,6 miljarder pund, eller knappt tio procent av totalen, i år.

En slutsats från Londonkonferensen är att bedrägeriomfattningen är större än man tidigare trott och att det är en ”tillväxtbransch”.

Finansiella bedrägerier är ett brett begrepp. Här ryms kontobedrägerier, penningtvätt, korruption, rena bedrägerier som pyramidspel och Nigeriabrev, moms och tullbrott, svartjobb med mera.

De flesta bedrägerierna blir aldrig kända. Det kan förstås vara så lyckade brott att de aldrig upptäcks, men ett tyngre skäl är att mycket av vad som sker i företag och organisationer aldrig blir offentligt.

Dessutom har många bolag varit ovilliga att tala om att de drabbats av externa brott, men enligt amerikanska FBI har nu problemet blivit både stort och accepterat så att fler bolag nu anmäler vad som hänt.

Brotten globaliseras

En annan slutsats vid konferensen var att brotten blir mer och mer internationella, nästan oavsett vilken typ av bedrägeri det gäller. I många fall är ju gränsöverskridandet en förutsättning (som vid tullbedrägerier) men med flera inblandade blir kontrollmöjligheterna mindre. Olika länder har olika lagstiftning, och frågan om var brottet skett blir snabbt komplicerad. Är det där de drabbade finns, dit pengarna fördes, dit pengarna därefter flyttades, där förövarna finns?

Enligt Bill Cleghorn sprids bedrägerierna mer och mer och blir dessutom svårare att klara upp. Bedrägerierna utvecklas hela tiden, inte minst som nya varianter på redan kända former.

Martin Grives, i ledningsgruppen på brittiska Serious Fraud Office (som arbetar med flera departement), påpekade vikten av att internetbedrägerier inte får bli en accepterad risk – på det sätt som kanske sker med ”vanliga” kontokortsbedrägerier. Där vältras dessa kostnader över på kunderna. Och enligt Grieves skulle mer ansvar kunna läggas på internetoperatören för de risker som kunderna (både köpare och säljare) löper.

Konferensens inledningstalare, kriminologiprofessorn Michael Levi (University of Cardiff) var inte lika säker på hur stor omfattningen finansiella bedrägerier har. Det finns, med en forskares krav på bevis, inga säkra uppgifter.

Att få bort alla bedrägerier är inte att hoppas på, enligt Michael Levi. Men att minska riskerna, eller att få varje bedrägeri att bli mindre är viktiga steg på vägen.

Michael Levi tog också upp exempel på hur den tekniska utvecklingen gått bedragarnas väg.

Piratprogram kan beställas via Internet, mer diskret för tillverkaren av dessa som inte behöver ha antingen den distribution som tidigare krävdes, eller marknadsföring som annonser i tidningar – både butiker och framförallt annonser kan vara lätt synliga för antingen polis eller tillverkaren av de ”riktiga” programmen.

Men med Internet kan program och förfalskare (och säljare) finnas i ett helt annat land, med ett juridiskt system som kan vara till god hjälp. Det finns gott om skatteparadis, som kanske också har andra lagar som gör det svårt att komma åt ekonomiska (och andra) brottslingar.

Gamla brott blir mer effektiva

”Gamla kända” bedrägeriformer får också större och snabbare spridning med hjälp av Internet. Till exempel är stölder av kontokortsnummer inte nytt, men med Internet finns det både fler möjligheter att komma över kortinformationen och att utnyttja dem. Ett annat exempel är värdepappersbedrägerier, där en trovärdig hemsida kan vara mångfalt effektivare och billigare än att som tidigare använda till exempel nyhetsbrev och försäljare som ringer (samt i vissa fall ha förtroendeingivande kontor att visa upp).

Och uppmärksamheten på de här ”nya” typerna av gamla brott, som att skumma ett kontokorts nummer och personuppgifter, får inte dölja det faktum att de gamla men mindre spektakulära riskerna finns kvar – till exempel att kreditkortet helt enkelt stjäls och används – påpekar Michael Levi. Även om ökningstakten i en del internetrelaterade brott är hög, så sker tillväxten i många fall från en låg eller mycket låg nivå.

”Mer allmänt uttryckt, vi kan bli fixerade vid ”databedrägerier” eller ”internetbrott” och glömmer att det finns andra och större bedrägeririsker”, som den egna personalen i ett företag eller organisation.

Exempel på bedrägerier

3. Lisa Kate Osofsky:

Så här jobbar FBI

Lisa Kate Osofsky, arbetar på Federal Bureau of Investigations (FBI) där hon är rådgivare/sakkunnig i juridiska frågor om tillslag bland annat mot misstänkta bedrägerier. Hon talade om olika angreppssätt mot finansiella bedrägerier i den datoriserade världen.

Var är brottslingarna ? Och varför ?

”Klockan är tre på morgonen. Din mobiltelefon ringer, du svarar och får besked att bege dig direkt till Strategic Information Operations Center (SIOC) vid FBIs huvudkontor. Du kör fort och väl framme knappar du in rätt kombination och den tjocka metalldörren öppnas. Du går in i ett rum där tio andra beslutsfattare redan finns. Datorskärmarna som finns runtom i rummet flashar fram information från hela världen. Hela tiden uppdateras vilka nya incidenter som inträffar och var de sker.

Det du vet nu är att någon tagit sig in i det amerikanska försvarsdepartementets datasystem, liksom i två av de största bankernas system och i flygledningssystemet vid O´Hara-flygplatsen i Chicago. Vidden av intrången är inte kända, men det verkar som inkräktarna arbetat från en rad ställen runt världen, från Europa till Mellanöstern till USA. Du förstår ännu inte hur de olika attackerna hänger ihop, men det är ditt jobb att ta reda på det och stoppa dem innan något förskräckligt händer.

Är det terrorister, i USA eller någon annanstans? Eller är det ett finansiellt bedrägeri som använder datorer runt hela världen? Är det en samlad attack? Eller är det två eller fler? Det finns många andra frågor, inte minst om vilka länders lagar som är tillämpliga, om det finns diplomatiska ställningstaganden?

Det här är bara några av de frågor som lagövervakarna i världen har att ta ställning till i kampen mot dagens brottslighet. Och problemet är att när brotten inträffar, så kan vi inte vara säkra på exakt vad det är som händer. Mer sofistikerad teknologi och den alltmer globala världsekonomin gör att gamla gränser inte längre gäller. Vi upptäcker att vi

verkar i en era där satelliter runt världen gör det möjligt för bedragarna att kommunicera utan att upptäckas av några tillsynsmyndigheter, där en tangenttryckning kan flytta miljonbelopp från en hemisfär till en annan, där en begåvad hacker kan infiltrera ett datasystem som styr ett lands vapenutvecklingsprogram.

Goda nyheter – på gott och på ont

Datorer och andra tekniska framsteg har länkat oss samman på ett sätt som var otänkbart tidigare. Det är goda nyheter för ärliga, hårt arbetande entrepenörer, affärsmän och konsumenter av allt från finansiella tjänster till kontorsutrustning. Det är goda nyheter för oss som ska se till att lagar följs, vi kan kommunicera med våra kollegor i andra länder snabbt och effektivt. Vi kan nu använda datorer för att konstruera sinnrika program som samlar information om kriminella och analyserar denna nästan omgående. Så teknologin gör det möjligt att täcka sådant som tidigare inte gick att övervaka.

Men det är också goda nyheter för de kriminella. Bedragarna som vill bli rika snabbt behöver inte sätta en fot på banken som han/hon vill stjäla stora belopp från. Han behöver inga flyktbilar eller flykthjälp. Med hjälp av kryptering och annan teknik kan han kommunicera med sina ”kollegor” elektroniskt, som sagt på sätt som inte någon kan upptäcka.

Om min presentation målar upp de problem som vi har att möta som skrämmande, så är det precis så verkligheten är. Om den får hindren att verka oöverstigliga, så stämmer det däremot inte. Trots brottslingarnas resurser och kunskaper så kan vi lösa många brott, dessutom snabbt.

Lyckade FBI-exempel

Till exempel kunde FBI avslöja den som spred Melissaviruset över världens datorer innan en katastrof inträffade. Med hjälp av polis och andra myndigheter runt nationen, systemadministratörer och andra i företag kunde FBI ta fast den skyldige innan han kunde ställa till stora systemkrascher i datavärlden. I en annan undersökning, känd som Solar Sunrise, hjälpte det amerikanska försvarsdepartementet, justitiedepartementet, NASA och israeliska myndigheter, för att nämna några, FBI att avslöja hackers i Israel och Amerika som hade tagit sig in i hemliga

databaser runt världen. Det fallet gällde klassificerad, eller hemlig, statsinformation men det kunde lika gärna ha rört sig om finansiell information.

PairGain

Så sent som förra månaden (april 1999, föredraget hölls i maj, rapportskrivarens anmärkning) dömdes en 25-åring från North Carolina i USA för fem åtalspunkter för finansiellt bedrägeri. Han hade uppsåtligen spridit falsk information på Internet som gällde hans arbetsgivare PairGain Technologies. PairGain tillverkar utrustning för höghastighetsöverföring över telenäten. Den sista april 1999 dömdes Gary Hoke för att skickat ut en falsk nyhetssida med nyhetsbyrån Bloomberg News Service som avsändare. Där hävdades att PairGain skulle köpas upp, till dubbla den aktuella börskursen, av ett israeliskt företag, ECI Telecom. Hoke hade gjort sin rapport så lik en Bloombergsida som möjligt. Utifrån den falska informationen steg PairGains aktiekurs med över 30 procent innan bolaget och Bloomberg upptäckte vad som hänt. Sju gånger fler PairGain-aktier än vanligt hann omsättas under den dagen, på grund av den falska informationen.

Hoke, ingenjör på PairGains enhet för utveckling och design, använde anonym e-post och websideservice för att få ut sin falska hemsida. Trots att han vidtagit många steg för att sudda ut spåren efter vad han gjort kunde databrottsspecialister från FBI och SEC (den amerikanska finansinspektionen, tillsynsmyndighet för finansmarknaden, rapportskrivarens anmärkning) spåra honom genom att gå igenom skuggfiler från den webservice som Hoke använt för att lura aktiemarknaden. Lagren av anonymitet som Hoke använt räckte inte långt utan spåren ledde till PairGains eget datanätverk, till Hokes dator och hans internetkonton. Det nära samarbetet mellan myndigheter och den privata sektorn gjorde det möjligt att identifiera och åtala Hoke innan skadorna blev för stora. Vem vet vilken falsk marknadsinformation som publicerats därnäst om inte samverkan fungerat så effektivt?

”Antik” pc räckte

För lite mer än ett år sedan dömdes Vladimir Levin till tre års fängelse och 240 000 dollar (drygt två miljoner kronor) i återbetalning för onlinebankrån som han och hans medbrottslingar begick mot Citibank

1994. Som många av er känner till använde Levin en ”antik” persondator med 286-processor samt stulna lösenord och id-nummer till anställda hos tre av Citibanks företagskunder. Levin tog sig in i Citibanks system där företagskundernas bankkonton hanteras, där stora flöden av pengar styrs mellan konton i olika länder. Mellan juni och oktober 1994 förde Vladimir Levin vid 40 tillfällen över pengar, sammanlagt 10 miljoner dollar. I oktober 1994 lyckades anställda vid ryska televerket identifiera var överföringarna skedde, nämligen mjukvaru- och redovisningsfirman AO Saturn, där Levin var systemansvarig. Ryska och amerikanska myndigheter beslagtog datorer och disketter och kunde efter analys av innehållet binda Levin och hans kumpaner till den brottsliga verksamheten.

Ur FBIs perspektiv var en av de viktigaste punkterna med Levinfallet att Citibank gick till FBI redan i juli 1994, när de första 400 000 dollarna togs ut. Banken samarbetade nära med myndigheterna och därigenom gick operationen snabbt framåt. Konton dit Levin förde pengarna kunde frysas och till sist kunde allt utom 400 000 dollar återföras.

Fler, men för få, rapporterar

Men det är inte alla banker, företag eller andra drabbade som rapporterar vilka databrott de utsatts för. I en undersökning från 1997 riktad till säkerhetschefer, där 563 företag och myndigheter svarat, hade 49 procent förra året utsatts för dataintrång. Och det var inte bagateller, här ingick sabotage, bedrägerier, stöld av hemlig information som gjorts av både egna anställda och utomstående. Endast 18 procent av offren rapporterade vad som hänt till polismyndigheterna. Men utvecklingen går åt rätt håll, i mars 1999 visade en liknande studie att nära en tredjedel av alla drabbade nu anmält det inträffade.

För att få fast databrottslingarna måste vi ha de verktyg som behövs. Vi har möjligheterna att få in information, vi kan få hjälp av kunniga personer från den privata sidan, vi har ett fungerade nätverk med myndigheter i andra länder, liksom med privata säkerhetsexperter. Vi måste fortsätta att använda dessa kanaler effektivt. Vi är mycket medvetna om att både de som finns i och utanför tillsynsmyndigheterna måste utbildas i hur sårbara datorer och system är och vad som krävs för att skydda dem. Vi har experter som kan den mest sofistikerade tekniken och vi fortsätter att rekrytera sådan kompetens. Dess-

värre kan vi inte alltid betala lika bra som Silicon valley, så ibland för vi här en kamp i uppförsbacke.

Ställ klockan rätt

Det finns sätt att skydda sig, som varje finansiell institution och många företag borde överväga. Installera brandväggar (firewalls), elektroniska barriärer mellan interna och externa nätverk. Installera system som avslöjar om någon försöker att ta sig in (men de måste vara tillräckligt bra för att klara upprepade attacker). Använd nummerpresentatörer som talar om var ingående telefonsamtal kommit från. Rapportera intrång som sker till myndigheterna. Anlita säkerhetsexperter. Använd användar-id:n och lösenord. Använd program som upptäcker virus, kryptera informationen – använd högsta tillåtna krypteringsgrad, 128-bitar. Och, för att hjälpa oss få fast bovarna, se till att era datasystems interna klockor är synkroniserade till rätt tid. Det är en god hjälp för att kartlägga en bedragares steg.”

4. Nicholas Ridley:

Hotet från öst

Nicholas Ridley, intelligence analyst vid Europol (samarbetsorgan för europeiska polismyndigheter), och rådgivare till EU-kommissionen, talade om bedrägerihot från det forna östblocket – ett område han följt under nästan 15 år.

Å ena sidan har ökad politisk öppenhet, massmediebevakning och en allt snabbare informationsspridning gjort att vi vet mycket mer och snabbare idag än tidigare. Inte minst gäller det järnridåns fall och vad som hänt under det decennium så gått sedan dess.

Å andra sidan är vi på väg att blunda för hur kriminaliteten, framförallt den ekonomiska, från de forna östländerna kommer att påverka oss.

Ryssland med världens sämsta centralbank

För att börja med Ryssland, så har landet under en del av 1990-talet haft en centralbanksledning med usla kunskaper. En centralbankschef, Gerashenko, utnämnde till och med sig själv till den sämsta centralbankschefen i världen, utan att skämmas för det. Den ryska centralbanken har under decenniet fått en mängd tuffa uppgifter och en viktig roll i uppbyggnaden av Ryssland. Men, det har skett utan tillräckliga resurser, både vad gäller kunskap, människor och finanser. Detta är en förklaring till hur så mycket pengar har kunnat försvinna ur landet, inte minst över fyra miljarder dollar av Internationella Valutafondens (IMF) lån till landet. Fem chefer i den ryska centralbanken har nu dömts till fängelse för olovliga utbetalningar. Vidare har banken, i strid med lagen, erbjudit banker lägre räntor, banksanställda har givit otillåtna lån och en rad andra finansbrott. Och tre EU-länder har drabbats av lånebedrägerier av bolag med kopplingar till Ryska Banken, ett namn som påminner om Ryska Centralbanken men med adress och kontor där en annan, riktig, rysk bank finns.

Globala ryssar

Men ryska finansligor härjar inte bara i Ryssland, utan också i andra

länder (i augusti i år skrevs det till exempel om hur amerikanska banker använts för pengatvätt av ryska ligor, rapportskrivarens anmärkning. Så långt bort som i Australien kombineras organiserad illegal invandring med ekonomiska brott. En grupp av dessa ryssar som verkar i Australien har visat sig vara största ägare i banker med säte i Sibirien. Och en rad bulgariska bolag har visat sig ha kopplingar till bedrägerier med falska affärsverksamheter (bland annat momsbrott och ”vanliga” bedrägerier). De bulgariska bolagen har i sin tur kopplingar till tillgångar med ryska intressen. Västerländska banker och andra finansiella institutioner används därpå för pengatvätt. Och de ryska aktörerna kan visa fram rekommendationsbrev eller intyg som kommer från den ryska centralbanken – som i och för sig gör sitt bästa men som inte klarar alla arbetsuppgifter efter snart ett decennium med ständigt mer och viktigare saker att göra.

Så till Polen, som till skillnad från Ryssland kan visa upp en lysande ekonomisk tillväxt under det senaste decenniet. Men även här finns det en rad exempel på finansiella bedrägerier. År 1990 kollapsade banken Safe Savings Bank sedan dess grundare, som han planerat, drog sig ur. Bankens verksamhet togs därefter över av en grupp som under tre år tvättade motsvarande 3,5 miljarder dollar med hjälp av banken. Därefter övertogs banken av en tidigare sovjetisk medborgare som tjänade pengar på bedrägerier i samband med de stora utförsäljningarna av statliga bolag till allmänheten i Ryssland. I nästa vända råkade de polska banken i händerna på en rysk bank, som ”av en händelse” verkat under samma femårsperiod som en grupp kända ekonomiska brottslingar.

I Kalifornien i USA får myndigheterna problem med organiserad rysk brottslighet, som har en lång historia i landet, vad gäller försäkringsbedrägerier. Till exempel arbetsplatsolyckor, hälsoförsäkringar och andra olyckor. Mönstren känns igen från till exempel de rysk-australiska härvorna: Några personer ser till att få anställning hos respektabla företag (som läkarhus) för att få tillgång till dokumentation, få rätt kontakter och annat. Så ordnas personer som kan ställa upp som offer. Och när nätet börjar dras åt på ett håll så flyttas verksamheten till en annan stat, de medicinskt kunniga börjar på en annan firma, men i bakgrunden finns hela tiden samma ryska ligor. Det som framförallt ger myndigheterna något att oroas över är skrupellösheten. Försäkringsbedrägerierna innehåller hot eller till och med mord på den som vågar vittna. Åklagare har hotats.

Efter denna uppräkning av allehanda brott med ryska förtecken var Nicholas Ridleys sammanfattande profetia för framtiden: ”We ain´t seen nothing yet” vad gäller hur dessa kriminella organisationer kan påverka finansiella system, branscher och hela samhällen.

5. Neil Jeans:

Finansmarknaden som tvättmaskin

Neil Jeans, före detta aktiemäklare och polis vid enheten för pengatvätt hos Londonpolisen. Nu anställd vid den brittiska tillsynsmyndigheten Financial Services Authority.

”De finansiella marknaderna har rykte om sig att vara rena och rättvisa platser att göra affärer på. Detta gör också att den globala finansmarknaden lockar även kriminella entrepenörer, lika mycket som vanliga investerare.”

Optioner och terminer, bra för pengatvätt

Neil Jeans talade om hur värdepappershandel används för pengatvätt, inte minst pengar från narkotikahandel. Enligt FN genererar världens narkotikahandel varje år 400-500 miljarder dollar i intäkter (ungefär två gånger den svenska bruttonationaprodukten). Ett allt vanligare sätt att få in en del av dessa pengar i det finansiella systemet är att använda derivat på de finansiella marknaderna. De vanligaste formerna av derivat (ett värdepapper som baseras på ett underliggande värde, som en aktie, eller en korg av valutor, eller en obligation etcetera) är optioner och terminer. Optioner ger rätten men inte skyldigheten att inom en viss tid köpa eller sälja till exempel hundra aktier i Volvo för ett bestämt pris. Terminer är till skillnad från optioner tvingande, det vill säga jag köper eller säljer skyldigheten att köpa eller sälja.

Derivat för pengatvätt lyftes fram som en snabbt växande trend i den rapport som en grupp inom brittiska finansmyndigheter tog fram i början av året (The Financial Action Task Force Typologies Report, förkortat FATF). Också aktiehandel på den amerikanska ”börsen” Nasdaq (som framförallt listar nyare bolag och därmed har många teknologiföretag som just nu lockar placerarna) lyfts fram som ”tvättmaskin”. Handeln med derivat eller aktier sker alltså helt enligt reglerna, men resultatet blir att svarta pengar görs vita, utan stora kostnader som pengatvätt normalt innebär.

Neil Jeans beskrev ett exempel på hur derivathandeln används för pengatvätt. En tungt skäl till varför den här handeln nu lockar den här typen av affärer är att omsättningen i derivathandeln skjutit i höjden under senare år. Inte ens stora tvättransaktioner märks egentligen i det stora hela.

Spegelhandel

De många varianter på derivat och storleken på handeln, kombinerat med att detta är en komplex och svårgenomtränglig materia, ger stora fördelar för den som vill och kan använda de här marknaderna för att tvätta pengar. Neil Jeans exempel handlar om ”mirror trading”, fritt översatt spegelhandel. Det innebär, förenklat, att ta en position som ger vinst om priset på den tillgång som derivatet baseras på stiger och en likadan position som betyder vinst om priset på den underliggande tillgången faller. Därmed uppkommer alltid en vinst- och en förlustaffär. Och genom vinsten kan den som haft pengar att tvätta visa fram ett legitimt sätt på hur pengarna har tjänats. Han/hon har alltså inte mer pengar än tidigare (hela derivataffären är ett nollsummespel, förutom kostnaderna för själva affärerna) men pengarna är alltså vita istället för svarta.

Spegelhandel är inget nytt fenomen. Neil Jeans refererade till Capcom, som var derivatverksamheten för banken BCCI, som kraschade efter en rad otillåtna affärer i början av 1990-talet. Capcom använde den här typen av handel för att tvätta åtskilliga tiotals miljoner dollar för sina kunder. Redan de gamla grekerna höll faktiskt på med optionsaffärer, Aristoteles refererade drygt 300 år före Kristus till filosofen Thales som tecknade rätten (alltså en option) på att få använda en rad bönders olivpressar. När skörden blev stor kunde han hyra ut pressarna till betydligt högre pris än vad han behövde betala bönderna.

Billigt tvättmedel

Derivathandel är alltså ett billigt sätt att tvätta svarta pengar. Trenden är dessutom att det blir billigare och billigare att handla på världens kapitalmarknader. Den stora kostnadsminskningen sker när skillnaderna mellan köp- och säljkurser (vad som på finanssvenska kallas spread) minskar. Denna spread är dessutom den tunga kostnaden för pengatvättarna. Spreaderna minskar här likviditeten ökar, det vill säga

att det handlas mer och mer (och riskerna att bli sittande med innehav som inte kan säljas snabbt eller utan att kurserna rör sig minskar).

Dessutom gör den tekniska utvecklingen, där värdepappershandel via Internet är en av de snabbast växande delarna, att transaktionskostnaderna sänks av den ökade konkurrensen (samt att kunderna själva gör alltmer av det jobb som mäklare tidigare gjorde).

”Möjligheterna till bedrägerier och pengatvätt på världens snabbrörliga och snabbt föränderliga finansmarknader snarast ökar. Inte bara vad gäller derivat. Men det är inte åtgärder som drabbar själva handeln som ska till, utan istället att få till en global standard, till exempel vad gäller sekretess, som gör det lättare att se tvättoperationer”, säger Neil Jeans.

6. John Shockey:

Landet som är ett bedrägeri

Ett av de två mest underhållande föredragen på konferensen var den amerikanske åldermannen John Shockeys presentation av landet Melchizedek. John Shockey är nu rådgivare till det amerikanska finansdepartementet (US Treasury) där han tidigare var anställd (sedan 1946!). Han har arbetat med finansiella bedrägerier sedan 1974 och bland annat vittnat i över 80 rättegångar i ett halvdussin länder.

Melchizedek har enligt John Shockey verkat runt världen sedan 1990. Detta utan att de personer som står bakom ens åtalats. Under åren har John Shockey svarat på frågor om landet i skilda medier som affärsmagasinet Forbes, dagstidningarna Times, Washington Post, Wall Street Journal samt flera tv-stationer. Han har skrivit brev till över 20 tillsynsmyndigheter för finansmarknaderna i olika länder för att varna för vad han betecknar som ”fenomenet”. Men det lever vidare.

Dominon of Melchizedek

Vad är då Melchizedek, eller Dominion of Melchizedek (DOM) som är det ”officiella namnet”? Jo, enligt John Shockey är det en påhittat land, skapat av far och son, David och Mark, Pectley, båda flera gånger dömda för andra brott.

”De två dök upp för första gången tidigt 1980-tal när jag deltog i FBIs utredning om ett finansiellt bedrägeri. Resultatet av det blev åtal och rättegång 1983 där sonen Mark Pectley dömdes. Samtidigt satt fadern fängslad i Mexiko för bedrägerier där mexikanska pesos skulle växlas till dollar via en offshorebank, en form av pengatvätt. När sonen Mark suttit av sitt straff dömdes han för nya bedrägerier 1986. Strax därefter rapporterades att fadern dött i det mexikanska fängelset och hans kropp sägs ha skickats tillbaka till USA. Men det finns ingen bekräftelse på dödsfallet och jag, tillsammans med många andra, tror att han fortfarande lever och verkar i USA och är arkitekten bakom DOM”.

Melchizedek är för övrigt det bibliska namnet på den högsta posten i mormonkyrkan.

DOM sades först vara beläget på den obebodda ön Malpelo, som

tillhör Columbia. Malpelo ligger under vatten under halva året. När det blev för mycket publicitet om den adressen ”flyttade” DOM till Antarktis och en rad ändringar senare är nu den senast kända hemvisten en obebodd atoll som tillhör Marshallöarna.

John Shockeys första kontakt med Melchizedek var i juni 1990, några månader efter det att Mark Pectley åter frigivits efter domen 1986. Det var då förfrågningar om banknamn, som Banco de Asia, Guardian Savings & Guarantee and Express Bank, med flera. Det visade sig att dessa banker hade licenser för att bedriva bankverksamhet från DOM. Ytterligare undersökningar visade att de var undertecknade av (under namnet Consortium Finance Corporation) John Hayden eller Branch Vinedresser. Strax därpå tog FBI in Branch Vinedresser för förhör och då avslöjades att det i själva verket var Mark Pectely, som därmed bröt mot villkoren för sin frigivning.

Hjälp med trovärdigheten

Ett eget land kan användas för en rad olika bedrägerier. Som hjälp används då påhittade myndigheter och liknande som ger trovärdighet. Till exempel skapade Melchizedek ”International Auditors”, en fejkad revisionsfirma som försåg andra DOM-bolag (som banker) med förtroendeingivande intyg.

Trovärdigheten ökade också när Melchizedek lyckades få plats i gula sidorna i Washington DC:s telefonkatalog under rubriken ”ambassader”.

Vad kan då ett falskt land och dess verksamheter göra?

Bankerna kan ta emot insättningar (som aldrig kan tas ut), de kan skriva ut och ta betalt för värdelösa garantier eller lånelöften, värdera och intyga andra DOM-verksamheter – till exempel garantera skuldsedlar för hundratals miljoner dollar. Detta har DOM lyckats utnyttja på olika sätt.

Själva landet ger också goda affärsmöjligheter, som att utfärda falska medborgarskap, ambassadörstitlar, ambassader, diplomatpass, licenser för att driva olika typer av verksamhet, en värdepappersbörs och så vidare. Det är upphovsmännens fantasi som sätter gränserna. Gemensamt för allt som ”uppfinns” är att det går att ta ut olika former av avgifter.

Kosmiska presidenten Pearlasia

De adresser som DOM använder sig av, inklusive ambassaden i Washington som fortfarande ”finns”, är postboxar, och såväl post som telefon skickas vidare till Pectley som enligt John Shockey är i Kalifornien i USA. Men Mark Pectley kallar sig numera TzemachBen David Netzer Korem, står gärna till tjänst med information om DOM. Det kan också hans ”kosmiska hustru”, en kvinna från Filippinerna som nu heter Pearlasia som också råkar vara president i DOM. På DOMs hemsida (givetvis har de tagit steget in i internetåldern) finns mycket uppgifter om DOM som ett suveränt och självständigt land med världsomspännande kontakter med andra länder. ”Trots förklädnaden av religiösa kopplingar som ska få allt att se respektabelt ut är det lätt att med kritisk granskning tränga genom den fasaden”, säger John Shockey.

Vid flera tillfällen har DOM lyckats förbättra sin trovärdighet. En del av de finansiella aktiviteter som man sagt sig bedriva, har rapporterats av den ansedda nyhetsbyrån Bloomberg. Dit hör till exempel kursnoteringar på olika räntebärande värdepapper. Bloomberg har också listat valutakursen för DOMs valuta Equi.

En rad afrikanska stater, som Nigeria, har svarat på korrespondens på ett sätt som tyder på att DOM är ett erkänt land. Ett antal stater i USA har registrerat olika Melchizedek-företag som godkända verksamheter.

Under de senaste åren har Melchizedek hittat offer runt hela världen, enligt John Shockey. Under 1998 lyckades man lura filippinska medborgare på över en miljon dollar. När den politiska och finansiella oron var stor i Filippinerna sålde DOM falska medborgarskap och pass. Dessutom med falska utfästelser om välbetalda jobb.

Till de mer märkliga inslagen i Melchizedeks verksamhet hör breven om vädjan om fred som skickats till Sadam Hussein i Irak och till Kosovo. Detta har dock inte hindrat DOM att förklara Frankrike krig efter landets kärnsprängningsprov.

Exemplet Melchizedek visar på några av de problem som måste lösas för att internationella bedragare ska kunna stoppas:

1. Vem ska övervaka och reglera vad som händer på Internet?
2. Är det ett gemensamt ansvar för regeringar över hela världen?
3. Skulle en sådan strikt kontroll hjälpa för att få bukt med den här typen av brottslingar?

”I många länder där DOMs bedrägerier skördat offer har myndigheterna undrat varför inte USA har ingripit mot ”landet” eftersom det både grundats och styrs därifrån. Jag slutar med den obesvarade frågan”, sa John Shockey.

7. Gus Mackenzie:

Dyra och tomma löften

Gus Mackenzie, chef för Forensic Accounting på revisions- och konsultjätten KPMG, tidigare polis i över 30 år, varav många med bedrägeriutredningar. Han talade om tecken på ”Advance Fee Fraud”.

Advance Fee definieras som: ett oärligt eller förledande (deliberate) löfte av en bedragare att mot en avgift (som erläggs i förtid) antingen betala ut ett fördelaktigt lån eller förmedla kontakt med en tänkbar långivare, med vetskapen att det varken finns medel att låna eller att det aldrig kommer att bli något lån.

Gammalt beprövat bedrägeri

Detta är ett gammalt och känt brott, men finns i så många varianter att Gus Mackenzie talade om det under rubriken ”gamla brott, nya skepnader – kameleontbedrägeriet”. Han har erfarenhet av olika varianter sedan i mitten av 1970-talet när han för första gången jobbade på Scotland Yards bedrägerienhet.

Skälet till att det finns en efterfrågan på sådana här tjänster är att banker och andra konventionella långivare, enligt Mackenzie, inte är tillräckligt benägna att finansiera projekt under utveckling. ”De flesta projekt som jag arbetat med har gällt fastighets- eller markutveckling, oavsett om det gällt att bygga helikoptrar, köpa marinor, anlägga golfbanor eller något annat”.

Eftersom bankerna inte ställer upp måste de som ändå vill finansiera sina projekt vända sig till förmedlarna på bakgatorna, några andra alternativ har de inte.

Bedragarna annonserar

Och låneförmedlarna är inte svåra att hitta. De annonserar i tidningar som International Herald Tribune, The Sunday Times ekonomidel med mera. De kan också nås via personliga introduktioner, fastighetsmäklare eller revisorer. Och numera också via Internet.

Bedragarna arbetar sällan från kontor, utan har i regel mobiltelefo-

ner, tillgång till kontor med fax och kopieringsapparat och ibland verkar de helt enkelt från sin bostad. Telefon, fax med mera sköts via svarsservice, som telefonsvarare. Ibland kan de nås via ett telefonnummer som går utomlands, men då ofta är vidarekopplat till det land där de befinner sig.

Bedragarna träffar sina klienter/låntagare/offer på i hotellfoajeer, eller i konferensrum. De förklarar att lånen kommer via en bank i något offshoreland (länder eller domäner som av skatte- eller andra skäl ofta är hemvist för svarta pengar) som i Fjärran Östern. Saudiarabien, Jungfruöarna eller Karibien. Skälet till detta uppges vara att undvika eller minimera beskattning för långivaren. Ofta har låntagaren sympati för detta argument ”Ingen gillar att betala skatt”.

Offret får sedan veta att den här vägen har fungerat för andra, vid många tillfällen, och att avgiftspengarna behövs i förskott för att täcka legala kostnader och själva låneupplägget. Ett annat argument för att låntagaren ska skicka över pengar är att denne måste visa att han verkligen är seriös och inte slösar med låneförmedlarens tid.

Som en del i låneprocessen får låntagaren skriva på ett avtal, som bland annat innebär att förskottsavgiften går förlorad (för låntagaren) om inte hela transaktionen genomförs (inom en kort tid).

Innan den förhoppningsfulla låntagaren skickar iväg sina pengar har mäklaren vanligen kunna meddela den glada nyheten att långivaren sagt ja. Och inte bara det, långivaren kan dessutom få låna dubbelt så mycket till sitt lysande projekt.

Se upp med banknamnen

Långivaren presenteras som en av de 50 eller 100 prime-bankerna i världen. ”Om någon använder den beteckningen finns det skäl att dra öronen åt sig, i hela världen finns inte mer än en handfull banker som heter något med prime. Ordet är däremot vanligt i bedrägeritransaktioner”.

Och när den noggranne eller misstänksamme låntagaren inte hittar den bank som sägs förmedla lånet i Bankers Almanac (som listar alla världens banker) så blir svaret att den bank som angivits som långivare bara är en av många i ett syndikat som ska förmedla lånet.

Avgiften som krävs för att få igenom lånet kan vara allt mellan motsvarande ett tusen och fem miljoner svenska kronor. Vanligen får låntagaren skulden för att något i det avtal som tecknats inte uppfyllts och lånet därför inte kan bli av.

Andra varianter på förskottsbedrägerier:

Köp av räntebärande papper (till exempel vad som kallas prime bank instruments), den förhoppningsfulla placeraren skickar över pengar, som aldrig investeras utan försvinner in på bedragarnas konton.

Nigeriabrev

Nigeriabrev (kopia på sådant bifogas – lägg märke till undertecknarens namn, George Lucas) är en massindustri, som i korthet går ut på att nigerianska tjänstemän behöver ett konto för att föra stora summor pengar till. ”Du är utvald” och behöver bara skicka en mindre summa för att få transaktionen genomförd samt kontonummer. En variant är att bedragarna behöver ett respektabelt företags- eller kanske personnamn för att kunna genomföra transaktionen (plus förskottspengarna förstås).

Den nigerianska centralbanken och regeringen har under flera år varnat för att de här breven, till exempel i tidningsannonser så sent som i år. Men breven fortsätter komma år efter år. Den brittiska polisen drog under enbart 1998 in 572 000 Nigeriabrev, som alltså aldrig kom fram till mottagaren. Därtill kommer 300-400 per vecka som når sina adressater. Även frankeringen på kuverten med breven är falsk.

I USA lade postverket under samma år beslag på 2,5 miljoner brev. Den genomsnittliga förlusten för den som låter sig luras är, så vitt känt, 200 000 dollar, alltså drygt 1,5 miljoner kronor. ”Märkligt nog svarar hela 10 procent av de som får breven och 0,01 procent (en av 10 000) förlorar pengar. Att lägga beslag på breven innan de distribuerats är ett bra sätt att förebygga bedrägerier, säger Gus Mackenzie. ”De flesta offer är från USA och Kanada. Efter OS i Atlanta fanns inte en telefonkatalogdel med gula sidorna på många miles radie. Att få med sådana uppslagsverk över tänkbara offer var viktigare än att få med kläderna.”

Bedragarna har emellanåt dålig kontroll på vem de skickar sina brev till. Sir Paul Condon, chefen för Metropolitan Police fick ett direkt till Scotland Yard.

Ny teknik stor besparing, för bedragarna

När det gäller Nigeriabrev, eller den typen av bedrägerier, öppnar Internet nya möjligheter. På sikt kan kanske bedragarna spara mycket på

att inte behöva skicka ut alla dessa brev – som nu alltså stoppas av polis och post. Istället blir det e-post som får förmedla erbjudandena.

De senaste versionerna av förskottsbedrägerierna finns i cyberspace och på Internet. ”Nu tvingas inte längre de stackars bedragarna slava vid telefoner, de behöver inte skicka drösvis av brev för att fånga in tänkbara offer. Allt de behöver göra är att sätta upp en hemsida, utan stora overheadkostnader och genast få access till miljoner människor och tänkbara offer.”

Deras jobb förenklas av att många människor använder sig av Internet för att hitta sätt att tjäna snabba pengar. Med anonymiteten på Internet blir det lätt för bedragarna att försvinna lika snabbt som de dök upp och istället starta på nytt på med någon annan hemsida.

Elektroniska hot och försvar

8. Steve Carter:

Kunskapens makt

Steve Carter är anställd hos Bank of America där han bland annat är ansvarig för säkerhetsavdelningens teknologiteam. Han har 15 års erfarenhet av banksäkerhet och var dessförinnan polis. Han håller ofta föredrag om teknologi och säkerhet, och var en av fyra talare under samlingspunkten ”Försvaret mot det elektroniska hotet”. Sammantaget handlade talen mer om själva hoten än om försvaren, som avhandlades i mer allmänna ordalag.

”Financial Times hade i går en artikel om hur datakryptering forceras och en text om hur skivbolaget EMI är på väg att skicka ut musik via Internet, genom att göra det möjligt att ladda ned digitala inspelningar. Och så rullar det på, vi kan inte öppna en tidning, slå på tv´n eller lyssna på radion utan att det handlar om Internet, hur tekniken tagit världsscenen i besittning.”

För världens finansindustri, med de risker för bedrägerier som finns, gäller det enligt Steve Carter att se till att ligga före bedragarna, men frågan är då hur sådan kunskap byggs upp, leds och försvaras? Allt detta kan samlas under namnet ”knowledge management”, fritt översatt kunskapsstyrning (i betydelsen att styra kunskap).

Spionaget växer

En del av denna kunskap är att veta så mycket som möjligt om konkurrenterna. Sådan kunskap kan antingen hämtas ur öppna källor (konkurrentanalys med ett bättre ord) eller fås ur ekonomiskt spionage. Det ekonomiska spionaget, bruket av olagliga eller oetiska vägar att få fram information, ökar. Företag och organisationer måste bli bättre på att bevara affärshemligheter. De hemligheter som är viktigast att bevara i finansbranschen är uppgifter man har om kunder. Dessa får inte blir kända utanför till exempel banken. Ekonomiskt spionage riktas oftast mot strategiska teknologier, företag som utvecklar avancerade informationssystem, rymdteknologi, sensorer, lasrar och elektronik.

Steve Carter använde som exempel Four Pillars Enterprise, ett taiwanesiskt bolag där två personer i ledningen dömdes i april i år för

ekonomiskt spionage i USA. Bolaget hade betalt uppskattningsvis 150 000 dollar (drygt en miljon kronor) till en anställd vid en amerikansk konkurrent, Avery Dennison, i utbyte mot hemlig information. På klassiskt agentmanér fick de information på använda post-it-lappar, på namnbrickor och på blöjtejp (!) För Avery Dennison betydde informationen till taiwaneserna 200 miljoner dollar i minskade intäkter. För varje satsad dollar fick alltså Four Pillar 1 000 dollar tillbaka.

Amerikanska uppskattningar av hur mycket som industrispionaget kostar hamnar som regel i intervallet 50-100 miljarder dollar, eller som uppemot börsvärdet på två Ericsson för att försöka översätta till en ”svensk valuta”.

Spionaget sker på många sätt, från länders underrättelsetjänster, via korrupta medarbetare hos konkurrenterna, genom underleverantörer, överköp av nyckelpersoner, eller tekniskt spionage som övervakningskameror, telefonavlysning, dataintrång och så vidare. Det senaste tillskottet är intrång i databaser.

Tillåten informationssökning växande bransch

Men det går att hitta mycket information även i legala databaser. Uppskattningsvis finns det över 4 000 databaser runt världen som går att använda för att bygga upp kunskap om konkurrenter. Därtill kommer Internet, en närmast oöverskådlig källa. Hemsidor, chat med anställda, eller diskussionsgrupper är några informationskällor. Andra legala vägar är experter från den aktuella industrin, eller från den akademiska världen, flygfoton av fabriker, kontor och parkeringsplatser. Psykologiska profiler av ledningen för ett bolag kan visa sig användbara vid förhandlingar om ett uppköp eller joint venture.

I EU finns nu en intressant lagstiftning som ännu, enligt Steve Carter, testats i verkligheten. Det gäller kundinformation där det från oktober i fjol är förbjudet för medlemsstater att överföra data från EU till länder som inte har samma skydd som EU-länder har. Samtal pågår mellan USA och EU, men frågan berör många fler länder än så.

Vad är då en affärshemlighet? Ja, enligt Steve Carter krävs det att tre saker är uppfyllda. För det första ska informationen ha ett kommersiellt värde. För det andra ska den inte vara offentlig och för det tredje ska ägaren ha vidtagit i alla fall några mått och steg för att hålla den hemlig.

Att bevara en hemlighet

Hur hålls då informationen hemlig? En viktig sak är att kulturen i organisationen eller företaget innefattar att hålla saker hemliga. Därutöver krävs dock en analys av vad som är verkligt kritisk information, så att man vet vad som måste skyddas extra väl.

Ett enkelt steg i skyddet är att kryptera meddelanden, vilket också andra talare påpekade. Detsamma gäller persondatorer, ett program för hundra dollar gör visserligen inte datorn helt säker, men betydligt säkrare än förut.

Anlita experter. Det kan inte vara för dyrt, utan tvärtom är det för dyrt att låta bli.

Ta reda på vad som går att få fram via offentliga källor om det egna företaget/organisationen. Vad kan konkurrenter och medier veta? Rapportera stölder och märkligheter till polisen.

Och på nationsnivå, hur kan regeringar hjälpa till att bevara affärshemligheter? ”Jag uppmanar er att trycka på för mer kraftfulla lagar”, sa Steve Carter.

9. John Austin:

Databedrägerier

John Austin, en av många före detta poliser som numera är konsulter i säkerhetsfrågor. John Austin är specialiserad på databrott, började arbeta med området 1976, och är chef för firman Computer Crime Consultants.

Efter att ha utrett sitt första databrott för snart 25 år sedan trodde han och polisen att sådana brott framförallt skulle syfta till att komma över pengar direkt. (Det första fallet var en brittisk bank där pengar olovligt fördes över till Argentina. Det var en biträdande bankchef som var skyldig, han erkände så snart polisen var honom på spåren, kanske gick det enklare eftersom förövaren var med i Frälsningsarmén, funderade John Austin).

Men det var och är inte pengar som är det direkta målet (om än målet längre fram i kedjan). Istället är det information som är väsentlig. ”Försäljningen och handeln med information får narkotikahandeln, mätt i pengar, att verka futtig”, hävdar Austin.

Hackerfaran en myt

Men det är en myt att tro att det stora hotet mot datasäkerheten är 16-åriga hackers som tar sig in i Pentagon och länders säkerhetstjänster, även om medier älskar den bilden. Det händer visserligen att det är rena hackers som ertappas, men i så fall är dessa ofta använda av andra, som betalar dem för att få fram information. ”De professionella, som du aldrig ser, är de som betalar och organiserar”. De som är farliga är professionella hackers.

John Austin tog ett exempel på informationshandel som berör Skandinavien. Där upptäckte en mobiltelefontillverkare (det var Nokia, jag frågade John Austin efteråt) att någon tagit sig in i de interna systemen och laddat ned hela databasen för forskning och utveckling.

Det här var ett allvarligt slag (speciellt som Nokia för några år sedan var ett finansiellt mycket utsatt företag, vilket vi inte tänker på idag, rapportskrivarens anmärkning). Informationen som stulits innehöll bland annat nya typer av SIM-chips (som styr mobiltelefonerna)

och ny teknologi, som soldrift. Informationen bjöds sedan ut till försäljning och såldes för 300 miljoner dollar, knappt 2,5 miljarder kronor. (Med facit i hand hade köparen gjort ett enormt klipp, om förövarna inte avslöjats).

Men både förövaren, som fanns i USA även om det lagts ut spår mot Storbritannien och kanalöarna, och köparen kunde avslöjas. John Austin berättade efteråt att Nokia också anställt den finska polis som höll i utredningen i hemlandet vid sin egen säkerhetsavdelning.

Men hackers, professionella eller inte, är inte ensamma om att försöka komma över information. Här finns ”intelligence agencies”, som ur öppna och andra källor samlar information åt uppdragsgivare som betalar för det.

Databrott tillväxtområde för maffiaorganisationer

Organiserad brottslighet har identifierat databrott som en tillväxtbransch. Den organiserade brottsligheten jagar framförallt där det finns pengar ”Om du tillhör en organisation som inte har eller tjänar så mycket pengar är risken liten, men om du har eller tjänar mycket pengar, eller kan antas ha det, så är du ett mål”.

Detektivbyråer, kom ihåg att de alltid jobbar för den som betalar, så även om du anlitar dem nu så kan du själv bli deras nästa mål.

Medier och frilansare, de köper in information (John Austin talade utifrån ett brittiskt perspektiv, rapportskrivarens anmärkning). Framförallt tabloidtidningarna betalar stora pengar för bra historier.

Så finns det extremistorganisationer. För att finansiera sin verksamhet kan de till exempel sälja verktyg för att ta sig in i datasystem (kanske med ”konsult i datasäkerhet” som täckmantel). John Austin nämnde också två organisationer, Loft med 360 medlemmar och Root med minst 140 runt världen, som tar sig in i system för att ta över systemen (Med deras egen terminologi äga systemen).

Men många hot mot information och system kommer också från den egna organisationen. Det kan vara anställda som har större behörighet än de ska ha, och alltså inte har några svårigheter att utnyttja systemen.

Ett vanligt sätt att komma åt information är att använda identiteten för någon som nyss slutat, men där behörigheter ändå kan leva kvar.

Se upp med tredjepartsanslutningar. Det vanligaste sättet att ta sig in i till exempel en banks system är inte att ta sig in i bankens egna

system direkt utan att gå via någon som i sin tur är ansluten till banken.

Testa den egna säkerheten

John Austin gav samma råd som många andra för att öka säkerheten:

Väl fungerande brandvägg – och se till att den är korrekt ”monterad”.

Behörighetskontroller – som förstås också måste vara korrekt installerade.

Kryptering för transaktioner – men den smarta bedragaren ger sig inte på den krypterade transaktionen direkt, han eller hon söker informationen där den utgick ifrån. Där är den i regel inte krypterad.

Det rätta sättet att skydda sig från attacker är att se till att den egna säkerheten verkligen fungerar. Testa och testa igen. Det är visserligen svårt att testa över Internet, men inte omöjligt.

Och även om det är en webdesignfirma eller internetkonsult som byggt din hemsida så är det ändå du som är ansvarig. Allmänheten struntar i vem som gjort och sköter sidan, vad den anbelangar så är det din.

Se till att följa upp dataintrång, var skedde intrånget, vilken väg gick man och så vidare. För att veta vad som kan vänta är det till god hjälp att följa med vad som händer inom till exempel nätverksteknologin. Vi måste veta vad andra kan göra, kanske mot oss.

10. David Chaikin:

Att ta sig in i en banks system

Doktor David Chaikin, chef för Cyberbrief Associates och expert på lagar inom affärsjuridik, skatter och finansiella undersökningar. Tidigare chefsåklagare i Australien. Chaikin talade om hur lätt eller svårt det är att ta sig in i en affärsbanks kontosystem. Utgångspunkten var en artikel i maj i år i tidskriften Newsweek där det hävdades att den amerikanske presidenten Bill Clinton och USA skrivit under ett hemligt direktiv (där det är märkligt hur ofta sådana hemligheter så ofta når pressen i USA, konstaterade David Chaikin) som ska tillåta CIA att föra ett cyberkrig mot den jugoslaviske presidenten Slobodan Milosevic. Målet är att hackers ska ta sig in på den jugoslaviske presidendentens bankkonton.

Kontoinformation mest skyddat

Och, om dessa konton skulle finnas i en schweizisk bank, hur ska då detta gå till? Frågan ställs inte för att Schweiz ska pekas ut, utan istället för att landets banker legat i frontlinjen vad gäller säkerhet och sekretess, även vad gäller elektronik och teknik. Det mest skyddade i alplandets banker är också uppgifter om privata bankkonton.

För det första kan till exempel USA inte gå via schweiziska bankers kontor i USA. Tjänstemännen där kommer inte åt informationen om kontona i Schweiz, varken elektroniskt, på papper eller muntligt. Det säkraste, ur schweizarnas (och deras kunders) perspektiv är om de två ländernas datasystem helt enkelt är skilda åt, även om det rör sig om samma bank. Vidare är det vanligt att behörigheterna är mycket begränsade, där en anställd bara kan ta fram uppgifter om en kund i sin region, där det krävs särskild behörighet för att kunna ta fram uppgifter på privata konton etcetera.

Den schweiziska specialiteten med nummerkonton är också till god hjälp för att bibehålla sekretessen. Här är det bara enstaka personer i banken som känner till kundens namn – vanligen bara den kontoansvarige eller placeringsrådgivaren. För resten av organisationen är kunden bara ett nummer.

Tre säkerhetsnivåer

Normalt finns det tre säkerhetsnivåer i en schweizisk bank. För att komma in på ett lokalt nätverk krävs användaridentitet och lösenord. För att ta sig vidare till uppgifter om privatkonton krävs ännu ett id och ett nytt lösenord. En förteckning över vilka kontor och/eller personer som får arbeta med dessa konton ska finnas hos de kontoansvariga. Det är heller inte på alla datorer i banken som det går att gå in på kontosystemen. Därigenom minskas risken för att obehöriga, inte minst bland bankanställda, försöker ta sig in i systemen,

För det tredje har inte ens den som har rätt att gå in i nätverket med uppgifter om privatkonton möjlighet att se all information där utan ytterligare en kod, till exempel en behörighet för placeringsrådgivare.

Insiders har bäst chans

Sammanlagt är risken för att hackers ska ta sig in mycket liten. Hoten kan istället komma inifrån, från säkerhetsfolk, systemavdelningspersonal eller andra behöriga personer som faktiskt har access.

För att minska den risken krävs att allt som händer med och kring konton och system registreras och loggas. Med dessa uppgifter går det sedan att kartlägga precis vem som gjort vad och när i olika system.

Så att komma åt Milosevics bankuppgifter i Schweiz, om han nu har några konton där, är inte enkelt. Den som har bäst förutsättningar att lyckas är en intern hacker, eller en anställd som bryter bankens regler. Men den anställde måste känna till hur systemet är byggt, hur säkerheten ser ut, han måste komma över rätt access, eller stjäla någon behörigs identitet. Och han måste kunna gömma spåren efter vad han gjort.

För om uppdragsgivaren går att spåra (i det här fallet USA) är det inte alls säkert att den information som kan ha plockats fram går att använda i en rättegång (eftersom uppgifterna togs fram med olagliga metoder). Detta är några av de punkter som de amerikanska myndigheterna måste ha klart för sig, innan det är dags för cyberkriget.

De schweiziska bankerna har också legat långt fram när det gäller säkerheten i att göra banktjänster via telefon eller Internet. De två största bankerna utvecklar säkerheten för telefonbanking via ett bolag som heter Securenet, ägt av bankerna och Swiss in line. Tre saker krävs för att göra bankaffärer på nätet, för det första ett avtal mellan banken

och kunden – som ger ett behörighetsnummer, för det andra ett lösenord och för det tredje en lista med slumpmässiga nummer, som stryks när de använts. Hur säkra transaktionerna blir beror på kunden. Om denne låter någon annan använda datorn och listan med nummer så ökar naturligtvis riskerna. Utveckling av andra sätt att identifiera kunden pågår, till exempel via röstigenkänning.

Internetaffärerna krypteras också via Securenet. Deras mjukvara för kryptering kan laddas ned från nätet till den egna datorn. Krypteringen är 128 bits.

Vad minskar sekretess och säkerhet?

Elektronisk kommunikation är till naturen mer känslig för störningar än tal öga mot öga (som var det som gällde under tusentals år), skrivna meddelanden (gällde under några hundra år) och telefon (under de senaste hundra åren). Men, det ska sägas, även de ”gamla” kommunikationssätten är både avlyssnings- och störningsbara. Kraven på snabbare och mobilare kommunikationer ökar känsligheten för störningar. Affärsmän som använder sina mobiltelefoner och datorer utanför det egna kontoret löper större risk både för avlyssning och dataintrång. Och intrången är ofta svåra att upptäcka, vilket också minskar säkerheten.

Vad ökar säkerhet och sekretess?

Vetskapen om det växande behovet av säkerhet och sekretess driver i sig den utvecklingen framåt. Den ökade användningen av kryptering är ett sätt att möta riskerna. Det står så mycket pengar på spel både i världshandel och till exempel handel på Internet att det eldar på säkerhetsutvecklingen.

Kryptering är omdiskuterad, inte minst försöken att stoppa alltför avancerade lösningar eftersom dessa skulle vara alltför tids- och kraftkrävande för myndigheter att knäcka, till gagn för brottslingar av olika slag. Men kryptering har kommit för att stanna, oavsett vad myndigheter i världen tycker. PGP, pretty good privacy, har blivit en världsstandard som kan tas hem via Internet. Och kryptering som tidigare var närmast en svårgripbar konstform är nu en del vanligt datoranvändande. Kryptering kan petas in som ett startprogram i datorn, billigt och lättöverkomligt.

11. Jouke van der Zee:

Det växande hotet från IT

Jouke van der Zee, utvecklingschef hos Syfact International, som tar fram IT-mjukvaror för säkerhet och skydd. Holländaren har arbetat i femton år med hur IT kan användas för att bekämpa finansiell brottslighet.

När jag började i mitten av 1980-talet var hoten från IT bara en bråkdel av vad de är idag, ja det fanns egentligen inga hot, började holländaren. Idag finns det en uppsjö av hot från IT, inte minst till finansiella institutioner som vi hört ett antal talare ge exempel på.

Och på 1980-talet fanns därför knappast några försvar, men gå in i dag på Internet och sök på ”Financial crime” och ”software” så kommer ett otal produkter att listas. Det här är två vägar som jag tror utvecklingen kommer att ta de närmaste åren:

För det första kommer trycket på datasäkerhetsavdelningar i företag och organisationer att öka kraftigt.

För det andra; utvecklingen av system och arbetsmetoder för att avslöja misstänkta transaktioner och pengatvätt.

Under 1970-talet behövde en banks säkerhetsavdelning bara oroa sig för att pengarna skulle försvinna från banken rent fysiskt. Det var först på 1990-talet som uppgiften att identifiera misstänkta transaktioner, till exempel för pengatvätt, tillkom. Men med företagsfusioner, en alltmer global kapitalmarknad, interna omorganisationer om och om igen ökar trycket på säkerhetsavdelningarna. Resultatet blir att de ska klara av mycket mer jobb än tidigare, utan att deras resurser ökat i samma utsträckning.

Rutinjobb automatiseras

Ett sätt att kunna få ut mer och bättre resultat från säkerhetsavdelningens jobb är att låta en del arbetsuppgifter ”automatiseras”, att dataprogram tar över en del uppgifter som tidigare gjorts manuellt. Sådan automatisk support kan delas in i två delar. För det första program för att upptäcka pengatvätt och misstänkta bedrägerier, och för det andra intelligenta ledningssystem.

De vanligaste programmen som ska avslöja konstiga eller misstänkta transaktioner jämför hur en kund brukar agera (som till exempel hur han brukar föra pengar mellan olika konton) med hur han agerar i ett specifikt fall. Om hans eller hennes beteende skiljer sig för mycket från det väntade så rapporterar, eller flaggar, programmet det. Det är ett enkelt system, men har några hakar.

Den främsta är att någon människa måste titta på och ta ställning till de flaggningar som systemet visar. Är det en misstänkt handling, eller bara en helt rimlig, fast ovanlig för den här kunden? För kanske är det bara den gamla damen som blivit änka och därför sålt sitt hus och satt in pengarna på banken.

I en stor bank blir det väldigt många flaggningar som någon måste ta ställning till. I en storbank kan det handla om över 20 miljoner transaktioner per dag. Även om det är en liten andel av transaktionsmängden som ger en flaggning så blir det ändå ett väldigt stort antal. Och det är bara i en bråkdel av flaggningarna som det verkligen är något kriminellt som ligger bakom. Resultatet av mängden flaggningar är, paradoxalt nog, att det krävs mer mankraft, som kan kontrollera, trots att man använder informationsteknologi för att underlätta arbetet. Att bara lagra flaggningar på hög är ingen bra lösning. En dag knackar polisen på dörren för att ställa frågor om en kund, som du inte har hunnit att undersöka, trots flaggningar.

Mänsklig intuition överlägsen

Naturligtvis kommer också proffsen bland de kriminella att lära sig hur systemen fungerar och vad som kan passera utan att leda till en flaggning. Och om man bara litar på tekniken så missar man en viktig informationskälla; mänsklig intuition och erfarenheten hos till exempel kassapersonal i banken.

Detta visar ett exempel från Holland. Där rapporteras misstänkta aktiviteter, eller transaktioner, antingen utifrån ett objektivt kriterie, som att transaktionen är över ett visst belopp och innehåller mer än en valuta, eller från ett subjektivt, där personen bakom disken till exempel tycker att kunden uppträder märkligt. Av de rapporterade transaktionerna har under flera år 55 procent ”tagits ut” av objektiva kriterier och 45 procent av subjektiva. När polisen sedan undersökt vad som rapporterats så har det visat sig att knappt en femtedel av de rörelser som plockats ut objektivt men över fyra femtedelar av de subjektiva

klassades som misstänkta. Det ”biologiska intelligenssystemet” var alltså åtskilligt bättre på att hitta märkliga saker.

Sättet att lösa detta på är att först ha ett system eller program som plockar ut misstänkta transaktioner, därefter går dessa till ett nytt program som ska skilja falska och riktiga flaggningar åt. De som plockas ut även här får en människa bedöma.

Säkerhetsavdelningen ska vara omtyckt

Det är också viktigt att relationerna mellan de personer som möter kunden och säkerhetsavdelningen är de bästa. Det gäller att komma bort från den tidigare synen att säkerhetsavdelningen var organisationens polis eller vaktstyrka. Och var försiktig med att centralisera, att känna kunden är viktigt och det gör framförallt den eller de som träffar kunden. Centralisering och bank via telefon eller dator, där kunden gör alltmer av transaktionerna själv, kan bli ett hot mot banken, så lita inte bara på tekniska kontrollsystem.

Vårda kunskapen i system och organisation och se till att skydda den. Stora kostnader läggs på att samla in och analysera data om kunder och kanske anställda. Den här informationen är viktig del av strukturkapitalet i företaget/organisationen, så vårda den väl. Och se till att de kunskaper som finns, inte minst på säkerhetsavdelningarna, inte bara finns i huvudet på personer. I så fall går kunskapen ut genom dörren när den anställde gör det. Och folk slutar oftare än tidigare, inte sällan för att börja hos en konkurrent.

Det är viktigt att kartlägga och dokumentera var problem eller olyckor inträffar i en organisation samt vilka som berörts, hur mycket kostade problemet, kunde en del av förlusterna återvinnas och så vidare? Se till att alla ”fall” registreras på samma sätt, annars blir det omöjligt att hitta i materialet, se mönster och dra slutsatser.

Den som vill utnyttja ett system kommer alltid att angripa dess svagaste punkt. Om det är juridiken som är svagast så är det där en attack sätts in och om det är organisationen är akilleshälen så sker intrånget där. Informationsteknik kan aldrig ge ett vattentätt skydd mot kriminella attacker, men den som inte gör något, inte utbildar personalen, inte samlar information eller har en fungerande säkerhetsavdelning har goda förutsättningar att bli den svagaste punkten.

12. Peter Bentley:

Intelligentare system

Peter Bentley, doktor vid institutionen för datavetenskap vid University Collage i London (UCL), talade om hur intelligenta datasystem skulle kunna användas för att avslöja bedrägerier. Peter Bentley är ansvarig för utveckling av sådana system vid UCL.

Datorer och bedrägerier

Olyckligtvis är datorer extremt användbara för bedragarna, förmodligen har det aldrig någonsin tidigare varit så enkelt för en bedragare att komma undan med så mycket pengar som idag och lämna så lite bevis efter sig. Ofta är de enda tecken som finns fragment, eller fingeravtryck, av data som dessutom är utspridda över databaser runt världen. Problemet med att identifiera dessa databaser, vilka data som finns och hur de ser ut är något som vi datorforskare kan hjälpa till med. Så datorer är inte bara till nytta för förövarna utan även för oss som ska spåra dem.

De system som används på till exempel banker idag, som kan ha till uppgift att skydda transaktioner, förebygga dataintrång, avslöja vem som försöker tränga sig in i en databas etcetera, är dessvärre för gamla. En bank som Peter Bentley arbetar med använder till exempel en mjukvara som är över 20 år äldre än vad som testas på exempelvis UCLs laboratorier.

Rätt sätt är att använda intelligenta mjukvaror. Peter Bentley presenterade en rad varianter på sådana. Fördelen med intelligenta system är att de, till skillnad från vanliga program/system, kan hantera icke-linjära samband, de kan koppla ihop bitar av information från olika håll, de kan lära sig nya mönster i datamängder, eller anpassa sig till nya mönster. Vi kan tala om för systemet att ”så här ser en normal händelse i vårt affärssystem ut, säg till oss om något avvikande händer” – och så gör systemet det.

Här är några olika tekniker som används för intelligenta system:

Artificiellt ”neural” nätverk – modellerat på vår hjärna. Uppenbarli-

gen är en människa som är expert på ämnet bra på att identifiera bedrägerimönster i data. Den här mjukvaran kan, så snart den likt en mänsklig hjärna blivit lärd, identifiera och förutsäga saker i datamängderna. Ett sådant här system kan arbeta dag och natt, nöjer sig med enbart ström, och är minst lika träffsäkert som en mänsklig expert med många års erfarenhet. Nackdelarna då? Inga förklaringar till varför systemet lyfter ut något som misstänkt - det har visserligen oftast rätt men kan inte tala om varför.

Evolultions ”computation” – är Peter Bentleys område. Här plockas lösningar till olika problem in i datorn och populationer av lösningar byggs upp. De bättre lösningarna får egna ”barn”, ärver en del användbart från sina föräldrar och generationer byggs på med bättre och bättre lösningar.

”När vi talar om för datorn ”låt oss göra en lösning som är ett bra sätt att avslöja ett bedrägeri på” så får vi bättre och bättre metoder för det. Precis som för neuralnätverken så kan den här tekniken lära sig mönster i data, kan också leta datan, hitta samband i gigantiska databaser. Den stora nackdelen med tekniken är liksom för den förra att det inte blir några förklaringar till varför ett beteende lyfts fram som misstänkt.

Fuzzy logic (logik i det oklara) – till skillnad från de två tidigare teknikerna är fuzzy logic extremt bra att förklara saker. Det klarar av vaghet och osäkerhet, ”de flesta av oss uttrycker oss vagt även om vi inte vill erkänna det”. Vad betyder ”mycket misstänkt” eller ”ganska dyrt” eller ”han var lång”.

Fuzzy logic är gjort för att hantera glidande gränsdragningar och är mycket bra på att hantera det. Ett exempel är den här meningen, tagen ur luften: ”Om åldern är låg och han vill ha hög ersättning så kan det vara ett misstänkt fall av hemförsäkringsbedrägeri”.

Trots sitt namn är fuzzy logic mer konkret än traditionell logik. I Japan har tekniken blivit extremt populär och används för kontroller på en rad områden. I tunnelbanan ska den japanska tjänstemannen kunna somna stående utan att hålla i något utan att riskera att falla vid inbromsning, som sköts av logiksystemet. Nackdelen med tekniken är att något eller någon måste lära systemet regler för hur det ska agera, men tekniken är ändå mycket kraftfull.

Artificiellt immunsystem – Lika kraftfullt som neuralsystemet, men

baseras istället på hur immunsystemen fungerar, det vill säga ständigt på försvar mot inkräktare utifrån. Och i likhet med immunsystemet i kroppen så finns försvaret överallt, inte bara centralt i hjärnan eller på ett ställe i ett datasystem, istället har alla datorer i systemet en liten roll i att avslöja och försvara systemet. Så även om halva datasystemet slagits ut eller är ur drift av annat skäl så kommer resten att vara säkert. Men det finns förstås nackdelar och det är återigen att tekniken inte är bra på att förklara varför något är märkligt eller fel, precis som kroppens immunsystem.

Hybriditelligenssystem

Alla tekniker som nämnts har både för- och nackdelar. Det bästa resultatet nås genom att kombinera olika tekniker, för att kombinera styrkorna. Peter Bentley arbetar till exempel med en storbank i England för att utveckla ett system som ska avslöja bedrägerier med hemförsäkringar. I detta kombineras evolutionssystemering med fuzzy logic, det ska ge ett system som blir allt bättre på att spåra vad som ser märkligt ut och som dessutom kan förklarar varför. Dessutom inte som en svårbegriplig ekvation, utan som en begriplig mening.

Personligheten hos en bedragare

13. Raj Persaud:

Så tänker en finansiell psykopat

Konferensens mest underhållande inslag, tillsammans med beskrivningen av det påhittade landet Melchizedek, var Raj Persauds föredrag om kännetecken hos finansiella bedragare. Raj Persaud är doktor i psykiatri (Consultant Psychiatrist) vid Bethlem Royal and Maudsley Hospitals i London. Han har också hållit i ett antal tv-program, samt uttalar sig ofta för medierna, i liknande frågor. Efter att ha hört honom är det lätt att förstå varför.

Doktor Persaud talade om vilka psykologiska drag hos en individ som kan samvariera med finansiell brottslighet, eller i varje fall högre risk för brottslighet.

Slumpen avslöjar mest

Han började med att se på hur finansiella bedrägerier upptäcks. Enligt de uppgifter han refererade till upptäcks strax över hälften, 51 procent, av en ren slump. En femtedel, eller 19 procent, upptäcks vid revision medan interna kontrollsystem inte spårar mer än 10 procent, eller en tiondel.

Resterande femtedel, alltså lika mycket som revisorerna förmår hitta, står ”missnöjda eller förorättade älskare/älskarinnor” för, alltså personer som skvallrar om misshagligheter som de känner till för att hämnas på bedragaren.

Raj Persauds skämtsamma tolkning var att se till att alla nyckelpersoner i en organisation har en älskare/älskarinna och att därpå se till att denna blir förorättad.

Men det finns ett bra skäl till varför just en förorättad person är den som avslöjar bedrägeri, enligt Raj Persaud. Skälet är att revanschlustan/hämndbegäret eller vad det nu kallas ger motivation att avslöja. Och det är motivationen som är nyckeln till att hitta bedrägerierna.

Som exempel nämndes att de bedrägerier som avslöjas i genomsnitt pågått i tre och ett halvt år. Och när avslöjandet till sist kommer så beror det i regel på att bedragaren blivit alltför hagalen så att han eller hon till sist tar ut så mycket pengar så att det märks. Återigen är det

motivationen som avgör, först motivationen att hitta ett sätt att komma runt kontroller i systemet och sedan en alltför stor motivation att lura till sig så mycket som möjligt.

Den mest motiverade vinner

Varför fungerar då de kontroller som finns i organisationer och deras sätt att arbeta inte tillräckligt bra?

Jo, därför att kontrollerna i de flesta fall framförallt letar efter sätt att täppa till kryphål. Kryphålen hittas i regel inte förrän det är ”skurken” som hittat och utnyttjat dem. Snabba förändringar av teknik och teknologier ger också ständigt nya ställen att leta kryphål på. I många företag görs ständiga omorganisationer som också det ger förutsättningar för nya kryphål.

Och när den finansielle bedragaren, eller den finansielle psykopaten som Raj Persaud säger, är mer motiverad att hitta kryphål än vad resten av organisationen är för att täppa till dem så kommer internkontrollen sannolikt inte att fungera.

Med dagens snabba tekniska förändringar är det inte sällan så att yngre medarbetare vet mer om hur systemen fungerar än vad cheferna, trots många anställningsår, gör. Det här är något nytt och det ökar risken för att ledningen kan bli lurad.

Dessutom tror ledningar på att deras egna kontroller är bra för att upptäcka bedrägerier, vilket de alltså inte är. Och den som tror att han eller hon är bra på att se oärliga människor (och därmed litar på de som enligt den egna uppfattningen verkar ärliga) lurar lätt sig själv.

Den oärlige ser ärlig ut

Den som uppträder på ett visst sätt är, enligt vad vi tror, oärlig. Till sådant beteende hör att flacka med blicken, att inte behålla ögonkontakt, att gestikulera mycket och ge ett obekvämt intryck samt att prata fort. Men i själva verket visar psykologisk forskning att det i själva verket är hos personer med precis motsatt beteende som det finns skäl att vara vaksam för bedrägerier. Ett exempel är den duktiga lögnare som ljuger för dig och ser till att behålla ögonkontakten – för att se om du avslöjar dem eller inte samt för att de inte vill uppträda som en lögnare förväntas göra.

Och eftersom det kräver en god kognitiv förmåga att ljuga, så kom-

mer den professionelle lögnaren att tala sakta för att hinna tänka på vad de ska säga. Återigen – detta går stick i stäv med hur många tror att en lögnare ska uppträda, det vill säga tala snabbt.

Erfarenheten visar att de som har som jobb att upptäcka ohederlighet är dåliga på detta. Polis och tulltjänstemän är inte bättre än vem som helst, trots att både de och vi tror att det är en del av yrkeskunskapen. Den enda yrkeskår som är riktigt bra på att avslöja ohederlighet är Secret Service livvakter, som till exempel bevakar den amerikanske presidenten. Deras hemlighet: de litar inte på någon!

Ledningar hemmablinda

Ledningar har ofta för hög tilltro till den egna organisationen, och för liten tilltro till konkurrenternas. Det är därför de bedrägerier som avslöjas hos en konkurrent ”inte kan” ske i den egna verksamheten. Enligt amerikanska undersökningar av bankanställda så är en fjärdedel hederliga, oavsett vilka tillfällen till bedrägerier som gives. För hälften beror hederligheten på risken för upptäckt medan den sista fjärdedelen är mer bedrägerimotiverade och letar efter kryphål.

Men det finns några mönster hos många organisationer som drabbas av bedrägerier. Ett är att det varit oklart om vem det är som har uppdraget att övervaka den person som så småningom visar sig vara en bedragare. Chefen A tror att det är Bs jobb och tvärtom. Resultatet är att ingen bevakar.

Många tycker också att det är obehagligt och demoraliserade att kontrollera sin personal alltför mycket. Det främsta skälet till att cheferna plötsligt står där, lurade, är att de för det mesta letar på fel ställe, hos fel personer och inte hos de mest benägna – som ofta är de mest hyllade i organisationen.

Dessa high-flyers, golden boys, eller vad man nu vill kalla dem är de som ledningen ser allra minst som tänkbara bedragare, men det är de som har de drag i sin personlighet som också bedragare har. Det är dessa drag, som passar utmärkt i till exempel finansbranschen, som å ena sidan gör dem till ambitiösa, karriärinriktade påläggskalvar men å andra sidan kan vara grogrund för bedrägerier.

Ett exempel gäller Orange County (en del av Los Angelesområdet) i Kalifornien i USA, som försatte sig själva i en form av konkurs 1994 efter förluster på två miljarder dollar (cirka 16 miljarder kronor).

Den finanschef som erkände sig skyldig till en rad bedrägeripunk-

ter som ledde fram till storförlusten, Robert Citron, hade haft ansvaret för finanserna i över 20 år och var mycket uppskattad samt sågs som en finansiell guru. Han beskrevs som en man med kung Midas förmåga att skapa guld efter att ha tagit över ansvaret för en fond på sju miljarder dollar och fått värdet att stiga till 20 miljarder dollar på några få år, betydligt bättre avkastning än vad liknande fonder klarat av.

Vad som inte syntes var risken, att först belåna aktier och andra värdepapper stort för att därpå investera lånen i nya värdepapper och så vidare. När så räntan steg i början av 1990-talet så föll hela det finansiella korthuset.

Svårt gå emot den som är guru

Robert Citrons chef kommenterade efteråt ”Här var en person som försåg oss med miljontals dollar. Han fick oss alla att verka begåvade, men jag vet inte hur han gjorde det”. Det här är ett av huvudskälen till att finansiella bedragare, eller dito psykopater, är så svåra att avslöja; genom sina bedrägerier skapar de en situation där det inte finns några incitament för en person (som drar nytta av vad bedragaren gör eller i alla fall synes göra) att avslöja vad som sker. Precis så reagerade Robert Citrons chef.

För vem vill avslöja den stjärna som drar in mycket pengar till en firma, som kanske syns i mångas bonus? Raj Persaud nämnde inte den forna stjärnmäklaren på Barings Bank Nick Leeson, men det är ett exempel på samma sak.

Det är heller inte lätt att ifrågasätta en person som har gurustatus eller anses vara ett geni på vad hon eller han gör. Och det är inte lätt att inför andra säga ”Jag förstår inte hur han/hon gör. Det kan inte stå rätt till.” Ingen vill framstå som en idiot inför andra.

En finansiell psykopats personlighet

Så till personligheten, hur de drag som å ena sidan gör dem till stjärnor också har en mörkare sida. Ett första drag hos en finansiell psykopat är att det inte är en lat människa. Han/hon arbetar mycket hårt. Alla vill ha hårt arbetande arbetskraft i sina organisationer, men frågan är varför personen arbetar så hårt? Varför stannar han så länge på kvällen? Varför är hon alltid den sista att lämna kontoret?

Ett skäl till det hårda arbetstempot är att den här typen av människor lätt ledsnar. De behöver mycket stimulans, och sådan kan komma från att göra saker som inte ledningen upptäcker. De gillar att ta risker. De flesta av oss andra, som tycker att jobbet är stressigt som det är, vill inte lägga till risken för upptäckt som ytterligare stressfaktor. Detta är ett vanligt skäl till varför vi inte gör några bedrägerier.

Den finansielle psykopaten är ofta en kreativ person. Och återigen är det ett drag som ”alla” vill ha i sin organisation. Men den här kreativiteten kan också användas för att hitta det kryphål som du inte hittat själv.

Den finansielle psykopaten är ofta också charmig, och charm är till god hjälp i en organisation – både när det gäller att bli framgångsrik och när det gäller att föra folk bakom ljuset. Så det finns även här en ljus och en mörk sida av samma karaktärsdrag.

När Nick Leeson frågades ut av de brittiska bedrägerimyndigheterna om de förluster på 700 miljoner pund (närmare tio miljarder svenska kronor) som han förorsakade Barings Bank så ansågs han å ena sidan trevlig och charmig, men utan ånger för vad han gjort (”Tja, aktiekurser går upp och de går ned, jag är inte stolt över vad jag gjort, men det finns inget jag kan göra åt det nu”) Bristen på skuldkänslor är också en del i bedragarkaraktären.

Också detta kan vara bra för den som arbetar i finansbranschen. Då gräver du inte ned dig i dina misstag eller misslyckade affärer. Man vill inte ha folk som inte vågar agera av rädsla för att misslyckas. Återigen, en ljus och en mörk sida hos karaktärsdraget.

Stort självförtroende

Detsamma gäller impulsivitet, också det ett drag hos bedragare. De tar beslut, utan att ha tänkt över alla alternativ och utan att stämma av med andra. Men beslutskraft är en efterfrågad förmåga. Att ta snabba beslut, utan att kolla med andra, tyder också på god självkänsla – något som är efterfrågat i företag och organisationer – men den negativa sidan är att de har så mycket självförtroende att de blir arroganta. De tror att de kan gå på vatten och eftersom de är smartast i sin organisation så kan de inte bli avslöjade. Detta drag leder mot bedrägerivägen, tilltron till förmågan att hitta bedrägerivägar som inte avslöjas.

Men den som är så utvald, både i organisationens och sina egna ögon, anser ofta att han eller hon är berättigad till specialbehandling eller speciella belöningar.

Och han eller hon blir aldrig nöjd utan hittar alltid andra, som nått längre, att jämföra sig med. Den här tävlingsinstinkten, att hela tiden bli bättre (belönad) än andra är ännu en faktor som dels lockar i en organisation, dels har en mörk sida.

Ett amerikansk undersökning av medaljörerna i OS I Barcelona visade att bronsmedaljörerna ofta var mer nöjda än silvermedaljörerna. Skälet var att tvåorna jämförde sig med guldmedaljören – och alltså inte hade nått ända fram, medan treorna jämförde sig med alla de som inte fått någon medalj alls.

Testa dig själv – är du en potentiell bedragare ?

När föredraget började delade Raj Persaud ut ett formulär med tio påståenden, ett test av karaktärsdrag. Han betonade dock att detta inte var rätt förutsättningar eller sätt att göra testet. Dels vet alla vad konferensen handlar om och vad syftet med testet är, dels är ett sådant test bara en del av en större process, dels ska frågorna komma instuckna i ett mer omfattande batteri av frågor så att syftet är mer svårspårat. Och så ska en psykolog som kan tolka svaren riktigt vara med. Men frågorna mötte ändå stort intresse (och stor munterhet)

Här följer testet:

Varje påstående följs av svarsalternativen instämmer respektive instämmer inte. Tänk inte för mycket på varje fråga utan välj det alternativ som känns mest riktigt. Var så ärlig som möjligt. När alla frågorna är besvarade så summera antalet A respektive B.

1. Bra uppförande belönas i regel: Instämmer A, instämmer inte B
2. Det är bättre att imponera än att vara bra. Instämmer B, instämmer inte A.
3. Världen är i stort sett rättvis. Instämmer A, instämmer inte B
4. Charm väger tyngre än kompetens. Instämmer B, instämmer inte A
5. Jag är generös mot mina konkurrenter. Instämmer A, instämmer inte B
6. Jag tar för mig av alla fördelar jag kan få. Instämmer B, instämmer inte A
7. De flesta människor försöker att inte fuska. Instämmer A, instämmer inte B

8. Att erkänna en skuld ska belönas. Instämmer B, instämmer inte A
9. Att vinna är inte allt. Instämmer A, instämmer inte B.
10. Framgång handlar ganska litet om hårt arbete. Instämmer B, instämmer inte A.

Ju fler B-alternativ, desto mer benägenhet att vara eller bli en finansiell psykopat. Den som har fler än sju B har sannolikt redan gjort sig skyldig till något bedrägeri. Men, den goda sidan av saken, det betyder också (om du inte är upptäckt) att du är en av de mest uppskattade medarbetarna i din organisation. Framförallt hos dina chefer.

14. Jeremy Phipps:

Att undvika bedragare

Jeremy Phipps, chef för Pre-Employment Screening, Network International. Tidigare närmare fyra decennier i brittiska armén, bland annat med terroistbekämpning, gisslanräddning, krisledning och informationssökning. Han talade direkt efter Raj Persaud, om hur man kan undvika att anställda tänkbara bedragare i sin organisation.

Egna anställda de vanligaste bedragarna

”En undersökning från konsultjätten Ernst & Young 1998 visade de oroande resultaten att 84 procent av alla större bedrägerier begås av någon som är anställd i det bolag/den organisation som drabbas. Och 75 av de 100 största bolagen i undersökningen förklarade att de drabbats minst någon gång under de senaste fem åren. Och 87 procent förklarade att bedrägerierna inte minskar.”

Network International delar in bedragarna i fyra grupper, som stämmer väl med vad Raj Persaud talade om tidigare.

Bedragaren – den som använder lögner och lurar folk för att direkt eller för att hitta vägar för att komma över något för egen vinning.

Den missnöjde – anser att han/hon inte fått vad han/hon har rätt till, som bonus.

Den desperate – spelskulder, skilsmässa, sjukdom i familjen.

Risktagaren – som drivs av kicken att hitta kryphål, att lura systemet.

”I dessa fyra kategorier går alla bedragare in, enligt våra 25-års erfarenhet att förebygga bedrägerier. Och det här är skälen till varför de sker:

Vem kollar mellanchefen?

Det första skälet är bristande intern kontroll. Nedskärningar i stora bolag och organisationer ökar riskerna. En undersökning från univer-

sitetet i Nottingham visar att det är chefer på mellannivå som är den största riskgruppen att bli bedragare. De vet hur rutinerna fungerar och hur de kan kringgås, de har en hel del behörighet och vem kollar egentligen en mellanchef, med kanske många år i bolaget/organisationen?

Skäl två är dålig ersättning. Företag och organisationer är dåliga på att belöna dem som presterar något extra. För det tredje blir moralen i arbetsliv och affärsliv lägre, i alla fall här i England, hävdar Jeremy Phipps och hänvisar till en undersökning som säger att en av tre brittiska män har dömts för något brott, trafikbrott oräknade, innan de fyller 40 år. För det fjärde är gapet mellan toppen och botten, ”mellan de feta katterna och de som gör jobbet”, stort.

”Samhället blir alltmer materialistiskt, där egennyttan går före kollektivet. In en del branscher, som finans, finns det möjligheter att tjäna väldigt mycket pengar. Med höga löner kommer förändrad livsstil, drömmar blir verklighet, det blir en BMW istället för en Golf Gti, en våning istället för en liten lägenhet, semester i Karibien istället för Mallorca och så vidare.

Samtidigt har trycket ökat. Unga sätts under extremt tryck, de ska prestera alltmer, eller också är de ute, simma eller sjunk, de arbetar mycket och ska samtidigt få privatlivet att fungera. Detta skapar aggressivitet, och kanske raseri, eller utbrott.

Och jag tror att lojaliteten med arbetsgivaren kommer i kläm i den här kulturen. Tidigare fanns tid att tala med och bry sig om personalen. Med ständiga trimningar har mellannivåer försvunnit – och med dessa ofta personerna som hade lärarrollerna i organisationerna. Vi bryr oss inte alls lika mycket om våra anställda som vi gjorde tidigare. Och de bryr sig inte om oss som arbetsgivare.”

Publiciteten värre än brottet

Till sist är risken att åka fast liten, väl under 50 procent. De flesta bolag som råkar ut för bedrägerier håller tyst. De vill inte riskera att aktiekursen faller, om de är ett börsnoterat bolag. De vill inte se ut som ett dåligt exempel. Bedrägerier är ett civiliserat brott, mycket bättre än att råna en bank – där risken att åka fast är så mycket större.”

Det här är bakgrunden till varför vi förstås anser att det är nödvändigt att kontrollera vilka det är som får jobb i företaget/organisationen. Det finns många trista konsekvenser av att få in fel personer, allt

från ekonomiska förluster via missnöjda aktieägare till myndigheters intresse och utredningar.

Diplom från Oxford – 50 pund

Enligt vår erfarenhet har en av fyra jobbansökningar någon information som inte stämmer. Så visar Jeremy Phipps upp sitt diplom från Oxford University och förklarar att han köpt det för 50 pund via en annons i tidningen Private Eye förra året. ”Att trycka sådana här är inte illegalt, jag kan sätta upp det på väggen hemma. Men att använda det för att få ett jobb är olagligt.”

Men ett större problem är falska universitet och andra institutioner som utfärdar fina, men falska betyg och examina. Ofta har de namn som låter riktiga och seriösa, men som är påhittade. Några exempel är Emmanuel College Oxford – som snyltar på riktiga Emmanuel College i Cambridge. Men den som ringer till det falska i Oxford får ändå svar med hela namnet, det finns en dam anställd för att svara – det ingår i priset för den falska examen.

”En av mina favoriter, som nu lämnat marknaden var London Insitute of Applied Research, förkortat LIAR. Ställföreträdande chefen för FN-organet WHO fick avgå i februari i fjol sedan det avslöjats att alla de kvalifikationer han uppgivit var falska.

Vilka fuskar med kvalifikationerna?

Till den första gruppen hör förstås de som inte har tillräckliga kunskaper, som den redovisningsansvarige som inte kunde matematik, men fick ett välbetalt jobb, trots att han var traktorförare på en gård i Irland.

Så finns de farliga individerna, antingen våldsamma eller med avvikande socialt beteende. De kan vara en fara för resten av organisationen.

I den tredje gruppen finns de som har något att dölja. Ett sätt att avslöja dessa personer är att läsa deras CV:n mycket noga och se om det finns några luckor, antingen i tid eller i logik. Två års konvalescens kan vara två år i fängelse. Och mer än var fjärde CV innehåller överdrifter vad gäller kvalifikationer. ”Varför? Jo, därför att människor vill ha arbete. Folk kan ljuga för att få ett jobb!”

”Utomstående kan bidra i en process som syftar till att undvika

olämpliga personer, som Raj Persaud mycket riktigt talade om, eftersom det är nyttigt med en objektiv syn utifrån. Men dessutom är det ett tidskrävande arbete att kartlägga personer, där erfarenheten om hur man gör är viktig. En del av uppdraget är att bestämma hur hög risken är i de arbetsuppgifter som ska utföras."

Marknaden för tillfällig arbetskraft, som hyrs in från personaluthyrningsföretag, ökar. Men detta ökar sårbarheten hos uthyrarnas kunder. Här finns möjligheter för den organiserade brottsligheten. "En hög polistjänsteman beskrev i slutet av förra året för mig hur brottssyndikat framförallt noga följer annonser där banker söker tillfällig hjälp. Deras egna personer lotsas in i organisationen och "tappas" därefter på information varje lördag. Det här ger möjligheter till utpressning eller bedrägerier."

Frågestund med Raj Persaud och Jeremy Phipps:

Till Raj Persaud: Finns det någon skillnad mellan finansiella bedragare och "vanliga" brottslingar?

Svar: En skillnad är intelligensnivå, IQ. Det kan mycket väl vara så att en psykopat med hög IQ kommer att arbeta i finansbranschen, vara hög chef i ett bolag eller i den offentliga sektorn, medan den som har samma psykopatdrag men lägre IQ rånar banker med vapen.

Fråga: Vad är sannolikheten för att en person som testats och kontrollerats och befunnits hederlig ändrar sig?

Svar: Jeremy Phipps: Det är inte lätt att börja testa och undersöka personer som varit anställda länge, utan att detta tas illa upp. Jag försöker få mina uppdragsgivare att testa vart femte, sjätte år. Det kan ha hänt mycket i personens värld, som en skilsmässa.

Raj Persaud: En sista reflektion apropå folks hederlighet. Det finns intressant psykologisk forskning som visar att utseendet spelar stor roll för om en person ska uppfattas som hederlig eller inte. Folk tänker "Han eller hon ser hederlig ut". Men erfarenheten är snarast att det är personer som går omkring och ser hederliga ut som det finns skäl att oroa sig för, för de vet och kan använda att de ser trovärdiga ut. Personer som ser skumma ut är ofta hederliga, därför att de vet att de kommer att bli misstänkta och därmed kontrollerade.

Telematik 2004 genomförs i samarbete mellan KFB och TELDOK. Programmets utgångspunkt är de förändringar som sker i samband med att Sverige omvandlas till ett informationssamhälle. En viktig aspekt är att IT väntas övergå från att vara expertteknik till att bli massteknik, och de följder detta får.

Programmet bygger på att mycket i informationssamhället år 2004 kan skönjas och granskas i verkliga livet och i demonstrationsmiljöer flera år före år 2004. Inom ramen Telematik 2004 produceras småskrifter och rapporter. Småskrifterna på ca 30-50 sidor dokumenterar rundabordssamtal och/eller intervjuer där olika åsikter och erfarenheter lyfts fram. Rapporterna på max 100 sidor ger en mer heltäckande bild av tidiga användare samt en tydlig framåtblick mot år 2004.

Utgivna publikationer inom programmet Telematik 2004:

Carlsson, Bengt	Ny teknik som drivkraft och hjälpmedel för finansiella bedrägerier

telematik 2004

KFB (www.kfb.se) och TELDOK (www.teldok.org) driver fram till mitten av 2001 programmet Telematik 2004 för att finansiera och publicera studier av tidiga användare och användningsområden i "informationssamhället". Projekten som finansieras (hittills nio stycken) resulterar i två slags publikationer: "småskrifter" med samtal och intervjuer (30–50 sidor) samt lite längre rapporter (ca 100 sidor).

Ny teknik som drivkraft och hjälpmedel för finansiella bedrägerier

Internet gör det enklare att vara bedragare. Det som tidigare krävde personal och lokaler för att skilja folk från sina pengar kan nu skötas med hjälp av en hemsida på internet, som kräver mindre resurser att göra och är lätt att flytta. Det är den dåliga nyheten. Den goda nyheten är att internet och annan teknisk utveckling gör det enklare även för dem som ska fånga bedragarna, som polis och tillsynsmyndigheter.

Framtiden blir en kapplöpning mellan "det onda och det goda". Och det handlar om gigantiska belopp. Enligt en beräkning beräknas finansiella bedrägerier under 1999 ha omsatt mer än 20 miljarder pund, runt 275 miljarder svenska kronor. Ingen vet säkert hur mycket det är.

Internetbedrägerierna dominerar och står för drygt hälften av de finansiella bedrägerierna enligt de uppskattningar som gjorts. Det finns en uppsjö av bedrägeriformer, från falska länder – rapporten beskriver Melchizedek – via falska råd i värdepappersaffärer till "vanliga" stölder av kreditkortsnummer.

För den som vill utnyttja Internets alla möjligheter finns bara ett enkelt råd: Var på Din vakt. Tre faktorer, förutom kunskap, kan vara hjälp på vägen: tips i medierna, information från andra användare – sprids inte minst via internet – och en rejäl dos sunt förnuft.

Småskriften – den första i programmet Telematik 2004 – har skrivits för KFB och TELDOK av Bengt Carlsson (bengt.carlsson@dn.se), journalist på Dagens Nyheter.

KFB & TELDOK
KFB-rapport 1999:36 • Via TELDOK 37