Projekten

Vad skall ni göra?
Hur skall ni göra det?

Om projekten

Projekt = säkerhetsutvärdering

16 givna fall

Utförs solo eller i par

Analysera och föreslå åtgärder

Använd metoder givna i kursen!

Uppgiftsämnen

- **Biljettbeställning över nätet**
- **Dagligvarubutik**
- **Distansarbete**
- **Egen tidigare arbetsplats**
- **Enmansfirma**
- **Forskargrupp**
- **Hasardspel**
- **Hemstyrsystem**
- **Kommunal hemtjänst**
- **Kemiindustri**
- **Lantbruk**
- **Morbror August**
- **Säkerhetsdelen i offert**
- **Familjen Vringhed**
- **Vaktbolag**
- **Veterinärklinik**

Innehåll: Analys + åtgärd

CIA-analys

Identifiera brister

Hotanalys

Riskanalys

Åtgärder med prioritering

Storlek och bedömning

Ca 6-8 sidor. Sidanatal är oviktigt, det är innehållet som räknas!

Lämnas in på sätt som meddelas senare. Säger jag inget så E-posta. Märk rapporten med LiU-ID i både titel och innehåll!

Plagiera inte! Rapporterna testas i Urkund.

Generativ AI

Viktig aspekt numera: Användning av generativ AI, t.ex. ChatGPT.

Flera varianter:

1) Använd inte ChatGPT alls. Tryggt och säkert.

2) Använd ChatGPT som rådgivare. Dokumentera detta och *kritisera resultatet*. Hitta fel och brister, eller notera anmärkningsvärda positiva saker som inte var väntade.

3) Låt ChatGPT skriva hela rapporten. INTE TILLÅTET! Jag ser det och kommer att examinera er hårdare. Det räknas som FUSK och jag måste dessutom rapportera er. Låt bli!

Generativ AI -> muntlig presentation

Ni kommer att presentera era resultat muntligt på seminarier, 3-4 grupper i taget.

Detta är en nödvändig ändring i år på grund av generativ AI. Jag måste kunna kontrollera att ni vet vad ni talar om.

Detta tar plats i januari, under tentaperioden.

Poängsystem infördes förra året för mer rättvis bedömning. Justeras i år baserat på de nya redovisningarna. Preliminärt:

Struktur och läsbarhet: 3 poäng
Problemanalys: 5 poäng
CIA eller AAA: 5 poäng
Hotobjekt och hotagenter: 3 poäng
Riskanalys: 5 poäng
Åtgärder med prioritering: 5 poäng
Muntlig presentation: 5 poäng NY!

Max 31 poäng. Preliminära poänggränser: 12 för betyg 3, 17 för betyg 4, 23 för betyg 5.

Viktiga datum

Första utkast behöver lämnas in senast 1/12 för att jag skall få med det i återkopplingen på sista föreläsningen (8/12).

Fö 10 8/12 återkoppling men även social engineering.

Presentationer under tentaperioden i januari.

Slutversionen lämnas in innan tentaperiodens slut i januari.

Möjlighet till examination senare. Kommer att ge visst poängavdrag.

Exemplen: Pickup at South Street och Lewis Avery Filer

Låt oss gå igenom två fall för att visa hur analysen går till.

- Problembeskrivning
- CIA
- Risker
- Prevention-detection-reaction
- Åtgärder
- Prioriteringar

Lewis Avery Filer

eller

Over 50? Steal!

Exempel: Lewis Avery Filer

Vem är hotad? Vem är offret? Försäkringsbolaget.

Du skall göra en rapport om detta. Vem är kunden, uppdragsgivaren? Försäkringsbolaget! Du har i uppdrag att analysera säkerheten för försäkringsbolaget!

Vi tar det steg för steg.

Exempel: Lewis Avery Filer, problemanalys

Problemanalys:

Bolagets kunder har varierande säkerhetsnivå och hanterar stora ekonomiska värden.

Bolagets anställda har stor kunskap om kunderna.

Bolaget har nyligen gått samman med ett annat och ett betydande antal anställda har avskedats, rationaliserats bort. Många av dessa är mycket erfarna, 50+, har arbetat för företaget i decennier. De avskedades enkelt och informellt.

Dessa har god kunskap om typiska tjuvar, deras beteende och bakgrund och deras säkerhetssystem (kassaskåp mm).

Exempel: Lewis Avery Filer, CIA

Confidentiality: Huvudproblemet! Insiders vet om känslig information.

Integrity: Inte relevant för rånet, men han har dessutom förfalskat spår som pekar på fel personer. Är det integrity? Inte för företagets information. Det är ett problem för polisen men inte för vår kund!

Availability: Tillgängligheten för juvelerna helt enkelt.

Vilken sorts angripare: Definitivt blue hat, han är ute efter hämnd. Expertnivå.

Exempel: Lewis Avery Filer, risker

Skicklig tjuv (teknisk kompetent, stor kunskap om målet, använder social engineering), betydande mätbar kostnad = hög risk för nya stölder.

Kommentar på detta: Underskattning av stöldrisk på grund av god kunskap om andra typer av tjuvar = man trodde att man var säker. Slutsats: Ovanstående ökad risk är en revision av tidigare uppskattning.

Risk för försämrat rykte om kopplingen till försäkringsbolaget upptäcks.

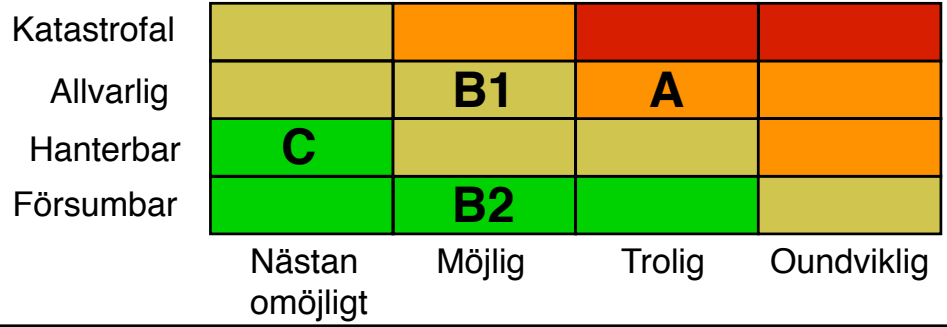
Risk för skador på personal.

Exempel: Lewis Avery Filer, riskanalys

A: Risk för ekonomisk förlust: Hög sannolikhet (0.75), rätt hög skada.

B: Risk för skador på personal: Liten (0.4), han vill inte skada dem men kan pressas till det. Hög skada om de är försäkrade hos företaget, annars irrelevant.

C: Risk för försämrat rykte. Mycket liten risk. (0.1) Måttlig skada.



Exempel: Lewis Avery Filer, sök åtgärder

Hitta åtgärder genom att dela upp dem i prevention-detection-reaction.

Prevention: Avskeda folk på ett trevligare sätt. Betala rejäla avgångsvederlag. Var medveten om att dessa har insider-info! Värdera företagets trotjänare högre. Ändra informationen.

Detection: Trivialt. Han ser till att angreppet syns, tydligt! Men att upptäcka det i förväg är svårare.

Reaction: Förutse troliga nästa mål, förbättra säkerheten, ändra rutinerna. Hjälp polisen gripa tjuven.

Exempel: Lewis Avery Filer, åtgärder på A0-A1

A0. Reaction på A: Ingen åtgärd. Betydande summor måste betalas ut. Kostnad: Hög (d ≈ 1M$) Risk efter åtgärd: Samma.

r = p*d = 0.75 * 1 = 0.75

A1. Långsiktig prevention för A: Rejäla avgångsvederlag. Kostnad: Mycket hög. Risk efter åtgärd: försumbar, p' = 0.1. (k ≈ 10M$)

r'+k = p'*d + k = 0.1 * 1 + 10 = 10.1

Exempel: Lewis Avery Filer, åtgärder på A2-A3

A2. Långsiktig prevention för A: Bra rekommendedationsbrev. Kostnad: Mycket låg för brevet, medelhög för framtida konkurrens. Risk efter åtgärd: hanterbar, p' = 0.2. (k ≈ 2M$)

r'+k = p'*d + k = 0.2 * 1 + 2 = 2.2

A3: Långsiktig prevention på A: Sparka INTE 50+are! Kostnad: Ganska låg: lön mot fortsatta insatser. Viss kostnad pga övertalighet, kan ge vinst men kan kosta upp till k ≈ 5M$. Låt oss säga 2.5. p' = 0.

r'+k = p'*d + k = 0 * 1 + 2.5 = 2.5

Exempel: Lewis Avery Filer, åtgärder på A4-A5

A4. Prevention för A: Utbilda personalen om riskerna, speciellt social engineering. Kostnad: Medel, k ≈ 100k$. Risk efter åtgärd: Hanterbar, p' ≈ 0.3

r'+k = p'*d + k = 0.3 * 1 + 0.1 = 0.4

A5. Prevention för A: Förändra hos kunderna för att göra insidesinformationen meningslös. Kräver sponsring av kunderna! Risk efter åtgärd: Hanterbar, 0.3. Kostnad: Hög (Uppskattas till 5M$)

A5. r'+k = p'*d + k = 0.3 * 1 + 5 = 5.3

Exempel: Lewis Avery Filer, åtgärder på B

B0. Reaction på B: Ingen åtgärd, betala sjukhusräkningarna.
Kostnad: Rätt hög (för det är Hawaii = USA) Uppskattas till 100k$
Risk efter åtgärd: Oförändrad

B0. r = p*d = 0.4 * 0.1 = 0.04

B1. Prevention för B: Utbilda personalen att inte provocera tjuven till våld. Kostnad: Låg (Uppskattas till 1k$) Risk efter åtgärd: Försumbar (0.1).

B1. r'+k = p'*d + k = 0.1 * 0.1 + 0.001 = 0.011

Exempel: Lewis Avery Filer, åtgärder på C

C0. Reaction på C: Ingen åtgärd. Kopplingen är offentlig. Risk 0.3, måttligt troligt att kunderna reagerar. Skadan är måttlig, lite förlorade intäkter. (Uppskattas till 0.2M$)

r = p*d = 0.3 * 0.2 = 0.06

C1. Prevention för C: Hemlighåll kopplingen. Enkelt. Kostnad: Låg (Uppskattas till 0.01M$) Skadan sjunker till 0.

r'+k = p'*d + k = 0.01 = 0.01

Exempel: Lewis Avery Filer, skada och kostnad

p = sannolikhet (probability), antar linjär skada/kostnad
p' = sannolikhet efter åtgärd
k = kostnad för åtgärd
d = skadan, kostnad om attacken lyckas

A0. r = p*d = 0.75 * 1 = 0.75

A1. r'+k = p'*d + k = 0.1 * 1 + 10 = 10.1

A2. r'+k = p'*d + k = 0.2 * 1 + 2 = 2.2

A3. r'+k = p'*d + k = 0 * 1 + 2.5 = 2.5

A4. r'+k = p'*d + k = 0.3 * 1 + 0.1 = 0.4

A5. r'+k = p'*d + k = 0.3 * 1 + 5 = 5.3.

Exempel: Lewis Avery Filer, skada och kostnad

p = sannolikhet (probability), antar linjär skada/kostnad
p' = sannolikhet efter åtgärd
k = kostnad för åtgärd
d = skadan, kostnad om attacken lyckas

B0. r = p*d = 0.4 * 0.1 = 0.04
B1. r'+k = p'*d + k = 0.1 * 0.1 + 0.001 = 0.011

C0. r = p*d = 0.3 * 0.2 = 0.06

C1. r'+k = p'*d + k = 0.01 = 0.01

Exempel: Lewis Avery Filer, prioriteringar

A4. Utbilda för att undvika stöld = 0.4 i stället för 0.75
C1: Hemlighåll, 0.01 i stället för 0.06
B1: Utbilda personalen, 0.001 i stället för 0.011

Alla andra åtgärder bedöms dyrare än skadan!

Men är mina uppskattning korrekta?

Exempel: Lewis Avery Filer, slutsats

Många åtgärder är alldeles för dyra.

Enbart utbildning av personalen bedöms som rimligt för att undvika stöld.

Det är också lönsamt att undvika personskador!

Pickup at South Street

Exempel: "Pickup at South Street"

Lite mer komplext fall!

Eller är det det?

Exempel: Pickup at South Street

Vem är hotad? Alla! Vem är vår kund?

Spionorganisationen! :)

(Inte för att jag gillar kommunistiska spioner utan för att det är deras situation som är intressant.)

I neutralitetens namn så bestämmer jag att kommunisterna är bordurier och de bestulna är syldaver.

Du skall göra en rapport om detta.

Exempel: Pickup at South Street

Problemanalys:

Spionerna stjäl en hemlig mikrofilm och skall frakta den ur landet till det onda kommunistlandet Bordurien.

De väljer att låta detta göras av en söt och till synes oskyldig flicka som lägger den i handväskan och åker tunnelbanan som vanligt.

Det finns en viss risk att hon är bevakad av polisen, men hon är omgiven av en massa vanligt folk så man räknar med att hon försvinner i mängden.

Exempel: Pickup at South Street

Confidentiality: Håll stölden och transporten hemlig.

Integrity: Det finns frågor här. Är vi så säkra på att hon verkligen har rätt mikrofilm? Tänk om de snälla syldaverna har bytt ut den och lagt dit en falsk!

Availability: Tillgängligheten för mikrofilmen är kritisk!

Vilken sorts angripare: Beror lite på synvinkel men från din uppdragsgivares synvinkel är syldaverna Black Hat, det är fienden som är ute efter att förstöra dina planer.

Exempel: Pickup at South Street

Risker:

- Hon blir tagen av polisen
- Ficktjuvar
- Väskryckare
- Hon tappar bort väskan av misstag
- Hon har fått fel mikrofilm
- Personskada på grund av strid med polis eller tjuv
- Personskada på grund av bestraffning

Exempel: Pickup at South Street, prevention

Prevention:

Blir tagen av polisen:

• Utbildning. Få henne att upptäcka om hon är skuggad och lär henne hur man smiter undan.
• Lär henne hur man snyggast gör sig osynlig i folkmassor.
• När det inte kan undvikas, göm undan mikrofilmen så en kollega kan få tag i den senare.
• Spring av bara katten.

Exempel: Pickup at South Street, prevention

Ficktjuvar:
• Bättre väska. Lås på väskan. Kan rentav använda en väska med biometrisk lås så ficktjuven inte ens kan dyrka den. Väskryckningssäker.
• Vilseled angriparen: Ha falska saker lättstulna, värdefullt dolt.

Tappa bort väskan av misstag: Se nedan, medföljare.

Både polis och ficktjuvar:
• Ha en medföljare som har till uppgift att
1) höja hennes säkerhet, upptäcka hot och åtgärda dem.
2) Ta tillbaka mikrofilmen om den stjäls.

Exempel: Pickup at South Street, prevention

Prevention:

Fel mikrofilm:

• Utför kontroller tidigast möjligt.
• Analysera situationen. Var mikrofilmen lite väl tydligt falsk? Var det en "honungsfälla" för att sätta dit spionerna?

Exempel: Pickup at South Street, detection

Ganska enkelt i detta fall.

- Upptäck ficktjuvar och poliser innan de hinner göra skada
- Upptäck om mikrofilmen är falsk

Exempel: Pickup at South Street, reaction

Reaction:

Tjuv & polis: Försök ta tillbaka mikrofilmen från polisen eller tjuven. Förfölj dem tills det är möjligt.

Falsk mikrofilm:

Avbryt och gör ny plan.

Exempel: Pickup at South Street, riskanalys

A: Ficktjuv/väskryckare: Stor risk på tunnelbanan. 0.5

B: Polis: Ganska stor risk. 0.3

C: Slarv: Låg risk. Hon vet att hon bär något värdefullt. 0.1

Samtliga fall ovan ger stor skada.

D: Personskada på grund av konflikt (0.2)

E: Personskada på grund av bestraffning (0.4)

Dessa fall ger låg skada. Spionerna bryr sig inte om sin personal men i fallet D kan det vara personal med visst värde.

Exempel: Pickup at South Street, risker

Hot om personskada varierar lite med olika hot. Låg skada för bestraffning, högre när det är strid mot tjuv eller polis.

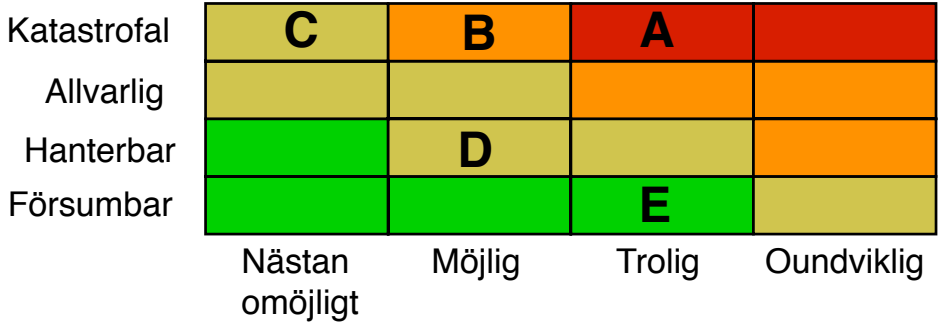
Vi sammanfattar alla hot mot mikrofilmen som ett, "förlust av mikrofilmen" med total sannolikhet 0.7.

1. Strid med ficktjuv (i sig 0.5). Låg sannolikhet för personskada. 0.1 Skada 3.

2. Strid med polisen (0.3). Medelhög sannolikhet för personskada. 0.5 Skada 3.

3. Bestraffning (0.7). Hög sannolikhet efter förlust av mikrofilm (0.8) Skada 1.

Exempel: Pickup at South Street, riskanalys



Exempel: Pickup at South Street, åtgärder mot stöld

Vi sammanfattar alla hot mot mikrofilmen som ett, "förlust av mikrofilmen" med total sannolikhet p = 0.7 och maximal kostnad på 10. (Jag väljer här tiogradig skala på skada och kostnad.)

1. Bättre väska. Kostnad: Låg (k = 1). $p' \approx 0.2$

2. Avancerad väska. Kostnad: Hög (k = 5). $p' \approx 0.1$

3. Falska objekt. Kostnad: Låg (k = 2). $p' \approx 0.1$

4. Medföljare. Kostnad: Medel (k = 2). $p' \approx 0.3$

5. Utbildning. Kostnad: Medel (k = 3). $p' \approx 0.4$

Kostnaden för risken och åtgärden

p = sannolikhet (probability), antar linjär skada/kostnad
p' = sannolikhet efter åtgärd
k = kostnad för åtgärd
d = skadan, kostnad om attacken lyckas

0. Ingen åtgärd	r = p*d = 0.7*10 = 7
1. Bättre väska.	r'+k = p'*d + k = 0.2 * 10 + 1 = 3
2. Avancerad väska	r'+k = p'*d + k = 0.1 * 10 + 5 = 6
3. Falska objekt	r'+k = p'*d + k = 0.1 * 10 + 2 = 3
4. Medföljare	r'+k = p'*d + k = 0.3 * 10 + 2 = 5
5. Utbildning	r'+k = p'*d + k = 0.4 * 10 + 3 = 7

Exempel: Pickup at South Street, åtgärder, personskador

Utbildning och medföljare är de effektiva åtgärderna. Riskerna sammanfattas till 1 - (1-0.5)*(1-0.3)*(1-0.1) = 0.7

Förväntad skada är maximala d = 0.7*3 = 2.1

1. Ingen åtgärd. r = p*d = 0.7 * 2.1 = 1.5
2. Medföljare. p' ≈ 0.3. r'+k = p'*d + k = 0.3*2.1 + 2 = 2.6
3. Utbildning. p' ≈ 0.4. r'+k = p'*d + k = 0.4*2.1 + 3 = 3.8

Slutsats: Låg kostnad utan åtgärd. Svag påverkan på prioriteringen.

Vi kan gå längre genom att koppla åtgärderna till att de påverkar flera risker och därmed gör dubbel effekt.

Exempel: Pickup at South Street, slutsats

Högsta prioritet är väskan samt falska objekt. Båda har stor effekt för låg kostnad.

Efter denna kommer medföljaren.

Avancerad väska är dyrt.

Utbildning har lägst prioritet, hög kostnad och låg effekt

Hela listan av motivation, risker, åtgärder och prioriteringar levereras till uppdragsgivaren.

Dock kan mikrofilmen värderas högre, och då blir alla åtgärderna önskvärda. De skall fortfarande ha en prioritetsordning