
# Incidenthanteringsplan och preliminära undersökningar

## Vad är en datorincident?

## Incidenthantering

# Datorincidenter och informationspolicy

- En datorincident är
  - En händelse som strider mot någon av en organisations explicita policys för t.ex. säkerhet eller användande av datorsystem etc.
- Exempel på datorincidenter
  - Ladda ner och gömma kopieringsskyddad musik, film, program etc.
  - Använda programvara i datorsystemen som stjäl användarnamn, lösenord etc.
  - Använda programvara som förstör data eller gör vissa tjänster eller system oanvändbara
  - Använda organisationens datorer för personlig användning utan tillåtelse på arbetstid!
  - Fler?

# Datorincidenter och informationspolicy

- När incidenter inträffar
  - Problemen identifieras och åtgärder vidtas för att det inte skall hända igen
    - Nya/förändrade grupp-policys
      - Software rights policy – vilka programvaror får exekvera
      - Software audit – logga vad programvaror gör
    - Firewalls eller proxy-servrars konfigurationer ändras
    - Konfigurationer för routrar eller annan aktiv hårdvara ändras
- Anställda kan få sparken för att de brutit mot någon policy
  - Bevis kan vara tvunget att skaffas fram om arbetstagaren bestrider uppsägningen
- Bevis kan till en början verka röra sig om en överträdelser mot policyn
  - Efter undersökning kan det visa sig vara kriminell aktivitet

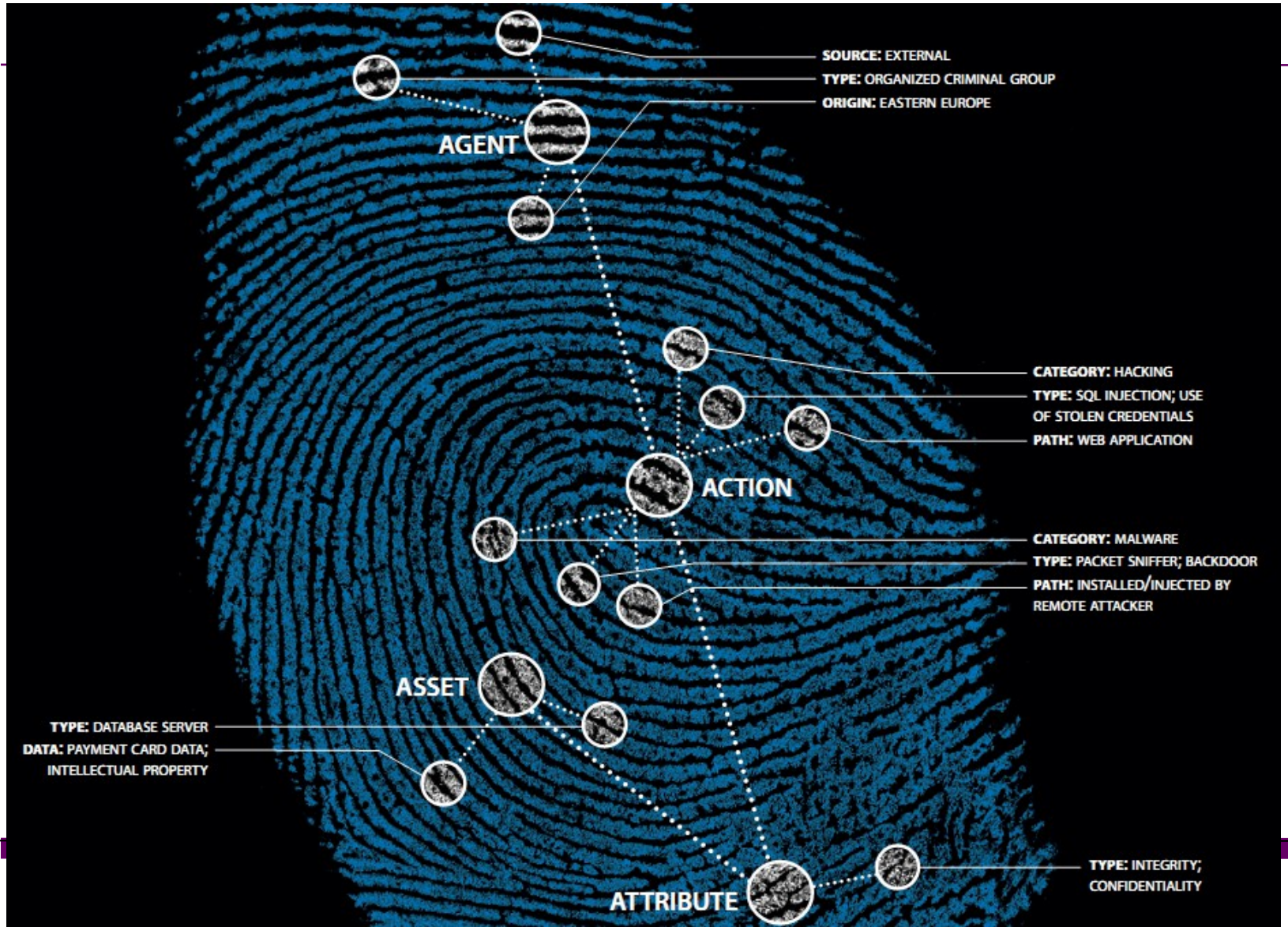
# Databrott

- Databrott är användandet av datorer för att begå brott
  - I Sverige finns bara rubriceringen dataintrång
- När/om ett databrott upptäcks
  - Kontakta säkerhetsansvariga direkt om det finns, de kommer att hantera kontakten vidare
  - Försök avgöra när bevis behöver säkras
    - Direkt, om du tror att bevis kan försvinna
    - Senare, för att få ”bättre” bevis
  - Se till att ”chain of custody” underhålls
  - Räkna med att fullmakt kan behövas
- Tänk på att lagar skiljer sig åt i världen!!
- Bli inte en ”agent of the law” som äventyrar caset!

# Databrott statistik

- I USA visar ”senaste årens” statistik från CSI/FBI ( www.gocsi.com) att otillåten användning är på väg ner, främst på grund av
  - Ökad användning av personliga brandväggar
  - Kraftfullare och påtvingade säkerhetspolicys
  - Beror främst på Windows XP sp2 och nyare Windows
- Malware (backdoor/trojans, spyware etc.) och
- Web application hacking (stolen login, backdoor/remote control channels, SQL injection etc.) är de nu ledande typerna av attackerna
- **Antalet organisationer som rapporterar intrång till polismyndighet minskar!!**

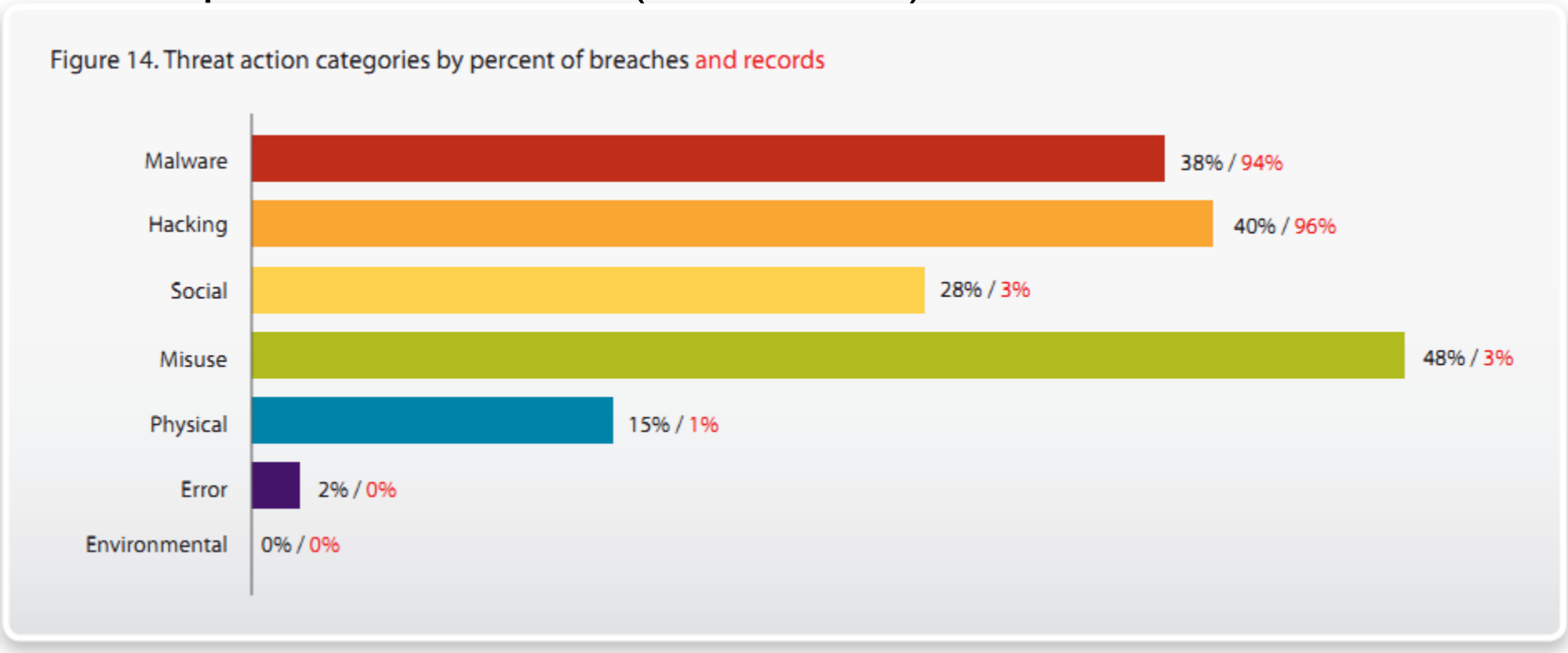
# 2010 Data Breach Investigations Report – Verizon Business and US Secret Service




HÖGSKOLAN Dalarna

# 2010 Data Breach Investigations Report – Verizon Business and US Secret Service

Threat actions (y) along with the percent of breaches and compromised records (stolen data) associated with each



# 2010 Data Breach Investigations Report – Verizon Business and US Secret Service

Figure 16. Threat action categories over time by percent of breaches (Verizon cases)

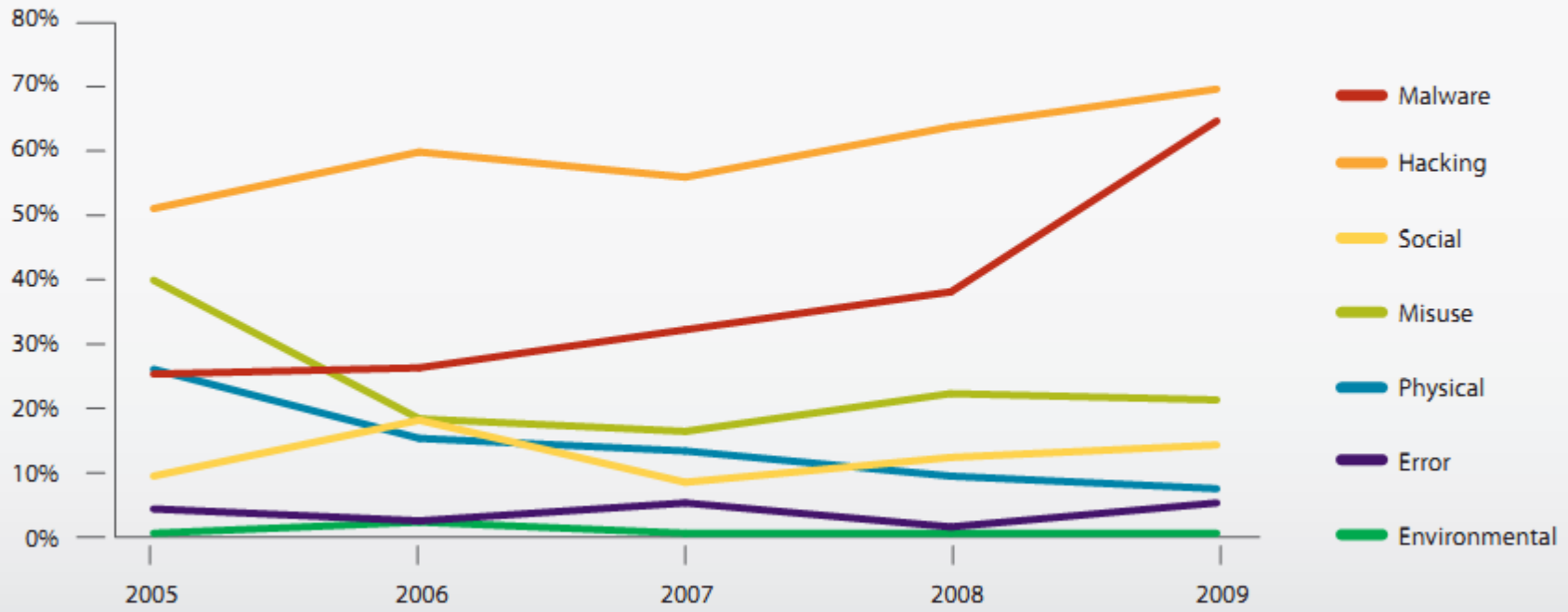


Figure 19. Malware functionality by percent of breaches within Malware and percent of records

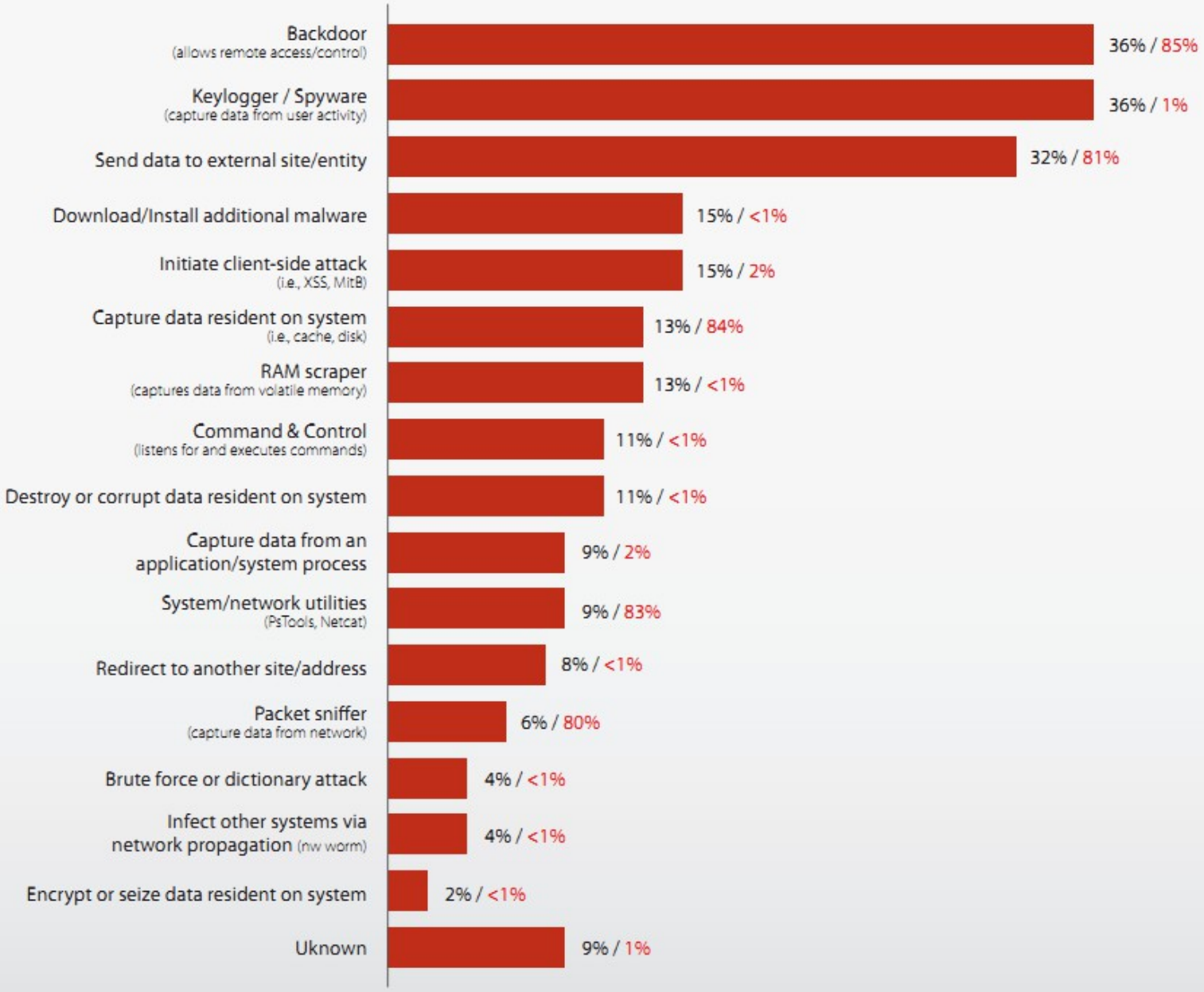
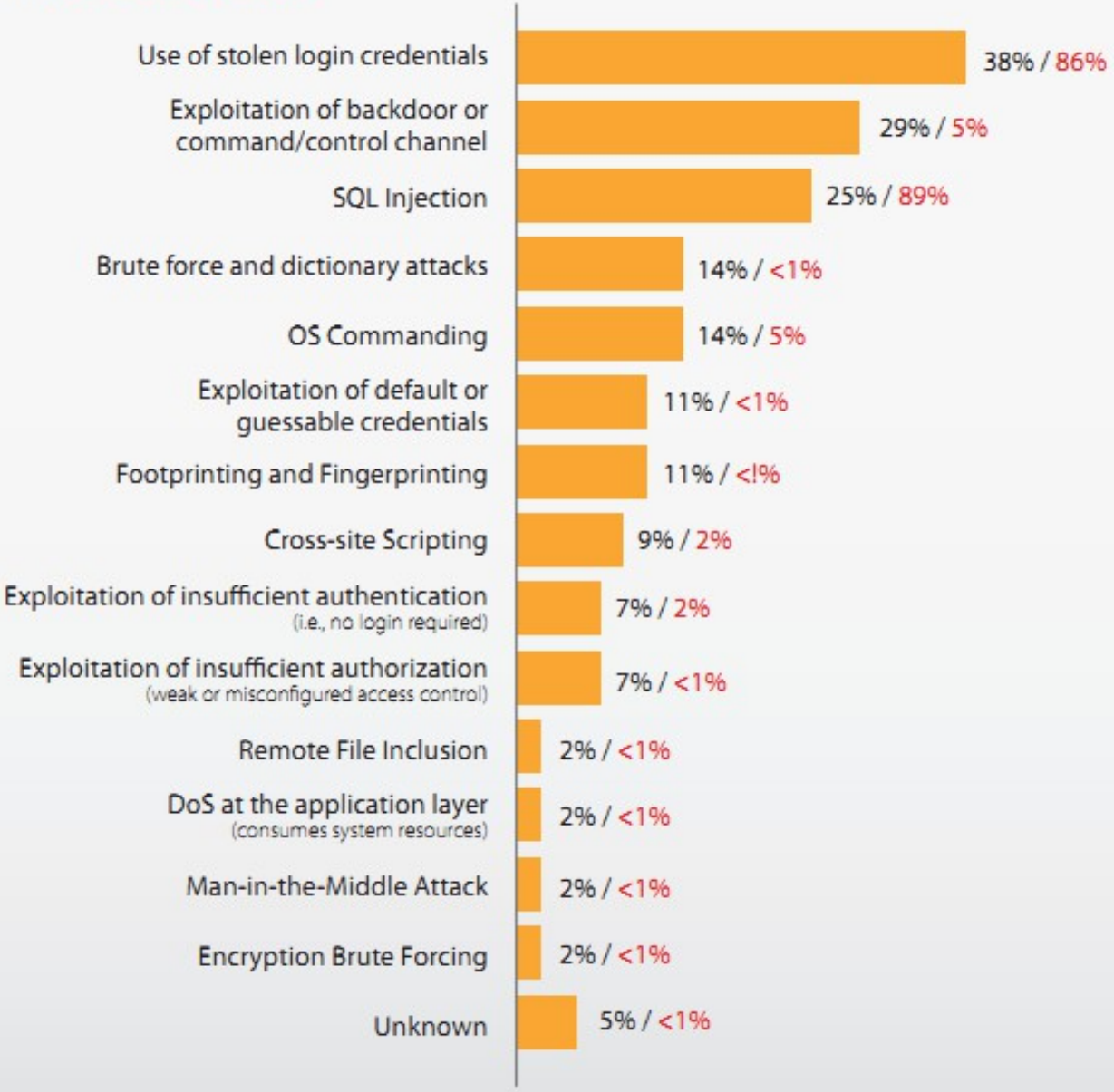
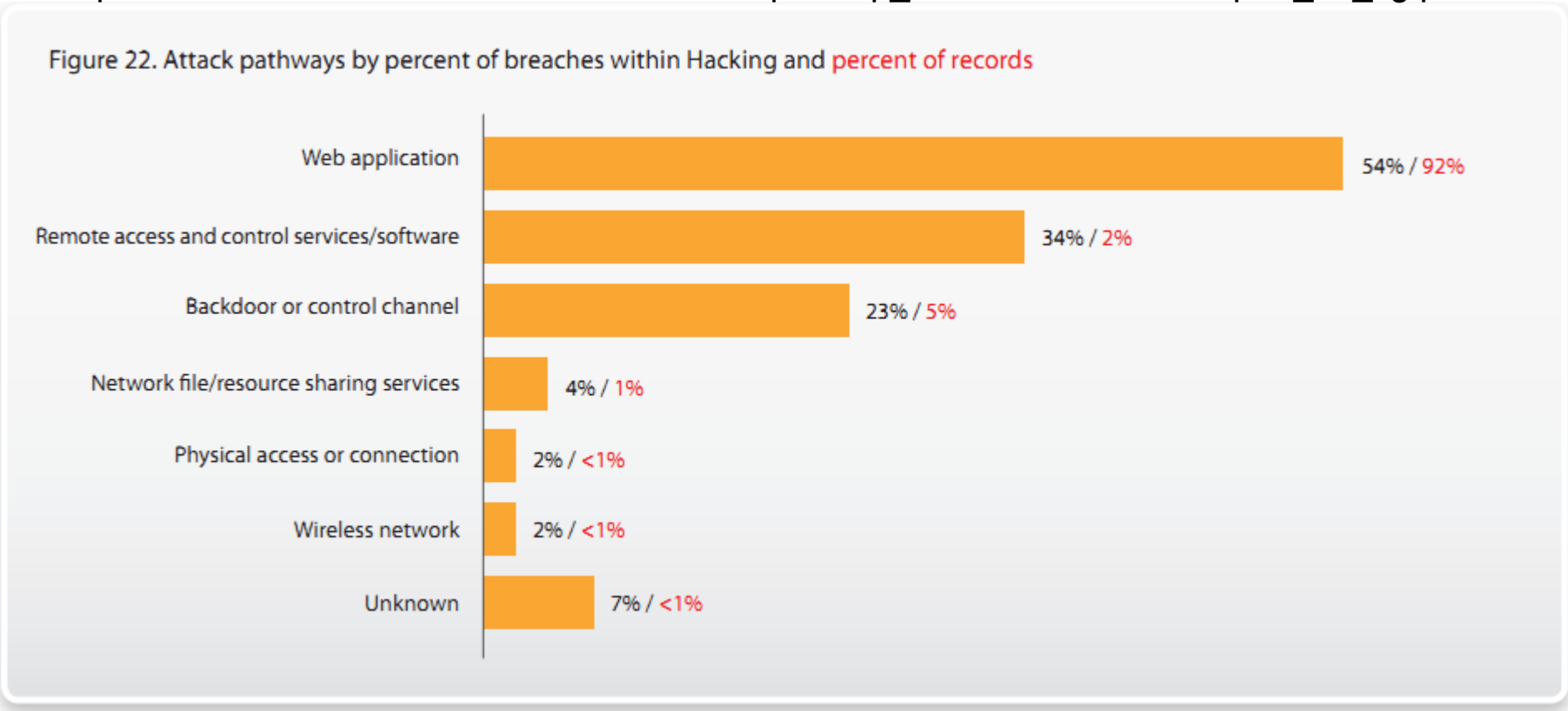


Figure 21. Types of hacking by percent of breaches within Hacking and percent of records



# 2010 Data Breach Investigations Report – Verizon Business and US Secret Service

http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf



# Skyldig eller oskyldig?

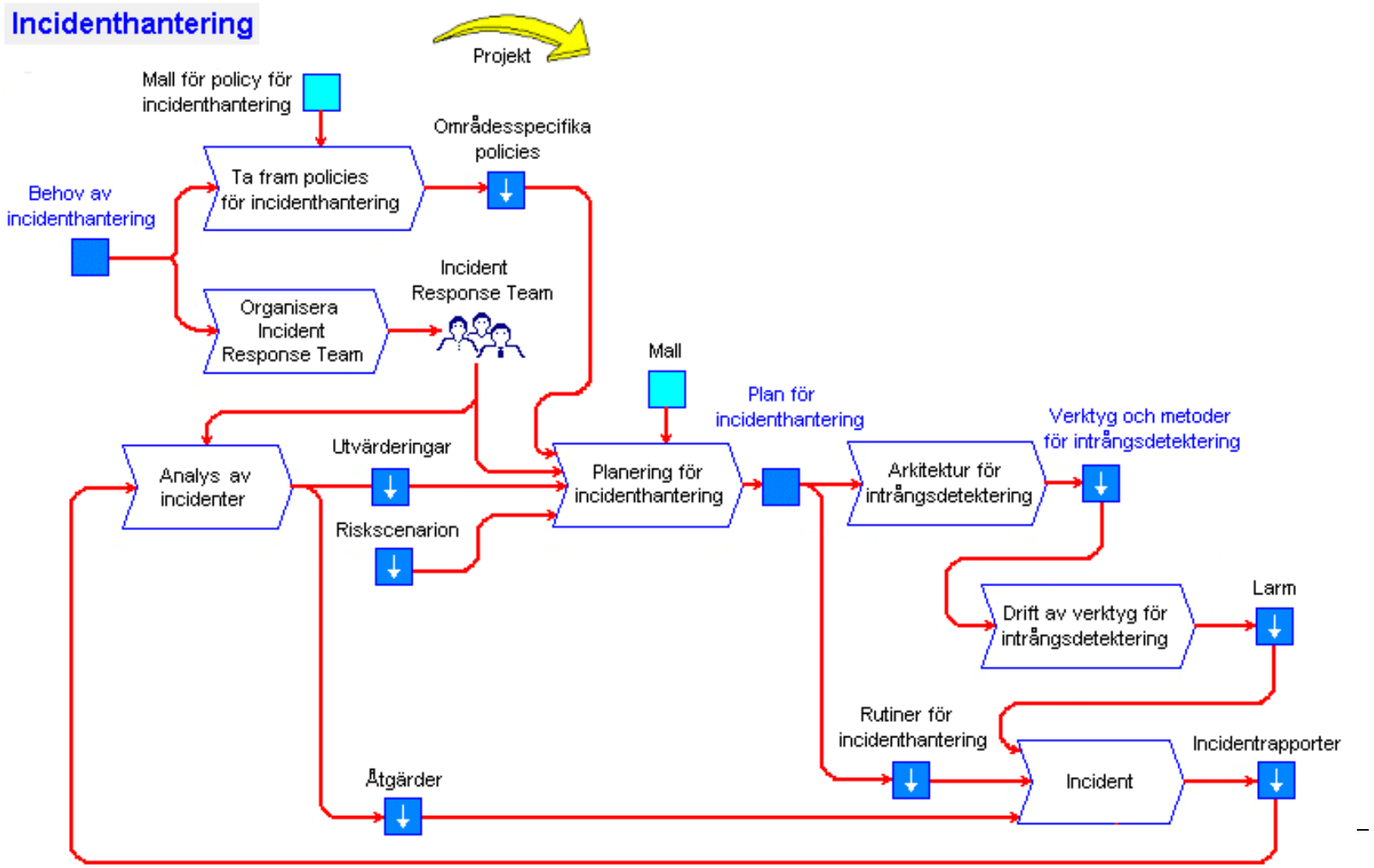
- Individer i de flesta länder är förmodat oskyldiga tills dess motsatsen har kunnat bevisats
- Personen du utreder
  - Kan vara oskyldigt dömd eller offer för
    - Hämnd
    - Konspiration (för att bli av med någon t.ex.)
    - Omständigheter (fel plats – fel tidpunkt)
- Datorn kan vara hackad eller använd av någon annan
- Bevis kan vara ledande (ofullständiga) eller till förmån för den åtalade
  - Anta aldrig att någon är skyldig, var **objektiv** i ditt agerande
  - Låt fakta tala!

# Incidenthantering

- Planer för att agera på incidenter bör vara
  - Väl genomtänkta
  - Fullständiga och regelbundet testade
  - Komplett dokumenterade och publicerade
  - Regelbundet uppdaterade vid förändringar
- Det finns flera företag som säljer ”incident respons plans” tjänster
- Incidenthanteringsplaner ingår ofta i katastrofplaner
- Ex. på mjukvara för incidenthanteringsplan
  - IMCD, http://www.contingenz.com
  - PAPAI, http://www.papai.se

CERT.SE – CIHSP - https://www.cert.se/incidenthantering

# Incidenthantering livscykel (PAPAI)




HÖGSKOLAN Dalarna

NAVIGERING

- Sammanfattning
- Steg 1 - Förebygga
- Steg 2 - Identifiera
- Steg 3 - Begränsa
- Steg 4 - Återställa
- Steg 5 - Erfarenheter

DE VIKTIGASTE FRÅGORNA VID EN INCIDENT

**Vid en första kontakt med en intressent som har råkat ut för en misstänkt incident så är det några frågor som organisationen bör få svar på. De viktigaste är listade nedan.**

- Vad har hänt, hur och när upptäcktes problemet?
- Vilka åtgärder har gjorts?
- Är incidenten fortfarande pågående, kan data läcka ut?
- Vad vill organisationen ha hjälp med?
- Vilka har organisationen kontaktat?
- Kan organisationen tänka sig att dela med sig av information, data eller loggar till tredje part eller andra drabbade organisationer?
- Vill organisationen polisanmäla incidenten?

# CERT-SE:s incidenthanteringsprocess (CIHSP)

CERT-SE:s incidenthanteringsprocess baseras på delar ur andra processer för incidenthantering, som till exempel SANS och NIST:s. De delar som CERT-SE, som incidenthanterare, först och främst arbetar med är: Identifiera, Begränsa och Förebygga.
Processen är först och främst till för CERT-SE:s egna arbete med incidenthantering men görs här tillgänglig för andra organisationer att använda sig av i informationssyfte.

**Det går att klicka i bilden eller använda navigeringsmenyn till vänster för att navigera igenom processen.**


Uppdaterad 2011-01-10 10:41 | Publicerad 2010-10-15 08:23

HÖGSKOLA Dalarna

# Förberedelse för incidenter

- Viktig initial information att hantera
  - **Vem, vad, när, var och hur**
- En form-baserad webb-sida för inrapportering kan vara en bra start
- Snabb hantering av incidenten är kritisk
  - Bevis kan skadas, förstöras eller förändras
  - Kritiska servrar kan hinna bli skadade
  - Känsliga uppgifter kan läcka ut
- Ingen katastrof om incidenten ej kan åtgärdas omedelbart
  - Kan leda till att mer bevis skapas eller att inkräktaren kan gripas (kanske blir ”oförsiktig” och gör ett nytt intrång)
- Hur användare skall agera vid incidenter skall framgå av **IT/incident-policyn**
- Vidare hantering (internt eller av polismyndighet) av incidenten bör avgöras av **incident-response gruppen**

# Inrapportering av incidenter

Myndigheten för samhällsskydd och beredskap

- CERT-SE (www.cert.se) IT-säkerhet för näringsliv och offentlig sektor
  - Oberoende organisation för stöd i samhället - **del av MSB**
  - All personal på CERT-SE är placerad i en högre säkerhetsskyddsklass (organisationers svagheter ska/får ej spridas)
- Varför Incidentrapportera?
  - Kortfattade IR ger säkerhetsinformation som för stunden är intressant
  - Mer detaljerade IR ökar kunskapen om angrepp på detaljnivå
  - Sammanfogas IR med statistiskt material ökar kunskapen om trender över tiden
- Vad ska rapporteras?
  - Definitionen av en incident kan variera, vanligtvis definieras en IT-incident som:
    En verklig eller uppfattad händelse av säkerhetskritisk karaktär i en dator eller ett nätverk
- Vem?
  - Alla är välkomna ☺

CERT SE | KONKURRENSNEUTRAL IT-SÄKERHET FÖR NÄRINGSLIV OCH OFFENTLIG SEKTOR

# Myndigheter och lagar

- Om ett ärende går så långt att det blir ett polisärende så kan följande lagar vara aktuella
  - Regeringsformen 2 kap. - Grundläggande fri och rättigheter
  - Brottsbalken
  - PUL (PersonUppgiftsLagen)
  - Arbetsrättslagar, osv.
- Överskottsinformation vid datoranvändning/avlyssning/övervakning
  - Särskilda tillstånd krävs
- Utredare måste hantera all information under sekretess
- Andra länder har t.ex.
  - U.S. Freedom of Information Act (FOIA)
  - U.K. Regulation of Investigatory Powers (RIPA)

# Incidentanalys

- Några aspekter för incidenten att utreda
  - Var var det som hände och när?
  - Hur påverkade incidenten den pågående verksamheten?
  - Hur känslig är påverkad information?
- Arbete som hör till (utförs först)
  - Identifiera och samla in all relevant information
  - Spar alla bevis och hanteringen (vilka steg du vidtagit) i en logg
    - Skapa *"**chain of custody**"* i händelse av att läget blir skarpt
  - Fotografera incidenten/brottsplatsen
  - Tillverka spegelkopior (image) av all media som varit inblandad i incidenten
  - Utför en forensisk analys enligt en **vetenskaplig repeterbar process** och som påverkar organisationen i minsta möjliga mån

# Begränsa och Återstart

- Begränsa och isolera attacker och minimera spridning
- Målet är att databaser, servertjänster och personal snabbt skall vara online och i produktion
  - Kan innebära mycket arbete!
    - Nya lösenord, uppdaterade versioner av programvara, nya rutiner, införande av ny policy (eller uppdatering av gällande)
    - Rensning av malware och återställning från backup-enhet
- Om ärendet går till domstol kan katastrofplaner behöva sättas i verket
  - Ersätta hårdvara
  - Total återställning från backup-enheter

# Erfarenheter – ”postanalys”

- Hade  processen som helhet kunnat göras bättre?
  - Togs rätt steg i rätt ordning?
  - Var rätt personal berörd/inblandad?
  - Fanns tillräckligt med underlag/styrdokument?
- Gjordes det några misstag?
  - Kan de undvikas?
  - Hur minimera skadan om den inte går att undvika?
- Användes verktygen korrekt?
- Fungerade informationsutbytet inom organisationen?
  - Mellan organisationen och intressepartners?
- Kan framtida incidenter av denna art förhindras?
  - Upptäckas tidigare?
- Behöver säkerhetspolicys modifieras/uppdateras eller synliggöras bättre?
- Behövs mer träning/utbildning av personal?

# Undersökningar - ej kriminella

- Det kan vara stor skillnad på dina befogenheter beroende på typ av organisation och land/nation
- Policyn på företaget är din ledstjärna!
  - Beskriver vad som är tillåtet eller otillåtet vid datoranvändning
  - Ger rätten att göra undersökningar
- Otillgängliga policys ger dåligt intryck - en policy bör vara väl exponerad, exempelvis redan vid inloggning
  - Ska innehålla klara/tydliga regler
    - Tillstånd att logga användare
    - Bestraffning vid överträdelse
    - **Inloggning innebär ditt godkännande av gällande policy**
- Policy som beskriver undersökningsprocedurer bör även finnas

# Undersökningar kriminella

- Vid konstaterad eller misstänkt kriminell aktivitet bör en organisations **juridiska** avdelning omedelbart kontaktas och all vidare korrespondens skötas av den
- Domstolsförfarande
  - Kan bli dyrt
  - Alla bevis måste överlämnas till polis och åklagare
  - Nyckelsystem kan komma att tas off-line
  - En rättsrisk finns alltid om inte allt hanterats ordentligt… följ uppsatta lagar
  - Företagshemligheter kan läcka ut
- Privata företag kan dra sig för att genomföra rättsliga processer på grund av ovanstående förfarande

# Lagar

- USA har sin ”**Fourth Amendment”** som skyddar mot olagliga genomsökningar och beslagtagning av egendom
- UK har **”The Police Powers Code of Practice”** som reglerar ovanstående
- UK har även **”The Regulation of Investigatory Powers Act”** RIPA (i 5 delar)
- Sverige har inga liknande dokument ännu
- Lagar varierar från land till land
  - Kolla Wikipedia/Google (ta med forensics)

# Organisationens avdelningar

- Help Desk Support - bör vara insatta i datasäkerhet
  - Kvalitén på deras instruktioner till användare kan påverka undersökningen eller brottsplatsen
  - Information i system är endera volotile eller non-volotile
    - Vad brukar supporten ge för råd när datorn beter sig underligt?!?!
- Personalavdelningen – hanterar vid incident
  - Individer, interna relationer, PR, etc.
- Alla avdelningschefer
  - Bör känna till det mesta om policys och procedurer

## When a first responder or sysadmin approaches a system to "investigate" they seem to like to do some combination of the following

- Run task manager
- Run netstat
- Run a rootkit detector
- Run an antivirus scan
- Delete files that look like they are related to something bad
- Run a backup/restore job
- Defrag the hard drive - usually because someone said the computer was slow
- *thwack* (http://www.forensicir.blogspot.com)