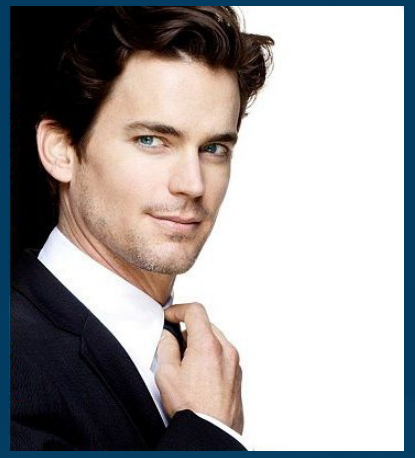
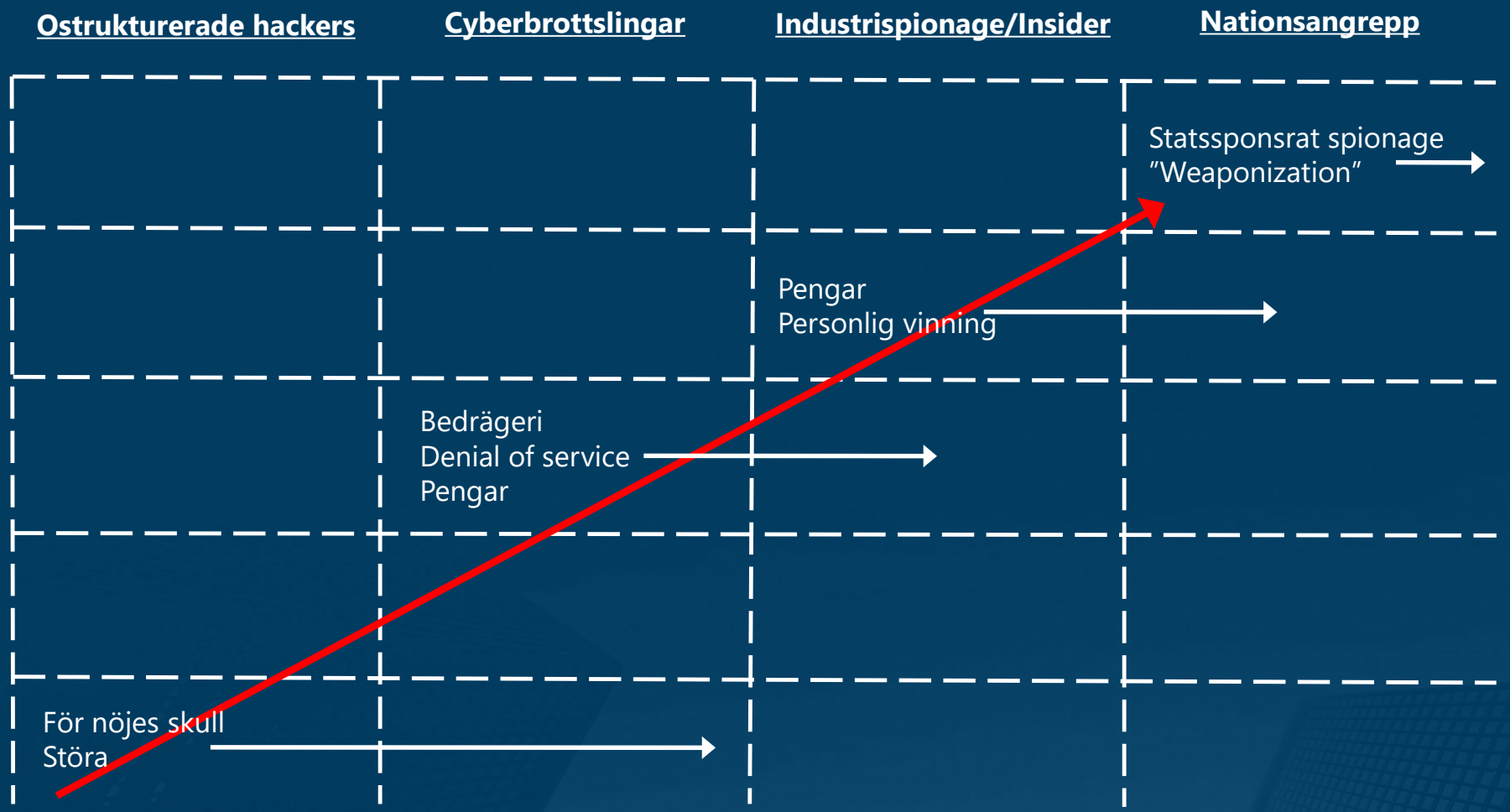
Cyberriskstyrning

Mårten Thomasson
Informationssäkerhetsrådgivare
Addlevel

Omvärldsanalys – Aktörer



Omvärldsanalys – Aktörer (förr)



Optimized
- Good practices are followed and automated
- Advanced IT security controls implemented with flexible and adaptive solutions

Managed and Measurable
- Processes are monitored and measured
- Specific IT Security Controls are protecting sensitive assets

Defined process
- Processes are documented and communicated

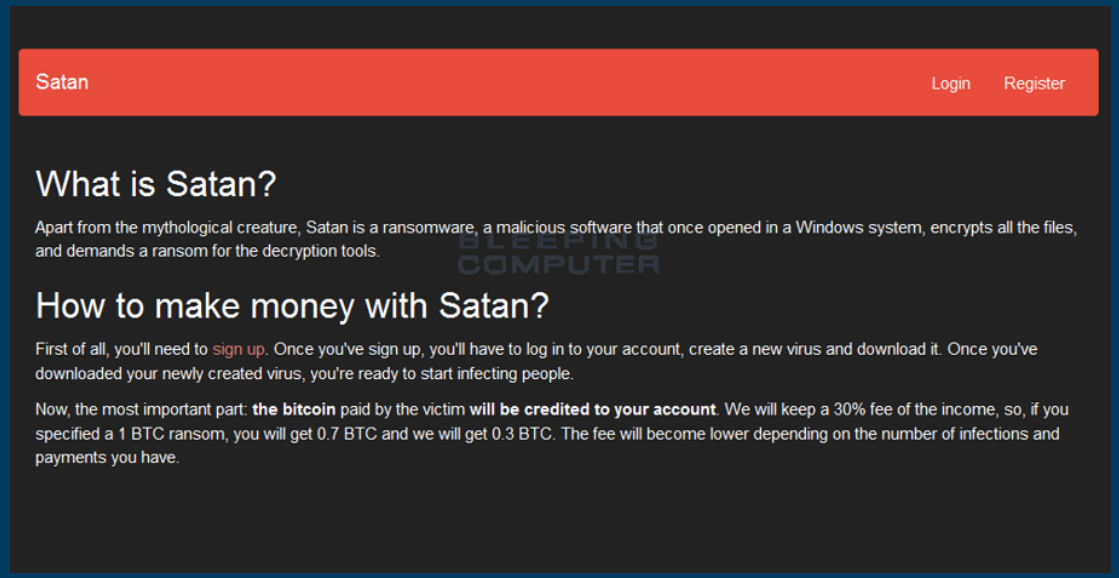
Repeatable but Intuitive
- Processes follow a regular pattern
- Common IT Security controls are defined and correlated

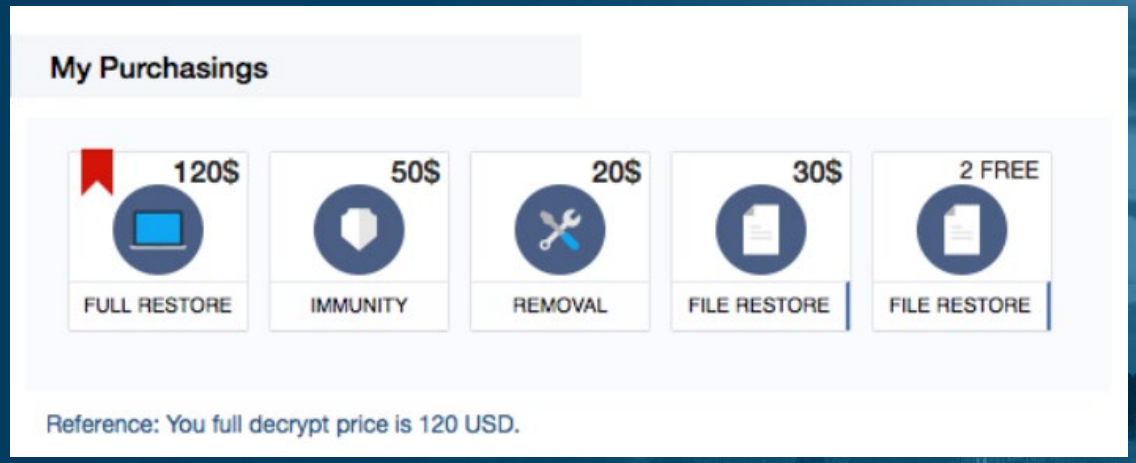
Initial/ Ad Hoc
- Processes are ad hoc and disorganized.
- Basic IT-security controls are fulfilled.

Läckage av cybervapen ändrar förutsättningarna

Hybrid kringföring

Ransomware-as-a-Service





Hur ser det ut idag? - Threat intel från Recorded Future

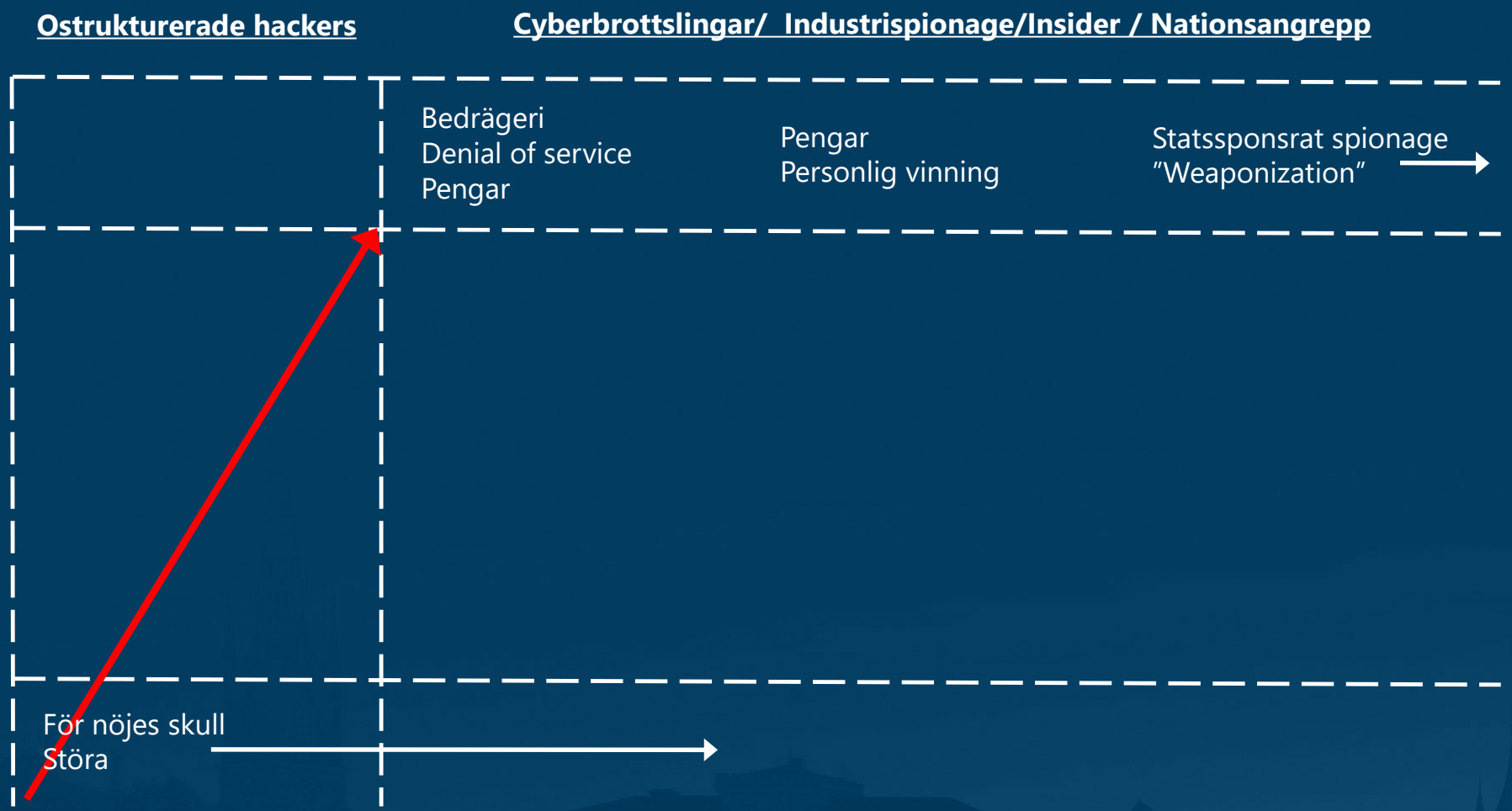
10/26/18 – gizas (Intelligence Card), a member of multiple underground forums including Club2CRD Forum, is selling access to Polish banking accounts. The actor states that for 650 euros, the buyer will receive a debit card, pin code, SIM card, internet bank login details, and an ID photo if needed. The actor states that the accounts are from such banks as ING, Millennium, and more.

https://app.recordedfuture.com/live/sc/1zHv6DX2Z533

10/27/18 – Cavalliere (Intelligence Card), a member of Exploit forum, is renting Internet traffic from compromised machines. The actor has separated the machines by country of residence, renting 25 thousand machines from the EU, another 50 thousand machines from Korea, and other traffic from USA and Canada upon request. The actor does not say how the machines were compromised.

https://app.recordedfuture.com/live/sc/XCAYM8GstFa3

Omvärldsanalys – Aktörer (nu)



Optimized
- Good practices are followed and automated
- Advanced IT security controls implemented with flexible and adaptive solutions

Initial/ Ad Hoc
- Processes are ad hoc and disorganized.
- Basic IT-security controls are fulfilled.

Vilka är era relevanta hotaktörer?

Har er organisation gjort en hotanalys för att identifiera relevanta hotaktörer:

- Cyberbrottslighet?
- Främmande makt?

Har er organisation identifierat vilka delar av verksamheten eller förvaltningsobjekt som är utsatta för dessa hotaktörer?

Kan ni svara på om dessa förvaltningsobjekt är adekvat skyddade?

Cyberrisker nu bland de störa riskerna för organisationer

- *"The biggest vulnerability for the financial system is the threat of cyberattacks"*

James Dimon, CEO JPMorgan Chase

Digitaliseringen och cyberrisk

Ökade krav på IT gällande dess hastighet, kompetens och verksamhetsförståelse

I takt med digitalisering ökar cyberhotet

Kompetenskraven på IT ökar i enorm takt

Shadow IT har blivit standard

I siffror (Sverige)

- Verksamhetsfinansierad IT har tillväxt på 4,4 procent för 2018
  - IT-budgetarna ökar i snitt 1,6 procent

- IT-beslutsfattare uppskattar att publika molntjänsters andel av deras totala IT-kostnader kommer att tiodubblas under de närmsta tre åren från 2,9 procent till mellan 27 och 32

- Radar -> Publika molntjänster på längre sikt kommer att utgöra omkring 70–80 procent av nordiska verksamheters IT-portföljer, sett till volym och effekt, och 40–50 procent av verksamheternas totala IT-kostnader

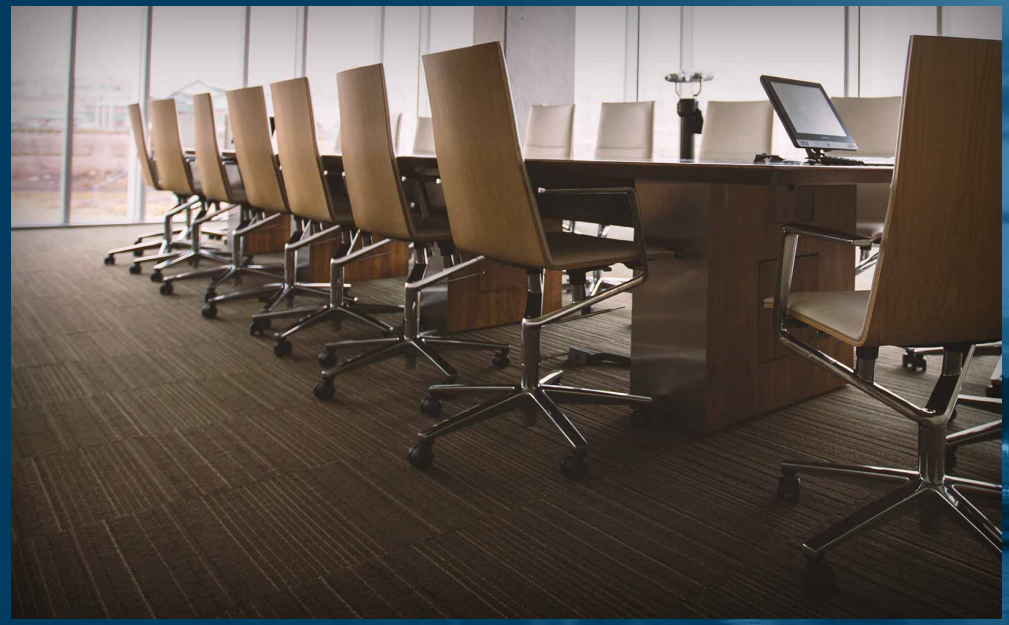
Transformation av IT-avdelningar

- IT blir en naturlig del av den vanliga verksamheten
- Kodnära
- Förstå modern IT-arkitektur och moderna lösningar
- Säkerhetsexperter (inte bara tillgänglighet)

Ökade krav på verksamhetens gällande dess förståelse för IT

Förvaltningar måste förstå och ta sitt informationssäkerhetsansvar, och kunna agera kompetenta kravställare och förstå cyberrisker

Förutsätter ett tätare samarbete mellan verksamheten och IT (IT 2.0)



Digitalisering skapar förutsättning för automatisering

Effektiviserar

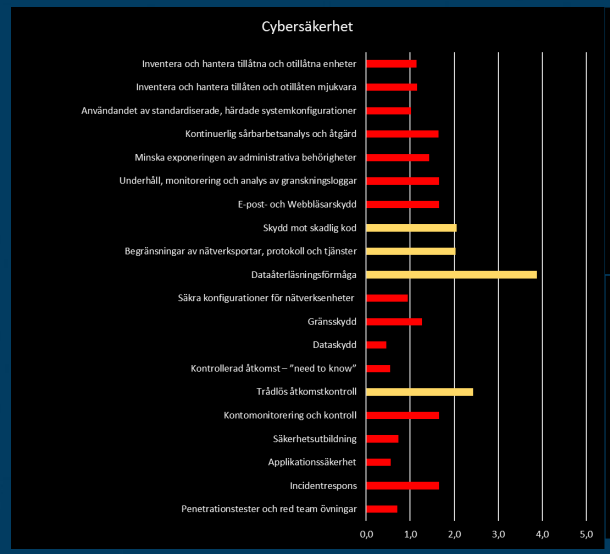
Tar bort manuella fel

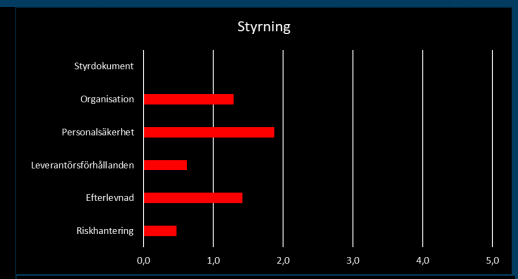
Lätt att påvisa compliance

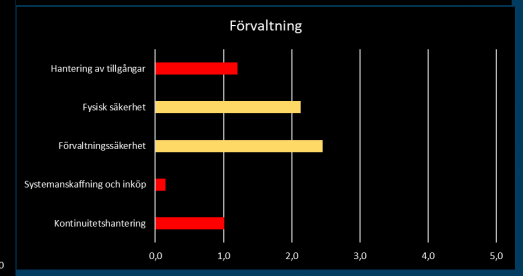
Styrning och efterlevnadskontroll

ISO 27000

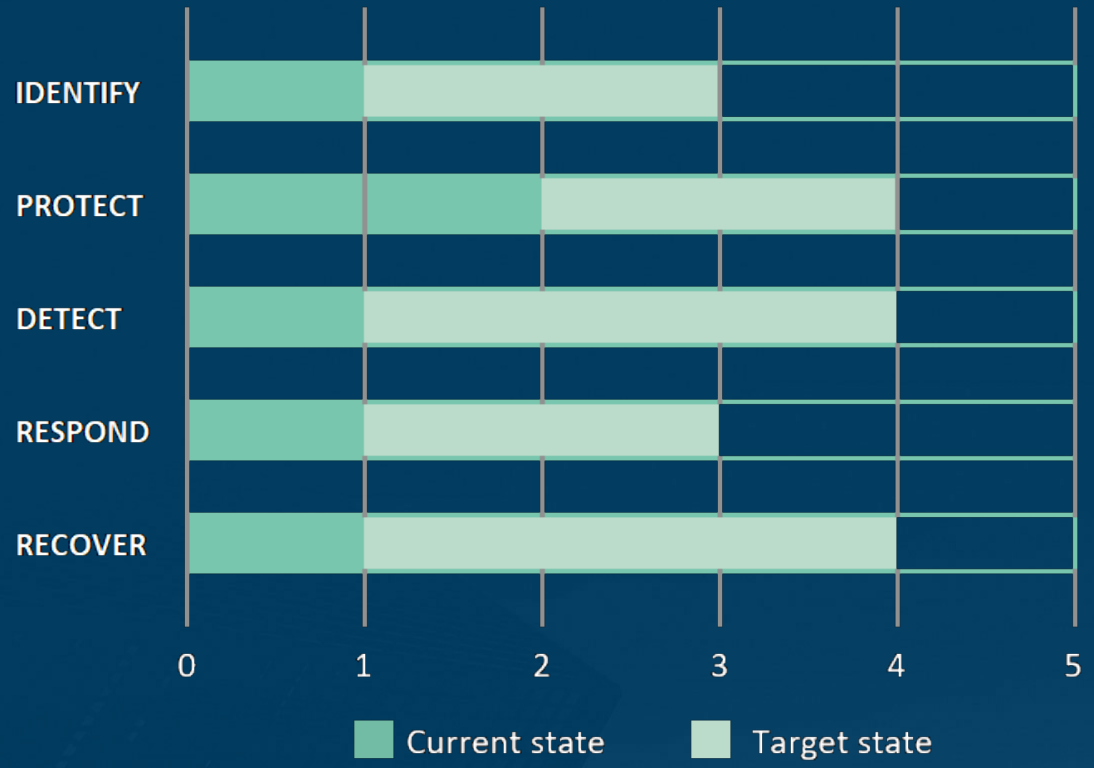
- Branschagnostisk syn på cybersäkerhet
- Vanligt förekommande krav i upphandlingar
- Riskbaserat
- Kontinuerlig bedömning av nuläget
- Certifiering ger en oberoende validering av säkerhetsarbetet







NIST Cybersecurity Framework

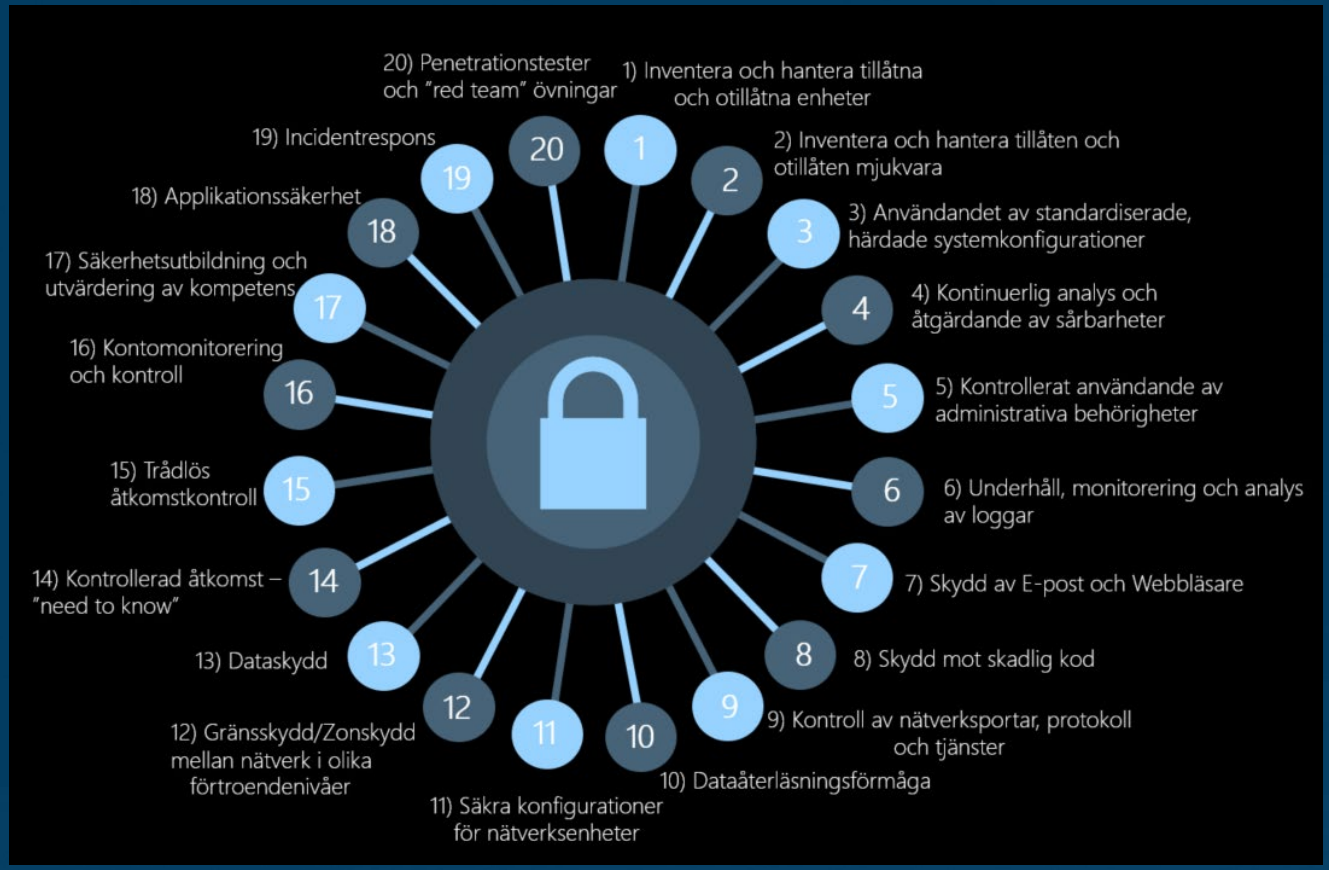


Lämpligt för att mäta förmåga

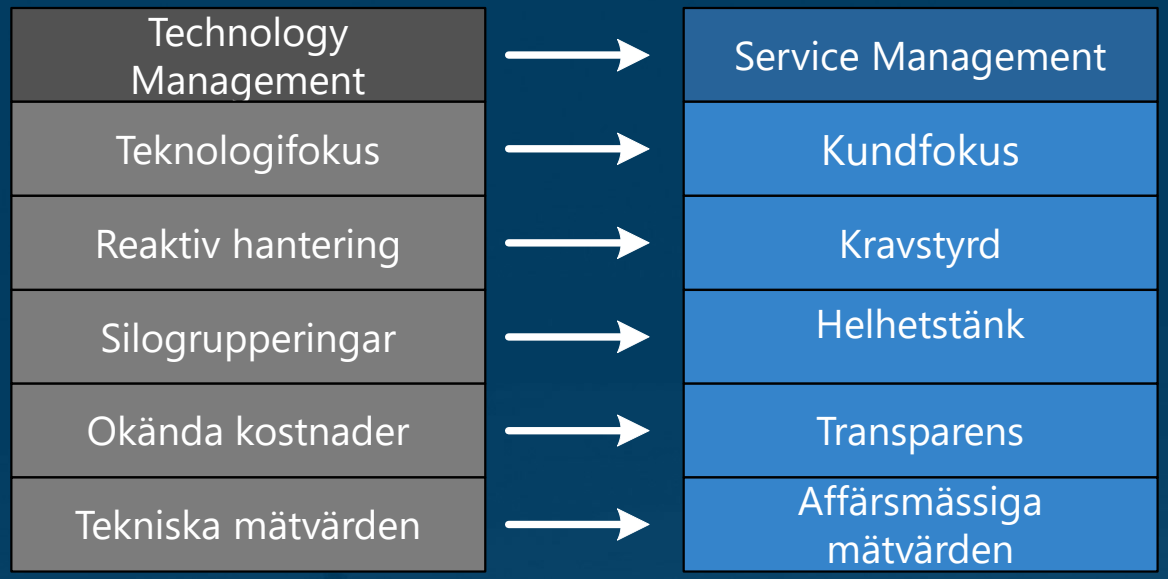
FUNCTION	CATEGORY
IDENTIFY	• Asset Management
	• Business Environment
	• Governance
	• Risk Assessment
	• Risk Management Strategy
	Supply Chain Risk Management
PROTECT	• Identity Management, Authentication, Access Control
	• Awareness and Training
	• Data Security
	• Information Protection Processes and Procedures
	• Maintenance
	Protective Technology
DETECT	• Anomalies and Events
	• Security Continuous Monitoring
	• Detection Processes
RESPOND	• Response Planning
	• Communications
	• Analysis
	• Mitigation
	• Improvements
RECOVER	• Recovery Planning
	• Improvements
	• Communications

Kritiska säkerhetskontroller (CSC 20)

- Baseras på verkliga händelser och statistik
- Väldigt konkreta
- Bra komplement till otydligare ramverk
- Mätbara
- Bygger på automation av säkerhet

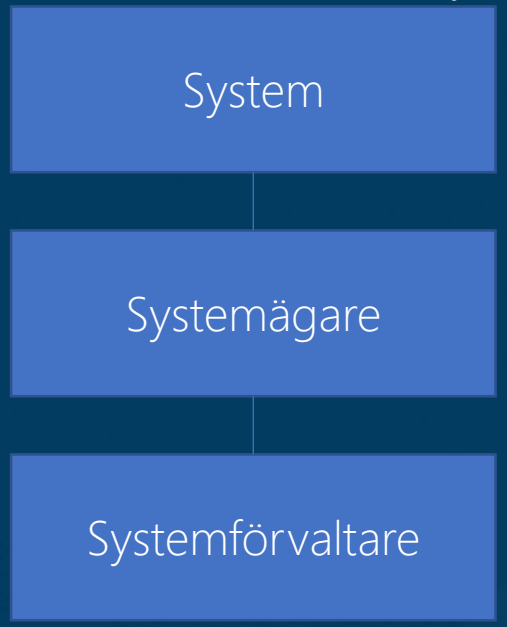


Processramverk för ITSM (t.ex. ITIL)



Förvaltningsmetodik

Traditionell modell (Teknikstyrd)



PM3 (Verksamhetsstyrd)

Hantera klyftan mellan verksamhet och IT med förvaltningsmodell (PM3)

- Syfte: Skapa ett nära samarbete, korta kommunikationsvägar
  - Styrning utifrån ett tvärfunktionellt perspektiv
  - Samverkan mellan IT-parter och verksamhetsparter
  - Skapar tydlig ansvarsfördelning
  - Strategisk, taktisk och operativ samverkan
  - Ökad verksamhetsnytta p.g.a. helhetssyn, transparens och tydlig prioritering
  - Samma befattning kan tillhöra flera förvaltningsobjekt

	Verksamhet	IT
Budget	Objektägare	Objektägare IT
Beslut	Förvaltningsledare	Förvaltningsledare IT
Operativ	Objektspecialister	Objektsspecialister IT

Inköp och Projektledning

- Checklistor och metodstöd för:
  - Säkerhetskrav & riskanalyser (glöm ej DPIA)
    - Projektstart
    - Överlämning till förvaltning
- Arkitektråd eller motsvarande funktion
  - Mandat att ”säga nej”
  - Etablerade arkitekturella principer
  - Tydlighet i förväntad input (DPIA/Riskanalys av informationssäkerhet)
- Anpassning av agila metodiker
  - Säkerhetskrav med i modellens alla faser
  - Säkerhetstestning

Informationssäkerhetskrav i upphandling

Informationssäkerhetskrav i upphandling

- Nyttjar med fördel befintliga styrdokument
- Behöver vara detaljerade – kräver organisationens commit
- Specificera i avtal hur efterlevnad skall påvisas
- Följ upp status i alla led (kravställ påvisad efterlevnad)
- Inför säkerhetssamtal

Grundkrav för Informationssäkerhet i upphandlingar

Stäm av mot styrdokument och landa grundkrav som kan bifogas upphandlingar

addlevel

Krav-nummer	Källa	Krav	Nätinfrastruktur	Inbrott - brandlarm	Active Directory	VDI	Extern Webb	Ska/Bör
1	k	Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett **ledningssystem** för informationssäkerhet (LIS) som baseras på SS-EN ISO/IEC27001:2017 eller motsvarande. **Ledningssystemet ska omfatta bland annat att samtliga säkerhetskritiska administrativa och tekniska processer är dokumenterade och vilar på en formell grund där roller, ansvar och befogenheter finns tydligt definierade.**	x	x		x		Bör
2	k	Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett ledningssystem för informationssäkerhet (LIS) som baseras på SS-EN ISO/IEC27001:2017 eller motsvarande.			x		x	Ska
4	k	Leverantören ska ha tillsett att ansvar och arbetsuppgifter som står i konflikt med varandra och kan leda till missbruk är **tekniskt eller organisatoriskt** åtskilda.	x	x		x		
6	k	Leverantören ska ha upprättat och **upprätthålla kontakter** med de myndigheter som berörs av leveransen	x	x		x		
8	k	Leverantören ska ha en policy som beskriver hur de anställda får arbeta på distans avseende drift, förvaltning och support av de levererade tjänsterna. **Leverantören ska regelbundet kontrollera att den efterlevs.**	x					
10	k	Leverantören ska ha processer och rutiner på plats **för bakgrundskontroll** av personal.	x			x		Bör
11	k	Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.		x	x		x	Ska
12	k	Leverantören ska ha avtal om tystnadsplikt med sina anställda. Tystnadsplikten ska omfatta information om leverantörens kunder. Via avtal ska leverantören även säkerställa tystnadsplikt för underleverantörer.	x		x	x		

Avtala om uppföljningspunkter – ”hur”

Det är avgörande att identifiera hur uppföljning skall ske

- Visar tydligt vad leverantören förväntas göra
- Ger bra beskrivning över kraven på den egna förvaltningen

addlevel

Krav	Efterlevnad
Leverantören ska ha en policy som beskriver hur de anställda får arbeta på distans avseende drift, förvaltning och support av de levererade tjänsterna. **Leverantören ska regelbundet kontrollera**	Leverantören ska kunna uppvisa policyn samt rutinerna för hur kontrollen av efterlevnad sker.
Leverantören ska ha avtal om tystnadsplikt med sina anställda. Tystnadsplikten ska omfatta information om leverantörens kunder. Via avtal ska leverantören även säkerställa tystnadsplikt för	Leverantören ska kunna uppvisa avtal om tystnadsplikt som signerats av dennes anställa och underleverantörer.
Behörighetssystemet ska logga information om när användare skapades, togs bort **eller förändrades samt senaste inloggning.**	Leverantör ska varje månad inkomma med rapport som visar anomalier i inloggningsförfarandet
Leverantören ska verifiera och begränsa den mjukvara som får exekveras inom den levererade tjänsten	Leverantören ska tillhandahålla listor över godkända mjukvaror.
All kommunikation till och från systemet ska vara skyddad mot obehörig åtkomst eller förvanskning. Det gäller både kommunikation mellan klient och server och mellan olika systemkomponenter. Skyddet ska uppdateras löpande utifrån kända sårbarheter.	Leverantören ska tillhandahålla uppdaterade systemkartor som tydligt beskriver hur kommunikationen skyddas
Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra system. Vid webbutveckling ska OWASP:s (www.owasp.org) rekommendationer följas.	Leverantören ska på förfrågan kunna redovisa genomförda hotmodelleringar
Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar.	Leverantören ska på förfrågan kunna uppvisa dokument som på strategisk, taktisk och operativ nivå beskriver hur man hanterar säkerhetsincidenter

Addera detaljkrav

Upphandling görs inte bra på molnfri höjd

- Motstå frestelsen att stryka krav i rädsla för att svar uteblir

addlevel

Krav-nummer	Källa	Krav
100	a	Indata bör ej innehålla sessionsinformation eller fil- eller katalognamn.
101	a	I webgränsnittet ska parameterar innehållandes känslig eller konfidentiell information ska skickas med POST till webbservern.
102	a	Leverantören ska säkerställa att sessionsstöld minimeras genom att kakor innehållande information skyddas mot obehörigt nyttjande (t.ex. använd flaggorna HTTPOnly och SECURE).
103	a	Leverantören ska tillse att behörighetsstyrning sker på serversidan.
104	a	Skydd vid uppladdning av data (såsom filer) ska finnas: - Filtrering ska ske så att endast uttryckligen tillåtna format kan laddas upp. Ska ske på serversidan: - Viruskontroll - Filstorlek och maximalt antal filer ska kunna konfigureras - Uppladdade filer ska alltid namnändras vid intern lagring.
105	a	Lagring av känslig info bör ej förekomma på klienter. Om det finns ska det redovisas och infon ska vara krypterad

Hur når man framgång i säkerhetsarbete?

Lärdomar från andra projekt och kunder

Tekniska åtgärder är primärt en fråga om budget och resurser, därav enklare att genomdriva.

Organisatoriska åtgärder brukar vara de som tar längre tid, är svårare att genomföra och kräver ett sponsorskap från ledningen.

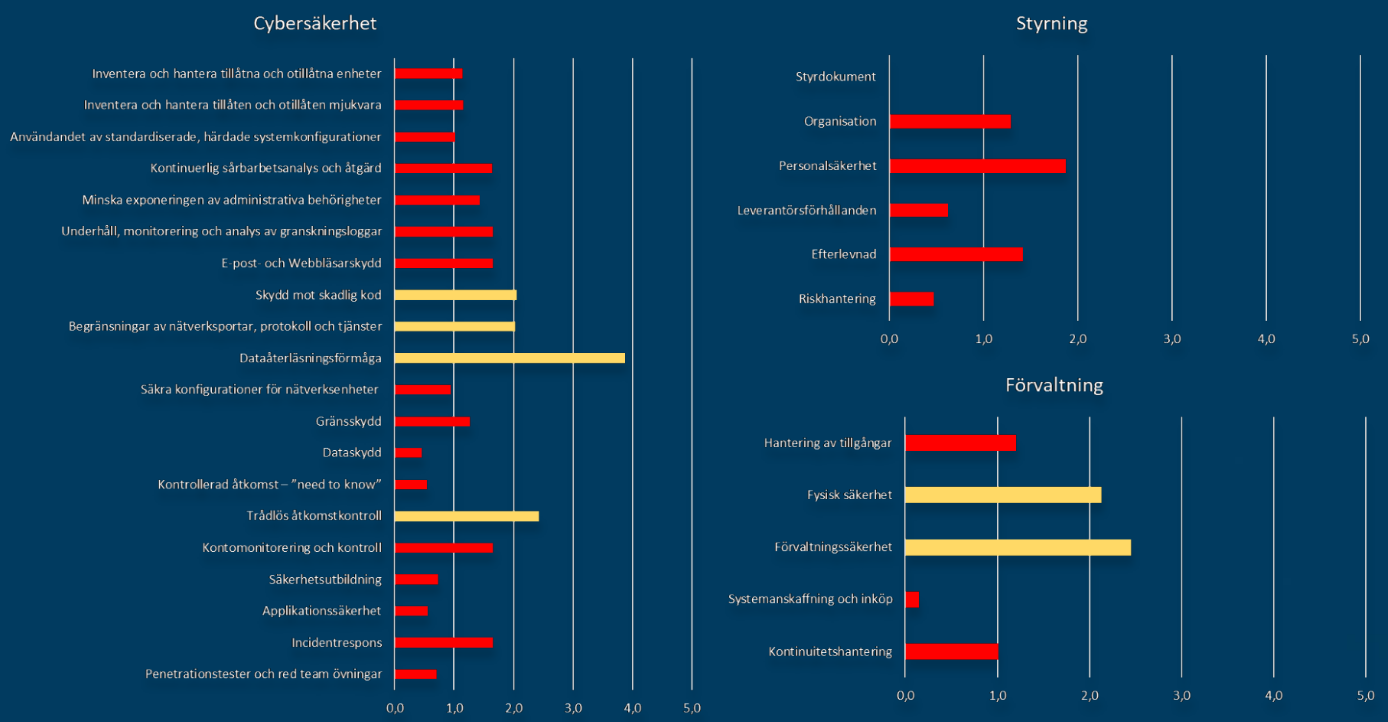
Utan de organisatoriska åtgärderna fallerar eller uteblir effekten av de tekniska åtgärderna.

Etablera förvaltningsmodell

- Enormt viktigt för dialogen inom verksamheten
- Bör inkludera informationssäkerhetsansvar för respektive roll – inkl. att riskanalyser genomförs

	Verksamhet	IT
Budget	Objektägare	Objektägare IT
Beslut	Förvaltningsledare	Förvaltningsledare IT
Operativ	Objektspecialister	Objektsspecialister IT

Mät efterlevnad av kontroller i ledningssystemet



Organisationens Informationssäkerhetsprogram

Styrning	Förvaltning	Cybersäkerhet
Policys	Hantering av tillgångar	Kritiska säkerhetskontroller
Organisation	Fysisk säkerhet	
HR Säkerhet	Förvaltningssäkerhet	
Leverantörsförhållanden	Systemanskaffning, utveckling och underhåll	
Efterlevnad	Kontinuitetshantering	
Planering och risk		

Risk

ISO 27001 & 27002 20 Kritiska Säkerhetskontroller

Externa krav (t.ex. avtal), Policy, Legala, och regulatoriska ramverk (NIS-direktivet, Säkerhetsskyddslagen, Finansinspektionens föreskrifter, EU GDPR)

Fokusera på det som är viktigt

- Skydda de mest kritiska tillgångarna
  - Åtgärda sårbarheterna för dessa ”på riktigt” – använd experter för att säkerhetsgranska
- Fokus på snabba resultat – bättre med iterativa förbättringar än långa projekt
- Bygg upp en upptäcksförmåga (och testa den!)

Arbeta aktivt med riskhantering

- Etablera en standardiserad process för riskanalys av informationssäkerhet
  - Genomför en Business Impact Analysis (BIA) av verksamhetskritiska funktioner
  - Genomför en konsekvensbedömning av samma system gällande personuppgiftsbehandling
  - Genomför riskanalyser för förvaltningsobjekt

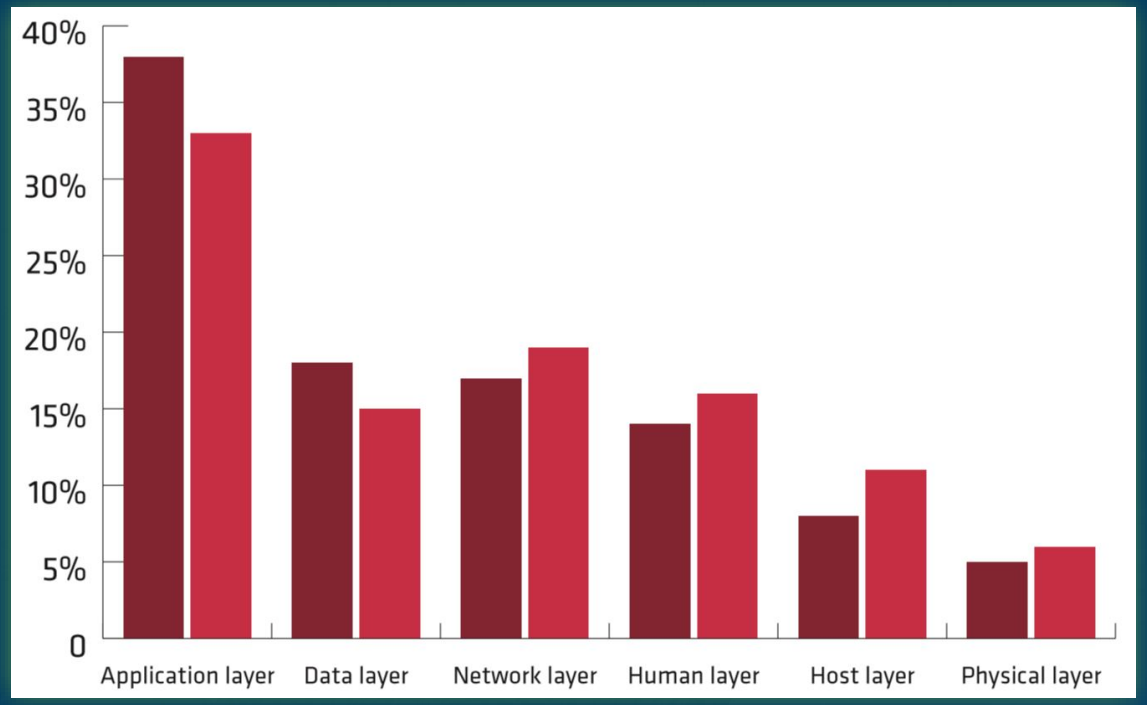
- Klassificera information och system
  - Låt användare klassificera information
  - Låt BIA klassificera system

Awarenessprogram och riktade utbildningar

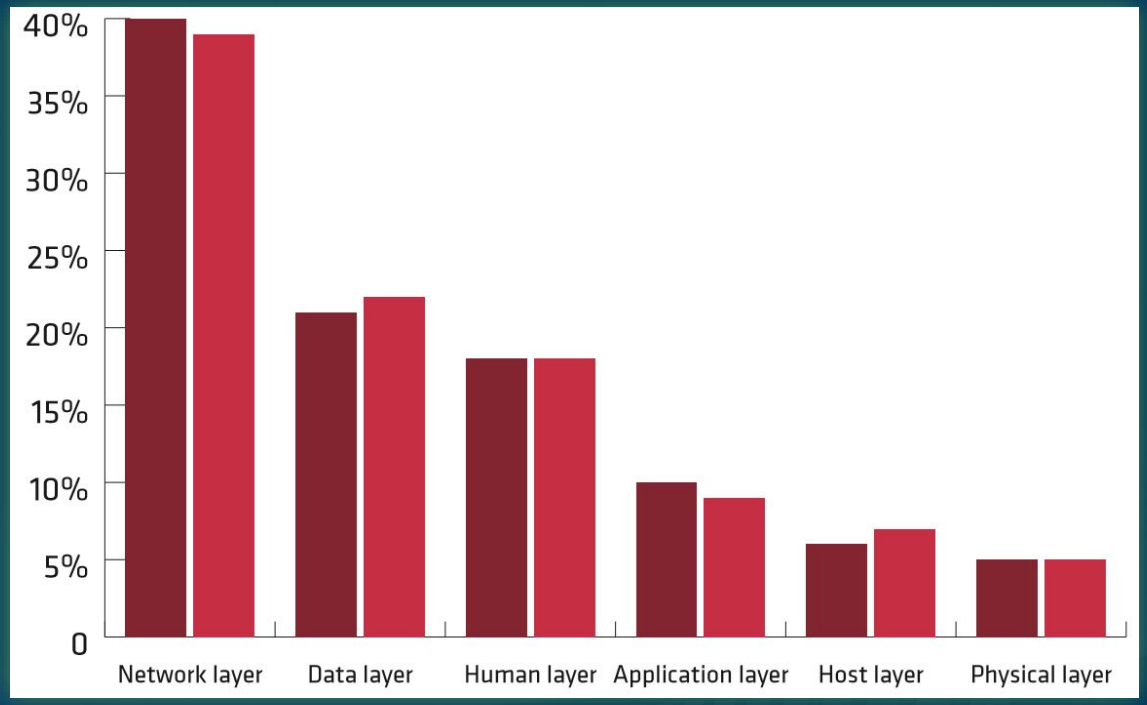
- Inför awareness program
- Riktade utbildningar för känsliga roller – ”VIP-konton”
- Riskarbete/BIA – när flera samlas i en workshop för att prata risker höjs medvetandet

Riskhantering

Många organisationer implementerar fel skydd

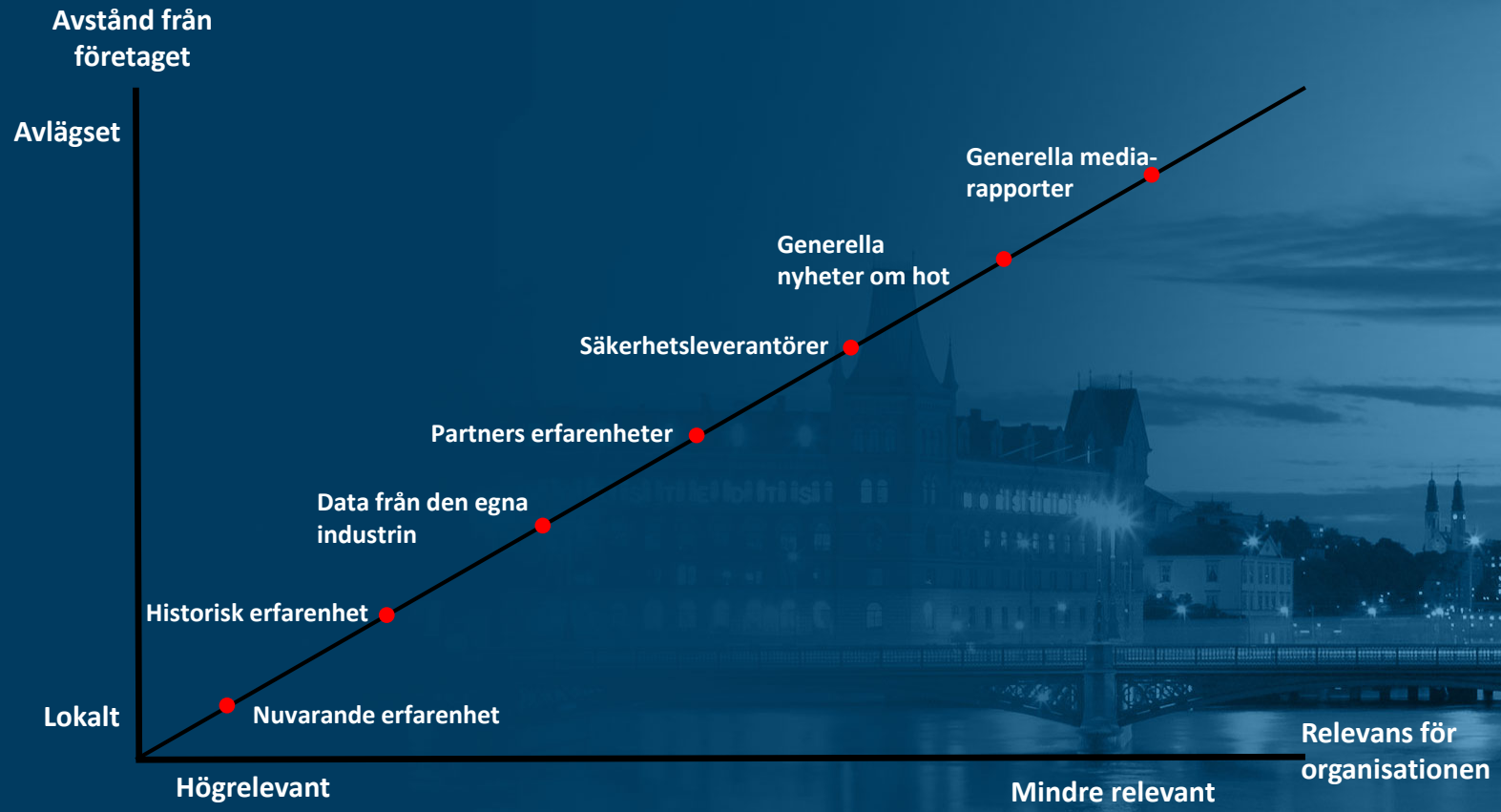


UK-företags uppfattning om vart de största riskerna finns i OSI-modellen



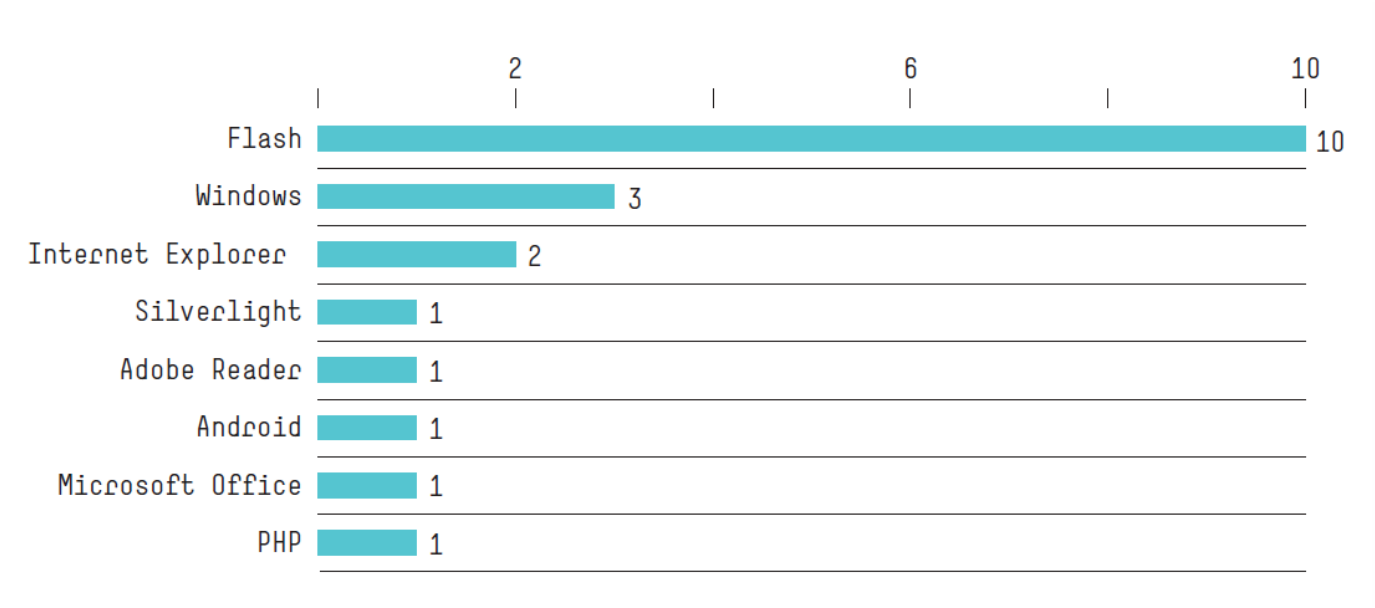
UK-företags uppfattning om vart man satsar mest i OSI-modellen

Nyckelkomponenter i datadriven säkerhet

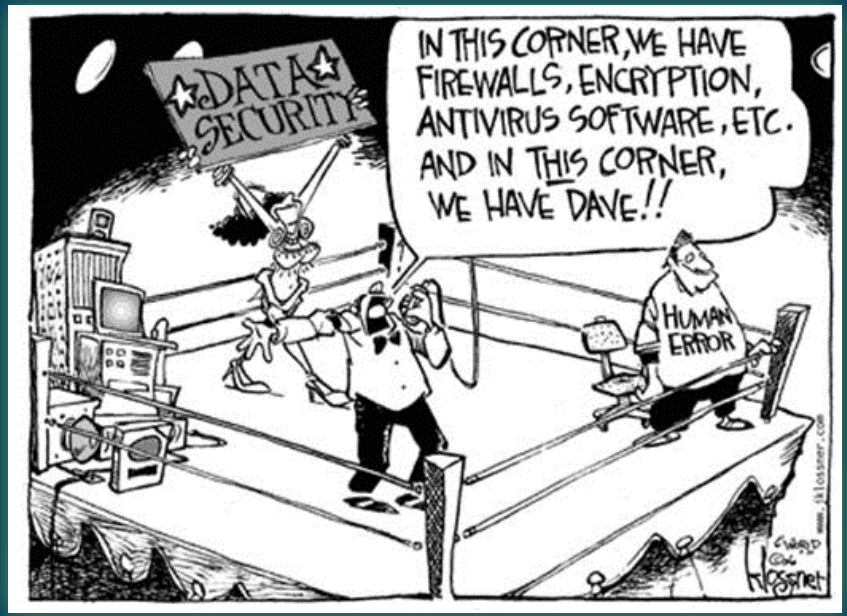


De största angreppsvektorerna

Ej uppdaterade (och hanterade) mjukvaror



Social Ingenjörskonst



Riskanalys av förvaltningsobjekt

- Riskbedömning behöver ske i flera steg – på organisationsnivå för att kunna identifiera organisationsgemensamma risker, och på objektsnivå för objektspecifika risker.

- Exempel på bolagsgemensamma risker
  - Nätverk
  - Arbetsplats
  - Kritisk infrastruktur (domänkontrollanter/Azure AD/PKI)
  - Styrdokument
  - Ansvar/förvaltningsmodeller
  - Förändringshantering

- Dessa risker ärvs till de flesta förvaltningsobjekten, som vart och ett har liten möjlighet att påverka den organisationsgemensamma risken.

Målsättning med riskanalysen

- Att kunna prioritera hot avseende sannolikhet och konsekvens genom att jämföra dem med varandra och beräkna relativa vikter.
- Måste ägas av förvaltningarna

Kan tyckas uppenbart men - de flesta organisationer idag saknar:

- mikrosegmentering, skyddade VIP-konton och SOC/log analys
- en fungerande change process och user awareness träning
- härdade arbetsstationer med säkerhetsuppdaterade applikationer

Exempel – Locker Goga

- RansomWare
- Slog ut delar av Norsk Hydro
- Kostnad – ca 450-500 Msek

Riktad attack

- Troligtvis spearphishing med macros i word
- Credential theft
- Manuell anpassning av logon skript
- Filkopiering över nätet
- Potentiellt cybersabotage