Cybersäkerhetslagen: Fem steg för att komma i gång

Secured By Telia Cygate

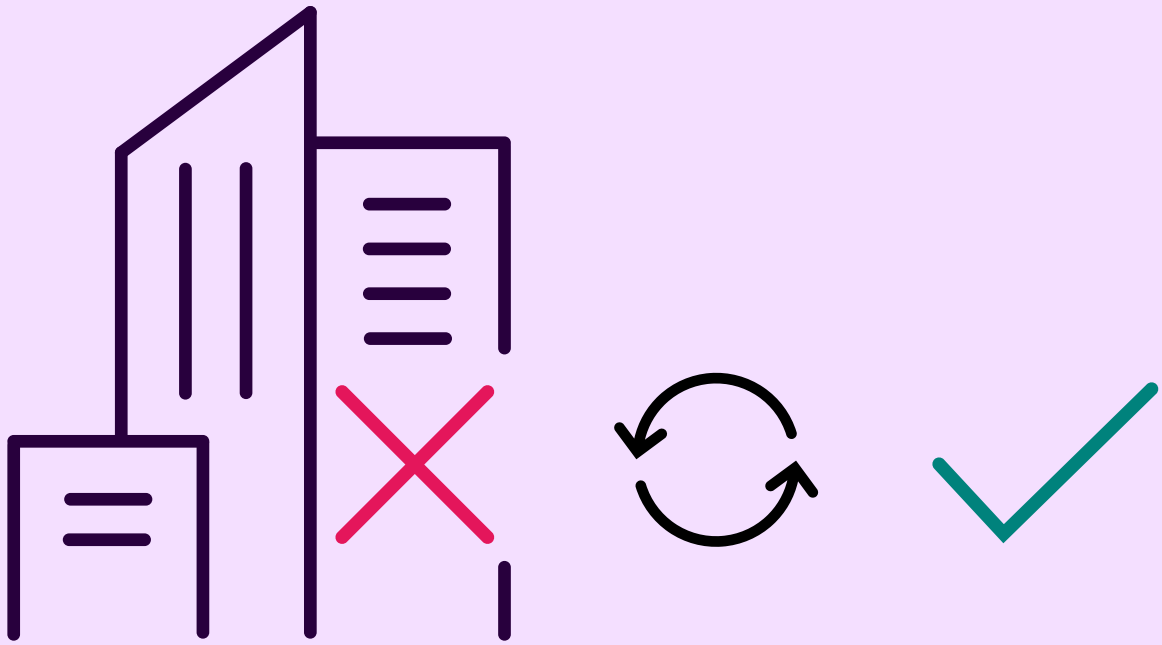
Cybersäkerhetslagen innebär nya och tydligare krav på hur organisationer ska arbeta med säkerhet. För många känns den både omfattande och svår att översätta till praktisk handling. Vad är rimligt att börja med? Vad måste vara på plats direkt, och vad kan komma senare?

Lagen kräver inte perfektion från dag ett, men den kräver riktning, struktur och förmåga att visa hur arbetet bedrivs och följs upp. Här är fem steg som hjälper er att komma i gång på ett sätt som är både hanterbart och hållbart.

1. Skapa en gemensam bild av ansvaret

Utmaning:
Ett vanligt hinder är att cybersäkerhet ses som en IT-fråga. När ansvar, mandat och ägarskap är otydliga blir arbetet fragmenterat och personberoende.

Lösning:
Börja med att tydliggöra vem som ansvarar för vad – i verksamheten, i IT och i ledningen. Det handlar inte om att flytta ansvar, utan om att synliggöra det. Vem äger riskerna? Vem fattar beslut när något händer? Och vem följer upp att åtgärder faktiskt genomförs? När ansvar blir tydligt skapas också bättre förutsättningar för dialog mellan verksamhet och IT, där säkerhet blir en gemensam angelägenhet snarare än en teknisk stödfunktion.



2. Utgå från risk, inte från checklistor

Utmaning:
Många försöker tolka lagen genom att bocka av krav eller jämföra sig med andra. Det leder ofta till fel prioriteringar och onödig komplexitet.

Lösning:
Utgå från den egna verksamheten och dess verklighet. Vilka system är mest affärskritiska? Vad händer om de ligger nere? Vilka beroenden finns – internt och externt?
När riskbilden blir tydlig blir det också lättare att prioritera rätt åtgärder och att förklara varför vissa insatser är viktigare än andra.

3. Fokusera på förmåga, inte bara dokument

Utmaning:
Policyer och riktlinjer tas fram, men används inte. De finns på papper, men hjälper inte när något faktiskt händer.

Lösning:
Säkerställ att arbetssätten fungerar i praktiken. Det handlar om enkla, kända och relevanta rutiner som människor förstår och kan följa, även när man befinner sig under stress. Testa dem, prata om dem och.

4. Bygg förmåga att upptäcka och hantera incidenter

Utmaning:
Organisationer upptäcker incidenter för sent, eller är osäkra på vem som ska agera när något inträffar. Det lever till att värdefull tid går förlorad i osäkerhet.

Lösning:
Skapa tydlighet kring hur avvikelser fångas upp, vem som bedömer allvarlighetsgrad och hur eskalering ska ske. Kunskapen om hur behöver finnas hos rätt personer, inte vara samlad hos några få. När roller, kontaktvägar och beslutsmandat är tydliga går det att agera snabbt och samordnat, även under press.

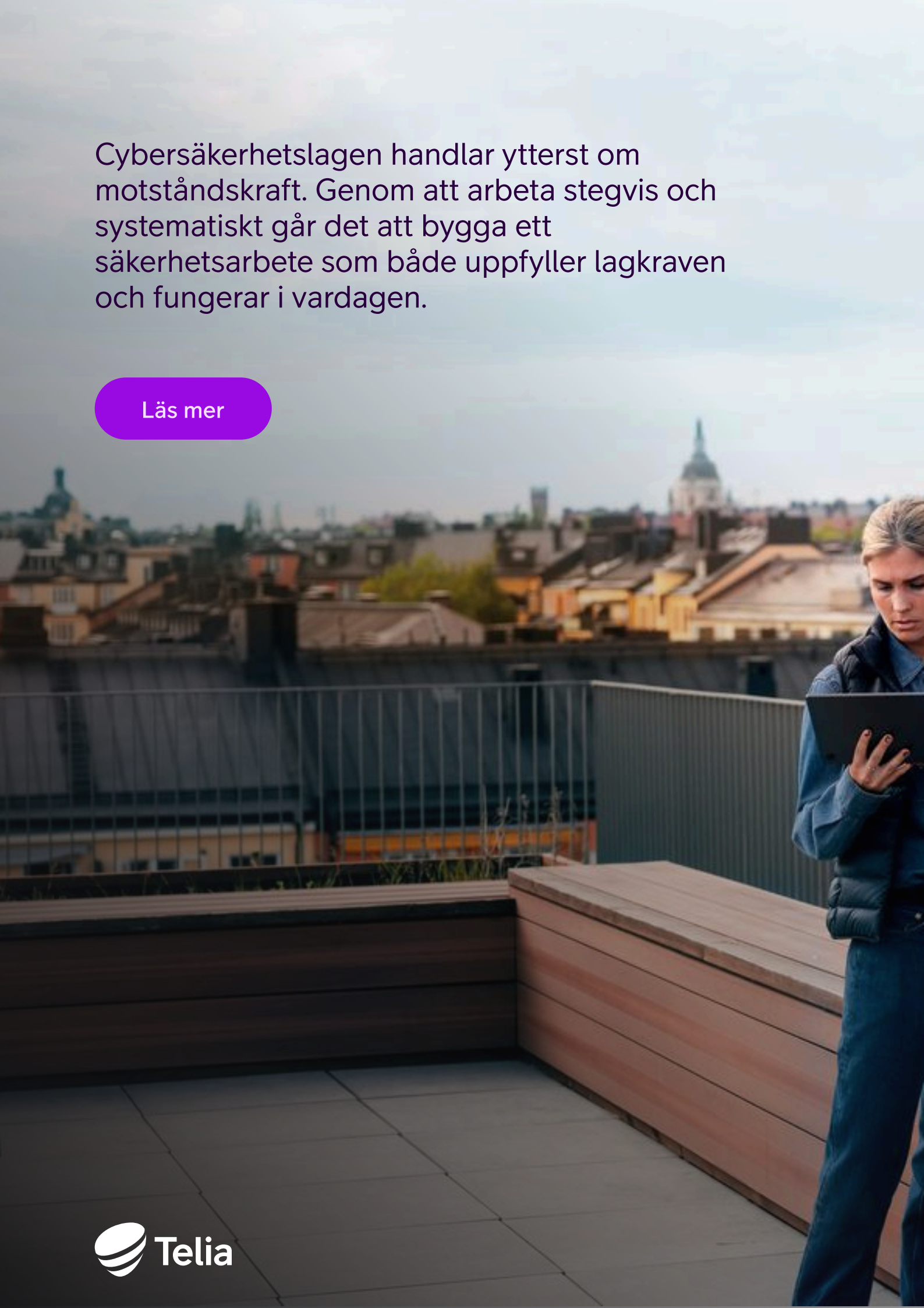
5. Börja där ni står – och bygg vidare

Utmaning:
Ambitionen att “göra allt rätt” riskerar att bli ett hinder. Arbetet skjuts upp i väntan på den perfekta lösningen.

Lösning:
Acceptera nuläget och ta nästa rimliga steg. Cybersäkerhet är ett kontinuerligt arbete, inte ett projekt med ett slutdatum. Det viktiga är att kunna visa medvetenhet, riktning och förbättring över tid.

Cybersäkerhetslagen handlar ytterst om motståndskraft. Genom att arbeta stegvis och systematiskt går det att bygga ett säkerhetsarbete som både uppfyller lagkraven och fungerar i vardagen.

Läs mer



Telia