

Säker tillsammans

Varför en sund säkerhetskultur börjar
med dina medarbetare

Vilka är kulturens byggstenar

Om det är hos er som i de flesta organisationer, att medarbetare som inte har IT som sitt specialområde utgör majoriteten av din arbetsstyrka. Då spelar det en betydande roll att forma säkerhetskulturen för att snabbt kunna anpassa sig till hemmakontor, köksbord och distansmöten.

Medarbetarnas beteende och sätt att tänka är viktig i kombination med innovation, digitalisering och teknikutveckling vilket ligger till grund för en bra arbetskultur.

Säkerhetskulturen är inte annorlunda!





Alla har ett ansvar

Vi har länge fokuserat på teknik och processer för att upprätthålla säkerheten och vi människor har ofta kommit i andra hand. Däremot, i en värld med snabb förändring och en bredare attackyta upptäcker organisationer att de måste komma på en ny säkerhetsmodell, en modell som förenar alla delar av verksamheten och som kan anpassa sig till förändrade förhållanden samtidigt som den följer övergripande regler. Detta innebär att det nu är viktigare än någonsin att säkra en organisation när det gäller människor, såväl som processer och teknologi.

Till skillnad från andra arbetsvanor är de anställda inte alltid så snabba på att anpassa sig till nya säkerhetsrutiner. De kanske inte ens är medvetna om sitt ansvar. Det är ofta en självuppfyllande profetia där anställda tror att cybersäkerhet är någon annans jobb.

På samma sätt som andra förändringar är det nu dags att bygga upp en sund säkerhetskultur. I den här guiden får du reda på vad som krävs för att vara säker, var du kan börja med din organisations cybersäkerhetskultur, och hur vi kan hjälpa dig.

Vem är ansvarig för cybersäkerheten?

45%

I en organisation tror att det flesta anställda antar att cyber säkerheten inte har något med dem själva att göra

56%

Anställda ser till sina linjechefer, snarare än ledare för cybersäkerheten, för att uppmuntra säkerhetsmedvetenheten.

54%

Av anställda tror att deras högre chefer förstår och aktivt stödjer kulturen för cybersäkerhet och initiativ för medvetenhet.

Källa: All information som citeras i denna rapport har hämtats från "Building a Cyber Smart Culture", en global undersökning som genomfördes i september 2020 av Longitude/Financial Times på uppdrag av Fujitsu.



Behovet av att stärka CISO

Precis som säkerhet inte bara är informations-säkerhetschefens (CISO) jobb, handlar cybersäkerhet inte bara om att försvara en organisation från potentiella intrång. En modern CISO bidrar till verksamheten genom att utforma en strategi för tillväxt som identifierar och begränsar potentiella risker.

Detta gör det möjligt för organisationer att inta en proaktiv hållning när det gäller cybersäkerhet och hitta sätt att förhindra att en incident inträffar från första början.

Det krävs en del för att en organisation ska bli säker. Låt oss ta en titt på några av de utmaningar som kringliggar cybersäkerhet för att se var dina medarbetare kan hjälpa till.

Nya prioriteringar

Varje dag, vecka, månad och år kommer med nya utmaningar, vissa större än andra och dessa utmaningar skapar nya ekonomiska prioriteringar för organisationer.

Nya arbetssätt, nya modeller för tillhandahållande av tjänster och nya affärsstrategier dyker upp i alla branscher. Även sättet på hur du interagerar med andra från dina leverantörer till dina konkurrenter förändras. Dessutom styrs det mesta av branschstandarder och nya bestämmelser om dataskydd och integritet.

Organisationens prioriteringar fastställs inte bara internt utan även externt. Strävan efter nya, bättre arbetssätt kräver fler prioriteringar än någonsin och en säker strategi samt en budget som gör det möjligt.



Hitta möjligheterna i förändringarna

Det som började som en kortsiktig lösning har blivit en långsiktig vision.

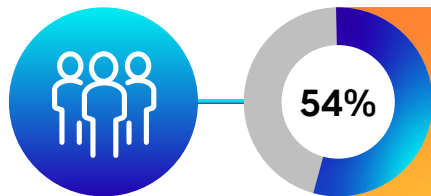
Er organisation och era medarbetare är motståndskraftiga - de kan vända förändringar till möjligheter med hjälp av ny teknik och ett öppet förhållningssätt. Men glöm inte att cyberbrottslingar har tillgång till samma nya teknik och branschkunskaper som du har. Dataintrång har blivit mycket svårare att upptäcka och cyberbrottslingar tar varje tillfälle i akt för att komma in, till exempel phishing e-post som är förklädd till viktiga uppdateringar om aktuella och angelägna ämnen.

Samtidigt har cyberbrottslighet blivit en industri med stora resurser som sträcker sig från ihärdiga individer till nationellt finansierade grupper med stora resurser. Fria från alla bestämmelser och regler är de vanligtvis snabba att omsätta tekniken och kunskaperna.

När din organisation har anpassat sig till nya sätt att arbeta, måste den också reagera på nya angreppsytor. För att, medan arbetssätten har utvecklats, har säkerhetskulturen för det mesta förblivit densamma.

Det är därför som mer än hälften (54 %) av alla företagsledare kringgått vissa säkerhetsprinciper eftersom de ansåg att det var viktigare att hålla jämna steg med förändringarna än att följa de bästa säkerhets "best practices".

När ni antar nya affärsmetoder, behöver cybersäkerhet hitta en balans mellan att skydda din organisation som en självklarhet och att driva den framåt som en konkurrensfördel.



Av företagsledarna kringgick vissa delar av säkerhetsprinciperna år 2020 och motiverar detta med att det är viktigare att följa med i förändringarna än att följa de bästa säkerhetsrutinerna.

Källa: All information som citeras i denna rapport har hämtats från "Building a Cyber Smart Culture", en global undersökning som genomfördes i september 2020 av Longitude/Financial Times på uppdrag av Fujitsu.

Främja medvetenhet

Det räcker med ett enda misstag för att hota organisationen, och det misstaget kan komma från var som helst.

Bristande medvetenhet om cybersäkerhet bland de anställda är en sak, men missförstånd kring cybersäkerhet och vem som är ansvarig för den kan också leda till passivitet om ett intrång skulle inträffa. Faktum är att, 48 % av de anställda tror att människor i deras organisation är rädda för att flagga för potentiella cybersäkerhetsproblem. Anställda tror att företagsledarna kommer att leta efter någon att skylla på när man egentligen bara letar efter någonstans att börja..

Medvetenhet om cybersäkerhet handlar om mer än årlig utbildning och kvartalsvis repetition, särskilt eftersom 45% av medarbetarna beskriver befintlig säkerhetsutbildning online som ineffektiv. En god medvetenhet om cybersäkerhet kombinerar beteendeförändring, att uppmuntra människor att tänka och agera annorlunda samt dela med sig av sin kunskap och vision om cybersäkerhet till alla i organisationen



48%

Av anställda tror att människor i deras organisation är rädda för att flagga för potentiella cybersäkerhetsproblem.

Källa: All information som citeras i denna rapport har hämtats från "Building a Cyber Smart Culture", en global undersökning som genomfördes i september 2020 av Longitude/Financial Times på uppdrag av Fujitsu.



Ni är trygga tillsammans

Många faktorer kan stå i vägen för ditt företags cybersäkerhet. Det räcker med en av dem för att bryta igenom ditt försvar. Det betyder att hela din organisation är så säker som en enda del av den, och starkast när ni arbetar tillsammans.

Att bygga upp en kultur med säkerheten i centrum kräver - människor, processer och teknik - som arbetar tillsammans för att stödja CISO och säkra organisationen.

Lösningen är att utforska kreativa och interaktiva metoder. Att uppmuntra ett säkert beteende varje dag. Säkerheten kommer att stå i centrum för en kulturell förändring, ett av flera försvar ditt företag kan använda mot digitala hot.

På Fujitsu vet vi det eftersom det är något vi själva ständigt arbetar med.

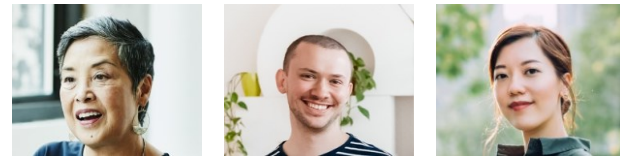


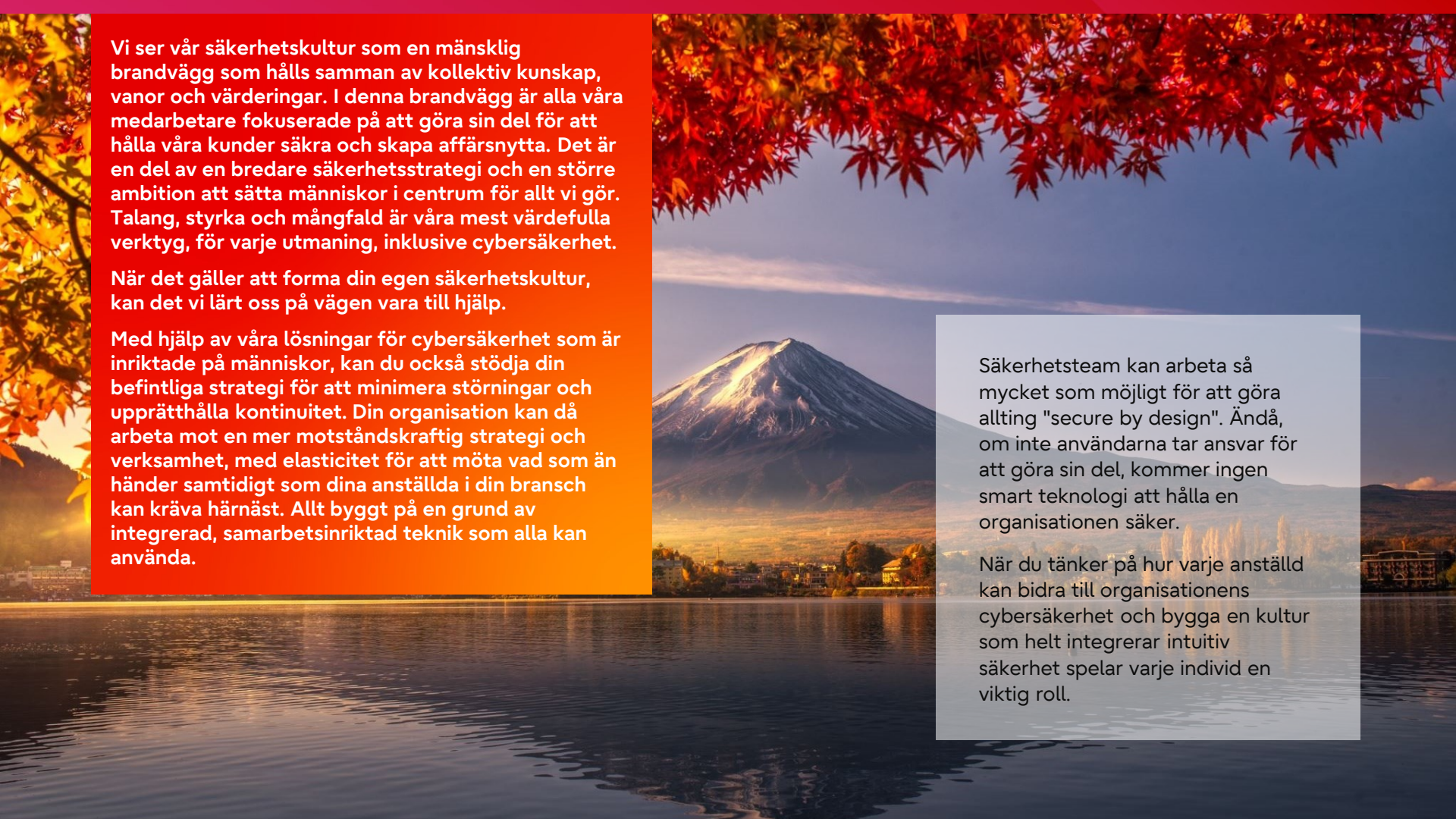
Ett sätt att säkra vår verksamhet

När du har över 4000 säkerhetsexperten i 100 länder som hjälper 1 400 kunder globalt, att arbeta tillsammans.



FUJITSU





Vi ser vår säkerhetskultur som en mänsklig brandvägg som hålls samman av kollektiv kunskap, vanor och värderingar. I denna brandvägg är alla våra medarbetare fokuserade på att göra sin del för att hålla våra kunder säkra och skapa affärsnytta. Det är en del av en bredare säkerhetsstrategi och en större ambition att sätta människor i centrum för allt vi gör. Talang, styrka och mångfald är våra mest värdefulla verktyg, för varje utmaning, inklusive cybersäkerhet.

När det gäller att forma din egen säkerhetskultur, kan det vi lärt oss på vägen vara till hjälp.

Med hjälp av våra lösningar för cybersäkerhet som är inriktade på människor, kan du också stödja din befintliga strategi för att minimera störningar och upprätthålla kontinuitet. Din organisation kan då arbeta mot en mer motståndskraftig strategi och verksamhet, med elasticitet för att möta vad som än händer samtidigt som dina anställda i din bransch kan kräva härnäst. Allt byggt på en grund av integrerad, samarbetsinriktad teknik som alla kan använda.

Säkerhetsteam kan arbeta så mycket som möjligt för att göra allting "secure by design". Ändå, om inte användarna tar ansvar för att göra sin del, kommer ingen smart teknologi att hålla en organisationen säker.

När du tänker på hur varje anställd kan bidra till organisationens cybersäkerhet och bygga en kultur som helt integrerar intuitiv säkerhet spelar varje individ en viktig roll.

Varför Fujitsu?

Vi tror att ett starkt samarbete är nyckeln till att säkra din organisation.



Vi samarbetar med dig för att driva säkerhetsstrategier som kan skapa värde under utmanande tider.



Vi agerar som en betrodd rådgivare som bygger upp säkra åtgärder som möjliggör digital omvandling.



Det går längre än att säkra din organisation

En kultur för cybersäkerhet, hjälper dig att skydda din organisation, dina anställda och kunder samt deras data.



En säkerhetskultur stöttar din strategi genom att hjälpa er göra **prioriteringar**. Genom att utföra förebyggande åtgärder, kan resurser frigöras.



En säkerhetskultur stöttar din strategi genom att hjälpa er att se möjligheter genom förändring. När alla kan identifiera och bedöma risker kan snabbare gå framåt med större självförtroende, för att undvika att utvecklingen fastnar.



En säkerhetskultur stöttar din strategi genom att uppmuntra medvetenhet. Mer öppna samtal innebär att ni kan hitta processer som alla förstår och följer. Genom att uppmuntra dina anställda att ta ansvar för cybersäkerheten innebär det även att de känner ett ägarskap för frågan.

Vart börjar vi?

Kulturen beror lika mycket på människor som på processer och teknologi. Så hur får ni med er medarbetarna på en resa mot cybersäkerhetskultur?

Ta reda på mer om den mänskliga sidan av affärsidén för en cybersäkerhetskultur i denna forskningsstudie, "Building a Cyber Smart Culture". I studien får du veta vilka utmaningar organisationer som din organisation står inför när de försöker bygga upp en stark cybersäkerhetskultur. Du får också några rekommendationer som kan hjälpa dig att förändra dina anställdas cybersäkerhetstänkande - för att bli säkra tillsammans.



Ladda ner rapporten idag!





Telefon: +46 (0)8-793 70 00
Email: info.se@fujitsu.com

FUJITSU