

Whitepaper

Sikring af elektroniske dokumenter

Hvad betyder regulativer og politikker for danske virksomheders håndtering af e-dokumenter?

Sarbanes Oxley
HIPAA
Basel II
m.fl.

Personalepolitikker

Civile retssager

Udarbejdet af
DocTech 2005

Indholdsfortegnelse

3 gode argumenter.....	3
Forretningsmæssige overvejelser	3
Argument 1: Compliance.....	4
Definition af Compliance	4
Relevante regulativer.....	4
Compliance kræver sikre e-mails	6
Retssager anlagt af myndigheder.....	8
Argument 2: Civile retssager	8
Argument 3: Personalesager.....	10
Tekniske argumenter	11
Konklusion.....	12
Kravsspecifikation til løsningen	12
Oversigt over regulativer.....	15
BS7799/ISO/IEC17799: 2000 IT Security Standard	15
The Companies Act 2004.....	15
COSO rapporten	15
Data Protection Act 1998.....	15
Financial Service Authority	16
Freedom of Information Act 2000.....	16
Health and Safety at Work Act	16
Money Laundering Regulations 2003.....	16
Privacy and Electronics Communications Regulations	17
Proceeds of Crime Act 2002.....	17
Sarbanes-Oxley	17
SEC Rule 17a-4.....	17
NASD Rule 3010 og 3110	17
Kilder.....	18
Andre kilder	18

3 gode argumenter

Ud over rent tekniske argumenter, er der tre grundlæggende argumenter for at en virksomhed seriøst bør overveje implementering af både politikker og IT-løsninger til sikker håndtering af elektroniske dokumenter - herunder e-mail dokumenter som dette whitepaper primært fokuserer på.

1. Compliance
2. Risici/muligheder i civile retssager
3. Personalesager

Compliance handler om overholdelse af eksterne love og regulativer samt interne politikker og regler udarbejdet af virksomheden selv.

Risici/muligheder i retssager mellem private virksomheder handler om, at den part som i en retssag har den bedste dokumentation til støtte for sin påstand, uanset om dokumentationen anvendes til angreb eller forsvar, har den største chance for at vinde sagen. Så her er der både en risiko og en mulighed, alt efter hvilken situation virksomheden befinder sig i. Risiko for den part der ikke har sin elektroniske dokumentation i orden og mulighed for den som har orden i sagerne og kan fremlægge relevant dokumentation samt kan dokumentere at der ikke mangler dokumenter.

Personalesager hvor der indgår e-mails som dokumentation ses oftere og oftere. Også her er der både risici og muligheder, alt efter hvem der har fordel af dokumentationen.

Dette whitepaper gennemgår alle 3 argumenter, giver dokumentation via cases, beskriver best practices og konkluderer at der findes løsninger der kan sikre virksomheden mod de beskrevne problemstillinger.

Forretningsmæssige overvejelser

Selv om de fleste virksomhedsledelser anser e-mail for at være et område, som IT-afdelingen skal tage ansvar for, bør bestyrelser og den øverste ledelse måske overveje at påtage sig noget mere af dette ansvar. Som dette whitepaper søger at dokumentere, bliver konsekvenserne af manglende politikker, sikkerhed og dokumentation, pålagt netop den øverste ledelse.

Konsekvenserne af manglende compliance pålægges primært direktører og økonomichefer. Som dette dokument viser, kan disse konsekvenser for især amerikanske

virksomheder være ganske voldsomme set med danske øjne.

Konsekvenserne af manglende dokumentation i personalesager pålægges direktører og HR-chefer og endelig vil konsekvenserne af eventuelle civile søgsmål ramme bredt i topledelsen.

Uanset årsagen til at virksomheden får brug for at fremfinde og fremlægge dokumentation i form af e-mails, vil cases som omtales vise at konsekvenserne i visse situationer kan være så tyngende, at selve virksomhedens overlevelse står på spil.

Forfatteren til nærværende whitepaper bliver oftest henvist til den IT-ansvarlige, når problemstillingerne tages op i diskussioner eller ved henvendelse til virksomheder som burde være potentielt interesserede i emnet. Dette er i princippet også udmærket, hvis blot der foreligger et mandat til IT-chefen og en strategisk målsætning på forhånd. Men det er ikke IT-chefen der skal være alene om ansvaret eller selvbestaltet bør tage beslutning om nedprioritering af andre IT-opgaver til fordel for systemer til håndtering af dette dokumentations problemstillinger. Der kan dog være rent tekniske argumenter for sådanne systemer, der kan gøre denne type af systemer interessante at opprioritere (og måske derfor mere IT-chefens ansvar), men de bliver kun overfladisk berørt i dokumentet.

Nærværende whitepaper er altså lige så relevant for virksomhedens topledelse og bestyrelse som for de IT-ansvarlige.

Infoconomy d. 8. december 2004 refererer udtalelser fra Charlie Brett, analytiker hos Meta Group (rådgivning indenfor IT management):

"Det største emne i email compliance er, at forstå hvilke regulativer som er relevante. Dette er specielt for USA, hvor regulative myn-digheder såsom SEC og juridiske forhold som HIPAA og Sarbanes-Oxley, har sat krav for hemmelighed, arkivering og overvågning af email."

"Resten af verden, inkl. EU, Canada og Japan samt adskillige andre lande er ikke langt bagefter med implementering af lignende regulativer", tilføjer han. "Dog er råt-og-brutalt / lige-ud-ad-landevejen arkivering og lagring stadig standardproceduren, specielt i miljøer med tusindvis af brugere."

"I organisationer som ikke er så hårdt regulerede, anbefaler amerikanske rådgivere at emails bliver slettet aggressivt - men det er

stik i mod hvad der typisk bliver anbefalet i Europa."

"Uanset hvad," udtaler Brett, "organisationer bliver nødt til at begynde at interessere sig for effektive metoder til at fange, lagre og søge disse emails, og at behandle alle emails som værdifuld virksomhedsinformation - selv om de er potentielt risikable."

(Kilde 19)

IT Week (UK) refererer d. 25. november 2004 til en undersøgelse foretaget af sikkerhedsspecialisten Diagonal Security:

"Firms neglect email policies"

Chefkonsulent Michael Stimson udtaler bl.a.:

*"...næsten 1 ud af 10 af de adspurgte ledere var ude af stand til at svare på om deres firma havde en e-mail politik eller ej." (...)
"Mange virksomheder har ikke indset at e-mail kan betegnes som et forretningsdokument i juridisk forstand. E-mail er vokset op med forretningen, men ses ikke som en vigtig sag for forretningen. Men samfundet ændrer sig, primært på grund af corporate governance initiativer som SOX og Basel II, som får firmaer til at rette sig op og bliver opmærksom på at gemme dokumenter."*

(Kilde 28)

Argument 1: Compliance

Dette afsnit vil give et indblik i, hvad relativt nye amerikanske regulativer, samt eksisterende og fremtidige EU-regulativer vil komme til at betyde for danske virksomheders måde at håndtere elektroniske forretningsdokumenter (specielt e-mails) på. Eller sagt på en anden og meget rammende måde – citat fra et tillæg til ComputerWorld "Hvorfor Sarbanes-Oxley også kan give dig hovedpine".

Definition af compliance

Det ville have været glædeligt, hvis det var muligt at finde et godt og enkelt danske udtryk for det engelske ord compliance. Da det danske sprog jo ikke indeholder tilnærmelsesvis så mange ord som det engelske, er det faktisk ikke muligt for hverken forfatteren eller Økonomiministeren at finde et enkelt dansk ord der dækker betydningen. Selv grundig efterforskning har ikke kunnet løse dette, så vi må nok leve med at "compliance" ender med at blive en del af dansk sprogbrug.

I stedet for selv at beskrive ordets danske betydning, vil jeg ty til at citere uddrag af Økonomiminister Bendt Bendtsens tale ved

Advokatrådets høring om Compliance fra 30. januar 2003:

"Her gik jeg og troede at Corporate Governance var mantraet, når man taler om ansvarlig virksomhedsledelse. Og straks introduceres et nyt engelsk begreb compliance."

Er det nødvendigt med alle disse fine ord? Samlet handler det om selskabsstyring, regler og normer. Eller sagt på godt dansk: ansvarlig ledelse."

Hvis vi skulle finde et dansk ord for compliance skulle nok være "efterlevelse". Eller måske bedre med lidt flere ord "en ekstra indsats for at sikre efterlevelse". Og det er der ikke noget i vejen med. Det er tværtimod et meget interessant og aktuelt emne."

(Kilde 10)

Relevante regulativer

Det regulativ vi hører mest om i pressen er det amerikanske Sarbanes-Oxleys Act (Ofte kaldet SOX, Sarbox eller SarOx - i dette dokument dog forkortet SOX). Det er da også det regulativ, som har og vil få størst indflydelse på virksomheders måde at agere på i fremtiden for sikring af compliance. For det første er SOX det første regulativ som søger at dæmme op for den type af økonomisk kriminalitet, som bl.a. Enron og Arthur Andersen skandalerne handlede om og derfor vil få stor indflydelse på hvordan EU's fremtidige lovgivning kommer til at se ud. De amerikanske myndigheder lægger jo hårdt pres på EU, for at få indført lignende lovgivning i Europa. For det andet fordi SOX allerede er blevet 'best practice' i en lang række virksomheder - også i Danmark.

Et eksempel på at SOX er blevet best practice kan ses på Danske Bank koncernens hjemmeside:

Danske Bank-koncernen er ikke omfattet af den amerikanske Sarbanes-Oxley-lov, da koncernen ikke har offentligt handlede udstedelser i USA.

Den amerikanske Sarbanes-Oxley-lov er dog med til at påvirke den globale standard for corporate governance. Derfor er loven relevant for alle virksomheder med internationale investorer.

(Kilde 23)

En række andre amerikanske regulativer samt nuværende og forventelige fremtidig EU-lovgivning er også relevante at tage i betragtning, når man skal overveje virksomhedens politikker og strategier for sikring af sin dokumentation i fremtiden. Visse regulativer dækker specielle brancher, som f.eks. finanssektoren eller sundhedssektoren, mens andre, som f.eks. SOX, være gældende generelt.

Mængden af regulativer på begge sider af Atlanten, er dog ved at være så stor, at det kan ende med at blive en ganske stor byrde - specielt indenfor udsatte brancher, såsom medico og finans - at holde styr på hvilke regulativer som virksomheden skal være i compliance med. Man kan endog risikere at regulativer er i modstrid med hinanden i visse tilfælde.

Dan Warmenhoven skriver d. 20. november 2005 i The Financial Express under overskriften "The Sarbanes Oxley Act: Causing Confusion?" bl.a.:

"3 års fødselsdagen for [SOX] er et godt tidspunkt at reflektere over lovens indflydelse på amerikansk forretningsliv. Selv om ånden i datadrevne regulativer såsom SOX blev udformet i den bedste mening, har de haft en enorm byrdefuld indflydelse på amerikanske virksomheder, idet de har påført krav som er komplekse, omkostningstunge, forvirrende og ofte modstridende.

Og SOX er ikke det eneste regulativ firmaer skal adressere. Der er separate dataregulativer udformet under [HIPAA], SEC 4, Department of Defense, Check 21 og de mange andre love og regulativer som har spredt sig som ukrudt de seneste år.

Alene mængden af dataregulativer gør fuld compliance i ethvert selskab en enorm udfordring. Ifølge en undersøgelse fra 2003, gennemført af Enterprise Storage Group, vil hele verdens mængde af compliant dokumenter have en samlet vækst på 64% fra 2003 til 2006. Indenfor naturvidenskabelige virksomheder vil denne vækst være 86% og indenfor helsebranchen 52%. (...)

Compliance er også problematisk fordi mange eksisterende regulativer konflikter med hinanden. I mange tilfælde kan samme virksomhed eller vertikale virksomhedstype stå overfor flere og konfliktende regulativer på forbundsniveau (federal), statsligt (state)

niveau og globalt niveau. Det skulle være unødvendigt at sige at dette tilføjer flere omkostninger, som i nogle tilfælde er meget svært at klare for små og mellemstore firmaer."

(Kilde 27)

Amerikanske regulativer er først og fremmest et problem for de danske virksomheder som enten selv er noteret på en amerikansk børs, eller eventuelt datterselskab af et sådant. SOX vil være direkte gældende for disse virksomheders afdelinger i Danmark. Andre amerikanske regulativer kan være gældende for datterselskaber af unoterede amerikansk registrerede virksomheder.

Amerikansk lovgivning behøver dog ikke nødvendigvis at være juridisk gældende for den danske virksomhed for at have indflydelse på, hvordan virksomheden bør agere for at undgå problemer med hensyn til virksomhedens relationer til amerikanske myndigheder og domstole. Virksomheden kan f.eks. risikere at amerikanske myndigheder kan bede om (eller måske endda kræve) dokumentation fra udenlandske partnere (datterselskaber, handelspartnere etc.) i forbindelse med undersøgelser. Om ikke andet, så kan det måske risikere at give en amerikansk partner et problem, hvis ikke en forespørgsel om dokumentation kan imødekommes fra den danske virksomhed.

Ovenstående betragtning støttes af DANSK IT, som for nyligt har oprettet et fagråd for IT-governance med medlemmer fra dansk erhvervsliv.

Uddrag fra DANSK IT's hjemmeside om et nyt fagråd under overskriften: "Har du en it-governanceplan?"

Danske anbefalinger

DANSK IT har i foråret oprettet et fagråd for it-governance, og det er fagrådets plan, at der skal udarbejdes et sæt retningslinier eller anbefalinger til, hvordan man strukturerer en it-governance-plan. Mange danske virksomheder vil som underleverandører til større udenlandske virksomheder opleve, at der bliver stillet krav til dem om at kunne dokumentere deres styring af it-processer. Dette er en udløber af de store virksomhedsskandaler som f.eks. Enron og Worldcom, hvorefter der blev udarbejdet de såkaldte Sarbanes-Oxley regler til god virksomhedsskik for børsnoterede selskaber.

-Man kan forestille sig at de udenlandske selskaber stiller krav til deres underleverandører, og så er det nemmest, hvis underleverandøren kan bevise, at de har styr på deres processer, fortalte Knud Fiil-Nielsen fra fagrådet for it-governance og partner hos revisionsfirmaet KPMG.
(Kilde 25+26)

I Europa kendes først og fremmest Basel II regulativet, som dog principielt kun er gældende for finanssektoren, men som også ofte bliver refereret til som best practice på forskellige områder. Et andet EU-regulativ, som kan være relevant at forholde sig til er "Privacy and Electronics Communications Regulations, som trådte i kraft i december 2003. Men også her er det gældende at grundlæggende elementer kan forventes at blive generelt gældende og i hvertfald best practice for virksomheder.

I England findes endvidere lokale regulativer, så som Data Protection Act og Freedom of Information Act 2000 (FOI) samt Operating and Financial Review (OFR), som er relevante at henvise til.

Compliance kræver sikrede e-mails

Selv om de fleste regulativer ikke specifikt nævner at virksomhederne skal arkivere og sikre e-mails af hensyn til fremtidig dokumentation, er der mange eksperter der anser dette som en forudsætning for compliance. Regulativerne taler typisk om forretningsdokumenter generelt og de fleste regulativer fortolker e-mails med forretningsmæssig indhold som et forretningsdokument.

På Infostor.com kan man i februar 2005 læse en omfattende artikel om emnet under overskriften: "Case Studies: How users are addressing regulatory compliance":

"SEC, NASD Investment Advisors Act, HIPAA og Sarbanes-Oxley anerkender alle specifikt e-mail som et forretningsdokument. Faktisk ligger 70% af al vigtig forretningsdokumentation i eller er tilgængelig via e-mail [via link]. Direktører kan ikke længere ignorere kravene, eller bøderne, både overfor dem selv eller overfor deres virksomhed."
(Kilde 8)

Som artiklen nævner ligger meget store dele af virksomheders forretningsdokumentation i form af e-mails. Enten som tekst i selve mailen

eller som et vedhæftet dokument. Langt de fleste virksomheder anerkender f.eks. at tilbud afgives og ordrer modtages via en e-mail. Eller at en kontrakt fremsendes som en vedhæftet fil.

Specielt amerikanske virksomheder har allerede mærket konsekvenserne af denne tolkning og i visse tilfælde har non-compliance kostet mange penge.

En artikel i ComOn fra d. 20. august 2004 under overskriften "Fortrolige e-mails havner hos forkerte modtagere", kan man læse at en refereret undersøgelse viser at:

"Det er efterhånden helt almindeligt at udveksle forretningshemmeligheder over internet (...) Ni ud af ti af de adspurgte [i en undersøgelse blandt britiske virksomheder] sender og modtager regelmæssigt mails med fortrolige dokumenter. Det er fortrinsvis ansatte i it-afdelinger (45%), som har et ubekymret forhold til at udveksle interne dokumenter på nettet, mens medarbejdere i personaleafdelinger (23%) har lidt mindre tillid til elektronisk post."
(Kilde 14)

Computerworld skriver d. 14. oktober 2005 i en artikel under overskriften "Virksomheder kæmper med gamle e-mails":

"Risikoen ved ikke at have styr på sine e-mails står højt på dagsordenen hos danske koncerner med stort engagement i USA – ikke mindst inden for medicinalindustrien og finanssektoren. Øjenåbneren for, hvor alvorlige konsekvenser rod i arkiveringen af e-mails kan få i USA, er en erstatning på 10 milliarder kroner, som investeringsbanken Morgan Stanley blev idømt for nogle måneder siden. Banken kunne ikke give sikkerhed for, at alle e-mails med relevans for en bedragerisag var præsenteret for retten, og så faldt hammeren. Men der har været andre alvorlige sager om mangelfuld arkivering af e-mails, herunder i Norge og Sverige. - Sagerne medvirker til, at salget af systemer til e-mailarkivering stiger drastisk, også herhjemme, siger Carla Arend, senioranalytiker med ansvar for infrastruktur og storage hos analysehuset IDC. Hun tilføjer, at investeringerne især skyldes internationale reguleringer, såsom Sarbanes-Oxley og Basel II."
(Kilde 29)

I samme nummer af Computerworld findes yderligere en artikel under overskriften "E-mails med vedhæftede filer koster dyrt":

"Den konstante stigning i antallet af e-mails giver ikke alene de store koncerner grå hår i hovedet. Visse af dem stilles godt nok over for regulatoriske krav om, at e-mails skal arkiveres i syv år, men selv i små virksomheder, giver væksten ondt i pengepungen."

(...)

"Banker og andre i finanssektoren skal ifølge den såkaldte Basel II regulering, gemme e-mails i syv år. I forvejen kræver det amerikanske børstilsyn, at alle banker og børsrådgivere gemmer e-mails og øjeblikksbeskeder (instant messaging) i tre år. Fra juli 2006 gælder det alle virksomheder, der er børsnoterede i USA. Her er det Sarbanes-Oxley-loven, der kom til på grund af Enron-skandalen, der slår igennem."

(...)

"I Danmark findes der endnu ikke eksempler på, at manglende e-mails har udgjort et problem, oplyser advokat Peter Lind Nielsen fra Bender von Haller Dragsted. - Men vi frygter selvfølgelig de sager, der vil komme, og hvor man skal kunne dokumentere, at mailsystemerne og arkiveringssystemerne er pålidelige nok, siger advokaten."

(Kilde 30)

At der ikke kun er tale om nødvendigheder for virksomheder med amerikanske relationer, bevidner også Dansk Standard ved at udbyde kurser og certificeringer i emnet records management.

Fra Dansk Standards hjemmeside:

"Få styr på dine dokumenter og records med ISO15489":

Records management og arkivering er blevet varme emner i enhver organisation og fokus og ressourcer til disse områder er ved at flytte fra de mørke kældre til direktionsgangene! Det at kunne dokumentere og bevise alle aktioner og processer er blevet strategisk vigtigt i alle private og offentlige organisationer.

Tendensen er klar i USA og mange andre lande og skyldes øget regulering fra myndighederne og indførsel af nye lovgivninger som f.eks. Sarbanes Oxley og FDA CFR 21 Part 11 i USA. I EU barsler

kommisionen med det 8. direktiv, der stiller vidtgående krav til dokumentation for virksomheder og i Danmark er den offentlige sektor i gang med strukturændringer og et omfattende digitaliseringsprojekt. Hvor det tidligere var kvalitetssikringssystemet i en organisation, der stillede dokumentationskrav er alle forretningsprocesser og medier nu omfattet.

(...)

At kunne sikre og genfinde records og dokumentation er vigtigt for enhver organisation i lyset af strammere lovgivning, digitalisering, myndighedskrav, standardisering, risikovurderinger og endelig har mange en forventning om at alt let kan genfindes til enhver tid. Et velfungerende records management system er et spørgsmål om organisationen kan forsvare sig og forklare sig under retssager, ved klager, pressen eller omverden stiller spørgsmål. På længere sigt kan det være et spørgsmål om overlevelse.

Der er masser af hjælp at hente for alle der står overfor udvikling og implementering af nye strategier, systemer politikker eller vurdering af de eksisterende i en international standard "ISO 15489 Information and documentation – Records management". Standarden er implementeret eller på vej i mange danske virksomheder og organisationer og beskriver best practice indenfor områderne records, document og information management."

(Kilde 7)

Compliance i henhold til flere af regulativerne (specielt SOX) er dog allerede generelt blevet best practice for mange virksomheder, og det faktum at SOX skulle gå hen og blive best practice – også i Europa – støttes af Advokatrådet i Danmark.

På portalen for advokatbranchen, Advokatnet, kan læses:

"Det er Advokatrådets opfattelse, at den eksterritoriale virkning af Sarbanes-Oxley Act fra 2002 er så væsentlig, at reglerne i praksis i Europa må anses for "best practice" – også for virksomheder, der er børsnoterede uden for USA. Udviklingen med at implementere bl.a. habilitetsreglerne fra Sarbanes-Oxley Act har endvidere bredt sig til ikke noterede selskaber i Europa. Overholdelse af regler, som tilsvarende Sarbanes-Oxley, må derfor i dag anses for best practice også uden for USA."

(Kilde 12)

Retssager anlagt af myndigheder

Der er masser af eksempler på konsekvenserne af manglende compliance relaterede til e-mails. Men alle de eksempler, som har kunnet findes, handler alle om problemer med at virksomheder ikke har kunnet fremlægge dokumenterne - ingen sager af denne type handler om selve *indholdet* i mailen (måske bortset fra en enkelt, som er et grænsetilfælde).

De fleste sager drejer sig om, at virksomheden ikke er i stand til at finde de *relevante* mails. Hvis virksomheden udelukkende arkiverer deres mails på backup-bånd, vil disse ligge sekventielt uden mulighed for at de relevante kan identificeres indenfor rimelig tid. Dommere stiller krav om at dokumentationen skal fremlægges indenfor *rimelig tid* og det kan simpelthen ikke lade sig gøre i praksis, hvis alle relevante dokumenter skal fremsøges manuelt og der skal være rimelig sikkerhed for at der ikke mangler nogle.

Andre sager handler om at virksomheden må "gå til bekendelse" og fortælle dommeren at de krævede e-mails er blevet slettet ved en fejl, eller fordi virksomheden konsekvent sletter mails der er mere end x dage gamle.

Dommene er dog uanset "undskyldning" ofte meget hårde og bødekravet i en størrelsesorden der virkelig gør ondt.

En civilretssag mod Morgan Stanley, som omtales i kapitlet om civile retssager, viser også at man kan risikere en undersøgelse og retssag fra myndighedernes side, hvis man i en civil retssag ikke har kunnet fremlægge dokumentation. I sagen mod Morgan Stanley gik SEC efterfølgende ind og har truet med en bøde på 10 mio. dollars, fordi den civile retssag viste at Morgan Stanley ikke var i compliance med regulativer for finansvirksomheder. Det blev så senere nedsat til 2,1 mio. dollars.

I februar 2005 pålagde SEC bøder på i alt 2,1 millioner dollars mod J.P. Morgan Securities (værdipapirhandler) for ikke at være i stand til at levere alle e-mails som blev påkrævet under en efterforskning. Firmaet undskyldte sig med forsvundne og ødelagte backup bånd.
(Kilde 4)

I marts 2005 betalte Banc of America Securities en bøde på 10 millioner dollars for at bilægge en sag anlagt af SEC for ikke at kunne levere e-mail dokumentation der var anset for vigtige i en undersøgelse.
(Kilde 4)

D. 19. oktober 1999 beordrede Columbia distriktsdomstol Philip Morris Inc., til at sikre alle dokumenter som indeholdt information som kunne være relevante i en sag mellem staten og selskabet. På trods af denne ordre, fortsatte Philip Morris med at slette e-mails som var over 60 dage gamle [i henhold til intern politik] i en periode på mindst to år efter ordren fra domstolen. På trods af at Philip Morris selv opdagede problemet i februar 2002, blev domstolen først informeret i juni 2002.

Domstolen krævede Philip Morris idømt en bøde på 2,75 mio. dollars.

(Kilde 2)

Argument 2: Civile retssager

I retssager mellem to virksomheder kan der indgå e-mail dokumentation som bevis. I Danmark er der i princippet ingen problemer i at fremlægge beviser i form af e-mails, men det har ikke været muligt at finde sager, hvor dette er sket.

I USA har der været adskillige sager, hvor sagsøgte er blevet afkrævet at fremlægge e-mail dokumentation og endog i store mængder. I mange af disse sager er det dog blevet pålagt sagsøgeren at betale omkostningerne for at fremfinde de relevante dokumenter fra sagsøgtens harddiske, backup-bånd etc. Dette kan selvfølgelig afskrække en del fra at bede om dette, idet det kan blive en ret så bekostelige affære, hvis sagsøgte virksomhed ikke har et e-mail arkiveringssystem, hvor der kan søges på emne, periode eller andet relevant.

De sager hvor dommeren kræver af sagsøgte at fremfinde dokumentationen, kan det ofte ikke lade sig gøre. Undskyldningerne er typisk at de relevante mails er blevet slettet p.g.a. virksomhedens mailpolitik eller ved en fejl.

Men netop manglende evne til at fremlægge dokumentation, bliver ofte vurderet som suspekt af dommeren og kommer til at koste sagsøgte en anselig erstatning.

Mange sager bliver afgjort ved forlig uden for dommerens indflydelse, hvilket måske kan spare sagsøgte nogle penge. Men det er ofte lige så vigtigt for sagsøgte at få stoppet mediernes dårlige omtale, samt at spare omkostningerne til fremfindning af dokumentation.

Eksempler:

En civilretssag anlagt af Burst.com mod Microsoft i juni 2002, hvor Burst anklagede Microsoft for at stjæle firmaets video-streaming teknologi, er refereret i Infoconomy d. 8. december 2004. Under den første høring i sagen, pointerede Burst's advokater at der var noget besynderligt ved Microsofts e-mail-dokumentation, som var blevet fremlagt. Der manglede e-mails fra den 35 uge lange periode, hvor de to firmaer var i diskussioner. Forelagt problemstillingen med de manglende e-mails, forklarede Microsofts advokater at de var blevet slettet. Uheldigvis kunne Burst's advokater huske et vidnesbyrd fra en retssag mellem Sun Microsystems og Microsoft, hvor repræsentanter for Microsoft havde udtalt at der blev taget backup to gange af alle interne mails - een intern og een eksternt fra hovedkontoret. Dommeren i Burstsagen beordrede Microsoft til at producere de manglende e-mails, men et år senere virker det som om Microsoft stadig arbejder på at genskabe disse e-mails.

(Kilde 19)

Det tog åbenbart lang tid at producere disse e-mails, da der først dukker nyheder op i sagen d. 3. november 2005, hvor IT-World kan fortælle at de to virksomheder har indgået forlig og Microsoft har betalt 60 mill. dollars til Burst. (Kilde 21)

Computerworld skriver d. 14. november 2005 under overskriften: "Softwarefejl og sjusk hos Morgan Stanley":

"Milliardæren Ronald Perelman, bestyrelsesformand for kosmetikfirmaet Revlon, blev 1,57 milliarder dollars rigere - næsten 10 mia. kroner - for nogle måneder siden. Gevinsten skyldtes, at investeringsbanken Morgan Stanley ikke havde styr på sine e-mails.

Perelman sagsøgte investeringsbanken i 2003. Anledningen var hans salg af et af sine selskaber for 1,5 mia. dollars i slutningen af 90'erne. Køberne betalte knapt halvdelen med egne aktier, men gik konkurs kort efter, og konkursen afslørede regnskabsfusk i sværvægtsklassen. Morgan Stanley måtte, som køberens investeringsbank, have kendt til problemerne, men sagde intet, lød Perelmans anklage.

Morgan Stanley blev af domstolen i Florida afkrævet flere års e-mailkorres-

pondance fra de i alt 36 ansatte, der havde været involveret i sagen. Ordren blev efterkommet i juni 2004, men forinden var yderligere 1.423 backup bånd fundet i et skab på et Brooklyn-kontor, og de var ikke blevet tjekket for de e-mails. Senere blev der fundet flere bånd hist og pist, og ingen kunne være sikker på, at alle bånd var fundet.

Til sidst mistede dommer Elizabeth Mass tålmodigheden og krævede omvendt bevisbyrde. *Juryen blev anmodet om at gå ud fra, at Morgan Stanley havde bistået i bedrageriet mod Perelman, der dog også skulle bevise størrelsen på sit tab. Men Morgan Stanley evnede ikke at overbevise juryen om sin uskyld netop på grund af usikkerheden om e-maildokumentationen.*

Fra investeringsbankens it-ansvarlige lød forskellige forklaringer på problemet.

- *Der manglede skriftlig instruktion i, hvorledes søgning skulle ske i et nøglesystem.*
- ** En softwarefejl bevirkede, at store og små bogstaver ikke blev ligestillet i søgning.*
- *En tidligere it-chef havde været for nærig med diskpladsen.*
- *Softwarefejl hindrede, at der kunne søges i bilag til e-mails og i 7.000 e-mails sendt via et særligt e-mailprogram.*

Desuden havde ingen givet høj prioritet til opgaven med at få det gamle tapeindhold over i databasen før retssagen var lige op over.

(...)

Om Morgan Stanley risikerer endnu en bøde. Det amerikanske børstilsyn, SEC, overvejer at idømme investeringsbanken en bøde på 10 millioner dollars, netop fordi den ikke har beholdt e-mails, som kunne være relevant for sagerne.

(Kilde 31)

Beskrivelsen af Dansk Standards certificering nævner "Et velfungerende records management system er et spørgsmål om organisationen kan forsvare sig og forklare sig under retssager...".

Det er ikke nødvendigvis kun retssager anlagt af en myndighed mod en virksomhed, hvor der kan være brug for at kunne fremlægge sikker dokumentation i form af e-mails. Der skal ikke megen fantasi til at forestille sig, at hvis en sagsøger i et civilt søgsmål er i stand til at fremlægge dokumentation i form af e-mails til støtte for sin sag og modstanderen ikke kan gøre det samme, så har man en meget bedre sag. Det omvendte er selvfølgelig gældende hvis man bliver sagsøgt af en anden virksomhed, men er i

stand til at afvise sagen ved at kunne fremlægge støttende dokumentation i form af e-mails.

Da de fleste civile retssager mellem 2 virksomheder jo foregår bag lukkede døre i f.eks. sø- og handelsretten, er det sjældent man hører detaljer om hvilken form for dokumentation der er fremlagt, så her er det vanskeligt at finde relevante cases.

Michael Osterman, direktør i Osterman Research, udtaler d. 27. september 2004 i Storage Networking Online:

"implementering af et mailarkiveringssystem er billigere for de fleste virksomheder end omkostningerne til bare én sag, hvor e-mails skal genfindes [manuelt]."

(Kilde 3)

Sarbanes-Oxley Compliance Journal skriver d. 6. juli 2005:

"Forsømmelse med håndtering af e-mail kan ende i en dyr straf for virksomhedsledere. Sidste år blev tidligere CSFB [Credit Suisse First Boston] bankansatte Frank Quattrone idømt 18 måneders fængsel for at have sendt en enkelt e-mail som opfordrede personalet til at "rydde op" i deres e-mail filer."

(Kilde 9)

Computer Business Review skrev allerede i september 2003:

"Datalagres retsstilling ændrer sig. Indtil videre er det kun få virksomheder som gør nok for at sikre dem selv eller deres ansatte mod at ende foran en jury."

Dette kan lyde lidt overdramatisk, men to sager fra Wall Street i juli 2003 illustrerer det stigende pres på amerikanske virksomheder for at gøre deres elektroniske dokumenter lette at genfinde, og det ser ud som om Europa vil blive tvunget til at gøre det samme.

I den første sag, blev investeringsbanken UBS Warburg beordret til at genskabe e-mails i en retssag. Omkostningerne til dette løb op i et seks cifret beløb i dollars.

I den anden sag afkrævede tre regulativmyndigheder e-mails og andre data fremfundet i forbindelse med en sag som involverede 50 ledere i 12 banker.

(Kilde 6)

I samme artikel interviewes Jon Fell, som er partner i advokatfirmaet Mason.

Jon Fell udtaler at de samme principper er begyndt at blive anvendt i engelske retssale og andre steder i Europa - dog i mindre målestok.

En del aktuelle sager har involveret e-mail og advokater er begyndt at forstå ideen med at bede om e-mail dokumentation, når det er relevant. E-mail er accepteret som berettiget bevis, og virksomheder risikerer at opdage at de har enorme mængder af e-mail korrespondance at skulle igennem. Der er også spørgsmålet om integriteten af e-mail dokumentet - har virksomheden nogen form for revisionsspor, som kan sikre at en e-mail som bliver fremlagt i retten, rent faktisk var sendt og til hvem?

(Kilde 6)

Personalesager

Der er 3 slags personalsager hvor e-mail problematikker kan være involveret: 1) sager hvor en person har foretaget en kriminel handling, 2) sager hvor en person overtræder en ansættelsesaftale eller en personalepolitik og 3) sager hvor en person sagsøger sin arbejdsplads for at denne har brudt en ansættelsesaftale, en personalepolitik eller en generel etisk handlemåde.

Ad. 1: Sager hvor en person foretager en kriminel handling kan f.eks. være sletning af en e-mail som skal arkiveres af hensyn til regulativer.

Ad. 2: Overtrædelse af en ansættelsesaftale kan være videregivelse af kundeinformation til en konkurrent.

Der har så vidt vides endnu ikke været danske retssager, hvor e-mail dokumenter har været fremlagt som bevis eller forsvar i personale-sager. Men man kunne vel godt forestille sig at en ansat ville fremlægge e-mails som dokumentation for uretmæssig afskedigelse eller bortvisning. Til gengæld findes personale-sager, som på anden måde har e-mails eller SOX som emne.

Der kendes mindst to danske sager, hvor der i en afskedigelsessituation refereres til Sarbanes-Oxley lovgivningen, som kan være relevant at nævne på trods af at der ikke nødvendigvis har været e-mail dokumentation involveret.

ComputerWorld skrev d. 6. august 2004 under overskriften: *"IBM-topchefer fældet af intern revision"* og henviser til SOX:

"Sagen er endnu et eksempel på, hvordan de hårde opstramninger i kølvandet på Enron-skandalen stadig sender drastiske dønminger ud i amerikanske koncernes danske datterselskaber. Det første kendte danske offer for minutiøse revisorers ekstra kritiske øje blev Peter Perregaard, Oracles europachef." "Kommunikationschef i IBM Anders Lund Rendtorff aviser at kommentere sagen: - Men jeg kan bekræfte, at vi lever op til den lovgivning, vi skal – inklusive den amerikanske Sarbanes Oxley-lovgivning, siger han."

(Kilde 5)

Internetavisen ComOn skriver d. 8. november 2005 under overskriften: "Bortvisning for slettede e-mails var uberettiget":

"En medarbejder fra den jyske it-virksomhed EDB-Gruppen har vundet en principiel sag i Vestre Landsret om uberettiget firing. Medarbejderen havde slettet vigtige e-mails med kundeoplysninger fra sin computer, hvorefter ledelsen valgte at ty til øjeblikkelig bortvisning og stoppe lønudbetalingen. Men Vestre Landsret mener ikke, at medarbejderen kunne bortvises, selv om virksomheden havde klare regler på området."

(Kilde 16)

Tydeligvis har EDB-Gruppen ikke et sikkert system til automatisk arkivering af e-mails, hvilket kunne have løst den ene af de 2 problemstillinger i sagen. At medarbejderen har overtrådt en intern politik, er en sag for sig.

Internetavisen ComOn skriver d. 14. marts 2005 under overskriften: "E-mail skandaler kan forebygges med klare regler":

"I sidste uge blev en virksomhed i Sønderborg dømt for uberettiget bortvisning af en medarbejder, der havde omtalt sin chef som 'en sæk' i en privat mail sendt fra arbejdspladsen."

(Kilde 13)

Dette er en sag af typen 3 (jvf. indledningen), da den drejer sig om dokumentation af uetisk handlemåde via e-mail.

Men det er samtidig også dokumentation for, at virksomheder som ikke har klare politikker for brug af e-mails kan komme i problemer. Hvis der er tale om en privat e-mail, har virksomheden i henhold til loven ikke ret til at læse den, med mindre dette er klart beskrevet i en politik på området.

Samme artikel nævner i øvrigt en sag fra 2003, hvor en IT-chef fra Haldor Topsøe blev fyret for at have rundsendt en racistisk vittighed. Her må man dog gå ud fra at loven om brevhemmelighed ikke er brudt, da medarbejderen jo har sendt mailen rundt i virksomheden.

(Kilde 14)

Computerworld skriver d. 10. september 2004 under overskriften "Dotcom-milliardær sendt bag tremmer":

"En e-mail til kollegaerne har bragt den tidligere børsstjerne Frank Quattrone til fald, skriver Cnet.

Den 48-årige bankmand skal 18 måneder i fængsel og betale en bøde på 550.000 kroner, fordi han i december 2000 sendte en e-mail til kollegaerne, hvori han bad dem om "at rydde op" i deres filer.

E-mailen kom, efter at de amerikanske myndigheder var begyndt at undersøge, om Frank Quattrone havde fusket med aktierne i de lukrative børsnoteringer for at skaffe penge til sig selv og firmaet."

(Kilde 15)

Som tidligere nævnt, bør virksomheden indføre politikker der dækker hvad en ansat må bruge sin firmamailadresse til, hvilke informationer der må sendes via mail og hvordan disse mails efterfølgende skal behandles.

Sager som omfatter misbrug af en mailadresse eller hvor indholdet i en mail ligger ud over, hvad de interne regler foreskriver vil helt sikkert blive reduceret voldsomt, i det øjeblik virksomheden indfører automatisk arkivering af alle e-mails. Hvem vil f.eks. risikere at blive forelagt en e-mail med diskriminerende indhold 3 år efter den er skrevet.

Tekniske argumenter

Formålet med dette dokument omfatter i princippet ikke tekniske eller teknologiske argumenter for at implementere løsning af e-mailproblematikkerne. Men nogle grundlæggende synspunkter skal alligevel med.

Et af de helt store problemer med håndtering af e-mails som forretningsdokumenter er nemlig de store og voksende mængder af mails, som en virksomhed har liggende på deres mailserver.

Her følger nogle fakta, som kan give lidt stof til eftertanke:

Ifølge det amerikanske analysefirma The Radicati Group er mængden af e-mails fordoblet de seneste to år og at trenden vil holde af den simple grund at e-mail er blevet den foretrukne metode til forretningskommunikation.

(Kilde 2)

Ifølge Radicati Group's rapport "The E-mail Archiving Industry Report 2003-2007" sender og modtager en typisk ansat 7 Mb per dag, hvilket forventes at øge til 14,7 Mb.

(Kilde 3)

Ifølge Radicati Group genererer en medarbejder i gennemsnit 84 e-mails pr. dag, hvilket kræver ca. 10Mb lagerplads daglig. Radicati tror at e-mails vil kræve ca. 15,8 Mb plads i 2008.

(Kilde 9)

Ifølge IDC genereres hele 35 milliarder e-mails hver arbejdsdag, imod kun 10 mia. for 5 år siden. Og med de nye compliance-drevne regulativer, som f.eks. SOX, har forretningsbeskeder i form af e-mails opnået samme status som andre almindeligt anvendte forretningsdokumenter. Forretningsmails repræsenterer en omtvistelig "guldmine" af information til udforskning i forbindelse med retssager. Afhængig af det installerede records management, content management og lagringssystem, repræsenterer produktion af e-mail-baseret bevismateriale et tidskrævende og dyrt krav for mange organisationer.

(Kilde 9)

Ifølge en Internet afstemning som InformationWeek har gennemført og refereret maj 2005, anvender 24% backup software til arkivering af e-mails. 31% udvider deres mailserver med mere diskplads, 28% gør ingenting overhovedet. Kun 17% anvender et politikstyret mailarkiveringsystem.

(Kilde 4)

SEC, NASD Investment Advisors Act, HIPAA og Sarbanes-Oxley anerkender alle specifikt

e-mail som et forretningsdokument. Faktisk ligger 70% af al vigtig forretningsdokumentation i eller er tilgængelig via e-mail [via link]. Direktører kan ikke længere ignorere kravene, eller bøderne, både overfor dem selv eller overfor deres virksomhed.

(Kilde 8)

Konklusion

De gennemgåede argumenter og dokumentation for, at det også kan give en dansk virksomhed problemer, hvis der ikke er styr på sikkerhed og tilgængelighed omkring e-mails, giver anledning til at konkludere følgende:

Uanset virksomhedsstørrelse, uanset branche og uanset om man umiddelbart er underlagt specifikke regulativer, er det i dag at betragte som best practice at have styr på virksomhedens mailpolitikker og systemer. Det kan være risikofyldt og omkostningstungt at ignorere problemstillingerne. På den anden side kan en IT-løsning der håndterer e-mails på samme vis som andre forretningsdokumenter give virksomheden store fordele ved at få nemmere adgang til den store mængde af information som ligger gemt her.

Kravsspecifikation til løsningen

Hvad skal der så til, hvis virksomheden vil tage konsekvensen af argumenterne og implementere politikker og IT-løsninger der kan sikre compliance, sikre mod manglende dokumentation i retssager eller sikre sig mod personalemæssige problemer?

1) Indførelse af politikker

For det første er det vigtigt at virksomhedens ledelse (og ikke bare IT-afdelingen) får analyseret hvilke typer af e-mails, som bliver sendt til og fra virksomheden, skal anses som forretningsdokumenter. Er der måder at identificere dem på? F.eks. kan det være mails til specifikke afdelinger (økonomi, personale, direktion) som skal håndteres på én måde og mails til marketingafdelingen på en anden måde. Det kan også resultere i, at det viser sig at være umuligt at skelne sikkert mellem relevante og irrelevante mails og derfor vælger at behandle alle mails på samme måde. Compliance kan jo være i fare, hvis man ikke er 100% sikker på at få alt relevant med.

For det andet bør der indføres politikker der fastsætter, hvordan medarbejderne må og skal håndtere deres firmamailadresse. Må

medarbejderen anvende mailadressen til private mails, og hvis han/hun må, skal disse så kunne identificeres som private. Man kan f.eks. overveje om alle private mails skal starte med ordet PRIVAT i emnet. Dette kan anvendes til at si disse fra, så de ikke bliver arkiveret på samme måde som forretningsmails i et mailarkiveringsystem. Det vil også sikre at loven om brevhemmelighed nemmere kan overholdes, da det jo i princippet er forbudt for uvedkommende at læse andres mails - også selv om de kunne indeholde en jobansøgning til en konkurrent.

For det tredje bør man overveje om der skal indføres politikker der beskriver hvad der må sendes som e-mails eller vedhæftet en e-mail. Må man sende en ordre, en konfidentiel oplysning (og hvad er konfidentielt), beskrivelse af et nyt produkt etc. For det første kan man risikere at mailen havner i de forkerte hænder. Der findes masser af eksempler på at en mail er blevet sendt til en forkert person ved en fejltagelse - og når der først er klikket på 'Send' er der ingen fortrydelsesmulighed. Under min research til dette whitepaper kom jeg forbi et godt råd: 'Definer det som må sendes i en e-mail, som alt hvad du kan tåle at se på forsiden af Financial Times dagen efter.' I det mindste kan man sikre sig at der i bunden af alle e-mails findes en tekst som tilsiger at indholdet skal betragtes som konfidentielt og at hvis mailen ved en fejl er havnet hos en forkert modtager, skal denne betragte indholdet konfidentielt og slette den straks.

Et eksempel på en virksomheds e-mail og Internetpolitikker, kan findes hos det engelske organ som overvåger finansielle institutioner, Financial Services Authority (FSA), hvor følgende link giver adgang til deres egne interne politikker. Disse kan give inspiration, men er sandsynligvis mere rigide end en gennemsnitlig dansk virksomhed ville vælge.
www.fsa.gov.uk/pages/library/other_publications/staff/staff_handbook/security/equipment/index.shtml

En anden god inspirationskilde er FSA's interne regulativhåndbog (Records Management Policy and Standards) om hvad 'God dokumenthåndtering' er for dem selv:

*God dokumenthåndtering kræver at følgende grundregler er opfyldt:
Regelmæssig gennemgang af informationen
Kontrolleret bevarelse af information*

*Kontrolleret destruktion af information
God håndtering af dokumenter og informationen heri vil opfylde FSA's egne krav til:
Dokumenter skal være lette og hurtigt at genfinde, tilgå og genskabe
Information er bedre beskyttet og lagret mere sikkert.
Dokumenter slettes sikkert og i rette tid.*

Grundreglerne for dokumenthåndtering er udarbejdet for at sikre at dokumenter er håndteret igennem hele dokumentets livscyklus, d.v.s. oprettelsen eller modtagelsen af et dokument, opdatering af dokumentet, håndtering af dets brug, tilgang til det, lagring, genfindning, og endelig bortskaffelsen af det.

Samme dokument angiver livscyklusen for forskellige typer af dokumenter:

*Ovenstående er et skoleeksempel på en gennemtænkt politik for elektroniske dokumenter og en ILM strategi.
(Kilde 24)*

Hvis virksomheden ikke har et IT-system som automatisk "fanger" alle ind- og udgående mails, er det vigtigt at der indføres politikker vedrørende *hvad* der skal arkiveres og *hvordan* det skal gøre samt *hvad* der må slettes. F.eks. er det ikke særligt sikkert at lade en medarbejder arkivere sine forretningsmails på sin bærbare PC og derefter slette dem fra indbakken. En teknisk problemstilling som kommer ind her, er jo at mange IT-afdelinger giver brugerne en begrænset størrelse mailbox, hvilket betyder at de selv skal finde ud af hvilke mails der skal slettes for at holde sig indenfor rammerne. Dette kan næsten ikke undgå at gå ud over e-mails som burde være gemt.

Disse politikker skal i øvrigt stadig overvejes og vedtages, hvis virksomheden implementerer et mailarkiveringsystem. På engelsk kaldes et sådant sæt af politikker for "Retention policies", som kan oversættes til bevaringspolitikker.

Information Systems Security offentliggjorde i oktober 2005 artiklen "Retention of Corporate E-Documents under Sarbanes-Oxley". Her fra citeres:

"Ingen lovgivning eller retsafgørelse har nogensinde krævet at en organisation skulle bibeholde sine dokumenter til evig tid. For

tidlig sletning/makulering, derimod, kan føre til straf i både civile og kriminelle sager. Hvis en organisation ikke er i stand til at fremlægge relevante dokumenter i retten, vil en dommer eller jury sandsynligvis antage at organisationen har destureret bevismaterialet med vilje"

(...)

"Etablering og håndhævelse af en nedskrevet bevaringspolitik er essentiel. Der skal tages speciel hensyn til sikring af al elektronisk materiale, inklusive e-mails, indtil sagen er afgjort [sagen = intern undersøgelse]. Dette kan kræve indkøb af nødvendigt computer hardware til at forøge virksomhedens elektroniske lagringskapacitet. Selv om det kan være omkostningskrævende, er bevarelse af elektronisk materiale essentielt i dagens verden."

(...)

"En nøje udviklet dokument-bevaringsprocedure kan spare en organisation penge, plads og tid. Risikoen for en retssag er en anden grund til at iværksætte en dokument-bevaringsprocedure. Elektroniske dokumenter skal være tilgængelige hvis en myndighed beder om dem eller hvis man i en civil retssag bliver afkrævet sådanne. Hvis en virksomhed ikke har en nedfældet beskrivelse af hvordan dokumenter bevares og slettes, kan modparten hævde at virksomheden har destrueret de elektroniske dokumenter for at undgå at fremlægge dem i retten."

(Kilde 18)

2) Information Lifecycle Management

Et af de relativt nye buzz-ord inden for IT, er konceptet Information Lifecycle Management (ILM). Det dækker over at forskellige typer af information ikke nødvendigvis skal behandles på samme måde over tid. Man kalder det at klassificere de forskellige informations- eller dokumenttyper. Processen går ud på at for hver type af dokument, skal virksomheden afgøre om det skal arkiveres, hvor det skal arkiveres og hvor længe det skal arkiveres.

En forretningsmail skal måske arkiveres på en arkivserver med hurtig tilgang - og er dermed dyr i drift - i 12 måneder, hvorefter den kan flyttes til et langsommere miljø i yderligere 12 måneder, før det ender på f.eks. en optisk disk i de sidste 24 måneder af sin levetid. Når indholdet af den optiske disk er blevet ialt 48 måneder gammelt, kan den dermed destrueres. Bemærk at visse regulativer faktisk stiller krav om at dette rent faktisk sker, hvilket et

arkiveringssystem bør kunne håndtere automatisk.

En anden dokumenttype kan måske allerede efter 3 måneder overføres til et inaktivt og dermed billigere lagringsmedie. Hele idéen med ILM er at få identificeret de forskellige dokumenttyper og lægge differentierede politikker for disse. Derved sikrer man sig for det første at de informationer der skal være hurtigt tilgængelige, også er det. Og at de informationer som "bare" skal gemmes sikkert og ikke ændres (f.eks. årsregnskaber, indgåede kontrakter etc.), bliver gemt på en hensigtsmæssig måde.

Resultatet vil faktisk vise sig på bundlinjen i de fleste virksomheder, idet de fleste kan flytte store datamængder over på billigere medier samt reducere antallet af servere.

Dette bringer os nu nærmere det at kunne definere kravet til en arkiveringsløsning, som skal opfylde virksomhedens ønsker til sikkerhed, compliance, politikker m.v.

Ultimativt bør følgende krav kunne opfyldes:

- 1) Automation: Systemet skal være i stand til automatisk at "fange" og arkivere alle ind- og udgående e-mails og indeksere dem.
- 2) Sikkerhed: Da både juridiske og lovmæssige aspekter kræver autentikation, bør alle arkiverede mails sikres og logges, så det kan dokumenteres, at de ikke har været ændret. Det samme gælder for vedhæftede filer.
- 3) Kontrol af arkiveringspolitik: Hver mail bør klassificeres i henhold til den vedtagne ILM-politik.
- 4) Lifecycle Management: Systemet bør automatisk kunne flytte mails til det mest økonomiske arkiveringsmedie under hensyntagen til ønsket svartid ved genfindning og vedtagne politikker. F.eks. at mails der er over 1 år gamle automatisk skal flyttes til optisk disk og derved aflaste arkivserveren.
- 5) Indeksering og søgemuligheder: Arkiveringssystemet bør ikke kun indekser mailens emne, men også hele mailens tekst samt de vedhæftede filers tekstmæssige indhold. På denne måde vil det være nemt at fremfinde alle mails som indeholder information om bestemte emner. Endvidere vil det være en fordel, hvis systemet giver mulighed for at anvende en browser til søgning og ikke kun

selve mailsystemet. Derved vil en bruger f.eks. kunne søge i arkiverede mails fra en ekstern arbejdsplads, samt at søge selv om mailserveren skulle være ude af drift.

6) Adgangskontrol: Et sikkert mailarkiveringssystem skal kunne styre hvem der må læse hvilke mails efter arkivering. I praksis vil det normalt betyde at kun de som har modtaget eller afsendt en mail efterfølgende vil få adgang til at læse den. Herudover vil en administrator selvfølgelig kunne få adgang, men denne adgang skal kunne logges.

7) Håndtering af arkiveringen: Det bør være muligt at lade en såkaldt "stub" forblive tilbage i brugernes mailboks efter at en mail er arkiveret og slettet fra brugerens mailboks. Stubben fylder meget lidt, men viser mailens afsender og emne og er et link til den fulde arkiverede mail, som dermed kan hentes tilbage i mailboksen.

8) Revisionsspor: En nødvendighed for dokumentation af overholdelse af love og regulativer (compliance) er, at alle hændelser logges og kan anvendes som revisionsspor. Der bør logges hver gang en mail arkiveres, genetableres, åbnes, slettes eller ændres. Ét er jo at kunne fremlægge en række mails som dokumentation, men det er jo i princippet lige så vigtigt at kunne dokumentere at der ikke mangler én.

9) Support af flere mailplatforme: Da implementering af et mailarkiveringssystem er en langsigtet beslutning, kan man komme ud for at skulle supportere flere forskellige mailsystemer (f.eks. både Exchange/Outlook og Lotus Notes) i fremtiden. Det vil derfor være en fordel at vælge et system som understøtter flere standarder. Endvidere vil det være en fordel hvis systemet har en historik der sandsynliggør at systemet også vil følge med mailsystemernes udvikling, så man ikke pludselig står med et arkiveringssystem som ikke kan håndtere en ny version af Exchange.

10) Rapportering: Det er vigtigt at systemet har funktioner til at udarbejde relevante rapporter af hensyn til revision og administration.

Oversigt over regulativer

Her følger uddybende forklaringer på, hvad de enkelte love og regulativer dækker over:

BS7799/ISO/IEC17799:2000 IT Security Standard

Britisk Standard og ISO standard for IT-sikkerhed.

Læs mere her:

www.iso-17799-security-world.co.uk/

Companies (Audit, Investigations and Community Enterprise) Act 2004

Engelsk lovgivning.

Læs hele loven her:

<http://www.opsi.gov.uk/acts/acts2004/20040027.htm>

og forklarende noter til loven her:

www.opsi.gov.uk/acts/en2004/2004en27.htm

samt guide til forståelse her:

www.dti.gov.uk/cld/companies_audit_etc_act/guidance_new.pdf

COSO rapporten

Som følge af en række uventede virksomhedskollaps tilbage i slutningen af 1980'erne iværksatte en organisation i USA – Committee of Sponsoring Organisations of the Treadway Commission, hvilket blev forkortet til COSO – arbejdet med at definere en begrebsramme for etablering af intern kontrol i større organisationer.

Dette arbejde resulterede i offentliggørelsen af COSO rapporten i USA i 1992 og 1994, og dette blev startskuddet til øget fokus på god ledelsesskik. Den oprindelige COSO rapport blev alene fremsat som en anbefaling.

COSO rapporten pegede på, at virksomhedens overordnede kontrolmiljø, herunder integritet, etik, ledelsesstil, organisations- og personaleudvikling og bestyrelsens involvering samt virksomhedens interne og eksterne kommunikation er vigtige elementer i et velfungerende ledelseskoncept.

COSO rapporten har fået fornyet relevans som følge af kravet i Sarbanes-Oxley loven, hvorefter ledelsen årligt skal offentliggøre vurdering af effektiviteten i selskabets interne kontroller og procedurer. COSO begrebsrammen anses for en relevant og dækkende begrebsramme for vurdering af en virksomheds interne kontroller og procedurer, og begrebsrammen har derfor en central placering i implementeringen af Sarbanes-Oxley.

Data Protection Act 1998 (DPA)

Engelsk lovgivning.

DPA giver en person ret til at få oplyst hvilken information en organisation opbevarer om denne. Loven bestemmer hvordan organisationer kan benytte personlig information som de

opbevarer, samt hvordan de indsamler, lagrer, videregiver samt sletter informationen.

PDA er et resultat af det fælleseuropæiske direktiv: 95/46/EC af 24. oktober 1995.

Det engelske regulativ findes her:
<http://www.opsi.gov.uk/acts/acts1998/19980029.htm>

EU direktivet her:
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

Financial Service Authority (FSA)

Engelsk lovgivning.

Disse regulativer er gældende for banker, ejendomsselskaber, investeringsfirmaer, forsikringselskaber, Lloyd's, elektroniske pengeinstitutter og lignende.

Regulativet tilsiger generelt bl.a. at et dokument sendt til en klient skal gemmes i sin oprindelige form i 3 år. I visse tilfælde dog op til 6 år (afhængig af dokumentindhold og type af kommunikation).

Læs mere om FSA her:
<http://www.fsa.gov.uk/>

Freedom of Information Act 2000 (FIA)

Da en del dokumenter der refereres til nævner den engelske regulativ kaldet FIA, skal den nævnes, selv om den ikke umiddelbart ligger indenfor nærværende dokumentets hovedemner. Denne lovgivning handler om en borgers ret til at få at vide hvilken information en offentlig myndighed har arkiveret om borgeren, samt regulativer omkring hvad og hvordan sådan information må indhentes, lagres og anvendes.

Læs mere her:
[http://](http://www.informationcommissioner.gov.uk)

www.informationcommissioner.gov.uk

USA har en tilsvarende lovgivning, som kan findes her:

<http://www.usdoj.gov/04foia/>

Her har man endog en speciel lovgivning vedrørende information som FBI skulle have om en person. Mere information om dette regulativ kaldet 'Freedom of Information Privacy Act' kan findes her:
<http://foia.fbi.gov/>

HIPAA (Health Insurance Portability and Accountability Act)

Også kendt som Kennedy-Kasselbaum Act. HIPAA kræver at organisationer og virksomheder indenfor healthcare og som beskæftiger sig med patientinformation skal tage skridt til at simplificere og standardisere dataudveksling og at beskytte og sikre konfidentiel information som håndteres. Dette betyder i praksis at virksomheden skal overgå til elektronisk udveksling af information, samt kryptering og sikring af sådanne udvekslinger. Alle juridiske enheder som håndterer, opbevarer, arkiverer og udveksler private helbredsoplysninger eller patientrelaterede informationer, uanset størrelse, skal overholde HIPAA.

Selv om HIPAA's krav har indflydelse på et bredt område, er fokus for denne målgruppe primært sikkerhedsreglementet [The Security Rules]. Det seneste sikkerhedsreglement blev offentliggjort d. 20. februar 2003 og giver et ensartet niveau af beskyttelse af alle sundhedsinformationer som opbevares eller overføres elektronisk og som angår en person.

Sikkerhedsstandard [The Security Standard] pålægger sikkerhedsforanstaltninger for fysisk arkivering og opbevaring, overførsel, og tilgang til individuel sundhedsinformation. Andre krav relateres til genetablering efter katastrofesituationer, omfattende brugeridentifikation, databeskyttelse, sikkerhed og revisionssport.

Læs mere her: <http://www.hipaa.org/>

Money Laundering Regulations 2003

Engelsk lovgivning indført efter fælles EU-regulativ kaldet 'Det tredje penge-hvidvask-ningsdirektiv'. Dansk lovgivning om samme emne formodes at være tilpasset samme regulativ.

Regulativet tilsiger pengeinstitutter at bevare og lagre dokumenter, som kan formodes at være bevismateriale i sager om hvidvaskning af penge.

Læs mere her:

http://www.hm-treasury.gov.uk/documents/financial_services/money/fin_money_index.cfm

og her:

<http://www.hm-treasury.gov.uk/media/5E8/8F/200509RIA1.pdf>

Privacy and Electronics Communications Regulations (PECR)

EU-direktiv som trådte i kraft december 2003 og afløste et direktiv fra 1999.

PECR beskriver regler vedr. marketing via telekommunikation, e-mail, fax etc.

Direktivet er ikke direkte relevant vedrørende dette whitepapers emner, men nævnes fordi visse kildetekster omtaler det.

Læs mere her:

www.informationcommissioner.gov.uk

Proceeds of Crime Act 2002 (POCA)

Engelsk kriminallovgivning som blev indført for at dæmme op for bl.a. hvidvaskning af penge. Bliver overvåget af Assets Recovery Agency.

Læs mere her:

http://www.cps.gov.uk/legal/section21/chapter_a.html#_Toc40070596

Sarbanes-Oxley (SOX)

Sarbanes-Oxley loven repræsenterer den mest gennemgribende ændring af de børsretlige regler i USA siden vedtagelsen af fondsbørslovene i 1933 og 1934.

Sarbanes-Oxley loven blev vedtaget d. 30. juli 2002 som følge af en række selskabs- og regnskabsskandaler i USA. Loven blev gennemført for at genoprette offentlighedens tillid til den regnskabsmæssige rapporteringsproces, og den medfører grundlæggende ændringer i den måde, hvorpå ledelsen, revisionkomitéer og de eksterne revisorer udfører deres respektive opgaver.

Læs mere her:

<http://www.sarbanes-oxley.com/>

SEC Rule 17a-4

Hvis virksomheden er i 'risikozonen', hvor den kan være under amerikansk lovgivning, er dette en af de vigtige regulativer, som skal iagttages nøje.

I et tiltag for at beskytte investorer mod svindel og vildledning indenfor handel med værdipapirer, vedtog Securities and Exchange Commission (SEC) i 1934 the Securities Exchange Act [Loven om handel med værdipapirer], som er et sæt af love som krævede journalisering af alle handler af hensyn til revision af alle transaktioner. I 1997 tilføjede kommissionen 17a-4 reglen som tillader værdipapirhandlere at arkivere

disse journaler elektronisk, men også at kommunikere elektronisk via f.eks. e-mail og instant messaging.

Lovgivningen har indflydelse på alle juridiske enheder som har med værdipapirhandel at gøre: Brokerfirmaer, rådgivere, banker m.v. Disse inkluderer også alle juridiske enheder som er under overvågning af domsmyndigheden the National Association of Securities Dealers (NASD) [Sammenslutningen af værdipapirhandlere].

De mest relevante paragraffer er SEC 17a-3 som kræver skabelse af journaler og SEC 17a-4 som omfatter krav om at gemme disse journaler. 17a-4 udspecificerer regler omkring gemmetid, at storage ikke kan overskrives og at det skal være nemt at genfinde og revidere data.

Loven kræver at investerings-selskaber gemmer dokumenter, inkl. e-mails, i en periode på seks år og de første to år på en lettilgængelig måde. Endvidere stilles der krav til medietype, idet data i visse tilfælde skal lagres på medier der ikke kan overskrives.

Læs mere her:

<http://www.sec.gov/rules/final/34-46473.htm>

og her:

www.law.uc.edu/CCL/34ActRIs/rule17a-4.html

og her:

<http://www.sec.gov/rules/interp/34-47806.htm>

NASD Rule 3010 og 3110

National Association of Securities Dealers er den amerikanske sammenslutning af værdipapirhandlere. Regulativer for disse overvåges af SEC. I 1998 blev regulativerne udvidet med NASD 3010 og 3110, som refererer til og har arvet de samme krav som SEC 17a-3 og 17a-4 (se disse) og kræver endvidere at virksomheden skaber politikker og arkivering af reviderbare kunde- og transaktionsdata.

Læs mere her:

http://www.ici.org/issues/dis/arc-prx/98_nasd_rule3010_final_jan.html

Kilder

Her følger kildeliste og URL'er til de kilder som kan findes Internettet:

- (1) Sarbanes-Oxley loven i sin fulde længde kan hentes her:
www.neupart.com/cmseasy/cmseasy.nsf/0/5B49347BF62868E6C1256FDB006D8AA9?opendocument&expand=L%C3%A6r!&page_name=Sarbanes-Oxley&lang=DK
- (2) www.dcd.uscourts.gov/99-2496ap.pdf
- (3) www.snwonline.com/implement/email_archiving_09-27-04.asp?article_id=454
- (4) informationweek.com/shared/printableArticleSrc.jhtml?articleID=163100559
- (5) www.computerworld.dk/default.asp?Mode=10&ArticleID=24643
- (6) www.cbronline.com/content/COMP/magazine/Articles/Storage/000172.asp
- (7) Dansk Standards hjemmeside:
www.ds.dk/2775
- (8) www.infostor.com/articles/article_display.cfm?Section=ARCHI&C=Feat&ARTICLE_ID=221840&KEYWORDS=Case%20Studies%3A%20how%20users&p=23
- (9) Sarbanes-Oxley Compliance Journal:
www.s-ox.com/Feature/detail.cfm?ArticleID=913
- (10) Økonomi- og Erhvervsministerens tale ved Advokatrådets høring om compliance:
www.oem.dk/sw7747.asp?usepf=true
- (11) Børshåndbogen 2005, udgivet af PricewaterhouseCoopers. Kan downloades gratis fra PwC's hjemmeside:
www.pwc.com
- (12) www.advokatnet.dk/Default.asp?ID=4935&M=News&PID=9079&NewsID=3273
- (13) www.comon.dk/index.php/news/show/id=21488
- (14) www.comon.dk/index.php/news/show/id=18846
- (15) www.computerworld.dk/art/25117?a=search&i=0
- (16) <http://www.comon.dk/index.php/news/show/id=24233>
- (17)
- (18) www.infosectoday.com/SOX/Freeman.pdf

- (19) www.infoeconomy.com/pages/politics-management/group101698.adp
- (21) www.itworld.com/Man/2699/050311burst/pfindex.html
- (22) <http://europa.eu.int/jurisp/cgi-bin/form.pl?lang=da&Submit=S%C3%B8g&alldocs=alldocs&docj=docj&doco p=docop&docor=docor&docjo=docjo&numaff=&datefs=&datefe=&nomusue l=&domaine=&mots=e-mail+dokumentation&resmax=100>
- (23) www.danskebank.dk/CorporateGovernance
- (24) www.fsa.gov.uk/pages/information/pdf/records_policy.pdf
- (25) <http://dansk-it.dk/default.asp?id=3815>
- (26) <http://dansk-it.dk/sw3245.asp>
- (27) http://www.financialexpress.com/fe_full_story.php?content_id=109114
- (28) <http://www.itweek.co.uk/articles/print/2085710>
- (29) <http://www.computerworld.dk/art/30442?a=search&i=0>
- (30) Artikel fra Computerworld d. 14.10.2005. Kun i den trykte udgave.
- (31) Artikel fra Computerworld d. 14.10.2005. Kun i den trykte udgave.

Andre kilder:

EU's hjemmeside om data beskyttelse:
http://europa.eu.int/comm/justice_home/fsj/privacy/

Der er stort set uendeligt med dokumenter på Internettet omhandlende dette whitepapers emner. Det største problem er at sortere og filtrere informationen. Hvis du vil vide mere kan vi anbefale at søge via Google på søgeord som: SOX, Sarbanes-Oxley, Compliance, e-mail archiving, legislations, SEC, HIPAA, NASD og kombinationer heraf.

© DocTech ApS

Alle rettigheder tilhører DocTech og de angivne kilder.

Dette dokument må ikke - helt eller delvist - reproducere eller refereres i nogen form uden forudgående aftale med DocTech.

Alle refererede kildetekster skal ligeledes behandles som tilhørende kilderne og deres forfattere.

Bemærk

Dette dokument er så korrekt og up-to-date som det har været muligt. Visse kildetekster er oversatte og kan derfor risikere at indeholde fejl, men de fleste originaldokumenter kan findes på Internettet og URL'erne er angivet i kildelisten bagest i dokumentet. Andre originaltekster kan rekvireres hos OptoDenmark i det omfang DocTech har rettigheder til at videreformidle disse. Send mail til info@doctech.dk
Debello kan ikke tillægges ansvar for fortolkning af eller brug af de råd og vejledninger som dokumentet giver.

Dokumentet vil løbende blive opdateret med nye informationer og cases. Hvis du ønsker opdaterede versioner tilsendt automatisk, send da mail til info@doctech.dk