Indsigt i cybersikkerhed

Hvordan forbereder man sig på et sikkerhedsbrud?

DLA PIPER

Dagsorden

DLA Piper Denmarks Cybersikkerheds-team

Marlene Winther Plas
Advokat, Partner
T: +45 33 34 00 47
M: +45 22 47 82 18
Marlene.Plas@dlapiper.com

Jon Laurtizen
Advokat, Partner
T: +45 33 34 02 84
M: +45 40 73 58 16
Jon.Lauritzen@dlapiper.com

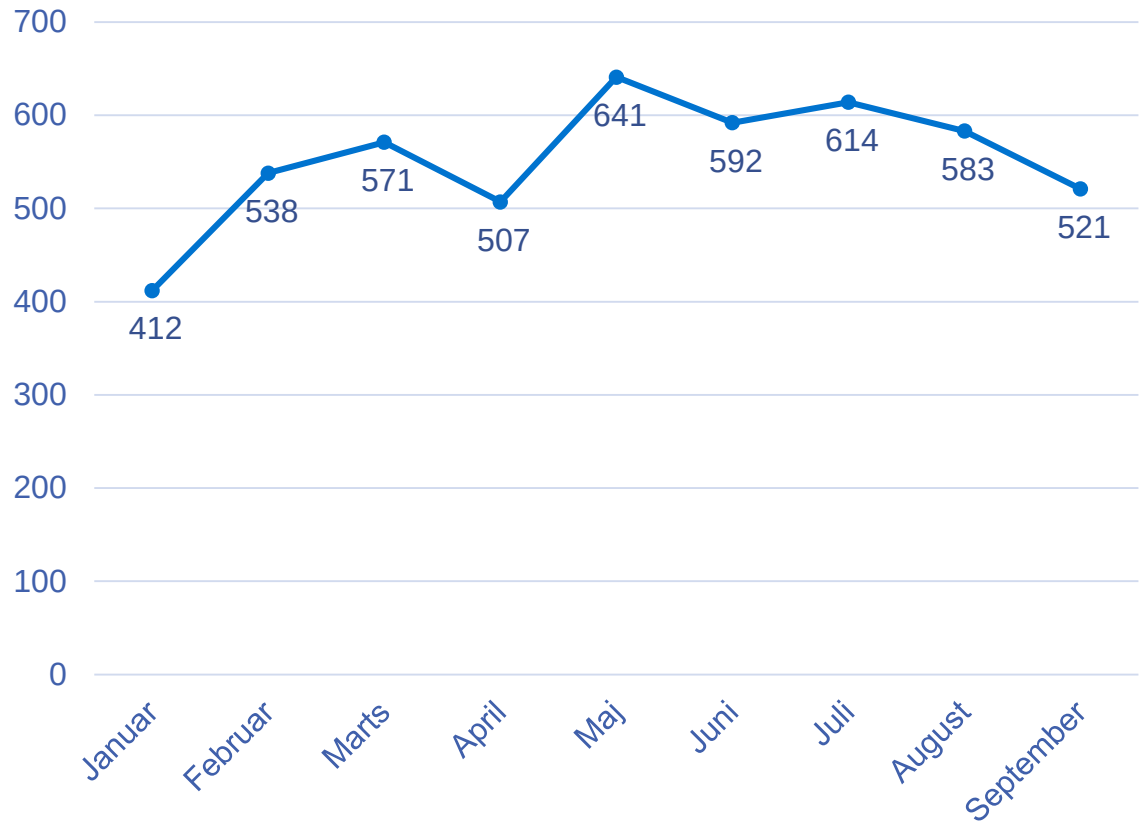
Emil Agerskov Thuesen
Advokatfuldmægtig
T: +45 33 34 00 65
M: +45 20 56 07 69
Emil.Agerskov@dlapiper.com

Sikkerhedsbrud i tal

Sikkerhedsbrud i tal

Danmark (kilde: Datatilsynet)

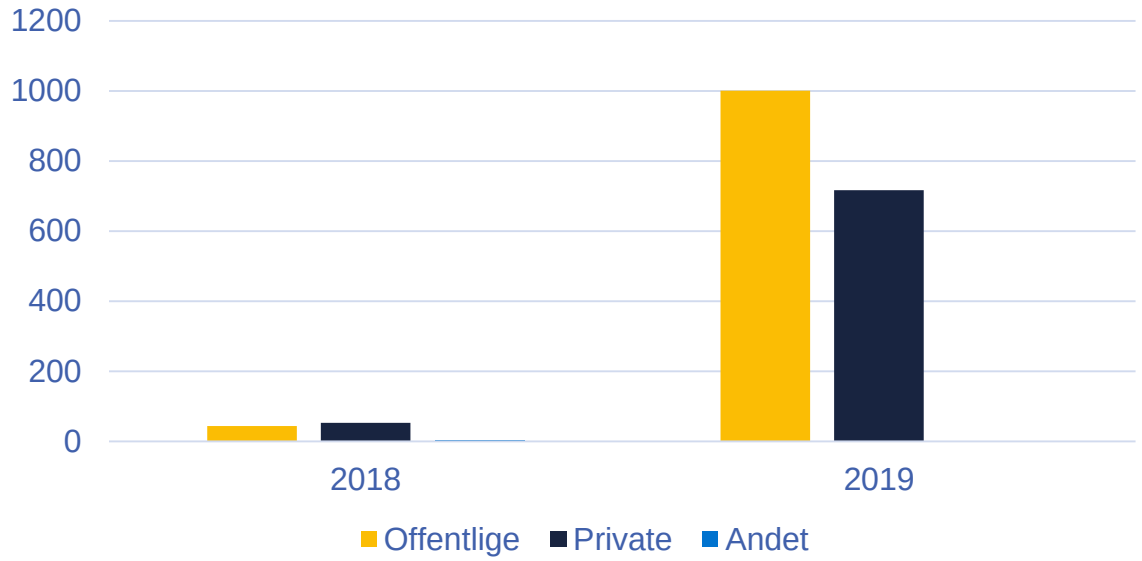
Antal anmeldte sikkerhedsbrud i 2019 (frem til 4. kvartal)

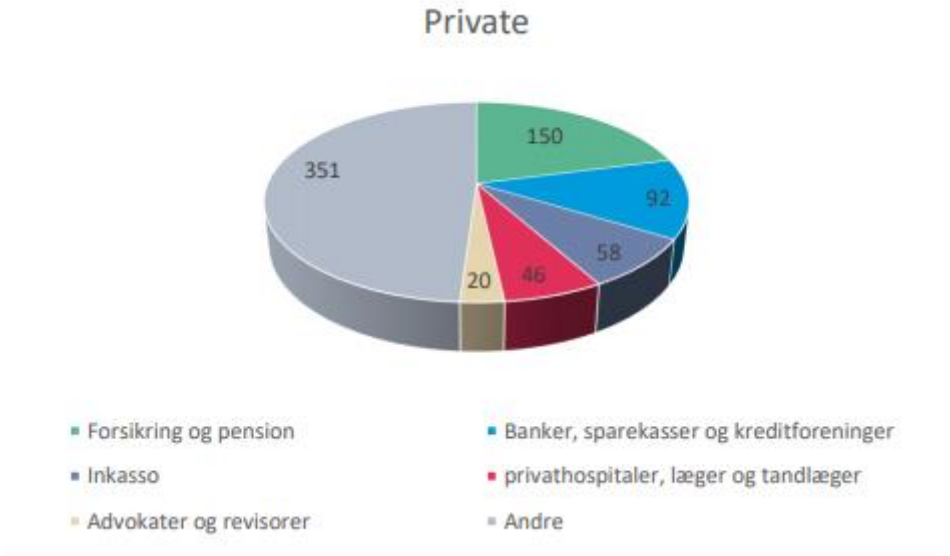


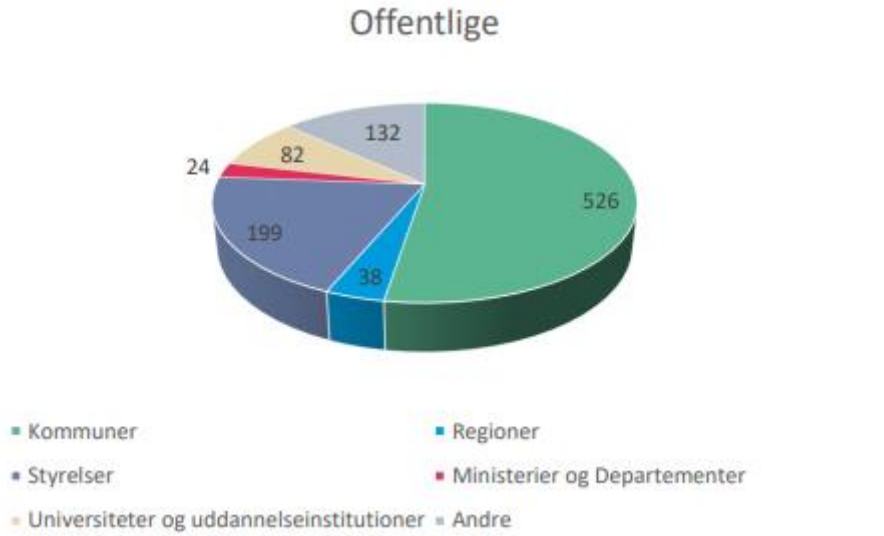
Sikkerhedsbrud i tal

Danmark (kilde: Datatilsynet)

Fordeling (procent)



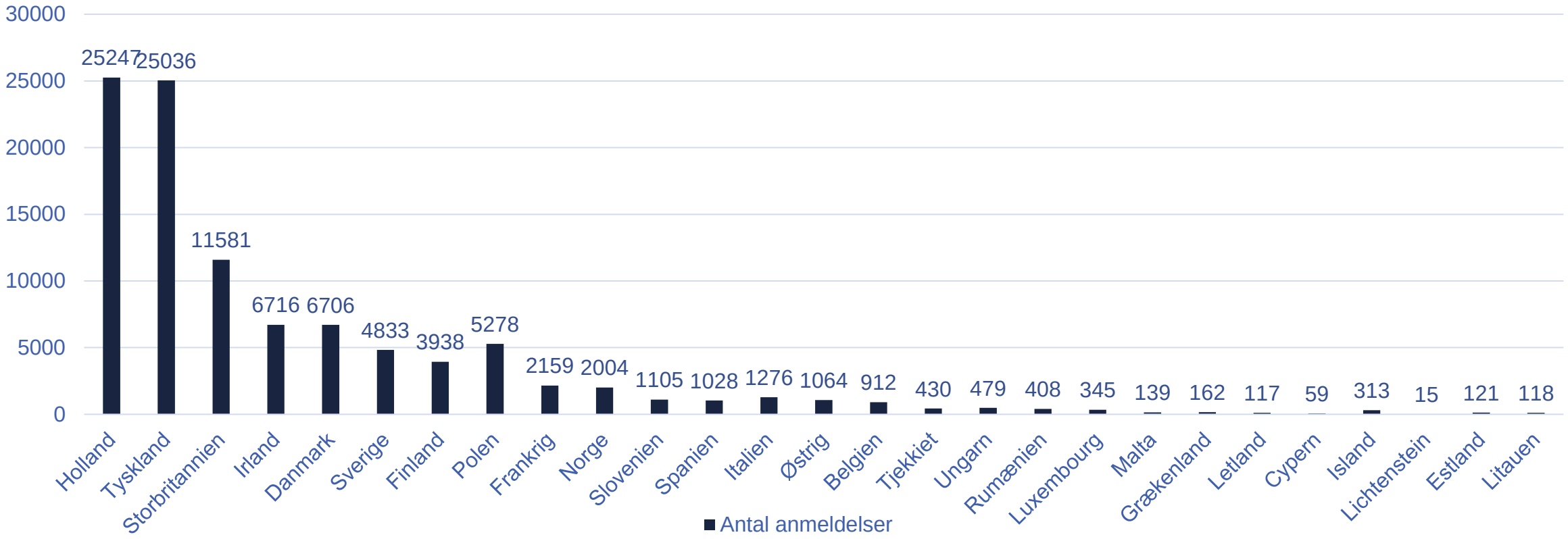




Sikkerhedsbrud i tal

Europa

Fordeling i Europa* (28. januar 2019-27. januar 2020)

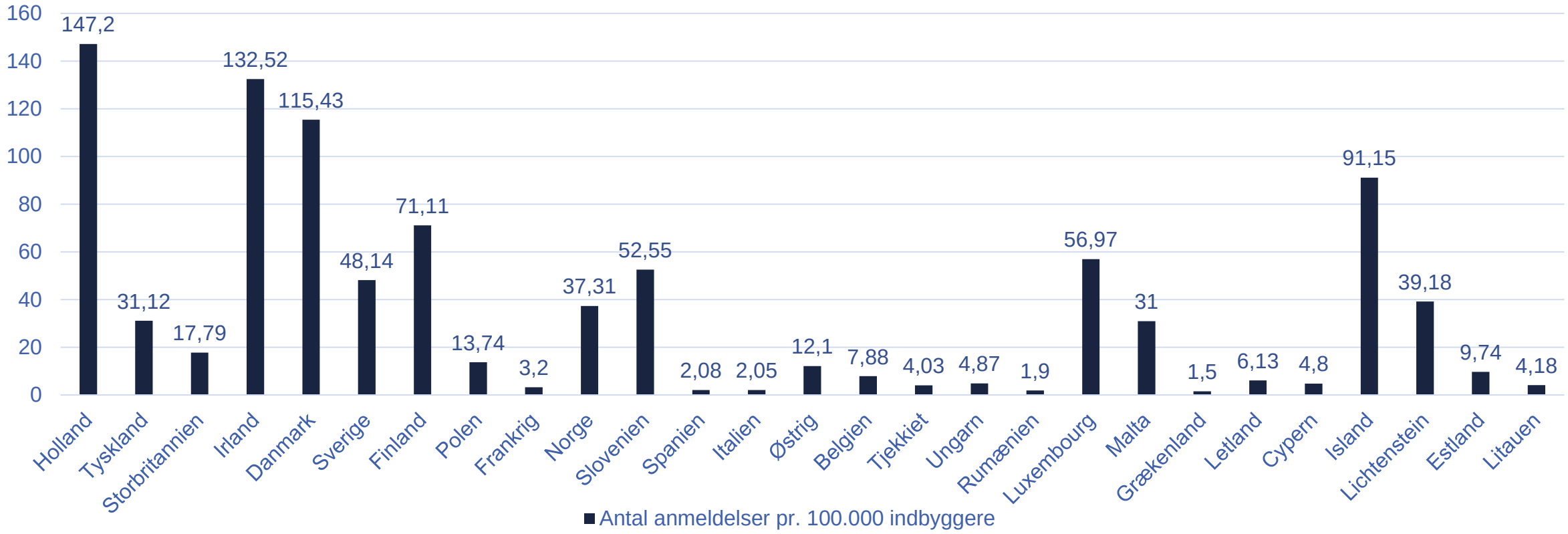


* Offentliggør ikke data: Slovakiet, Bulgarien, Kroatien, Portugal

Sikkerhedsbrud i tal

Europa

Fordeling ift. indbyggertal i Europa* (28. januar 2019-27. januar 2020)



* Offentliggør ikke data: Slovakiet, Bulgarien, Kroatien, Portugal

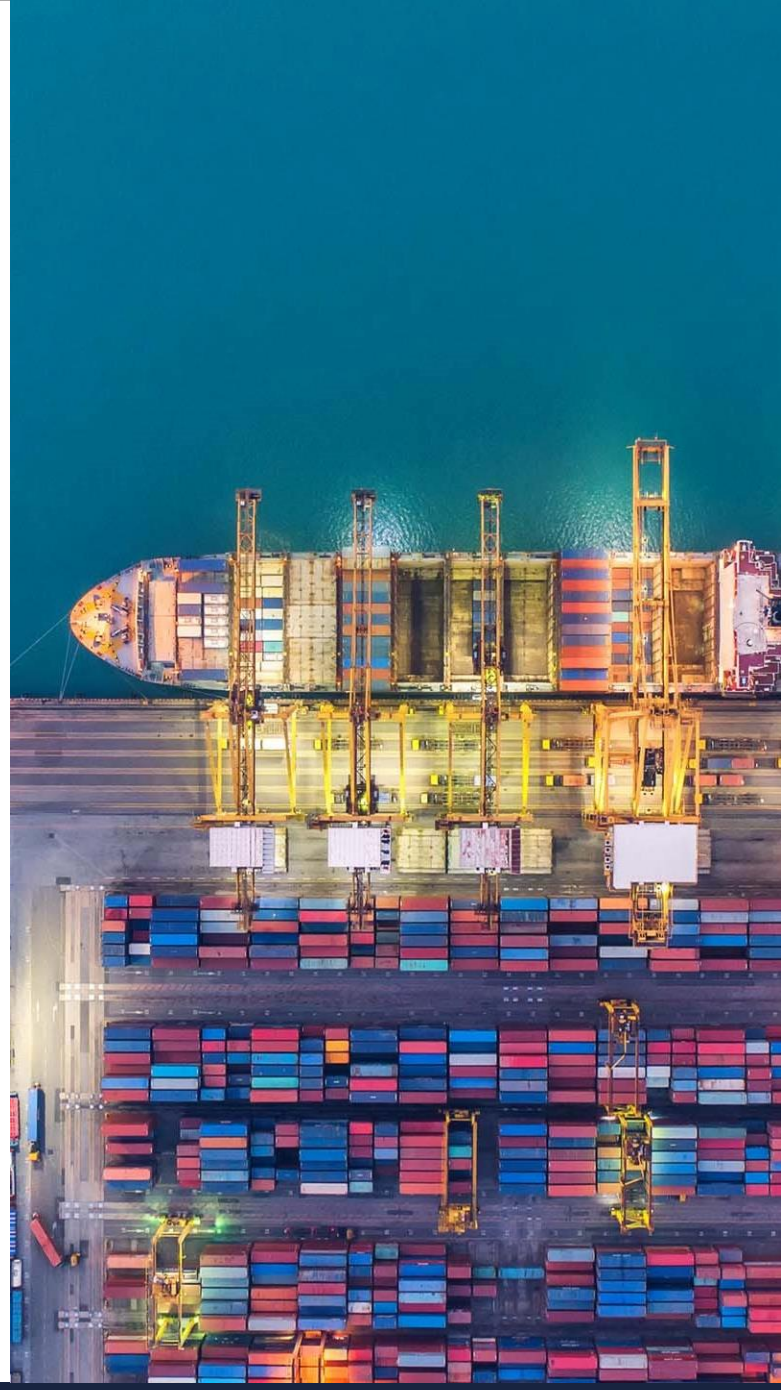
Enforcement

August 2019

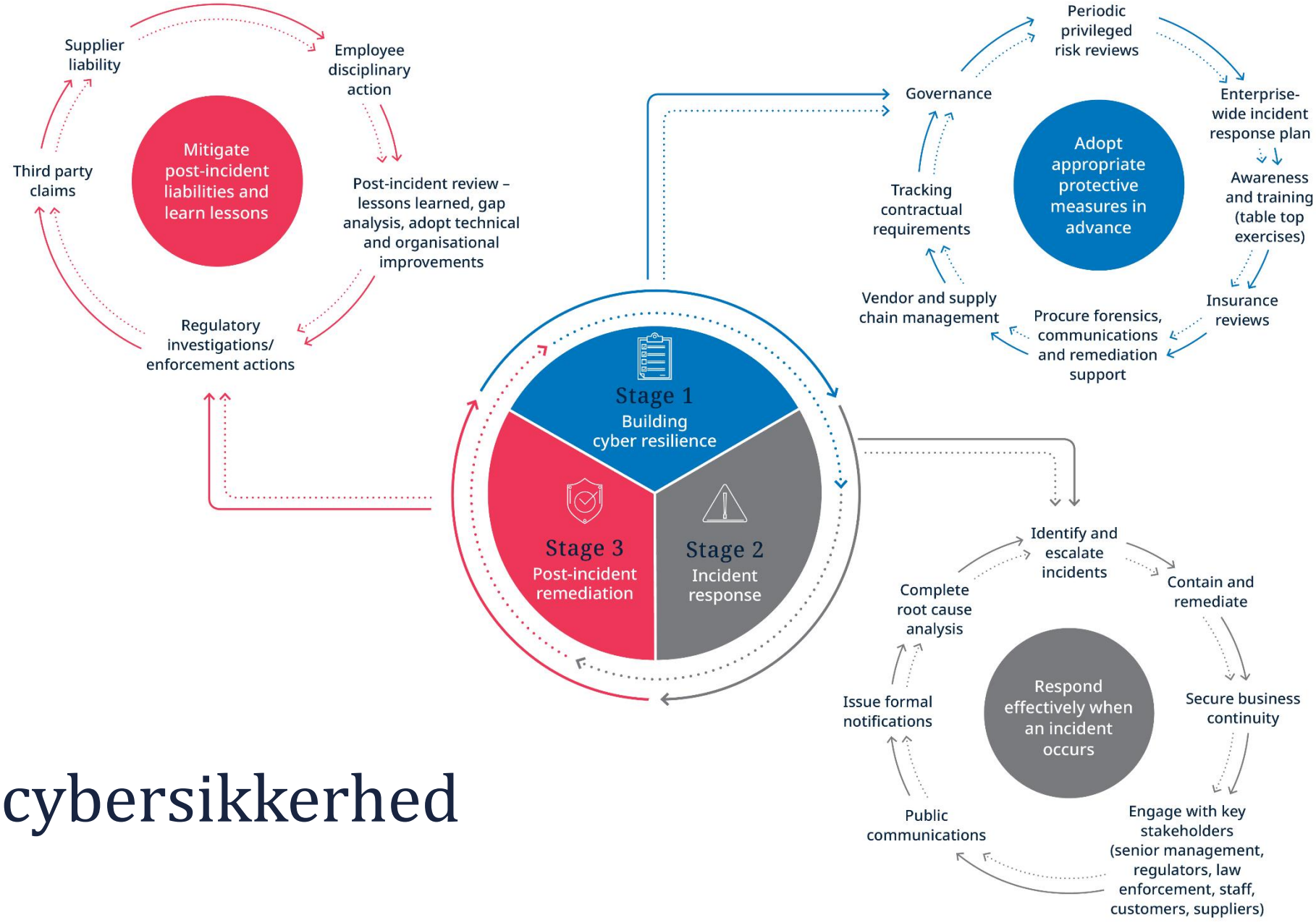
Et dansk eksempel

Mærsk

- Blev ramt af ransomware (NotPetya) i juni 2017
- Alle Mærsks containerterminaler lukkede ned i flere dage
- Anslået tabt omsætning: 1,6-1,9 milliarder DKK



Livscyklus for cybersikkerhed



Forberedelse

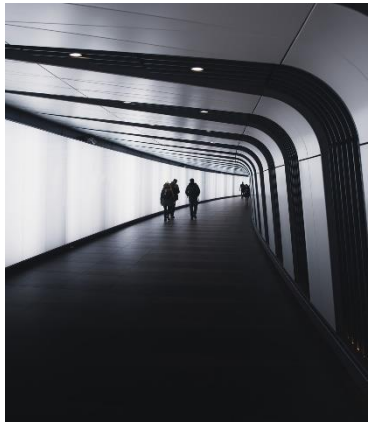
Hvordan begrænser man konsekvenserne af et sikkerhedsbrud, før det sker?

Forberedelse

Styring

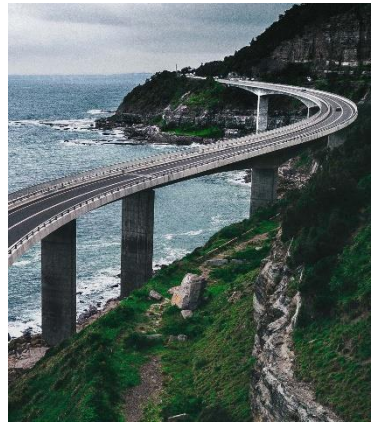
Kommunikation

Politikker



Mennesker

Træning



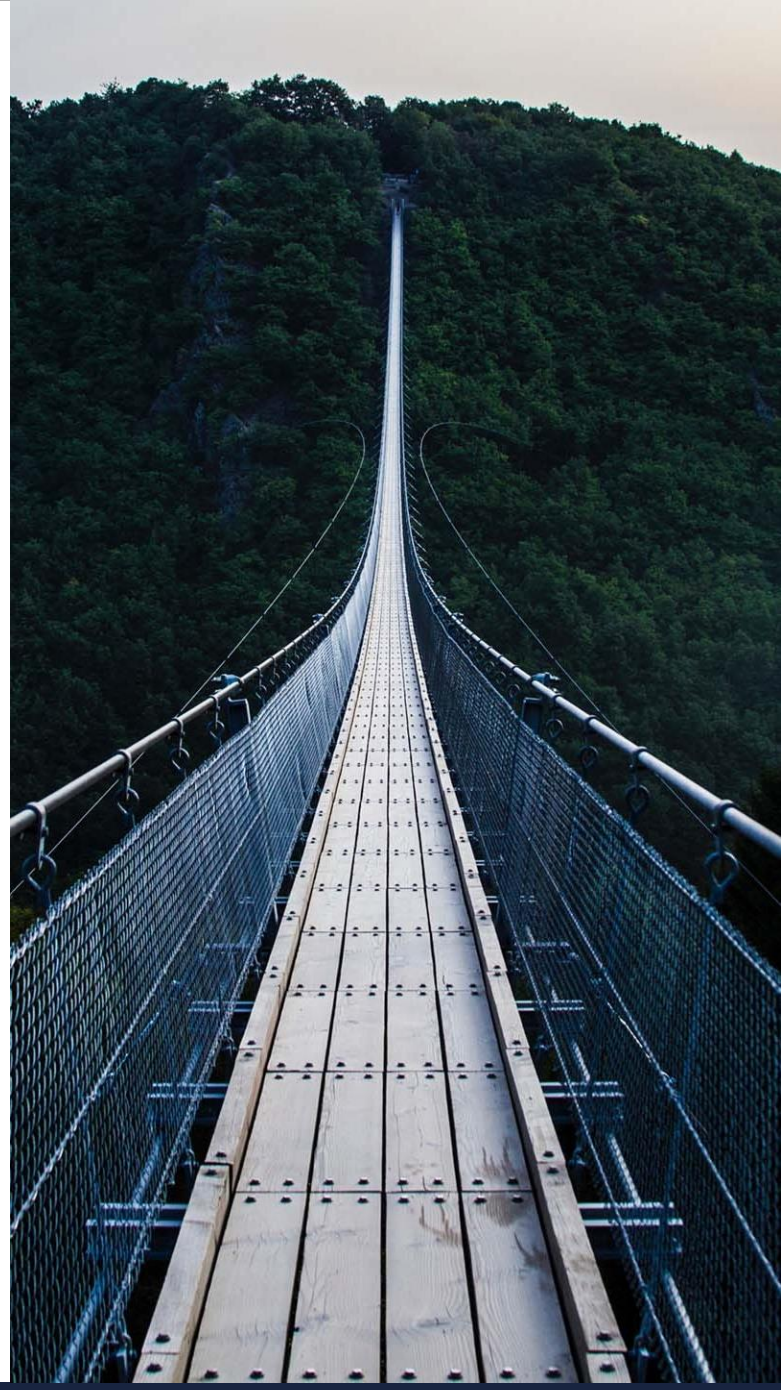
Rådgivere

Forberedelse

Styring

- Hvorfor?
  - Cyberangreb og sikkerhedsbrud er en stor risiko for mange organisationer og bør behandles som sådan

- Hvordan?
  - God ledelsesstruktur
  - Passende intern rapportering til den øverste ledelse
  - Opretholdt passende opsyn og integritet

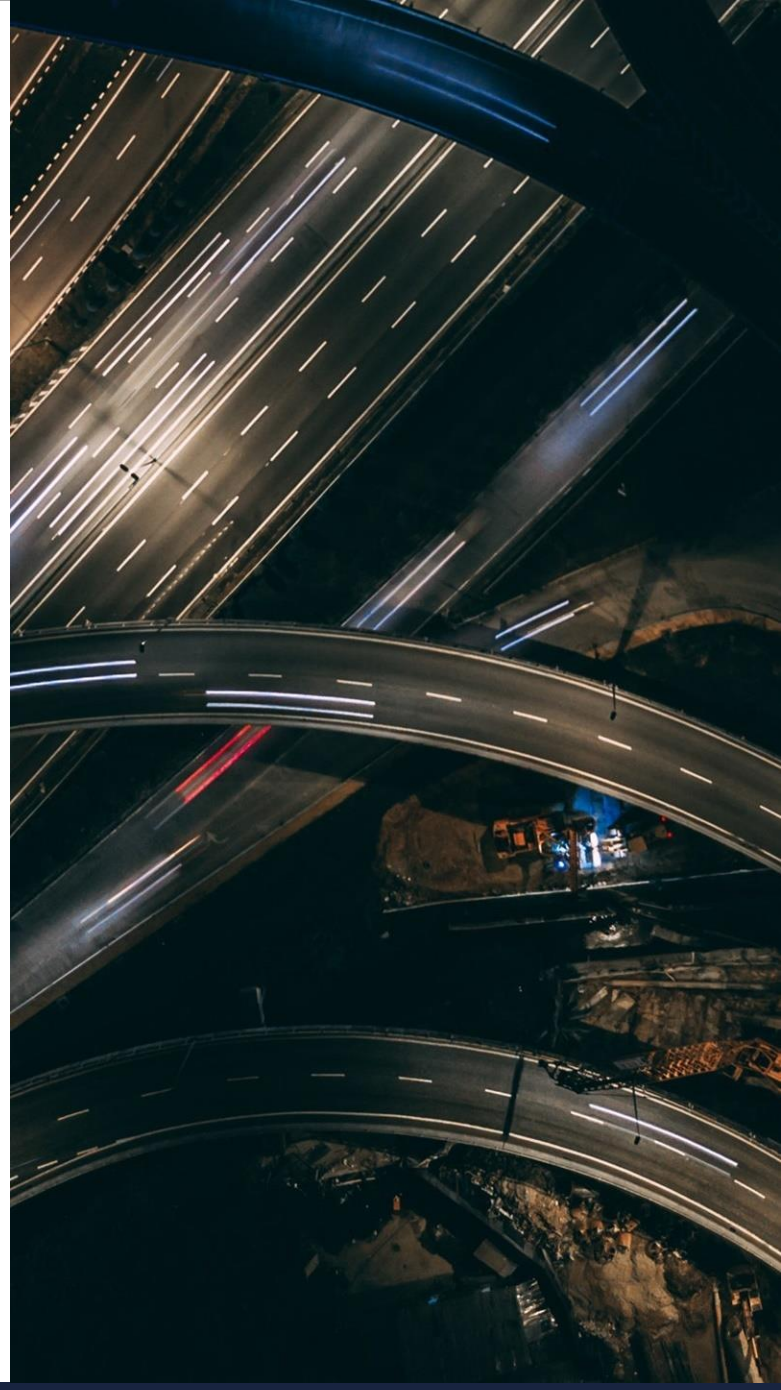


Forberedelse

Kommunikation

- Hvorfor?
  - Effektiv kommunikation er afgørende for udfaldet af et brud
  - Fejlhåndteret kommunikation gør en dårlig situation endnu værre

- Hvordan?
  - Nødkommunikationsplan på plads
  - Klare ansvarsområder (hvem beslutter, hvad der skal meddeles)?
  - "PR“-kommunikation vs. obligatoriske anmeldelsesforpligtelser

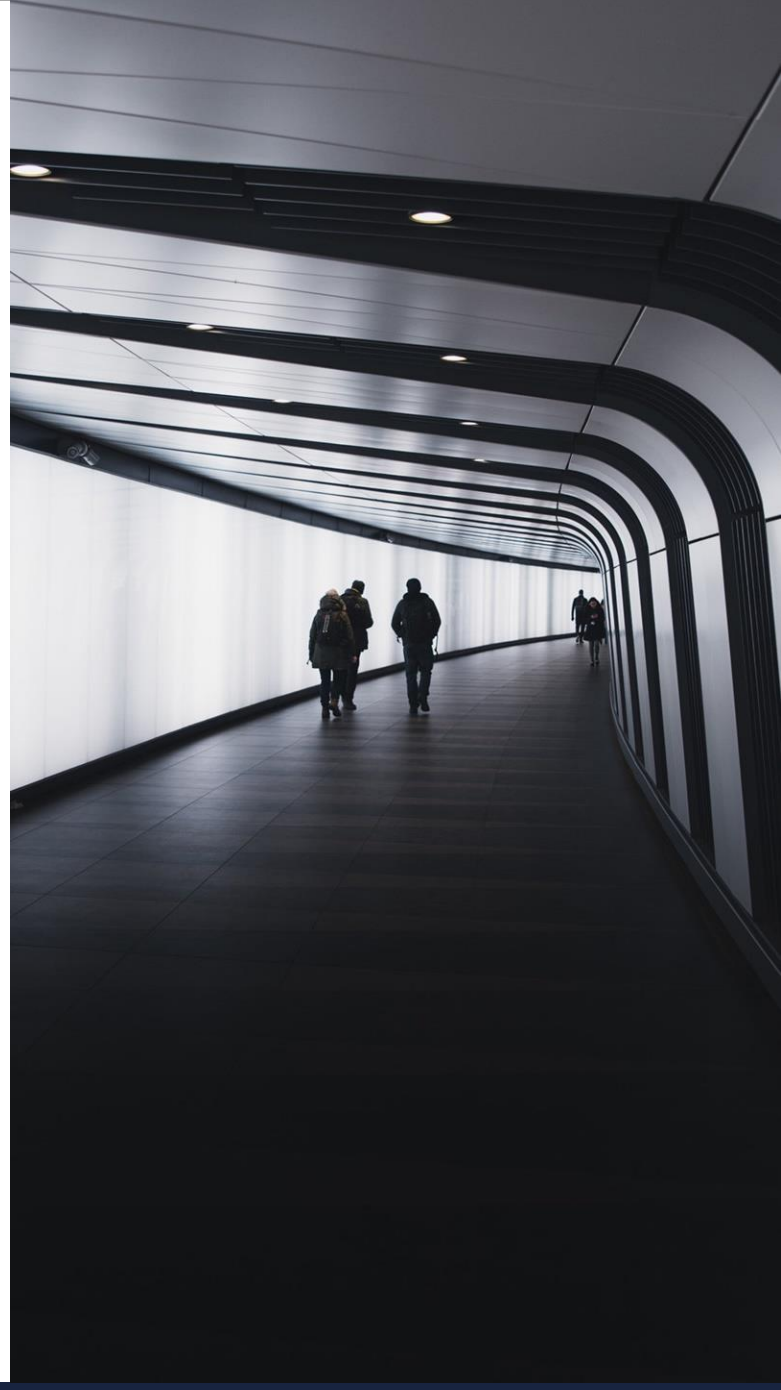


Forberedelse

Politikker

- Hvorfor?
  - Skriftlige procedurer, der skal følges af organisationen. Dokumentation

- Hvordan?
  - Levende dokumenter, der bygger på læring fra undervisning og virkelige hændelser
  - Politik for undersøgelse, standsning, afhjælpning, sikkerhed, anmeldelse af sikkerhedsbrud

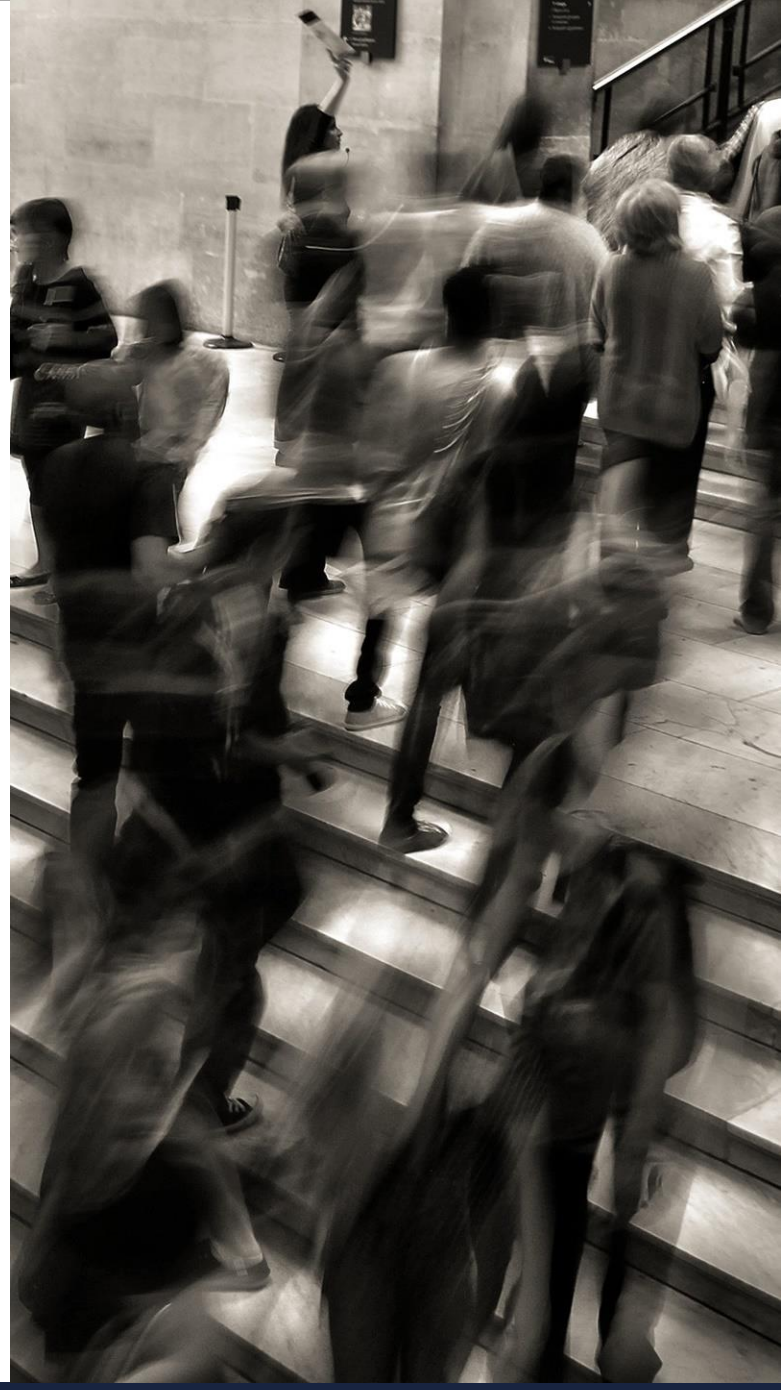


Forberedelse

Mennesker

- Hvorfor?
  - Reaktion på hændelser kræver en blanding af færdigheder, herunder inden for efterforskning, cyber, kommunikation og jura

- Hvordan?
  - Arbejdsgrupper skal etableres og helst øves, før de skal håndtere en faktisk hændelse
  - Klare ansvarsområder
  - Eksterne eksperter kan også give en grad af uafhængighed og objektivitet



Forberedelse

Træning

- Hvorfor?
  - Være klar og forberedt samt opdatere viden

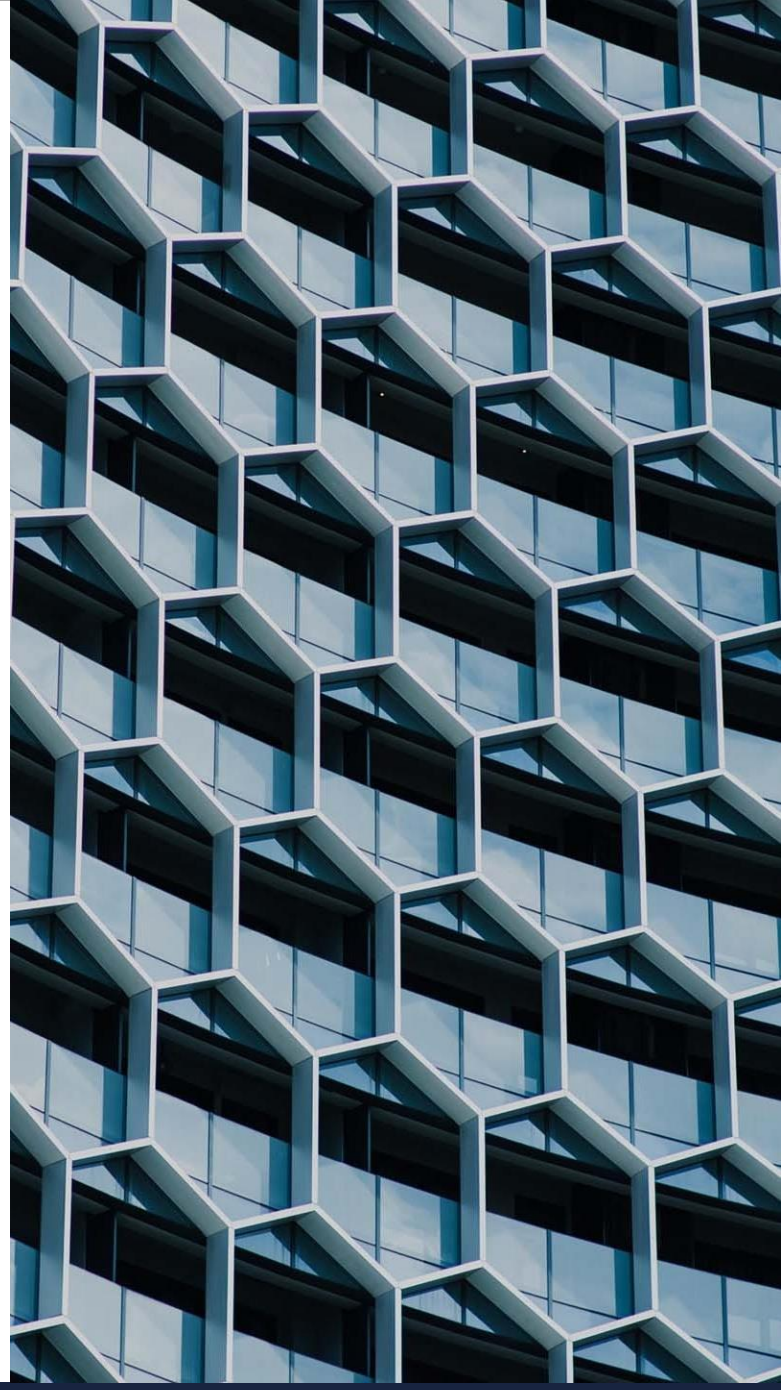
- Hvordan?
  - Det er nødvendigt at teste politikker og reaktionsberedskab
  - Test af IT-indtrængning
  - Vi anbefaler, at dette gennemgås årligt

Forberedelse

Rådgivere

- Hvorfor?
  - Man kan aldrig være sikker på, at et sikkerhedsbrud kan håndteres med kun interne ressourcer

- Hvordan?
  - Udpeg et eksternt team, der står klar til at assistere, hvis et sikkerhedsbrud skulle ske
  - Relationen bør etableres i rette tid og vedligeholdes regelmæssigt



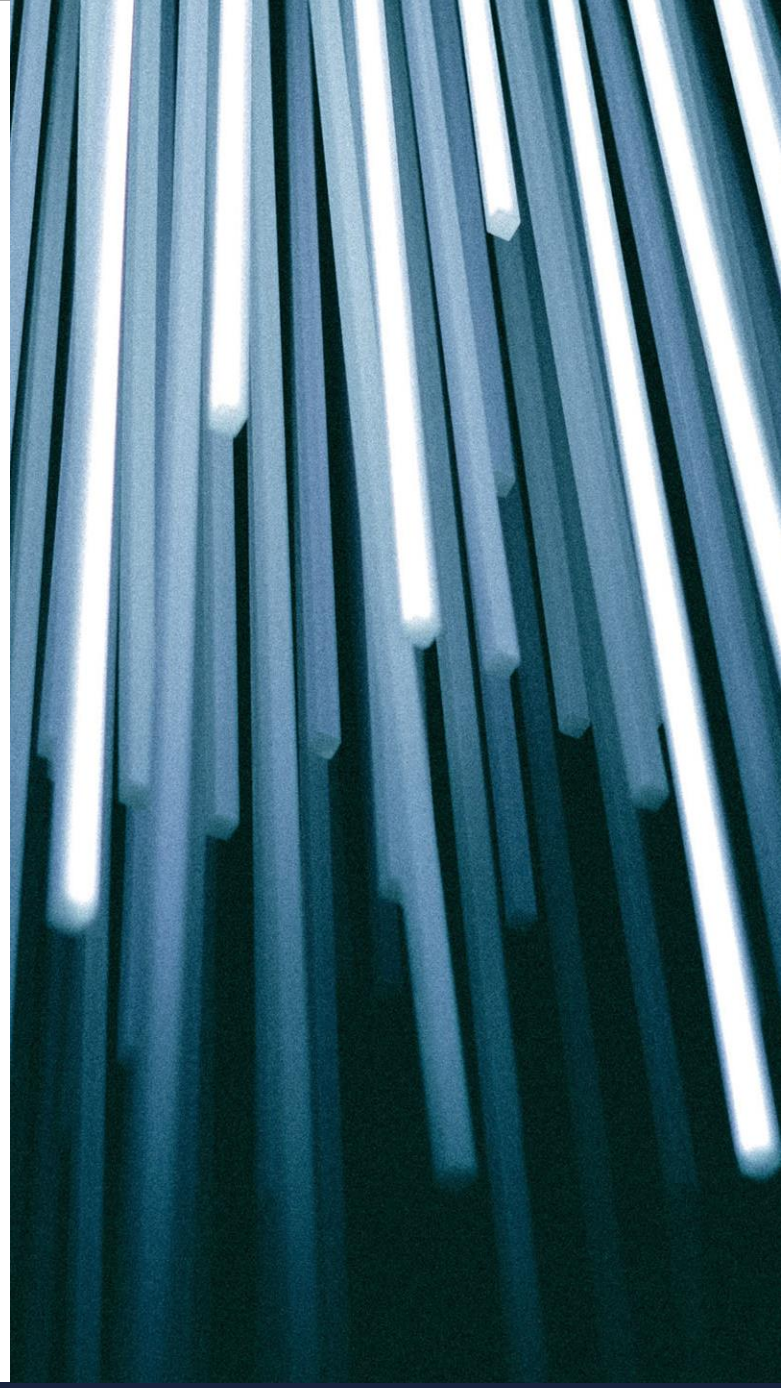
Sharing the Experience of our Cyber Incident

PRIVATE & CONFIDENTIAL

DLA PIPER

What happened?

- On 27 June 2017, a cyber attack (caused by malware called NotPetya) originating in Ukraine resulted in all DLA Piper IT systems being taken offline
- In the space of 90 minutes, NotPetya caused significant damage:
  - 1,500 of our 1,800 servers were hit and required rebuilding
  - all primary communications systems were affected: email, phones, voicemail, video, TelePresence, Skype/Lync
  - 500 applications (including time recording and document management) used by our people affected
  - 6,500+ PCs and laptops needed either to be wiped and rebuilt or inoculated
- NotPetya propagated itself, encrypted Windows files and hard disks, and deleted its own encryption keys as it went



What hit us and why?

- NotPetya was a particularly sophisticated “Supply Chain” attack on a trusted software vendor (M.E.Doc). The malware was embedded in a standard M.E.Doc software update. The malware harvested credentials spreading across the global network.
- M.E.Doc payroll systems were widely used in Ukraine by government and international companies, including DLA Piper
- DLA Piper was not specifically targeted. Over 2,000 organisations were affected
- UK and US have attributed NotPetya to the Russian military and is estimated to have cost businesses around the world more than $1.2 billion in total
- No evidence of access to or loss of client or business data – PwC IT forensic report
- Data stored on DLA Piper systems remained intact and retrievable via back ups
- “Wannacry” system patching was up to date but didn’t help

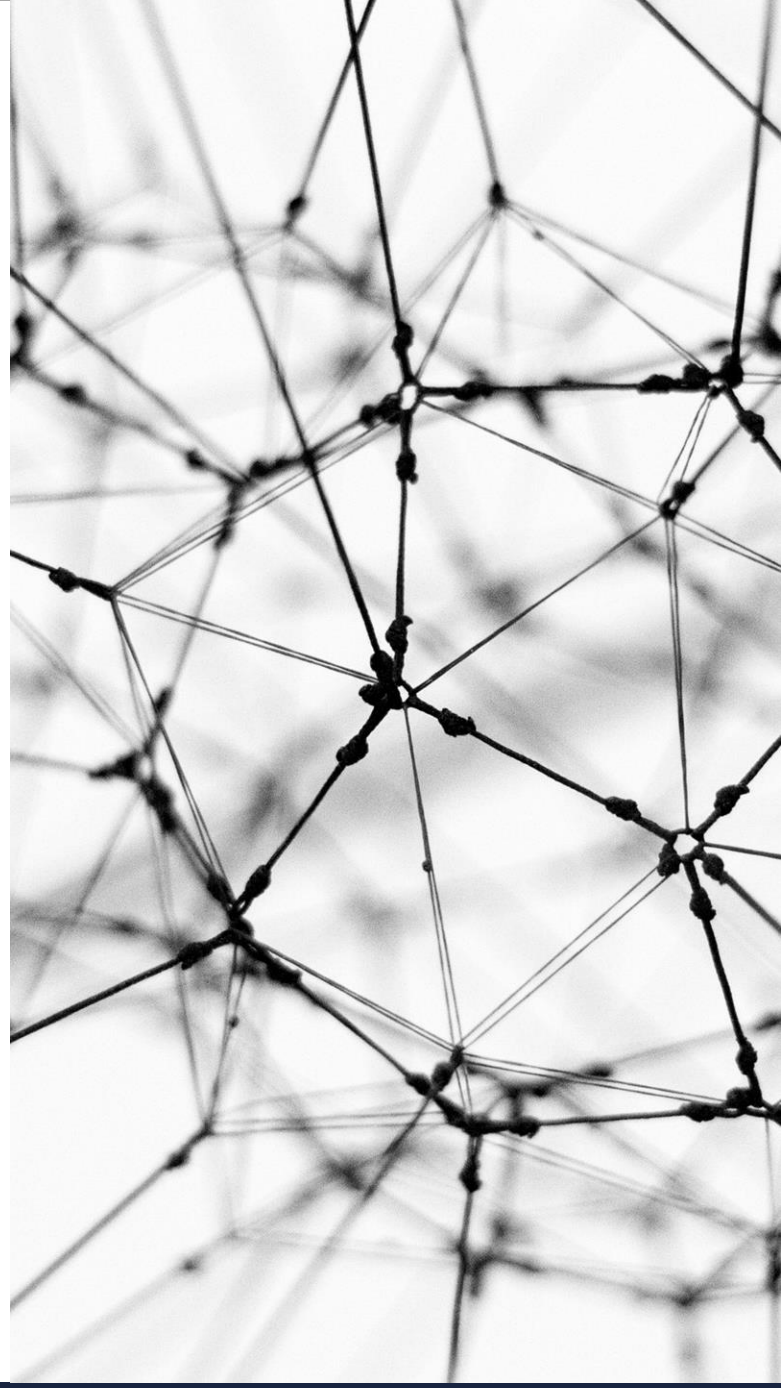
> *Richard Horne, a cyber security partner at PwC, explains how Russian hackers breached a software provider in Ukraine called MeDoc and inserted a "back door" into its next software update. 'Once that was inserted then the attackers could download their malicious code - a brilliant piece of code - which then spread within about 60 minutes,' adds Mr Horne.*
>
> The Financial Times Limited, 12 July 2018

Our response – crisis management

- The full Gold team met within one hour to receive updates and discuss strategy and continued to meet regularly
- Leadership began communicating internally, cascading messages through senior leadership via WhatsApp and Town Hall meetings
- Engaged specialist crisis management consultancy, Regester Larkin by Deloitte
- Legal, Risk & Compliance team, and lawyers in DLA Piper's data protection, privacy and cybersecurity practice, were consulted to provide advice on legal obligations, communications, response efforts and forensics investigation
- Engaged PwC to provide emergency support
- Transition from Gold team to Steering Committee comprising representatives from the Board and the Executive to co-ordinate day to day recovery

The recovery

- Initial focus was on establishing reliable global communications. WhatsApp became the default platform. Broadcast SMS was also used extensively in some regions
- From inception, the guiding principle was to make a secure recovery which would withstand future scrutiny (balancing speed with sustainability)
  IT and business priorities in the early stages were focused on recovering:
  - Email (4 days)
  - Document management (7 days)
  - Desktop/Laptop reimaging and Guest wireless (2 weeks)
  - Finance systems (3 weeks)
  - Remote working – incl. laptop encryption and 2FA (3 weeks)
  - Full telephony (5 weeks)
  - Payroll



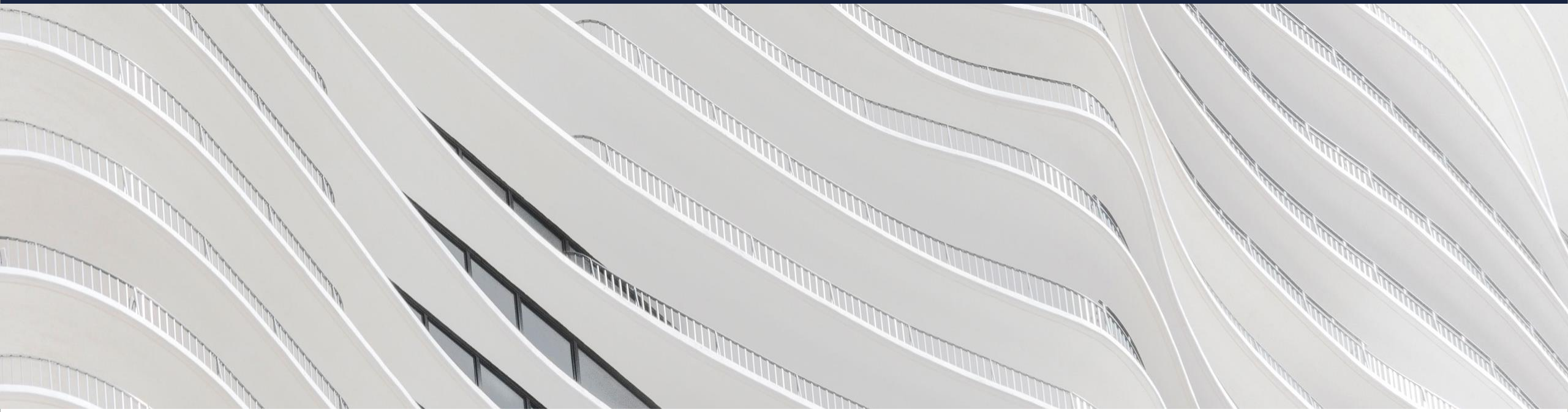
The recovery continued…

- During the first two weeks staff worked:
  - Onsite using *”off network”* computers (firm and personal) and mobile hotspots
  - Using business centres that were established *”off network”* in every office to provide basic computing, file sharing and printing services
- To the end of August (2 months):
  - IT operated 24/7
  - DLA Piper IT staff worked an additional 15,000 hours overtime (most of that in the first 3 weeks). Consultants and contractors were also used extensively

Improving our systems for the future

- Moving to Cloud-based email and document management systems – implemented alternative ”ff system” applications for use in emergency (e.g. Mimecast)
- xMatters emergency messaging system implemented to enable SMS messages
- Working with PwC cyber team on improving governance and controls
- Accelerated Windows 10 roll-out (which would not have prevented the attack)
- Reviewed alternative “emergency” or back up systems for key applications (e.g. document management system, voice, printing)
- Improved security controls built into recovered infrastructure and applications
- Segregation of Ukraine
- More stringent controls over use of administration credentials
- Enhanced network monitoring
- More rigorous supply chain management and review of third party applications

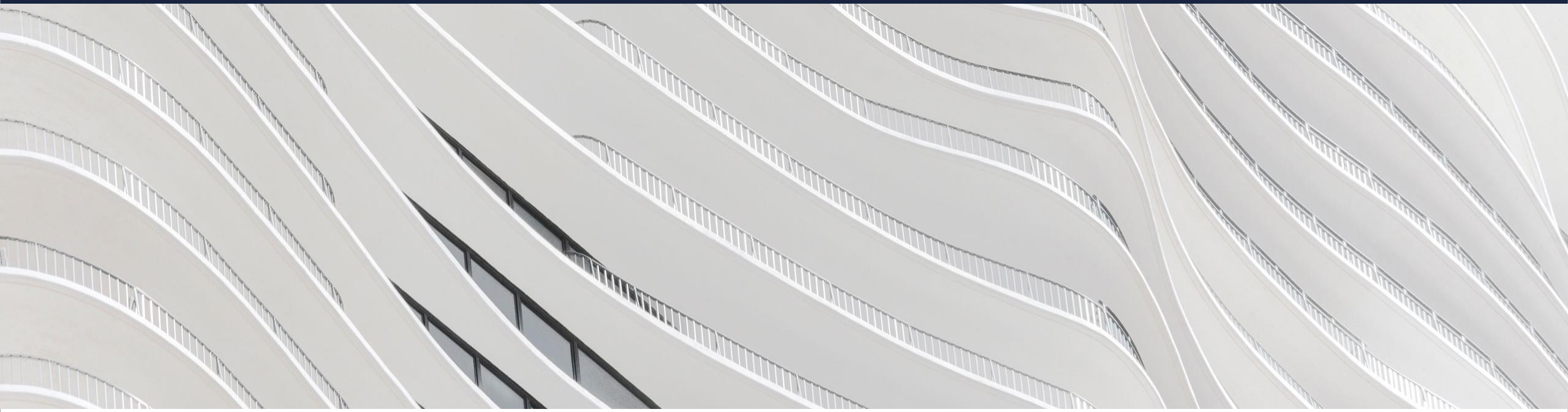
How did we work during the incident?



We found a way through: practical solutions to keep working

- Agreed protocols with clients regarding personal devices
- WhatsApp groups for communication
- Personal email usage for limited period (with client consent) and strict transfer protocols to get data back to DLA Piper systems
- Great support from clients and other law firms – working from client's or other law firm's offices, using their laptops, printers etc.
- Local business centres established
- Meeting with clients during the incident to explain what was happening and capitalise on the time available for relationship management
- Written time sheets
- Electronic banking ensured payroll and client funds transfers were still processed
- Working from the office encouraged to improve internal communication and team morale

What have we learned?



Learning from our experience

- A real cyber attack is nothing like a practice scenario! But it's important you practice what to do when it happens – make it as realistic as possible
- Need clear communication protocols (internal and external), particularly across multiple offices/countries
- Provide the IT team with "air cover" to give it the space to deal with the problem
- Ensure cyber incident response plan includes clearly defined working processes for when **all** IT systems are down
- Practical things are really important, like having a "grab bag" of essentials in each location
- Appoint cyber response advisers and embed them in the team – before it happens – if you have cyber insurance, ensure you can use your chosen advisers

Learning from our experience

- If there is an incident, involve your third party advisers immediately.
- Third party vendors – ensure you have the right relationships so you can get attention from the right resources.
- Give senior leadership access to external help to maintain perspective.
- Leadership (at every level of the organisation) is important. Humans respond to a crisis, not plans.
- Collaboration – working with the National Cyber Security Agency (NCSC) part of GCHQ in the UK in helping shape their cyber security offering to the Legal Industry.

Håndtering af sikkerhedsbrud

Hvorfor, hvornår og hvordan skal et sikkerhedsbrud anmeldes?

Under GDPR

Nu …

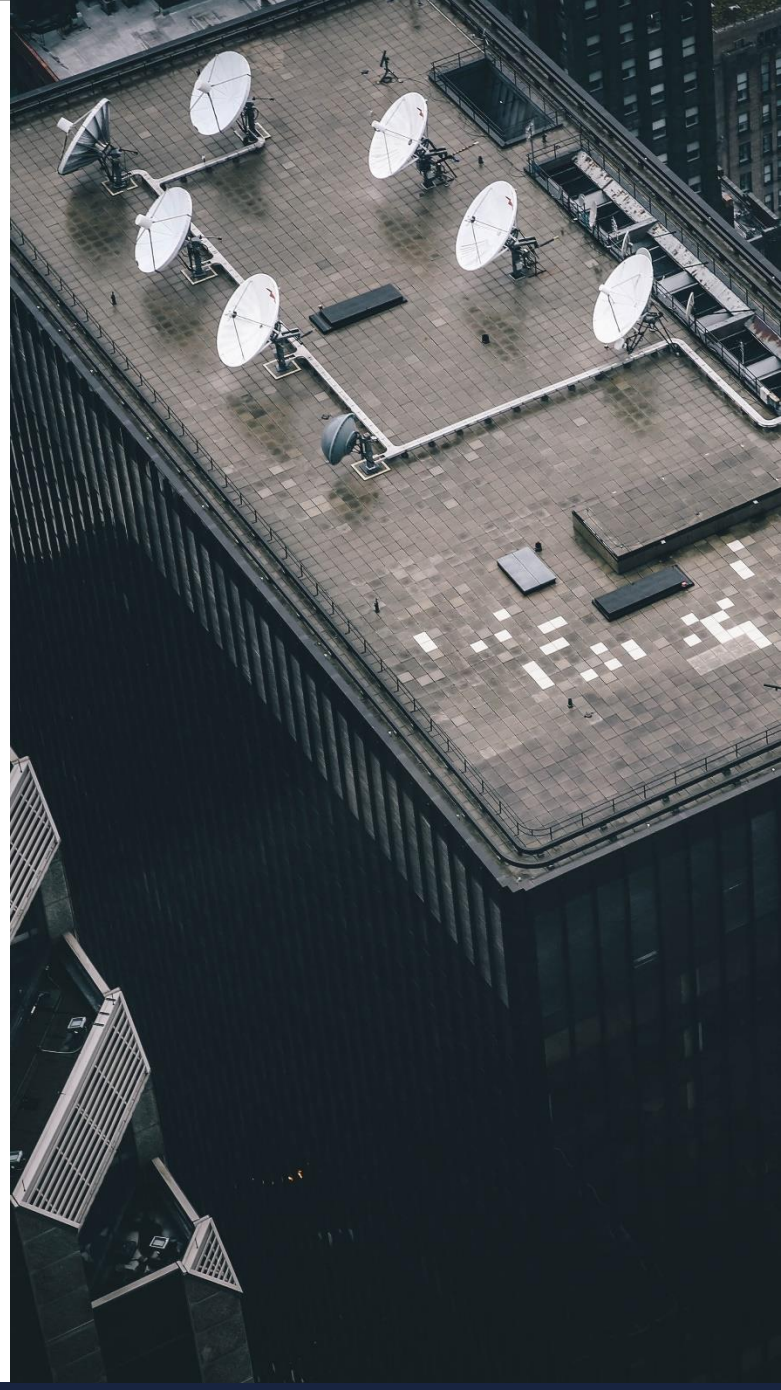
- GDPR trådte i kraft den 25. maj 2018
- Obligatorisk anmeldelsespligt af sikkerhedsbrud under visse omstændigheder
  - Både til Datatilsynet og til de registrerede
- Supplerer eventuelle eksisterende anmeldelses- og underretningspligter
- Anmeldelse til Datatilsynet sker via virk.dk

Anmeldelse af sikkerhedsbrud

GDPR artikel 4

Definitioner

- "*personoplysninger*" er enhver form for information om en identificeret eller identificerbar fysisk person ...
- "*brud på persondatasikkerheden*" er et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet



Oversigt over underretningsforpligtelser

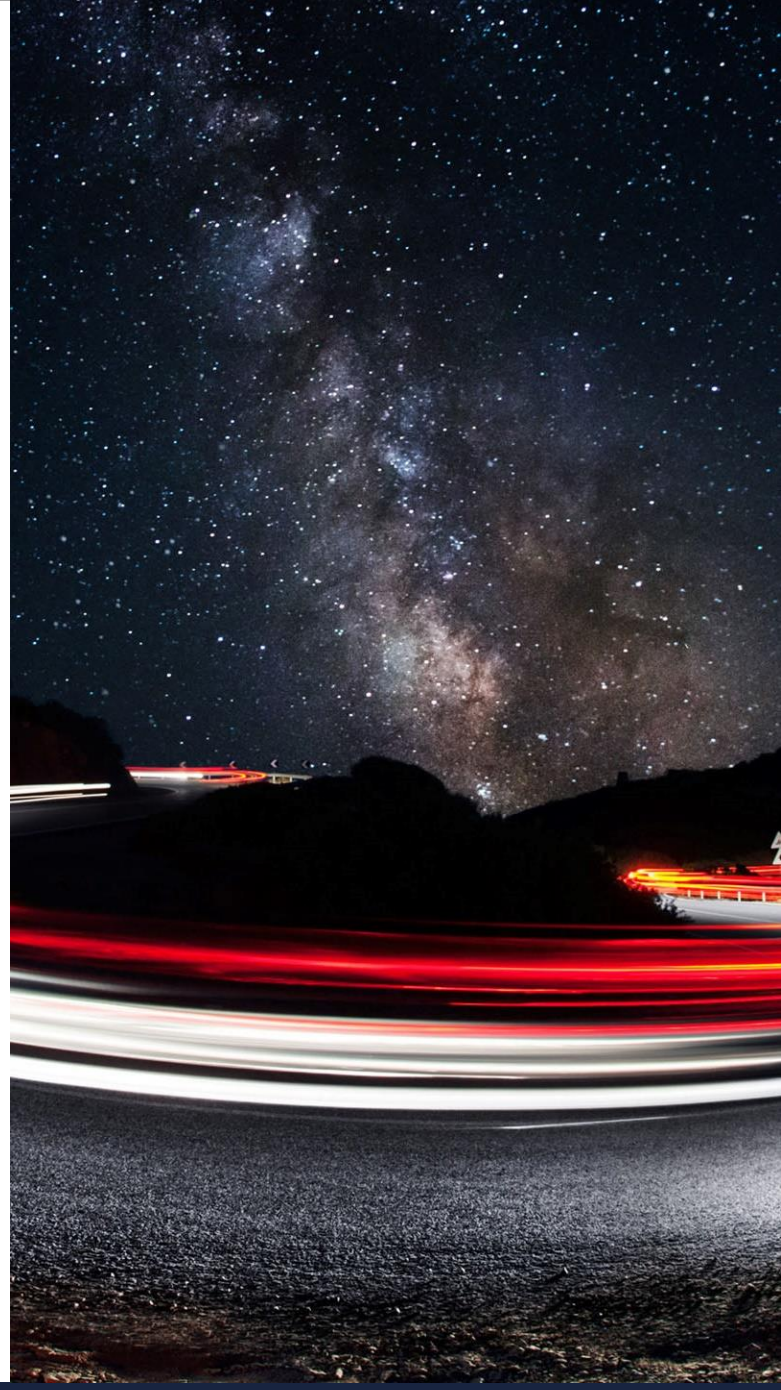
	GDPR	NIS	Børsnoterede selskaber	Telesektoren	Den finansielle sektor
Omfattede enheder	Dataansvarlige og databehandlere	Operatører af væsentlige tjenester inden for digital infrastruktur og udbydere af digitale tjenester	Børsnoterede selskaber	Telesektoren og virksomheder, som er omfattet af telelovgivningen	Udbydere af betalingstjenester og virksomheder, der udsteder elektroniske penge mv.
Pligten udløses af	Et "brud på persondatasikkerheden, der fører til utilsigtet eller uretmæssig ødelæggelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger …"	Hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som leveres	Oplysninger, der betragtes som "intern viden"	"tilstrækkeligt kendskab til, at en sikkerhedshændelse er indtruffet"	"større drifts- og sikkerhedshændelser"
Tidsfrister for underretning	"Uden unødig forsinkelse" og senest inden for 72 timer	"Hurtigst muligt"	"Hurtigst muligt", medmindre der er hjemmel til at udsætte offentliggørelsen	Inden for 24 timer	"Snarest muligt" og senest inden for 4 timer
Underretning til fysiske personer	Ja, hvis sikkerhedsbruddet sandsynligvis vil resultere i en stor risiko for de berørte personers rettigheder og frihedsrettigheder	Erhvervsstyrelsen kan oplyse offentligheden, hvis offentlig opmærksomhed er nødvendig, eller hvis oplysning er i almenhedens interesse	Ikke relevant	Ja, hvis bruddet på persondatasikkerheden kan forventes at krænke privatlivets fred for en fysisk person	Ja, hvis drifts- og sikkerhedshændelsen direkte eller indirekte har eller kan få indvirkning på brugeres økonomiske interesser
Underretning skal ske til	Datatilsynet	a) Erhvervsstyrelsen og b) Center for Cybersikkerhed	a) Offentliggørelse via selskabsmeddelelse b) Finanstilsynet, hvis offentliggørelsen udsættes	Erhvervsstyrelsen	Finanstilsynet

Anmeldelse af sikkerhedsbrud

GDPR artikel 33

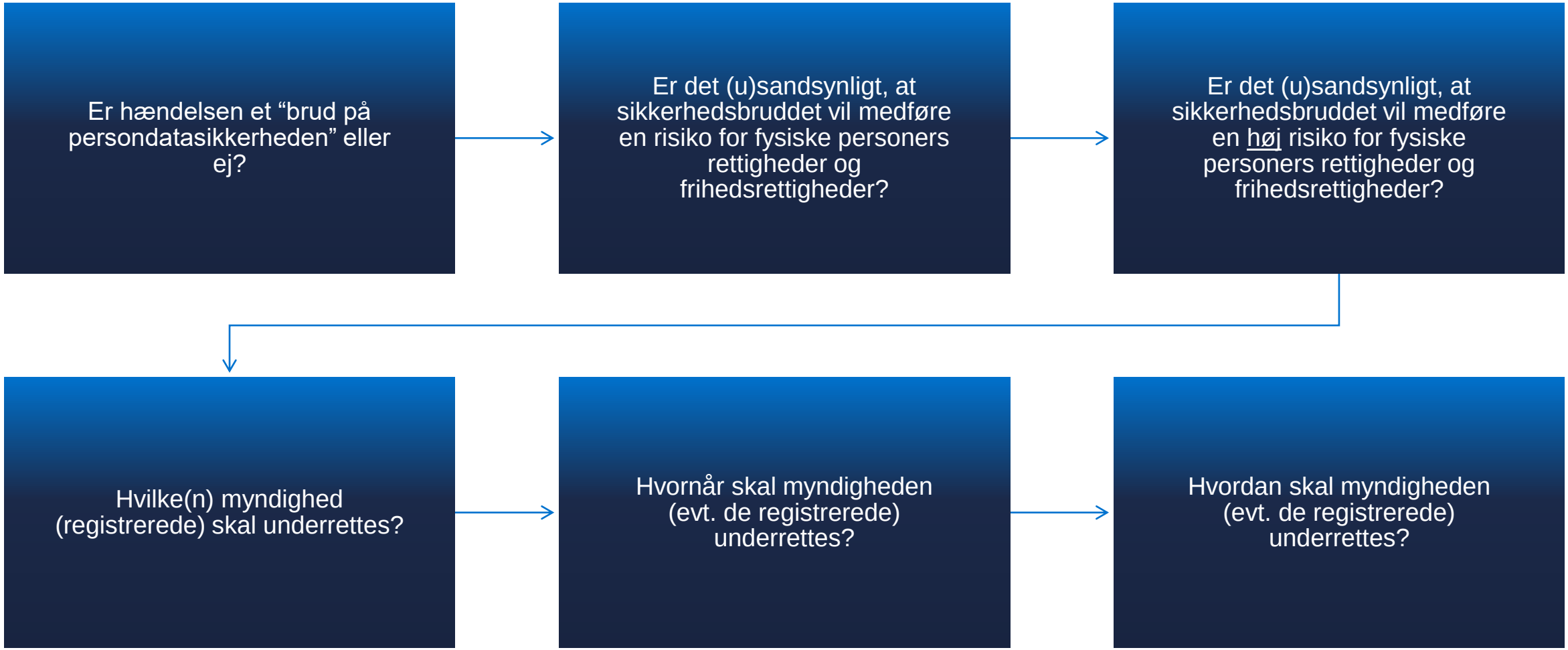
Anmeldelse til Datatilsynet

- Den dataansvarlige skal anmelde bruddet på persondatasikkerheden …
- … uden unødig forsinkelse og om muligt senest 72 timer …
  - (hvis anmeldelse ikke kan ske inden for 72 timer, skal den ledsages af en begrundelse for forsinkelsen)
- … efter at denne er blevet bekendt med det,
- … medmindre bruddet på persondatasikkerheden sandsynligvis ikke indebærer risiko for fysiske personers rettigheder eller frihedsrettigheder
- Selv hvis sikkerhedsbruddet ikke anmeldes, skal det dokumenteres i en log



Anmeldelse af sikkerhedsbrud

Oversigt over de juridiske udfordringer



Anmeldelse af sikkerhedsbrud

Hvorfor anmelde sikkerhedsbrud?

- Anmeldelsespligten skal sikre, at den dataansvarlige håndterer sikkerhedsbruddet på ansvarlig vis
- Bødeloft for manglende anmeldelse er på EUR 10 mio. eller 2 % af den årlige globale omsætning
- Sanktionerne (herunder størrelsen på en eventuel bøde) afhænger blandt andet af, hvordan Datatilsynet er blevet opmærksom på sikkerhedsbruddet

Anmeldelse af sikkerhedsbrud

Kategorisering af brud på persondatasikkerheden

- EDPB kategoriserer sikkerhedsbrud i tre grupper i henhold til følgende tre velkendte principper for informationssikkerhed:
  - "*Brud på fortrolighed*" – dvs. en uautoriseret eller utilsigtet videregivelse af eller adgang til personoplysninger.
  - "*Brud på integritet*" – dvs. en uautoriseret eller utilsigtet ændring af personoplysninger.
  - "*Brud på tilgængelighed*" – dvs. et uautoriseret eller utilsigtet tab af adgang til eller ødelæggelse af personoplysninger.
- Et sikkerhedsbrud kan omfatte brud på fortrolighed, integritet og tilgængelighed hver for sig såvel som en kombination af disse.

Anmeldelse af sikkerhedsbrud

Vurdering af *"opmærksomhed"*

- Det Europæiske Databeskyttelsesråds (Artikel 29-gruppen) retningslinjer:
  - *Hvornår en dataansvarlig nøjagtigt kan anses for at være "bevidst" om et bestemt brud på persondatasikkerheden* ***afhænger af omstændighederne*** *ved det konkrete brud på persondatasikkerheden. I nogle tilfælde vil det være relativt klart fra starten, at der har været et brud på persondatasikkerheden, mens det i andre tilfælde kan tage lidt tid at afgøre, om personoplysninger er blevet kompromitteret. Dog bør der lægges vægt på* ***hurtig indgriben for at undersøge en hændelse*** *for at afgøre, om personoplysninger faktisk er blevet brudt og i bekræftende fald tage afhjælpende foranstaltninger samt foretage underretning om nødvendigt.*

- *Efter først at blive informeret om et potentielt brud på persondatasikkerheden af en fysisk person kan en medievirksomhed, en anden kilde eller den dataansvarlige, når denne selv har opdaget en sikkerhedshændelse, foretage en* ***kort undersøgelsesperiode for at afgøre, om der faktisk er sket et brud på persondatasikkerheden eller ej.*** *I denne undersøgelsesperiode kan den dataansvarlige* ***ikke betragtes som "opmærksom****". Det forventes imidlertid, at den indledende undersøgelse skal begynde så hurtigt som muligt og med en rimelig grad af sikkerhed fastlægge, hvorvidt der er sket et brud på persondatasikkerheden; en mere detaljeret undersøgelse kan følge derefter.*

Underretning af de registrerede

Hvornår og hvordan skal de registrerede underrettes?

Underretning af de registrerede

GDPR artikel 34

Underretning af de registrerede

- Når et brud på persondatasikkerheden sandsynligvis vil indebære en **høj** risiko for fysiske personers rettigheder og frihedsrettigheder,
- … underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden
- … herunder en beskrivelse af de mulige konsekvenser ved bruddet på persondatasikkerheden; de foreslåede eller trufne afhjælpende foranstaltninger for at imødegå bruddet på persondatasikkerheden, herunder eventuel afbødning

Underretning af de registrerede

“risiko for fysiske personers rettigheder og frihedsrettigheder"

- Vurdering af risiko – den traditionelle måde og den persondataretlige måde
- Kan alle registrerede, der er påvirket, kategoriseres i samme klasse? Er de alle udsat for den samme risiko?
- Ud over bøder kan manglende eller forkert underretning af registrerede medføre erstatningsansvar
    - Sørg for, at underretning til de registrerede sker korrekt

Underretning af de registrerede

Eksempler på vurdering fra WP250

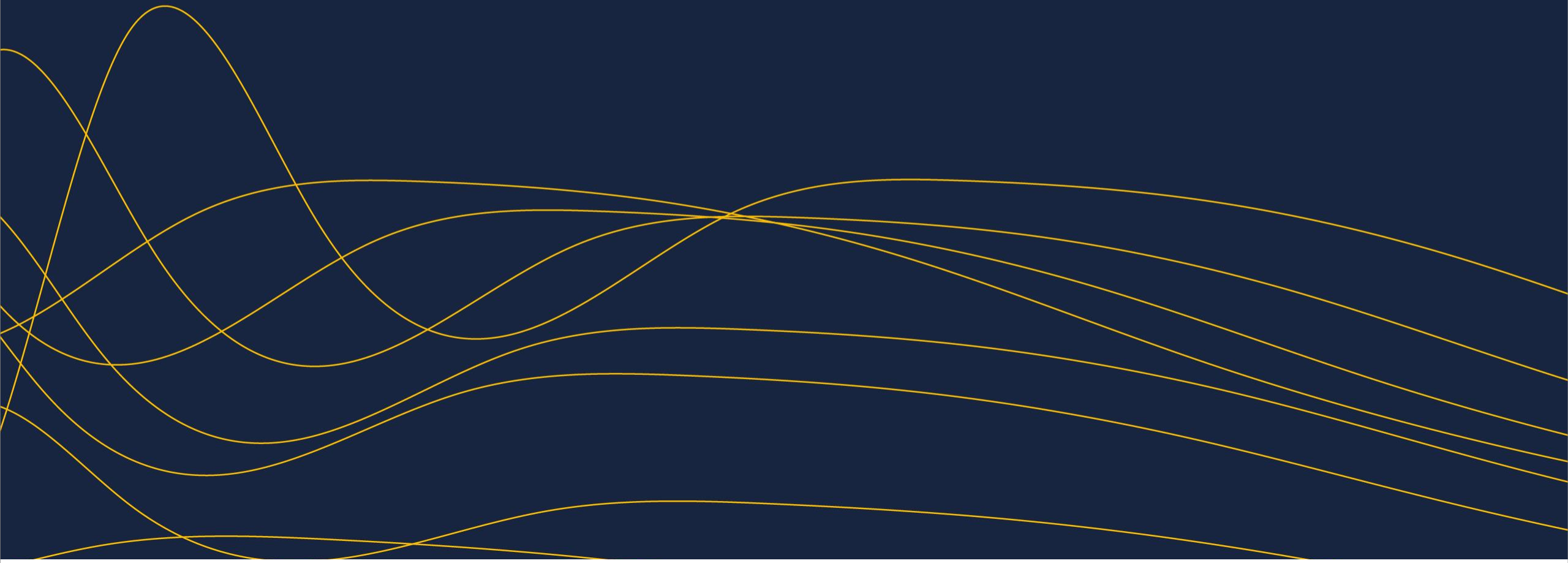
- På et hospital kan det indebære en risiko for personers rettigheder og frihedsrettigheder, hvis kritiske helbredsoplysninger om patienter ikke er tilgængelige, selv midlertidigt. Det kan f.eks. betyde, at operationer bliver aflyst, og at menneskeliv bringes i fare.
- Omvendt er det usandsynligt, at det forhold, at en medievirksomheds systemer ikke er tilgængelige i nogle timer (f.eks. på grund af en strømafbrydelse), og at virksomheden derfor ikke kan sende nyhedsbreve ud til sine abonnenter, indebærer en risiko for personers rettigheder og frihedsrettigheder.
- Ransomware-inficering (skadelig software, som krypterer den dataansvarliges data, indtil der betales en løsesum ("ransom")) kan medføre midlertidigt tab af tilgængelighed, hvis dataene kan gendannes fra backuppen. Der har imidlertid fundet en netværksindtrængen sted, og anmeldelse kan være påkrævet, hvis hændelsen kvalificeres som et brud på fortroligheden (dvs. at angriberen har fået adgang til personoplysninger), og dette indebærer en risiko for personers rettigheder og frihedsrettigheder.

Underretning af de registrerede

Hvordan underretter man?

- Afhænger af omstændighederne
- Kommunikationsmidler kan fx omfatte:
  - E-mail
  - Brev
  - SMS
  - Hjemmeside
  - Nyhedsbrev/Print

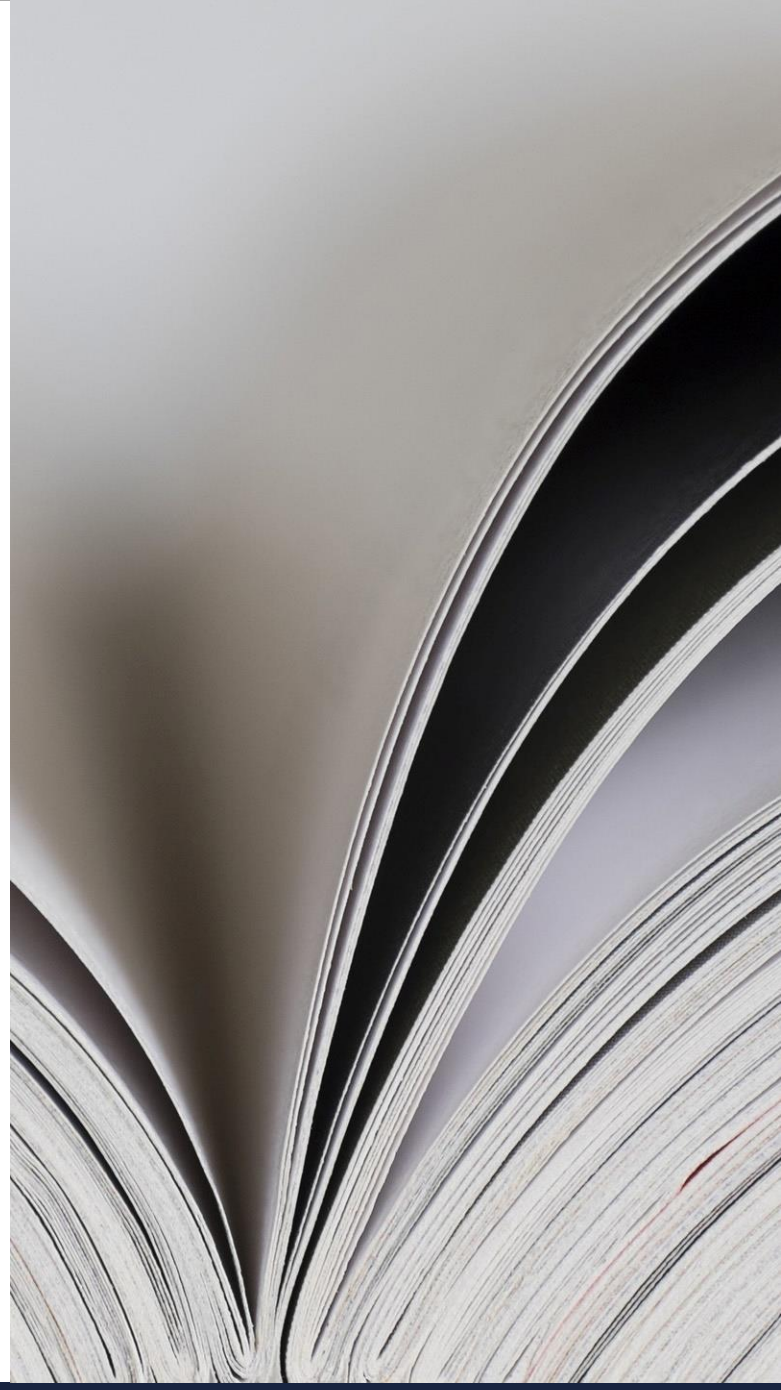
Afsluttende tips og tricks



Nyttige tips og tricks

Politikker og planer

- En synlig og indøvet politik for håndtering af sikkerhedsbrud og beredskabsplan er essentiel
  - Når et sikkerhedsbrud sker, er tiden kritisk!
  - Medarbejdere bør løbende påmindes om disse politikker og planer, som jævnligt bør opdateres
  - Intern træning er et krav



Nyttige tips og tricks

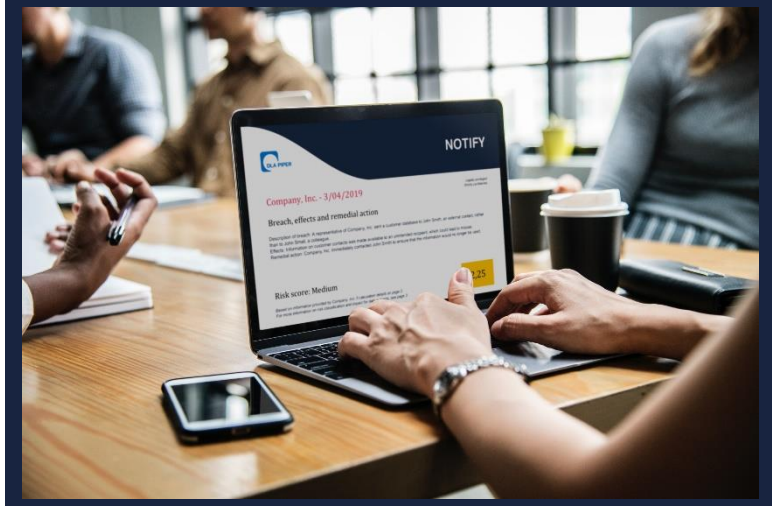
Styring og ledelse

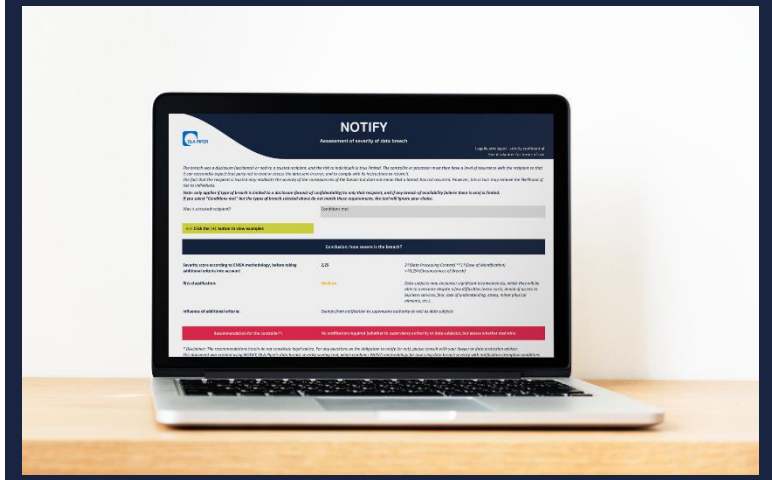
- Sørg for at have et foruddefineret, internt, synligt Incident Response-team på plads til at håndtere og behandle hændelser med brud på persondatasikkerheden
- Teamet bør omfatte CIO (IT-chef) og en direktør, der kan træffe beslutninger/være autoritet på bestyrelsens vegne
  - Inkluder øvrige juridiske og/eller IT-, HR- og PR-rådgivere efter behov
- Sørg for, at de foruddefinerede medlemmer af det interne Incident Response-team løbende rapporterer til den øverste ledelse
- Gå ikke i panik!

DLA Piper Notify

DLA Piper har udviklet et værktøj kaldet Notify. Værktøjet er i stand til at vurdere risikoen forbundet med et sikkerhedsbrud ved brug af en metodik, der er baseret på objektive kriterier fundet i offentligt tilgængelige kilder.

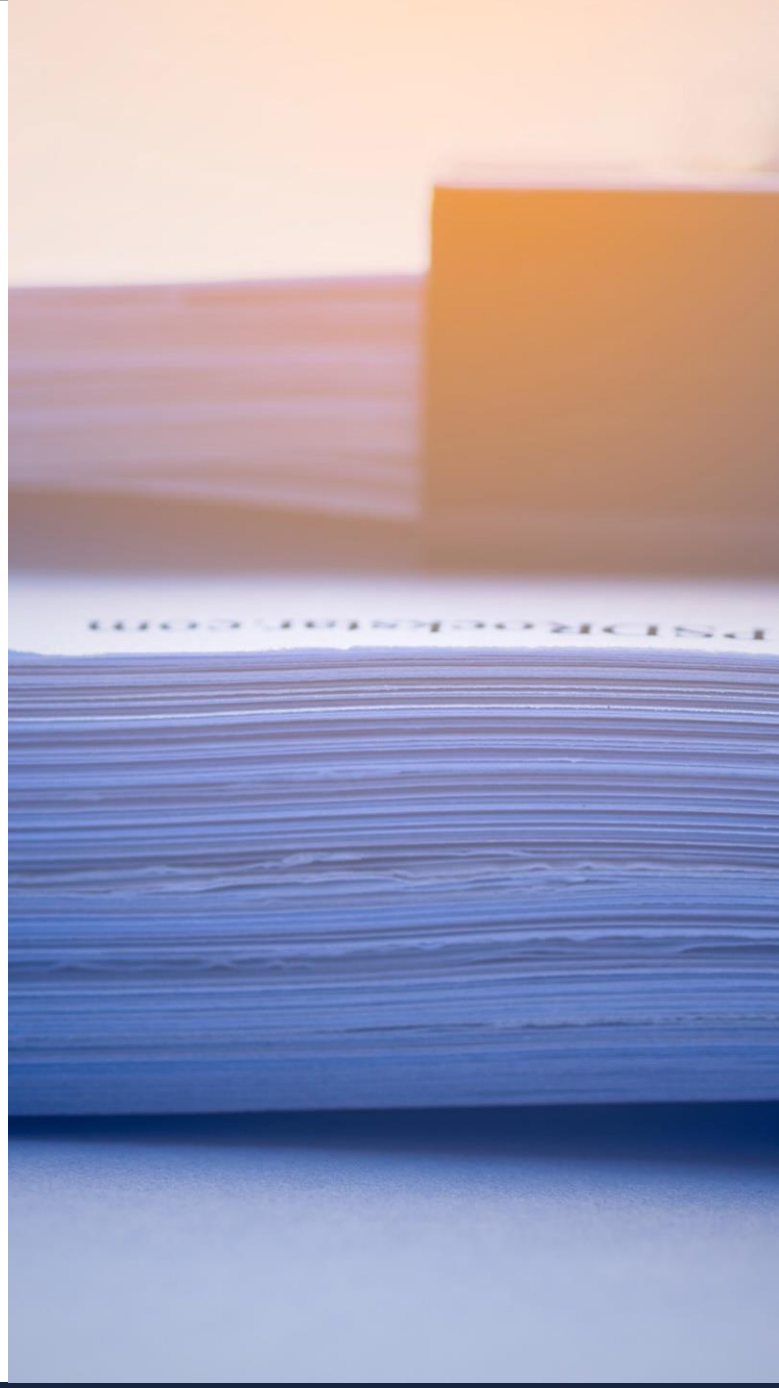
- Kvantitativ tilgang: I stedet for at basere risikovurderingen på løse beslutninger og mavefornemmelse, bruger værktøjet en kvantitativ tilgang og algoritmer, når det måler risikoen forbundet med et sikkerhedsbrud.
- Objektivitet: Kriterierne, der benyttes til at bygge algoritmerne og måle risikoen, stammer fra offentligt tilgængelige kilder såsom GDPR, ENISA (European Network Information Security Agency) og EDBP (Det Europæiske Databeskyttelsesråd).
- Konsistens: Værktøjet tvinger en til at gå igennem en liste af spørgsmål. Værktøjet vurderer alvorligheden baseret på svarene og sikrer dermed en konsistens i vurderingerne, uanset hvem der benytter værktøjet.
- Store tidsbesparelser: Værktøjet kan nedbringe tiden brugt på risikovurderingen fra mange timer til under én time
- Automatisk rapport: Værktøjet genererer automatisk en rapport, der kan benyttes til at dokumentere sikkerhedsbruddet i overensstemmelse med GDPR.





Yderligere dokumenter

- Databeskyttelsesforordningen (GDPR)
- WP29 Retningslinjer for anmeldelse af brud på persondatasikkerheden i henhold til forordning 2016/679 (WP250), som godkendt af EDPB den 25. maj 2018
- ENISA-anbefalinger til en metode til vurdering af alvorligheden af brud på persondatasikkerheden (arbejdsdokument, v1.0, december 2013)
- Vejledning fra de norske databeskyttelsesmyndigheder



Tak!