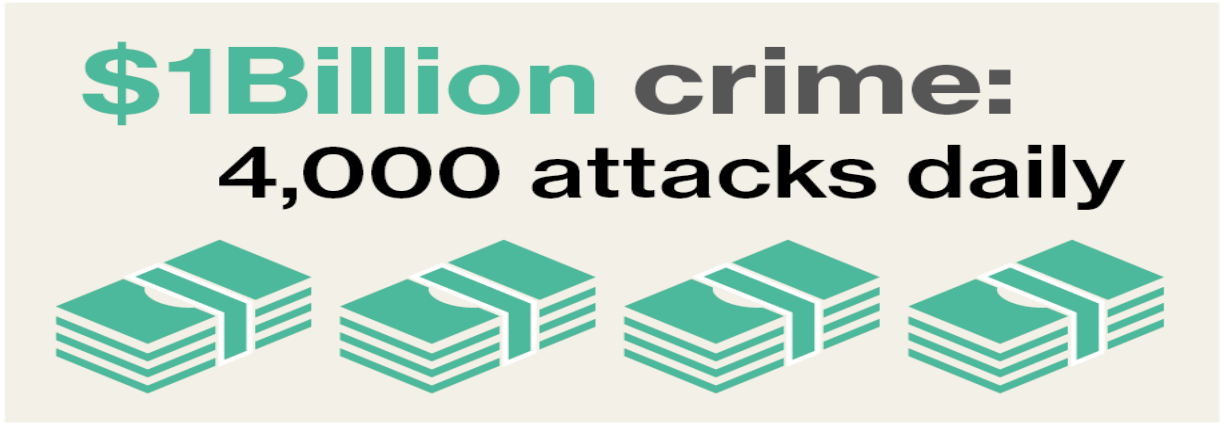
Cybersikkerhed

Willis Towers Watson og IBM kombinerer teknologi og cybereksperti se med risikostyring og forsikring.

11. September 018

Willis Towers Watson

Velkommen!



Cyber Eksponering

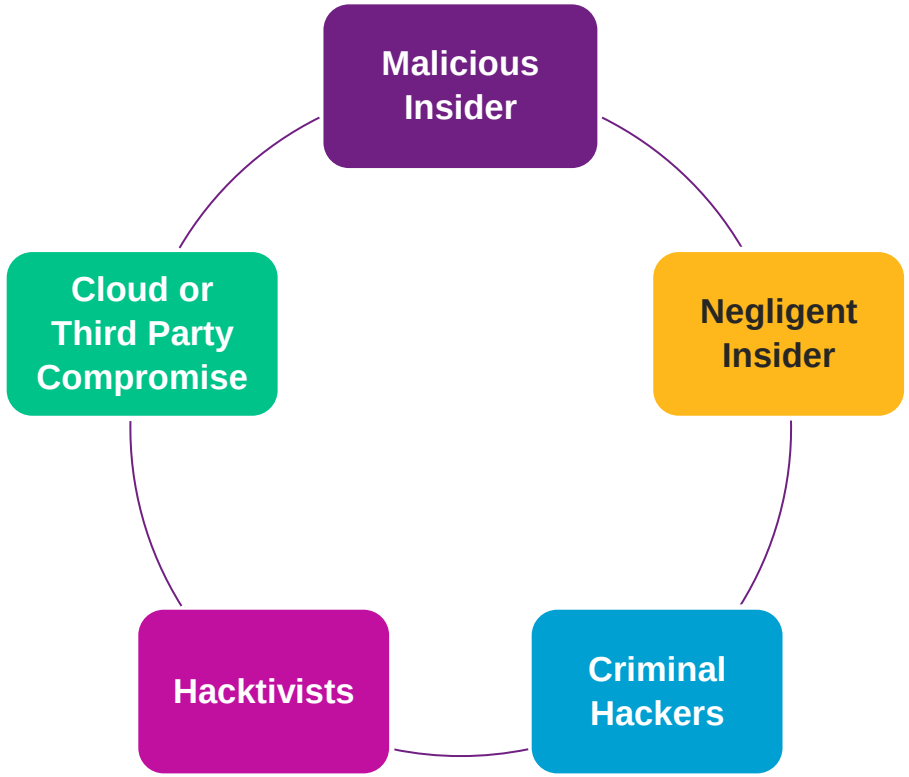
Top 5 årsager til driftstab, som virksomheder frygter mest.

42%	40%	39%	30%	23%
Cyber hændelser	Brand og eksplosion	Natur katestrofer	Leverandør fejl	Teknisk nedbrud af maskiner

Top 3 virksomheds risici på lang sigt (10+ år)

48%	26%	24%
Cyber hændelser	Ny teknologi	Globalt miljø

Source: Allianz Global



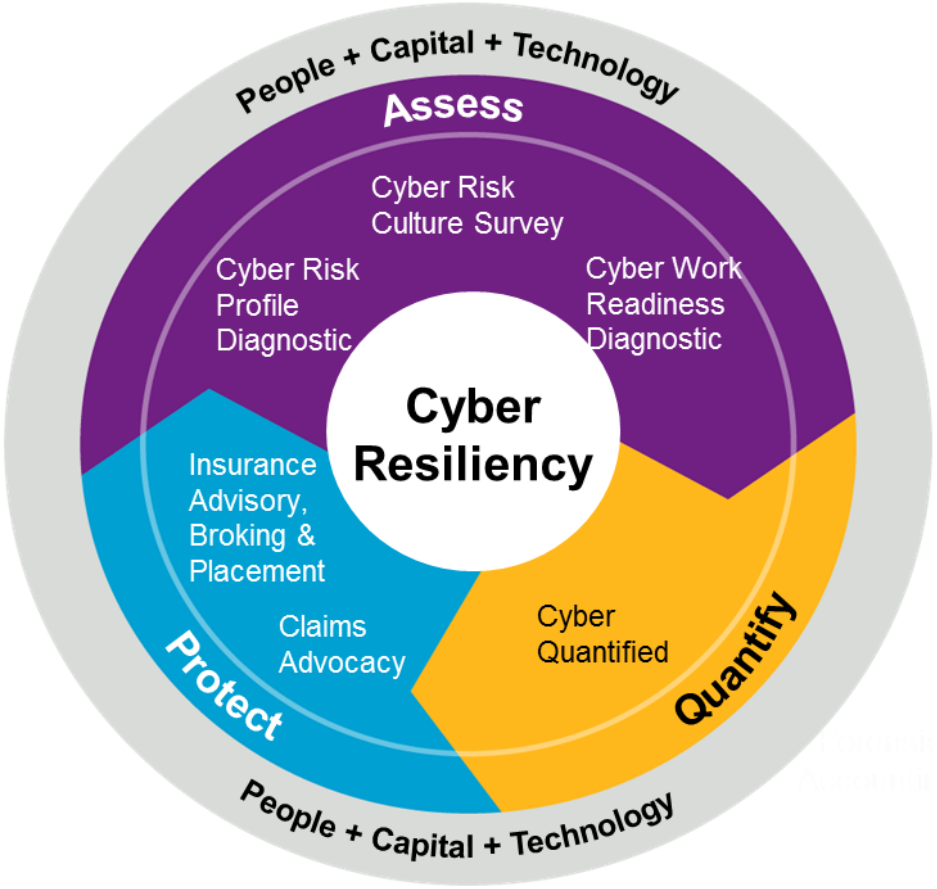
Cyber strategi

Willis Towers Watson har en holistisk tilgang til at forberede jeres cyber resilience

Willis Towers Watson anbefaler, at en robust cyber strategi tager udgangspunkt i følgende:

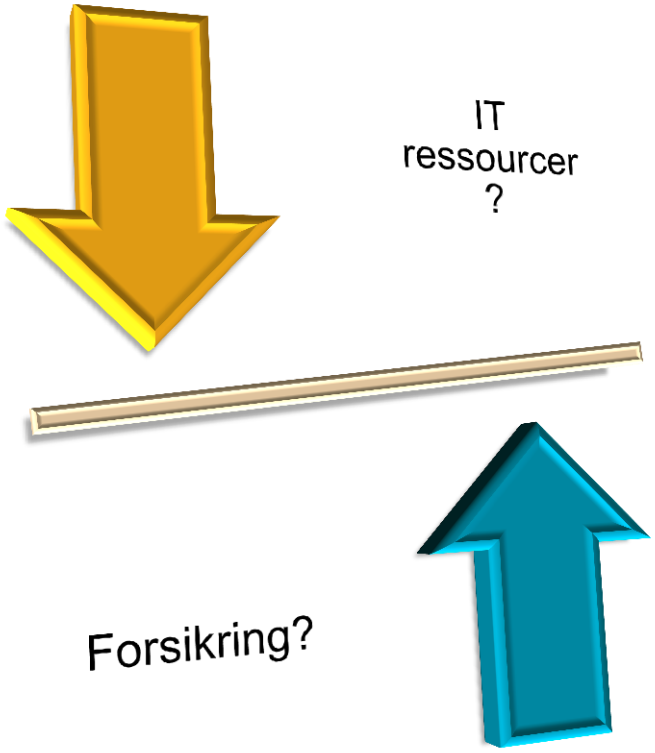
- Assessment = adressering og vurdering af cyber risikoen, risikokultur og risikostyringselementer.
- Quantification = Kvantificering af de økonomiske konsekvenser der følger af et cyberangreb.
- Protect = Beskyttelse, mitigering og financiering af risikoen.

Willis Towers Watson tilbyder en global ekspertrådgivning inden for både forsikring og risikostyring. Desuden har Willis Towers Watson samarbejde med andre partnere for at skabe et bindeled mellem risikostyring, risikofinancering og teknologiske løsninger.



Risikofinansiering og forsikring

Investering i sikkerhed – hvor skal man starte?

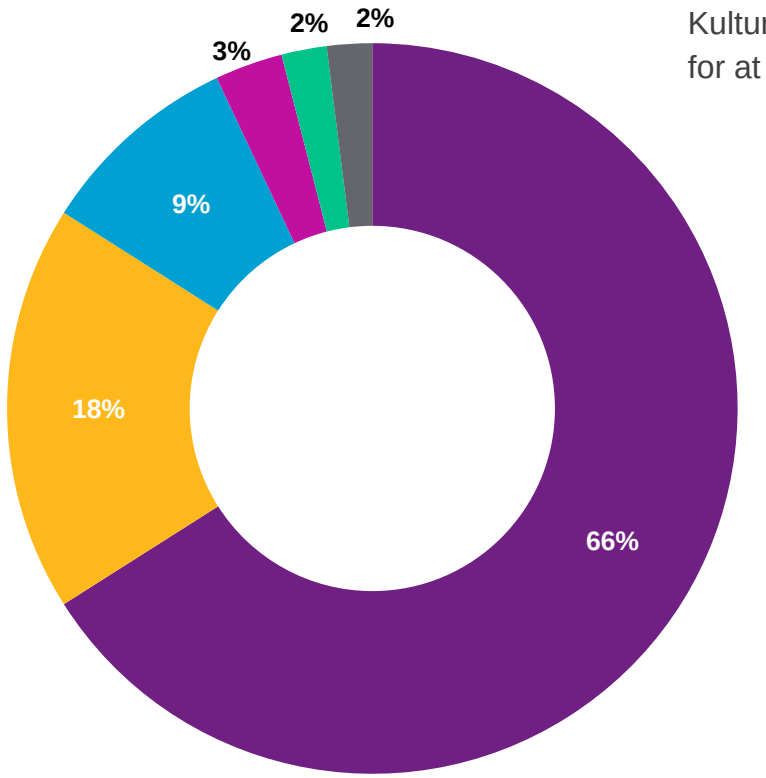


Risikofinansiering og forsikring

Investering i sikkerhed – hvor skal man starte?

Overvej hvilke personer der inddrages I risikovurdering og håndtering:

- IT?
- Jura?
- Salg?
- HR?



Medarbejdere er fortsat den største risiko!

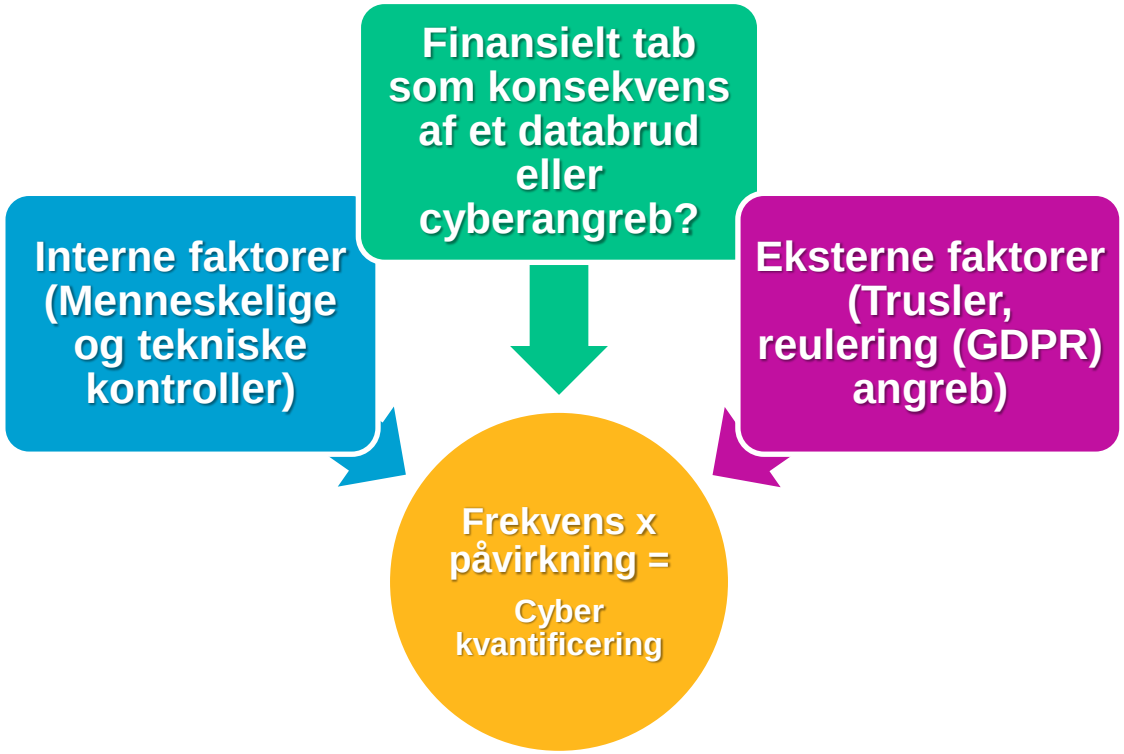
Kultur og medarbejderes engagement påvirker sansynligheden for at blive ramt af et cybernedbrud eller et databrud.

- Employee negligence or malfeasance
- External threat factor
- Other
- Social engineering
- Cyber extortion
- Network business interruption

Risikostyring - kvantificering og prioritering

Hvilke omkostninger indgår i kvantificering?

- IT konsulenter
- Juridiske omkostninger
- Notifikationsomkostninger
- Data genetablering
- Data backup
- Services til kunder/datasubjekter?
- Overvågning af konto og bevægelser?
- PR håndtering
- Driftstab
- Sanktioner (Bøder)
- Kontraktuelle forpligtelser
- Kompensation til kunder/datasubjekter
- Erstatningskrav
- Transportomkostninger



Risikofinansiering og forsikring

Hvad dækker en typisk cyberforsikring?

Når virksomheden oplever en cyberhændelse, som f.eks. :

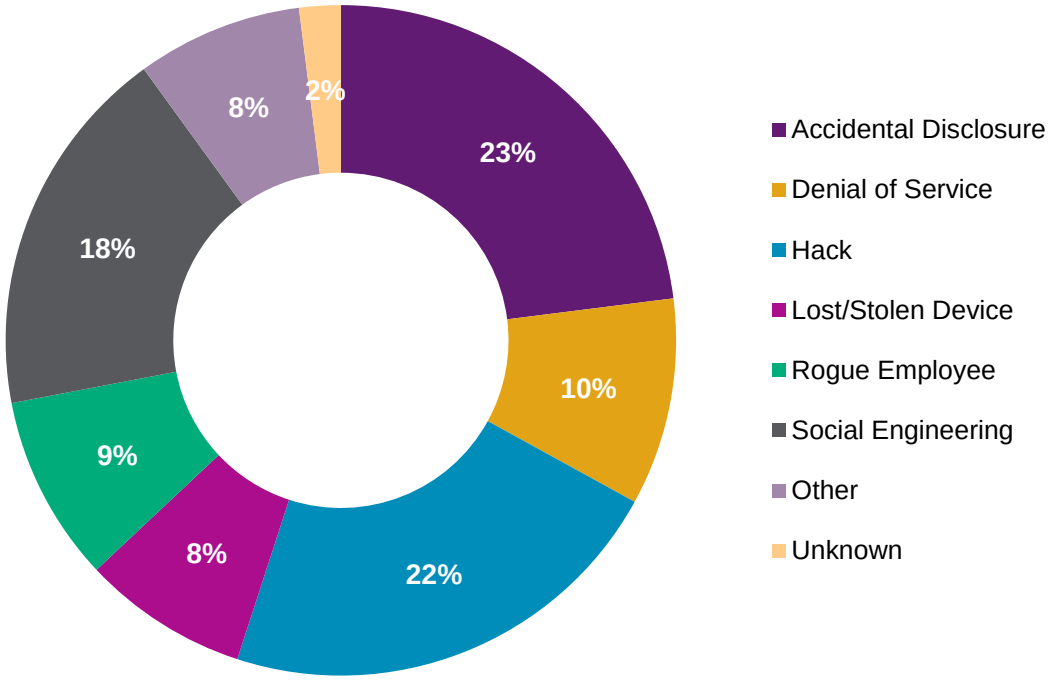
- Ddos angreb
- Netværks-forstyrrelser
- Ransomware
- Data Brud
- Malware/Virus
- Hacking

…vil en cyberforsikring dække følgende:

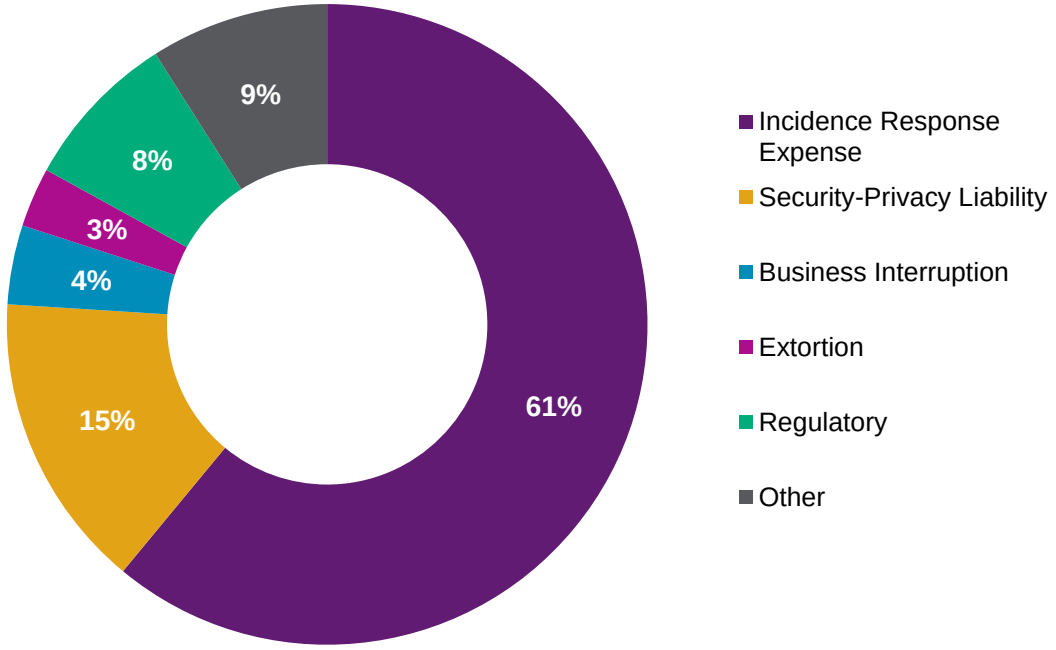
- Krise håndtering
- Ansvar overfor tredjemand
- Sikredes eget tab

Risikofinansiering og forsikring

Type of loss



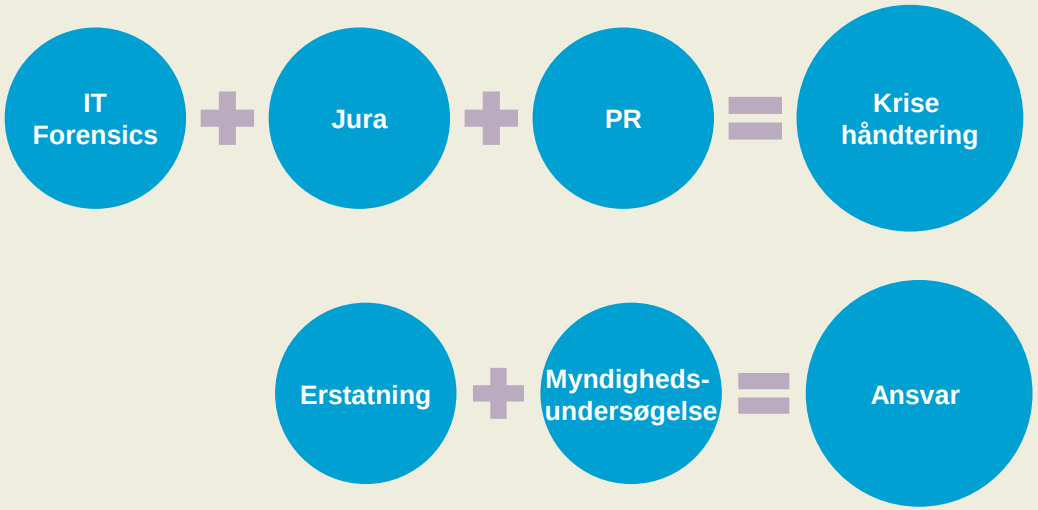
Coverages Implicated



Risikofinansiering og forsikring

Hvordan virker forsikringen, når der sker en skade?

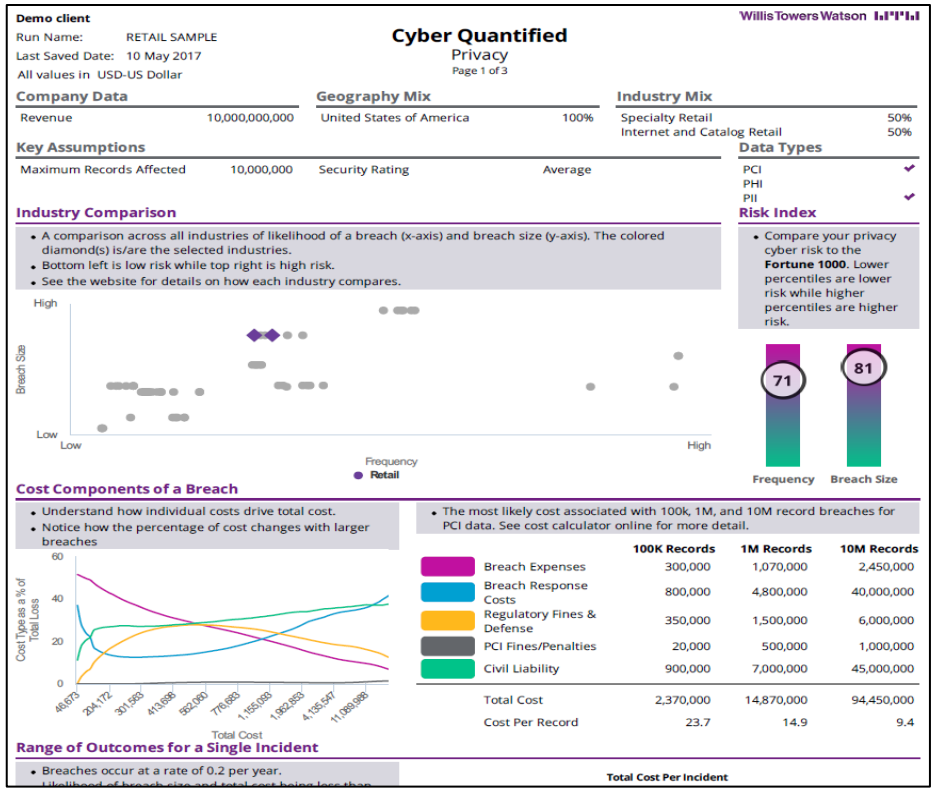
Databrud

Hvad sker der?	Hvilke dækninger er relevante?
[Hacker→ indtrænger virksomheden]  Hackeren skaffer sig adgang til virksomhedens it-system eller netværk. Hackeren får adgang til fortroligt data, der indeholder alle data om ansatte.	Så snart virksomheden indser, at de lider et cyberangreb, så kan de aktivere forsikringen. Typisk gøres dette i første omgang ved at ringe til den hotline, der findes på forsikringspolicen. Derefter har virksomheden adgang til følgende:
[Hacker→ Data → Videresender]  Hackeren downloader det fortrolige data, information og enten vælger hackeren at lægge dataene ud på internettet eller sælger dataene på "the dark web" = **Virksomheden har nu lidt et databrud.**	
[Virksomheden vil nu (most likely) opleve en krise]  ▪ Virksomheden skal straks undersøge, håndtere og begrænse databruddet! ▪ Medierne vil begynde at dække eventet = *DÅRLIG OMTALE.* ▪ De berørte datasubjekter vil forlange en forklaring og eventuelt kompenation. ▪ Virksomheden skal måske forklare skaden til data-tilsynet.	

Risikostyring - kvantificering og prioritering

Dette nye forudsigende værktøj kvantificerer den risiko en organisation står overfor som følge af et databrud eller forkert håndtering af data, der fører til misligholdelse af personers privatliv.

Modellen er den første af sin slags i industrien og måler blandt andet effekten og sandsynligheden for både et data brud og et netværks udfald på grund af en cyberbegivenhed. Desuden kan de finansielle konsekvenser af en sådan begivenhed estimeres i et omfang der har betydning for organisationens risikoplanlægning



Demo client
Run Name: RETAIL SAMPLE
Last Saved Date: 10 May 2017
All values in USD-US Dollar

Willis Towers Watson

Cyber Quantified
Privacy
Page 1 of 3

Company Data

Revenue	10,000,000,000

Geography Mix

United States of America	100%

Industry Mix

Specialty Retail	50%
Internet and Catalog Retail	50%

Key Assumptions

Maximum Records Affected	10,000,000	Security Rating	Average

Data Types

PCI	✔
PHI	
PII	✔

Industry Comparison

- A comparison across all industries of likelihood of a breach (x-axis) and breach size (y-axis). The colored diamond(s) is/are the selected industries.
- Bottom left is low risk while top right is high risk.
- See the website for details on how each industry compares.

Risk Index

- Compare your privacy cyber risk to the **Fortune 1000**. Lower percentiles are lower risk while higher percentiles are higher risk.

Cost Components of a Breach

- Understand how individual costs drive total cost.
- Notice how the percentage of cost changes with larger breaches

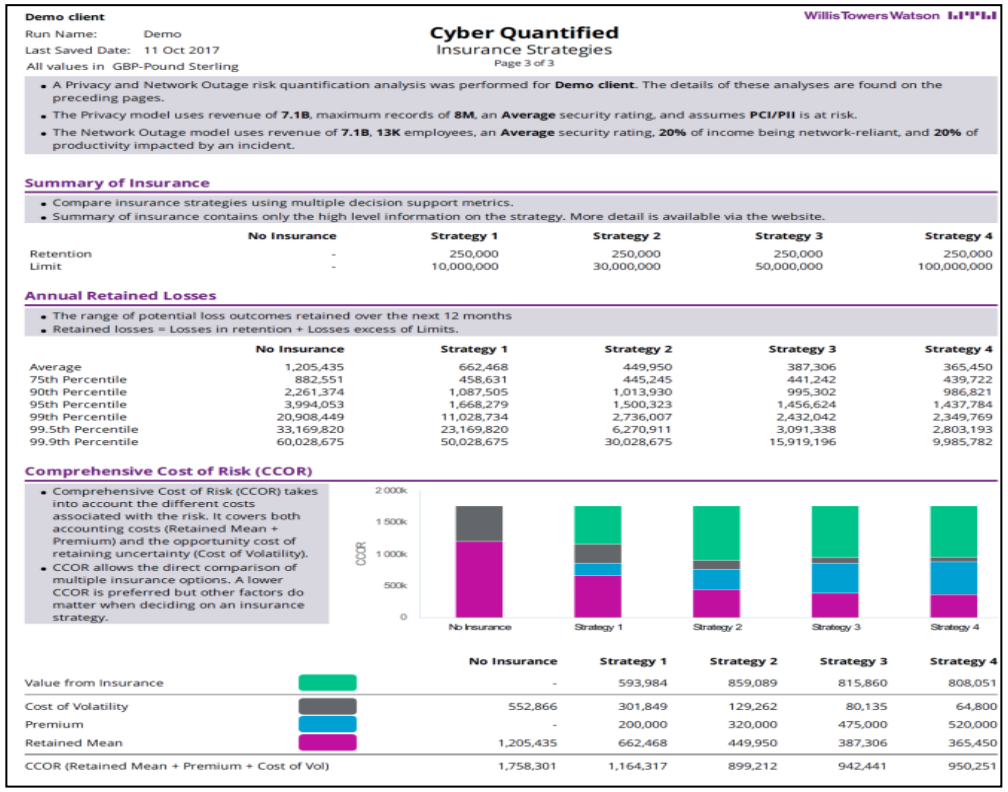
- The most likely cost associated with 100k, 1M, and 10M record breaches for PCI data. See cost calculator online for more detail.

	100K Records	1M Records	10M Records
Breach Expenses	300,000	1,070,000	2,450,000
Breach Response Costs	800,000	4,800,000	40,000,000
Regulatory Fines & Defense	350,000	1,500,000	6,000,000
PCI Fines/Penalties	20,000	500,000	1,000,000
Civil Liability	900,000	7,000,000	45,000,000
Total Cost	2,370,000	14,870,000	94,450,000
Cost Per Record	23.7	14.9	9.4

Range of Outcomes for a Single Incident

- Breaches occur at a rate of 0.2 per year.

Total Cost Per Incident



Demo client
Run Name: Demo
Last Saved Date: 11 Oct 2017
All values in GBP-Pound Sterling

Willis Towers Watson

Cyber Quantified
Insurance Strategies
Page 3 of 3

- A Privacy and Network Outage risk quantification analysis was performed for **Demo client**. The details of these analyses are found on the preceding pages.
- The Privacy model uses revenue of **7.1B**, maximum records of **8M**, an **Average** security rating, and assumes **PCI/PII** is at risk.
- The Network Outage model uses revenue of **7.1B**, **13K** employees, an **Average** security rating, **20%** of income being network-reliant, and **20%** of productivity impacted by an incident.

Summary of Insurance

- Compare insurance strategies using multiple decision support metrics.
- Summary of insurance contains only the high level information on the strategy. More detail is available via the website.

	No Insurance	Strategy 1	Strategy 2	Strategy 3	Strategy 4
Retention	-	250,000	250,000	250,000	250,000
Limit	-	10,000,000	30,000,000	50,000,000	100,000,000

Annual Retained Losses

- The range of potential loss outcomes retained over the next 12 months
- Retained losses = Losses in retention + Losses excess of Limits.

	No Insurance	Strategy 1	Strategy 2	Strategy 3	Strategy 4
Average	1,205,435	662,468	449,950	387,306	365,450
75th Percentile	882,551	458,631	445,245	441,242	439,722
90th Percentile	2,261,374	1,087,505	1,013,930	995,302	986,821
95th Percentile	3,994,053	1,668,279	1,500,323	1,456,624	1,437,784
99th Percentile	20,908,449	11,028,734	2,736,007	2,432,042	2,349,769
99.5th Percentile	33,169,820	23,169,820	6,270,911	3,091,338	2,803,193
99.9th Percentile	60,028,675	50,028,675	30,028,675	15,919,196	9,985,782

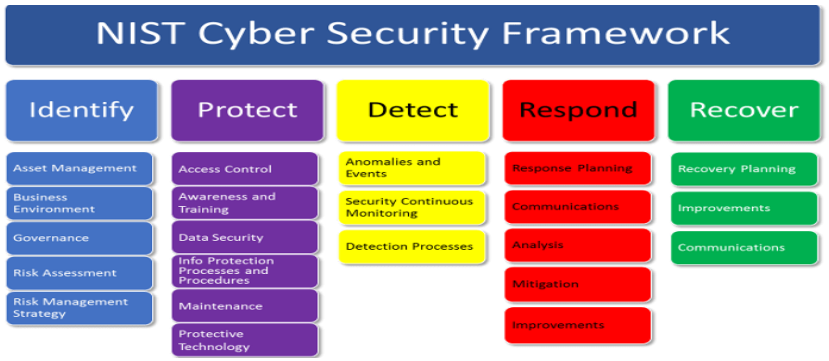
Comprehensive Cost of Risk (CCOR)

- Comprehensive Cost of Risk (CCOR) takes into account the different costs associated with the risk. It covers both accounting costs (Retained Mean + Premium) and the opportunity cost of retaining uncertainty (Cost of Volatility).
- CCOR allows the direct comparison of multiple insurance options. A lower CCOR is preferred but other factors do matter when deciding on an insurance strategy.

	No Insurance	Strategy 1	Strategy 2	Strategy 3	Strategy 4
Value from Insurance	-	593,984	859,089	815,860	808,051
Cost of Volatility	552,866	301,849	129,262	80,135	64,800
Premium	-	200,000	320,000	475,000	520,000
Retained Mean	1,205,435	662,468	449,950	387,306	365,450
CCOR (Retained Mean + Premium + Cost of Vol)	1,758,301	1,164,317	899,212	942,441	950,251

Risikostyring - kvantificering og prioritering
Cyber Risk Profile Diagnostic: Hvad er det?

Benchmarking op imod topstandarder indenfor cybersikkerhed



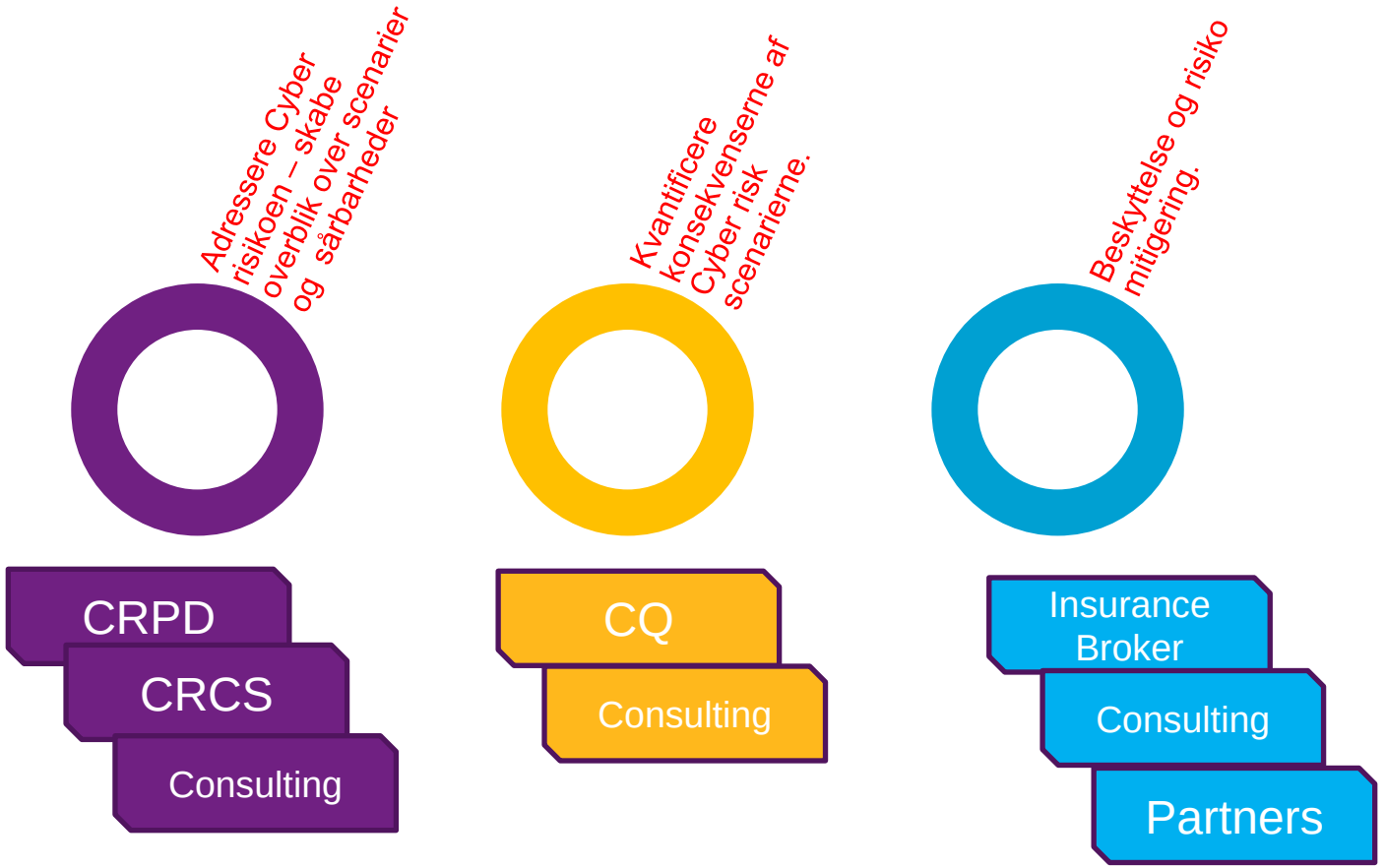
CRPD measures an organization's "cybersecurity maturity" against the ISO27001 and/or NIST Standards

CRPD provides three main outputs during two phases that support the design of informed cybersecurity strategies:

- **On-line Self-Assessment:**
  - Dashboard assessment of an organization's cyber risk posture
- **On-site Workshop:**
  - Risk register developed through deep dive review and prioritization of online assessment results
  - Action Plans based on survey's outcomes, semi-automatic reccomendations and cost/benefit analysis

Løsninger baseret på professionel service, værktøjer og pålidelige partnere

WTW værktøjer, løsninger og professionelle serviceydelser.



IBM Security

Cybersikkerhed
Willis Tower Watson Event

11 SEPTEMBER 2018

Uffe Spohr. Senior Security Consultant
uffespohr@dk.ibm.com
Jackie L Halling, Security Offering Manager
jclh@dk.ibm.com

IBM

IBM Security

https://securityintelligence.com/as-seen-on-tv-important-lessons-for-winning-the-fight-against-cybercrime/

IBM Security

We exist to protect the world, freeing you to thrive in the face of cyber uncertainty

Largest enterprise cybersecurity provider

Leader in 12 security market segments

3,700+ security patents

20+ security acquisitions

60B+ security events monitored per day

Ponemon study shows the true cost of a data breach

Global findings at a glance

$3.86M/6.4% ↑
Average total cost of data breach

$148/4.8%
Average cost per record lost or stolen

24,615/2.2% ↑
Average number of breached records

27.9%
Likelihood of a recurring material breach over two years

477 companies participated
Currency: US dollar

Per-record costs for top three industries

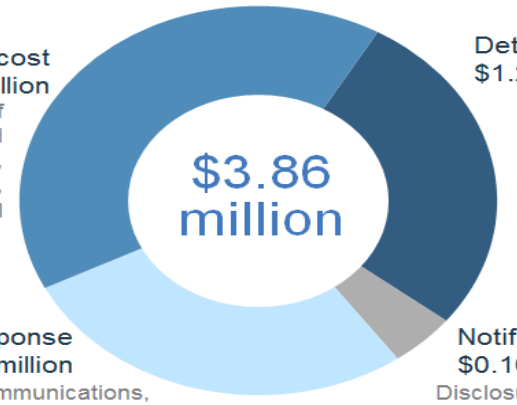
$408 Health

$206 Financial

$181 Services

The largest component of the total cost of a data breach is lost business

Components of the $3.86 million cost per data breach



Lost business cost
$1.45 million
Abnormal turnover of customers, increased customer acquisition cost, reputation losses, diminished goodwill

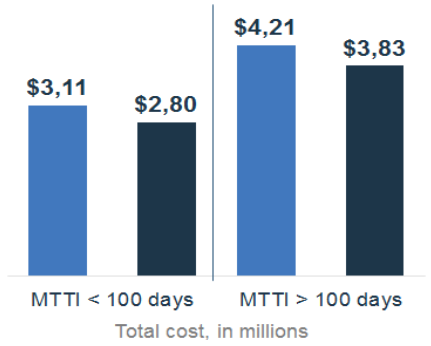
Detection and escalation
$1.23 million
Forensics, root cause determination, organizing incident response team, assessment and audit services

Post-breach response
$1.02 million
Help desk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions

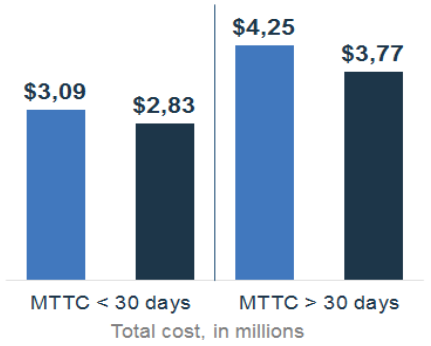
Notification
$0.16 million
Disclosure of data breach to victims and regulators

Gaining visibility and responding faster help to reduce costs

Mean time to identify (MTTI)
(The time it takes to detect that an incident has occurred)



Mean time to contain (MTTC)
(The time it takes to resolve a situation and ultimately restore service)

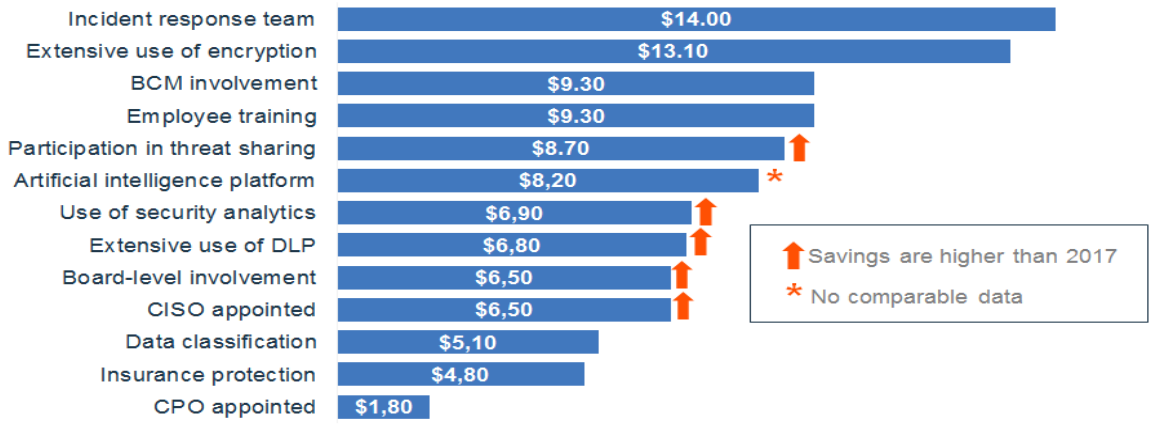


FY 2018 FY 2017

Currencies converted to US dollars

What you can do to help reduce the cost of a data breach

Amount by which the cost-per-record was lowered



The Ponemon study can be accessed here: https://www.ibm.com/security/data-breach

https://www.ibm.com/security/data-breach

IBM's 10 Essential Practices provides a board-ready framework for evaluating the security function and defining a security strategy

1 Build a risk and compliance-aware culture and management system

2 Establish intelligent security operations and rapid threat response

3 Secure collaboration in social and mobile workplace

4 Develop security-rich products, by design

5 Manage IT hygienically

6 Create a security-rich and resilient network

7 Address security complexity of cloud and virtualization

8 Manage third-party security compliance

9 Assure data security and privacy

10 Manage the digital identity lifecycle

GOAL:
Intelligent cyber threat protection and risk management

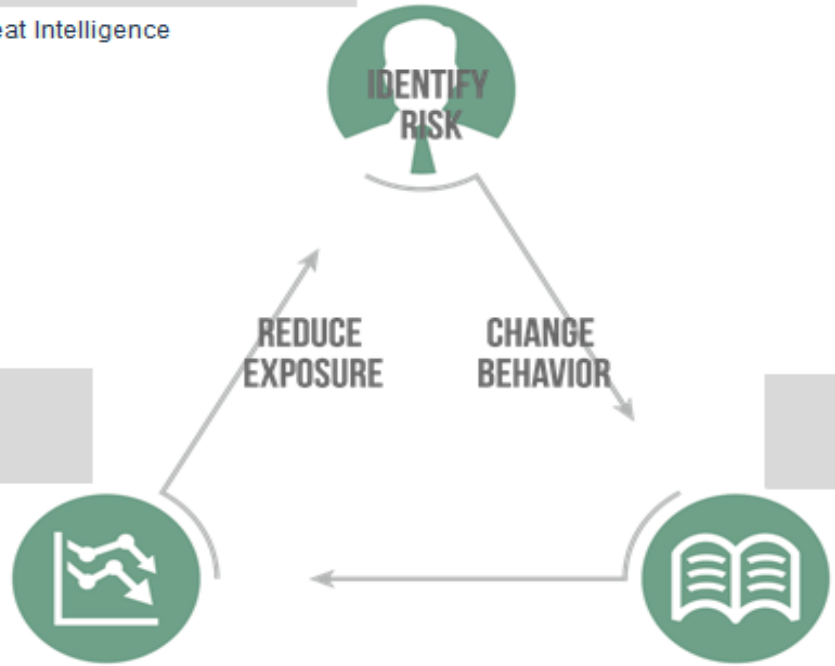
Security Awareness and Training platform
People-Centric Risk Reduction

Global strategic partnership between IBM & Wombat

- Able to deliver Wombat as a managed service solution
- Jointly leveraging best practices to deliver best-in-class security awareness solutions to clients

Identify who is being attacked and evaluate their ability to protect themselves

Proofpoint Threat Intelligence
CyberStrength
ThreatSim



PhishAlarm
PhishAlarm Analyzer
Threat Response Auto-Pull (TRAP)

Knowledgeable end users report potential threats which reduces attack surface

Interactive Training
Awareness Videos and Materials

Deliver training based on actual threats, user behavior, and knowledge gaps

wombat security technologies
Change Behavior. Reduce Risk.

IBM X-Force IRIS uses best practice technologies supported by consulting and services expertise

IBM X-Force IRIS

Incident Response and Intelligence Services

Combines intelligence, incident response, and remediation into one

- **IRIS Vision Retainer**:
- IR Program Assessment & Playbooks
- Tabletop Exercises
- Incident Response & Breach Remediation

- **Cybersecurity Incident Response Planning**
- **Active Threat Assessment**
- **Managed Detection and Response**

- **IBM X-Force Threat Analysis service**
- **X-Force Cyber Threat Intelligence (CTI) Workshop**
- **Strategic Threat Assessment**
- **Threat Impact Analysis**

X-Force Red Penetration Testing across all the technologies you use

Application

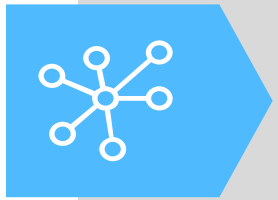
- Web
- Mobile
- Terminal
- Thick-client
- Mainframe
- Middleware

Network

- Internal
- External
- Wireless
- Other radio frequencies
- SCADA

Human

- Physical
- Social engineering
- Phishing

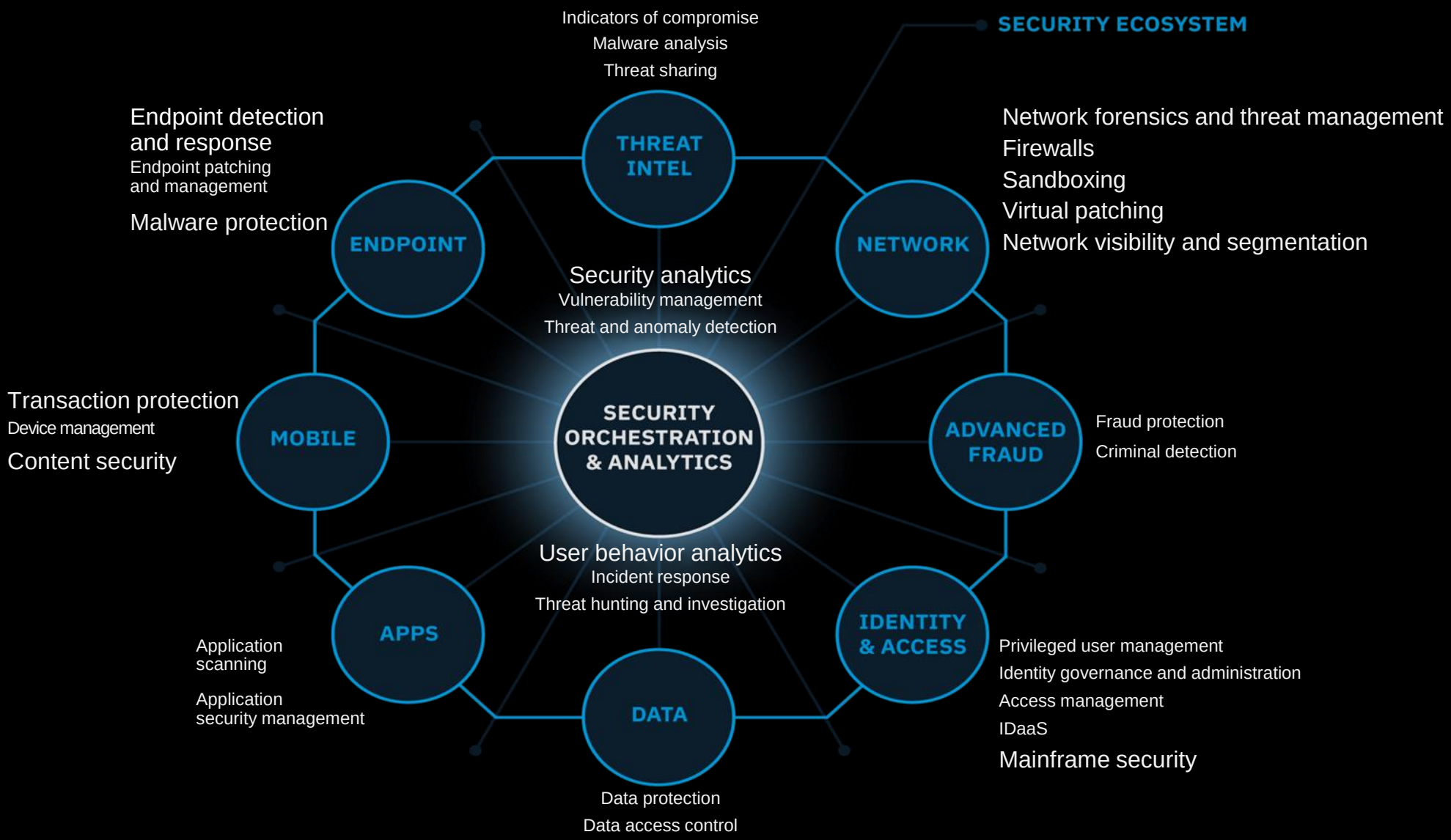


Hardware and embedded devices

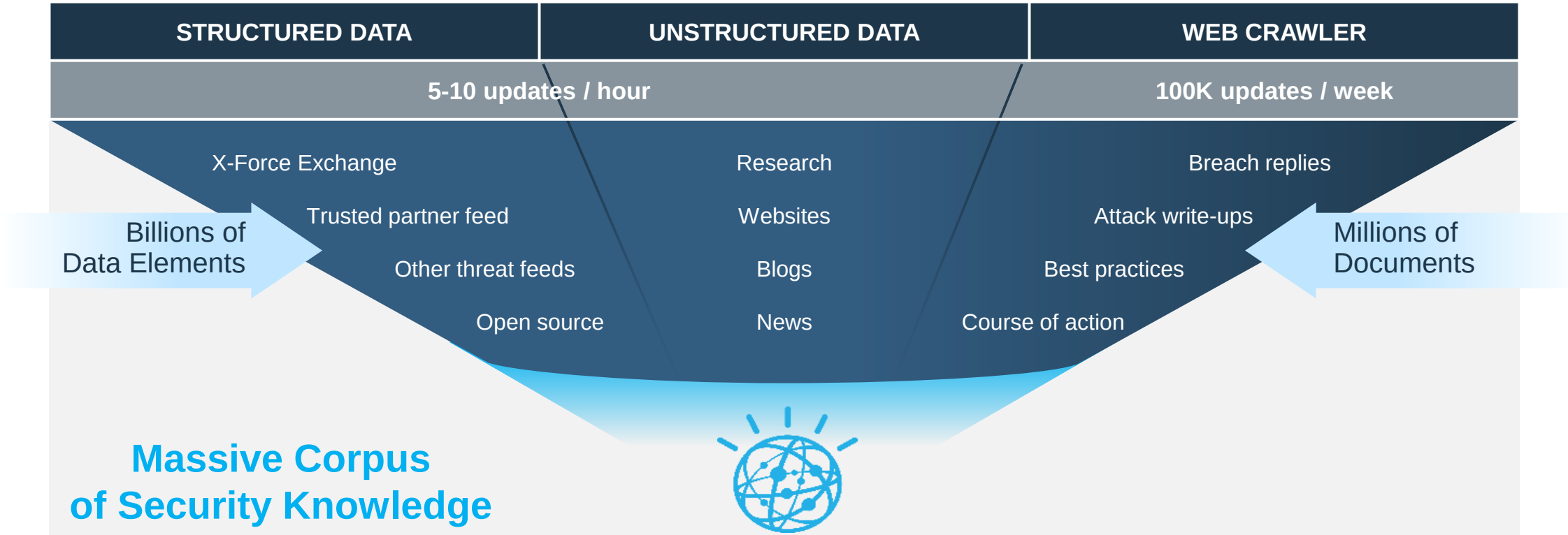
- IoT and IIoT
- Wearable technologies
- Point of Sale
- ATMs
- Self-checkout kiosks

- Criminals **need only** one vulnerability; **the four pillars of testing require a comprehensive program to mitigate risk**.
- **Vast** global collective experience means that **IBM** can test **virtually any** type of target, no matter how obscure.

An integrated and intelligent security immune system



How the Watson for Cyber Security helps stop threats … continuously



Cyber Resiliency Best Practices

1. Reduce your attack surface by ensuring that all systems are regularly scanned and patched. Remove unnecessary services
2. Deploy port blocking technologies for external hosts and from the local network to the WAN
3. Ensure network segmentation is in place and policies are enforced with logging enabled
4. Back-up critical data on a regular basis and freeze pre-infection backups to protect from backup infection
5. Have a Cyber Resiliency Plan in place that is tested regularly
6. Educate your employees not to click on attachments especially that launch macros
7. Regularly conduct internal and external human based penetration tests
8. Implement strict privileged user credential monitoring and restrictions
9. Ensure critical data is protected, isolated and validated on a frequent basis
10. Have a complete and accurate Configuration Management Database of all IT Assets
11. Ability to lockdown your Network/Infrastructure quickly in the midst of a Cyber Attack
12. Whitelist services, processes and application on critical infrastructure

Afslutning:

Når du går i dag er din tilgang til Cyber sikkerhed så den samme, som da du kom?

Mennesker

Risikokultur og awareness

\+

Kapital

Økonomiske konsekvenser og investeringer

\+

Teknologi

Tekniske løsninger

=

Cyber Resiliency

Tak for i dag !

Uffe Spohr
IBM Senior Security Consultant
IBM Security

Phone: +45 28 80 36 65
E-mail: uffespohr@dk.ibm.com
Location: Proevensvej 1, 2605 Broendby, Denmark

Jackie L. Halling
IBM Security Offering Manager
IBM Security

Phone: +45 41202564
E-mail: jchl@dk.ibm.com
Location: Proevensvej 1, 2605 Broendby, Denmark

Tine Olsen,
Deputy FINEX Cyber Practice Leader Western Europe
Practice Lead CYBER Denmark**,** Willis Towers Watson
Cand. Jur., HD(O).

T +45 88139600
D +45 88139431
M +45 29213810
tine.olsen@willistowerswatson.com
Willis I/S Rundforbivej 303, DK-2850 Nærum