Cyberskills

Intro to Information Security

CYBER SKILLS

kea
KØBENHAVNS ERHVERVSAKADEMI

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

Info-Security

Er vigtigt, da verden afhænger af det!

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

If you think technology can solve all your IT-security problems. You don´t understand the technology and you don´t understand the problem.
Quote : Bruce Schneier

CYBER SKILLS

kea
KØBENHAVNS ERHVERVSAKADEMI

Lars Blomgaard

Cybersecurity Specialist

I love to share knowledge about IT-security

You can find me at @linkedin leb56751gvgr

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

CV

- Cybersecurity Specialist
  - NNIT - Security Specialist
  - NC3 - Digital investigations and prevention
  - DSV - Senior IT-Security Architect
- Spare time
  - Underviser på KEA in Governance and DFIR

CYBER SKILLS

KEA KØBENHAVNS ERHVERVSAKADEMI

KEA - Københavns Erhvervs Akademi - Studies

Governance

- ISO, CIS, NIST
- DK Criminal LAW §
- Risk management
- Awareness
- Preparation plans
- Study preparation
- Exam preparation

Threat Handling

- Preparation - technical
- Phases for incident response
- Digital Forensics
- Analysis labs
- File, malware, log, network forensics
- Reporting
- Study preparation
- Exam preparation

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

“Disclaimer”

Her afspejler jeg mine personlige holdninger og repræsentere ikke nogen af førnævnte virksomheder.

Afspejler min viden fra KEA og personlige holdninger

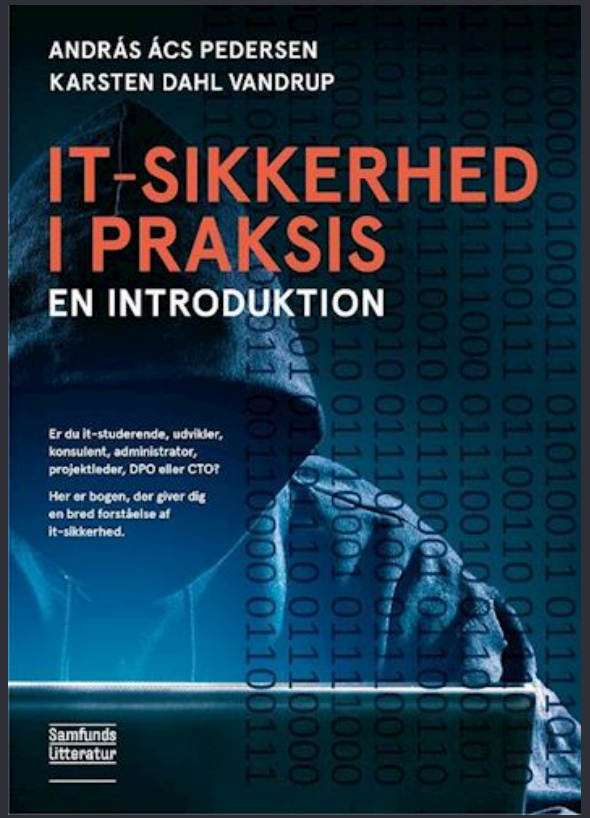
COPENHAGEN SCHOOL OF DESIGN AND TECHNOLOGY

“When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.”

Kilde: https://www.chathamhouse.org/chatham-house-rule?gclid=EAIaIQobChMI_vyv4-bL5wIVxOR3Ch3aJAauEAAYASAAEgKR5PD_BwE

“Inspiration”

I have been inspired by this book “IT-sikkerhed i praksis - an introduction”. Written in Danish and the first book of its kind.



Kilde: https://www.saxo.com/dk/it-sikkerhed-i-praksis_bog_9788759339299

Agenda

- Your beginning - you start today
- What is Infosec
- How is this managed
- Frameworks and strategy
- Risk management and vulnerabilities
- Disaster, when everything fails
- Your path and round up

Your Beginning

you start today

You are you

But who are you on the Internet?

- Look over your shoulder
- Or make your friends do this
- Look for what fx Google, Bing, Duckduckgo know
- SoMe
- And many more

What is Infosec?

Governance why?

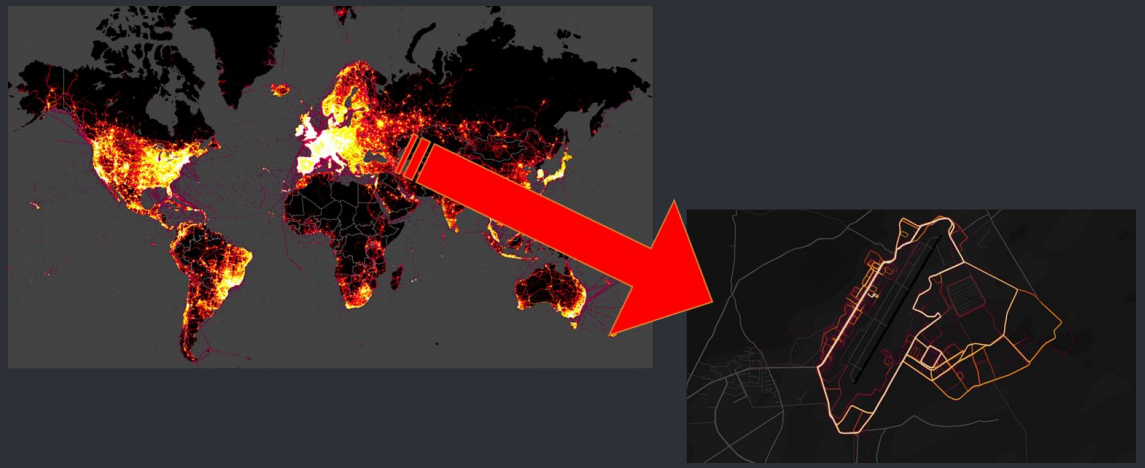
1 Problem, Who is responsible?

- Strava = Fitness app
- Soldiers exercising, App collects data and shares with the world
- Who is responsible for this ?
- Secure location exposed

Governance why?

1 Problem, Who is responsible?

- Strava = Fitness app
- Soldiers exercising, App collects data and shares with the world
- Who is responsible for this ?
- Secure location exposed



Governance why?

1 Problem, Who is responsible?

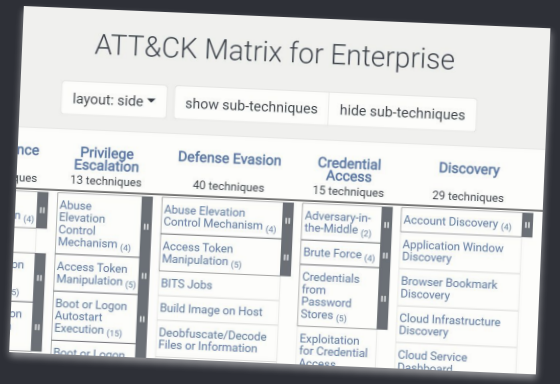
- Strava = Fitness app
- Soldiers exercising, App collects data and shares with the world
- Who is responsible for this ?
- Secure location exposed

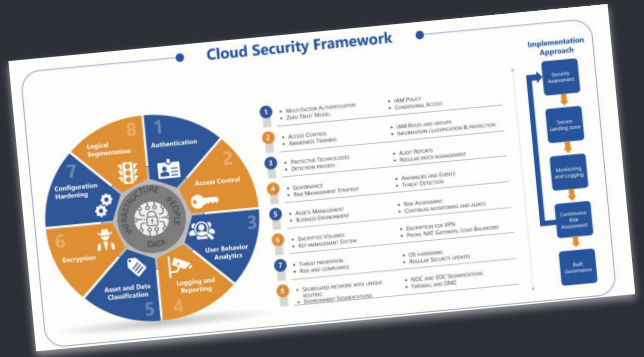
Link = https://www.bellingcat.com/resources/how-tos/2018/01/29/strava-interpretation-guide/
Link = https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/

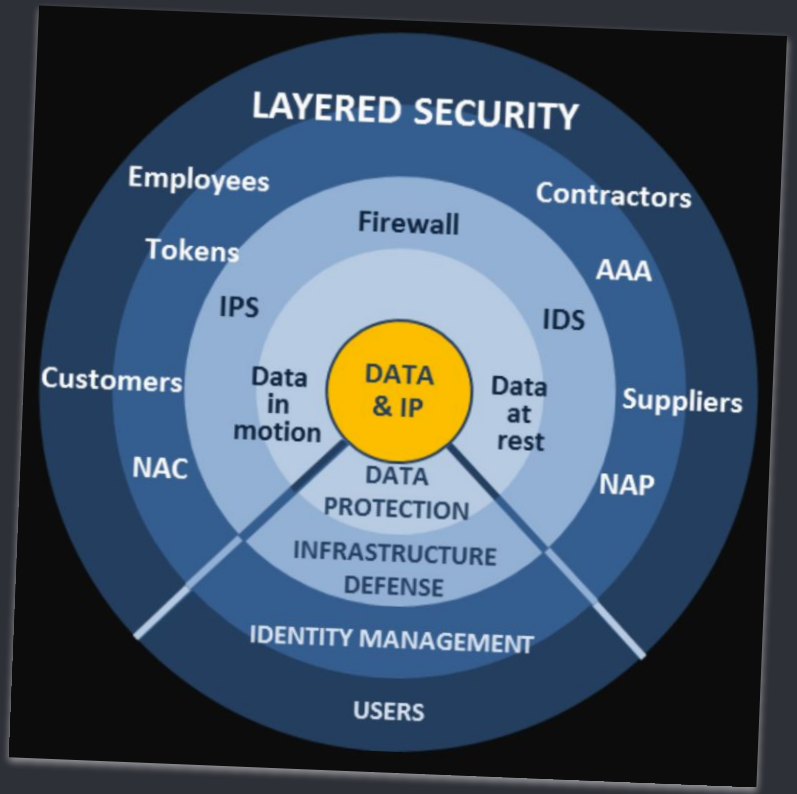
How to control

Frameworks help us

Corporate Business - Complexity







CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

We are all in the same boat

People need

- Training and awareness
- Guidance
- Nudging and a push in the right direction
- Single Point Of Contact (SPOC) when in doubt
- Continuous care

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

We are all in the same boat

IT-People need

- Training and maintenance
- Guidance
- Nudging and a push in the right direction
- Continuous care
- A clear plan when things don't go as expected

CYBER SKILLS

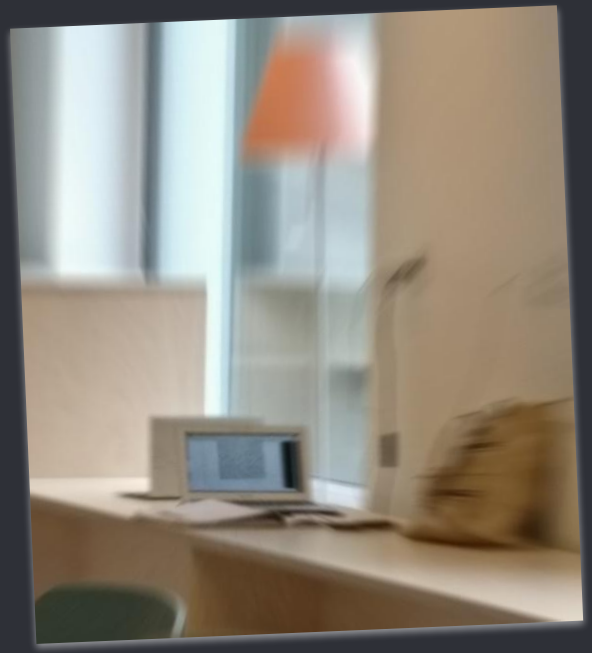
KØBENHAVNS ERHVERVSAKADEMI

We are all in the same boat

Management need

- Make decisions and have mandate
- Guidance
- Be part of the plan
- Continuous update and follow up
- A clear plan when things don't go as expected
- **Take ownership**

We are all in the same boat



People are the threat but also the solution

- Make your personal strategy
  - Use password manager w MFA
  - Use MFA where possible
  - Seperate your technology, have multiple browsers, password managers for different tasks
  - Don't use corporate email for personal stuff

People are the threat but also the solution

Make room for

- People make mistakes
- Changes in the company
- Explaining the necessity of Information security.
- Make it ok to ask when in doubt
- Show your ID when asked

Information Security is a concern for all !

Management

How to we manage information security?

The adversaries

So many data available from the past

Leaks

Enriched data

Pictures (facebook, instagram, snap .....)

The nation sponsored actors - the really bad ones!

2010 - Nuclear centrifuges (Stuxnet)

2015 - German parliament hack

2016 - US clinton hack

2017 - Vault 7 (est 60-70 zero-days)

2021 - Colonial Pipeline

Adversaries - Criminals

Often from countries in the developing world

Work with little risk and repercussions

They can get access with little effort

They are skillful

Have all the time in the world

High motivation for high gain

Source stuxnet: https://en.wikipedia.org/wiki/Stuxnet
Vault 7: https://www.nextgov.com/cybersecurity/2017/03/wikileaks-dump-shines-light-governments-shadowy-zero-day-policy/136079/ and https://wikileaks.org/ciav7p1/#FAQ
US clinton: https://www.bbc.com/news/election-us-2016-36927523
German Office: https://www.reuters.com/article/us-germany-cyber-idUKKCN1GE2H5
Colonial pipeline : https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

The adversaries make use of

Unpatched systems

People make mistakes, mistakes get into software, software are sold/distributed.

Webpages

Webpages are often overlooked and miss TLC

Embedded systems

Embedded systems, that is on the network gets forgotten. Firmware are software!

Weak passwords

The mother of all fun

Open ports

Services are exposed to the internet. Port 3389 is the gate to doom if left open

No monitoring of service

No monitoring of a service, you don't know the adversaries use bruteforce, no one knows og looks

The adversaries make use of

Forgotten services

If a service is labeled as end of life (EOL). Check it´s EOL. If a vps, this will be abused

Test that went to production

The local IT-hero went to IT-zero, because the system was not backed up

Peoples trust

Phishing, Vishing, Smishing, Social Engineering. We are too trusty against unknown people

People's greed

Employees can turn to malicious actors, if the money is enough

Complexity of a company

Too much technology and compliance will suffocate a business and the overview

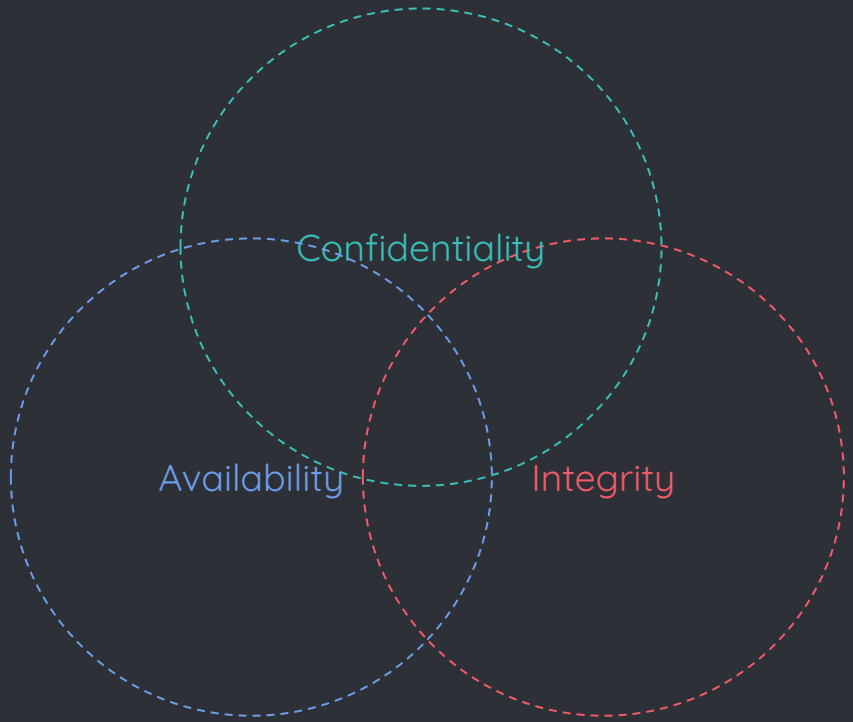
The cloud

Can we get transparency in the cloud? Can we se if the systems are used or abused?

Frameworks

and strategy

CIA



Mitigation

Minimize surface

Knowledge for employees

What's in it for me?

- Missing training
- Password strategy
- Culture of admitting errors
- Why should spend time on security?
- Is it ok to ask for the ID-card

We are all in the same boat

Complexity as we grow

- Big companies - big complexity
  - Missing preparation
  - Overlook the details
  - Product blindness
  - Too little time to investegate
  - Miss the picture of vital data
- This is not a easy quick fix - prepare to defend

Physical is often overlooked

- Physical
  - Do we know you?
  - Who is your appointed, lets guide you there
  - What countermeasures do your business need?
  - Surveillance of property
  - Physical safety (out of hours)

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

Physical is often overlooked

Physical Security is also a part of information security

- ID-cards
- Fences
- Surveillance
- Clean desk policy
- Log out when PC is idle
- Awareness of where you communicate about what

Technologies that can assist

- Our systems are many
  - SIEM - log mgmt
  - IDS
  - SOC / SAC
  - AV, FW, IPS, DLP, DMARC, IAM and much more
  - Cloud (by the way its someone elses computer)
- Don't get product blind

Technologies that can slow us down

- Where is our data when we need it?
  - It is in the Cloud nowhere to be seen (or downloaded)
  - How can it be obtained?
  - What is in the data?
  - Is it correct?
- Do we have what we need, when we need?

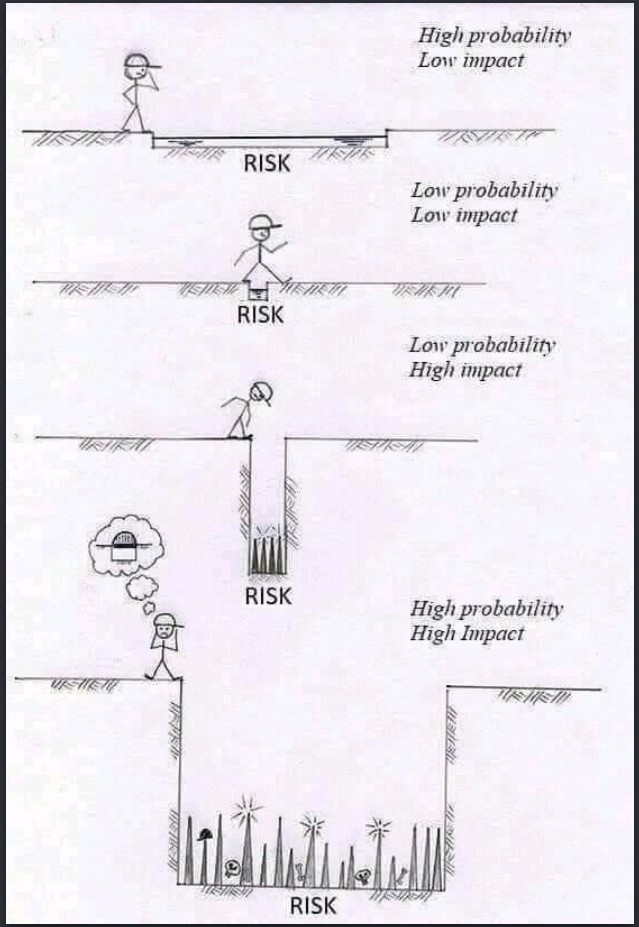
Technologies that can assist

- Our data gives knowledge
  - Missing preparation
  - Overlook the details
  - Product blindness
  - Too little time to investegate
  - Miss the picture of vital data
- This is not a easy quick fix

Risk

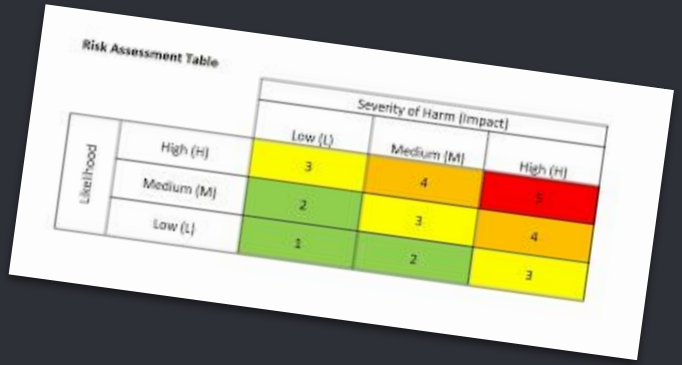
Risk management and vulnerabilities

Risk and score



Risk calculation

Risiko faktor	Sandsynlighed (S)	Konsekvens (K)	S * K	Prioritet
System 1	4	2	8	2
System 2	2	3	6	3
System 3	5	2	10	1
System 4	1	5	5	4



Eksempel på udregning fra CIS: https://www.cisecurity.org/blog/the-one-equation-you-need-to-calculate-risk-reduction-roi/

og fra risk management guru: https://riskmanagementguru.com/residual-risk-scoring-matrix-example.html/

Risk management

IMPACT	Risk Management Actions		
Significant • Financial Loss > $5MM • Stakeholder faith impacted and lasts > 18 months • Isolated or Multiple Loss of Life • Multiple events of fine, fraud or legal action • Complete system crash with loss of critical data • Inability to recruit, retain staff to operate • Labour disruption that impacts graduation	Considerable Management Required	Must manage and monitor risks	Extensive management essential
Moderate • Financial Loss < $5 MM • Stakeholder faith impacted and lasts 6-12 months • Significant injury to one or more • Isolate incidents of fine, fraud, or legal action • System crash during a peak period • Difficulties in recruiting and retaining staff • Labour disruption that impacts operations of any duration	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor • Financial Loss < $500,000 • Stakeholder faith impacted and lasts < 6 months • Isolated injury • Civil or criminal action threatened • System off-line periodically during non-peak periods	Accept risks	Accept but monitor risks	Manage and monitor risks
	Low > 36 months	Medium 18 to 36 months	High 12 to 18 months
	LIKELIHOOD		

Patch management

- Patch tuesday from MS.
- Patch in OT environments (other strategy)
- Identify patch , vulnerability management
- Patch review
- Emergency patch
- Compliance review

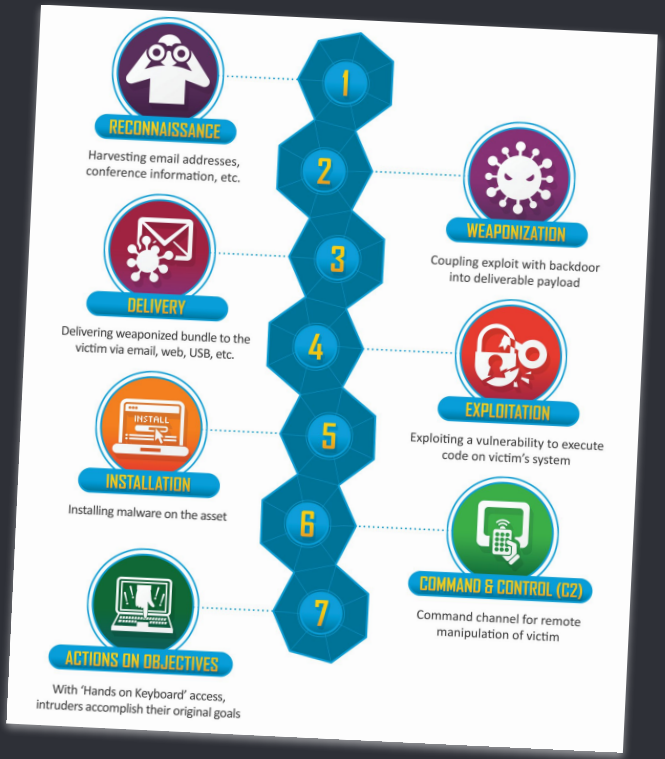
The adversaries make use of

Zero-days

The stuff no one knows about

Advanced Persistent Threats - APT

Gain persistence in a system
(Average 197 days (2018) - 280 days (2018))



Killchain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
Average time for breach: https://securityboulevard.com/2018/07/survey-finds-breach-discovery-takes-an-average-197-days/ and https://www.schneiderdowns.com/our-thoughts-on/2021-data-breach-cost

Malware

Key Malware Statistics

- 560,000 new pieces of malware are detected every day.
- There are now more than 1 billion malware programs out there.
- Every minute, four companies fall victim to ransomware attacks.
- Trojans account for 58% of all computer malware.

Source: https://dataprot.net/statistics/malware-statistics/

Combination

Patch race

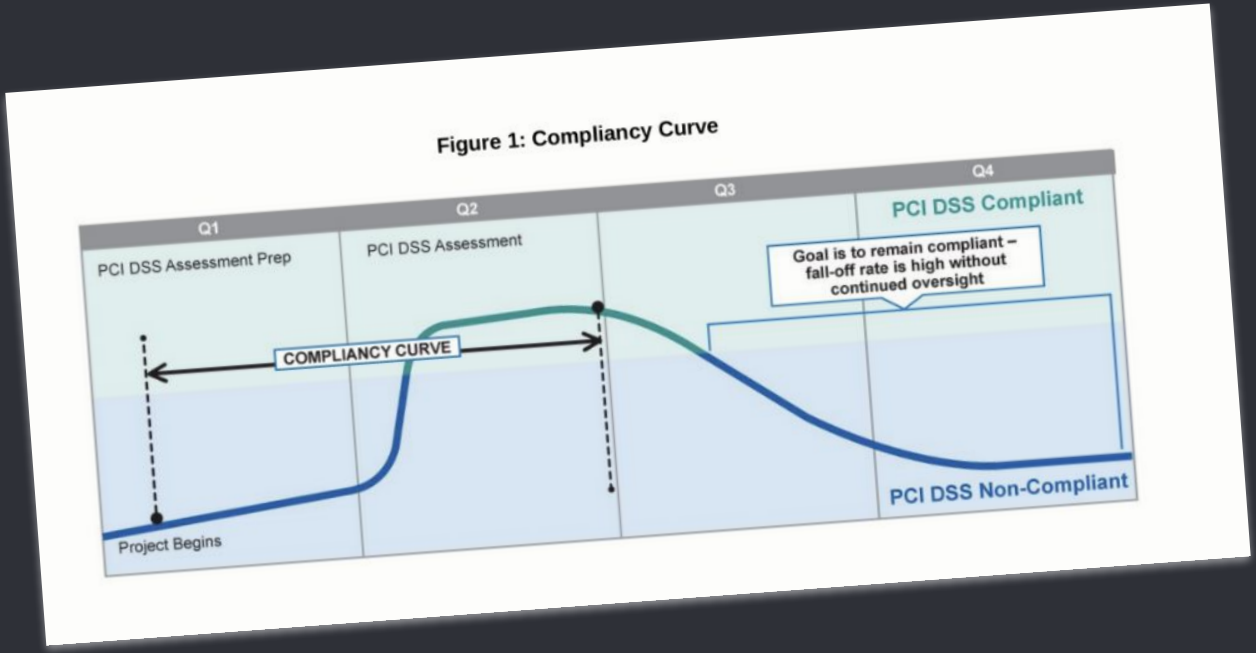
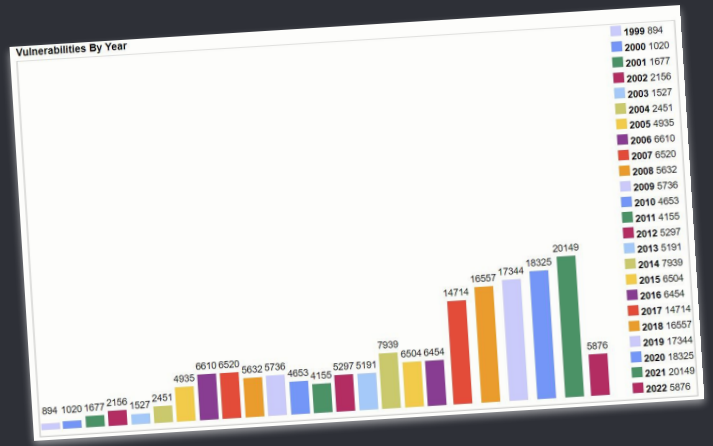
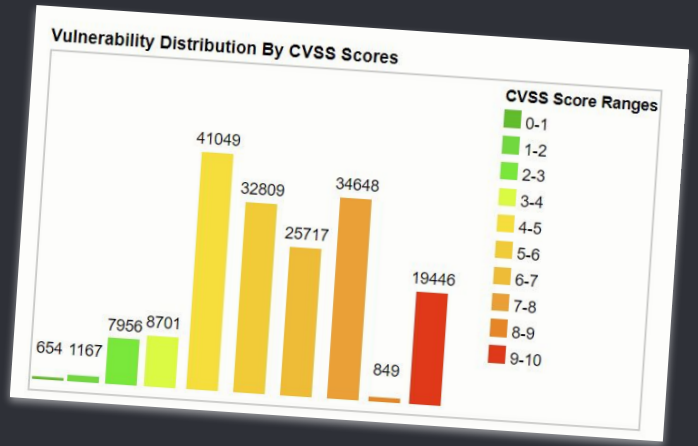


Figure 1: Compliancy Curve
Q1
Q2
Q3
Q4
PCI DSS Assessment Prep
PCI DSS Assessment
PCI DSS Compliant
Goal is to remain compliant – fall-off rate is high without continued oversight
COMPLIANCY CURVE
PCI DSS Non-Compliant
Project Begins

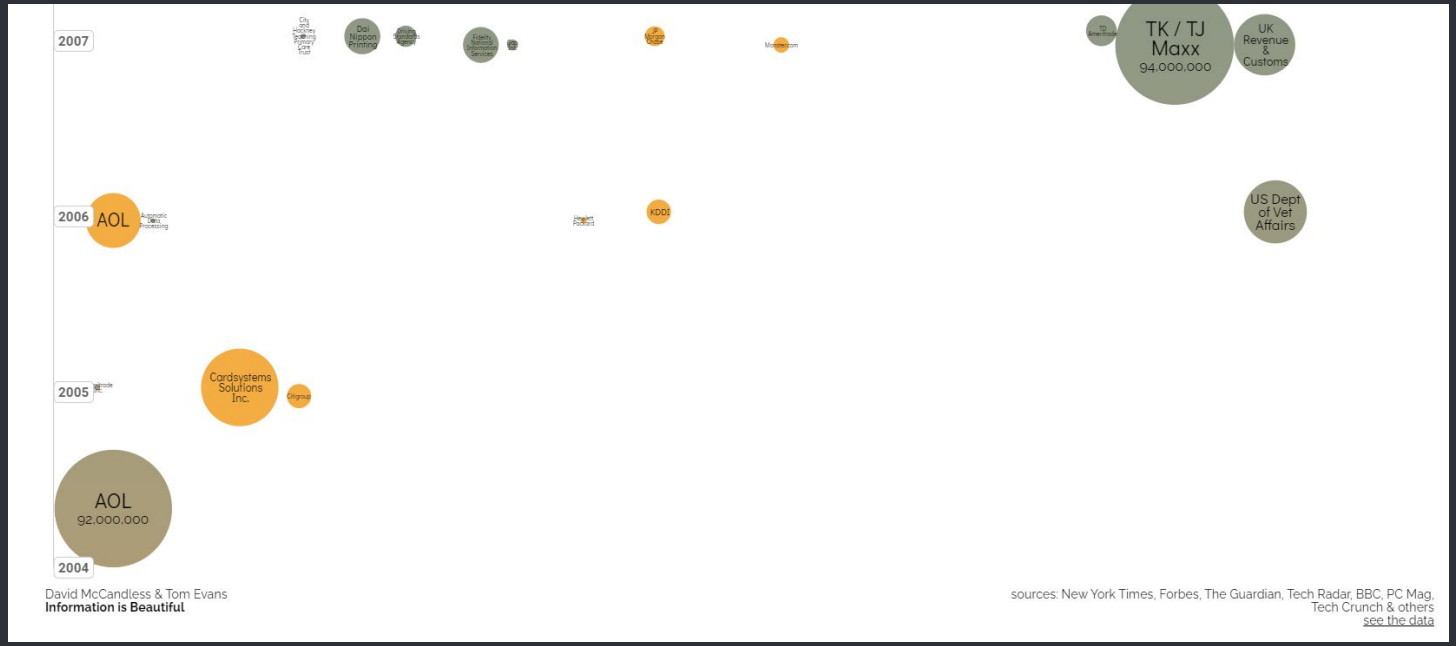
The dry statistics





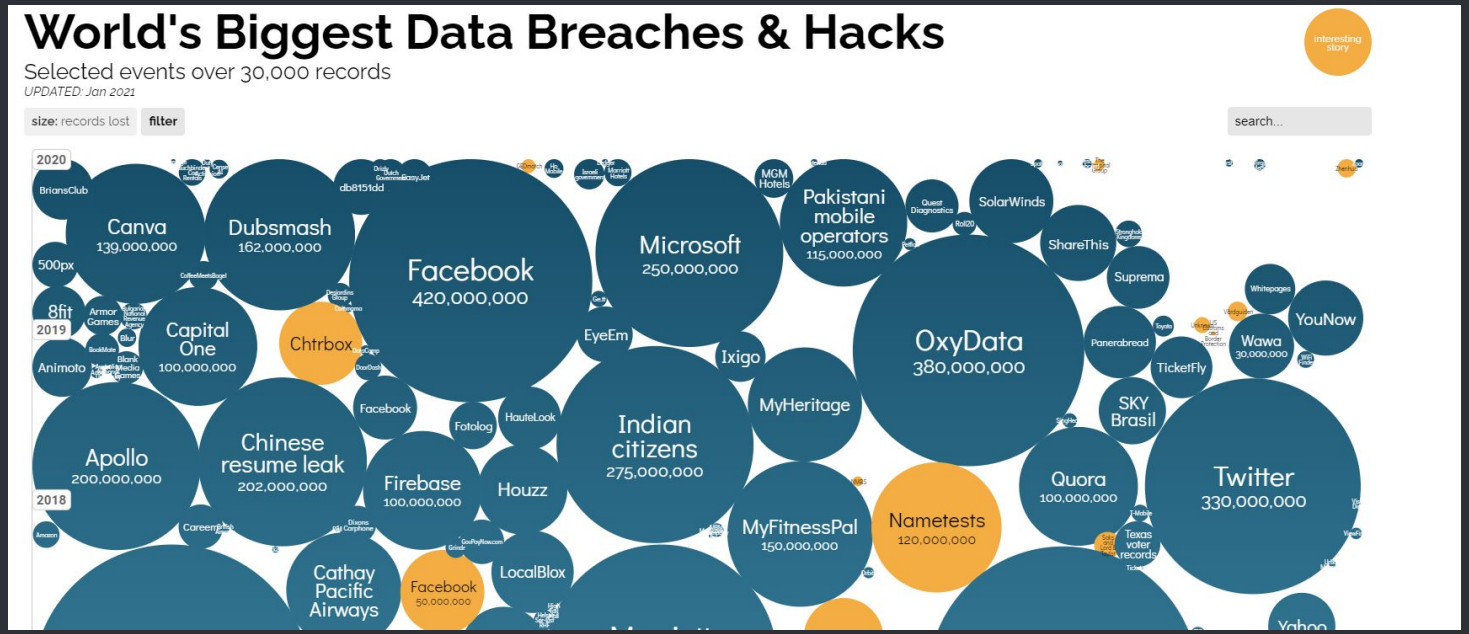
CVE-details: https://www.cvedetails.com/browse-by-date.php

In the 00´s



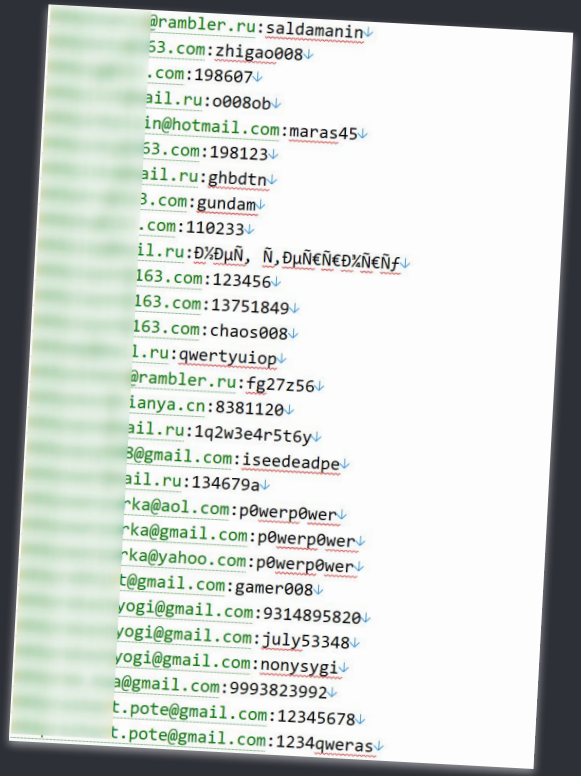
Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

In the 20'ies



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Leaks



```
@rambler.ru:saldamanin
53.com:zhigao008
.com:198607
ail.ru:o008ob
in@hotmail.com:maras45
53.com:198123
ail.ru:ghbdtn
3.com:gundam
.com:110233
il.ru:Ð¼ÐµÑ, Ñ,ÐµÑ€Ñ€Ð¼Ñ€Ñƒ
163.com:123456
163.com:13751849
163.com:chaos008
l.ru:qwertyuiop
@rambler.ru:fg27z56
ianya.cn:8381120
ail.ru:1q2w3e4r5t6y
3@gmail.com:iseedeadpe
ail.ru:134679a
rka@aol.com:p0werp0wer
rka@gmail.com:p0werp0wer
rka@yahoo.com:p0werp0wer
t@gmail.com:gamer008
yogi@gmail.com:9314895820
yogi@gmail.com:july53348
yogi@gmail.com:nonysygi
a@gmail.com:9993823992
t.pote@gmail.com:12345678
t.pote@gmail.com:1234qweras
```

Frameworks

Managements anchor of IT-security in the company

What is a control

con • trol
/kən trōl/

A control is the power to influence or direct behaviors and the course of events. A control is a means of managing risk, which includes policies, standards procedures, practices or other means of an administrative, technical, management or legal nature.

Link: https://www.complianceforge.com/blog/is-cmmc-really-a-maturity-model-or-just-a-controls-catalog-with-5-control-sets/

Center For Internetsecurity = CIS (CIS18)

Center For Internetsecurity = CIS (CIS18)

Implementation Groups

IG1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

IG2 (Includes IG1)

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3 (Includes IG1 and IG2)

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

Center For Internetsecurity = CIS (CIS18)

- Inventory and Control of Enterprise Assets
- Inventory and Control of Software Assets
- Data protection
- Secure Configuration of Enterprise Assets and Software
- Account Management
- Access Control Management
- Continuous Vulnerability Management
- Audit Log Management
- Email and Web Browser Protections
- Malware Defenses
- Data recovery
- Network Infrastructure Management
- Network Monitoring and Defense
- Security Awareness and Skills Training
- Service Provider Management
- Application Software Security
- Incident Response Management
- Penetration Testing

Center For Internetsecurity = CIS (CIS18)

Control	Title	Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5

Benefits of CIS kubernetes example (Container management)

Benchmarks

The listing below displays all the benchmarks you currently have access to.

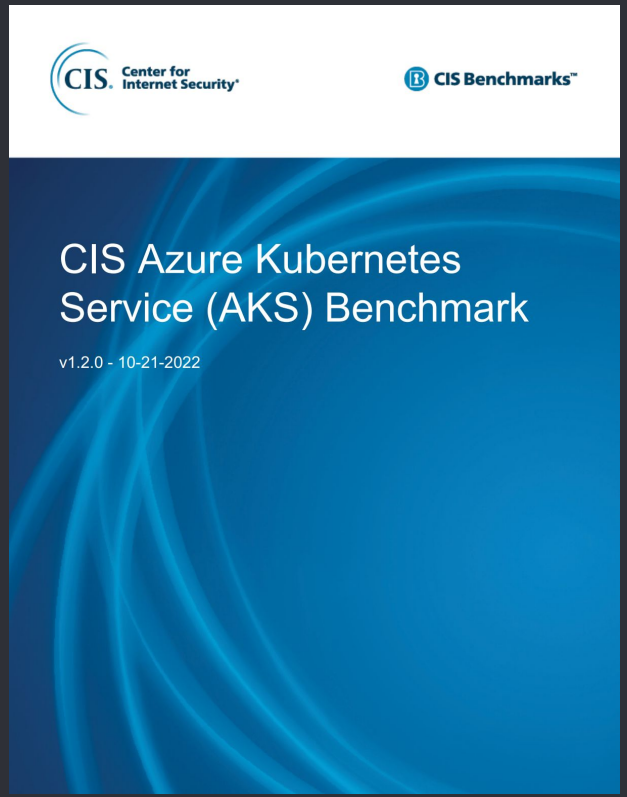
Search | Status All | Filter

All 858

Title	Version	Status	Community	Collections	Owner
CIS * Microsoft Windows Server 2012 R2 Benchmark [imported]	v1.0.0	Published	CIS Microsoft Windows Benchmarks		bfrantz
Tailored **Draft**_Microsoft Windows 10 Enterprise Release 1909 Benchmark	v1.8.1	Draft			ronantiu
CIS Alibaba Cloud Container Service For Kubernetes (ACK) Benchmark	v1.1.0	Draft	CIS Kubernetes Benchmarks		rmowen
CIS Alibaba Cloud Container Service For Kubernetes (ACK) Benchmark	v1.0.0	Published	CIS Kubernetes Benchmarks		mvogelerpeterson
CIS Alibaba Cloud Foundation Benchmark	v1.1.0	Draft	CIS Alibaba Cloud Benchmarks		mwicks

Link: https://workbench.cisecurity.org

Benefits of CIS kubernetes example (Container management)



3.1.2 Ensure that the kubelet kubeconfig file ownership is set to root:root (Manual)

Profile Applicability:

- Level 1

Description:

If `kubelet` is running, ensure that the file ownership of its kubeconfig file is set to `root:root`.

Rationale:

The kubeconfig file for `kubelet` controls various parameters for the `kubelet` service in the worker node. You should set its file ownership to maintain the integrity of the file. The file should be owned by `root:root`.

Impact:

None

Audit:

SSH to the worker nodes
To check to see if the Kubelet Service is running:

```
sudo systemctl status kubelet
```

The output should return `Active: active (running) since..`
Run the following command on each node to find the appropriate kubeconfig file:

```
ps -ef | grep kubelet
```

The output of the above command should return something similar to `--kubeconfig /var/lib/kubelet/kubeconfig` which is the location of the kubeconfig file.
Run this command to obtain the kubeconfig file ownership:

```
stat -c %U:%G /var/lib/kubelet/kubeconfig
```

The output of the above command gives you the kubeconfig file's ownership. Verify that the ownership is set to `root:root`.

Remediation:

Run the below command (based on the file location on your system) on each worker node. For example,

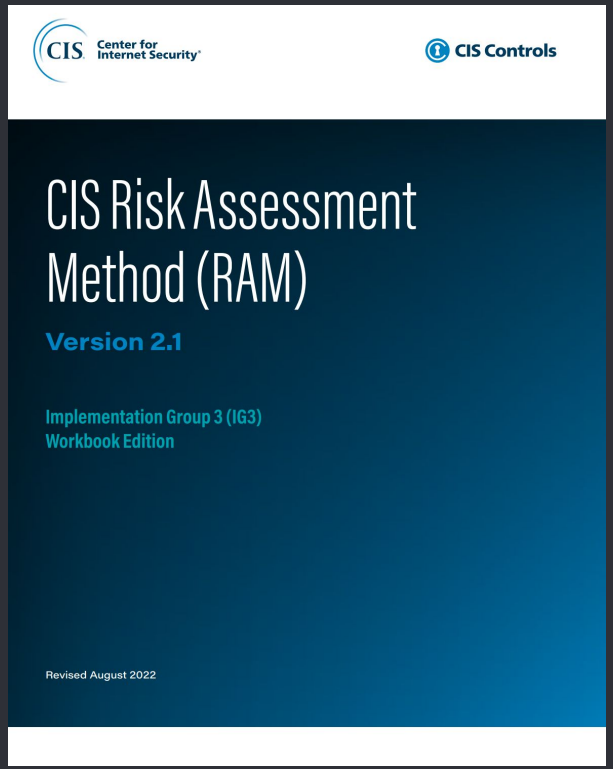
```
chown root:root <proxy kubeconfig file>
```

Default Value:

See the Azure AKS documentation for the default value.

Link: https://workbench.cisecurity.org/files/4128

Manage risk in CIS



Impact Magnitude	Prompt	Response
Negligible	What observable evidence would you have that your financial objectives - as you defined them above - would be unaffected?	$1,000
Acceptable	What observable evidence would you have that your financial objectives would be compromised, but it would not require correction?	$10,000
Unacceptable	What observable evidence would you have that your financial objectives would be compromised in a way that would require correction, but the correction could be achieved through the normal course of business?	$500,000
High	What observable evidence would you have that your financial objectives would be compromised so badly that extraordinary efforts would be required to restore them?	$5,000,000
Catastrophic	Leave this blank	

Impact Magnitude	Prompt	Response
Negligible	Describe a condition where others would not be harmed.	No harm could foreseeably result.
Acceptable	Describe a condition where others would not be harmed to a degree that required correction or compensation.	Any harm that could result would not require correction, repair, or compensation to make the harmed parties "whole."
Unacceptable	Describe a condition where one or few others would be harmed to a degree that you could correct.	Correctible harm may occur to one or few others.
High	Describe a condition where many others would be harmed to a degree that you could correct, or where few others are harmed to a degree that others would always have a small degree of impairment.	Correctible harm may occur to many others, or harm that can be partially corrected for a few others may occur.
Catastrophic	Describe a condition where others would be irreparably harmed.	We would not be able to protect others from any degree of harm.

Link: https://workbench.cisecurity.org/files/3919

ISO27001

ISO27001

Mandatory ISO 27001 documents

Here are the items you must document if you want to be compliant with ISO 27001, and the most common ways to title those documents:

What must be documented	ISO 27001 reference	Usually documented through
Scope of the ISMS	Clause 4.3	ISMS Scope document
Information security policy	Clause 5.2	Information Security Policy
Risk assessment and risk treatment process	Clause 6.1.2	Risk Assessment and Treatment Methodology
Statement of Applicability	Clause 6.1.3 d)	Statement of Applicability
Risk treatment plan	Clauses 6.1.3 e, 6.2, and 8.3	Risk Treatment Plan
Information security objectives	Clause 6.2	List of Security Objectives
Risk assessment and treatment report	Clauses 8.2 and 8.3	Risk Assessment & Treatment Report
Inventory of assets	Control A.5.9*	Inventory of Assets, or List of Assets in the Risk Register
Acceptable use of assets	Control A.5.10*	IT Security Policy
Incident response procedure	Control A.5.26*	Incident Management Procedure
Statutory, regulatory, and contractual requirements	Control A.5.31*	List of Legal, Regulatory, and Contractual Requirements
Security operating procedures for IT management	Control A.5.37*	Security Procedures for IT Department
Definition of security roles and responsibilities	Controls A.6.2 and A.6.6*	Agreements, NDAs, and specifying responsibilities in each security policy and procedure
Definition of security configurations	Control A.8.9*	Security Procedures for IT Department
Secure system engineering principles	Control A.8.27*	Secure Development Policy

*Note: ISO 27001 documents or records required by Annex A controls are mandatory only if there are risks or requirements from interested parties that would demand implementing those controls.

Link: https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-revision

CYBER SKILLS

kea KØBENHAVNS ERHVERVSAKADEMI

ISO27001

Annex A documentation

Organisations must also complete documents in Annex A, which details a list of information security controls that must be considered – whether they are implemented or not.

Indeed, you don't have to implement all 114 of its controls; they are simply a list of possibilities you should consider based on your organisation's requirements.

However, there are several controls that almost every organisation should implement. This includes:

- 7.1.2 and A.13.2.4 Definition of security roles and responsibilities
- 8.1.1 An inventory of assets
- 8.1.3 Rules for the acceptable use of assets
- 8.2.1 Information classification scheme
- 9.1.1 Access control policy
- 12.1.1 Operating procedures for IT management
- 12.4.1 and A.12.4.3 Logs of user activities, exceptions, and security events
- 14.2.5 Secure system engineering principles
- 15.1.1 Supplier security policy
- 16.1.5 Incident management procedure
- 17.1.2 Business continuity procedures
- 18.1.1 Statutory, regulatory, and contractual requirements

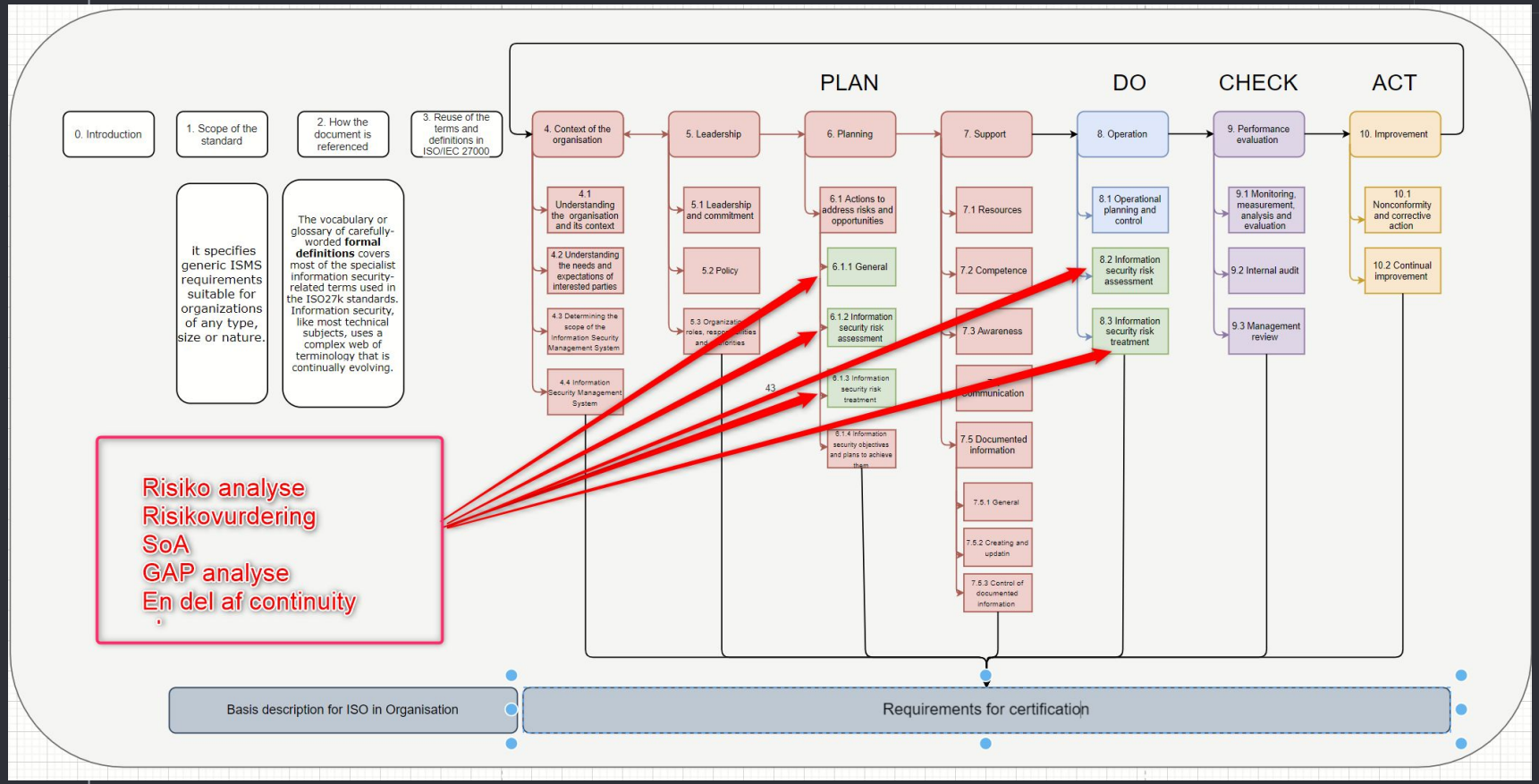
Link: https://www.itgovernance.co.uk/blog/documentation-required-by-iso-27001-2

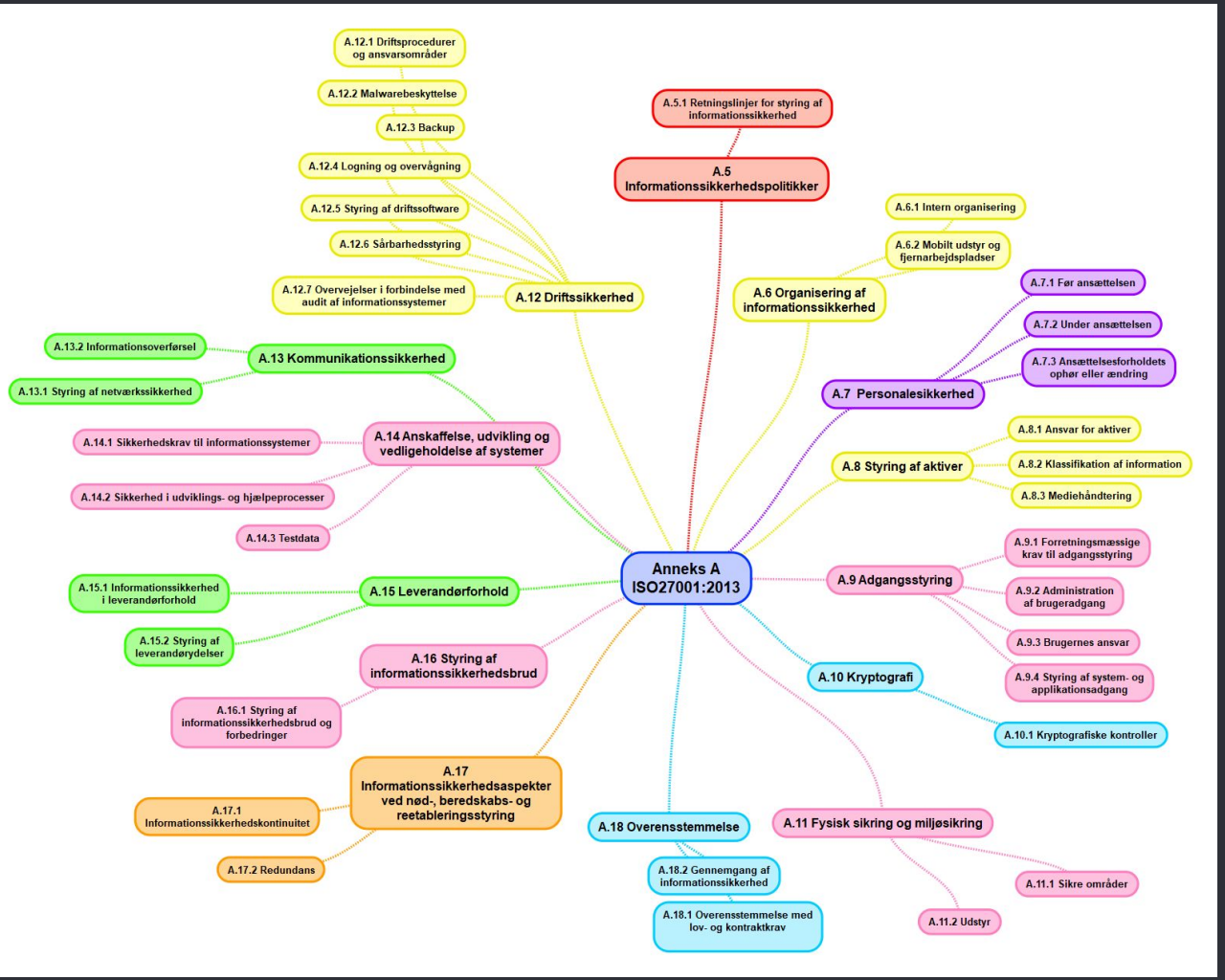
ISO27001

New security controls in ISO 27001:2022	Existing ISO 27001 documents where these controls can be included
A.5.7 Threat intelligence	Incident Management Procedure
A.5.23 Information security for use of cloud services	Supplier Security Policy
A.5.30 ICT readiness for business continuity	Disaster Recovery Plan
A.7.4 Physical security monitoring	Procedures for Working in Secure Areas
A.8.9 Configuration management	Security Procedures for IT Department
A.8.10 Information deletion	Disposal and Destruction Policy
A.8.11 Data masking	Secure Development Policy
A.8.12 Data leakage prevention	Security Procedures for IT Department
A.8.16 Monitoring activities	Security Procedures for IT Department
A.8.23 Web filtering	Security Procedures for IT Department
A.8.28 Secure coding	Secure Development Policy

To get the templates for all mandatory documents and the most common non-mandatory documents, along with a wizard that helps you fill out those templates, **sign up for a free trial** *of Conformio, the leading ISO 27001 compliance software.*

Link: https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-revision


PLAN
DO
CHECK
ACT
0. Introduction
1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Context of the organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement
4.1 Understanding the organisation and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the Information Security Management System
4.4 Information Security Management System
5.1 Leadership and commitment
5.2 Policy
6.1 Actions to address risks and opportunities
6.1.1 General
6.1.2 Information security risk assessment
6.1.3 Information security risk treatment
7.1 Resources
7.2 Competence
7.3 Awareness
7.5 Documented information
7.5.1 General
7.5.2 Creating and updatin
7.5.3 Control of documented information
8.1 Operational planning and control
8.2 Information security risk assessment
8.3 Information security risk treatment
9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit
9.3 Management review
10.1 Nonconformity and corrective action
10.2 Continual improvement
it specifies generic ISMS requirements suitable for organizations of any type, size or nature.
The vocabulary or glossary of carefully-worded formal definitions covers most of the specialist information security-related terms used in the ISO27k standards. Information security, like most technical subjects, uses a complex web of terminology that is continually evolving.
Risiko analyse
Risikovurdering
SoA
GAP analyse
En del af continuity
Basis description for ISO in Organisation
Requirements for certification


Anneks A
ISO27001:2013
A.5
Informationssikkerhedspolitikker
A.5.1 Retningslinjer for styring af informationssikkerhed
A.6 Organisering af informationssikkerhed
A.6.1 Intern organisering
A.6.2 Mobilt udstyr og fjernarbejdspladser
A.7 Personalesikkerhed
A.7.1 Før ansættelsen
A.7.2 Under ansættelsen
A.7.3 Ansættelsesforholdets ophør eller ændring
A.8 Styring af aktiver
A.8.1 Ansvar for aktiver
A.8.2 Klassifikation af information
A.8.3 Mediehåndtering
A.9 Adgangsstyring
A.9.1 Forretningsmæssige krav til adgangsstyring
A.9.2 Administration af brugeradgang
A.9.3 Brugernes ansvar
A.9.4 Styring af system- og applikationsadgang
A.10 Kryptografi
A.10.1 Kryptografiske kontroller
A.11 Fysisk sikring og miljøsikring
A.11.1 Sikre områder
A.11.2 Udstyr
A.12 Driftssikkerhed
A.12.1 Driftsprocedurer og ansvarsområder
A.12.2 Malwarebeskyttelse
A.12.3 Backup
A.12.4 Logning og overvågning
A.12.5 Styring af driftssoftware
A.12.6 Sårbarhedsstyring
A.12.7 Overvejelser i forbindelse med audit af informationssystemer
A.13 Kommunikationssikkerhed
A.13.1 Styring af netværkssikkerhed
A.13.2 Informationsoverførsel
A.14 Anskaffelse, udvikling og vedligeholdelse af systemer
A.14.1 Sikkerhedskrav til informationssystemer
A.14.2 Sikkerhed i udviklings- og hjælpeprocesser
A.14.3 Testdata
A.15 Leverandørforhold
A.15.1 Informationssikkerhed i leverandørforhold
A.15.2 Styring af leverandørydelser
A.16 Styring af informationssikkerhedsbrud
A.16.1 Styring af informationssikkerhedsbrud og forbedringer
A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
A.17.1 Informationssikkerhedskontinuitet
A.17.2 Redundans
A.18 Overensstemmelse
A.18.1 Overensstemmelse med lov- og kontraktkrav
A.18.2 Gennemgang af informationssikkerhed

CIS vs ISO27001

CIS Control	CIS Sub-Control	Title	Description	Relationship	ISO 27001 Objective Number	ISO 27001 Control Objective
1		**Inventory and Control of Hardware Assets**	***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***			
1	1,1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	small subset	A.8.1.1	Inventory of assets
1	1,2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	small subset	A.8.1.1	Inventory of assets
1	1,3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	small subset	A.8.1.1	Inventory of assets
1	1,4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	large subset	A.8.1.1	Inventory of assets
1	1,5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	small subset	A.8.1.1	Inventory of assets
1	1,6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	small subset	A.11.2.5	Removal of assets
1	1,7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	small subset	A.13.1.1	Network Controls
1	1,8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	large subset	A.9.1.2	Access to networks and network services
1	1,8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	small subset	A.9.3.1	Use of secret authentication information
				small subset	A.13.1.1	Network Controls

CIS mappings ISO27001: https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mapping-to-iso-27001/
(Download Excel = CIS Controls and Sub-Controls Mapping to ISO.xlsx)

Demands for certifying

The following mandatory documentation is explicitly required for certification:

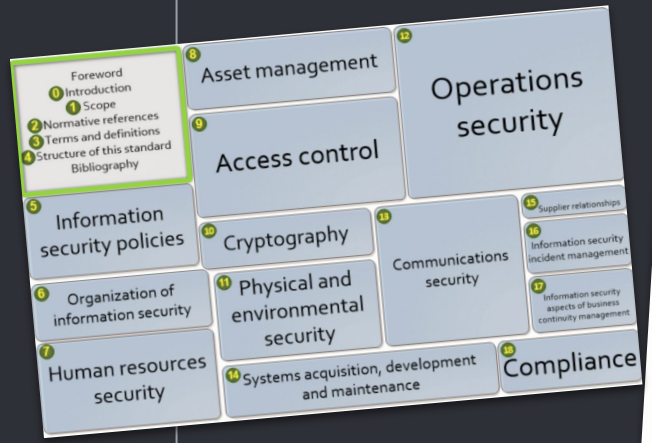
- ISMS scope (as per clause 4.3)
- Information security policy (clause 5.2)
- Information risk assessment process (clause 6.1.2)
- Information risk treatment process (clause 6.1.3)
- Information security objectives (clause 6.2)
- Evidence of the competence of the people working in information security (clause 7.2)
- Other ISMS-related documents deemed necessary by the organization (clause 7.5.1b)
- Operational planning and control documents (clause 8.1)
- The results of the [information] risk assessments (clause 8.2)
- The decisions regarding [information] risk treatment (clause 8.3)
- Evidence of the monitoring and measurement of information security (clause 9.1)
- The ISMS internal audit program and the results of audits conducted (clause 9.2)
- Evidence of top management reviews of the ISMS (clause 9.3)
- Evidence of nonconformities identified and corrective actions arising (clause 10.1)

Kilde: https://www.isms.online/iso-27001/requirements-controls/

- Various others: Annex A mentions but does not fully specify further documentation including the rules for
  - acceptable use of assets,
  - access control policy, operating procedures,
  - confidentiality or non-disclosure agreements,
  - secure system engineering principles,
  - information security policy for supplier relationships,
  - information security incident response procedures, relevant laws,
  - regulations and contractual obligations plus the associated compliance procedures and information security continuity procedures.

However, despite Annex A being normative, organizations are not formally required to adopt and comply with Annex A: they can use other structures and approaches to treat their information risks.

Hvorfor starter Annex A fra A5?



Why do the ISO 27001 Controls Start at A5?

It may seem odd that the controls in Annex A start at A5 rather than A1. This is because the controls of Annex A correspond directly to those in another standard from the ISO 27000 Family, ISO 27002.

In ISO 27002 there are some introductory and explanatory sections 1-4, so the controls begin at section 5.

During an ISO 27001 Certification audit, you will be audited against the control text within ISO 27001 only. However, there are many benefits to reading the extended guidance on each control within ISO 27002.

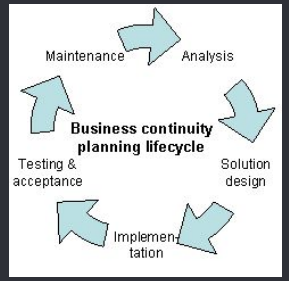
Kilde: https://www.assent1.com/what-are-the-iso-27001-controls/ og https://www.iso27001security.com/html/27002.html#Contents

Minimize disaster

And mitigate risk

Business Continuity Plan - BCP

An organization's resistance to failure is "the ability ... to withstand changes in its environment and still function".[7] Often called resilience, it is a capability that enables organizations to either endure environmental changes without having to permanently adapt, or the organization is forced to adapt a new way of working that better suits the new environmental conditions.[7]



Link: https://en.wikipedia.org/wiki/Supply_chain
Link: https://en.wikipedia.org/wiki/Risk_management
Link: https://en.wikipedia.org/wiki/Business_continuity_planning

Business Continuity Plan - BCP

Elements of business impact analysis

	Fire in data center	Loss of specialized staff	Vehicle crash in front entrance of office building	Vandalism to primary product assembly line	Loss of staff due to COVID-19 illness
BUSINESS ACTIVITY AFFECTED	All activities in data center	Activities that require specialized staff	All activities at that location unless an alternate access option is available	Loss of primary production line	Loss of possibly key employees needed to run the business
POTENTIAL OPERATIONAL LOSS	Inability to function normally	Reduced ability to function normally	Nominal disruption based on how quickly the vehicle can be removed and the front entrance reopened	Inability to produce the company's primary product	May be nominal to significant depending on who is affected
POTENTIAL FINANCIAL LOSS	$3,000 to $4,000 revenue loss per hour	None, assuming backup staff is available	None, assuming alternate entrance is available and access to building facilities is available	$25,000 to $40,000 per hour in lost revenue	Could be minimal assuming employees can work remotely
MINIMUM TIME NEEDED TO RECOVER OPERATIONS	Three to four hours	One to two hours	Depending on the damage from the crash, up to one day	Days if a work-around can be built; weeks if an alternate production facility must be found and launched	24-48 hours depending on health status and if employees can work remotely

SOURCE: PAUL KIRNAN; ICONS: JUSTINROQUE, ANTTOHOHO, APPLEUZR/GETTY IMAGES

Link: https://www.techtarget.com/searchstorage/definition/business-impact-analysis

Business Continuity Plan - BCP

Maximum RTO [edit]

Maximum time constraints for how long an enterprise's key products or services can be unavailable or undeliverable before stakeholders perceive unacceptable consequences have been named as:

- **Maximum Tolerable Period of Disruption (MTPoD)**
- **Maximum Tolerable Downtime (MTD)**
- **Maximum Tolerable Outage (MTO)**
- **Maximum Acceptable Outage (MAO)**[27][28]

Link: https://en.wikipedia.org/wiki/Supply_chain
Link: https://en.wikipedia.org/wiki/Risk_management
Link: https://en.wikipedia.org/wiki/Business_continuity_planning

Business Continuity Plan - BCP

Tiers of preparedness [edit]

SHARE's seven tiers of disaster recovery[37] released in 1992, were updated in 2012 by IBM as an eight tier model:[38]

- **Tier 0 - No off-site data** • Businesses with a Tier 0 Disaster Recovery solution have no Disaster Recovery Plan. There is no saved information, no documentation, no backup hardware, and no contingency plan. Typical recovery time: ***The length of recovery time in this instance is unpredictable***. In fact, it may not be possible to recover at all.
- **Tier 1 - Data backup with no Hot Site** • Businesses that use Tier 1 Disaster Recovery solutions back up their data at an off-site facility. Depending on how often backups are made, they are prepared to accept **several days to weeks of data loss**, but their backups are secure off-site. However, this Tier lacks the systems on which to restore data. Pickup Truck Access Method (PTAM).
- **Tier 2 - Data backup with Hot Site** • Tier 2 Disaster Recovery solutions make regular backups on tape. This is combined with an off-site facility and infrastructure (known as a hot site) in which to restore systems from those tapes in the event of a disaster. This tier solution will still result in the need to recreate several hours to days worth of data, but ***it is less unpredictable in recovery time***. Examples include: PTAM with Hot Site available, IBM Tivoli Storage Manager.
- **Tier 3 - Electronic vaulting** • Tier 3 solutions utilize components of Tier 2. Additionally, some mission-critical data is electronically vaulted. This electronically vaulted data is typically more current than that which is shipped via PTAM. As a result there is ***less data recreation or loss after a disaster occurs***.
- **Tier 4 - Point-in-time copies** • Tier 4 solutions are used by businesses that require both greater data currency and faster recovery than users of lower tiers. Rather than relying largely on shipping tape, as is common in the lower tiers, Tier 4 solutions begin to incorporate more disk-based solutions. ***Several hours of data loss is still possible***, but it is easier to make such point-in-time (PIT) copies with greater frequency than data that can be replicated through tape-based solutions.
- **Tier 5 - Transaction integrity** • Tier 5 solutions are used by businesses with a requirement for consistency of data between production and recovery data centers. There is ***little to no data loss*** in such solutions; however, the presence of this functionality is entirely dependent on the application in use.
- **Tier 6 - Zero or little data loss** • Tier 6 Disaster Recovery solutions ***maintain the highest levels of data currency***. They are used by businesses with little or no tolerance for data loss and who need to restore data to applications rapidly. These solutions have no dependence on the applications to provide data consistency.
- **Tier 7 - Highly automated, business-integrated solution** • Tier 7 solutions include all the major components being used for a Tier 6 solution with the additional integration of automation. This allows a Tier 7 solution to ensure consistency of data above that of which is granted by Tier 6 solutions. Additionally, recovery of the applications is automated, allowing for restoration of systems and applications much faster and more reliably than would be possible through manual Disaster Recovery procedures.

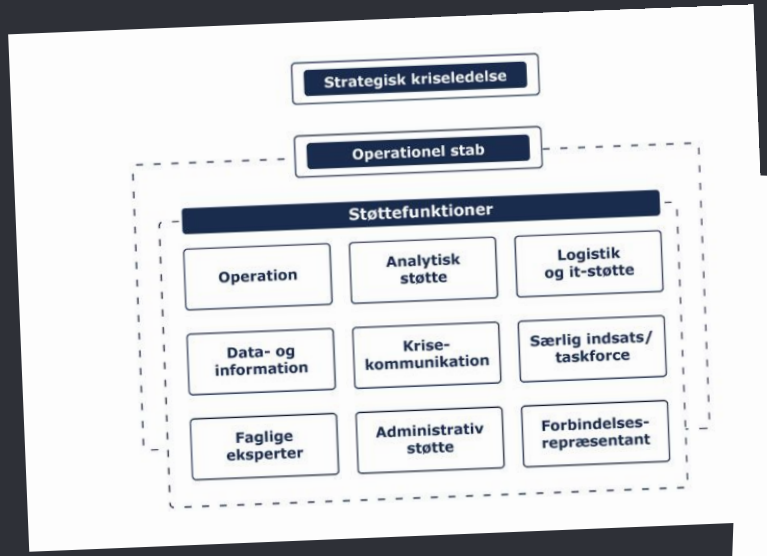
Link: https://en.wikipedia.org/wiki/Supply_chain
Link: https://en.wikipedia.org/wiki/Risk_management
Link: https://en.wikipedia.org/wiki/Business_continuity_planning

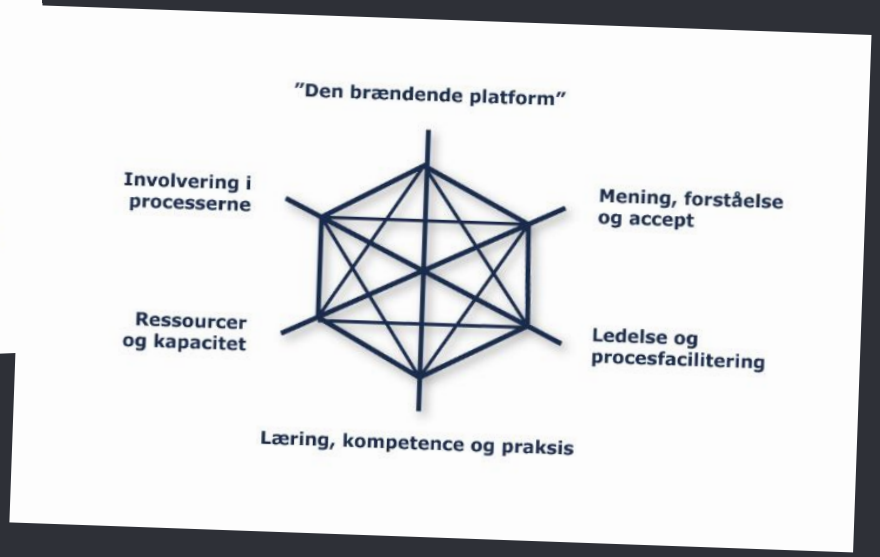
Disaster

When everything else fails - what then!

Part 1 - overall management

Overview





Link: https://www.brs.dk/da/redningsberedskab-myndighed/krisestyring2-og-beredskabsplanlagning/

Overview

Model A
Den basale

Forberedelse
- Overblik
- Tids- og aktivitetsplan

Planlægning
Alle ni opgaveområder, men særlig fokus:
- Struktur og organisering
- Ledelse
- Faciliteter, systemer og udstyr
- Forebyggelse

Formidling og forankring
- Introduktion ved et fællesmøde
- Afholdelse af en mindre øvelse

Model B
Den mere detaljerede

Forberedelse
- Overblik
- Tids- og aktivitetsplan
- Gennemgå vejledningen
- Rådgivning og vejledning
- Vurdering af eget beredskab
- Bidrag fra strategisk ledelse

Planlægning
Alle ni opgaveområder, men særlig fokus:
- Planlægningsgrundlag
- Struktur og organisering
- Ledelse
- Faciliteter, systemer og udstyr
- Forebyggelse
- Uddannelse og træning

Formidling og forankring
- Introduktion ved et fællesmøde
- Uddannelse af stab og støttefunktioner
- Øvelser for stab og støttefunktioner

Model C
Den fuldt udbyggede

Forberedelse
- Overblik
- Tids- og aktivitetsplan
- Gennemgå vejledningen
- Rådgivning og vejledning
- Vurdering af eget beredskab
- Bidrag fra strategisk ledelse
- Egne og andres erfaringer
- Kommissorium

Planlægning
Systematisk og grundig vurdering, analyse og afklaring af alle ni opgaveområder:
- Planlægningsgrundlag
- Struktur og organisering
- Ledelse, herunder strategisk forankring af beredskabsplanen
- Faciliteter, systemer og udstyr
- Forebyggelse
- Uddannelse og træning
- Øvelser
- Evaluering
- Implementering af læring

Formidling og forankring
- Introduktion ved fællesmøder
- Uddannelse af krisele-delse (strategisk), krisestab og støtte-funktioner m.fl.
- Øvelser for kriseledelse, krisestab og støtte-funktioner

Figur 2: Beredskabsplanlægning – tre modeller for processen

Link: https://www.brs.dk/da/redningsberedskab-myndighed/krisestyring2-og-beredskabsplanlagning/

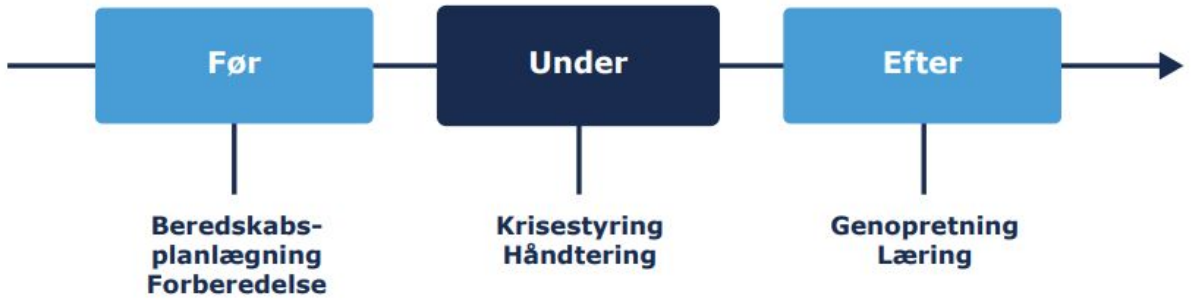
Overview

Beredskabsstyrelsen anbefaler, at organisationen:

- planlægger for både hverdagshændelser og for de sjældnere og mere omfattende, komplekse og langvarige hændelser
- ser tilbage, forholder sig til nuet, og tænker på kort, mellemlangt og langt sigt
- anvender de metoder, der passer til organisationens behov og foretrukne arbejdsformer
- gør brug af både kvantitative og kvalitative data
- henter inspiration i rapporter
- inddrager ekspertvurderinger
- nyttiggør erfaringer og læring fra tidligere hændelser og/eller øvelser
- opstiller risikoscenarier med fiktive hændelsesforløb.

Link: https://www.brs.dk/da/redningsberedskab-myndighed/krisestyring2-og-beredskabsplanlagning/

Overview



Figur 4: Før, under og efter kriser

Link: https://www.brs.dk/da/redningsberedskab-myndighed/krisestyring2-og-beredskabsplanlagning/

Disaster

When everything else fails - what then!

Part 2 - Incident Response

Prepare


I THINK WE MAY NEED TO UPDATE OUR DISASTER RECOVERY PLAN. THIS ONE SUGGESTS WE ALL RUN AROUND IN CIRCLES SHOUTING 'WHAT DO WE DO?!!' 'WHAT DO WE DO?!!'

The better preparation the faster to respond

Examples of escalation/collection

Escalation chart - severity escalation

Escalation Chart with Examples (This table is not inexhaustible)

severity	event	action	Capacity	Report to authorities	Preparation
level 1 (Low)	• potentially unwanted programs (PUP) • warning banners • clean alerts from antimalware solution • Adware	• Delete the files • Remove the software / service	• Normal operations • Register the event	no	• Normal service and follow up of Antimalware services.
level 2 (mid)	• Phishing • malware detected and deleted • Macro viruses	• Delete the files • Remove the software / service • Maybe look for online information.	• As level 1 • Escalate if more occurrences are detected	• As information only. Report, don't expect any investigation	• Normal service and follow up of Antimalware services. • validated and tested, response plan
level 3 (High severity and low spread)	• Copyright infringement • malware partially detected • Passwords leaks with e-mail • Spear phishing and data not delivered • Attempts to escalate privileges • Attempts of lateral movement • Usage of CVE 7+ vulnerabilities	• Escalate the Incident Response plan accordingly • Analyze the event to see what is the intention. • Set up monitoring for the events • Prepare for further events and inform management • Monitor closely for activity	• As level 2 • • Collection of data with integrity and timestamps (maybe Forensic less sound) • Carefully describe your process of evidence collection.	• Yes, share data and the identification findings. • Get case/report ID. • Get contact at the police and get JNR number (IT-engineer at NSK/NC3)	• The above, including below • Have updated and tested Incident Response plan • Forensic capability, and les forensic ways of data collection
level 4 (Critical, high impact - high spread - business critical)	• Zero days • APT • Malware not detected and activated • Spear phishing and data delivered • Services have been breached • Accounts have been escalated • Usage of CVE 7+ vulnerabilities	• Escalate the Incident Response plan accordingly • Create a communication plan if needed. (specially of company deliveries to the community) • Analyze the events for the intention. • Prepare 3'rd party	• As level 4 • Designate responsibility to file responsable. • Report to authorities (Get contact to appropriate level (NSK/NC3)) • Physical collect data from media if possible	• Yes, share data and the identification findings. • Get case/report ID • Get contact at the police and get JNR number (IT-engineer at NSK/NC3) • Prepare court case (if needed and	• Major incident plan. • Secondary communications channels

Examples of escalation/collection

A1 | Escalation Chart

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Escalation Chart														
2	Event	Action	Capacity	Preparation capability	Man lab	auto lab	Not WB	WB	Remote analysis	Isolation	Integrity calc	Report to authorities	Inform authorities	Sample Isolation	Severity
3	potentially unwanted programs (PUP)	remove program	monitor for recurrence	Corporate image					x		x				1
4	warning banners	remove program	monitor for recurrence	Corporate image					x		x				3
5	clean alerts from antimalware solution	remove program	monitor for recurrence	Corporate image					x		x				3
6	Adware	remove program	monitor for recurrence	Corporate image					x		x				4
7	Phishing	Rely on Spamfiltering	monitor for recurrence	Corporate image					x		x				5
8	Spear Phishing	analyse threat	analyze with detached system	Lab			x		x		x	x	x	x	8
9	malware detected and deleted	re-install system	monitor for recurrence	Corporate image		x			x	x	x				2
10	malware partially detected	re-stablish system from backup	monitor for recurrence	Corporate image		x			x	x	x				7
11	malwarebehaviour and not detected	re-install system	monitor for recurrence	Corporate image	x	x			x	x	x			x	10
12	Macro viruses	re-install system	monitor for recurrence	Corporate image					x		x			x	8
13	Copyright infringement	Withhold HW ans secure user traces	physical secure evidence	Writeblocker	x		x		x		x			x	10
14	Passwords leaks with e-mail	Change passwords and enable MFA	monitor for recurrence	Awareness plan			x		x		x				5
15	Spear phishing and data not delivered	Change passwords and enable MFA	monitor for recurrence	Awareness plan			x		x		x				4
16	Attempts to escalate privileges	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x		x		x	x	x	x	9
17	Attempts of lateral movement	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x		x		x	x	x	x	10
18	Usage of CVE 7+ vulnerabilities	re-stablish system from backup	inform senior management of risk	Corporate image + patch			x		x		x			x	9
19	CVE 7+ vulnerabilities identified	Create Risk analysis	governance plan	Forensic analysis and monitor	x		x		x		x				6
20	Rootkits detected on system	Determine MO and escalate to IR	datacollect and re-install	Forensic analysis and monitor	x		x		x		x	x	x	x	9
21	Remote Access Trojan (RAT)	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor	x		x		x		x	x	x	x	10
22	Zero days (internal systems/network)	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
23	Zero days (Facing Internet)	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor	x		x		x		x				10
24	APT	Determine MO and calculate risk	restore from backup	Forensic analysis and monitor	x		x		x		x	x	x	x	10
25	unpached systems	Roll into patch mangement	governance plan	Monitor activity			x		x		x				5
26	Malware not detected and activated	Determine action and severity	DFIR plan	Forensic analysis and monitor			x		x		x			x	10
27	Spear phishing and data delivered detected	Determine MO and calculate risk	inform senior management of risk	Monitor activity	x	x	x	x	x	x	x	x	x	x	10
28	Services have been breached	Analyze logs and periphials - restore	DFIR plan	Corporate image			x		x	x	x			x	10
29	Accounts have been escalated	Determine MO and escalate to IR	DFIR plan	Forensic analysis and monitor			x		x	x	x	x	x	x	8
30	Targeted attacks (unsuccessful)	Determine MO and calculate risk	inform senior management of risk	Forensic analysis and monitor	x	x	x		x		x			x	7
31	Targeted attacks (successful)	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x	x	x		x	x	x	x	x	x	10
32	Insider threats or paid actors	Determine MO and escalate to IR	DFIR plan	Forensic analysis	x		x	x	x		x	x	x	x	10
33	EOL software (Internal)	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
34	EOL software (external)	Determine MO and calculate risk	inform senior management of risk	vulnerability scanner			x		x		x				8
35	EOL hardware	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				4
36	Legacy systems	Create Risk analysis	governance plan	vulnerability scanner			x		x		x				5
37	User violated AUP	Determine MO and escalate accordingly	warn and inform (monitor)	Plan from HR	x	x	x	x	x	x	x	x	x	x	7
38	User violated AUP intentional	Determine MO and escalate accordingly	datacollect	Plan from HR	x	x	x	x	x	x	x	x	x	x	10

Decide your capability

Traditional forensics collection

- writeblock capability
- forensic sound collected data from hardware
- insider threats / malicious actors
- copyright infringements
- Chain of custody
- Witness colleagues (leader, HR etc.)

Data Collection as a bundle

- logs
- pictures (screenshots, mobile cell pictures)
- print to PDF
- save websites
- (“Save as” or “WGET”)
- Memory dump
- documents
- pictures (photos)
- collected remote (using remote agent)
- antimalware data
- OSINT links
- artefacts etc.

All described as a process

Pre-investigation

- Remote collection via agent
- Live collection of dynamic data (websites, drives, etc.)
- surrounding sources
- Indicators of compromise - IOC
- External sources (Virustotal, Joe sandbox, ect.)

Considerations for evidence?

- Data from more sources that point in the same direction (Triangulation)
- Data must prove the point
  (authenticity)
- Data that comes out of your observations
  (artefacts from systems, malware analysis … Your observables!)
- Data that show what happened and prove the point
  (A Well description of what happened and where its recorded)
- Data have to be admissible
  (Collected using legal methods)

Inspiration: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf
And : https://www.nist.gov/forensic-science/interdisciplinary-topics/evidence-management

Integrity is your file DNA

- Use good HASH like SHA256 to avoid hash collision
- Timestamps from the “snapshot”
- Describe the prerequisites of the collection
- Containerize the data, and turn on writeblock
- Make it easy to understand the data and describe it

Preserve the integrity

- Case-24052022-Incident_unwelcome_guests
  - Machine-PC23455_user_arne@virk.dk
  - Machine-PC27255_user_lise@virk.dk
  - Machine-PC45455_user_vibs@virk.dk
  - Server-SV-App234-DK-webserver

Machine-PC23455_user_arne@virk.dk

Navn	Ændringsdato	Type	Størrelse
File1.pptx	23-05-2022 20:27	Microsoft PowerPo...	0 KB
File2.pub	23-05-2022 20:27	Microsoft Publishe...	59 KB
File3.pub	23-05-2022 20:26	Microsoft Publishe...	59 KB
File4.docx	23-05-2022 20:26	Microsoft Word-d...	0 KB
File5.docx	23-05-2022 20:26	Microsoft Word-d...	0 KB
File6.rtf	23-05-2022 20:26	RTF-format	1 KB
File7.xlsx	23-05-2022 20:28	Microsoft Excel-re...	7 KB
HASH_Machine-PC23455_user_arne@	5-2022 20:24	Tekstdokument	1 KB

```
121CF9D2076962FD7D84A67129421915E626E59FB9D2EC8F89E35C7441553E6A  App\AppInfo\File1
573CED9FB3B5DBD183EF144532F3D36CB7D7EF444DC563B7243298DB2359E2DB  App\AppInfo\File2
F17B6E607BFB06E03551AEECE1BC928C0A9E80A42AD12CBE84FC5220145F6225  App\AppInfo\File3
C2048C3343F7837E43887D7AADE05411C165E796DFB82B0CF42438D50810FAE2  App\AppInfo\File4
AE0EEF67EDF75DD9C15E0C2B5653C8628AD42DED2BA0495F9A68E55E439AAD42  App\AppInfo\File5
2C101D62FFE213264CD69DA2118BC1735F2002BAD19C701937E046785BA71570  App\AppInfo\File6
1EBED2D9CD92376A0A27EEBC8C6C54C371DDDDB9F92E7FFFAE878EFCDC8B6059  App\AppInfo\File7
```

- Machine-PC23455_user_arne@virk.dk
- Machine-PC27255_user_lise@virk.dk
- Machine-PC45455_user_vibs@virk.dk
- Server-SV-App234-DK-webserver
- Machine-PC23455_user_arne@virk.dk_2361561673F42360C0431033D379D57C800E64FBB83465D042F764003C165356.zip

The better preparation the faster to respond

- Collect the tools in a jump bag
  - Preserve the evidence
    - Writeblock (HW/SW)
  - Prepare your software
  - Physical tools
  - IT-security plans (printed)

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

The better preparation the faster to respond

- Have a forensic room
  - Analyze the evidence
  - Extra USB-drives and hard drives
  - Dedicated hardware
  - Monitor activity (who gets in and out)
  - Physical preserve evidence
  - Trusted personnel only

CYBER SKILLS

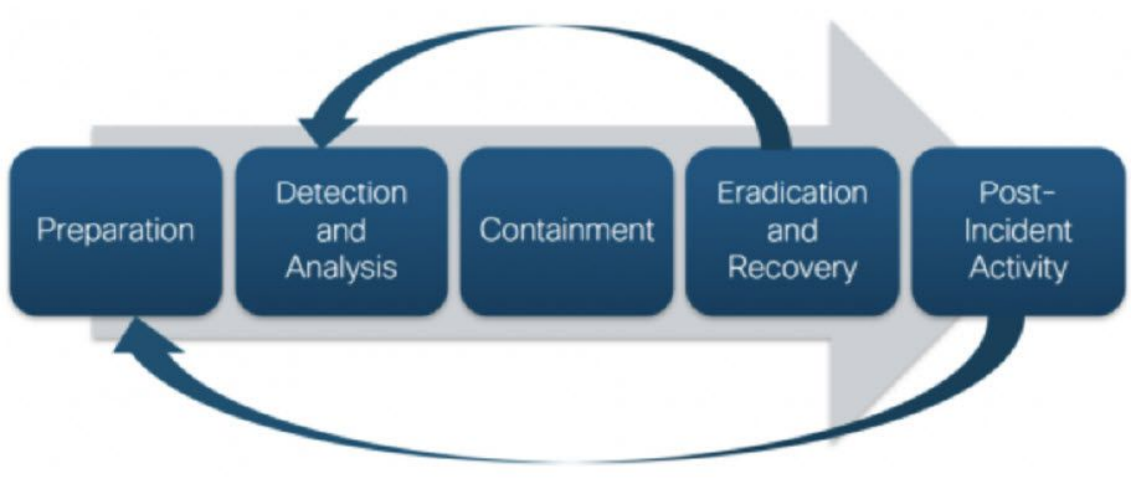
KØBENHAVNS ERHVERVSAKADEMI

The better preparation the faster to respond

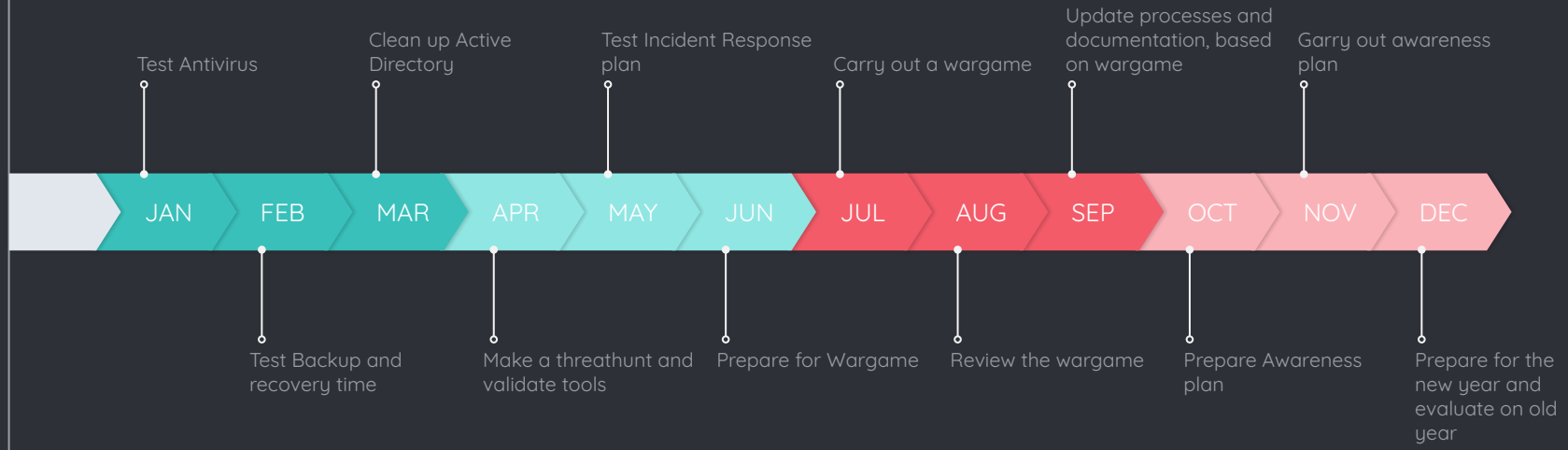
Have a clear plan

- Who is on call
- Who have the mandate to make decisions
- Who is responsible for communication
- Who are the tech people investigating
- Have this highlighted next to the war room
  (War Room is a place where the Incident team is placed)

Preparation is key



Timeline


Test Antivirus
Clean up Active Directory
Test Incident Response plan
Carry out a wargame
Update processes and documentation, based on wargame
Garry out awareness plan
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
Test Backup and recovery time
Make a threathunt and validate tools
Prepare for Wargame
Review the wargame
Prepare Awareness plan
Prepare for the new year and evaluate on old year

Plan ahead

Service Wheel is an ongoing task

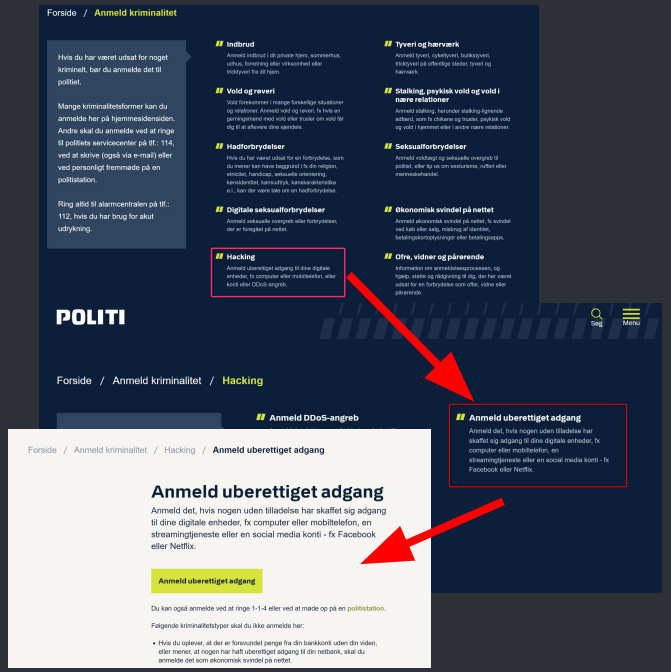
It's easier to prepare the tasks throughout the year

You get visibility to what needs to be carried out

Report or not

Do the business report or not
If so, to who?

The Authorities - Ask before you report



Link = https://politi.dk/anmeld-kriminalitet

Why the authorities?

- Give the authorities the power to **investigate and prosecute as they are supposed to do.** Else cybercrime will continue!

- We need to keep **politicians accountable and informed!** To make decisions going forward!

This will increase the **chance of an investigation and prosecution**

Why collect data?

Kære ,

De har 2021 anmeldt afpresning via ransomware til politiet. I den forbindelse har vi brug for de nedenfor oplistede oplysninger for at kunne behandle Deres sag:

- Baggrundsbillede eller tekstfil, som gerningsmanden har lagt på computeren, hvor der angives kontaktoplysninger. Helst original format.
- 3 krypterede filer på max ca. 5 mb. Gerne .zip eller .7Z fil.
- Kopi af filer, programmer eller andet der ved gennemgang af serveren findes efterladt af gerningsmændene. Fx krypteringssoftwaren. Gerne som .zip eller .7Z fil.
- Hvis det konstateres at adgangen til forurettedes computer var gennem RDP (Remote Desktop Port), så hvis muligt en kopi af hele loggen for den kompromitterede RDP port.
- Kopi af spor som gerningsmændene har efterladt i deres forsøg på at fremme deres brugerstatus.

Hvis der eventuelt skulle være andet på computerne/serverne, som I vurderer kunne have interesse for sagen, så et kopi af dette.

- Dokumentation for køb af Bitcoins i form af udvidet betalings- / overførselskvittering.
- Dokumentation for overførsel af de oplyste BTC sammen med dokumentation for afsender og modtageradresser.
- Redegørelse for hvorvidt forurettede eller dennes repræsentant har rettet henvendelse til kryptobørser eller lignende med henblik på indsigelse. I bekræftende fald dokumentation herfor.
- Mailkorrespondance med gerningsmanden (vedhæftet mails fra gerningsmanden fra første mail-modtager, så mailheaderen kan udlæses).
- Dekrypteringsfiler typisk decrypt.exe, som blev benyttet til at låse filerne op.

Det hele må gerne samles i en .zip eller .7Z fil.

Det er politiets anbefaling, at der ikke betales løsesum.

- Der er mulighed for at finde dekrypteringsværktøjer på NoMoreRansom.org, der måske kan dekryptere jeres filer. Alternativt kan harddisken gemmes, da siden opdateres løbende.

Dokumenterne bedes i én sammenfattende e-mail sendt hurtigst muligt og senest inden 14 dage til adressen: KBH-LCIK-sek3@politi.dk -I emnefeltet bedes De skrive journalnummeret: 01 LC-.

Når politiet modtager dokumenterne, vil de blive vedlagt Deres sag. Såfremt De har spørgsmål, bedes De rette henvendelse på e-mail: KBH-LCIK@politi.dk

Såfremt politiet ikke modtager oplysningerne, kan det betyde, at politiet ikke har mulighed for at efterforske sagen.

Side 1

Såfremt politiet ikke modtager oplysningerne, kan det betyde, at politiet ikke har mulighed for at efterforske sagen.

What now?

Your path

What is your path?

What do you like?

- Pentest - breaking stuff
- GDPR - DPO and privacy
- Management - ISO, NIST, CIS
- Incident Response - Protection and mitigation
- Education - Training others in awareness
- Development - program the future

What is your path?

How do i find out ?

- Get into the network
- Get out and look for arrangements like cyberskills
- Test out what the different areas include
- Buy a book or two to read about the topic.

The technical path?

- What is the requirements out here?
- What do the business need?
- Make sure there are jobs you can apply

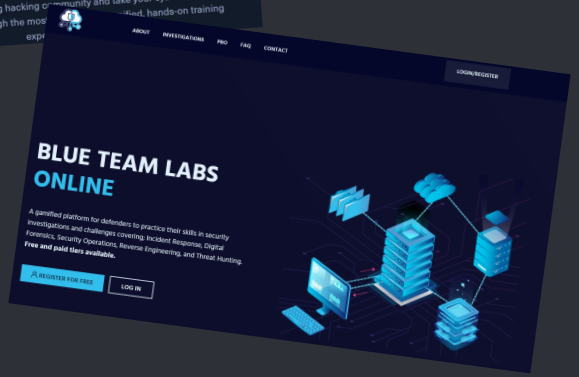
CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

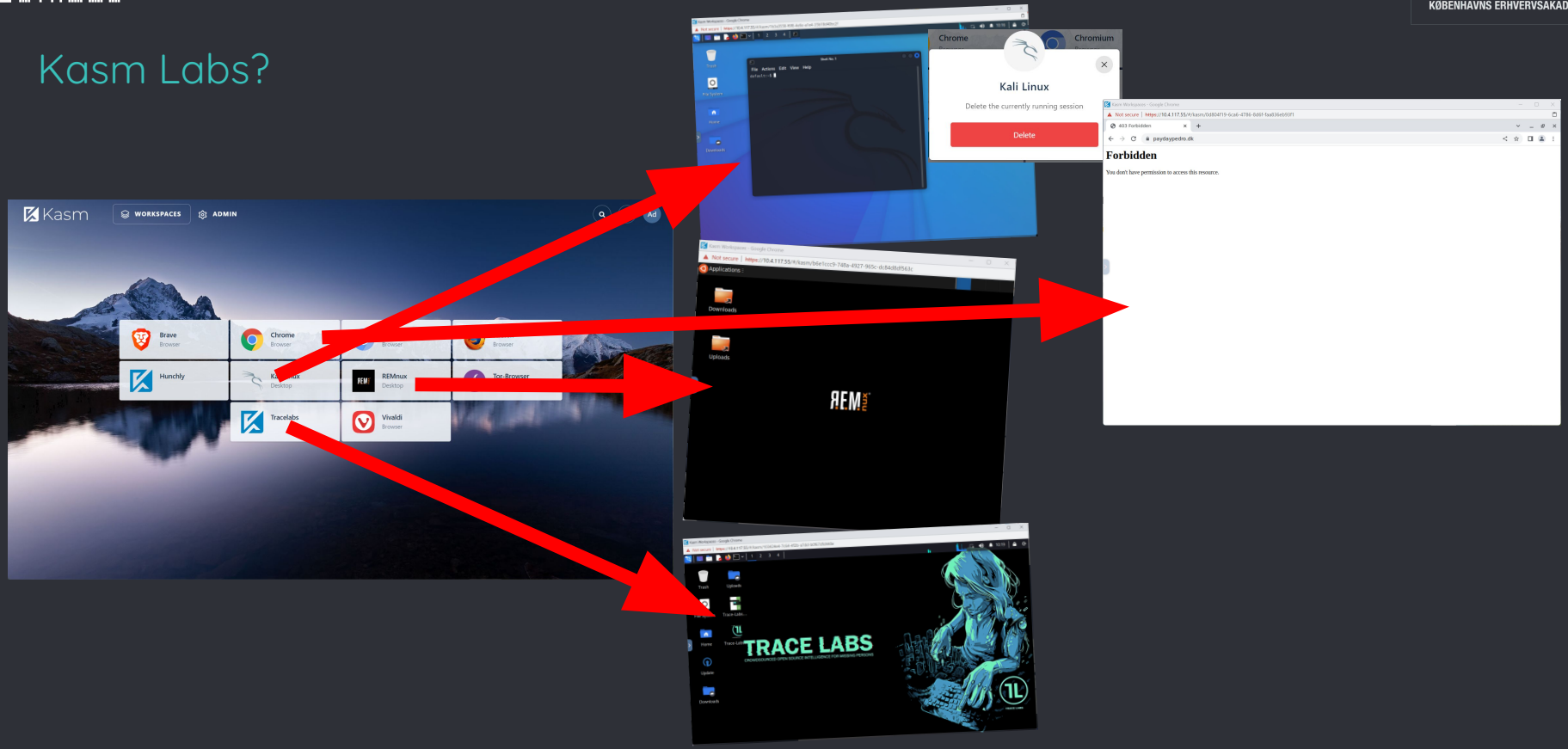
Try what you like

Start online

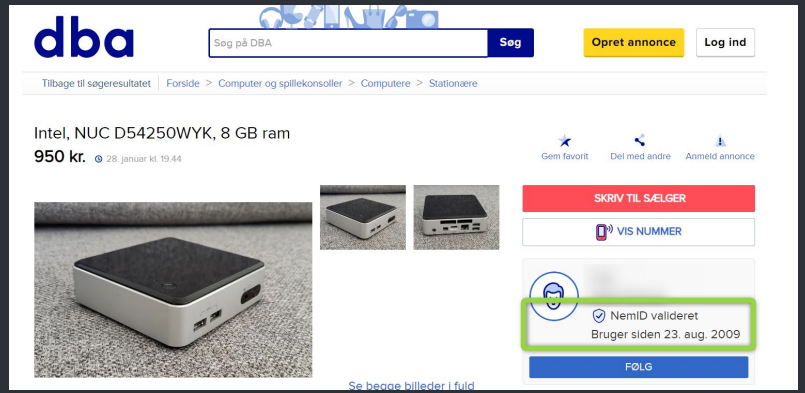
- Tryhackme.com
- Hackthebox.com
- blueteamlabs.online



Kasm Labs?


Kasm
WORKSPACES
ADMIN
Brave
Browser
Chrome
Browser
Hunchly
REMnux
Desktop
Tor Browser
Tracelabs
Vivaldi
Browser
Chrome
Chromium
Kali Linux
Delete the currently running session
Delete
Forbidden
You don't have permission to access this resource.
Downloads
Uploads
TRACE LABS

What can i use ?



CYBER SKILLS

kea KØBENHAVNS ERHVERVSAKADEMI

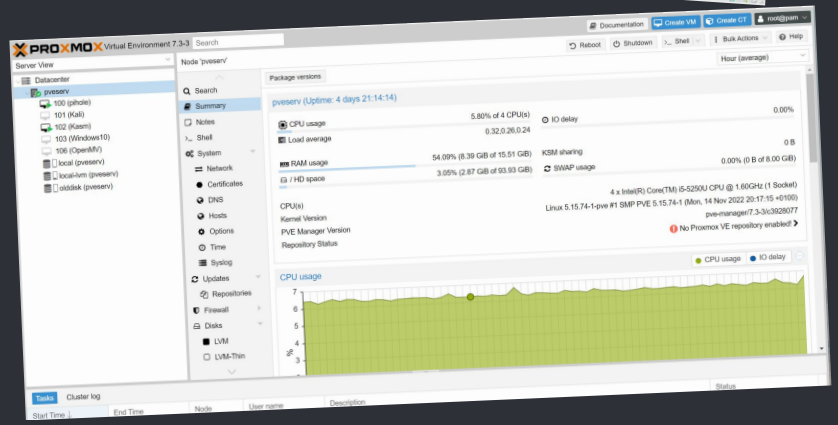
Create a lab ?

Physical hardware
(Old tech that is not used)

Virtual machines

Proxmox hypervisor

- kali linux
- linux
- windows
- Kasm (streaming apps to browser)



The Strategic path?

- What is the requirements out here?
- Frameworks for your business, there are so many others
- Learn the management decision making
- Know how the communication works

CYBER SKILLS

kea KØBENHAVNS ERHVERVSAKADEMI

Look at the frameworks ?

- NIST Cybersecurity Framework (fx NIST SP 800-53)
- ISO 27001 and ISO 27002 and (CIS controls and the guides they provide)
- SOC2
- PCI-DSS
- HIPAA
- GDPR (ISO 27701)
- FISMA
- COBIT (ISACA)
- CMMC (Cybersecurity Maturity Model Certification)
- European Union Agency for Cybersecurity (ENISA) National Capabilities Assessment Framework
- MITRE ATT&CK
- National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)

Link: https://securityscorecard.com/blog/top-cybersecurity-frameworks-to-consider

One Last Thing

Often not said - Taboo

Imposter

Syndrome

Why i brought this up

- I have met with a lot of students that have had this feeling
- I have the same feeling from time to time
- Its normal to experience this up to the exam

Disclaimer

Im not an expert, i sought the guide from out big friend the Internet and chat GPT.

What is that ?

- Imposter syndrome is a psychological phenomenon in which an individual doubts their own abilities, feels like a fraud, and fears being exposed as such despite evidence of their competence and accomplishments.
- People with imposter syndrome often believe that they are not deserving of their success or that they have somehow tricked others into thinking that they are competent.
- This feeling of inadequacy can be especially prevalent in high-achieving individuals, such as academics, professionals, and artists. It can lead to anxiety, stress, and self-doubt, and may negatively impact one's personal and professional life.
- It is important to recognize and address imposter syndrome so that one can gain the confidence and self-esteem needed to succeed and thrive.

Kilde: https://dm.dk/nyheder/2020/fem-raad-til-dig-der-lider-af-impostor-faenomenet

Why is that present?

Copied from article

"I forhold til den præstationskultur, som hersker i dag, så er der forskning, der tyder på, at præstationskultur fremmer aktivitet i den del af hjernen som knytter sig til at præstere og rangordne i et hierarki mellem os", siger Lise August

Kilde: https://dm.dk/nyheder/2020/fem-raad-til-dig-der-lider-af-impostor-faenomenet

How to fix it?

Overcoming imposter syndrome can be a challenging process, but there are several strategies that may be helpful:

- Acknowledge your feelings: **Recognize that feeling like an imposter is a common experience, and that you are not alone in feeling this way.**
- Identify your strengths: Make a list of your accomplishments and skills. Recognize your own abilities and acknowledge your achievements.
- **Set realistic expectations: Be realistic about your abilities and set achievable goals. Remember that it is okay to make mistakes and that failure is a normal part of the learning process.**
- Learn from others: Seek out mentorship or guidance from others who have experienced imposter syndrome. **Learn from their experiences and strategies for overcoming self-doubt**.
- Practice self-care: Take care of yourself physically, emotionally, and mentally. Engage in activities that make you feel good about yourself and that help you manage stress.

Kilde: https://dm.dk/nyheder/2020/fem-raad-til-dig-der-lider-af-impostor-faenomenet

My Interpretation

A few thoughts

- You have all the possibilities at your feet
- You are as equal as everyone else
- Expectation align with you delivery
- Trust you self, you are more capable than you think
- Do you best

Kilde: https://dm.dk/nyheder/2020/fem-raad-til-dig-der-lider-af-impostor-faenomenet

Company expectation?

A company should be willingly to this

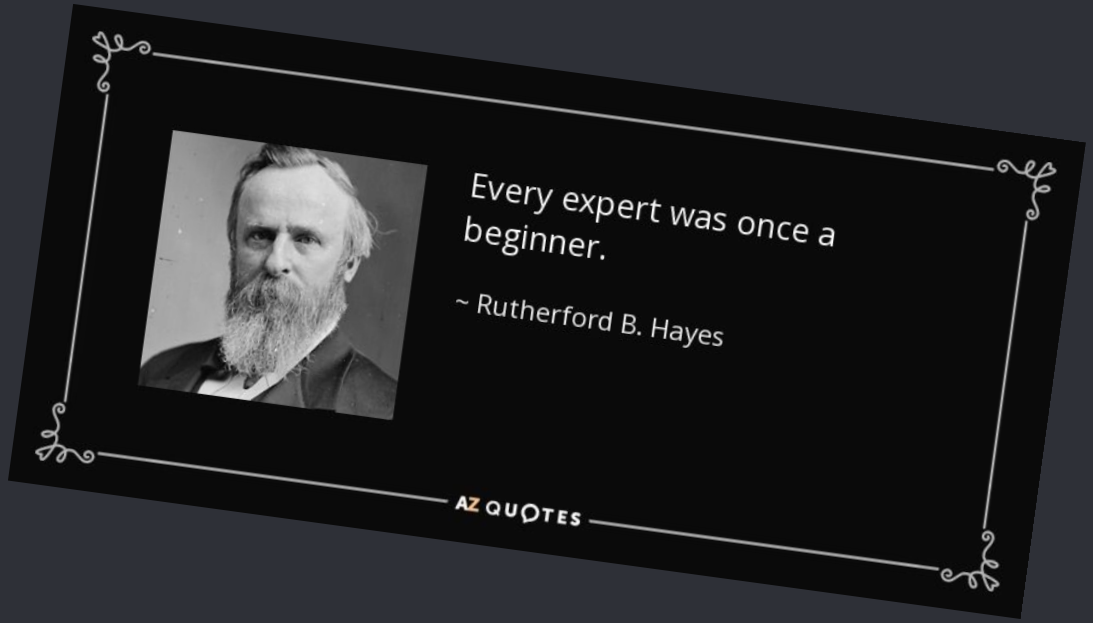
- Support your growth
- Support you needs
- Have good colleagues that support / coach you

Requirements of you

- Want to learn
- Curious
- Fail and accept the learning
- Be part of the assignments, no matter if you have the skills or not

Kilde: https://dm.dk/nyheder/2020/fem-raad-til-dig-der-lider-af-impostor-faenomenet

How to fix it?


Every expert was once a beginner.
~ Rutherford B. Hayes
AZ QUOTES

Round up

Summarize

Takeaways

- Know the framework in your company
- Get into the process and understand the key areas
- Build you own space here and argument your choices
- Know how to “sell” your arguments.
- Believe in your self

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

The most important!!!

Help each other be better in the IT-security world

If you see anything out of the ordinary

-

ACT ON IT!

CYBER SKILLS

KØBENHAVNS ERHVERVSAKADEMI

Thanks!

ANY QUESTIONS?

Slideshow
https://defencia.dk/