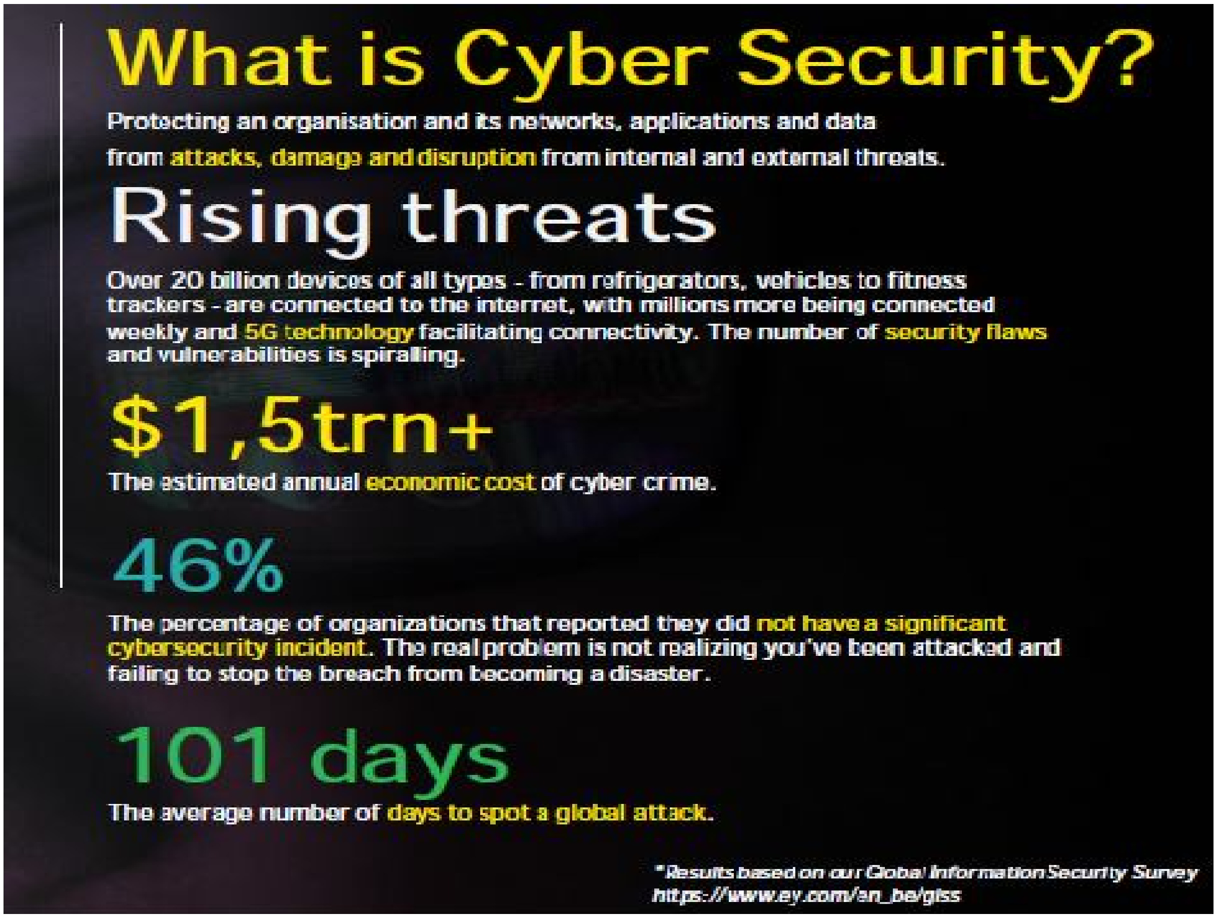
CYBER SECUTIRY MANAGEMENT
FD 5.9

What comes to mind when you think of Cyber Security Management?



What is Cyber Security?

Protecting an organisation and its networks, applications and data from attacks, damage and disruption from internal and external threats.

Rising threats

Over 20 billion devices of all types - from refrigerators, vehicles to fitness trackers - are connected to the internet, with millions more being connected weekly and 5G technology facilitating connectivity. The number of security flaws and vulnerabilities is spiralling.

$1,5trn+

The estimated annual economic cost of cyber crime.

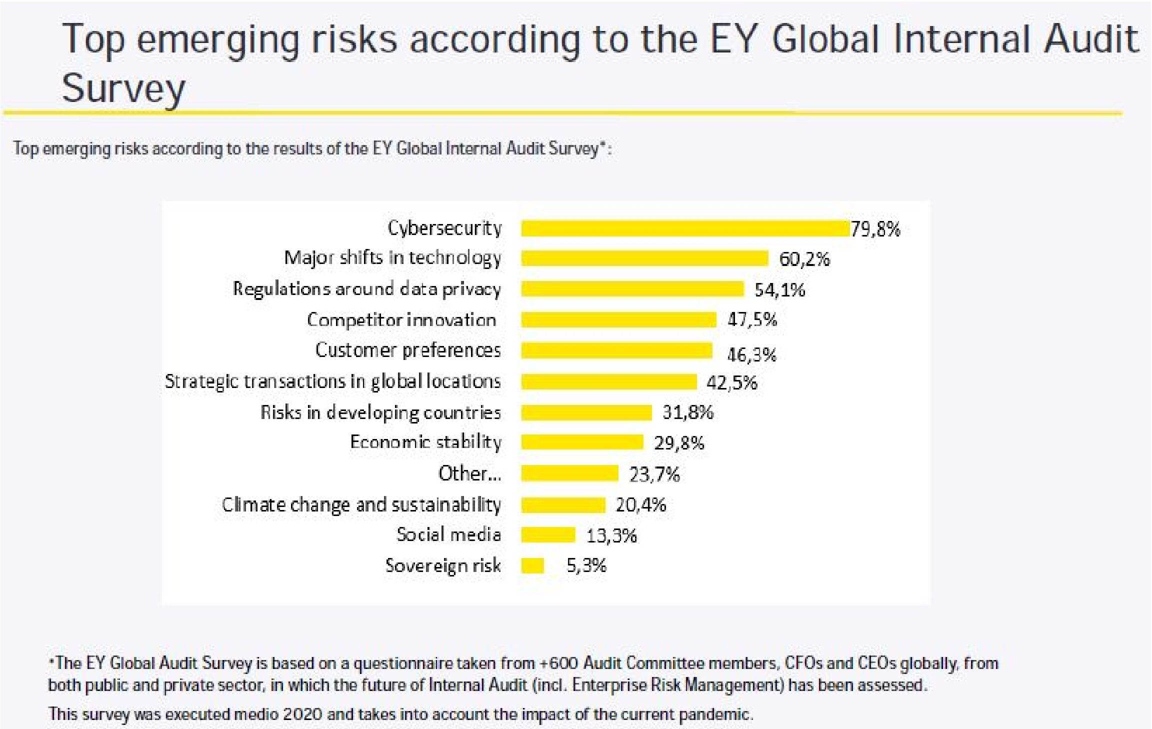
46%

The percentage of organizations that reported they did not have a significant cybersecurity incident. The real problem is not realizing you've been attacked and failing to stop the breach from becoming a disaster.

101 days

The average number of days to spot a global attack.

**Results based on our Global Information Security Survey*
https://www.ey.com/en_be/giss

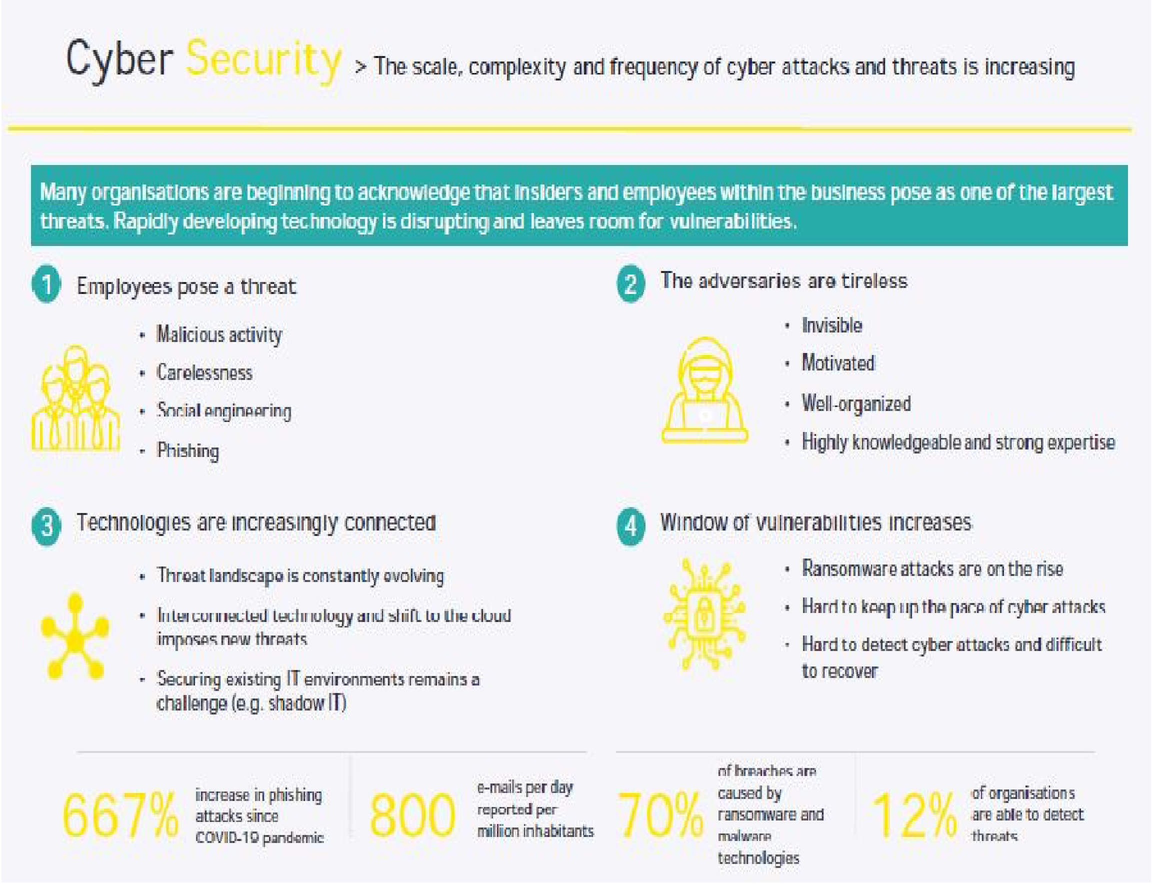


Top emerging risks according to the EY Global Internal Audit Survey

Top emerging risks according to the results of the EY Global Internal Audit Survey*:

*The EY Global Audit Survey is based on a questionnaire taken from +600 Audit Committee members, CFOs and CEOs globally, from both public and private sector, in which the future of Internal Audit (incl. Enterprise Risk Management) has been assessed.

This survey was executed medio 2020 and takes into account the impact of the current pandemic.



Cyber Security > The scale, complexity and frequency of cyber attacks and threats is increasing

Many organisations are beginning to acknowledge that insiders and employees within the business pose as one of the largest threats. Rapidly developing technology is disrupting and leaves room for vulnerabilities.

1 Employees pose a threat

- Malicious activity
- Carelessness
- Social engineering
- Phishing

2 The adversaries are tireless

- Invisible
- Motivated
- Well-organized
- Highly knowledgeable and strong expertise

3 Technologies are increasingly connected

- Threat landscape is constantly evolving
- Interconnected technology and shift to the cloud imposes new threats
- Securing existing IT environments remains a challenge (e.g. shadow IT)

4 Window of vulnerabilities increases

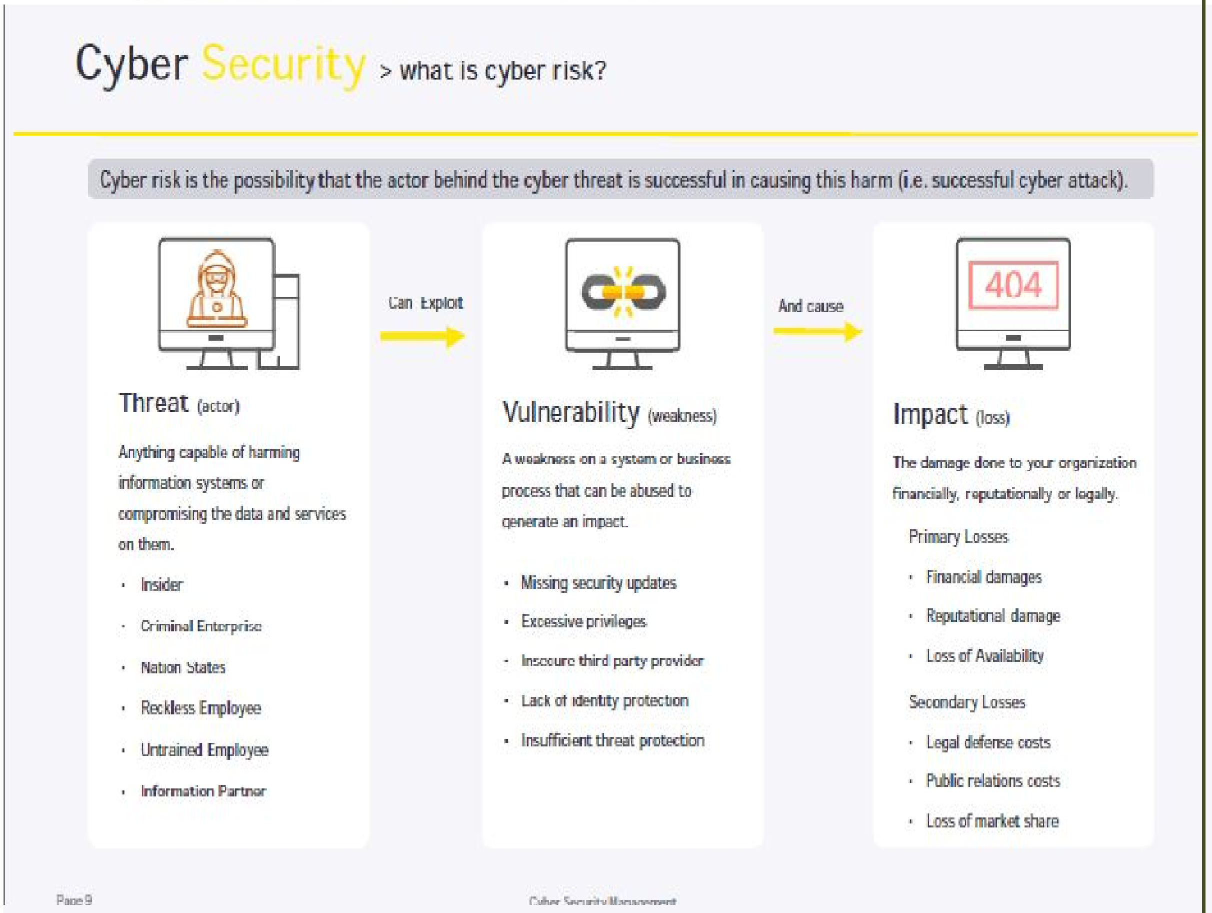
- Ransomware attacks are on the rise
- Hard to keep up the pace of cyber attacks
- Hard to detect cyber attacks and difficult to recover

667% increase in phishing attacks since COVID-19 pandemic

800 e-mails per day reported per million inhabitants

70% of breaches are caused by ransomware and malware technologies

12% of organisations are able to detect threats



Cyber Security > what is cyber risk?

Cyber risk is the possibility that the actor behind the cyber threat is successful in causing this harm (i.e. successful cyber attack).

Threat (actor)

Anything capable of harming information systems or compromising the data and services on them.

- Insider
- Criminal Enterprise
- Nation States
- Reckless Employee
- Untrained Employee
- Information Partner

Vulnerability (weakness)

A weakness on a system or business process that can be abused to generate an impact.

- Missing security updates
- Excessive privileges
- Insecure third party provider
- Lack of identity protection
- Insufficient threat protection

Impact (loss)

The damage done to your organization financially, reputationally or legally.

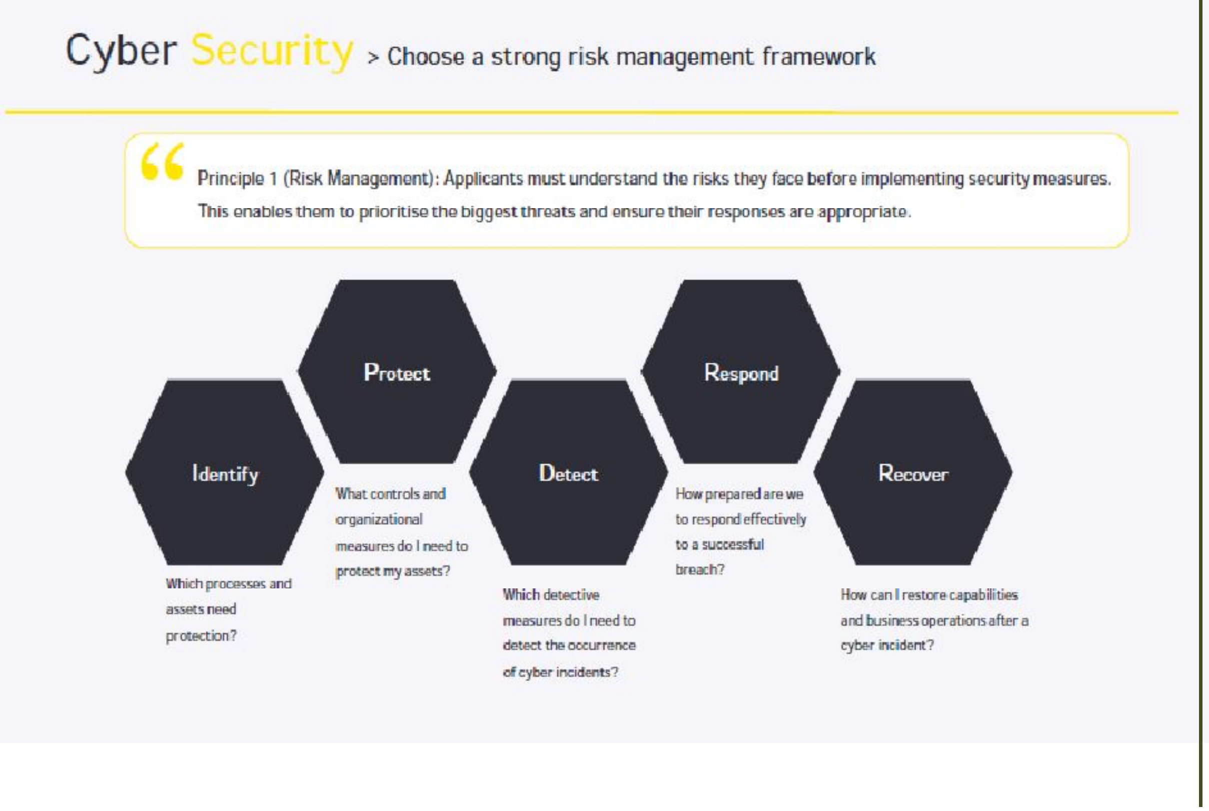
Primary Losses

- Financial damages
- Reputational damage
- Loss of Availability

Secondary Losses

- Legal defense costs
- Public relations costs
- Loss of market share

Page 9 Cyber Security Management



Cyber Security > Choose a strong risk management framework

> Principle 1 (Risk Management): Applicants must understand the risks they face before implementing security measures. This enables them to prioritise the biggest threats and ensure their responses are appropriate.

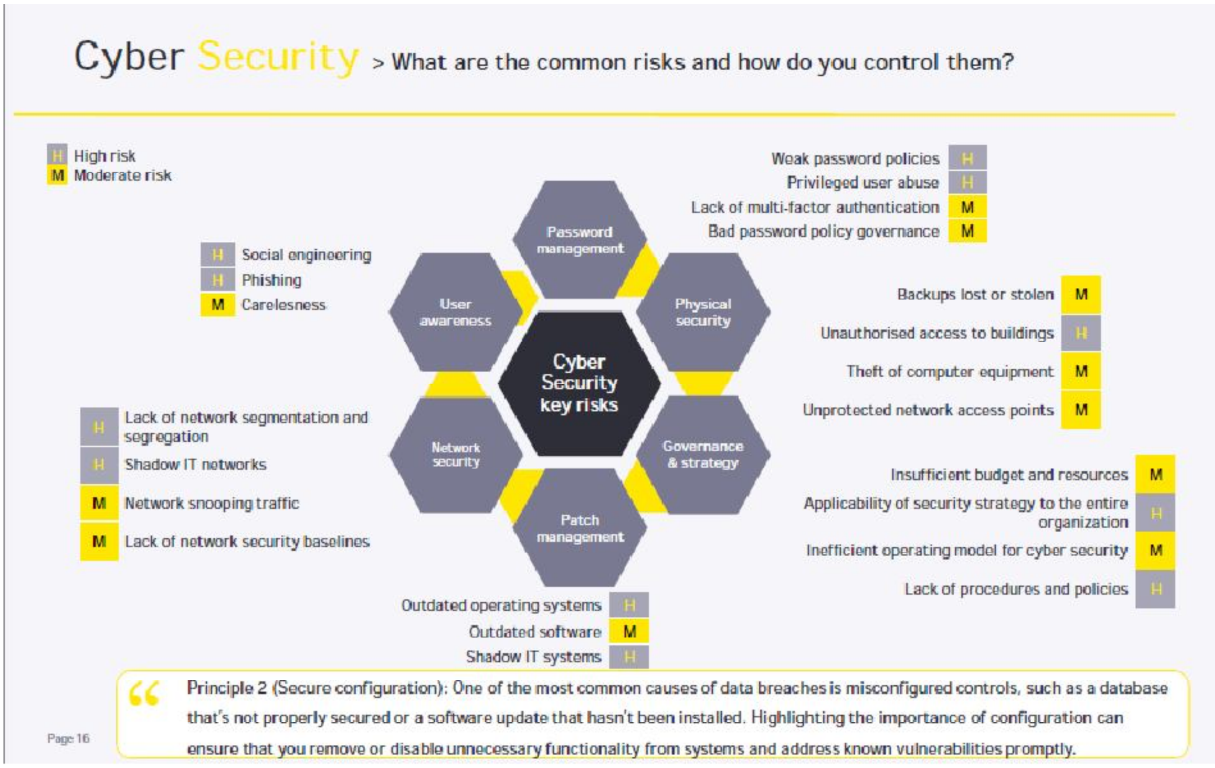
Identify – Which processes and assets need protection?

Protect – What controls and organizational measures do I need to protect my assets?

Detect – Which detective measures do I need to detect the occurrence of cyber incidents?

Respond – How prepared are we to respond effectively to a successful breach?

Recover – How can I restore capabilities and business operations after a cyber incident?



Cyber Security > What are the common risks and how do you control them?

H High risk
M Moderate risk

Password management:

Risk	Level
Weak password policies	H
Privileged user abuse	H
Lack of multi-factor authentication	M
Bad password policy governance	M

User awareness:

Level	Risk
H	Social engineering
H	Phishing
M	Carelessness

Physical security:

Risk	Level
Backups lost or stolen	M
Unauthorised access to buildings	H
Theft of computer equipment	M
Unprotected network access points	M

Network security:

Level	Risk
H	Lack of network segmentation and segregation
H	Shadow IT networks
M	Network snooping traffic
M	Lack of network security baselines

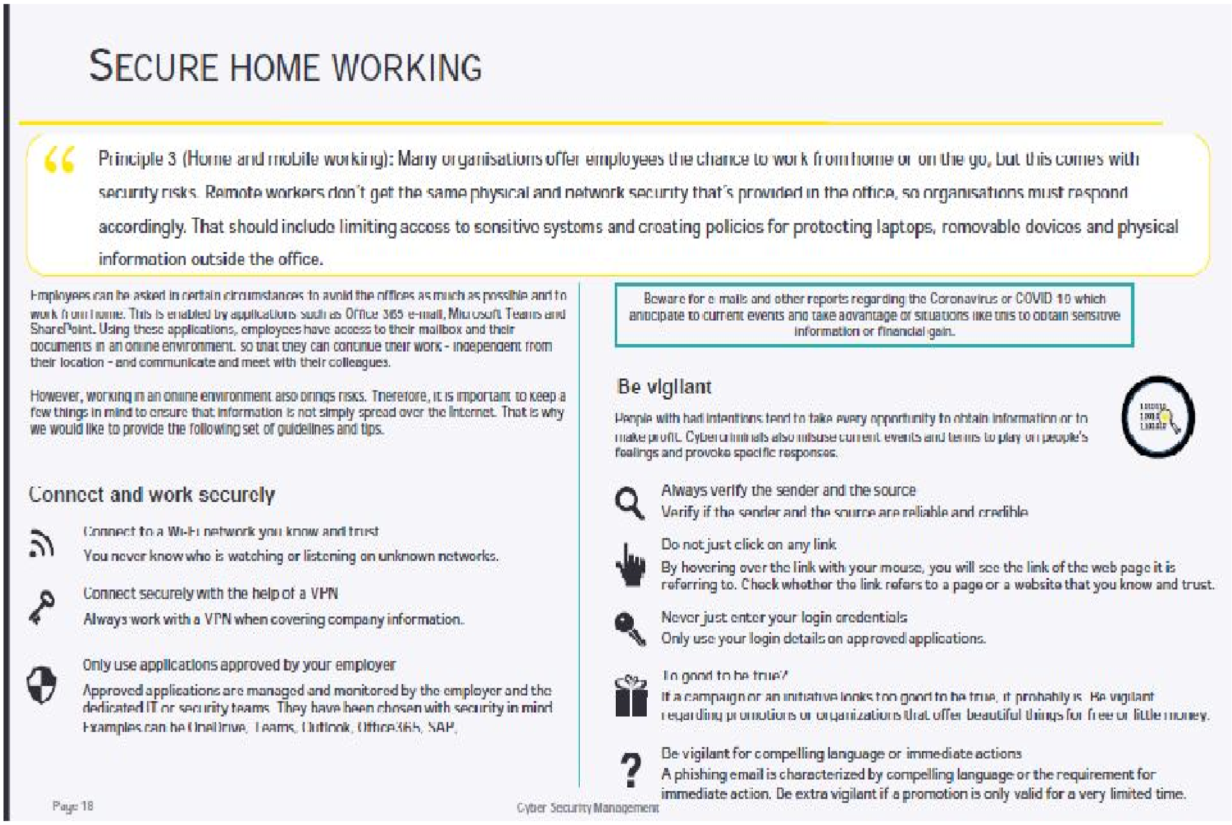
Governance & strategy:

Risk	Level
Insufficient budget and resources	M
Applicability of security strategy to the entire organization	H
Inefficient operating model for cyber security	M
Lack of procedures and policies	H

Patch management:

Risk	Level
Outdated operating systems	H
Outdated software	M
Shadow IT systems	H

> Principle 2 (Secure configuration): One of the most common causes of data breaches is misconfigured controls, such as a database that's not properly secured or a software update that hasn't been installed. Highlighting the importance of configuration can ensure that you remove or disable unnecessary functionality from systems and address known vulnerabilities promptly.



SECURE HOME WORKING

> Principle 3 (Home and mobile working): Many organisations offer employees the chance to work from home or on the go, but this comes with security risks. Remote workers don't get the same physical and network security that's provided in the office, so organisations must respond accordingly. That should include limiting access to sensitive systems and creating policies for protecting laptops, removable devices and physical information outside the office.

Employees can be asked in certain circumstances to avoid the offices as much as possible and to work from home. This is enabled by applications such as Office 365 e-mail, Microsoft Teams and SharePoint. Using these applications, employees have access to their mailbox and their documents in an online environment, so that they can continue their work - independent from their location - and communicate and meet with their colleagues.

However, working in an online environment also brings risks. Therefore, it is important to keep a few things in mind to ensure that information is not simply spread over the Internet. That is why we would like to provide the following set of guidelines and tips.

Connect and work securely

Connect to a Wi-Fi network you know and trust
You never know who is watching or listening on unknown networks.

Connect securely with the help of a VPN
Always work with a VPN when covering company information.

Only use applications approved by your employer
Approved applications are managed and monitored by the employer and the dedicated IT or security teams. They have been chosen with security in mind. Examples can be OneDrive, Teams, Outlook, Office365, SAP.

Beware for e-mails and other reports regarding the Coronavirus or COVID 19 which anticipate to current events and take advantage of situations like this to obtain sensitive information or financial gain.

Be vigilant

People with bad intentions tend to take every opportunity to obtain information or to make profit. Cybercriminals also misuse current events and terms to play on people's feelings and provoke specific responses.

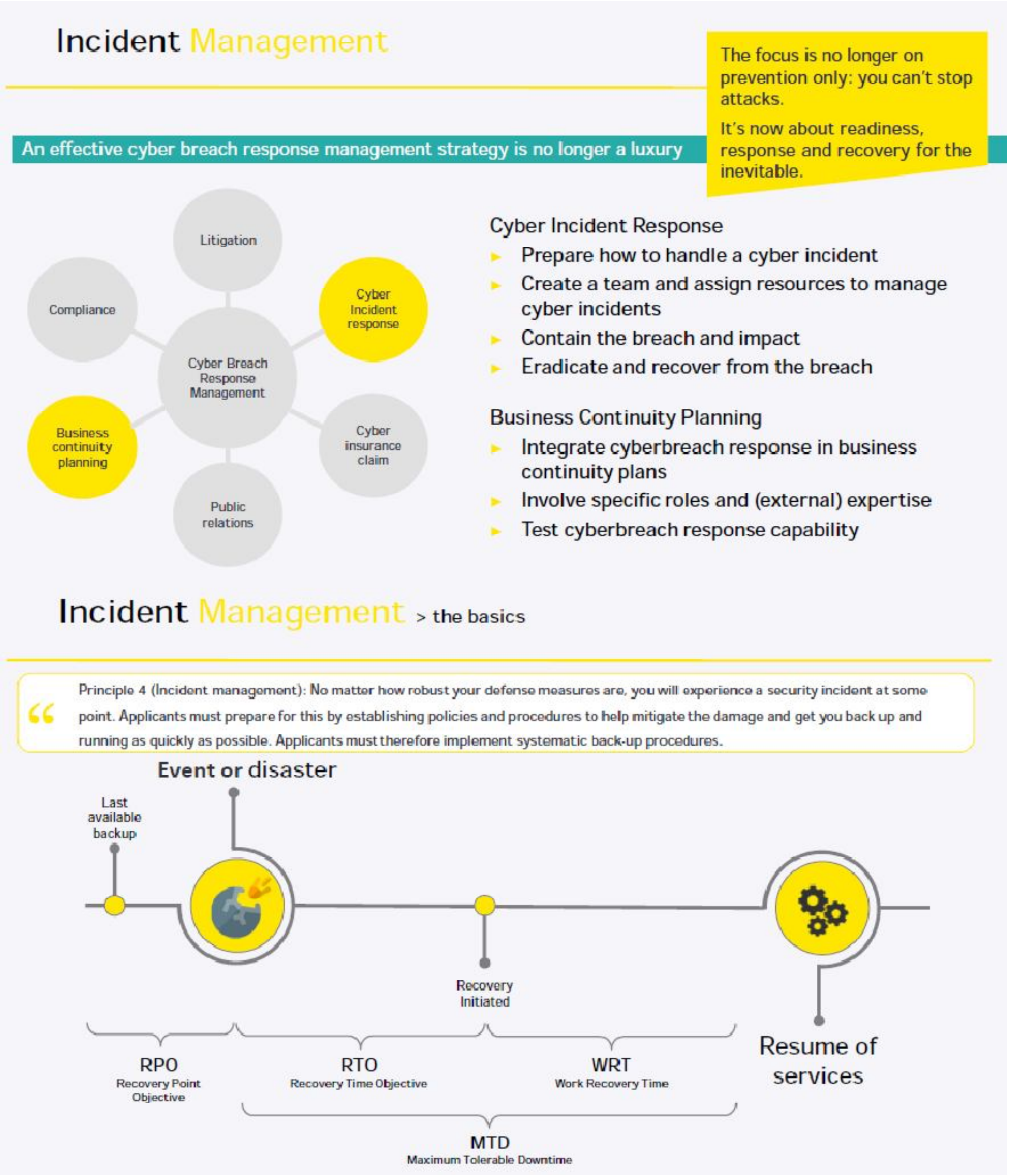
Always verify the sender and the source
Verify if the sender and the source are reliable and credible

Do not just click on any link
By hovering over the link with your mouse, you will see the link of the web page it is referring to. Check whether the link refers to a page or a website that you know and trust.

Never just enter your login credentials
Only use your login details on approved applications.

To good to be true?
If a campaign or an initiative looks too good to be true, it probably is. Be vigilant regarding promotions or organizations that offer beautiful things for free or little money.

Be vigilant for compelling language or immediate actions
A phishing email is characterized by compelling language or the requirement for immediate action. De extra vigilant if a promotion is only valid for a very limited time.



Incident Management

An effective cyber breach response management strategy is no longer a luxury

The focus is no longer on prevention only: you can't stop attacks.

It's now about readiness, response and recovery for the inevitable.

Cyber Incident Response

- Prepare how to handle a cyber incident
- Create a team and assign resources to manage cyber incidents
- Contain the breach and impact
- Eradicate and recover from the breach

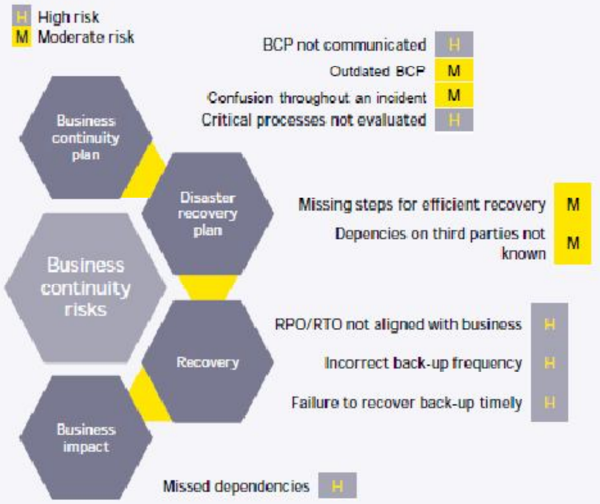
Business Continuity Planning

- Integrate cyberbreach response in business continuity plans
- Involve specific roles and (external) expertise
- Test cyberbreach response capability

Incident Management > the basics

> “ Principle 4 (Incident management): No matter how robust your defense measures are, you will experience a security incident at some point. Applicants must prepare for this by establishing policies and procedures to help mitigate the damage and get you back up and running as quickly as possible. Applicants must therefore implement systematic back-up procedures.

Incident Management > What are the common risks and how do you control them?



H High risk
M Moderate risk

BCP not communicated	H
Outdated BCP	M
Confusion throughout an incident	M
Critical processes not evaluated	H
Missing steps for efficient recovery	M
Depencies on third parties not known	M
RPO/RTO not aligned with business	H
Incorrect back-up frequency	H
Failure to recover back-up timely	H
Missed dependencies	H

Incident Management > points of attention

1 Who takes what responsibility?
Management?
Process owner?
ICT?

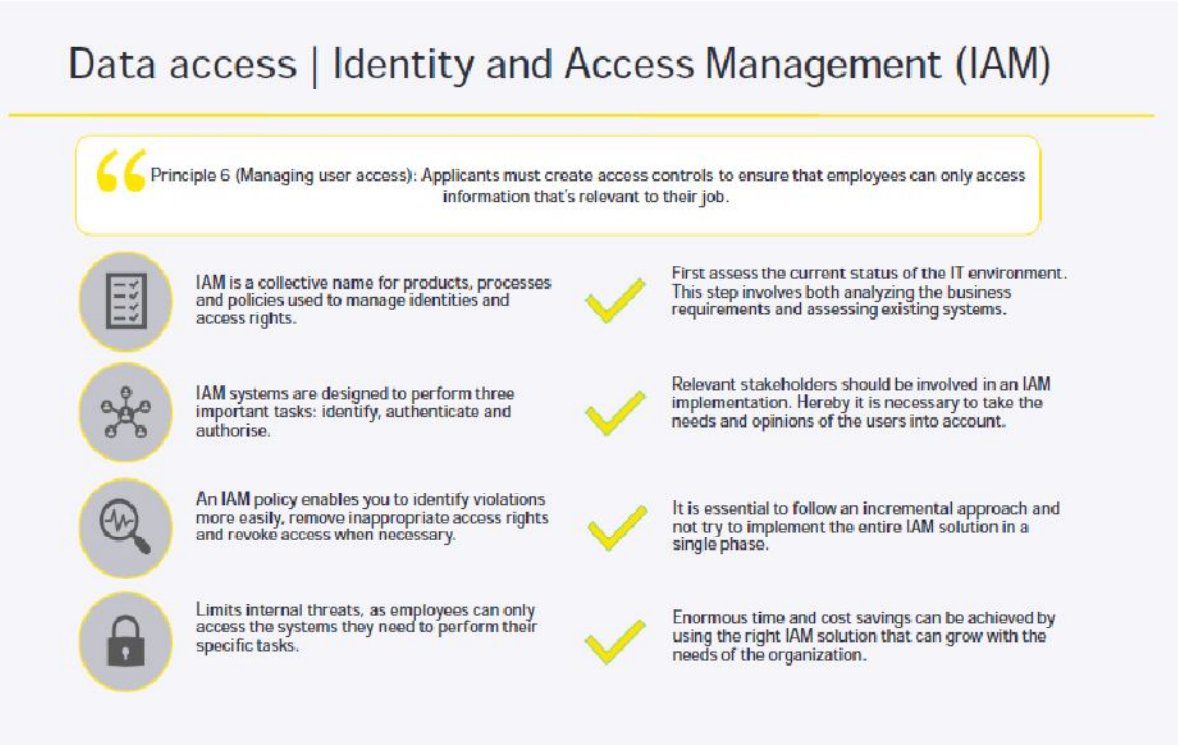
2 How prepared are the stakeholders?
Is documentation available?
Have plans been rehearsed? How and when?
Lessons learned?

3 Align business & IT
Are the expectations clearly aligned?

4 There are different types of incidents
ICT (small to large), environmental, health, ...

5 Define the priority of business processes
Payroll, HR, IT, Facilities, ...

6 Align with best-practice frameworks
For example ISO 22301



Data access | Identity and Access Management (IAM)

> Principle 6 (Managing user access): Applicants must create access controls to ensure that employees can only access information that's relevant to their job.

IAM is a collective name for products, processes and policies used to manage identities and access rights.

IAM systems are designed to perform three important tasks: identify, authenticate and authorise.

An IAM policy enables you to identify violations more easily, remove inappropriate access rights and revoke access when necessary.

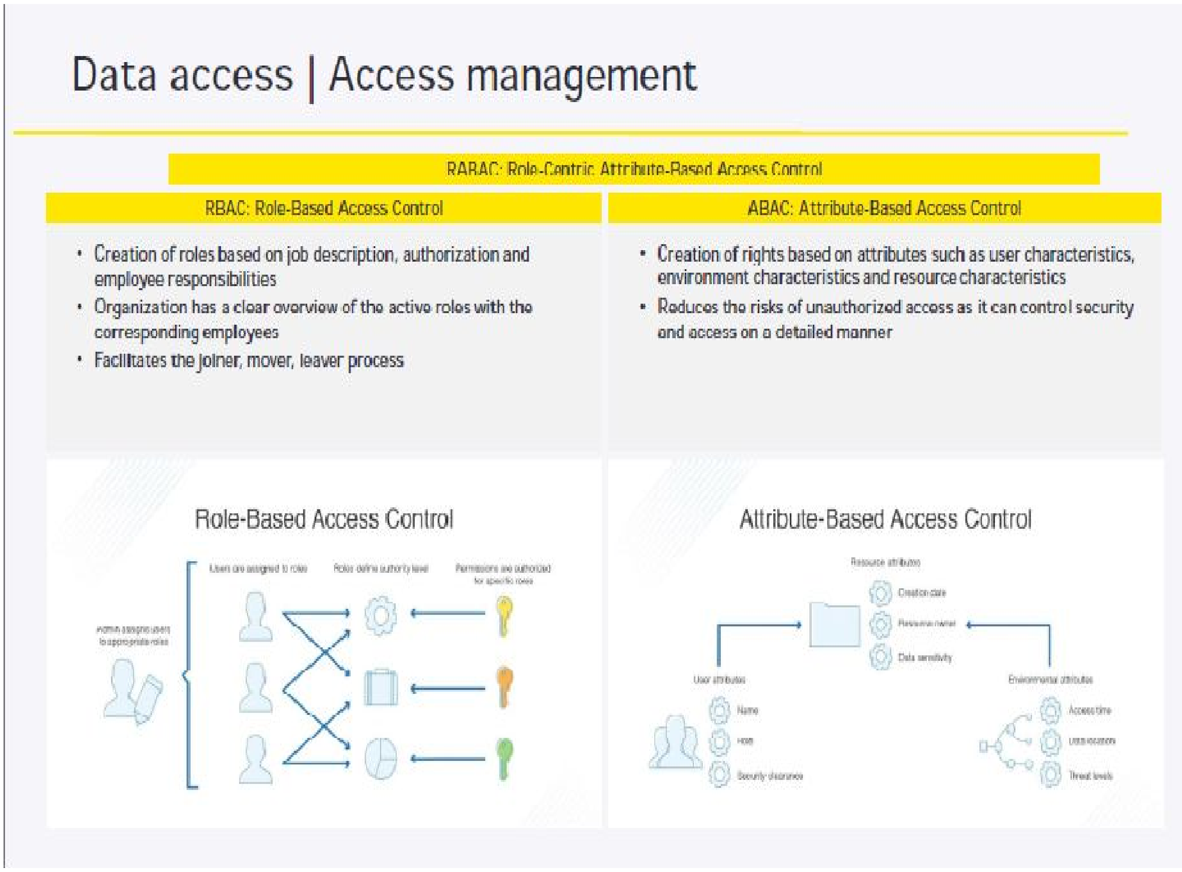
Limits internal threats, as employees can only access the systems they need to perform their specific tasks.

✓ First assess the current status of the IT environment. This step involves both analyzing the business requirements and assessing existing systems.

✓ Relevant stakeholders should be involved in an IAM implementation. Hereby it is necessary to take the needs and opinions of the users into account.

✓ It is essential to follow an incremental approach and not try to implement the entire IAM solution in a single phase.

✓ Enormous time and cost savings can be achieved by using the right IAM solution that can grow with the needs of the organization.



Data access | Access management

RABAC: Role-Centric Attribute-Based Access Control

RBAC: Role-Based Access Control

- Creation of roles based on job description, authorization and employee responsibilities
- Organization has a clear overview of the active roles with the corresponding employees
- Facilitates the joiner, mover, leaver process

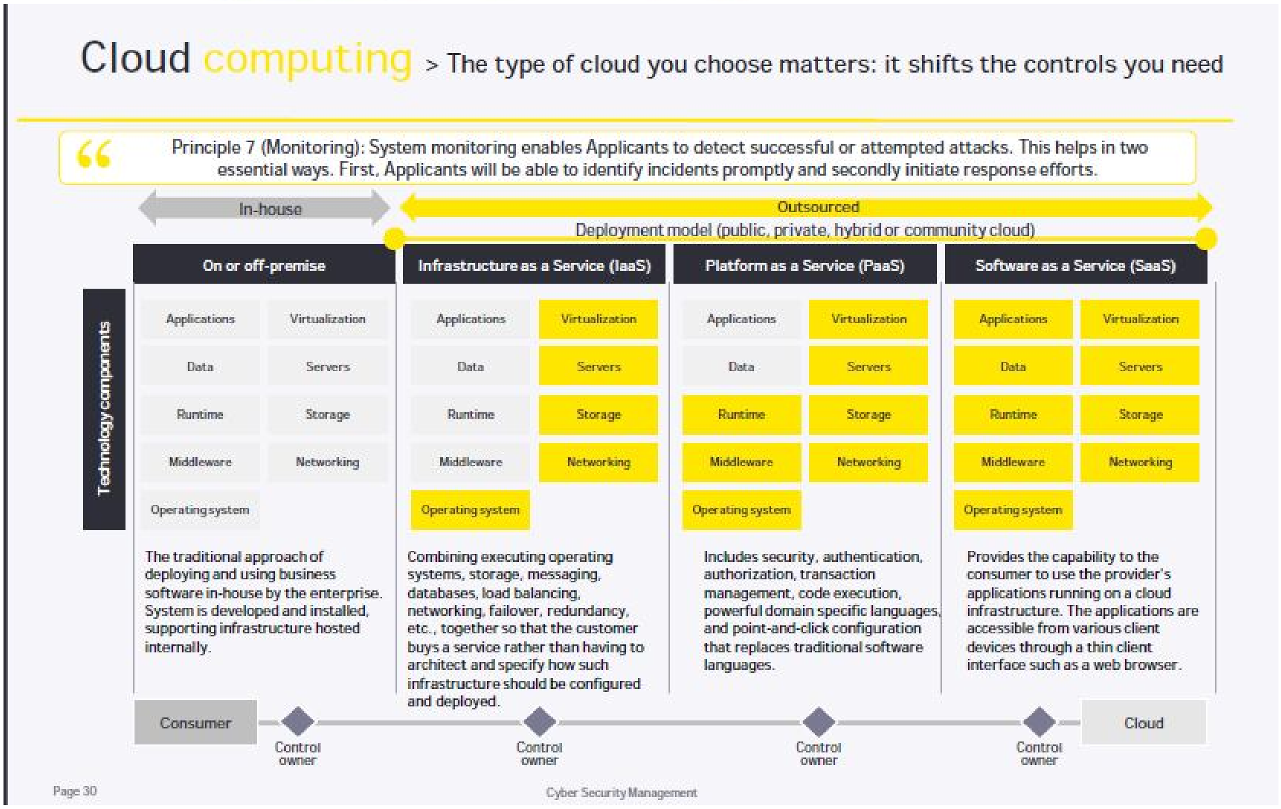
ABAC: Attribute-Based Access Control

- Creation of rights based on attributes such as user characteristics, environment characteristics and resource characteristics
- Reduces the risks of unauthorized access as it can control security and access on a detailed manner

Role-Based Access Control

Admin assigns users to appropriate roles
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles

Attribute-Based Access Control



Cloud computing > The type of cloud you choose matters: it shifts the controls you need

“ Principle 7 (Monitoring): System monitoring enables Applicants to detect successful or attempted attacks. This helps in two essential ways. First, Applicants will be able to identify incidents promptly and secondly initiate response efforts.

In-house
Outsourced
Deployment model (public, private, hybrid or community cloud)
Technology components

On or off-premise		Infrastructure as a Service (IaaS)		Platform as a Service (PaaS)		Software as a Service (SaaS)	
Applications	Virtualization	Applications	Virtualization	Applications	Virtualization	Applications	Virtualization
Data	Servers	Data	Servers	Data	Servers	Data	Servers
Runtime	Storage	Runtime	Storage	Runtime	Storage	Runtime	Storage
Middleware	Networking	Middleware	Networking	Middleware	Networking	Middleware	Networking
Operating system		Operating system		Operating system		Operating system	

The traditional approach of deploying and using business software in-house by the enterprise. System is developed and installed, supporting infrastructure hosted internally.

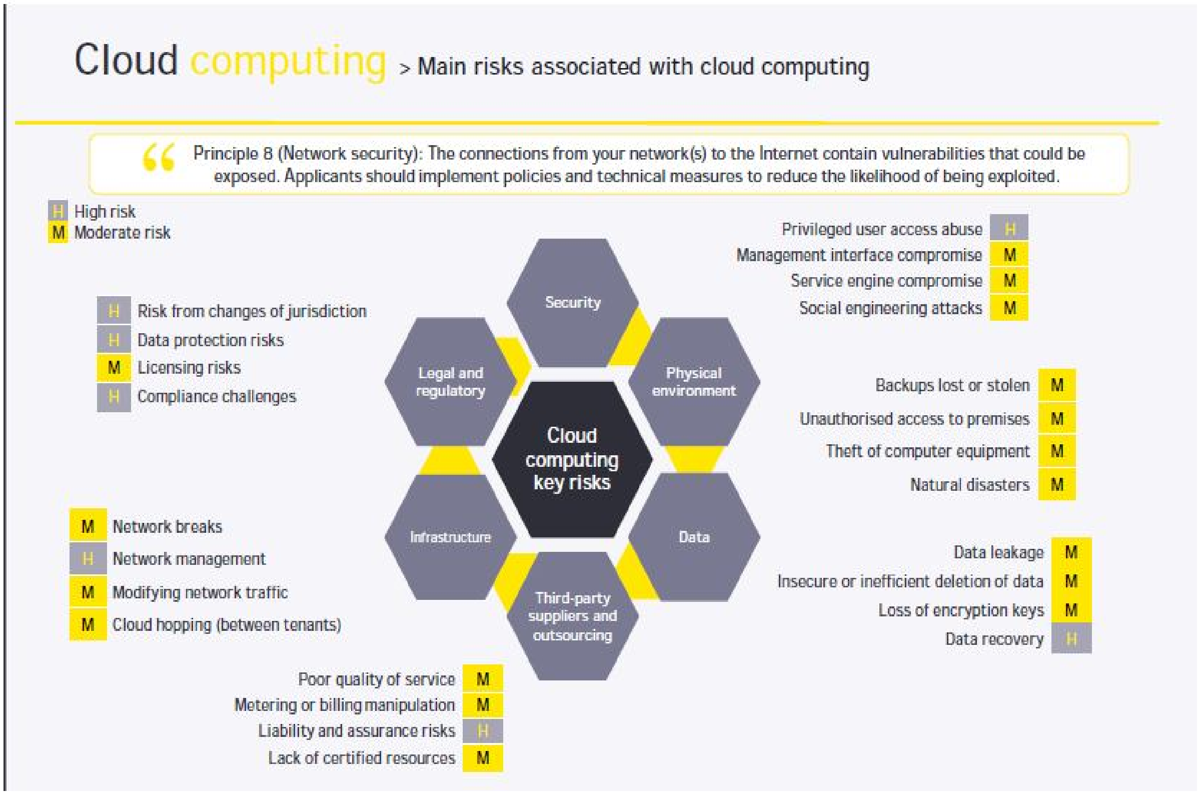
Combining executing operating systems, storage, messaging, databases, load balancing, networking, failover, redundancy, etc., together so that the customer buys a service rather than having to architect and specify how such infrastructure should be configured and deployed.

Includes security, authentication, authorization, transaction management, code execution, powerful domain specific languages, and point-and-click configuration that replaces traditional software languages.

Provides the capability to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

Page 30

Cyber Security Management



Cloud computing > Main risks associated with cloud computing

“ Principle 8 (Network security): The connections from your network(s) to the Internet contain vulnerabilities that could be exposed. Applicants should implement policies and technical measures to reduce the likelihood of being exploited.

H High risk
M Moderate risk

Privileged user access abuse	H
Management interface compromise	M
Service engine compromise	M
Social engineering attacks	M

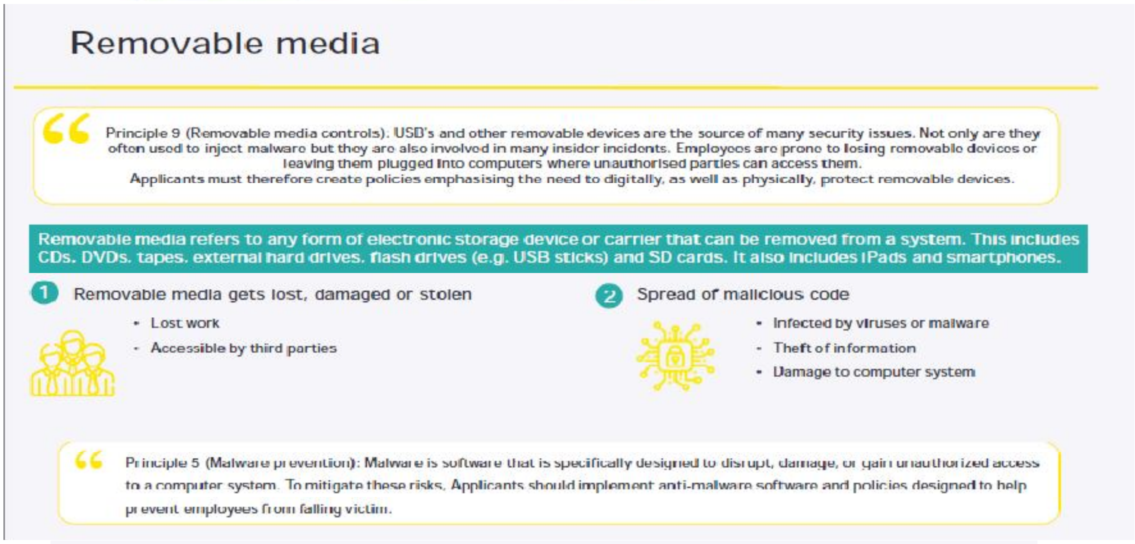
Backups lost or stolen	M
Unauthorised access to premises	M
Theft of computer equipment	M
Natural disasters	M

Data leakage	M
Insecure or inefficient deletion of data	M
Loss of encryption keys	M
Data recovery	H

Poor quality of service	M
Metering or billing manipulation	M
Liability and assurance risks	H
Lack of certified resources	M

M	Network breaks
H	Network management
M	Modifying network traffic
M	Cloud hopping (between tenants)

H	Risk from changes of jurisdiction
H	Data protection risks
M	Licensing risks
H	Compliance challenges



Removable media

> Principle 9 (Removable media controls). USB's and other removable devices are the source of many security issues. Not only are they often used to inject malware but they are also involved in many insider incidents. Employees are prone to losing removable devices or leaving them plugged into computers where unauthorised parties can access them.
> Applicants must therefore create policies emphasising the need to digitally, as well as physically, protect removable devices.

Removable media refers to any form of electronic storage device or carrier that can be removed from a system. This includes CDs. DVDs. tapes. external hard drives. flash drives (e.g. USB sticks) and SD cards. It also includes iPads and smartphones.

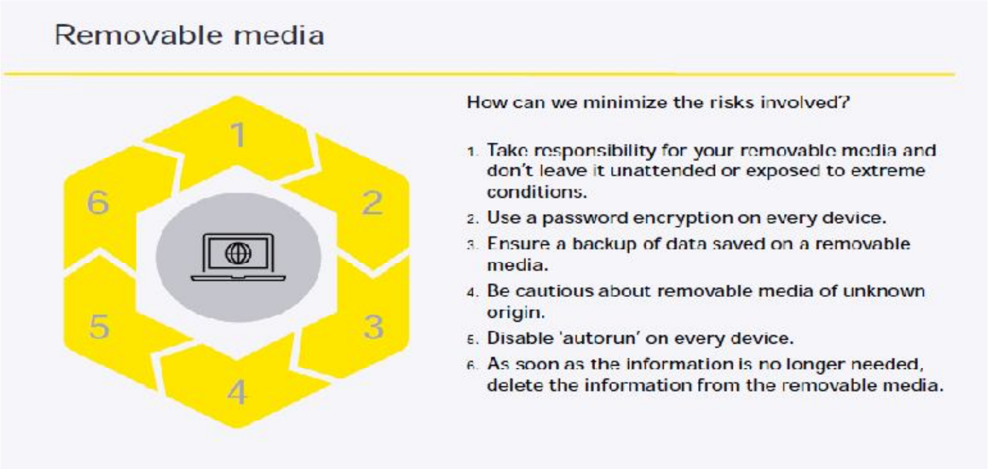
1 Removable media gets lost, damaged or stolen

- Lost work
- Accessible by third parties

2 Spread of malicious code

- Infected by viruses or malware
- Theft of information
- Damage to computer system

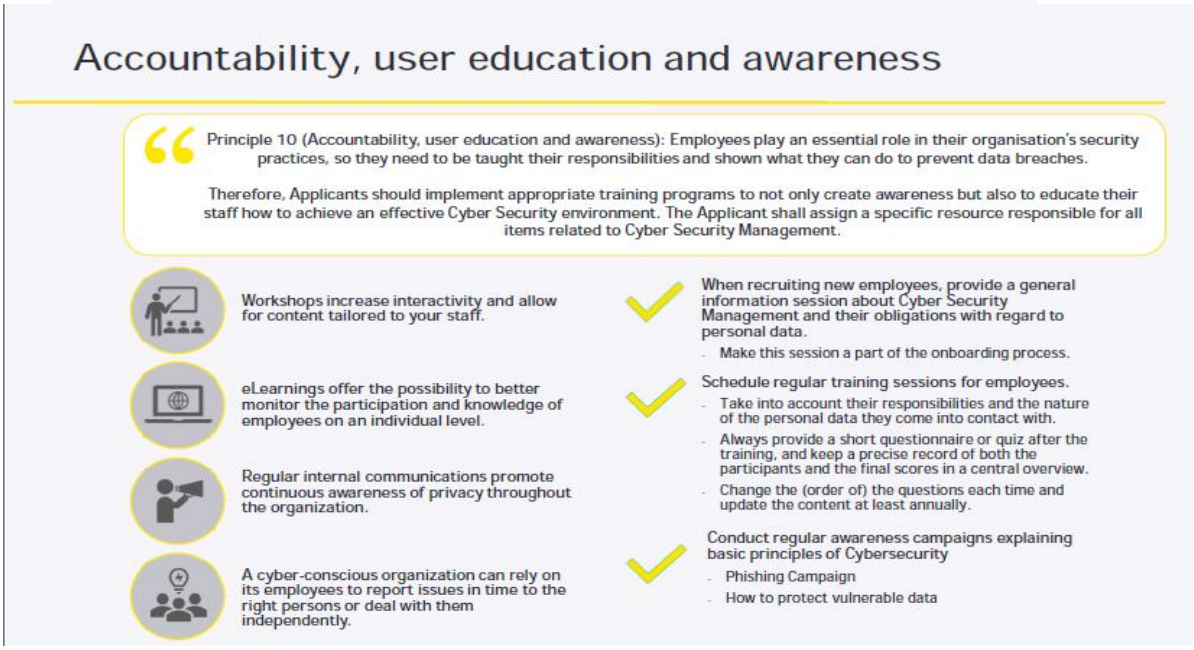
> Principle 5 (Malware prevention): Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. To mitigate these risks, Applicants should implement anti-malware software and policies designed to help prevent employees from falling victim.



Removable media

How can we minimize the risks involved?

1. Take responsibility for your removable media and don't leave it unattended or exposed to extreme conditions.
2. Use a password encryption on every device.
3. Ensure a backup of data saved on a removable media.
4. Be cautious about removable media of unknown origin.
5. Disable 'autorun' on every device.
6. As soon as the information is no longer needed, delete the information from the removable media.



Accountability, user education and awareness

> Principle 10 (Accountability, user education and awareness): Employees play an essential role in their organisation's security practices, so they need to be taught their responsibilities and shown what they can do to prevent data breaches.
>
> Therefore, Applicants should implement appropriate training programs to not only create awareness but also to educate their staff how to achieve an effective Cyber Security environment. The Applicant shall assign a specific resource responsible for all items related to Cyber Security Management.

Workshops increase interactivity and allow for content tailored to your staff.

eLearnings offer the possibility to better monitor the participation and knowledge of employees on an individual level.

Regular internal communications promote continuous awareness of privacy throughout the organization.

A cyber-conscious organization can rely on its employees to report issues in time to the right persons or deal with them independently.

✓ When recruiting new employees, provide a general information session about Cyber Security Management and their obligations with regard to personal data.

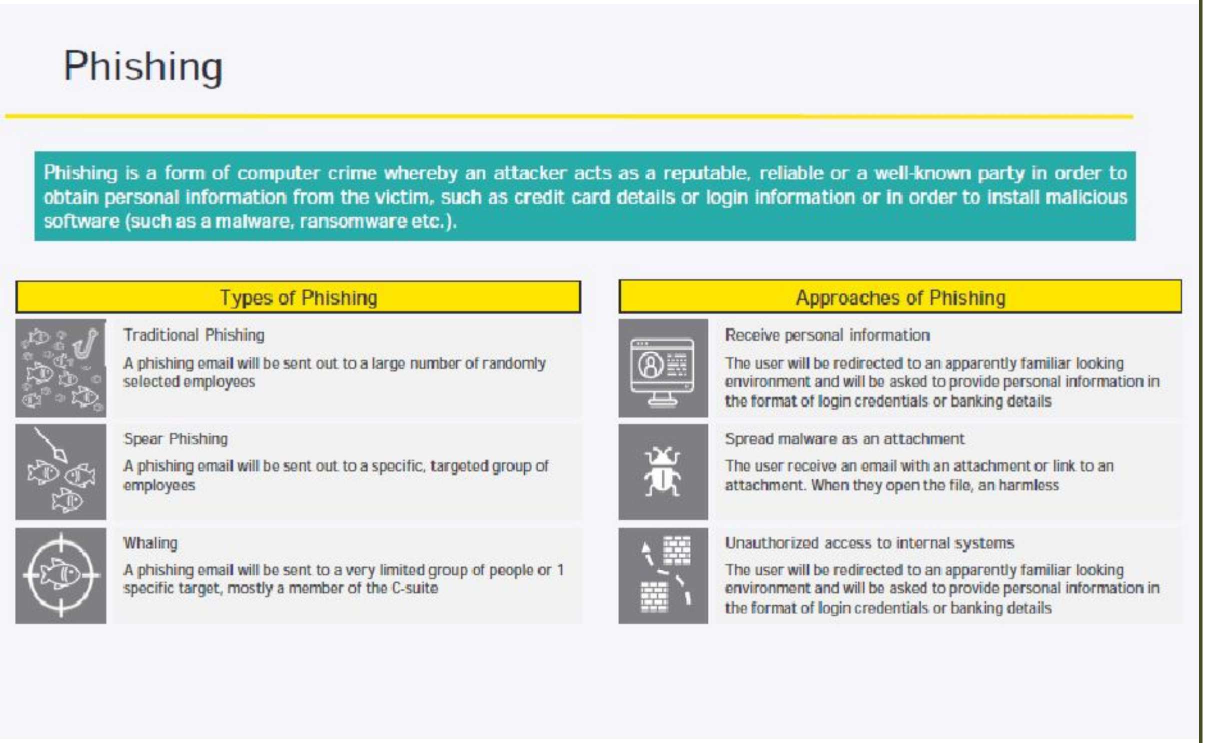
- Make this session a part of the onboarding process.

✓ Schedule regular training sessions for employees.

- Take into account their responsibilities and the nature of the personal data they come into contact with.
- Always provide a short questionnaire or quiz after the training, and keep a precise record of both the participants and the final scores in a central overview.
- Change the (order of) the questions each time and update the content at least annually.

✓ Conduct regular awareness campaigns explaining basic principles of Cybersecurity

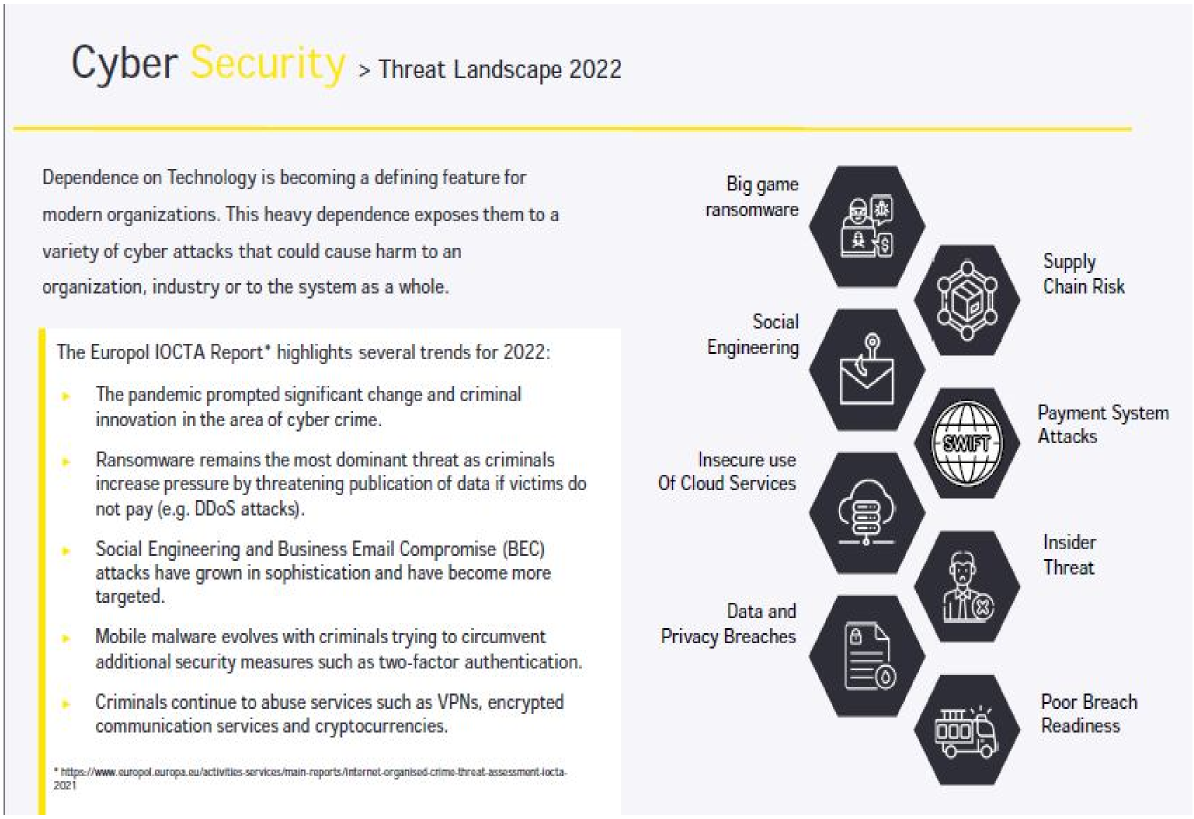
- Phishing Campaign
- How to protect vulnerable data



Phishing

Phishing is a form of computer crime whereby an attacker acts as a reputable, reliable or a well-known party in order to obtain personal information from the victim, such as credit card details or login information or in order to install malicious software (such as a malware, ransomware etc.).

Types of Phishing	Approaches of Phishing
Traditional Phishing A phishing email will be sent out to a large number of randomly selected employees	Receive personal information The user will be redirected to an apparently familiar looking environment and will be asked to provide personal information in the format of login credentials or banking details
Spear Phishing A phishing email will be sent out to a specific, targeted group of employees	Spread malware as an attachment The user receive an email with an attachment or link to an attachment. When they open the file, an harmless
Whaling A phishing email will be sent to a very limited group of people or 1 specific target, mostly a member of the C-suite	Unauthorized access to internal systems The user will be redirected to an apparently familiar looking environment and will be asked to provide personal information in the format of login credentials or banking details



Cyber Security > Threat Landscape 2022

Dependence on Technology is becoming a defining feature for modern organizations. This heavy dependence exposes them to a variety of cyber attacks that could cause harm to an organization, industry or to the system as a whole.

The Europol IOCTA Report* highlights several trends for 2022:

- The pandemic prompted significant change and criminal innovation in the area of cyber crime.
- Ransomware remains the most dominant threat as criminals increase pressure by threatening publication of data if victims do not pay (e.g. DDoS attacks).
- Social Engineering and Business Email Compromise (BEC) attacks have grown in sophistication and have become more targeted.
- Mobile malware evolves with criminals trying to circumvent additional security measures such as two-factor authentication.
- Criminals continue to abuse services such as VPNs, encrypted communication services and cryptocurrencies.

* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Big game ransomware

Supply Chain Risk

Social Engineering

Payment System Attacks

Insecure use Of Cloud Services

Insider Threat

Data and Privacy Breaches

Poor Breach Readiness

EY | Building a better working world

EY exists to build a better working world, helping to create long term value for clients, people and society and build trust in the capital markets. Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate. Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today. EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information please visit their organization, please visit ey.com.

ey.com/be

It’s also important for business to grasp the fact that, however strong their data security precautions, there will always be some risk. ‘You will never have the perfect system that can block everything,’ ‘Instead, it’s about creating awareness and, with something like phishing, making sure your employees know about this and the techniques the criminals use.’

THE VOICE OF THE INTERNATIONAL MOVING INDUSTRY

FIDI