CYPRUS FIDUCIARY ASSOCIATION

CYPRUS
FIDUCIARY ASSOCIATION

CYFA 2022 Seminar #1:

"Technology Risks and Electronic Crime in the Service Provider World: Common Problems/ Updated Solutions "

Thursday, 03rd February, 2022

Speakers: Mr Christos Gavriel & Ms Nadia Constantinidou

Exclusive Sponsors 2022


#RestartCY

About Renaissance

- A Cyprus-based risk consultancy and insurance brokerage
- 3 business practices:
  - ProFin: Professionals and Financial Institutions
  - Corporate: Medium/ Large Businesses
  - Private Client and Specialty: HNWs/ Family Offices, pure e-businesses and professional sports
- 3 core services:
  - Operational risk advisory
  - Insurance brokerage
  - Insurance claims advisory/ Disaster recovery/ Crisis Management

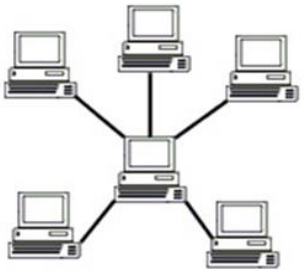
Interesting facts

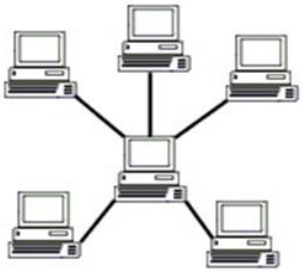
- Pan-European licence
- A registered Lloyd's broker
- Cyprus partner of Brokerslink

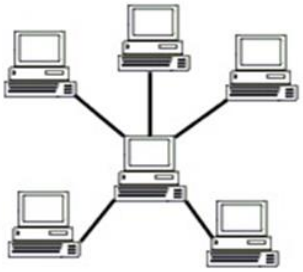
- Global mindset
- Global capabilities
- Supporting the "headquartering model"

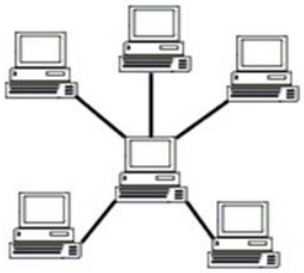
The evolution of technology

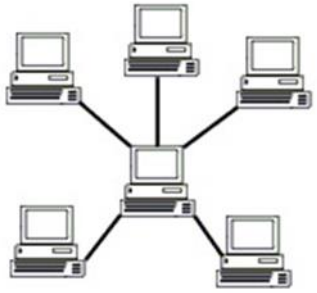
The evolution of technology

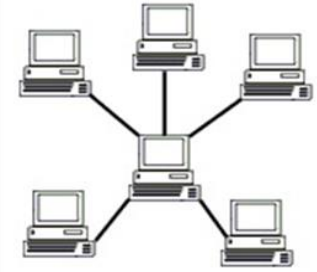




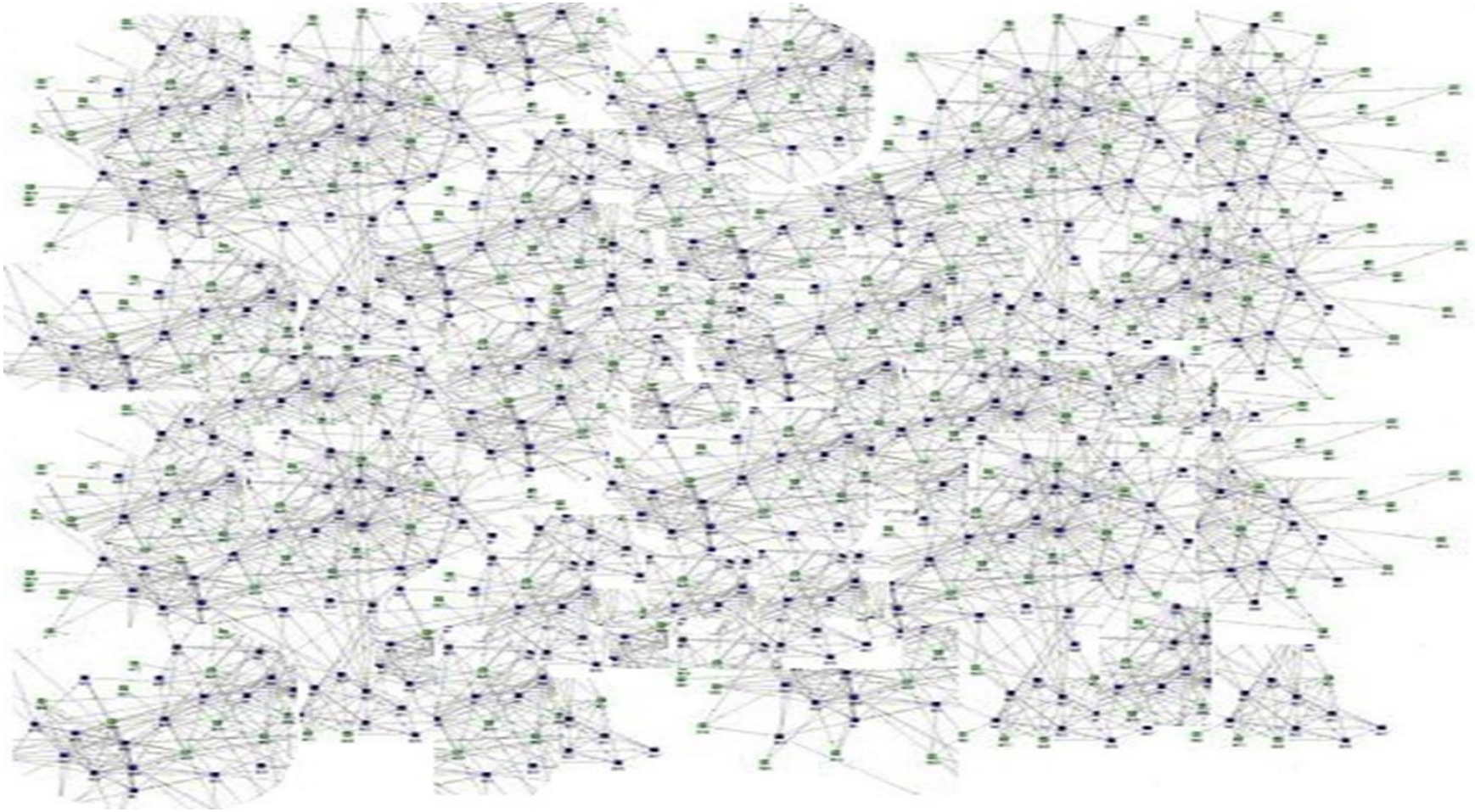








The evolution of technology



Why?

- During our lifetime Technology has made great steps
  - Our life is easier/ work more productive
  - Our life is more complicated/ work has more risks

- Rewards of this new economy impact people asymmetrically (e.g Bezos, Zuckerberg, Musk, etc)
- For the rest of us: convenience vs mental health, privacy, security

Why - continued

- Businesses hear about Technology risks in single dimensional conversations
  - IT companies: Manage Technology by buying more technology!
  - Law firms: Contracts/ policies and compliance manuals for everything
  - Consultants: New processes/ outsourcing partners/ software
  - Insurers: Excluding “Cyber risk” from all insurances and then trying to sell “Cyber Insurance”. What do they cover after-all?

Why - continued

- Result:
  - Business Technology risk conversations are single dimensional
  - Solutions are myopic
  - Businesses rely on external parties to embrace technology (banks/ clients)
  - Lack of confidence once they start embracing technology
  - Few Lose and many learn
- A trial and error process…

Why – at last!

- Present a fusion of technology risks
- Apply it to Service Providers' business
- Identify multi-dimensional problems
- Stimulate multi-dimensional holistic solutions/ thinking

Technology as a business partner

- Technology plays a major role in Service Providers business
  - Necessary to perform daily tasks
  - Necessary to communicate with clients abroad
  - Meetings with clients with no physical presence
  - Remote working
  - Related parties use technology as a means of communication (clients, associates, banks etc.)

Technology as a business partner

- Technology is a business partner!

- Think technology as a business partner
  - who often is treated like a silent partner
  - business lacks the resource to continually monitor it
  - tech runs in the background

Sometimes things go Wrong

Technology Risks

Proprietary/Package/Platform

Architecture/Internet Access/Capacity/ Facilities/Security

Counterparty Risk

Cloud / Vendors / other service providers

Selection

Documentation

Monitoring

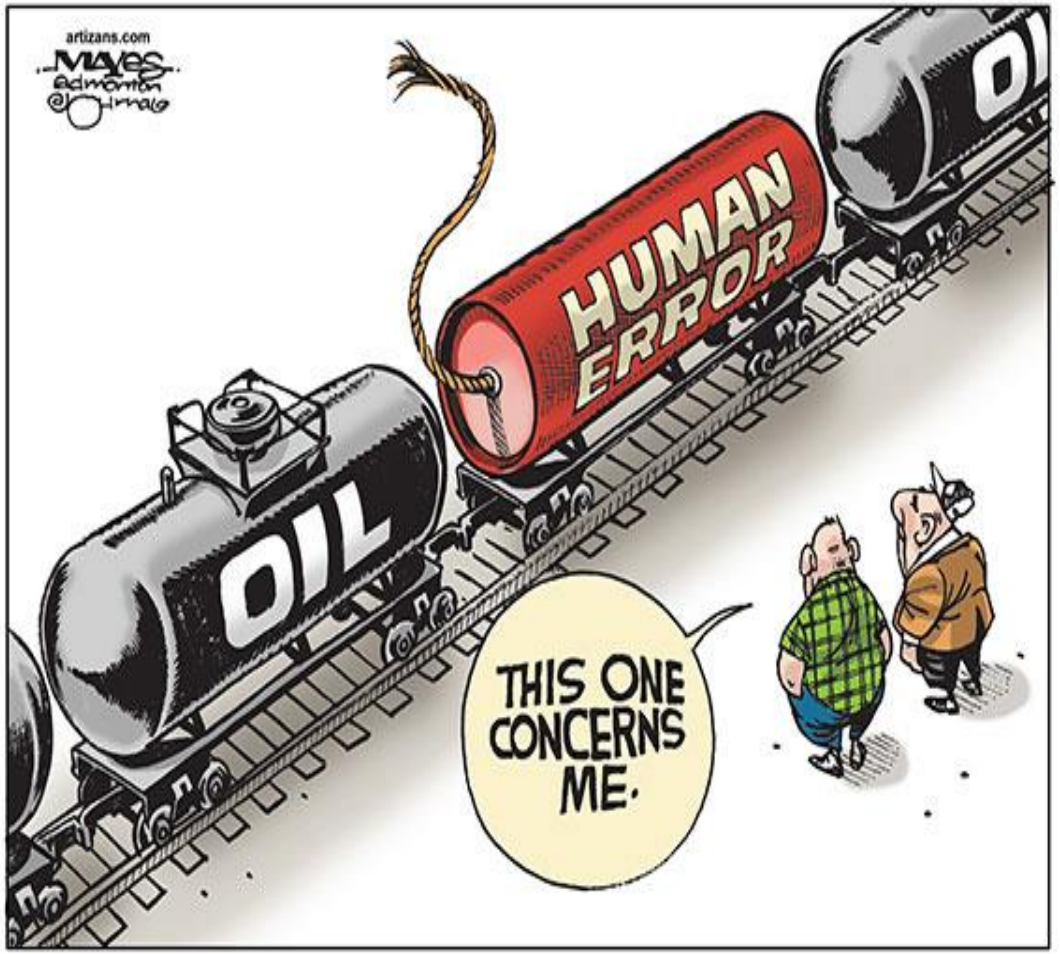
Process Risks

Complexity

Diversity

Disruptions

People Risks



Errors / omissions

Project / resources

Malice / fraud

Regulatory Risks

GDPR

Data Responsibilities

Data Breach

Fines and Penalties

Cyber Risks

- Who is a Hacker?
- Is a Service Provider an attractive target for cyber criminals?

Amazing mind reader reveals his 'gift' - YouTube

Main Cyber Risks

Social engineering / phishing	Malware	Ransomware attacks	Denial-of-service attacks	Outsourced Company Access
Access through business email accounts/ impersonation to acquire sensitive information or perpetrate fraud	A malicious software is installed on a computer system and used to access data or sensitive information without the company's knowledge	Locking/ Extraction of data to extract ransom payments	Malicious attacks intended to disrupt dependencies on telecom infrastructures	Access to data and company's system through compromised service provider

What is the Cost?

- A big question! ***Can we quantify the potential damage/ loss?***
  - Property Fire: The cost of rebuilding the property
  - Motor: The cost of repairing the damage caused to a car
  - Technology:
    - What is the Value at Risk?
    - We do not know!
    - Why?

What is at stake?

Reputation/ Confidence

- Clients
- Business
- Partners/ Associates

Business/ Network Interruption

- Loss of Income
- Loss of Profit

Loss of Data

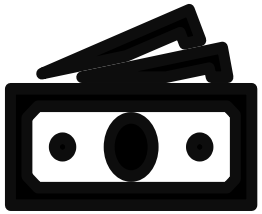
- Notifications
- Recover/Recreate Data

Litigation

- Defence Costs
- Damages to 3rd parties

Fines (GDPR)

- Fines
- Penalties



Financial Loss

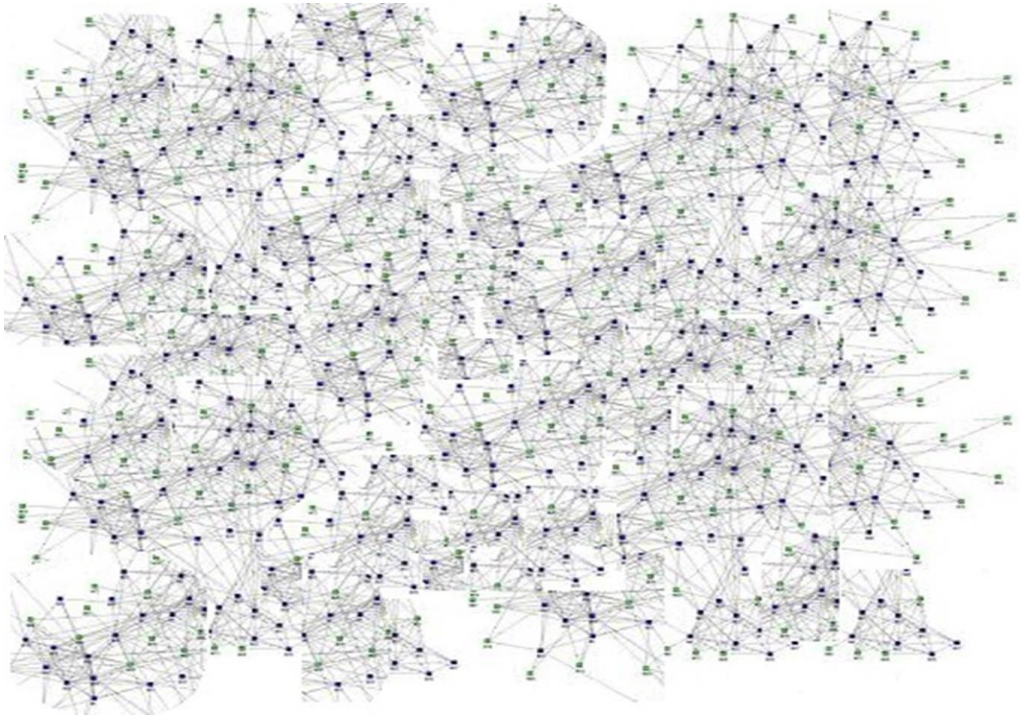
- Extortion
- Theft of funds
- Increased cost of workings

The evolution of Crime

- Real money vs electronic transfers
- Crime transforms
- Businesses still devote more time/ resources on physical crime

Electronic/ Cyber Crime

- Internal, External and Hybrid
  - What is external nowadays (outsourcing/ cloud etc)?
- Motivation
  - Financial
  - Information
  - Malice



Financial Crime

INTERNAL

- Unsophisticated/ Temptation
- Sophisticated
  - Financial need
  - Internal cooperation
- Easier to control when cash is not physical

EXTERNAL

- Infiltration/Malware/ Impersonation
- Systems/ Training

Data/ Info Crime

INTERNAL

- Bribery/ Competitors
- Access/ Controls

EXTERNAL

- 1st Gen – Access
- 2nd Gen Activity
- Access/ Controls
  - Layering information
  - Varying access
  - Specialist software

Malicious Crime

INTERNAL

- Relationships
- Be nice!

EXTERNAL

- All previous controls
- Low profile

The Future of Crime?

This AI Can Clone Any Voice, Including Yours - YouTube

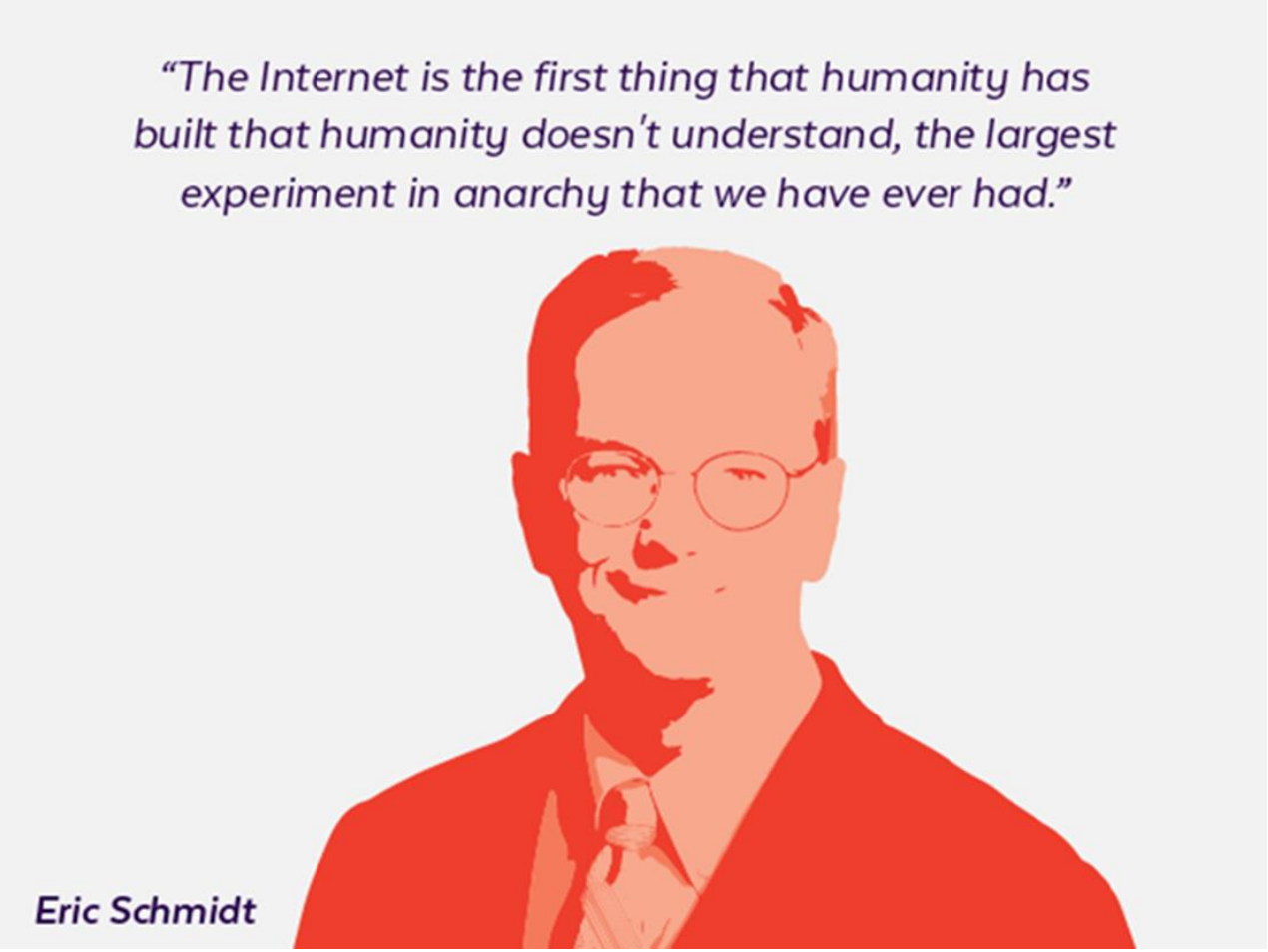
Fusion/ Best Practices

- In the past – Systems
- In the near past – Systems and Contracts
- Now and in the Future
  - Systems
  - Contracts
  - Controls
  - **People Training**
  - Insurance/ Hedging

Fusion/ Best Practices

- **Integrated** Risk Management
  - Risk identification
  - Risk analysis
  - Risk management
  - Risk transfer

CASE STUDIES



Case Study 1: Data Breach

- An employee received an email containing a link to download invoices, spreadsheets and Word documents
- He was prompted to ‘decrypt’ information or ‘enable content’
- By clicking on those buttons he downloaded malware on his work PC which allowed hackers to remotely access his computer and operate it in ‘silent mode’
- His Employer’s network security vendors picked this up on a routine system check
- His employer’s network contains personal data of 100.000 clients including credit card information
- It is unknown if the malware has infected the company’s network

Case Study 1: Data Breach

- What does the firm need to do?
  - Investigation?
  - Data subject notification/ regulatory notices?
  - When?
  - By whom?
  - Who pays for it?

Case Study 1: Breach – DoS attack

- Two shareholders of a company (‘’the client’’) fall out in an international litigation due to disputes they had
- The Service Provider as part of its services to its client (administration/ directorships) holds important and sensitive personal and commercial information of the company
- One of the shareholders (“the attacker”) in order to gain access on this information caused a Denial of Service attack by sending through a large amounts of traffic that the server was unable to handle
- The attacker took down the main server of the company
- PC’s and network became unavailable
- The attacker managed to gain access on email exchanges between company’s users and various clients including relevant communication with the shareholder in question

Case Study 1: Breach – DoS attack

- Who will be liable for this breach?
- What are the regulatory exposures from this failure?
- How would a cyber insurance be useful in such a case?

Case Study 2: Cloud storage

Data Leakage

- Your company is using cloud services for the storage of its data
- The cloud service was breached from hackers
- Hackers gained access to sensitive data
- Hackers chose to distribute this data!

Data Loss

- Your company is using a cloud services who has one data server for the storage of its data
- Due to a system failure occurred on the cloud storage, the stored information has been erased entirely
- There was no back-up!

Case Study 2: Cloud storage

- Who is the owner of the Data?
- So who will be liable for the breach? The Corporate Service Provider or the Cloud Storage Service Company?
- Who will be liable for this breach of data?
- Should the contract between the Service Provider and the Cloud storage facility clarify whose liability will be for any Data breach? Is this negotiable?
- What practices could be implemented by the company when sending data on cloud storage and in order to have back-ups in case of lost data?

Case Study 3: Ransomware attack

When an employee fails to recognize a malicious attachment and it prompts a full- blown ransomware attack

- One employee received an email from what they assumed was a trusted contact
- The email appeared as part of a pre-existing email chain and came with a Word document attached, with the latest email in the chain simply stating “Please see attached.”
- The employee while attempting to open the attached document, a notification popped up stating that the document in question was created in a previous version of Word, and in order to view the document, the “enable content” button at the top of the document would have to be clicked. Wanting to see what the document contained, the employee clicked the “enable content” button.
- By clicking the “enable content” button, the employee enabled macros to run.

Case Study 3: Ransomware attack

- Unfortunately for the firm, the document that the employee had clicked on contained malicious macros. By enabling macros, the Word document automatically executed a series of commands which resulted in malicious software being downloaded onto the employee's computer, allowing the hacker to gain remote access to the device.

- The malicious software also signalled basic network information back to the threat actor, such as the company's domain name, thus allowing the hacker to investigate the firm and decide whether it was worth infiltrating further.

- Having established that the firm made a suitably lucrative target, the threat actor then downloaded a password scraping software from the internet. This allowed the hacker to gain access to every password ever used on the employee's computer, including the domain administrator account and password originally used to set up the computer. The hacker was therefore able to gain higher access privileges across the firm's network and launch their encryption software.

Case Study 3: Ransomware attack

- This resulted in a **ransom note for the business**, and requesting a payment of €X amount to be made in exchange for the decryption key.

- Fortunately, the firm had offline back-ups stored on a USB flash drive that it could look to recover from, and the business had largely regained access to its computer systems within a 72- hour period without having to make the ransom payment.

- A few days after the firm had recovered from back-up, those responsible for the ransomware attack contacted the firm, explaining that they had **stolen data** during the attack and threatened to publish the data on a public file sharing website if the **ransom demand** was not met within a certain timeframe.

Case Study 3: Ransomware attack

- In what risk management area should focus the company after this incident?
- Would Insurance help?

Case Study 4: Software Shutdown

- A company fell victim to a ransomware attack that disabled their server.
- Their data back-ups were also kept on this server, meaning that these were also impacted by the ransomware and rendered inaccessible.
- The company engaged their IT vendor to fix the problem, and they quickly went about wiping the ransomware from the server and restoring the computer systems as best they could, allowing the firm to regain access to their server within a couple of weeks. In spite of this, though, they still faced a number of complications.
- One of the major problems for the business was in relation to their main software program used for producing their clients' financial reports.

Case Study 4: Software Shutdown

- Prior to the cyber incident taking place, the firm had recognized that the software was becoming increasingly outdated, and a decision had been made that over the coming year, the production of those reports would gradually be migrated to a more modern system. When the attack occurred, the firm had been in the process of planning this migration.

- But the ransomware spelled the end for the old software program: although the IT vendor managed to reinstall it, the software was so archaic that it wasn't possible to restore it to its original functionality and it was no longer capable of producing the financial reports in an effective manner. This meant that the firm had little option but to massively accelerate the implementation of the new software system, but they faced difficulty here too.

- Because the back-ups had not been saved externally from the server, it meant that these were lost when the server was wiped. With the data back-ups unrecoverable, the insured didn't have access to the electronic customer data necessary to complete their clients' financial reports on the new system.

Case Study 4: Software Shutdown

- Thankfully the firm had retained paper copies of this information going back many years. However, in order to have sufficient information to allow figures to be reported for both current and prior financial years and for long and short term trends to be shown in the monthly reports for customers, several thousand lines of data per client needed to be manually entered onto the new software.

- In order to rectify this situation, the business had to get staff members to work overtime to carry out the data re-entry and accelerate the software implementation. They also had to bring in a number of temporary agency staff members to assist with these tasks.

- Even with all this overtime and external assistance, though, it still took over four months to get the new software system ready. During this time, our insured was still manually producing monthly financial reports for their clients and were delays in the service.

- As a result, many clients chose to cancel their annual contracts with the firm and take their business elsewhere.

Case Study 4: Software Shutdown

- What were the two major problems apart from the ransomware incident?
- How would a Cyber Insurance help on this case?

Case Study 5: Bricking

- A firm stores all of its client data on a single server at its premises. The Management is afraid of having data on the internet.
- They buy property insurance for the firm's office contents and a standard Cyber insurance.
- They back up data on tapes, which are stored off site
- The server breaks down and is damaged beyond repair. A new one will need to be purchased
- When trying to retrieve data from the back-up tapes they realize that the tapes are corrupted. The database will need to be re-generated from physical records.

Case Study 5: Bricking

- Which insurance will cover the replacement server?
- Which insurance will cover the data re-build?
- Which insurance will pay the firm's staff while not operational?

Case Study 6: Power Failure

- A firm has on-site data and backs up everything on the cloud. An explosion of the island's main power station caused a power failure. Power is rationed until the power station is repaired.
- During a resumption of power flow the firm's UPS malfunctioned and the firm's main server was damaged beyond repair.
- The firm needs to arrange a virtual server on the cloud to maintain operations.
- It had a standard Property and Cyber Insurance policies in place.

Case Study 6: Power Failure

- Which insurance paid for the replacement server?
- Which insurance paid for the virtual server?
- Which insurance paid for the additional communication costs and the time costs from working on a cloud based virtual server at times of interrupted power?

Case Study 7: Hack/ Kidnap

- A Service Provider Executive is director in 50 companies, all belonging to the same UBO. She is a bank signatory with full authority.
- The client's bank account has a EUR50million balance, originating from an asset sale that took place last week.
- On a Friday morning the executive receives a video of her 5 year old daughter. She has been kidnapped. The kidnappers have been monitoring her and request a remittance of EUR50million to a specific bank account they have opened in the name of one of the 50 companies in a third country.
- If she does not send the funds they will harm her daughter. They say that her phone and email account have been hacked and if she talks to anyone she will never see her daughter again.

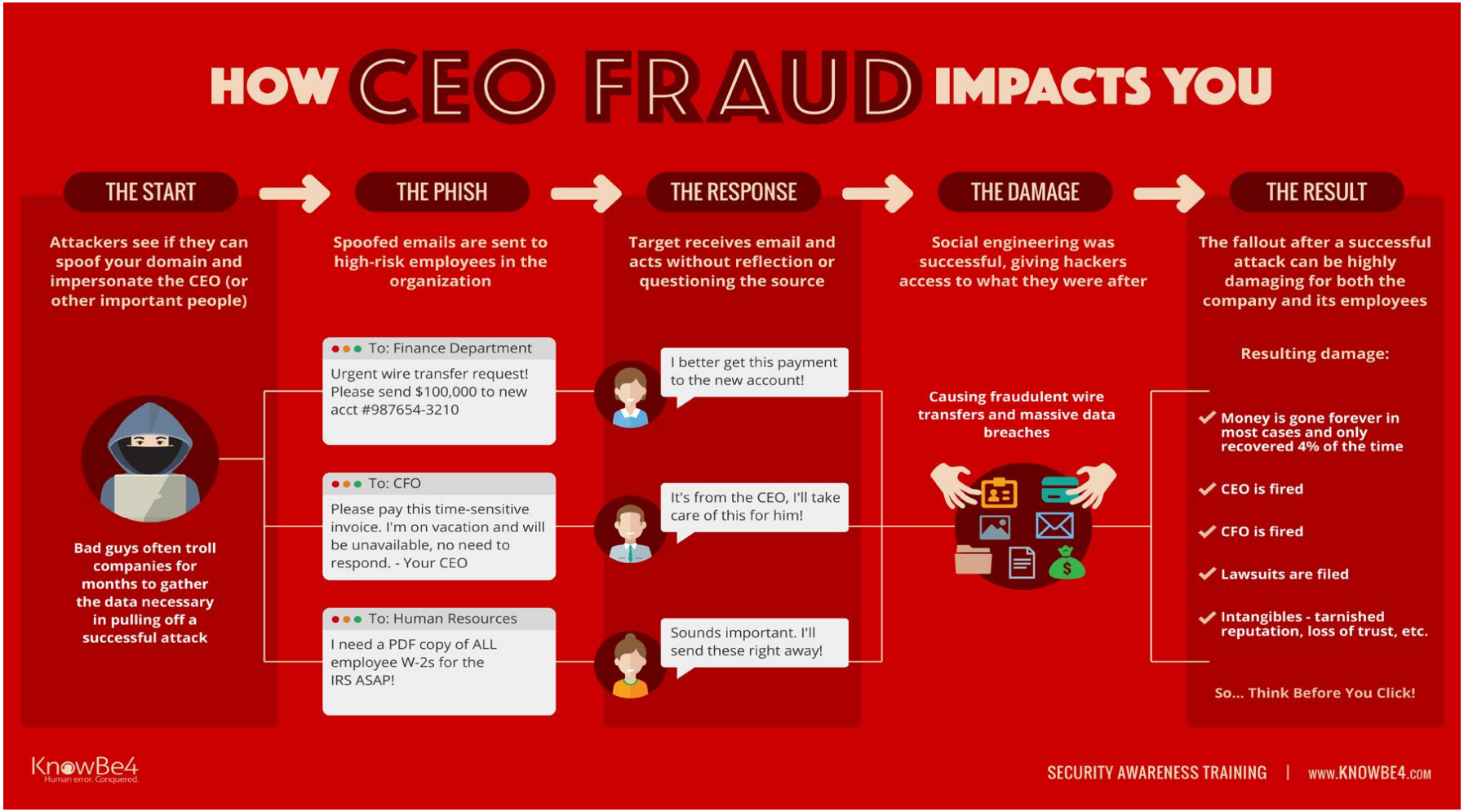
Case Study 7: Hack/ Kidnap

- Should she go to the police?
- Should she send the funds?
- Her firm has Professional Indemnity, Cyber Insurance and Directors' Liability Insurance for a combined limit of cover of EUR20million. Will the insurance pay out if she sends the funds?
- Her firm has Crime Insurance in place for EUR10million? Will they be able to recover?

Case Study 8: Clients' Funds

- The Director of a firm received an email from a client for whom provides fiduciary/ administrative services.
- The email appeared to be a trusted contact, since it was from the CEO and it was in continuity of previous email exchange for the purchase of an asset.
- The CEO was requesting the transfer of funds and at the same time informed that the banking details of the account to which transfer should be done was changed.
- The Director following the firm's internal policies and procedures, verified via a phone call that the email sent to him was by his client and proceeded with the execution.
- Unfortunately, the fraudster had managed to forward CEO's telephone number to his phone!!

Case Study 9: CEO Fraud



Case Study 10: Inside Job

- A client's CFO for the first time provides instructions to send funds from a transaction to a new bank account in the name of the client' company but in another country.
- Over email communication he insists that this is a new bank account and provides relevant background info.
- You call the CFO and he insists his instructions are firm. He complains you are wasting his time and threatens to report it to your firm's management.
- Do you send the funds if:
  - He is an authorized person?
  - He is not an authorized person?

The Future

- The future of cyber security | Financial Times (ft.com)

The Future

- Employee Mobility/ Remote working
- Super-fast internet
- Internet of Things
- Artificial intelligence
- Virtual reality

- Massive opportunities/ Massive cyber risks
- Integrated Risk Management= resilience

Thank you.

CYPRUS FIDUCIARY ASSOCIATION

Business Address:
Menandrou 1, Office 401,
Frosia House, 7001
Nicosia, Cyprus

Tel.: +357 22 256263
Fax: +357 22 256364

E-mail: info@cyfa.org.cy
Website: www.cyfa.org.cy