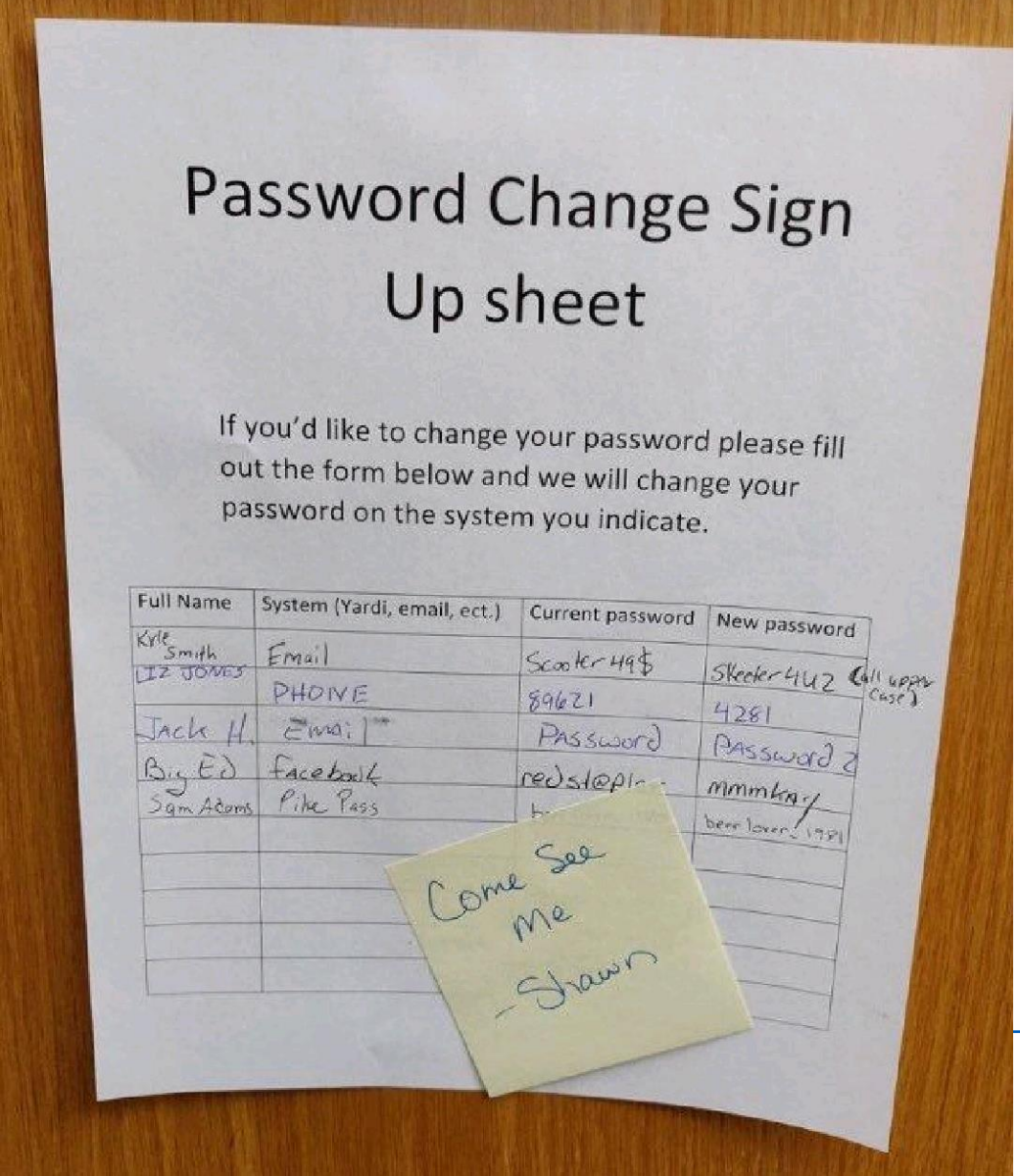
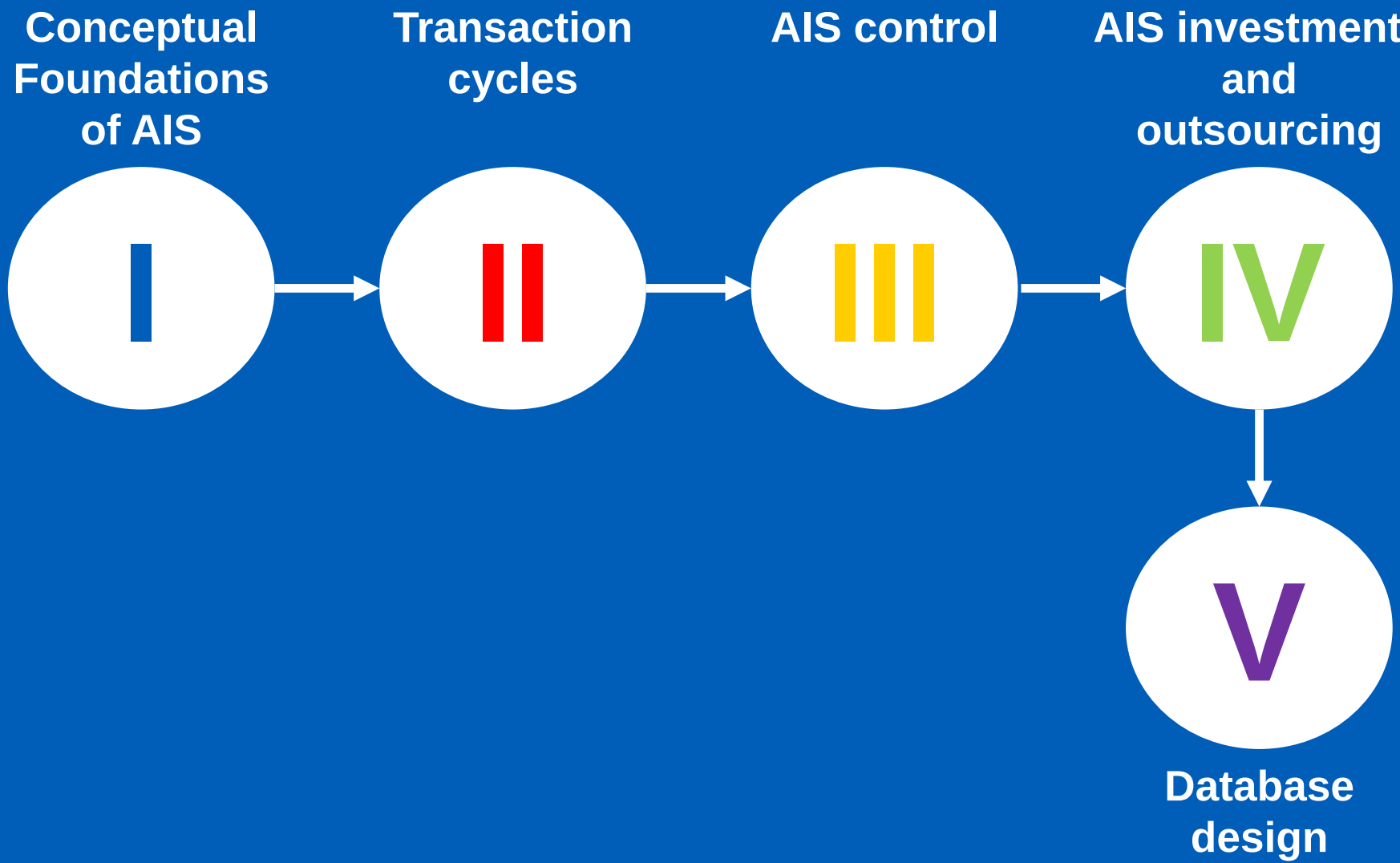


Don't be that guy/gal…


Conceptual Foundations of AIS
Transaction cycles
AIS control
AIS investments and outsourcing
I
II
III
IV
V
Database design

Aalto University
School of Business

AIS Fraud and Control

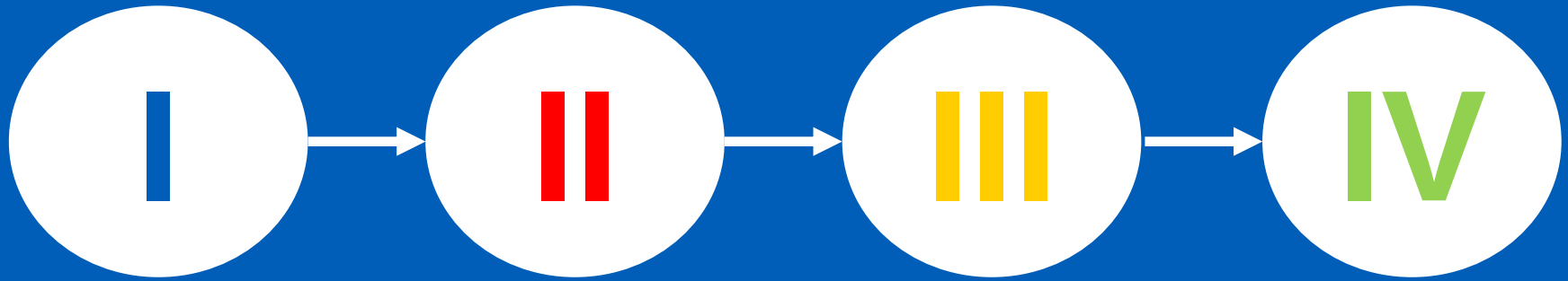
by David Derichs ©
Lecture 1

Why care?

Fraud

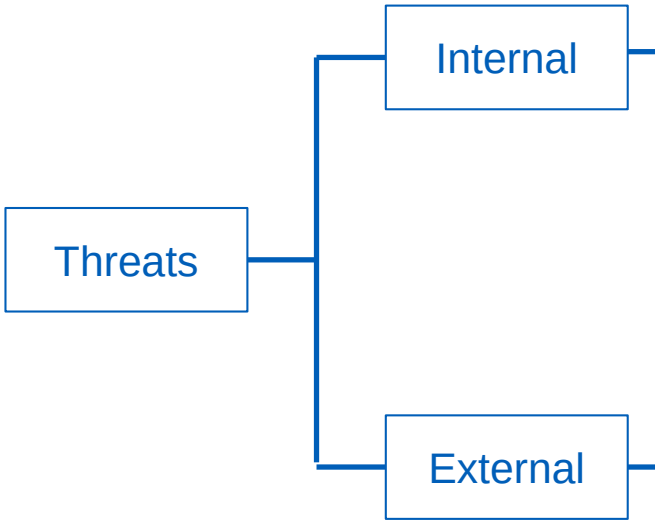
Computer Fraud

AIS Control



Recollection: What internal and external threats do AIS face?

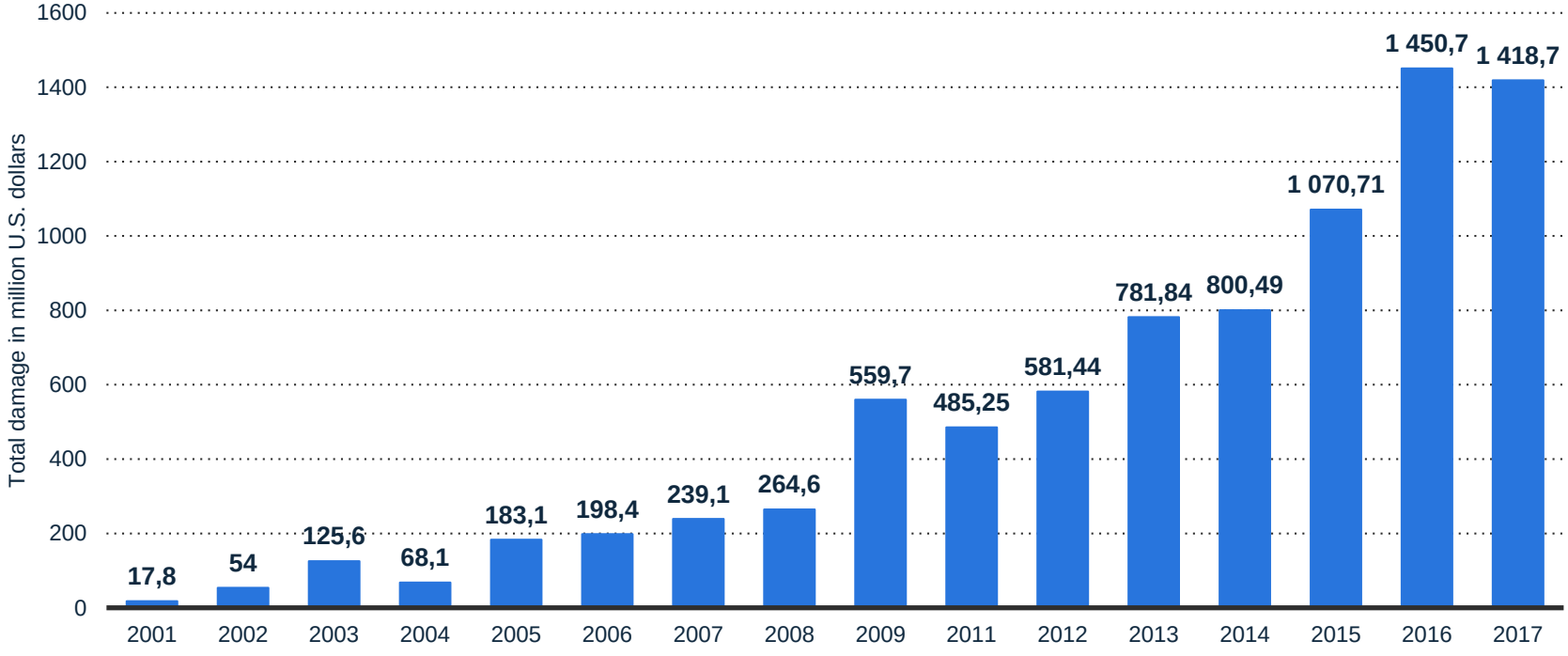
Main internal and external threats



I. Why (should YOU) care?

Cyber crime damaging is increasing exponentially!

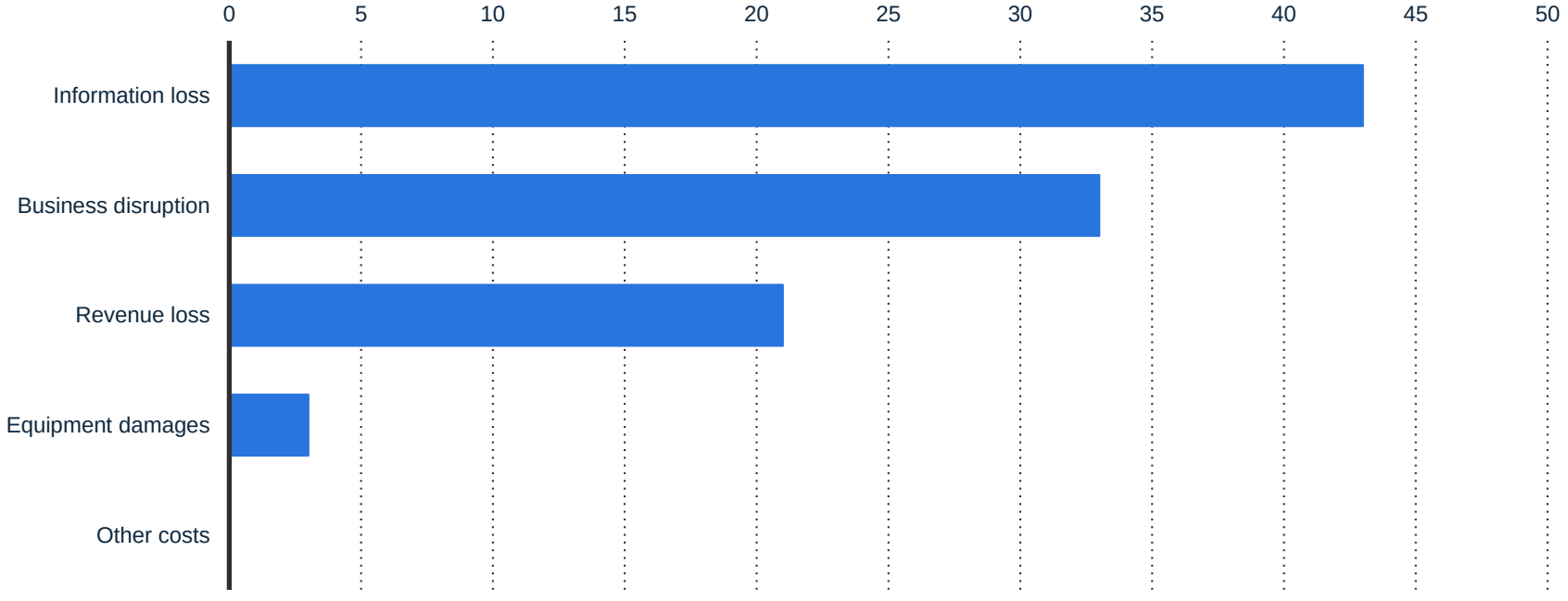
IC3: total damage caused by reported cyber crime 2001-2017 [m USD]



Source: Statista

Highest costs are related to information loss and business disruption

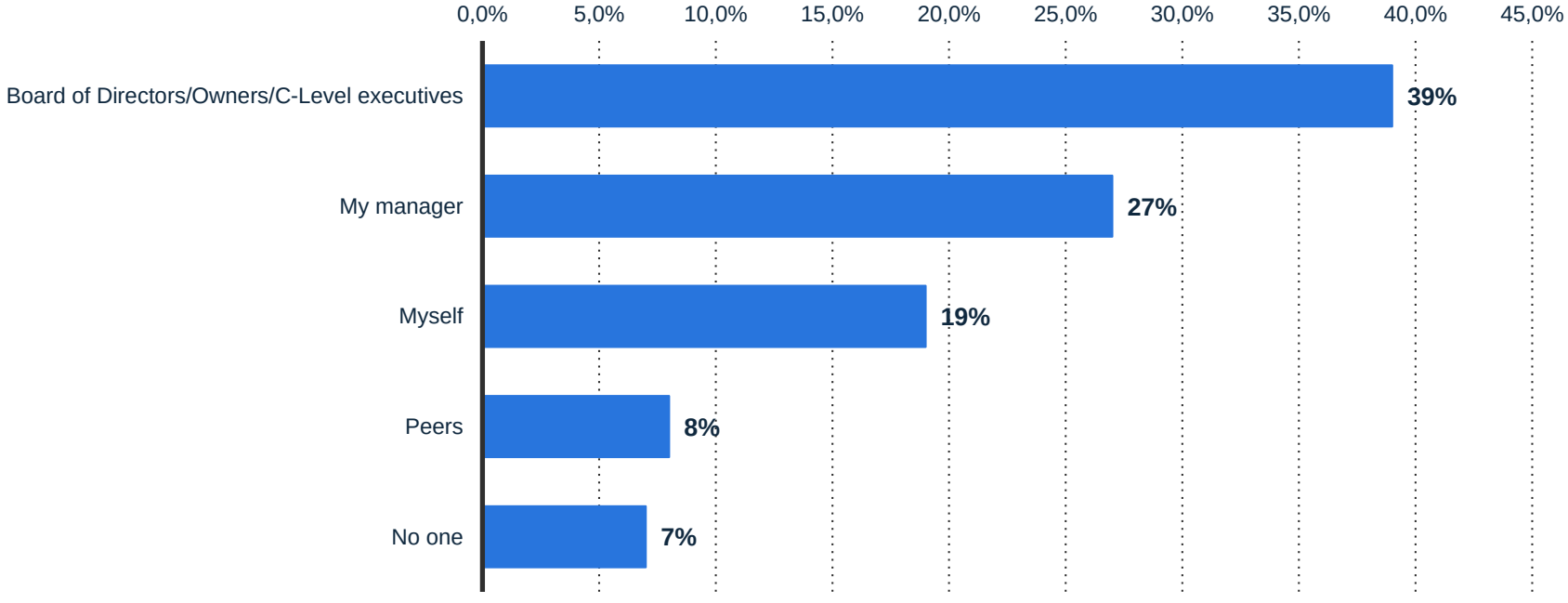
Distribution of annualized costs for external consequences of cyber attacks [%]



Source: Statista

Who exerts the most pressure on you related to IT security?

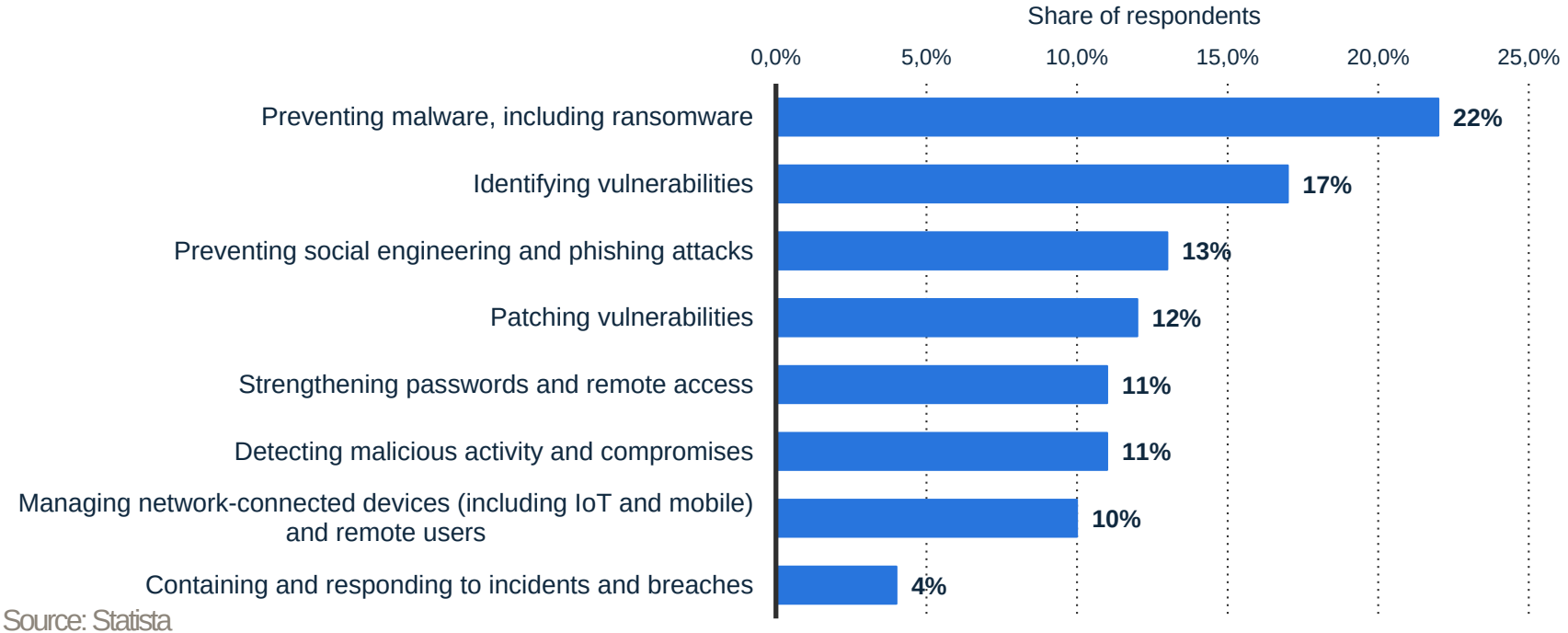
Global human cyber security pressures 2018 [%]



Source: Statista

Which IT security tasks are you facing the most pressure to address?

Most pressing cyber security issues according to IT professionals worldwide 2018



Source: Statista

II. Fraud

Movies: Office space, catch me if you can, the informant

https://www.youtube.com/watch?v=yLet69-JhW0

Fraud is commonly referred to as white collar crime

Any **means** a person uses to gain an **unfair advantage** over another person; includes:

- A **false statement**, **representation**, or **disclosure**
- A **material fact**, which induces a victim to act
- An **intent** to deceive
- Victim **relied** on the misrepresentation
- **Injury** or **loss** was suffered by the victim

Fraud comes in four stakeholder categories

Management	Employee	Customer	Vendor

Hidden in pre-lecture version

Why do people commit fraud?

Hidden in pre-lecture version

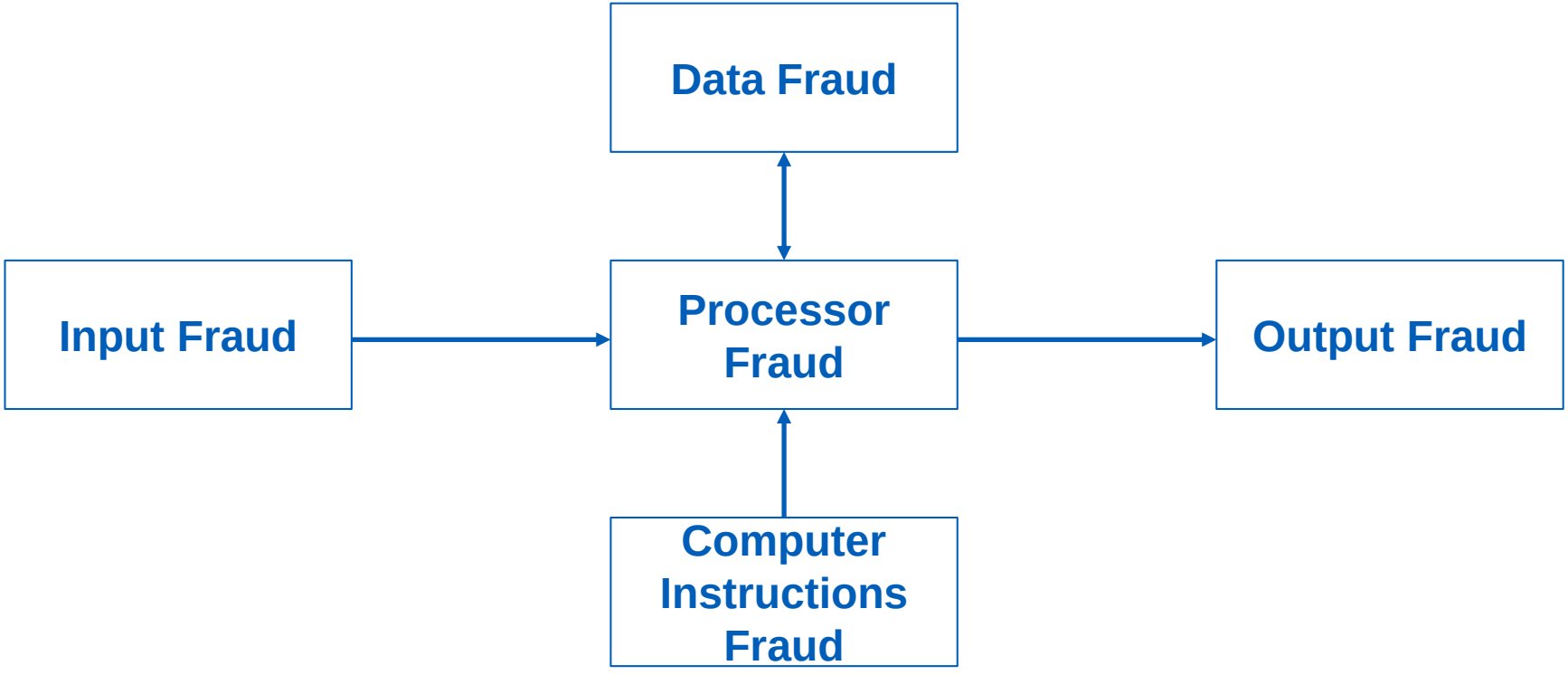
Hidden in pre-lecture version

Hidden in pre-lecture version

Hidden in pre-lecture version

Hidden in pre-lecture version

Fraud occurs at every step in the data processing cycle



III. Computer fraud

Attacks are commonly divided into three forms

- **Hacking:** Unauthorized access, modification, or use of an electronic device or some element of a computer system
- **Social Engineering:** Techniques or tricks on people to gain physical or logical access to confidential information
- **Malware:** Software used to do harm

Why would someone fall victim to manipulation?

Hidden in pre-lecture version

Minimize the Threat of Social Engineering by:

- Never let people **follow you into restricted areas**
- Never **log in for someone else** on a computer
- Never **give sensitive information** over the phone or through e-mail
- Never **share passwords** or user IDs
- **Be cautious** of someone you don't know who is trying to gain access through you

Hacking – Hijacking and Botnet (1/6)

- **Hijacking**
  - *Gaining control of a computer to carry out illicit activities*
- **Botnet (robot network)**
  - *Zombies*
  - *Bot herders*
  - *Denial of Service (DoS) Attack*
  - *Spamming*
  - *Spoofing*
    - Makes the communication look as if someone else sent it so as to gain confidential information.

Hacking – Spoofing (1/6)

- **Forms of spoofing**
  - *E-mail spoofing*
  - *Caller ID spoofing*
  - *IP address spoofing*
  - *Address Resolution (ARP) spoofing*
  - *SMS spoofing*
  - *Web-page spoofing (phishing)*
  - *DNS spoofing*

Hacking – with Computer Code (1/6)

Cross-site scripting (XSS)

- Uses vulnerability of Web application that allows the Web site to get injected with malicious code. When a user visits the Web site, that malicious code is able to collect data from the user.

Buffer overflow attack

- Large amount of data sent to overflow the input memory (buffer) of a program causing it to crash and replaced with attacker's program instructions.

SQL injection (insertion) attack

- Malicious code inserted in place of a query to get to the database information

Hacking – Other (1/6)

- **Man in the middle (MITM)**
  - *Hacker is placed in between a client (user) and a host (server) to read, modify, or steal data.*
- **Masquerading/impersonation**
- **Piggybacking**
- **Password cracking**
- **War dialing and driving**
- **Phreaking**
- **Data diddling**
- **Data leakage**
- **Podslurping**

Hacking – used for embezzlement (1/6)

Salami technique:

- Taking small amounts at a time
  - *Round-down fraud*

Economic espionage

- Theft of information, intellectual property, and trade secrets

Cyber-extortion

- Threats to a person or business online through e-mail or text messages unless money is paid

Hacking – used for fraud (1/6)

- Internet misinformation
- E-mail threats
- Internet auction
- Internet pump and dump
- Click fraud
- Web cramming
- Software piracy

Malware types

- **Spyware**
  - Secretly monitors and collects information
  - Can hijack browser, search requests
  - Adware, Scareware
- **Ransomware**
  - Locks you out of all your programs and data using encryption
- **Keylogger**
  - Software that records user keystrokes
- **Trojan Horse**
  - Malicious computer instructions in an authorized and properly functioning program
- **Trap door**
  - Set of instructions that allow the user to bypass normal system controls
- **Packet sniffer**
  - Captures data as it travels over the Internet
- **Virus**
  - A section of self-replicating code that attaches to a program or file requiring a human to do something so it can replicate itself
- **Worm**
  - Stand alone self replicating program

Thank you!
Questions?