Achieving Information Security

Beyond penetration testing and frameworks

ISACA Athens Conference – 25 November, 2014

Deloitte.

“All good information security presentations start with a Bruce Schneier quote”

- Not Bruce Schneier

#whois aridavies

- Born in GR, grew up in UK, living in NL

- Senior Manager with Deloitte (first UK, now NL)
- MSc in Information Security
- Over 12 years IS experience
- Working as part of a large ethical hacking team (40+ hackers)
- Background on Physical Security, Client-Side Attacks, Social Engineering, Infrastructure
- Concentrating on red teaming, simulations and threat intelligence

- *ISACA member for two years*
- *Passed CISM June 2013*
- *Just got around to submitting the application a week ago!*

Information Security & Compliance

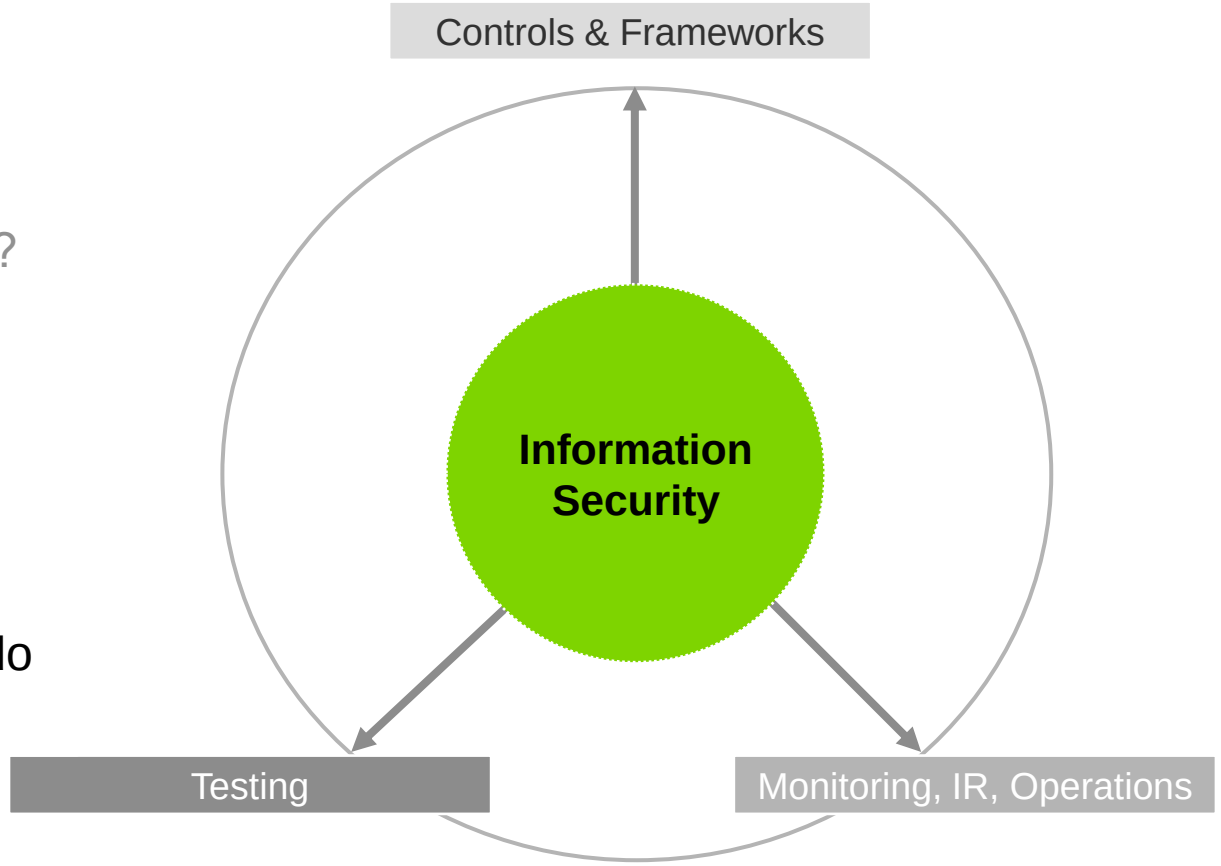
- We are compliant with a framework,
- We test controls based on risk assessments,
- We pentest infrastructure and applications.

…But are we secure?

- We have monitoring and incident response

…But has it been tested?

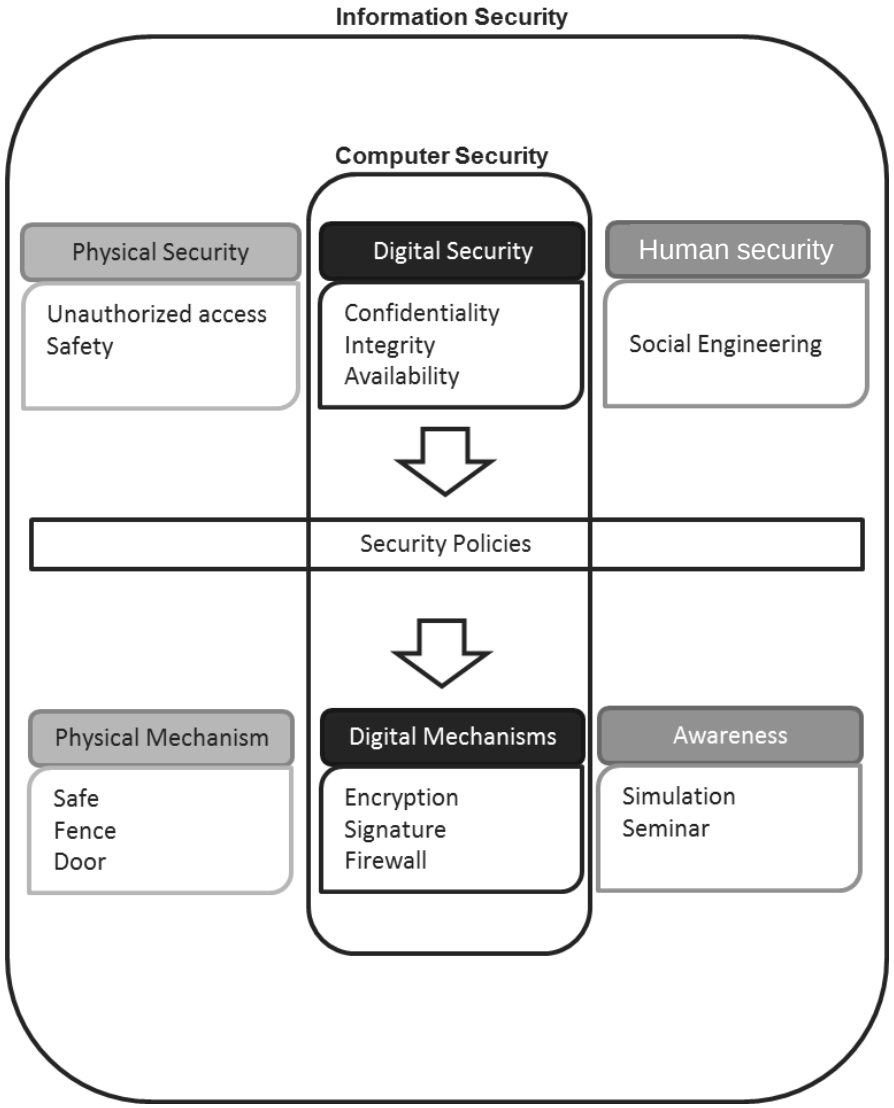
- Do we really understand what an attacker would do in our environment?



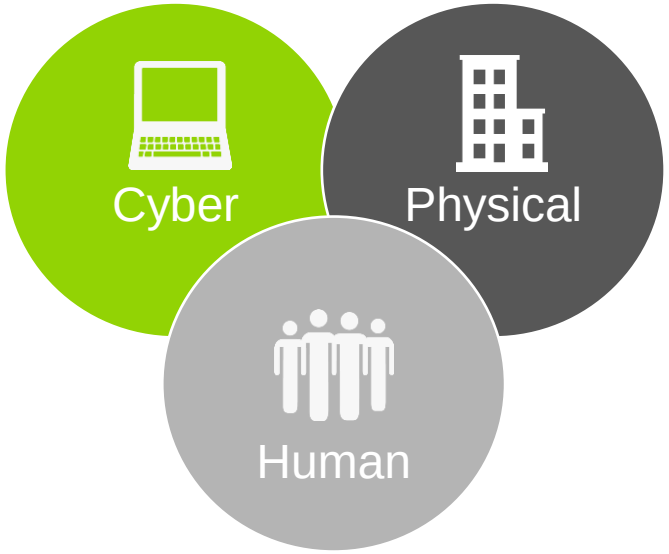
Information security vs. Computer security

- It is important that as corporations as well as employees we realize that information security is not just about computer security. Computer security can carry the wrong assumption that as long as our infrastructure and systems are secure we are also secure.

- The figure on the right side shows the difference between information and computer security by demonstrating the three elements of information security.
  - **Computer security** is only applicable to one of the three major pillars of information security.
  - **Physical security** & **human security** are equally important.
  - **Security policies** can and should be applied across all three elements.



The Information Security Trinity

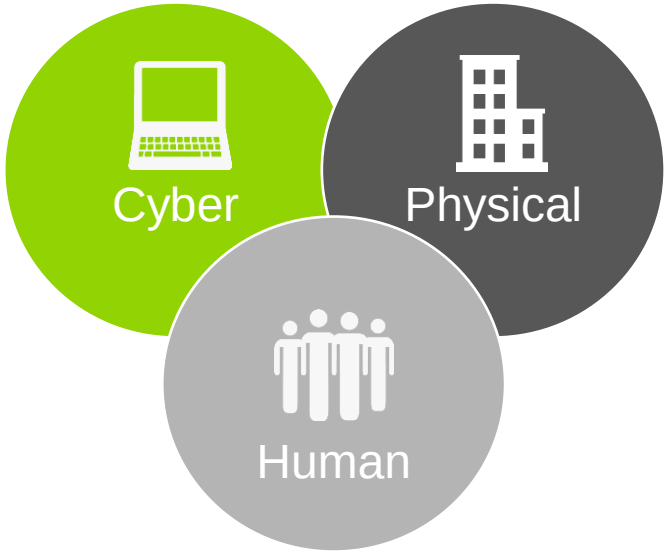


The three elements of information security are:

- **Cyber**: The online world, the Internet as well as corporate intranets and all other computer networks.
- **Physical**: this is the buildings, the desks, the safes and the IT Big Iron itself.
- **The Human**: the sometimes ignored or misunderstood link that binds the cyber and physical world together.

- "As long as our infrastructure and systems are secure, our organization is also secure."

The Information Security Trinity



The three elements of information security are:

- **Cyber**: The online world, the Internet as well as corporate intranets and all other computer networks.
- **Physical**: this is the buildings, the desks, the safes and the IT Big Iron itself.
- **The Human**: the sometimes ignored or misunderstood link that binds the cyber and physical world together.

- "As long as our infrastructure and systems are secure, our organization is also secure."

FALSE

Attackers won't limit themselves to abusing only computer security weaknesses. They will combine all aspects to identify the path of least resistance in an organization.

Examples from the news

Traffickers Hack Shipping Containers

Published on October 23, 2013 by Mark Lowe · No Comments

The scheme sounds like a work of near science fiction. But police in the Netherlands and Belgium insist its true, and say they have the evidence to prove it.

To Move Drugs, Traffickers Are Hacking Shipping Containers

By Alex Pasternack, Vice Motherboard

The scheme sounds like a work

NEW YORK (CNNMoney)

JPMorgan … cybercriminals gathered in… on m… account holders as part of a ma… hac…

The revelation follows news back in August that … country's largest banks, using sophisticat… to their … systems and manipulate records.

At JPMorgan (JPM), the hackers got c… act information for 76 million ho… million small businesses, including names, addresses, phone number… addresses, as well as "internal JPMorgan Chase information re…

… York Police Dept. impacts …000

… executive is accused of stealing computer tapes

…mer, Network World

…05, 2009 11:50 AM ET

Share/Email Tweet This 1 Com… Newsletter Sign-Up

The New York Police Dep… …usands of police officers that their personal informati… …e to a suspected data theft done by a… in the police… …reports in New York's daily newspape…

…ved as the pension fund's director of … …stealing computer tapes from a Staten … …n 80,000 current and retired police off… …York Post … sources.

…Businessweek

…://www.businessweek.com/articles/2014-03-13/… …credit-card-data

Missed Alarms and … Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dun… …ch 13, 2014

(Corrects to id… …g the story.)

Th… history wasn't particularly inventive, nor did it appear destined for success. In the days prior to … someone installed malware in Target's (TGT) security and payments system designed to steal every credit … company's 1,797 U.S. stores. At the critical moment—when the Christmas gifts had been scanned and bagged and … asked for a swipe—the malware would step in, capture the shopper's credit card number, and store it on a Target server commandeered by the hackers.

Stuxnet – transported through USB

Wikileaks – copied by CDs

Snowden – 4 laptops on a plane

Physical Security

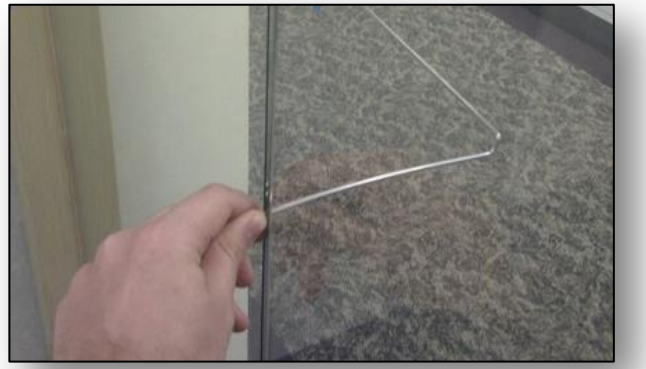
Physical Security

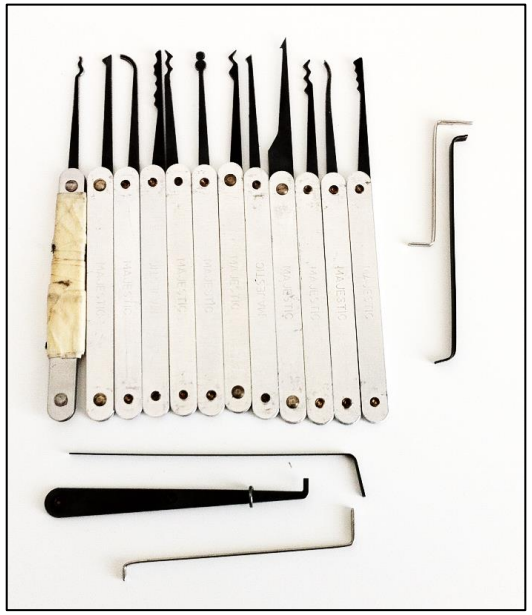
- It’s very common for physical security to be handled by a different team
- Partial communication between information and physical security teams
- Physical security can become a blind spot for information security

In any case, should we care?!

- Absolutely! Information exists in the physical world.
- Attackers will always take the path of least resistance!

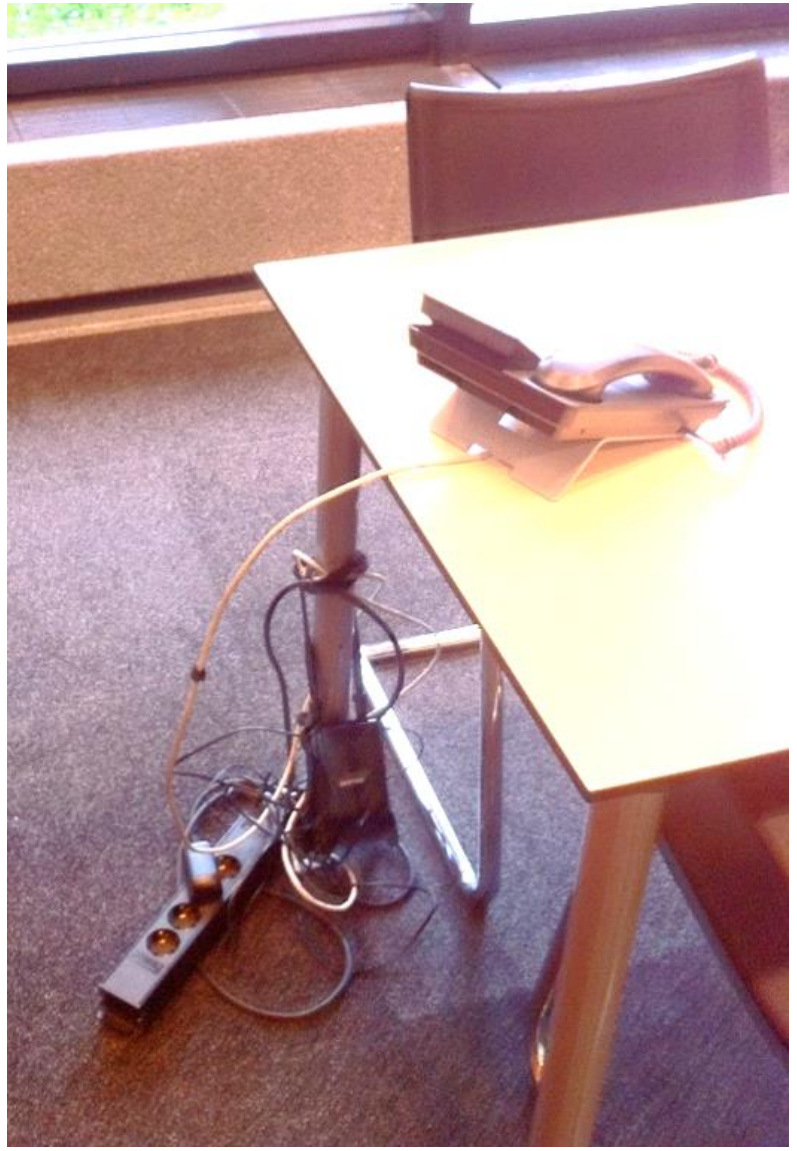
Physical Security – A hacker's toolkit





Physical Security – A hacker's toolkit

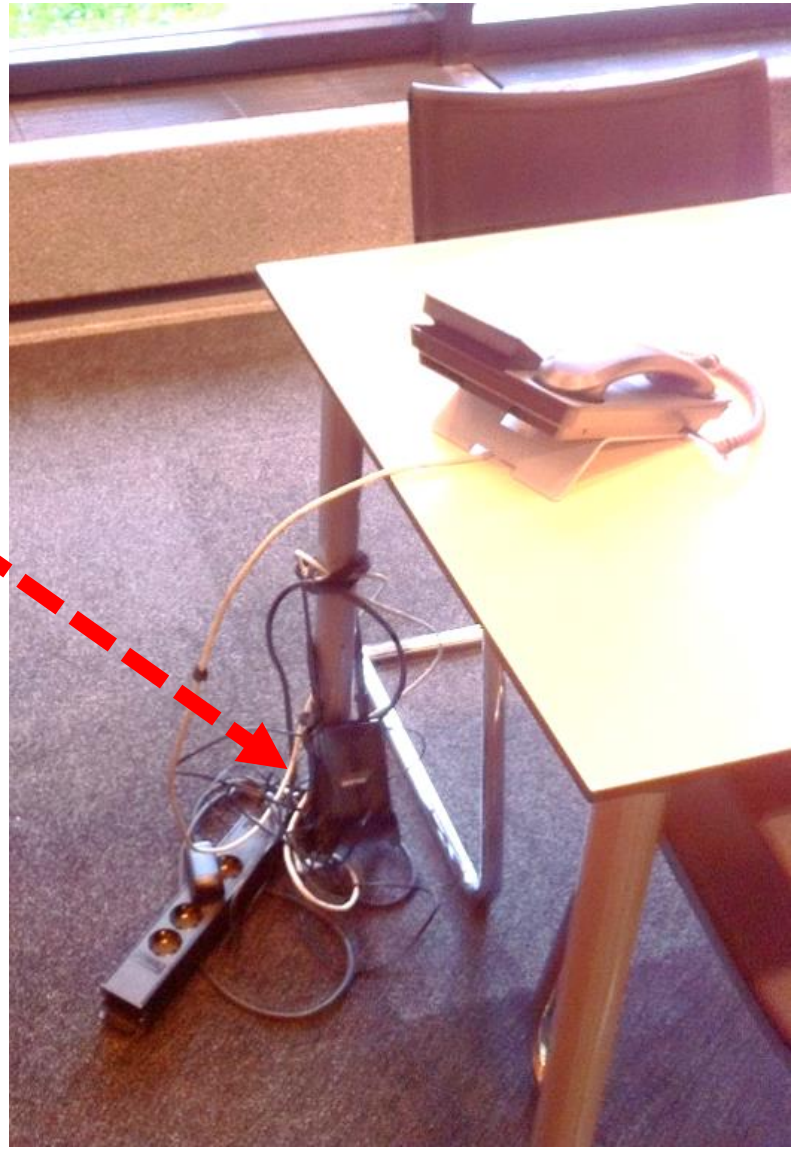
Anything **wrong** with this picture?



Physical Security – A hacker's toolkit

Anything **wrong** with this picture?

A few more examples…



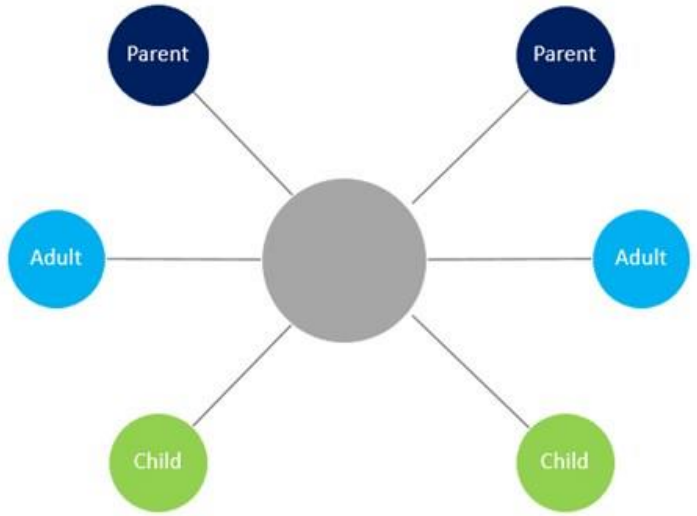
Human Security

Human Security

Social Engineering = Hacking the Human

- Without Social Interaction we would not have formed towns, cities or even businesses;
- We are trained **as children** to follow commands;
- We are trained **as children** to cooperate and be helpful;
- We are trained **as children** to respect authority (of one form or another);
- We are glad when people thank us for a job well done;
- Believe it or not, we seek to satisfy others.

> Social Engineering: The process of deceiving people to provide confidential information using a person's bias towards trust.
>
> - The human condition



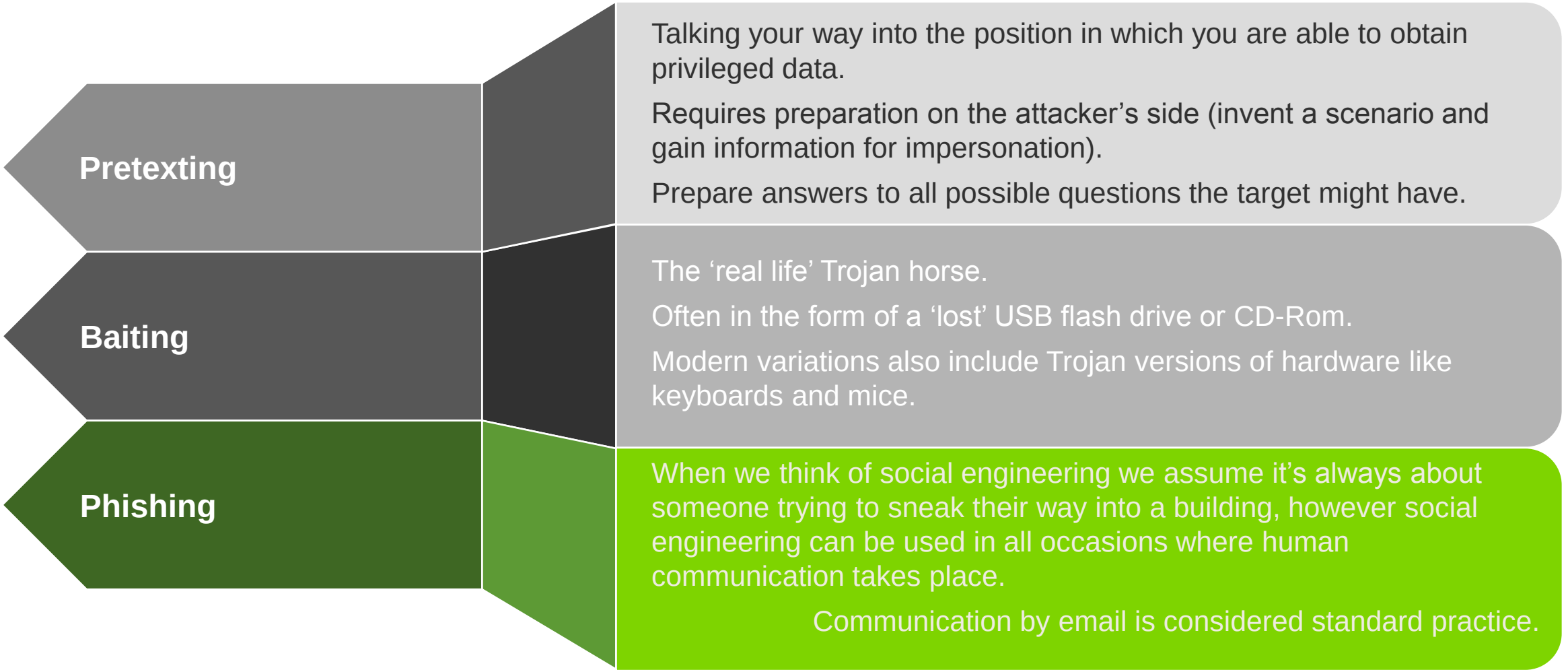
We respond to basic emotions such as

- Guilt
- Greed
- Love/Lust/Flirtation
- A sense of belonging/team
- Moral duty/responsibilities/duty
- Desire to succeed or accomplish tasks
- Following commands
- Pure survival

Human Security

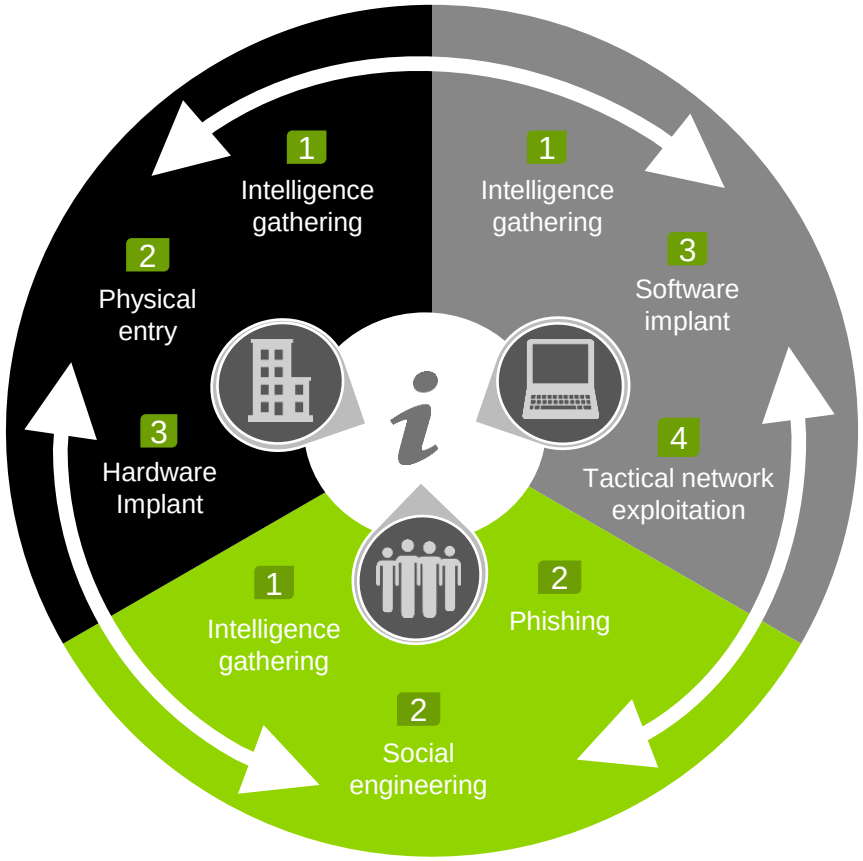
Type of Social Engineer	Motivation
Corporate Spies	Proprietary Information for completive advantage.
Disgruntled Employees	Proprietary Information for resale. Use of information to damage company's reputation, business processes or both.
Executive and Corporate Recruiters	Identify and recruit key employees with access to proprietary information offering financial incentives, to gain access to valuable intellectual property.
Hackers	Personal gain, thrill, maliciousness, social activism.
Identity Thieves	Personal gain through various forms of credit fraud.
Penetration Testers	White hat hackers engaged by a company to test security processes and employees.
Scam Artists	Personal gain, perpetrated as an individual or in groups may be associated with organized crime.
State Sponsored Spies	Proprietary Information for resale. Use of information to further national aims both commercial and military.

Human Security



Bringing it all together

Bringing it all together



Combined scenarios flow		
1	Attackers perform target reconnaissance and gather information required for the next stages of the attack. Such information might contain: employee and third party data, technical or physical aspects. **(Physical, Cyber and Human – Intelligence gathering)**	
2	Attackers break the physical perimeter and gain physical access to the target location. ***(Physical + Human – Physical entry via social engineering)***	Attackers trick employees into installing malware via an targeted email phishing attack. ***(Human – Mail phishing via social engineering)***
3	Taking advantage of the physical access priory obtained, attackers install a hardware implant in the target office building. ***(Physical – Hardware implant)***	The malware installed as a result of the phishing attack is used by attackers to implant other software necessary for remote access to the network. ***(Cyber – Software implant)***
4	Attackers gain remote access to the internal network via the implanted hardware and software. Further, attackers use this as a stepping stone to gain access to critical systems and data. ***(Cyber – Tactical network exploitation)***	

Conclusions

Conclusions

- *Information* Security is not just about *IT* security
  - Digital, Physical, Human; All matter equally.

- Compliance, Frameworks and pentesting is great! But…
- We still need to look at the bigger picture.
  - Are we secure? *Where do we base that?*
  - Will our Monitoring/Operations team identify an incident?
  - Will our Incident Response team react appropriately?

Increase the scope to the whole organisation, not just IT and not just individual controls and applications/infrastructure

Three-dimensional security testing shows what controls can (and will be) bypassed, but also allows us to understand how our teams (monitoring, system administration, incident response, etc.) will react to such an incident.

Watch the Deloitte Cyber Videos,
including “Companies Like Yours” at:
deloitte.nl/cybervideo

Deloitte.

Thank you.

Contact me

Ari Davies

twitter.com/kussic
adavies@deloitte.nl

Deloitte Contact in Athens

Ioannis Diveris

idiveris@deloitte.gr

Deloitte.

Deloitte.