Procedural and People Security

Security culture with organisations

- Information assurance becomes useless if the people it aims to protect are not security-conscious.

- How can we create a security-conscious culture within the organisation?
  - *Need to understand procedures*
  - *… and to understand people.*

Security Awareness

- All employees should be aware of the risks that exist within the organisation – and why they are risks.
- Training needs to be relevant to the staff in order to be effective.
- Staff may be familiar with confidential issues – what about integrity and availability though?

Contracts of employment

- Terms and conditions of employment, with legal standing.
  - Responsibilities of the employee to the organisation
  - Obligations of the organisation to the employee

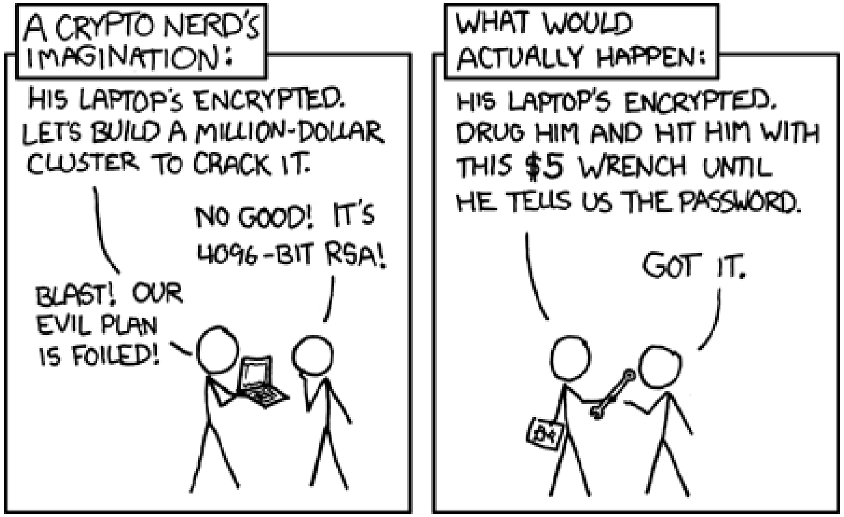
- Non-disclosure/confidential of information
- Acceptable use of company assets
- Ownership of intellectual property
- Acceptable standards of behaviour and conduct

Segregation of duties and avoiding dependence

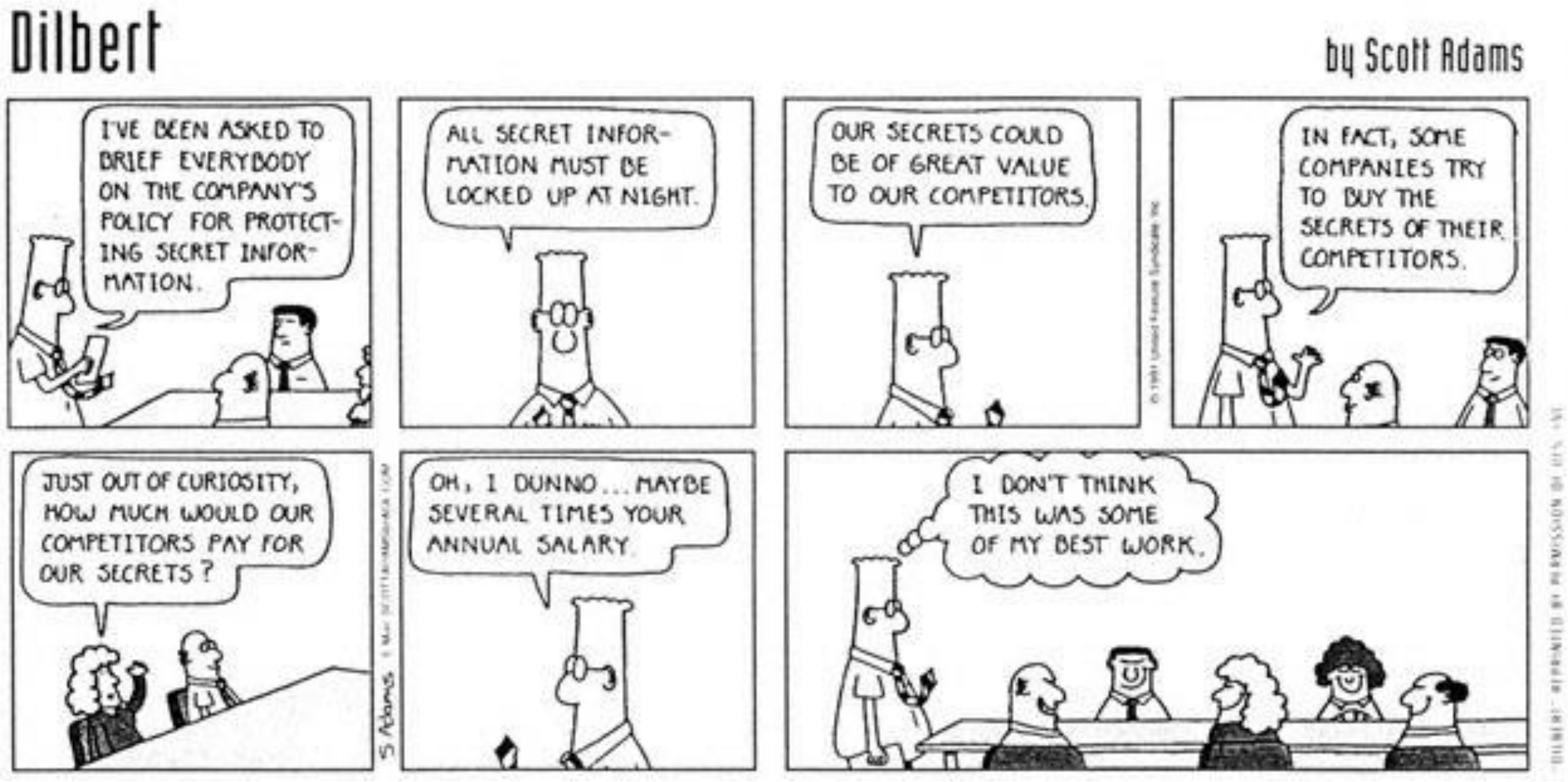
- One person may not perform the duties for more than one role where there could be a conflict of interest
- Limit scope that individual has to attack, or perform system misuse.
- Limit dependence that organisation has on any one individual.

Human factors

- The greatest security vulnerability by far is the human
- Attackers will exploit social etiquette to conduct their attack.
- "Social Engineering" – to engineer a social situation that provides an advantage or a means of attack.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
B4

Security Management in Practice


Dilbert
by Scott Adams
I'VE BEEN ASKED TO BRIEF EVERYBODY ON THE COMPANY'S POLICY FOR PROTECTING SECRET INFORMATION.
ALL SECRET INFORMATION MUST BE LOCKED UP AT NIGHT.
OUR SECRETS COULD BE OF GREAT VALUE TO OUR COMPETITORS.
IN FACT, SOME COMPANIES TRY TO BUY THE SECRETS OF THEIR COMPETITORS.
JUST OUT OF CURIOSITY, HOW MUCH WOULD OUR COMPETITORS PAY FOR OUR SECRETS?
OH, I DUNNO... MAYBE SEVERAL TIMES YOUR ANNUAL SALARY.
I DON'T THINK THIS WAS SOME OF MY BEST WORK.
S. Adams

Discussion:
"What are the security challenges of social engineering?"

Social Engineering – Passwords

- Passwords
  - – Commonly used passwords (mother’s maiden name, pet, school, teachers) are wide open to attack.
    - Attacker may attentively enquiry with victim.
    - Social Media is a big giveaway nowadays too!

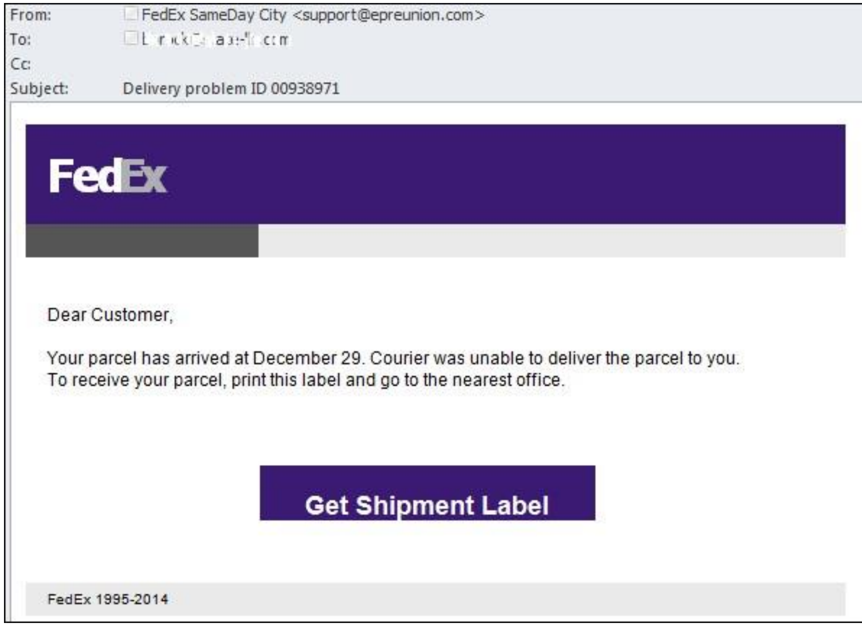
Social Engineering – Passwords

- 50% of Britons know someone whose account has been hacked
- One in six admit accessing someone else's account by guessing their password
- 10% have guessed a colleague's password
- Nearly half (48%) of those polled have shared a password with someone else
- Women are more likely to share their passwords than men, and over twice as likely to share it with their children
- As many as one in six use a password consisting of their pet's name

(https://grahamcluley.com/2013/08/pet-name-passwords/)

Social Engineering – Phishing

- Phishing e-mails still widely used and still quite successful among non-technical users.
- Spear-phishing e-mails are targeted towards particular users/organisations, with more specific details
  - More likely to be convinced this way!
- *“In the first quarter of 2015, the Anti-Phishing system was triggered 50,077,057 times on computers of Kaspersky Lab users. This is 1 million times more than in the previous quarter.”*



From: FedEx SameDay City <support@epreunion.com>
To: [redacted]
Cc:
Subject: Delivery problem ID 00938971

Dear Customer,

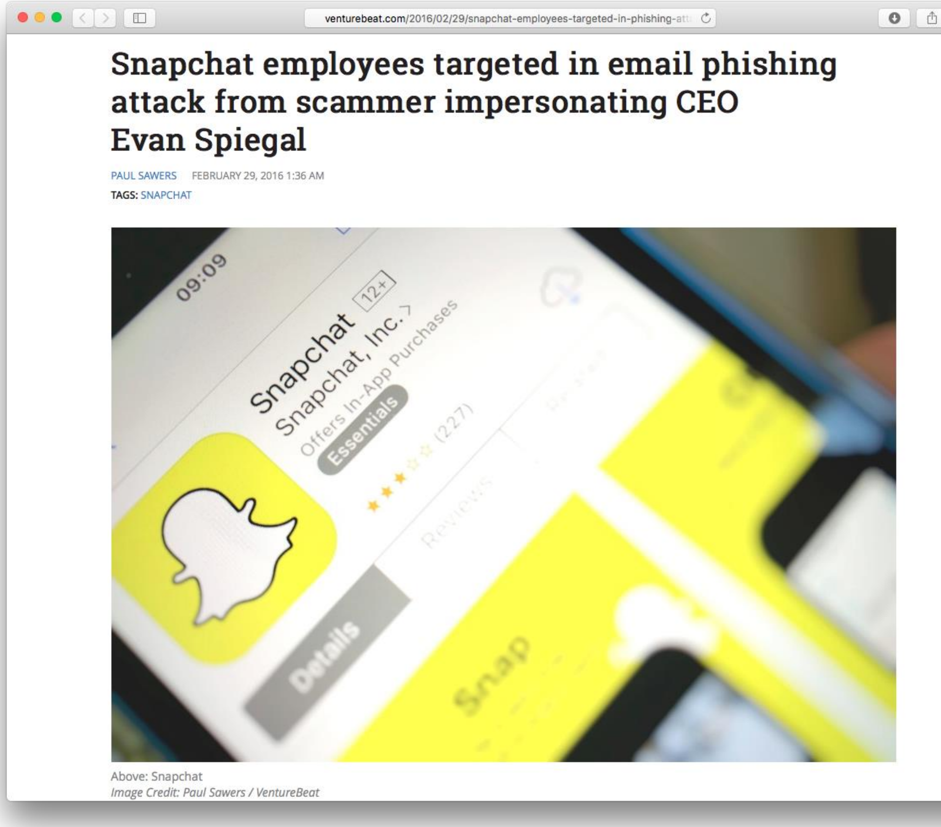
Your parcel has arrived at December 29. Courier was unable to deliver the parcel to you.
To receive your parcel, print this label and go to the nearest office.

FedEx 1995-2014

Social Engineering – Phishing

- Spear-phishing campaign impersonates as Snapchat CEO.
- Email requests payroll data for all employees.
  - Payroll department didn't notice it was a scam – they sent the details as asked.
- Employee personal data has been leaked – company now offering identity-theft insurance to employees as compensation.

- *http://venturebeat.com/2016/02/29/snapchat-employees-targeted-in-phishing-attack-from-scammer-impersonating-ceo-evan-spiegal/*



venturebeat.com/2016/02/29/snapchat-employees-targeted-in-phishing-att

Snapchat employees targeted in email phishing attack from scammer impersonating CEO Evan Spiegal

PAUL SAWERS FEBRUARY 29, 2016 1:36 AM

TAGS: SNAPCHAT

Above: Snapchat

Image Credit: Paul Sawers / VentureBeat

Social Engineering - Access

- What is social etiquette for holding doors open for others?
- Carrying heavy objects makes people more likely to comply.
- Who would ask to see ID to see whether this woman should have access?

Social Engineering - Theft

- E.g., A store operates security bag checks on staff at end of shift.
- Employee disguises stolen items by being ill in handbag!
- Should the security staff search the bag, despite being unpleasant…?
  - *Sounds extreme – but this was actually a real case that lasted months!*

How to avoid Social Engineering attacks?

- Be aware of social engineering – things are not always as they seem.
- Stay alert, and question anything that appears suspicious.
- Policy and procedure exists to protect against attacks – avoid distractions that aim to circumvent policy.

More on social engineering

- http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411
- http://www.social-engineer.org/framework/general-discussion/real-world-examples/
- https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
- http://resources.infosecinstitute.com/social-engineering-a-case-study/
- http://money.cnn.com/2012/08/07/technology/walmart-hack-defcon/
- http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
- http://www.oii.ox.ac.uk/webcasts/?id=213
- https://lra.le.ac.uk/handle/2381/10288
- http://www.dummies.com/how-to/content/a-case-study-in-how-hackers-use-social-engineering.html
- http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack
- http://www.highbitsecurity.com/casestudies-socialengineering-hospital.php
- http://www.infoworld.com/article/2617997/security/ex-hacker-spills-secrets-of-fighting-social-engineering.html
- http://www.ieee-security.org/TC/SPW2014/papers/5103a236.PDF

Recap

- Organisational procedure should introduce a culture of security
  - Security awareness
  - Clear guidance in contracts
  - Segregation of duties
- Human factors of Security
  - Social Engineering

Any questions?

Examples of Social Engineering

- https://www.youtube.com/watch?v=lc7scxvKQOo
- https://www.youtube.com/watch?v=PWVN3Rq4gzw