“...in 2005 Facebook didn’t exist for most people, “twitter” was still a sound, the cloud was something in the sky, 3G was a parking space, applications were what you sent to colleges, and “Skype” was a typo.”

Thomas Friedman
**Data Security - Landscape**

- Personal data has a value
- Different political reactions
- Different legal systems worldwide
- Different enforcement even within Europe
- Contrasting approach Europe v. US
- Snowden & Schrems has changed the game

---

**EU data protection law**

- Principles based
- Local law varies
- Enforcement varies
- Prior registration can be required to collect data
- Steps must be taken if transferring data to the US (or most other non-EU countries)

---

**Article 6, principle f**

Data must be:

"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
Article 32
Keep data secure

Article 33
If you fail to tell a regulator without undue delay and in most cases not later than 72 hours

Article 34
You might need to tell data subjects
Prevention

Dutch CBP: 
"Contingency plan
Every organisation should have a contingency plan indicating exactly what is to happen in the event of an emergency. However, such a plan is useful only if personnel are familiar with it and regular drills have been held to practise its implementation..."

Article 35

Data Protection Impact Assessments

Privacy class actions

- "Material or non-material damage"
- Controllers and processors could end up paying
- The Schrems case
- Morrisons
- Don’t look at GDPR in isolation (e.g. NIS Directive; e-Privacy Directive)
The Perfect Storm... More (& Less)

More...
- Attacks (and cheaper too)
- Reliance on 3rd parties, e.g. outsourcing; SaaS, Cloud
- Cost pressure
- Regulation and enforcement
- Geography
- Social networking
- Value in stolen data
- Speed
- Whistleblowers
- Chance of getting caught
- Focus on investigations
- Subject militancy e.g. Google case
- People trying to rewrite the past - because they can

Less...
- Care
- Compliance and legal resources
- Attention to contractual terms
- Vendor accountability
- Sympathy from courts & regulators

Top Tips

- Be secure
- Insure?
- Keep records (but do not fall for the Article 30 trap)
- Train your staff
- Have proper policies and procedures
- Fire drill

Resources

A Simulated Criminal Attack
Lessons from a Red Team Exercise

Mike McLaughlin

- Cyber Security Operations Manager
- Ethical Hacker and Social Engineer at First Base Technologies since 2006
- Published technical writer for TechTarget and ComputerWeekly
- Cyber Security commentator for BBC
Lessons from a red team exercise

“The story you are about to hear is true; only the names have been changed to protect the innocent vulnerable.”

Remote information gathering

- Remote information gathering CCP is situated in the UK, reviewed on Google maps and street views
- 4 registered domains
- 5 IP address ranges
- 72 Internet-facing hosts
- Metadata retrieved for Adobe, Office and QuarkExpress
- Scan revealed OWA in use
- Internet search for relevant email addresses
- LinkedIn searches to construct email addresses for employees
- 400 email addresses identified
- “Interesting” staff names and job titles from LinkedIn
- Emails sent to obtain responding email style and layout
Results of info gathering

1. Spear phishing is viable and can be used for theft of credentials
2. Head office will require legitimate appointment to gain physical access
3. Branch office may be when there is no security with remote backup
4. Significant number of other premises available as fallback
5. Phishing and other issues are typical remote vulnerabilities will apply

Spear phishing plan

1. Spear phishing fake domain name was used and sent out
2. OWA site cloned onto fake domain to steal credentials
3. Large number of email addresses used as targets
4. Design of real emails copied to facilitate spear phishing
5. Name on fake email gathered as fake sender
6. Someone will be used to test fake email credentials
7. Gemex will be used to test site on attacker's website (for future internal use)
Spear phishing exercise

1. Email sent from IT manager, using fake domain address
2. OWA cloned on to tester’s laptop, DNS set accordingly
3. Email sent to three groups of 100 recipients
4. Within a few minutes, 41 recipients entered credentials
5. Credentials tested on legitimate OWA site
6. Significant information gathered from each account
7. Further emails can now be sent from legitimate addresses

Branch office attack plan

1. Team member “Harry” to pose as a contractor working for a telecomms firm
2. Clothing and ID badge prepared
3. Works order fabricated
4. Engineering toolkit prepared, including laptop
5. Engineering toolkit obtained from spear phishing attack on email
6. Other team members on landline phones for remote verification

Branch office attack exercise (I)

- Harry arrives and tells receptionist he needs to fix a network fault
- Receptionist asks for assistant name for verification
- Harry claims to be the network engineer and gives the name of an IT employee (who is out of office)
- Receptionist confirms contact and requests that Harry’s name be added to IT Manager’s directory
- Receptionist asks for contact information for IT Manager
- Paul (manager) asks for Harry’s name and gives contact information
Branch office attack exercise (2)

Harry is escorted into the office and given a desk and a network point.

He is left unsupervised and plugs his laptop into the network.

He explores the network and identifies several Windows servers.

He authenticates to a domain controller using credentials obtained during the phishing exercise.

He explores various servers and identifies many interesting files.

He plants several files to demonstrate full read-write access.

He explains that he has run diagnostics and that the network connection seems ok. He is escorted to reception and signs out.

Head office attack plan (1)

A number of scenarios were considered:

• Apply for a job vacancy with a suitable fake CV
• Casual meeting with a potential client
• Research for items or news or publications
• Discussion about a school tour of premises
• Tour of premises as a prospective customer

Two alternatives were selected and developed:

• Tour of premises as a prospective customer for a specific product
• Interview for a charity magazine about corporate fund raising

Head office attack plan (2)

 Relevant domain names were obtained, email addresses and web pages created for both fake organizations.

1. Tour of premises as a prospective customer for a specific product:

   - “Anne” sent an email via the company’s online form
   - An exchange of emails occurred over the next few days and she obtained permission, as a new customer, to book a tour of the premises

2. Interview for a charity magazine about corporate fund raising:

   - “Anne” called the company and spoke to the head of fund raising
   - Press office called Anne and asked for more details
   - Background research proved convincing and pretext was accepted
   - Interview booked at head office

Option 2 entailed less risk of exposure so was attempted first.
Head office attack exercise

1. Anne and George arrive for the press interview, are given visitor passes and escorted to a meeting room
2. George asks to use the bathroom and is given directions
3. A senior employee joins the meeting and asks further questions to validate their story, which is answered satisfactorily
4. George returns from the bathroom but quickly exits the meeting again having a pack of diarrhoea medicine on the table
5. During his 'bathroom visit', George is able to access unattended lab computers, simulate installing keyloggers and remote control software and copying files on to a USB drive
6. When the interview concludes, Anne and George are escorted from the building

Lessons

1. No checks on social networking using work email addresses
2. No sanitisation of metadata in published documents
3. Insufficient staff training on spear phishing
4. Inadequate visitor validation at branch office
5. Unsupervised visitor at branch office
6. Unsupervised visitor at head office (bathroom break)
7. Unlocked, unattended laboratories and unlocked computers
8. No challenging of unescorted visitors
9. Sensitive information protected only by Windows credentials

GAME OVER

LIVES 0
Red Team Testing

- Spear phishing tests
- Exploit testing
- Authorization tests
- Engage in test scenario to validate control
- Test your preventive and detective controls
- Learn, improve, repeat!