The low down on data security post-GDPR

Frankfurt, 26 March 2018

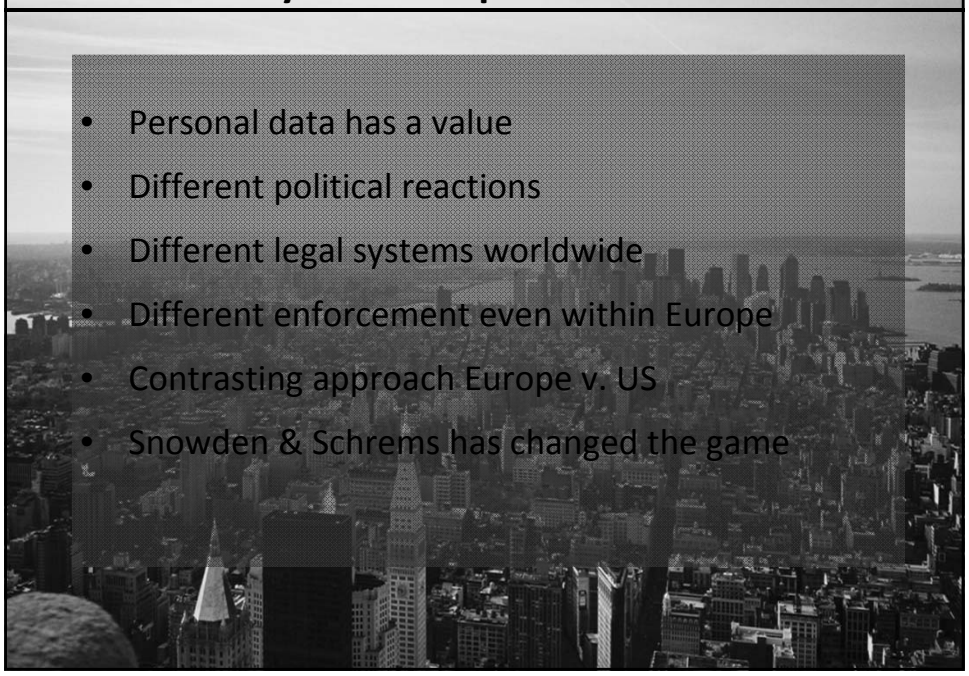
Jonathan Armstrong and Mike McLaughlin

@CorderyUK

"…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:

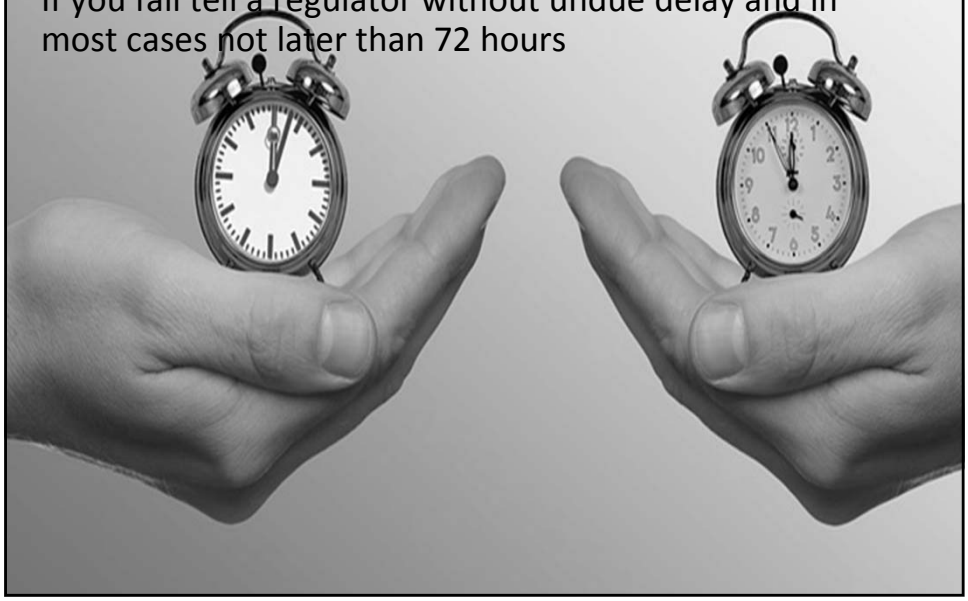
"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 32

Keep data secure

Article 33

If you fail 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

- Short GDPR film - www.bit.ly/gdprfilm
- GDPR FAQs – www.bit.ly/gdprfaqs
- EU Glossary – www.bit.ly/gdprwords
- GDPR Navigator – www.bit.ly/gdprnav
- Morrisons alert - http://www.corderycompliance.com/client-alert-morrisons-data-breach-litigation-succeeds/
- Data Breach Academy - http://www.corderycompliance.com/cordery-data-breach-academy-2/

FIRST BASE technologies

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 commenter for BBC

First Base Technologies

Cyber Resilience

Threat and Risk

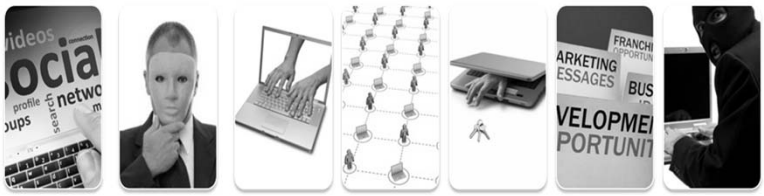
Cyber Awareness

Managed Services

Penetration Testing

Compliance Testing

How an Advanced Attack Works



Background Research	Social Engineering	Control Your PC	Explore the Network	Take Control	Find the Data	Steal the Data
• Internet searches • Social networks • Metadata • Phone calls • 192.com	• Spear phishing • USB attacks • Phone calls • Fake staff • Service staff • Visitors	• Malware • Key logging • Physical exploits • Wireless intercepts	• Servers • Desktops • Network devices • Firewalls • Wireless	• Windows admin • Network admin • Business apps • Database	• Strategy • Intellectual property • Marketing plans • HR data • Finance • Salaries	• VPN • Wireless • Email • FTP • Extranet • Physical devices

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!5 premises in UK, reviewed on Google maps and street view
- 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

On-site reconnaissance

- Head office:
  - Perimeter guards and external CCTV
  - Main reception manned and controlled
  - Goods entrance well controlled
  - No other access
  - Staff ID card design noted
  - Results used to plan on-site attack 2
- Branch office:
  - High street premises, no guarding
  - Small reception, one receptionist
  - Door intercom
  - Multi-tenanted building
  - Results used to plan on-site attack 1

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 vulnerable to ad hoc visitor with remote backup
4. Significant number of other premises available as fallback
5. Windows and Office in use, so typical network vulnerabilities will apply

Spear phishing plan

1. Convincing fake domain name available and purchased
2. OWA site cloned onto fake domain for credential theft
3. Large number of email addresses harvested as targets
4. Design of real emails copied to facilitate spear phishing
5. Names and job titles gathered as fake senders
6. Genuine OWA will be used to test stolen credentials (and gather further info)
7. Credentials will be deployed in first on-site attack

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. Credentials obtained from spear phishing stored on laptop
6. Other team members on landline phones for remote verification

Branch office attack exercise (1)

- Harry arrives and tells receptionist he needs to fix a network fault
- Receptionist asks for a contact name for verification
- Harry claims not to know and gives receptionist his works order number and a phone number to get details
- Receptionist calls and speaks to George who gives the name of an IT employee (who we know is 'out of office')
- Receptionist cannot make contact with absent IT employee, so tells Harry to call their IT Manager to resolve the problem
- Harry calls Charlie and asks him to impersonate the IT Manager
- Charlie (impersonating the IT Manager) calls receptionist and tells them to give Harry access

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 in to 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
- Courier delivery of a parcel
- Research and interview for newspaper or publication
- 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 organisations.

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

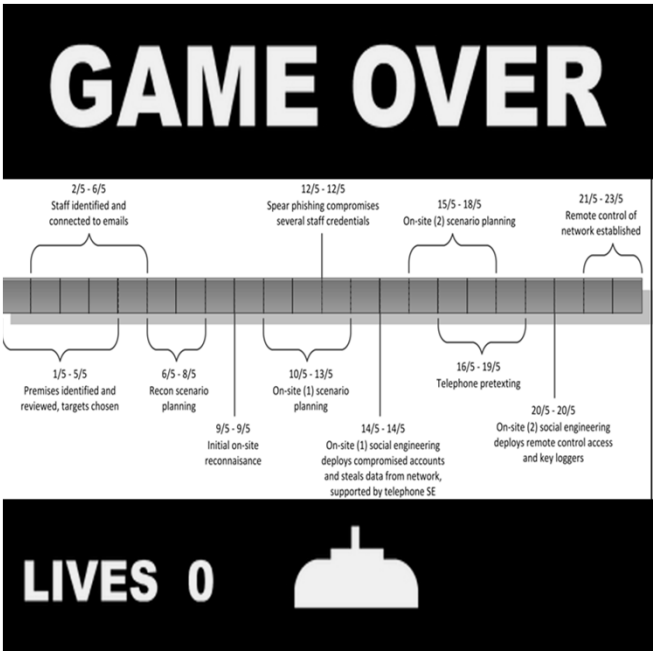
2. Interview for a charity magazine about corporate fund raising:

- "Anne" called the company and spoke to head of fund raising team
- 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 are answered satisfactorily
4. George returns from the bathroom, but quickly exits the meeting again leaving 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

Red Team Testing

- Use your threat analysis to pick a realistic attack scenario
- Use your asset register to identify realistic targets
- Engage a red team exercise to simulate a real attack
- Check your preventative and detective controls!
- Learn, improve, repeat!

Questions

Jonathan Armstrong
Cordery
jonathan.armstrong@corderycompliance.com
+44 (0)207 075 1784
www.twitter.com/armstrongjp

Mike Maddaughin
Cyber Security Operations Manager, FirstBase
mike.maddaughin@firstbase.co.uk
+44 (0)1273 / 64525
@mikemaddaughin