STRATEGY TALKS

infosecurity EUROPE

Steve Armstrong – Principal Incident Responder
and CyberCPR Architect

Building an IR Capability to Meet Modern Threats & Comply with GDPR

logically secure

CPR enterprise

Steve Armstrong – Principal Incident Responder and CyberCPR Architect

- In the Security field over 23 years
- Security Accreditor for Royal Air Force for 6 years
- Lead the RAF Penetration Testing teams for 3 years
- Incident Responder for last 7 years
- SANS Certified Instructor for almost 9 years

I will try to send you away with some understanding of how IR teams & GDPR are destined to be heavily entwined:

- Discover what types of data need to be protected
- Evaluate the protection that needs to be placed around incident related data and evidence that may contain private data
- Determine what forms of communication are suitable for investigations and what would be questionable under GDPR rules
- Identify what the key ‘gotchas’ are when managing personal data related incidents
- Understand how your organisation can integrate these new requirements into your existing procedures and practices.

As an Incident Responder do you view GDPR as a good or bad thing?

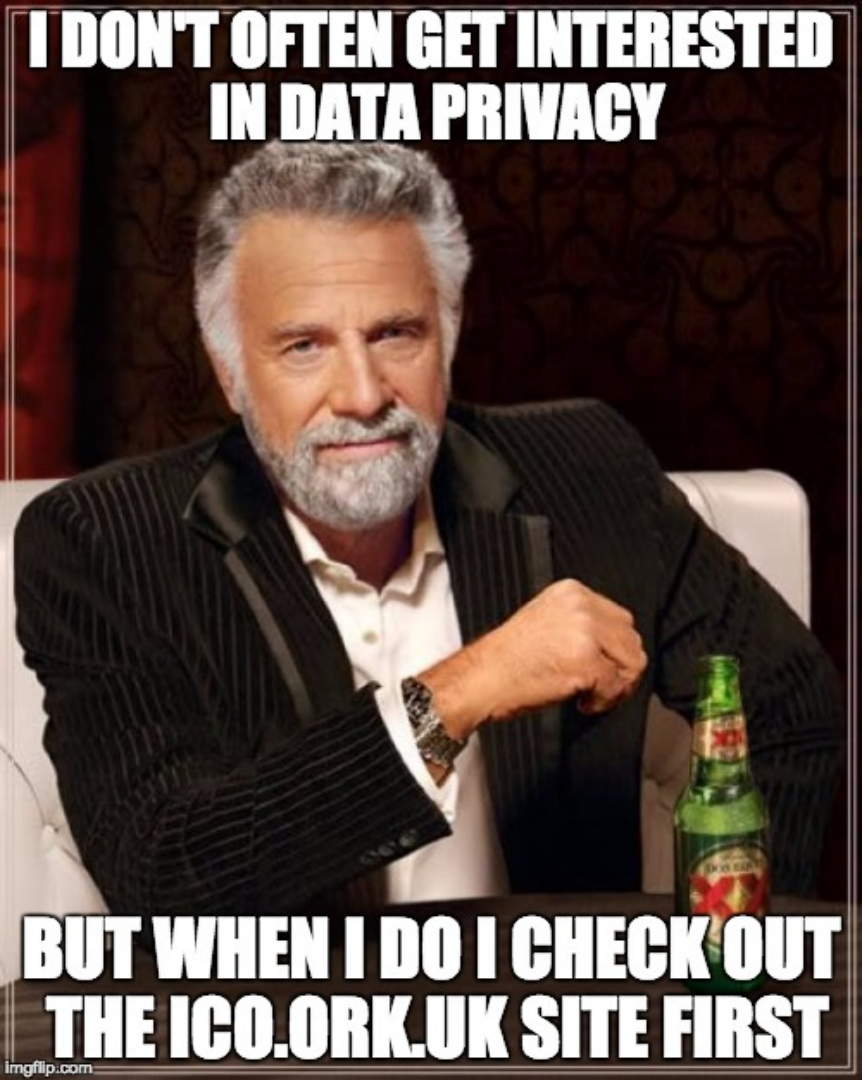
Now answer the question as a private citizen. Same answer?

As a responder and citizen I love both contexts! ☺

But as a business owner I am less pleased

Let’s get some admin out of the way;

every GDPR talk needs 2 things…..



352 Days

to become compliant with the EU GDPR (25th May 2018)

Building an IR Capability to Meet Modern Threats & Comply with GDPR

logically secure

CPR enterprise

Things I am always ask for as an Incident Responder:

- Where is the network diagram?
- Who knows the details of what keys servers do?
- Where are the logs from firewalls, web servers, Domain Controllers?
- Where are the logs from workstations?
- How can I get the network out-bound connection logs from proxies?
- Who is in charge and who knows what is going on?
  (Yes, sometimes I have to ask ☹)

How will this change post GDPR?

The main difference will be when I get to site the Regulatory damage will probably already have been done

- **GDPR Article 24** states: data controllers must implement "*appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation*". So if you suspect a breach you must have failed to have implemented enough controls.
- **GDPR Article 25** requires "Privacy by Design" has been baked into your network and system designs which will need to be demonstrable. So if you can't demonstrate your design was secure you will be in trouble.
- If you haven't reported the breach to the relevant authorities within 72 hours you may well on your way to fines.
- If you cite a lack of training or processes to quickly conduct data-subject notifications to data subjects, you will be failing to protect subject data rights.

Key issues facing organisations as they build an IR Capability*

*As seen by the presenter through his IR experience and exposure to students as he teaches around the world.

- Lack of visibility of log data, network activity and end points prevents many from proactively detecting any attackers activity.
- Lack of clear ***enforceable*** Incident Management policy that is both endorsed and actively supported by executive leadership.
- Lack of understanding of the impact losing systems/data/customers will have – not knowing what is important and what is not.
- No secure team/executive comms, workspaces or document exchange sites
- Malware making increasing use of HTTPS for Command and Control (C2)

What are these Modern Threats we are planning for?

- Historically, attackers focused on internet facing servers; today workstations and mobile devices are targeted heavily and then leveraged to pivot to other internal systems.
- Keystroke loggers, RAM scrapers and bots are widely deployed to extract sensitive valuable information.
- So, attackers are seeking the very personal data that GDPR seeks to protect.
- Modern malware is often Memory only Resident or “file-less” so RAM analysis is key to the investigation.

How do our Incidents looks now compared to years ago

- Mobile forensics has significantly matured and is sometimes the primary evidence source.
- RAM analysis has become mainstream and significantly matured. RAM holds large quantities of sensitive data including browsing history, passwords, emails and social or instant messaging data.
- Disks are considered by many to be too large to fully image so alternatives to this is remote live system forensics and file extraction.
- DNS logs, Web Proxy logs and Connection logs are often being forwarded to huge SIEM platforms and Logging Servers

Think about what your IR team are trying achieve….

Incident Response is all about trying to identify ***who*** did ***what***.

Thus, by maximizing the IR team's access logs and systems you increase the likelihood of detecting the attacker.

Therefore, almost every log of **interest** and value **must** contain vast volumes of personal data.

Learning Outcome 1:

Discover what types of data need to be protected

- Obvious:
  - Customer names, email addresses
  - PII, PHI, etc
  - Address, previous address, telephone numbers
- Less obvious or new additions to the list
  - Cookies as they can be identified as a online identifier
  - IP addresses are being treated in Germany as identifiable information [2]
  - Computer names where these include owners names e.g. **Armstrong's-MacPro**
  - Server with logs containing hostnames/IP addresses

Learning Outcome 2:

Evaluate the protection that needs to be placed around incident related data and evidence that may contain private data

- Having identified almost all logs are personal data.
- Data access controls are necessary on all evidence files.
- Need to know should be enforced and all access logged so data can be traced in the event a IR Team member is compromised.
- The Incident Team should not be on the main/corp network. This IR network should also be documented and the necessary ICO registration of this network is required; analysts are processing that personal log data!

Learning Outcome 3:

Determine what forms of communication are suitable for investigations and what would be questionable under GDPR

- In clear protocols are out! This includes Windows File shares (SMB v2).
- Strong encryption is a must for all communications where personal data maybe exchanged.
- Cloud systems will make this additionally difficult – seek clarification and confirmation from the cloud provider.
- Be careful of OOB cloud chat services that provide both history and file uploads while the client to server connections are encrypted the backups may not be thus evidence (personal data) may be stored

Learning Outcome 4:

Identify what the key ‘gotchas’ are when managing personal data related incidents

1. Not realising that **all incidents** are **actually personal data incidents**
2. Not encrypting evidence in transit and at rest to the necessary standard (TSL1.2 as a minimum as SSL and DES/3DES are no longer accepted).
3. Not checking where the 3rd party incident response teams are located and where the evidence (files, logs and malware) will be sent and how.
4. Not obtaining necessary confirmation from 3rd parties (check with legal before releasing data to Law Enforcement)on their compliance with GDPR.

Learning Outcome 5:

Understand how your organisation can integrate these new requirements into your procedures and practices

- Simply Follow the Data; For the next 5 years every new system you add to the network you should conduct a structured process to:
  - Identify what personal data it is arriving on the system from where and what is it used for and how is it protected (via encryption) in transit and at rest.
  - Identify what data processing is being conducted on the system.
  - Identify where that data goes to and how does it get there?
  - Confirm if the sender or recipient of the data are meeting GDPR requirements and coordinate how evidence of this can be obtained

So what about our IR team?

- Recognise the IR team are swimming in personal data.
- Review the ICO's guide on GDPR for the organisation and then conduct a separate analysis of the IR team's holdings.
- Get the IR team secure access to end-point log data, connection data and proxy data – especially HTTPS/TLS data.
- Establish a secure communications and an Incident coordination platform where the IR team and leadership can plan the incident remediation.
- Ensure IR, Legal and your Data Protection Officer work closely as they conduct Data Protection Impact Assessments (DPIAs) and correct the high risk areas.

Building an IR Capability to Meet Modern Threats & Comply with GDPR

Steve Armstrong
CyberCPR Architect

Any Questions please catch me after the session or at stand A145

References

Here are some handy references in relation to the topic

1. UK ICO Office site: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ (https://imgflip.com/i/1qd84d)

2. Analysis of the IP is an online identifier: http://eulawanalysis.blogspot.co.uk/2017/01/ip-addresses-as-personal-data-cjeus.html

3. TechCrunch article on Yahoo: https://techcrunch.com/2016/12/14/yahoo-discloses-hack-of-1-billion-accounts/