10 KEY STEPS TO BUILD A CYBER SECURITY STRATEGY FOR EU GDPR & PCI DSS

James Walker- MD & Principal Cyber Security Architect

Agenda

1. **Data Security First** - Why Perimeter Security is Dead
2. **Protection of Personal Data vs Payment Card Data** - What is the Difference?
3. **Building the Right Foundation-** Why a Good Cyber Security Strategy Starts with the Data
4. **Protecting “Critical" Data with Classification-** Extending Protection of Payment Card Data to Personal Data
5. **10 Prioritised Steps to Build a Cyber Security Strategy**
6. **Q&A**- (10 minutes)

Introductions

Speakers

James Walker

UK MD & Principle Cyber Security Architect, JAW Consulting UK

- Over 10 years' experience advising a clients with Cyber Security and Data Protection Strategies.
- Supported Multiple Clients on Data Security Programmes with Remediating Multi-TB's of Unstructured Data.
- Deployment of Data Classification, Data Loss Prevention and Information Rights Management (IRM) technologies

Data Security First. Why Perimeter Security Is Dead

The Data Challenge

"worldwide information volumes are growing at in excess of 60%"

"800% growth in unstructured data in next 5 years" (Gartner)

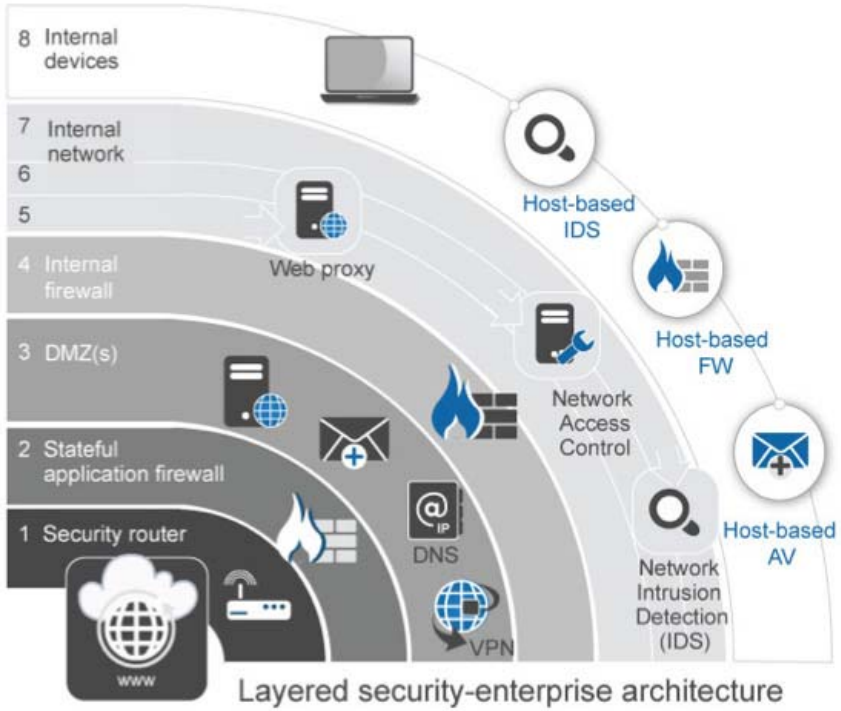
"the substantial growth of data is fast becoming unmanageable"

What data are we talking about?

What are the risks?

How do you know?

The Security Defense- Perimeter/Layered Approaches



The Insider Threat

Malicious Insider:

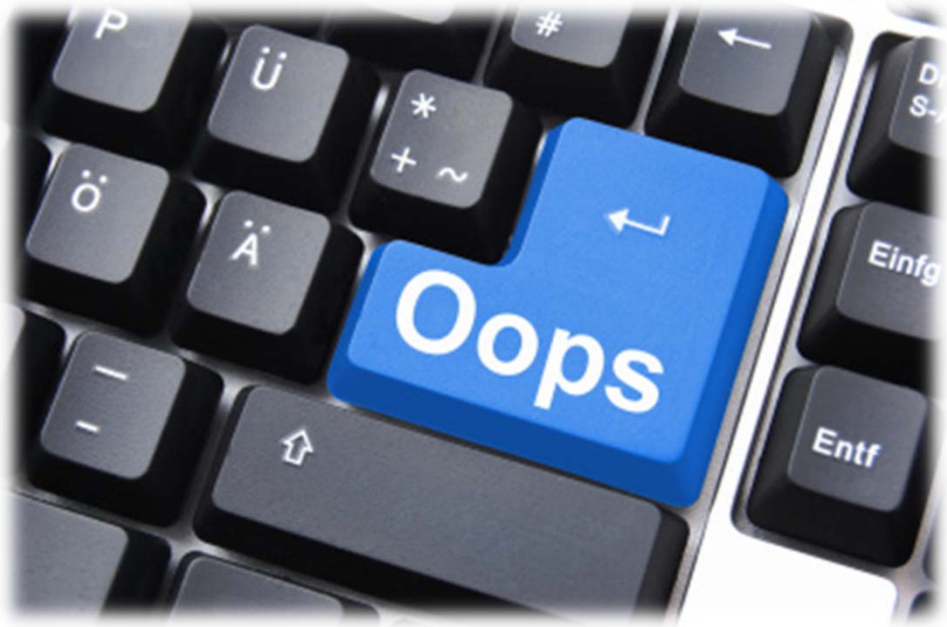
- Disgruntled former employee.
- Changing jobs and taking intellectual property.

Accidental Insider:

- Spear Phishing (Malicious Code/APT)
- Accidental disclosure online.
- Accidental loss of physical information assets.
- Improper or accidental disposal of information.

The crux of the problem. . .

…because we've all pressed this by mistake!!



Hard Truths around data loss

of data breaches were down to human error

The Ponemon Institute

of business users have sent an email to the wrong person by mistake

SilverSky

of business users said that the greater threat to businesses are employees unintentionally sending out sensitive information via email

SilverSky

said the CEO's confidential data had been breached within 12 months

Websense

Inadvertent misuse of data from insiders is responsible for **36%** of data breaches

Forrester

The ICO believe that over **50%** of data breaches are caused by human error

ICO

Increasing Regulation - EU GDPR

Increased Fines & Penalties

- Organisations face liability of 4% of global turnover or €100M, whichever is higher.

Extended Scope of Personal Data

- The definition of ‘Personal Data’ is expected to grow, bringing more enterprise data into scope.

Breach Disclosure & Reporting

- All organisations will be required to notify affected individuals within 72 hrs.

Right to be Forgotten

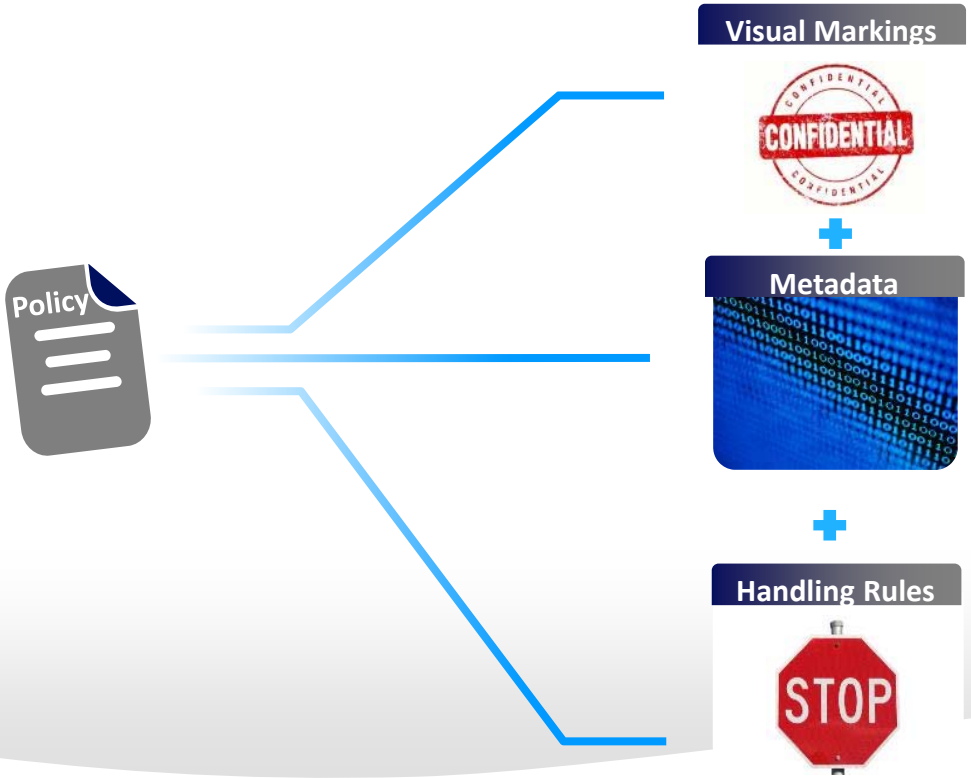
- If there is no legitimate grounds for retention, it must be deleted.

Protection of Card Holder Data Vs Personal Data. What is the Difference?

Critical Data is High Value

How Data Classification extends the concept of Payment Holder Data to Personal Data.

What Is Data Classification?



"Involving the user to place a **key identifier** onto a piece of information to ensure **appropriate handling**"

Types of Data to classify

Office Documents

E-Mail

Other Files

Establish the Right Foundations: Why a Good Cyber Security Strategy, starts with the Data.

Benefits of a Data Centric Cyber Security Strategy

1. **IMPROVE** data security awareness amongst employees
2. **ENFORCE** corporate security policy consistently.
3. **IDENTIFY** **Critical** Data, Applications and Infrastructure
4. **REDUCE COST** focus security budget protecting the critical data
5. **DEMONSTRATE** regulatory compliance & risk-based approach
6. **INCREASE** the effectiveness of DLP solutions & other tools
7. **ENCOURAGES** safer collaboration outside of boundaries

JAW. consultinguk

The 10 Prioritised Steps for Building a Cyber Security Strategy

Prioritised Steps for a Cyber Security Strategy- Step 1

1 **Identify** – your sensitive data

- Be aware of the types of data you are handling.
- Talk to the business- Understand the data types which are important to **them.**
- Be aware of the applicable regulations- PCI DSS, EU GDPR, SOX, DPA.

Prioritised Steps for a Cyber Security Strategy- Step 2

2

Classify– data according to its value to the organisation

- Define & agree data classification policy based on your data & privacy obligations.
- Implement a technical tool providing manual and/or automated classification of data.
- Assign data owners.

Prioritised Steps for a Cyber Security Strategy- Step 3

3 **Discover & Map The Data– identify the scope of the environment**

- What is the data flow within the organisation?
- Identify where the data is stored (File Shares, Databases, Cloud).
- Is your organisational data stored in another country? (Safe-Harbour now invalid!)
- Who has access to these systems?

Prioritised Steps for a Cyber Security Strategy- Step 4

4

Classify Applications & Infrastructure– according to the sensitivity of data it supports

- Which servers and data centre does this information reside?
- Who has access to these systems?
- Apply a classification rating to infrastructure components, supporting the critical applications.

Prioritised Steps for a Cyber Security Strategy- Step 5

5

Purge & Delete- Data that is no longer required

- Identifying data which has not been accessed.
- Use your judgement and remove data which is no longer required.
- This reduces the potential exposure, and assists with compliance with DPA and EU-GDPR.
- If you are breached, you will have to notify each customer. Maintain less, and the cost is reduced.

Prioritised Steps for a Cyber Security Strategy- Step 6

6

Secure – employ security control and protection measures

- Remediate weak ACL's on unstructured data shares.
- Implement strong encryption for critical data, tied to credentials.
- Use Information Rights Management (IRM) to secure data outside the organisation (Built into Office 365!).
- Implement role based access to data.

Prioritised Steps for a Cyber Security Strategy- Step 7

7

Security Awareness & Training – employees are your first, and last line of defence

Start with training in basic, but relevant security measures:

- Data classification raises awareness within organisations
- Handling of confidential information
- Anti-Virus software - on home machines
- How to create a strong passwords (no Post-it's!)

- Teach employees about spear-phishing, through creative means so they remember.

- Certify employees and vendors against your own internal measures.

Prioritised Steps for a Cyber Security Strategy- Step 8

8

Monitor – measure and evolve security practices
(Use Data Loss Prevention-like Technology)

- Determine metrics and processes for monitoring classification application and security tool performance, as well as how you will report and communicate the results.
- This is will evolve and adapt to changes that are required – process and infrastructure/solutions.
- Revalidate and improve security programme effectiveness.

Prioritised Steps for a Cyber Security Strategy- Step 9

9

Testing of Systems & Processes– Measure and evolve security practices

Security is a journey, not a destination- - Compliance is not static.

- Regularly test key defences, critical infrastructure and applications to find back doors.
- Review the operation of key security operational processes (e.g JML)
- Track & review security improvement initiatives, to ensure forward progress inline with the changing threat landscape.

Prioritised Steps for a Cyber Security Strategy- Step 10

10 **Establish & Practice Incident Response**

This should include:

- How affected individuals will be notified (within 72 hrs)
- How the incident should be reported, both to legal bodies and public

Have a system for figuring out what happened:

- How long that process takes.
- What customers, products or services were impacted, the extent to which it could have been avoided.
- How to manage continuing vulnerabilities.

Thank You.

Q&A (10 minutes)

Thank You

You can also find us here:

www.jawconsulting.co.uk

Contact us at:

james.walker@jawconsulting.co.uk