Enterprise Data Protection and the Principles of Least Access

Stuart McIrvine
CA Technologies

November 2018
Session FD

Agenda

1 **DATA AND REGULATIONS**

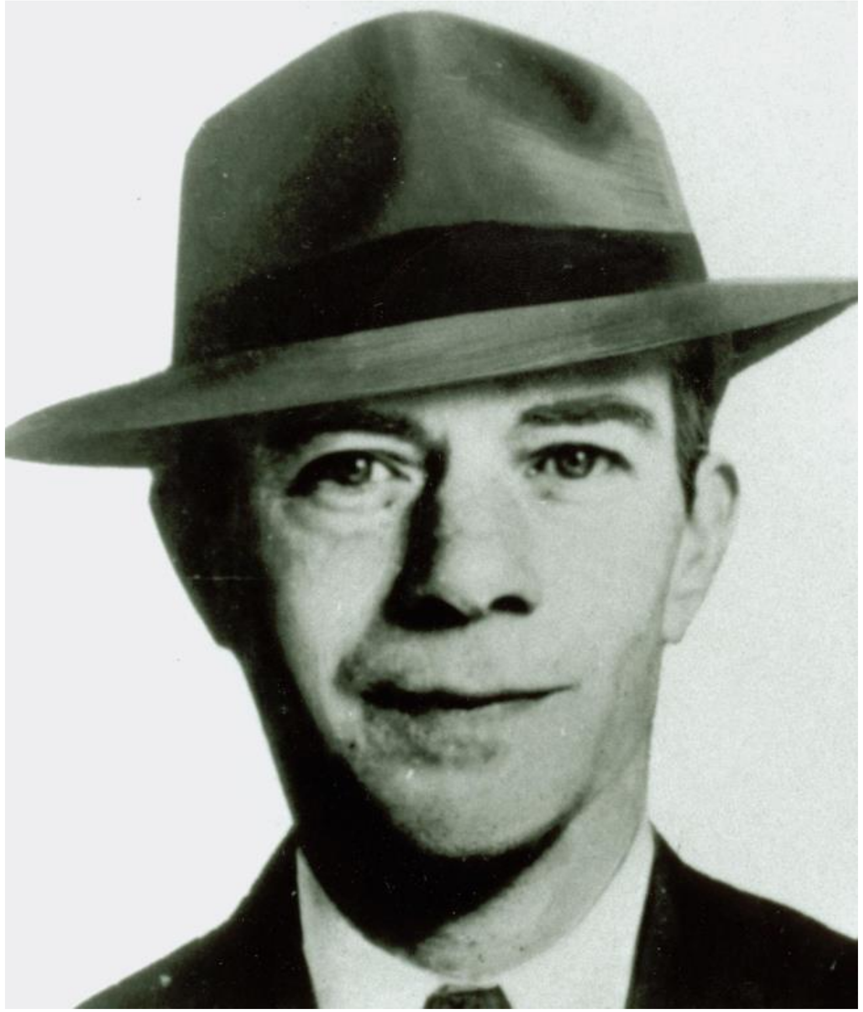
2 **THREATS & CHALLENGES**

3 **IMPROVING SECURITY & COMPLIANCE**

4 **BEST PRACTICES**

Data & Regulations

Who is this man?



Who is this man?

Willie Sutton

Born: June 1901, Died: Nov 1980

Bank Robber

Famous quote attributed to Willie?

Famous quote ….

Mitch Ohnstadn: “*Why do you rob banks?*”

Willie Sutton: “***Because that’s where the money is***”

Today’s robbers are much more sophisticated

If we asked the modern-day Willie Sutton:

“Why do you want to attack a Mainframe?”

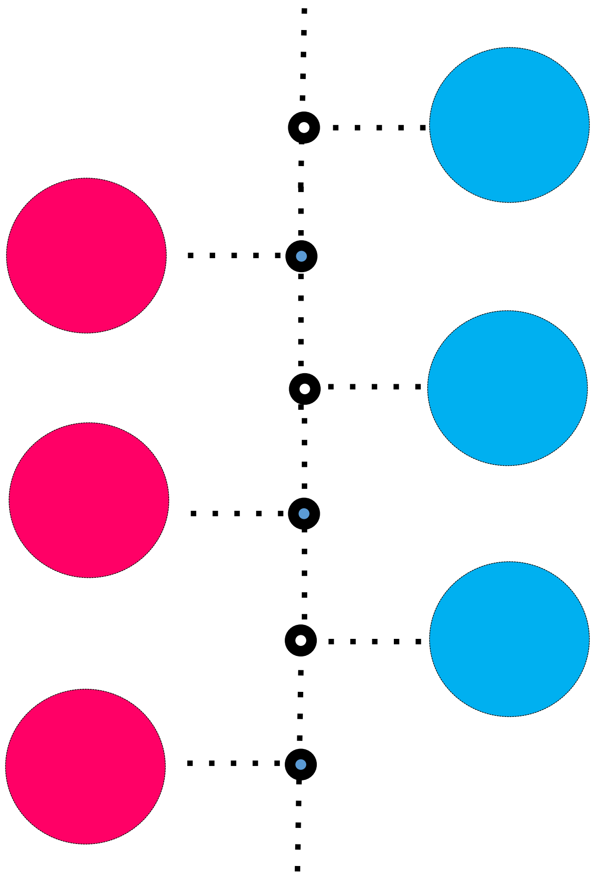
Today’s robbers are much more sophisticated

If we asked the modern-day Willie Sutton:

“Why do you want to attack a Mainframe?”

“Because that’s where the data is”

Data: an asset or a liability?



Asset

- Industries depend on data
- Data translates to business value
- More data is coming
  - 44 ZB of data
  - 6B phones
  - 50B devices

Liability

- Highly regulated
  - GDPR
    - Data Protection Act 2018 (UK, France, Italy, Spain, ……..)
    - BDSG (Germany)
  - PCI-DSS
  - Etc.
- PII is everywhere
- Data is the key to the future

The Data Security Challenge

GUIDE SHARE EUROPE UK REGION

High Cost

$11.5B

Ransomware damage costs in 2019[1]

Discovery Time

147

Days infiltrated before detection[3]

Data Breaches

53,000

Incidents in 2017[2]

2,216

Confirmed data breaches

Continuous Risk

49%

of those attacked were successfully attacked again within one year

Internal Threats

10,637

Incidents from privilege misuse

Skills Gap

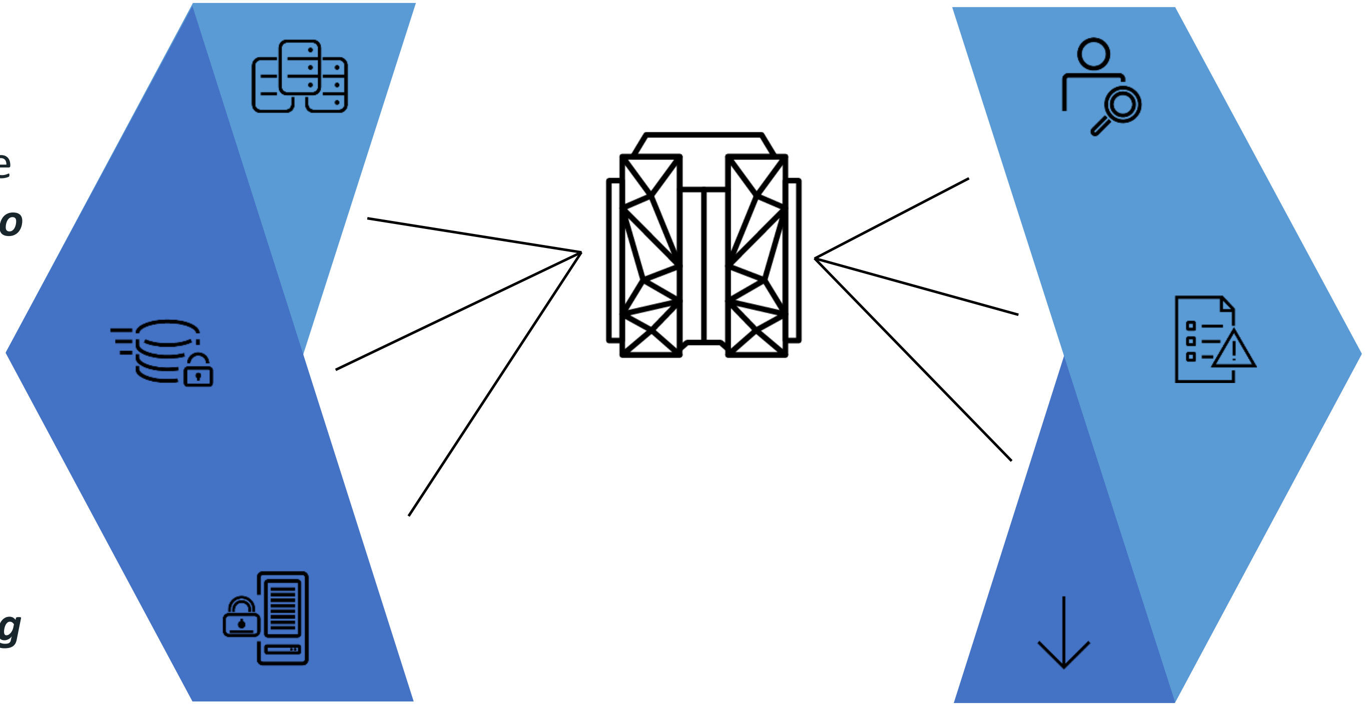
285,000

Cyber security roles went unfilled in the US last year

Challenges with Securing the Mainframe

Challenges:

- ❑ ***Copies*** of sensitive production data
- ❑ Files with possible sensitive data are accidentally ***sent to outside parties*** without validation
- ❑ Mainframe ***tenure***
- ❑ Large portions of PII data were collected and distributed with ***no tracking***
- ❑ Existing tools migrate data off the mainframe



Result:

- ❑ Enterprises are not prepared to comply
- ❑ Mainframe security confidence is low

Managing this risk on the Mainframe

Passing an Audit Requires Cross-Enterprise Security Controls & Forensics

People

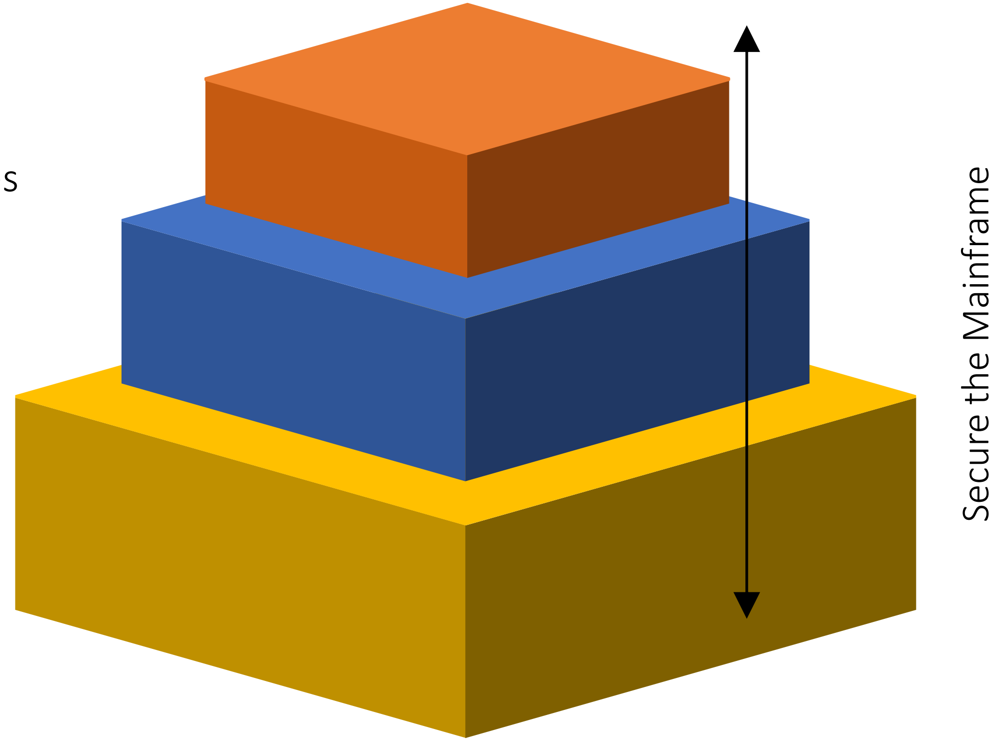
Insider threats range from malicious users to well-intentioned employees making a mistake.

Data

70% of today's corporate data – including sensitive and regulated data like PII – reside on the mainframe.

Systems

The mainframe is increasingly connected into the digital economy – applications, mobile devices, Big Data.



> *"Big iron is still very secure…unfortunately we have this thing called people that surround the mainframe."*
> *– Patrick Gray, Ex FBI Security Agent*

Protecting your data – where should you focus

DATA IDENTIFICATION

Discovery and Classification
Protect Data in motion and at rest
Data protection policies and rules

DATA ACCESS

Strong Authentication
Privileged Access Management
Principle of least privilege
Control access to test data

REPORTING

Demonstrate that you are in control

- Show list of users that can access sensitive data
- Show all privileged access requests and activity performed
- Identify breaches in real-time using comprehensive forensics

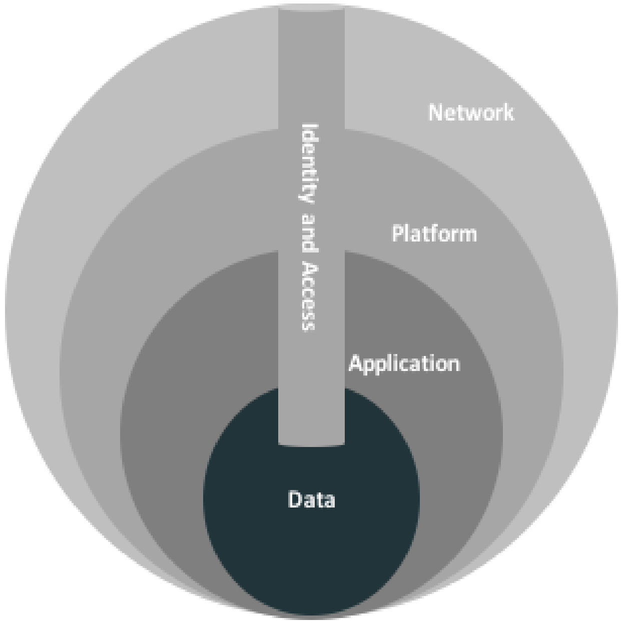
Improving Security & Compliance

Time has come to…

- Examine Mainframe Security from the bottom up – Start with the Data
- Switch from Traditional MF Security Strategy to Holistic Data-Centric Security

Start with the Data

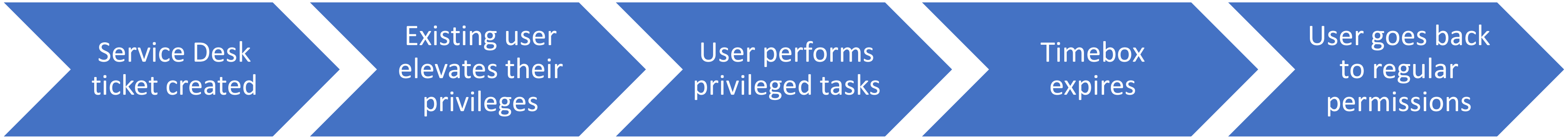
Understand What Data Is At Risk



Monitor Access To the Data

Limit Access

Reducing the Risk of Privileged Users



Service Desk ticket created

Existing user elevates their privileges

User performs privileged tasks

Timebox expires

User goes back to regular permissions

Ticket # used to validate elevation of privileges

Granular logging

Privileges last for predefined time

User can de-elevate their privileges or wait for timebox to expire

Best Practices

Best Practices

- Think with the end in mind – what is it that constitutes PII in your environment? Phone number? Doubt it! Therefore, don’t scan for it. Scan for the items that make sense to compound together and scan for things like SSN and Last Name.

- Don’t boil the ocean at the get go. Scan a small amount, review, tune and then continue to add to scans. High risk areas….

- Extract data from CRM. First name, last name, account number, etc. to create data dictionaries with exact matches to data in your environment.

- Run abbreviated scans followed by full scans as needed.

Best Practices

- Do a little spring cleaning!
- Save overhead; encrypt what makes sense
- Stay on top of new data added to environment
- Monitor data when losing mainframe security context
- Review who has access
- Review who’s been accessing
- Continuously monitor access of regulated/sensitive data

Solution for Mainframe Data-Centric Security

- **Find** sensitive data, that may be lost hidden or abandoned
- **Classify** discovered data based on sensitivity level for compliance
- **Protect** the enterprise and mitigate data breach risks
  - Advanced Auth
  - Privileged Access Management
  - Encryption

DATA-CENTRIC SECURITY
Data
1
id

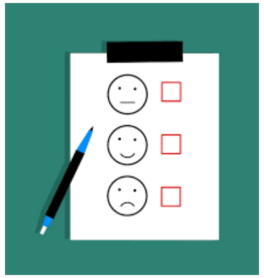
- **Alert** in real-time to violations of critical security systems and resources
- **Inspect** security issues deeper, with comprehensive reporting and forensics
- **Protect** to simplify regulatory compliance and mitigate negative security events

We want your feedback!

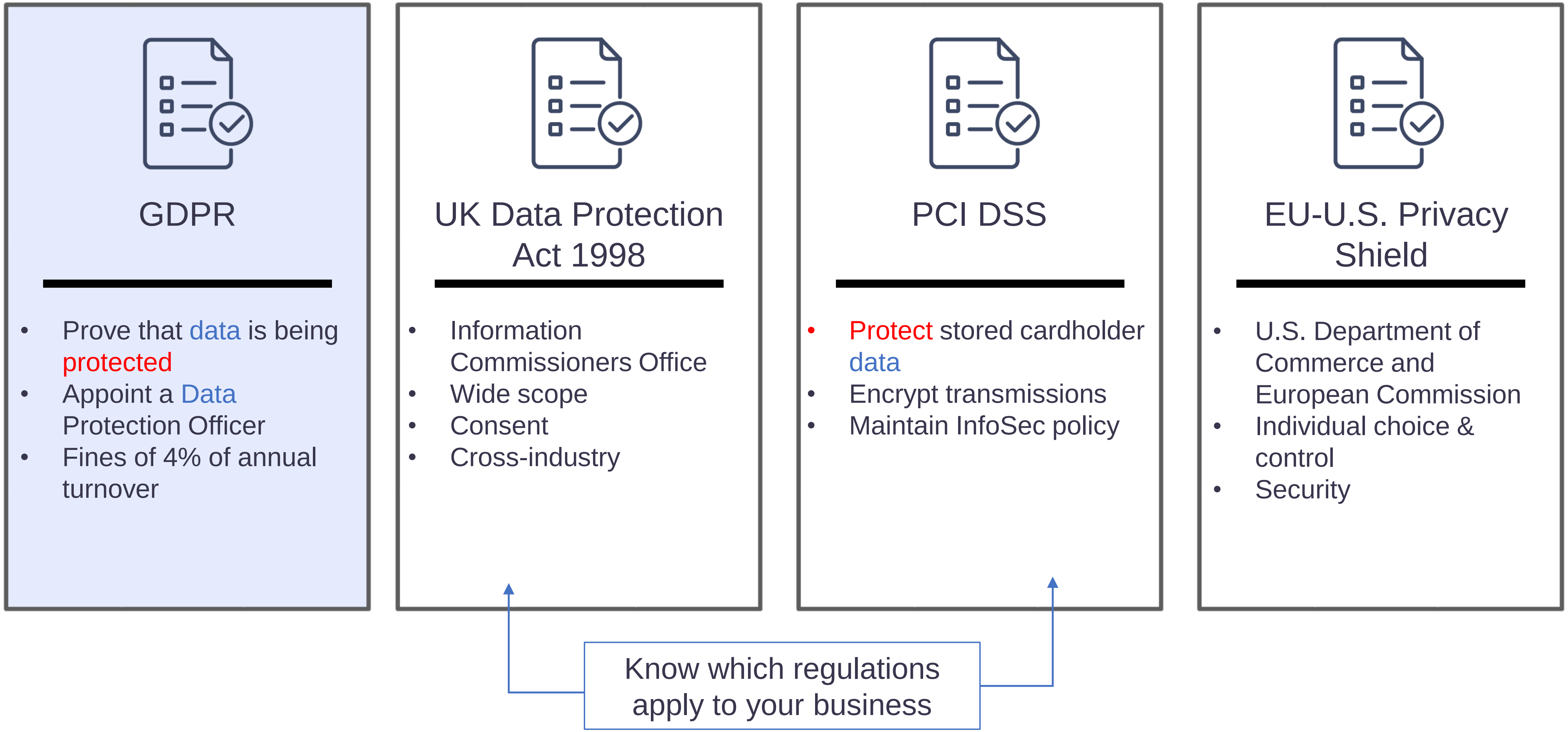
- Please submit your feedback online at ….
  - ➢http://conferences.gse.org.uk/2018/feedback/nn

- Paper feedback forms are also available from the Chair person

- This session is FD



The Regulatory Ecosystem



GDPR

- Prove that data is being protected
- Appoint a Data Protection Officer
- Fines of 4% of annual turnover

UK Data Protection Act 1998

- Information Commissioners Office
- Wide scope
- Consent
- Cross-industry

PCI DSS

- Protect stored cardholder data
- Encrypt transmissions
- Maintain InfoSec policy

EU-U.S. Privacy Shield

- U.S. Department of Commerce and European Commission
- Individual choice & control
- Security

Know which regulations apply to your business

Evaluate Your Regulatory Readiness

DATA ACCESS	Do you have systems in place to limit access on a need to know basis, ie. timebox the duration of privileged access? Do you have a strategy for designing “least access” controls? Can you manage your test data?
DATA IDENTIFICATION	Do you have complete visibility and control over your data? Can you automate discovery of sensitive data both at rest and in motion? Are you able to define risk-based data protection rules?
REPORTING	Can you audit all privileged access requests and activity performed? Can you identify data breaches in real-time using comprehensive forensics?

DATA CHALLENGES

- I have so much data, where do I start in classifying the data?
- What data should I pervasively encrypt?
- Who has access to my regulated data?
- Are all accesses to regulated data done with a business purpose?
- Where is my test data?

IDENTITY CHALLENGES

1

Who is my user? Are they who they say they are?

2

The privileged users on the system are *how seasoned*?

3

Risk and concern with shared Firecall IDs.

4

What are my users doing while on the system?

5

How will you know if hacker gets a hold of credentials?