IntaForensics

Forensic, Investigation and Support Services

IntaForensics Guarantee

Cost Effective

Agreed scope and fixed pricing
Transparent all-inclusive pricing
Efficient processes
Services focused on your needs
Large scale project discounts
Experienced with public sector contracting

Excellent Service Delivery

Flexible agreed timescales
Trained and security vetted logistics staff
Dedicated Case Manager for each case
Dedicated account management
Accurate billing and management information

Accessible & Responsive

24 hour Duty First Responder Service
Four secure UK laboratories
Leeds, Nuneaton, Stafford & Warrington
UK wide deployment within 4 hours
Client review facilities on-site

Best Practice and Quality

Processes – ISO 9001:2015
IT Security: Cyber Essentials Plus
IT Security – ISO/IEC 27001:2013
Forensic Labs: ISO 17025:2005
Forensic Science Regulator Code of Practice
ACPO Compliant

Experienced

Over 300 years combined experience
Criminal investigations experience
Payment Card Investigations experience
Civil Litigation experience
Qualified and certified staff

Secure & Discrete

All staff National Security Cleared
All staff NPPV-3 Law Enforcement Vetted
Annual DBS checks on all staff
Highly secure IT infrastructure
Commitment to information and data security

Qualified Security Assessor (QSA)

A Qualified Security Assessor (QSA) is an experienced Security Professional with a technical and auditing background, who has attained the PCI Qualified Security Assessor certification. A QSA's role is to assess rather than just audit. As part of a customer's PCI Compliance journey, the QSA reviews and samples the environment including:

- People
- Processes
- Systems and services

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

QSA Consultancy Service

Who is this service for?

Customers who already report on their PCI Compliance, through self-assessment or onsite assessment from a QSA company:

- Discussing changes to the environment and the impact this will have on compliance requirements;
- Reviewing payment channels and their transactional volumes to confirm the correct SAQs are being completed.

QSA On SIte Assessment Service

Who is this service for?

Merchants and Service Providers that are required by their Acquirer or Brand to complete an on-site assessment of their PCI DSS compliance.

Self Assessment Support

Who is this service for?

- Merchants or Service Providers that are able to self-assess their PCI compliance status.
- Existing Self-Assessment customers that need to review the Self-Assessment Questionnaire (SAQ) they are completing to confirm it is still correct for their environment.
- Customers who have taken over the assessment process from another party and need assurance that the self-assessment is correctly identified.

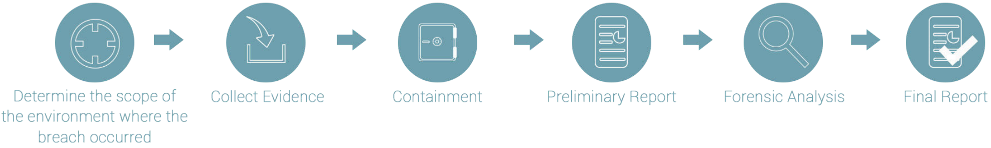
PCI Forensic Investigator (PFI)

Under the Payment Card Industry Data Security Standards (PCI DSS), merchants and payment service providers have a duty to maintain cardholder data securely. Failure to do so can result in significant fines if they are a victim of a data compromise or are found to be non-compliant with the PCI requirements. Organisations which hold cardholder data are also subject to the authority of the Information Commissioner's Office (ICO) which is able to impose substantial fines for breaches of the Data Protection Act (DPA).

PCI Security Standards Council®

PCI FORENSIC INVESTIGATOR™

Where such breaches have occurred, the merchant or entity suspected of being responsible and identified as the 'Common Point of Purchase' (CPP), will be instructed to undergo an immediate forensic investigation. They will be required to take steps to contain any breach, eliminate the risk of further cardholder data loss and progress to an audited state of PCI DSS compliance. The quicker any organisation responds to a suspected data breach, the potential for additional data loss is reduced and this can influence subsequent financial penalties and sanctions. It is therefore good business sense to engage a PFI company who has the resources and expertise to deploy instantly.


Determine the scope of the environment where the breach occurred → Collect Evidence → Containment → Preliminary Report → Forensic Analysis → Final Report

PCI Forensic Investigation

Who is this service for?

PFI Investigations are designed for merchants and service providers that have suffered a breach of cardholder data and have been instructed that they must undertake an investigation using an approved PFI Vendor. This includes customers who have been contacted by their acquiring bank and required to perform a 'PFI' investigation. All entities that meet one or more of the criteria below will require a PFI investigation:

- Merchant Level 1-3
- Are a Service Provider
- Have more than 3 electronic environments.*
- Transact more than 20,000 cards annually or more than 10,000 within the suspected compromise period
- Process transactions using a Virtual Terminal or EPDQ

PFI *Lite*

Who is this service for?

PFI *Lite* Investigations are a Visa Europe program for merchants that have suffered a breach of cardholder data and have been instructed that they must undertake an investigation using an approved PFI Vendor. This includes customers who have been contacted by their acquiring bank and required to perform a 'PFI *Lite*' investigation. Entities must meet all of the criteria below:

- Merchant level 4.
- Have no more than 3 electronic environments.*
- Transact less than 20,000 cards annually and no more than 10,000 Visa cards within the suspected compromise period.
- Do not process transactions using a Virtual Terminal or EPDQ.

Incident Response

“The difference between a good incident and a bad one is in how you respond, the expertise of your response and the ability to learn from experience”

Why do you need an Incident Response Service?

The current industry belief is that there are two types of businesses: those that have been hacked and those that don’t realise they have been hacked. This may sound a bit of a cliché but if you are the victim of a cyber-attack, what will you do? Do you have a documented, valid and proven incident response plan? You cannot afford to bury your head in the sand and hope that it will go away. A rapid, decisive and professional response could be the saviour of your business with the following benefits:

- Minimise/prevent data loss
- Reduce reputational/brand damage
- Limit financial penalties from Regulators
- Lessen operational downtime, loss of productivity
- Potential reduction in insurance premiums
- Known and agreed costs to assist in your budget planning

Incident Readiness Plan

£1,000 annual fee and then £200 per month fee. This would include:

- 2 Hour response window for telephone support
- Review or creation of Incident Response Plan for the organisation
- Agreed Terms of Engagement and mobilisation specific to your needs
- Advantageous rate per hour (£150) agreed in advance
- Next day onsite attendance guarantee

Cyber Preparedness Plan

£2,500 annual fee and £250 per month. This would include:

- 2 Hour response window for telephone support
- Review or creation of Incident Response Plan for the organisation
- Agreed Terms of Engagement and mobilisation specific to your needs
- Advantageous Rate per hour (typically £125) agreed in advance
- Cyber Essentials Basic Accreditation
- Cyber Essentials Plus Accreditation
- Next day Onsite attendance guarantee

Remote Emergency Response Team Plan

Variable Annual fee (between £5,000 and £15,000) depending upon technical deployment and £500 per month.

- 2 Hour response window for ‘remote hands on’ technical support
- Incident Response Server installed at client data centre allowing remote acquisition and investigation
- Review or creation of Incident Response Plan for the organisation
- Incident First Responder Training
- Agreed Terms of Engagement and mobilisation specific to your needs
- Advantageous rate per hour (£110)
- Cyber Essentials Basic Accreditation
- Cyber Essentials Plus Accreditation
- Same day Onsite if required
- Discounted Incident Response Training (25% discount on courses from IntaForensics)

Emergency Response Team Plan

£2,500 annual fee and £500 per month. This would include:

- 2 Hour response window for telephone support
- Review or creation of Incident Response Plan for the organisation
- Incident First Responder Training
- Agreed Terms of Engagement and mobilisation specific to your needs
- Advantageous rate per hour (£125)
- Cyber Essentials Basic Accreditation
- Cyber Essentials Plus Accreditation
- Same day Onsite if required
- Discounted Incident Response Training (25% discount on courses from IntaForensics)

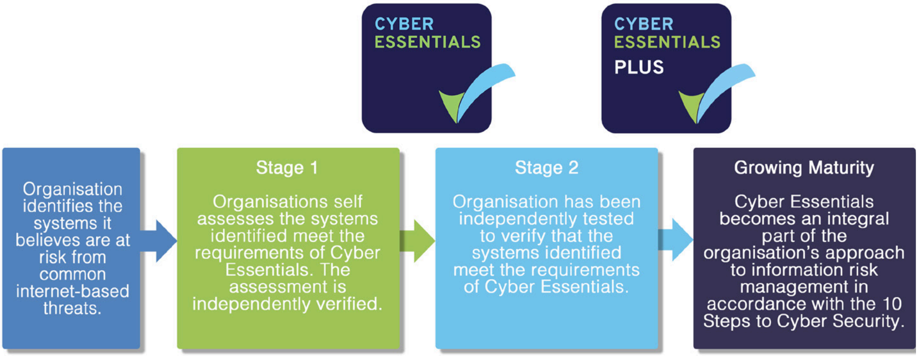
Cyber Essentials

What is the Cyber Essentials Scheme?

Cyber Essentials is a Government-backed, industry supported foundation for basic cyber security hygiene. The Scheme has been carefully designed to guide organisations of any size in protecting themselves against cyber threats.

Why do I need Cyber Essentials?

Cyber Essentials is now mandatory for all central government contracts advertised after 1 October 2014 which involve handling personal information and providing certain ICT products and services. Even if you are not a government supplier, you should still seriously consider embarking on the Cyber Essentials pathway to ensure that your business has implemented basic cyber security controls and by doing so, you have mitigated against common types of cyber attack such as phishing and hacking. With the average cost of a breach to a large business equating to £36,500, can you afford not to be safe?



Organisation identifies the systems it believes are at risk from common internet-based threats.

Stage 1

Organisations self assesses the systems identified meet the requirements of Cyber Essentials. The assessment is independently verified.

Stage 2

Organisation has been independently tested to verify that the systems identified meet the requirements of Cyber Essentials.

Growing Maturity

Cyber Essentials becomes an integral part of the organisation's approach to information risk management in accordance with the 10 Steps to Cyber Security.

Cyber Essentials

Cyber Essentials is an independently verified self-assessment. You complete an online assessment questionnaire which is approved by a Senior Executive. Upon submission, IntaForensics will independent review and verify your responses and if successful, we will award you the requisite certificate(s) and badge(s) that you can display on your company website.

Cyber Essentials Plus

This is the next stage of your security journey and involves both independent internal and external tests of your network and computers. Successful accreditation against Cyber Essential Plus provides a higher level of assurance that your organisation has a strong cyber security regime with correctly implemented controls thereby maintaining a robust defence against Internet-based attacks.

About IntaForensics

About Us

Established in 2006, IntaForensics has grown to become one of the leading providers of digital forensic services and IT Security in the UK. Our team has been built carefully and consistently through recruitment of the most technically competent and experienced cyber security and PFI experts from law enforcement, government agencies and the commercial world.

We operate from four secure laboratories across the UK – in Leeds, Stafford, Warrington and Nuneaton – operating a highly regulated and quality assured service consistently in all cases. Combined with having one of the largest forensic and cyber security teams in the UK this means that we are able to assist clients quickly, efficiently and cost effectively. We operate a unique 24 hour, 7 days a week Emergency service to enable clients to deal with emergency situations.

Professional Services

In response to the increasing growth of data breach incidents resulting in the compromise of payment card data, IntaForensics established a PCI accredited QSA PFI response within their Professional Services Business Unit. Operating from IntaForensics Advanced Digital Forensics facility in Stafford, UK, the PCI Team service the significant market needs of clients across the UK and Europe using existing and new specialist talent for this fast-growing area of business.

In addition to the provision of bespoke payment card investigation and compliance services, IntaForensics have been awarded the IASME (Information Assurance for Small and Medium Enterprises) audited Gold Standard and have achieved Cyber Essentials Plus certification. IntaForensics are also one of the most active Certification Bodies, trained, licensed and approved to assess against the IASME Standard and the Government's Cyber Essentials Scheme (https://www.iasme.co.uk/cyber-essentials-scheme).

PCI Security Standards Council®
PCI FORENSIC INVESTIGATOR™

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

IASME Consortium®
GOLD Certified Company

ISOQAR REGISTERED UKAS MANAGEMENT SYSTEMS 0026
ISO 9001:2015

ISOQAR REGISTERED UKAS MANAGEMENT SYSTEMS 0026
ISO/IEC 27001:2013

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

UKAS TESTING 7733
Accredited to ISO/IEC 17025:2005

intaforensics.com/cyber-security

cybersecurity@intaforensics.com

+44 (0)2477 717 780