Experian's Data Centres

Briefing for clients on Experian Business Continuity controls

CONTENTS

1. INTRODUCTION

Experian's data centre for it's European operations is located in Nottingham. The data centre operation is made up of two sites, one primary site at Fairham House in a business park on the outskirts of Nottingham and the second as a Disaster Recovery centre to 10 miles apart.

These centres currently host in excess of 5,000 Servers of which 3,500 are virtual. In total over 3.0 Petabytes of disk storage exists and over 28pb of tape storage. Experian provides data services to over 30,000 UK customers and supports the UK, Danish, Norwegian, Italian, Indian and Irish consumer and business credit bureau systems. It also hosts back office systems for over 42 countries.

The European Union Data Protection Regulation treats all EU countries on a common footing and ensures that standards are applied equally across member states. Based on this capability, the UK data centre has become a primary data centre for EU operations with much of the national processing of EU countries being transferred back to Fairham.

Experian policies dictate that all data within the company is treated as a highly secure business asset and that all client facing systems are assessed for their disaster recovery requirements. Experian data centres have been built in combination to meet these requirements and provide a secure hosting and management service for all client facing systems.

This document describes the benefits of using the Nottingham data centre complex and the facilities that are provided within it.

2. BENEFITS AT A GLANCE

2.1 Primary data centre

- Purpose built DC 8,000 square metres
- Computer Room space of 2,800 square metres
- Multiple power supplies providing capacity up to 4MVA with full UPS and generator backup
- Multiple chillers providing full site cooling capacity to meet electrical feed
- VESDA fire monitoring and two stage fire suppression system
- Environment monitored 24/7 with on site engineers
- High density areas to support blade enclosures and high power demand equipment

2.2 Secondary data centre

- Built for purpose 1,200 square metres
- 2MVA electrical supply backed by resilient UPS and generators
- Independent multiple chillers per computer room
- VESDA fire monitoring with Nitrogen gas suppression system
- Environment monitored 24/7 with on site security

2.3 Technical operations

- 24/7 on site operational monitoring
- 24/7 customer help desk for technical issues
- Over 250 technical specialists available on call to resolve incidents
- Media Centre processing over 150,000 file transfers per month with full service tracking system and secure encryption/ decryption services

2.4 Technical facilities

- Multiple resilient carrier services to site
- Full cross site network services using dark fibre with 1000Gbps capability
- Multiple supplier Internet pipe feeds with load balancing between sites
- Multiple carrier client network connection offerings including fully managed resilient services
- Over 5,000 servers 3 mainframes 28 petabytes of storage 3 petabytes of disk storage
- All critical data automatically backed up to remote site without requirement for tape handling

2.5 Security facilities

- 24/7 on site monitored access to building with 84 security cameras
- Multiple layers of physical security to data centres
- Full anti-virus protection for all managed servers
- Three layers of independent firewalls with full monitored intrusion detection and protection
- Services, ability to provide network based encryption using either server certificate or PKI based services
- No video units are installed in racks and only KVM access to devices is available from roll round screens.

3 FAIRHAM HOUSE – OUR PRIMARY DATA CENTRE

3.1 Physical construction

Fairham House is built on the edge of a business park with a country park to the rear. The building was purpose built as a data centre and is a concrete construction covering 8,000 sq metres with the data centre areas providing 2,800 sq metres

The data centre itself is split into three separate rooms which are functionally independent allowing the site to operate a data centre within a data centre concept. This enables systems to be planned with resilience between rooms so that high availability can be guaranteed by spreading systems across rooms.

Outside of the data centre there are three main areas:

- Operations Centre acting as a central monitoring point for all UK and other EU services supported from by the UK team. This area also has a client presentation suite which can be used for client presentations (see below).

- Staff offices providing accommodation for all technical and operational staff necessary to maintain the technical services within the site.

- Staff facilities including restaurant and rest areas as the site is manned 24 hours a day.

3.2 Site security

The site has three physical boundaries:

- Access perimeter made up of physical fences to the side and rear with pressure pads and red wall technology. To the front the site is guarded by a marsh bed with road access protected by “tank trap” ramps. Access through this perimeter can only be obtained by approval of the dedicated on site security team releasing either road ramps or staff gates.
- Building perimeter made up of an outer concrete skin to the building. There is then a zone of protection between the external building skin and the data centre areas. Data Centre zone made up of a secondary deep concrete wall construction surrounding the actual machine and plant rooms.
- There is physical manned security on site 24/7 with high density of CCTV coverage for every area of the building. Any access through external or key internal doors is made using staff security passes which trigger the card holder details to be displayed on a screen to security so that this can be verified to the actual entrant.

3.3 Electrical supply

Fairham House is supplied from two electrical substations with diverse routing of electrical feeds to the site. The primary bearers are 4MVA each with a third bearer for back up of 1MVA.

Within the site there is protection by two main Uninterruptable Power Supplies (UPS) covering data centre, operations bridge and office areas. Each area is separately supplied. Each computer room is independently supplied to 4 power distribution units (PDU) which are cross linked to each UPS enabling full continuity of supply unless manually shut down. Each rack or device in the site can be provided by two feeds from alternate PDU. In the event of failure of the two grid access points, the site is fully supported by 4 generators capable of maintaining the site indefinitely.These can be refuelled in flight but fuel is retained on site for 5 days of operation before this is required. Full load test every quarter and individual test every week

All electrical supply services are monitored by a control system, with 24x7 on site coverage of maintenance engineers.

3.4 Fire suppression

Fairham maintains the highest installation standards with all cables provided using Low Smoke/Zero Halogen cabling and the removal of all combustible materials from the machine rooms.

All computer rooms and office areas are monitored by Very Early Smoke Detection Apparatus (VESDA) units. Each machine room can be shut down independently in the event of a fire.

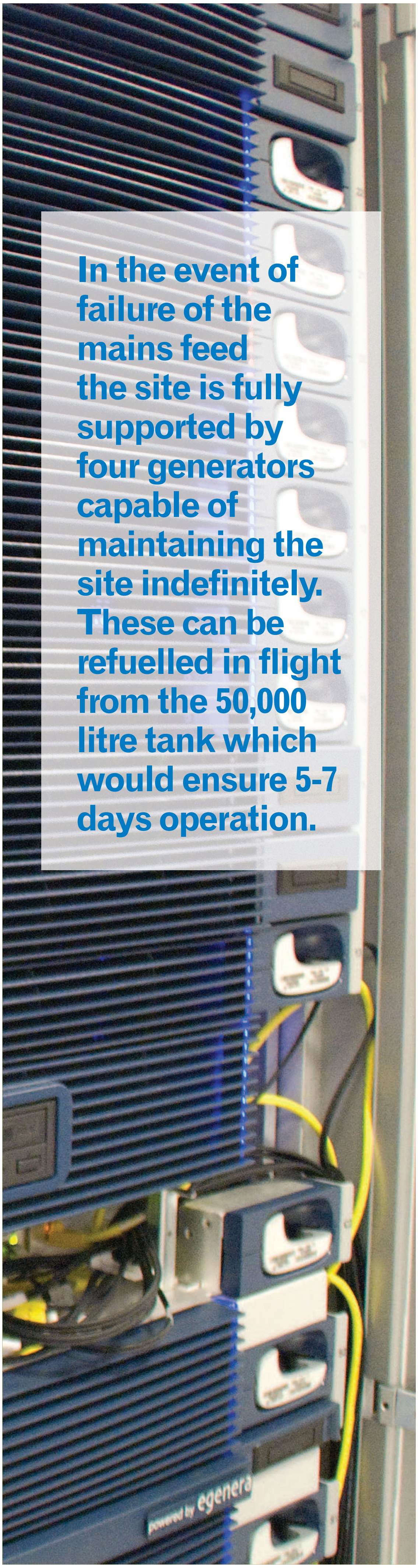
The complete site is covered by a two stage water fire control system which primes on the VESDA alarm but only discharges based on exceeding room temperature threshold.

3.5 Cooling

Cooling for the site is provided through 4 main cold water chiller units fed by two main cooling towers. Water supply is made under floor through the corridor areas with no flowing water to the computer room areas. Cold air down flow units (DFU) within the computer rooms are linked to the chilled water system to provide continual cooling. The DFU can be scaled to increase cold air supply in specific zones to meet high capacity equipment needs as computer density increases.

The complete site environment is monitored via a Building Management System which is linked to the Operations Centre and Security station.

A Modular evaporative free air cooling system is also in place to cool the main computer halls.This is achieved by using 12 Eco-cool modules that inject outside air via filters at 18C to supplement the other cooling system.This system has been instrumental in reducing the cooling costs of the Data Centre



In the event of failure of the mains feed the site is fully supported by four generators capable of maintaining the site indefinitely. These can be refuelled in flight from the 50,000 litre tank which would ensure 5-7 days operation.

4 BULWELL DATA CENTRE – OUR DISASTER RECOVERY CENTRE

4.1 Physical construction

Bulwell Data Centre is a purpose built Tier II facility comprising two separate data halls of 600 sq. meters each. The data centre also contains a small DR bridge which can be used to manage the full estate in the event of Fairham becoming inaccessible.

4.2 Site security

The site is occupied 24 hours a day by site security although the computer suite is operated as a dark site. Access to the computer rooms is independently secured and monitored for access.

4.3 Electrical supply

Bulwell Data Centre has a single power feed, within the site there is protection by a 2MVA modular Uninterruptable Power Supply system covering data centre and Operations Bridge. Each computer room is supplied through two separate PDU and each rack supplied from each PDU.

In the event of failure of the mains feed the site is fully supported by three generator capable of maintaining the site indefinitely. These can be refuelled in flight but fuel is retained on site for 5 days of operation before this is required.

4.4 Fire suppression

Fire suppression for Bulwell Data Centre is provided through a Nitrogen gas flood system. The system is monitored by VESDA units and released automatically.

4.5 Cooling

Cooling for the site is provided through 6 main cold water chiller units with N+1 redundancy.
Cold air down flow units (DFU) within the computer rooms are linked to the chilled water system to provide continual cooling. The DFU can be scaled to increase cold air supply in specific zones to meet high capacity

5 NETWORK SERVICES

5.1 Carriers

Fairham and Bulwell are connected together by a dark fibre network with diverse routes across Nottingham. This provides high speed, high capacity, low latency, and highly available 40 gig diverse cross site connectivity. To which further capacity can be added, and is constantly monitored. This service is provided by Virgin Media.

Both Bulwell and Fairham also have main carrier services from:

BT
Virgin Media (NTL)
AT&T
Vodafone

5.2 Diversity

Internet access bandwidth is provided by both Virgin Media & Level 3 through geographically diverse exchanges, and resilient connections.

Experian's Nottingham sites are connected, for internal services, to other Experian global data centres in Texas, Hong Kong and Sydney by a Global Backbone Network (GBN) provided using a secure global WAN solution from AT&T. Connectivity into AT&T is to both Nottingham data centres, and uses diverse exchanges.

Experian client network connectivity is provided using encrypted Multiprotocol Label Switching (an MPLS service known as GMNS within Experian) from C&W, and corporate office connectivity is provisioned using Dynamic Multipoint Virtual Private Network (DMVPN) technology. Both services are provided in a resilient and secure manner from both Nottingham data centres.

Both Bulwell and Fairham have two routes of entry so that telecom carrier services can be brought into each building from diverse exchanges. In addition, the use of both sites along with the cross site bandwidth provides an ability for both sites to act as one routed network providing continuous availability.

5.3 Client connections

As indicated above, clients can be connected to Experian using high capacity MPLS services described as the Global Managed Network Service (GMNS) to anywhere in the world. This allows Experian to route clients into either data centre so that in the event of a telecom failure at either site, traffic can still reach target systems. This network service can be provided with diversity at client sites as well including to diverse client data centres.

Alternatively, many clients now access systems using the Internet over either Virtual Private Networks (VPN), our Client Secure version of DMVPN, or other secure methods of connectivity. High bandwidth Internet connections to both sites ensure that these deliveries are consistent and resilient.

Some clients still prefer to provide their own bandwidth to Experian sites. The range of carriers within the data centres ensures that adequate services can be obtained from the major national carriers if this is required.

A formal security management organisation structure exists, with clear levels of responsibility to support security management and operations of physical and logical support.

6 DATA SECURITY

The importance of appropriately securing information has always been a core Experian value, providing the building blocks to ensure that assets are protected in line with Company and Client expectations. To accommodate this approach, Experian deploy a comprehensive Global Information Security Policy (GISP) encompassing all aspects of security. Such policy statements apply to all forms of information, and cover data stored on computer, in electronic format, communicated via e-mail, information or committed to paper, and including the spoken word.

A formal security management organisation structure exists, with clear levels of responsibility to support security management and operations of physical and logical support.

6.1 Security policy

As noted above, Experian deploy a comprehensive Global Information Security Policy (GISP) encompassing all aspects of security. In order to ensure that users are aware of such Policy and Security requirements, Experian Information Security Department underpin this expectation with a solid Security Awareness Programme.

Information Security controls have been deployed to meet legislative, regulatory, and contractual obligations. Such controls provide the means by which the requirements for confidentiality, integrity, availability, and accountability are maintained.

The GISP for Information Security defines the minimum mandatory standards, controls and procedures, which must be implemented in order to protect both Experian and Client information, with an approach based on 'Industry Best Practice', and the ISO27001 Security Standards.

- The deployed GISP encompasses: Confidentiality and integrity of Experian and Client information, its accuracy and completeness;
- Availability of the information and information systems to meet business requirements;
- Accountability of actions taken against information and that all actions can be justified;
- Regulatory, legislative and contractual requirements are fulfilled;
- Continued operation of the Business or its timely and effective recovery in the event of a disaster;
- Full understanding of all staff as to their responsibilities under the policy (awareness);
- Prompt and appropriate reporting of all information security breaches – either actual, inferred, or suspected;
- Requirements of the ISO27001 Security Standards;
- Application of appropriate standards for handling proprietary information - both Experian information and Experian managed (client) information;
- Realisation of the benefits of implementing appropriate risk assessment and management techniques.

6.2 Security policy compliance

Experian deploy a comprehensive process to ensure that compliance with the GISP is formally monitored on an ongoing basis through a combination of self-assessment reports and independent compliance reviews performed by Experian's Governance Teams.

6.3 Media services

Experian provides a secure file transfer management service for all of its customers. As our reputation is based on the security and the value of the data and information assets we own, we place particular care over managing client data.

The media services team handle 150,000 data transmissions per month and has eliminated the dispatch of physical media.

Experian provides a full encrypted process for electronic movement of data in and out of the data centre.

6.4 Logical security

The Experian network has been developed to industrial standards and contains a range of logical protection facilities:

- The network itself is fully protected by Intrusion Detection/Prevention systems which are monitored both internally and by third party specialists.
- The network is protected by two independent firewall layers of different manufacturer equipment to ensure that any inappropriate weaknesses in one manufacturer are defended by another.
- All mail and web traffic is monitored using mail and web scanning software both for content and use. All production mail services pass through separate gateways to the internal mail to ensure that these traffic flows cannot impact each other.
- Anti-virus scanning is performed both on inbound and outbound traffic flows. All servers (and desktops) are provided with automatically updated anti-virus engines and signature files to maintain their protection.
- Specific applications are protected by Verisign web certificates to provide system to client security of encryption.
- The core information systems from the UK are further protected by an Experian owned Public Key Infrastructure (PKI) which allows Experian to not only validate clients but end user devices as well.
- All client traffic is independently routed through to target systems using dedicated Virtual Networks (VLANs) ensuring that one client can never see another clients data.

The media services team process 150,000 electronic, encrypted data trans per month

7 OPERATIONAL SERVICES

7.1 Customer Interface

All calls received at the centre, which is covered 24 hours a day, are recorded on a central incident and problem management system and are tracked using industry standard best practices through to closure in line with agreed service levels.

7.2 Operations

The data centre operations team also operates 24 hours a day, 365 days per year. This team provides first line diagnosis and resolution of the majority of technical faults. The majority of technical issues are picked up through our own monitoring systems and resolved before any client impact is identified.

Operations also manages the full range of our technical supplier base ensuring that engineers are called in as soon as they are required to resolve either hardware or software issues.

7.3 Technical Specialists

Providing back up to the Operations team are over 250 professional service technicians with detailed knowledge in all strategic platforms ranging from mainframe through midrange, storage, networks and most major utility software services.

The technical specialists provide on-call coverage for out of hours incidents which cannot be managed by the operations teams. This cover is provided by remote access so that it is very rare that these engineers would be required to attend site to resolve an incident.

Some platforms are now being supported using Experian's global capabilities with UK and US teams providing remote specialist supports in key operating systems and platforms.

7.4 Project Management

Technology Services can provide full technical design consultancy and project management for implementation and changes required within the data centres. All project managers are PRINCE 2 accredited, most at Practitioner level. The technical consultants are also trained in line with the relevant British Computer Society consultancy standard as well as having an in depth knowledge of all technical products approved within the Experian technical strategy and the security requirements established in Experian global policies and procedures.

Customer reviews and further questions

This briefing is for general information only and is not intended to be legally binding. Experian offers Business Continuity as part of its many services; for further information please speak to your account manager.

Registered office address:
The Sir John Peace Building
Experian Way
NG2 Business Park
Nottingham
NG80 1ZZ
United Kingdom
www.experian.co.uk

Experian Ltd is authorised and regulated by the Financial Conduct Authority. Experian Ltd is registered in England and Wales under company registration number 653331.