Cyber Security Controls - Experian

Security measures Experian put in place to protect client data

Security sits at the core of Experian's operations. The vast majority of modern organisations face a significant number of risks relating to loss of information and due to the nature of our business, Experian is no different.

Experian takes cyber security attacks very seriously and in order to protect our data from such risks, Experian has developed a best of breed security framework based around ISO27001; the cornerstone of which is our information security policy. Experian also holds Cyber Essentials Certification and performs risk assessments against our critical and external facing applications annually.

Experian's customer access network is divided into 3 physically segregated layers. Customer access connections are attached to the access layer of the network. Virtual application services are installed in the content switching layer of the network and actual application servers and backend services are installed in the final application / service tier of the network architecture.

Each tier of the network is separated with a layer of firewall appliance from different vendors and is actively monitored by IDS and IPS systems. Firewalls are configured to only allow the network traffic required to conduct business. Routing controls are in place to segregate traffic and disallow unlimited network roaming.

Each network layer is provided by carrier grade switches installed to provide the physical connectivity. The switches provide physical inter layer connectivity and provide I/O ports for client and server connectivity. All layers have dual redundant switch fabric modules and 3 power supply units to provide N+1 power redundancy.

• Vulnerability Management

In line with our Global Information Security Policy, Experian performs regular vulnerability and integrity checks of our systems. The scheduling varies depending on criticality and exposure of the system being checked.

Experian has regular network security assessments conducted of both internal and external deployments, in which the Firewall Infrastructure is tested, including internal components, applications, and deployed servers.

Penetration tests are continually taking place, as a minimum mandatory penetration testing is performed as part of our PCI compliance remit. The output from these are annually reviewed by our external auditors who have not determined any issues that prevent re-certification.

Experian requires that every project undertakes a formal documented risk analysis and based on the security risk assessment, the project team, with assistance from the Global Security Office, identifies the security requirements and security-related functional requirements of the proposed service prior to beginning the development phase. This risk assessment includes an assessment of the information being served by the application to ensure that it is correctly classified and the right level of security control is designed for the transmission, processing and storage of the data.

As part of the software development lifecycle Experian requires that staff involved in the design, coding, project management and deployment of applications undertake specialised training on secure coding techniques, and for developers there is in-depth training on the OWASP top 10 and CWE/SANS top 25 application flaws.

Automated static code scanning tools are used to identify coding errors. Experian performs regular vulnerability scanning and security testing of our systems including network and application penetration testing. These tests are provided as part of the evidence for Experian's PCI DSS certification.

Experian have made a significant investment in establishing a Global Security function to ensure that security is embedded within our day to day activities across the world. The rest of this document is aimed at explaining this security framework in more detail and we hope will demonstrate the Experian commitment to maintaining the security of the data that we hold.

• Threat Management

Experian's systems are hosted in purpose built data centres with multi-layered physical security and resilient HVAC. Systems are designed and specified to comply with globally agreed Technical Security Baselines, with server builds hardened to security best practices. Server event logs on critical systems are monitored for notable security events. A command centre is staffed 24/7/365 to manage systems and monitor for security events. Experian's public facing network incorporates a multi-tiered firewall infrastructure with products from different vendors. IPS is deployed. Diverse antivirus systems are used for desktop and server systems, and web content and email filtering. Full disk encryption is deployed on desktops and laptops. Port control software restricts the ability of users to only write data to approved removable media devices with enforced encryption. Vendor software patches are applied on a monthly cycle with a risk-based approach taken to prioritisation. Vulnerability scanners are deployed both internally on the Experian network and externally from the internet, with systems scanned weekly.

Virus scanners are deployed at both the perimeter and individual stations, and are maintained in a fully up-to-date condition. Furthermore, the perimeter antivirus solution is not the same brand as that which is deployed at workstations, thus providing two layers of checking of for malicious content.

All Experian servers and PCs are built to a documented secure standard, which if appropriate (for example on Microsoft Windows machines) will include anti-virus and malware defences. All information assets will have a defined patching schedule which is determined by the system's criticality and the level of threat the patch is mitigating. Experian also actively monitor the threat environment and check the effectiveness of current security controls by reviewing both free and paid for sources of threat information, including; public information, major vendor feeds and also receiving information from specialist closed group mailing lists.

The overall process is also plugged into an automated Patch & Fix strategy which is underpinned with a technology infrastructure to deliver corrective updates.

Malware detection is carried out both on the Edge and internal infrastructure, and across all ingress points into Experian. Multiple vendor technologies are used for appropriate defence in depth.

Experian implements a tiered approach to protection against threats. Protection is present at each level within our network utilising different technologies and techniques. For example, virus scanners are deployed at both the perimeter, and at the client station, and are maintained in a fully up-to-date condition. Furthermore, the perimeter AV solution is not the same brand as that which is deployed at the client, thus providing two layers of checking of for malicious content. Multiple Firewall layers are deployed to protect both Internet, and Service Layers (client side). The environment is further enhanced with IDS to ensure that early visibility of adverse conditions, or attacks are achieved. The Firewall is also enabled with a Smart Agent which looks at the state of packets, and bandwidth consumption as an additional level of protection against DoS, and DDoS. Real-time logging and alerting is in place, and this is subject to regular reviews.

• Information Security Policy

The Global Security Policy is owned by the Experian Global Risk Management Committee which is an executive level body and which assumes ultimate responsibility for the Experian risk position. The Global Security Policy is available to all Experian employees on the Corporate Intranet. The Global Security Policy is reviewed regularly to ensure they properly address, the following concerns:

- Business needs and business environment;
- External technology environment;
- Internal technology environment;
- Legal, statutory, regulatory and contractual requirements; and
- Other requirements specific to new or unique circumstances

If required, security standards will be updated to include these controls.

• Cyber Security Investigations Team

Experian has a dedicated Cyber Security Investigations team who sits within Experian Global Security Office to safeguard the Experian brand and reputation by protecting Experian’s key assets. To identify and effectively mitigate at an early stage any security developments that may threaten Experian's people, process, or technology through intervention and the thorough investigation of security incidents.

• Risk Management

The Global Security Steering Committee assumes operational ownership of the Experian information security policies and standards. The Global Chief Information Security Officer oversees and provides guidance to Experian for the overall development, implementation and coordination of security for systems and physical security. This role is supported by the Global Security Office staff and Regional Information Security Officers. All information assets such as data, applications, software and hardware have a steward appointed who is responsible for ensuring the asset's security.

Experian manages risk via a global risk management framework that consists of a collection of policies, processes, and methodologies for managing risk integrated with Experian's governance structure and consistent with our risk management philosophy, organisational structure, strategies, and objectives. The framework provides the infrastructure and activities within which risk is proactively managed across Experian, including how risks are identified, measured, monitored, controlled, escalated, mitigated and reported. The framework provides a structured process within which to focus on the full spectrum of risks to which Experian is exposed as a result of our global strategy, business activities, and internal and external environment. Through the global risk management framework management collectively identifies, discusses, monitors, and manages the potential sources of risk.

Security roles are defined in the Global Security Policy. Each employee, whether permanent or temporary, is responsible for security. Specific business information security roles are also in place in lines of business, i.e. Information Security Officer and Information Stewards.

• Security Credentials

Our customers and our customer's data is at the core of the Experian business, our vision is to enable the Experian business to appropriately secure that data so we can provide assurances to our customers, our clients and our regulators. Going beyond compliance the team strive to provide a competitive advantage to Experian by ensuring we are meeting or exceeding globally recognized security standards and upholding our compliance to contractually and regulatory enforced security obligations. The Security Standards Compliance team provides a leadership role by partnering with the business to consult, support and coordinate standard and regulatory security audits, attestations and assessments.

• PCI

Experian UK&I is a Level 1 Service Provider and Merchant covering Credit Referencing (CAIS data), Fraud Prevention, Marketing Services, Customer Management and Consumer Services. We have applications that process card data across all business units. Experian is annually audited by an External QSA (Qualified Security Assessor) from Trustwave and have successfully maintained compliance since 2010.

• ISO 27001

Experian holds ISO27001 certification in 2 key areas, the Global Security Admin team who are responsible for administering logical access to systems and in the Data Centre.

• Cyber Essentials

Experian holds Cyber Essentials Certification and performs risk assessments against our critical and external facing applications annually.

• Training and Awareness

Experian places a strong emphasis on training to ensure that employees are aware of the importance of security within the business environment in an ever changing and evolving risk landscape. All staff are required to comply with a comprehensive suite of security requirements and procedures to ensure they operate all systems in secure manner.

The Global Security Office deploys a comprehensive awareness programme that addresses specific areas of compliance for those areas that have specific information security responsibilities. All Experian employees receive mandatory Information Security and Data Protection training upon being hired and subsequently on a yearly basis to ensure that they are aware of the security policies and their information security responsibilities.

New starters are given training on information security and data protection principles and processes when they join Experian. This includes the use of an information security compulsory training module. The initial training is complemented by ongoing training and awareness campaigns. Staff are subject to both on the job training, and where required, are also subject to targeted security training programmes. Experian also has a training portal where users can receive training tailored specific to their roles.

• Acceptable Use Policy

Acceptable usage requirements around the usage of company assets is covered in Experian's Global Information Security Policy which is available to all employees, contractors and third parties on the corporate intranet. All employees are required to sign up to the global policy.

Security software is in place on internet proxy gateways to prevent and notify of any attempted downloading of unapproved content.

The company applies a level of control of all access to the Internet to provide a level of protection to Experian employees and assets to ensure protection and integrity also Experian policy prohibits use of CD/DVD drives, USB sticks or pen drives. Laptops are encrypted with McAfee pre-boot software.

Experian conduct automated monitoring via data loss protection software to identify where potentially unauthorised transmission of information is identified and dealt with via the incident management process. Additionally, Experian use key data string validation monitoring to block certain data being emailed outside of the organisation.

• Data Protection Requirements

Experian has a Data Protection Policy in place which sets out the standards expected around data privacy. Experian Data Protection Procedures sets out what we must do to comply with the Global Information Security Policy and the eight principles of the DPA.

• Incident Management

Experian has a formally documented risk-based incident management process to respond to security violations, unusual or suspicious events and incidents. This process is coordinated by the Experian Global Security Office and is owned by the Executive. The purpose of this process is to limit further damage to information assets, identify root cause, and execute corrective actions. Incident communication is tightly controlled to ensure a 'need to know' principle while allowing the correct investigation and escalation to occur. Post incident reviews are held to analyse the effectiveness of the incident response and operational processes in order to continually improve them. The Experian incident response processes are periodically audited and tested to ensure their currency and effectiveness.

Trends and patterns of security incidents are reviewed and examined to determine enterprise issues or implications to the larger business. The incident management process feeds into other functional areas of the company including training and Awareness, risk management and business continuity.

All third party and partner staff must complete on a yearly basis a mandatory computer based information security training which covers recognising and reporting security incidents. This training is backed up with targeted awareness activities such as presentations, intranet articles and specialised training for staff in key positions on how to identify role specific incidents.

• IT Systems Security

Password Security

Experian has a strict password policy that enforces their security. Password management processes ensure the confidentiality of passwords, so that they are only known to the user that they are issued to. Initial and temporary passwords are set to expire on first use, forcing the user to select a new password known only to them. Password sharing and group passwords are strictly prohibited.

Experian's password composition and selection rules exist to ensure that passwords are complex enough to provide a good level of security, and passwords are required to expire so that if compromised any exposure is reduced.

Experian password policy requires that passwords are kept confidential. Initial and temporary passwords are set to expire on first use, forcing the user to select a new password known only to themselves. Password sharing and group passwords are strictly prohibited.

Before users can request a password reset they must verify their identity. User IDs are normally provided via email with password provided via phone following appropriate authentication.

Experian's minimum password control standards include:

Length

- Passwords must be at least eight characters (recommendation is ten)

Composition

- Passwords cannot be blank
- Passwords cannot contain the User ID
- Passwords must be changed from default values

Encryption

- Passwords must be encrypted using a one-way hash function and salt. For full requirements please refer to the Data Security, Information Classification and Handling Policy and Standard.
- Passwords must be not be transmitted in clear text.

Passwords in Batch Logons

- Passwords must not be included in batch logon sequences unless there are sufficient controls to prevent their unauthorized use.

Complexity

- Passwords must contain characters from three of the following categories:
  - uppercase characters (A through Z)
  - Lowercase characters (a through z)
  - Numeric characters (0 through 9)
  - Non-alphabetic characters (for example !, $, #, %)

Forced Changes

- Passwords must be changed at least every 90 days.
- System-to-system user accounts that are interactive must change the password at least every 90 days.
- System-to-system user accounts that are not interactive (not logged into by individuals) are exempt from this requirement.

History

- When changed, passwords cannot be the same as any of the previous thirteen used.

Account Lockout

- User accounts must be locked out after 5 consecutive incorrect attempts; and

- Must be locked out for a minimum of 30 minutes or until an administrator enables the user account.

Account Inactivity

- The system must automatically disable or revoke accounts after 60 days of inactivity.
- The system will permanently delete accounts after 120 days of inactivity.
- Exceptions to account inactivity (e.g., leave of absence) are made with management approval.

Privileged User Accounts

- In addition to the controls identified for standard user accounts:
  - Access rights must be reviewed at regular intervals to ensure the higher level of access is still relevant to the user's role, or that unauthorized privileges have not been obtained.
  - Passwords should be changed more frequently, but must be changed at least every 90 days.

• IT Equipment Disposal

Certified processes are used to destroy media whether it has held customer information or not. As part of the Global Information Security Policy, Experian deploy Guidelines as to how media or data retentive objects may be disposed of. This process/policy requires that ALL media is subject to an adequate control, based on both Experian Policy, and the Client expectation to assure it is safe at point of disposal.

All confidential paper is securely shredded via a 3rd party onsite at Experian buildings. This occurs under CCTV cameras and is supervised by Experian personnel at all times and adheres to BS8470:2006.

• Data transfer Standards

As a global provider of information solutions we continuously assess information threats and industry trends based upon The Experian Global Security Policy and we have identified a need to clearly define the controls and standards required for information exchanges between Experian, our clients, and other third party organisations.

This identifies the mechanisms currently approved for information exchange between our clients and Experian.

Data transfer security requirements

The principles of information security management define the requirements for effective information protection and these include;

- Non-repudiation – When transferring any information, the system must ensure that the sender and recipient are confident that any other party is known and trusted and there is evidence to prove this.

- Confidentiality/Integrity – Both parties in such an exchange require assurance that information is stored, transmitted and processed in a secure manner.
- Audit – For the assurance of information integrity all information transfer must be suitably recorded to ensure that key events from any transfer can be evaluated in a timely manner.

By applying these principles secure transfer of data can be achieved by either sending the data through an encrypted network communication channel or by encrypting the data file before sending along an unencrypted channel. All network communication types including the Internet can be provided with suitable encryption solutions to allow for data transfer.

Data Classification

Any data that is to be transferred or exchanged must be classified according to its value and importance. Each classification attracts specific controls to adequately manage and secure it.

For all data being transferred or exchanged between Experian and our clients (i.e. Experian to Client/Client to Experian), we regard that data to be confidential.

• Third Parties

Experian has a dedicated supplier review function as part of the Global Security Office. The team operate a Third Party Security due diligence process to assess third parties that provide services to or consume services from Experian. Each third party is assessed by using 'Risk Profile Form' that is used to determine the third parties level of risk to Experian. They are then categorised into one of four risk levels which then determine the level of assessment that is conducted by the Third Party Security team which range from the completion of a security questionnaire to a formal on-site review.

Experian's Third Party relationships are subject to due diligence upon engagement and periodically during their lifecycle. The frequency of assessment is based upon a number of factors which include risk profile (e.g. type of service and data access, importance/criticality). A review / assessment may also be triggered as a result of a change of service being provided. Security, and the safeguarding of information entrusted to Experian, is one of the top priorities of our business, and we must be constantly vigilant and invest extensively to protect our data. Experian strives constantly to provide secure systems and processes that reflect best practices in an effort to stay ahead of today's increasingly sophisticated cyber criminals. As a result, key processes (which include the assessment of Third Parties) are subject to continuous improvement activity to ensure that they are efficient, effective, relevant and appropriate.

From an Information Security perspective actions required to implement and monitor agreed controls based on the identified security risks are managed through ongoing reviews with the service provider.