October 2015
Issue No: 1.1

Good Practice Guide

Transaction Monitoring for HMG Online Service Providers

CESG
NATIONAL TECHNICAL AUTHORITY FOR INFORMATION ASSURANCE

CabinetOffice

Good Practice Guide No. 53

Transaction Monitoring for HMG Online Service Providers

Issue No: 1.1
October 2015

This document is issued jointly by CESG, the UK's National Technical Authority on Information Assurance and Cabinet Office, Government Digital Services. It is provided "as is" as an example of how specific requirements could be met, but it is not intended to be exhaustive, does not act as endorsement of any particular product or technology and is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take the appropriate technical and legal advice in using this document (and others accessed from the GCHQ/CESG website).

Document History

Version	Date	Comment
1.0	April 2013	First issue
1.1	October 2015	First public release

Purpose & Intended Readership

This document highlights the important contribution that Transaction Monitoring (TxM) can make towards helping to counter the risk of electronic attack against HMG and local government online public services (hereafter referred to jointly as 'online public services'). It provides an overview of TxM from first principles to a suggested organisational structure and outlines a number of questions that organisations need to take into account when considering the business case for a TxM system.

It is assumed that a wide range of IA professionals involved in the provision of online public services will find this document of use.

Executive Summary

This document is part of a 'suite' of complementary guidance documents concerned with the secure delivery of online public services by government.

There is an ever present risk of electronic attack against these services, especially those offering payment facilities to customers. TxM can be a very effective tool in countering this risk. TxM comprises a complementary set of business processes which monitor authenticated online transactions in real time for signs of abnormal behaviour and provides appropriate alerts accordingly.

It is important to recognise that TxM is a distinctly different capability from protective monitoring; the former has different business objectives and outputs aimed at detecting fraud while the latter oversees how an ICT system is used or abused.

Transaction data is captured and analysed against a variety of information available to the service provider for evidence of unusual or unexpected behaviour. Any such evidence detected will then trigger an alert, which should raise the risk profile of the transaction with the service provider. The service provider should have a process in place to respond to high risk transactions.

This risk to online services and the types of attack they are likely to experience are covered in detail in the complementary guidance documents, but are also outlined briefly for contextual purposes. Credential theft and session hijack attacks are of particular concern.

The business impact of a successful online attack can be considerable and will typically involve the loss of data, money, service availability or integrity of data, reputational damage and a breakdown in public confidence.

It is assumed that a Department's TxM service will be provided by a combination of Industry, central HMG service and Departmental service, and will draw on the services of Identity Providers (IdP) and Attribute Providers (AtP) in the process.

TxM by government organisations is compulsory in certain circumstances.

Contents:

Chapter 1 - Introduction: First Principles 3

Background 3
Definition and Purpose of TxM 4
Transaction vs. Protective Monitoring 4
Key Terminology.....4
Principles of Operation 5
Assumptions 7
Compliance with HMG's SPF 7
Privacy Impact Assessments.....8
Scope of this GPG.....8

Chapter 2 - Risk Landscape.....9

Introduction.....9
Risks.....9
Threats 9
Threats Specific to Online Services 10
Threat Sources and Actors.....10
Compromise Methods and Vulnerabilities 10
Business Impact 11

Chapter 3 - Types of Attack 12

General.....12
Credential Theft or Compromise....12
Man-in-the-Browser 12
Mobile Malware 13

Chapter 4 - Controls and Organisational Structure.....14

General.....14
Controls 15
Responsibilities of the Citizen.....15
Government-installed Software 15
Organisational Structure.....15
Transaction Event Monitoring 16
Behavioural Monitoring.....16
Data Entry Monitoring.....17
Situational Awareness / Intelligence Feed 17
Root Cause Analysis 17
Security Operations Centre (SOC) 18
System Testing.....18
Assurance of Controls 19

Chapter 5 - Response and Escalation 20

General..... 20
Response Options 20
Automated Intervention..... 21
Manual Intervention 21
Delegated Authority to Act 21

References 22

Glossary 23

Chapter 1 - Introduction: First Principles

Key Principles

- Risk levels to online public services will vary; deployment of a TxM system should therefore be supported by a business case
- Transaction data is captured, analysed and appropriate responses triggered, if required, to verify whether a transaction is fraudulent or not
- Response options should range from a request for additional information to the online service being suspended
- TxM arrangements must comply with UK law. TxM is compulsory in certain circumstances
- HMG's Security Policy Framework (SPF) (reference [a]) requires Departments and Agencies to consider TxM as one means of complying with Mandatory Requirement (MR) 9
- Privacy Impact Assessments are required where personal information is involved

Background

1. The trend towards placing increasing numbers of HMG services online, in line with the Government ICT Strategy (reference [b]), brings with it an ever present risk of electronic attack for fraudulent and other purposes, particularly where high-value transactions are involved. A transaction in this context can be regarded as any exchange of value between two or more participants. Transaction Monitoring (TxM) is widely deployed by online service providers, especially those offering payment services to customers, as an essential tool in the fight against criminals (and others) to protect the service from attack.

2. However, the decision to operate a TxM system is not necessarily an automatic one and should be supported by a firm business case based on need and value for money, together with a TxM policy covering all aspects of its intended operation. The case for TxM (and other mitigating defences) should be based on reducing service risk to an acceptable level commensurate with the Board's risk appetite. For proposals to gain acceptance, therefore, the Board will need to have a clear understanding of what the service risk entails. This should include the benefits of its online service to the citizen, including service value and functionality, as well as the threat levels involved, the mitigating defences required and what the impact of a successful attack is likely to be.

3. Equally important is the need for the business case and policy to provide for maximum flexibility as government service contracts develop in response to requirements.

4. Running costs will inevitably be a major factor. The nature of some organisations' online services means that the level of threat they face will be relatively low and the likely costs of running a TxM system may be greater than the anticipated losses of running without one. Another significant factor affecting cost will be whether or not to outsource the TxM system to a commercial provider.

Definition and Purpose of TxM

5. A TxM system compares all aspects of a transaction event against data and rule sets previously recorded as the normal profile for a particular user. Having already established what a normal transaction session should look like in terms of behaviour and various technical parameters, any element of the transaction event which falls outside the profile then triggers an alert which raises the risk score of the transaction.

6. It is important to note that a TxM system forms an integral part of an online public service's detection and response mechanism, preceded by deterrence:

   a. Deterrence – these are actions taken to create the perception for attackers that their efforts are unlikely to succeed. It will typically take the form of a variety of warning notices to the user advertising the existence of the TxM system together with a statement of intention to prosecute in the event of fraudulent behaviour.

   b. TxM – these are actions taken to detect fraudulent or otherwise illegal behaviour by monitoring the transaction event for signs of unusual activity which might indicate an attack.

   c. Response – these are actions taken in response to detected events as described above. The appropriate response will need to be determined by the business in accordance with the perceived risk to the system and the value of the transaction and service.

Transaction vs. Protective Monitoring

7. It is important to note that TxM is quite different to protective monitoring. The former has different business objectives and outputs aimed at detecting untrustworthy transactional requests originating from an individual or malware on an external internet connected computer or device, across the boundaries of an internally owned system. It does this by monitoring various status measurements and events and flagging an alert when something abnormal takes place, usually on the basis of either normal customer interaction in general or for that customer in particular, even when session authentication and transactional security seems to be valid.

8. Protective monitoring on the other hand oversees how an individual ICT system is used or abused, usually takes place within an internal network (albeit one with external / internet connections) under single ownership and is intended to indicate the presence of any rogue applications (including malware) and provide user accountability. It does this by monitoring internal network connections and functions and flagging an alert when users or applications attempt to perform actions they are not supposed to, without necessarily knowing exactly what is causing the problem.

Key Terminology

9. The following terms are commonly associated with TxM. For the sake of completeness, terms already defined above have been included:

- **Escalation –** increasingly extensive actions taken following insufficient responses to requests made by the Online Service Provider (see below) to confirm or deny the legitimacy of a particular transaction (e.g. by applying additional identification and authentication controls in response to an instance of suspected fraud)
- **Fraud –** actions committed by an attacker either to misrepresent themselves or otherwise generally deceive others for the purpose of personal gain or to inflict a damaging impact on the business
- **Online Service Provider (OSP) –** the organisation that has ownership and responsibility for the delivery of online services to its customers
- **Transaction** - any exchange of value between two or more participants
- **Transaction Monitoring (TxM) -** A system which compares all aspects of a transaction event against data and rule sets previously recorded as the normal profile for a particular user. Any element of the transaction event which falls outside the profile then triggers an alert which raises the risk score of the transaction
- **Root Cause Analysis (RCA)** – the examination and analysis of all available data about an incident, action or event in order to identify its original source
- **Rule Set –** the rules governing the operation of the system. They are a set of thresholds and triggers designed to provide a system response in the event of suspicious behaviour and are developed to support the enforcement of organisational security policies

Principles of Operation

10. The key principle of operation is the capture of transaction data and its analysis for indications of unusual or anomalous activity so that a response can be triggered. This means looking for signs of not only anomalous activity within a single transaction, but also of coordinated activity across many transactions occurring within a very short timeframe which may, therefore, also be a cause for concern. The level and nature of the response will be a business decision and can range from a straightforward, automated request for additional information to the online service being suspended.

11. A TxM system will pick up data from many different levels and stages of the transaction, including that from commercial Identity and Attribute providers, hereafter referred to as Identity Providers (IdP) and Attribute Providers (AtP) and will need multiple hooks into the transactional architecture. Relevant data is likely to include user IP address, transactional content, timing information on session responses, identity and credential attributes, out of band authentication data and bank account details.

12. Handling data in this way, especially personal data, brings with it issues concerning the aggregation of information. Organisations must ensure that all such information is handled appropriately and in accordance with legal requirements.

13. The combination of deterrence, detection and response referred to above is achieved by means of several organisational elements all working in unison. Some or all of these may be outsourced and provided as a service to Departments and Agencies. These elements cover the following areas of activity and are covered in more detail in Chapter 4:

    a. Transaction Event Monitoring – real time monitoring of the actual event.

    b. Behavioural Monitoring – a comparison of the behaviour associated with a transaction against that which is expected.

    c. Fraud and Error Monitoring – a comparison of data entered by the user during the transaction event against that held by the service provider in the customer's account.

    d. Intelligence Feed – a situational awareness input to decisions leading to changes in parameters or rule sets.

    e. Root Cause Analysis – post event analysis to learn from attacks, be they genuine, successful, or false alarms.

14. These organisational elements must be capable of jointly performing the following functions in real time before the TxM system can be regarded as fully operational:

    a. Capture of all transaction data.

    b. Detection, i.e. analysis of transaction data for indications of unusual online behaviour which might indicate that an attack is in progress. The output from the analysis is compared against a variety of parameters or rule sets of expected behaviour determined by the business.

    c. Data storage and records management. This is required for the purposes of audit, rule set refresh, root cause analysis and, where deemed applicable by the business, potentially for use in civil or criminal prosecution. With regard to the latter, organisations should ensure that they operate an up to date Forensic Readiness policy and put into practice the current ACPO guidance on standards of digital evidence required for prosecution purposes (reference [c]).

15. Co-ordination of some or all the TxM processes above, for example within a Security Operations Centre (SOC) or similar body, has obvious benefits and is recommended. However, reality dictates that, at least in the interim, the network architecture is likely to be physically dispersed. It will therefore be crucial that all the TxM processes described above need to be capable of implementation individually, or jointly, across the entirety of the network.

16. Successful and effective TxM depends on flexibility of service, that is, the ability to detect and change data analysis in response to changes in functionality offered by the service, and changes in functionality of cyber attacks against the service. Arguably, the ability to monitor and change analysis and levels of detection as an ongoing capability is more important than the functionality offered on initial implementation. This is likely to impact significantly the service contract agreed with third party service providers in that contracts will need to support proactive, responsive and flexible working. This is likely to be significantly different from

service contracts taken out by Departments in the past, for services that are not Internet-facing.

Assumptions

17. This GPG makes the following assumptions with regard to managing the risks involved with providing public-facing services online:

    a. There will always be significant levels of risk for both parties but these will vary according to circumstances. Certain transactions, especially where money or some other transfer of value is directly or indirectly involved, will always be more attractive to potential attackers than others.

    b. This GPG is based upon the assumption that government will choose to outsource parts of the operation to commercial providers, particularly Identity and Attribute provision i.e. IdP and AtP. Complete outsourcing of TxM will not be possible as the HMG Department or Agency providing the online service will need to retain a certain level of control. (See Chapter 4 for further details.)

    c. The requirement for a TxM system to be capable of detecting and responding to possible attacks in real time and to be ready to protect against new types of attack not experienced before, means that it must also be capable of accommodating, in real time, whatever changes are required to maintain the currency of its various scoring parameters and rule sets.

    d. It must also be able to accommodate in real time whatever hardware or software changes IdPs and AtPs may make to their own ICT systems in order to continue to receive a service from them.

    e. TxM will not interfere with government business.

    f. A TxM system must be capable of blocking any number of transactions simultaneously, as determined by the business.

    g. TxM is compulsory in certain situations (see, for example, The Financial Services Authority's, 'Money Laundering Regulations 2007' (reference [d]). Departments' and Agencies' arrangements for the provision of a TxM system **must** comply with all aspects of UK law, not only in terms of what is *permitted* but also what is *required*.

    h. Given the rate of technological change and the pace of development in online services, Departments and Agencies should consider checking on a regular basis to ensure that they remain within the law at all times, especially when changes to TxM systems are in prospect.

Compliance with HMG's SPF

18. Central Government Departments and Agencies bound by the SPF (reference [a]) are reminded that they **must** conduct technical risk assessments for all ICT systems or services.

19. For those organisations not mandated to use the SPF (reference [a]) an appropriate risk assessment method as mandated by their organisation should

be used. This should take account of threats and vulnerabilities, together with the value of the transaction or service to the business.

20. The SPF (reference [a]) also stipulates that Departments and Agencies are responsible for their data regardless of any outsourcing or service provision arrangements they may have in place. This will be especially important in cases where online service providers are relying on a third party SOC for their TxM arrangements.

Privacy Impact Assessments

21. For new policies or projects that include the use of personal information, all Departments and Agencies bound by the SPF **must** assess the privacy risks to individuals in the collection, use and disclosure of the information. The type of assessment required (Full / Cut Down / DPA compliance review) must be determined through a PIA screening process which applies the recommendations of the Information Commissioner (refer to MR7 and section entitled 'Personal Data' (reference [a]) and the Information Commissioner's Office website (reference [e])). In connection with this Departments and Agencies are reminded that they are also responsible for ensuring proper management of information risk on the part of their partner organisations, regardless of whether they are private or public organisations (reference [a]).

Scope of this GPG

22. This document is part of a 'suite' of complementary guidance documents concerned with the secure delivery of online public services by HMG and is intended to complement the information provided in the following which are available from the CESG IA Policy Portfolio:

- CESG Good Practice Guide No. 43 (GPG 43) - Requirements for Secure Delivery of Online Public Services (RSDOPS) (reference [f])
- CESG Good Practice Guide No. 44 (GPG 44) - Authentication Credentials in Support of HMG Online Services (reference [g])
- CESG Good Practice Guide No. 45 (GPG 45) – Validating and Verifying the Identity of an Individual in support of HMG Online Services (reference [h])

23. Any outsourcing arrangements in respect of TxM will only involve UK based commercial concerns; off-shoring of services is not covered.

24. For the most part this GPG only concerns itself with managing the risks to HMG assets arising from online interaction with the public (citizen/organisation). Guidance on managing the risk to the latter can be found in the aforementioned GPGs. However, some risks involving the citizen will have a 'knock-on' effect on HMG's risk management of some systems and are therefore mentioned where relevant.

25. This GPG is only concerned with monitoring transactions between HMG service providers and their customers using the Internet.

Chapter 2 - Risk Landscape

Key Principles

- A set of generic online service risks covering threats, vulnerabilities and business impacts is contained in GPG 43 (reference [f])
- A 'Medium' level risk of attack on online public services is likely to be the minimum experienced
- Majority of threats originate from authentication of credentials and the validation and verification of identity
- Business impact from a successful attack can be considerable and can typically involve the loss of data, money, service availability or integrity of data, reputational damage and a breakdown in public confidence

Introduction

26. A TxM system contributes to the active management of risks posed to HMG online services. A set of generic online service risks covering threats, vulnerabilities and business impacts is contained in GPG 43 (reference [f]) and should be referred to for detailed information. Below is a brief outline of what a TxM system has to contend with in this respect.

27. For those organisations bound by the SPF (reference [a]) compliance with certain Standards is required when conducting technical risk assessments and managing information risk. Other organisations should ensure that their normal risk assessment methodology and risk management procedures are suitable for a TxM environment and highlight the level of risk appropriately.

Risks

28. As mentioned earlier in this document, placing public-facing government services online will attract significant levels of risk of electronic attack for the purposes of fraud or possibly a variety of other motivating factors such as the generation of economic and / or political instability.

29. It is essential that online service providers have a clear understanding of the risk posed to their specific service and their individual transactions. The specific risk levels may vary depending on the nature of the online service and transactions.

30. Online service providers will also need to consider the risk of attacks being enabled by using other channels (e.g. telephone or face to face). TxM capabilities will therefore need to include the ability of capturing and analysing inputs from other channels such as these.

Threats

31. For the purposes of this GPG, threat actors to a HMG online service are defined as any individual(s) or organisation with the capability, opportunity and motivation to attack that service.

32. Online services present criminals with the opportunity to commit fraud at relatively low risk of discovery and prosecution. This can include traditional methods of fraud which can be carried out on a large scale due to capabilities of electronic systems. It can also include newer methods that are wholly enabled by the Internet and involve sophisticated and automated attack techniques, often achieved by using malware which is active on a large number of personally owned devices, including PCs, tablets, smartphones etc., which can be carried out on a large scale.

33. The technology used to deliver and protect online services is constantly evolving. Attackers will therefore continue to search out new technical and non-technical vulnerabilities to exploit.

Threats Specific to Online Services

34. There are several areas of activity in respect of online services from which the majority of threats originate:

    a. Validation and Verification of Identity – there are a number of threat sources and actors in respect of identity and range from, for example, members of the public who may accidentally or deliberately seek to compromise an identity verification service, through to serious and organised criminal groups who may seek to compromise the service for large scale financial gain.

    b. Authentication – threat sources and actors will seek to make use of compromised identity credentials to gain unauthorised access to systems, information and services and there is a lucrative criminal market engaged in the procurement and sale of such commodities.

    c. Session and Transaction Hijack.

    d. Phishing.

Threat Sources and Actors

35. Potentially any number of threat sources and actors can present a risk to the transactional security of an online service, including that originating from individuals working or operating in or for, or who are involved in providing services to, the online service.

36. With this in mind, and for the purposes of non-SPF mandated risk assessment, threat sources can be regarded as anyone that would benefit from a successful compromise such as criminal groups or organisations. Threat actors, on the other hand, can potentially include anybody with access to an ICT system connected to the Internet, including authorised system and service users.

Compromise Methods and Vulnerabilities

37. The compromise method can be thought of as a high level statement of the broad type of attack that a threat actor may attempt to deploy against the online system in an attempt to compromise or steal assets. A more detailed look at the different types of attack is given in Chapter 3.

38. The types of compromise to which an online system is subject typically involve the following:

    a. People - users and providers of the online service, including identity providers.

    b. Physical storage and handling of sensitive information.

    c. Procedure - weak and/or poor procedures in respect of sensitive information.

    d. Technical inadequacies - this can include anything from poor system design, development and implementation through to failure to keep operating systems and applications up to date and appropriately patched.

Business Impact

39. There are several major areas of concern regarding business impact for Departments and Agencies in the event that an attack is successful:

    a. Data Loss – this includes identity theft and the impact can range from the loss of personal information that constitutes an inconvenience, to that of sensitive details about an individual that could, in extremis, lead to an individual(s) coming to harm. When corporate data is lost the consequences can be profound, involve a wide range of business activity and threaten the continued existence of the enterprise.

    b. Financial Loss – this can range from a relatively small-scale loss for the individual up to and including large-scale loss. In the public or private sectors losses can range from relatively small-scale impacts to those that are devastating for the organisation concerned.

    c. Loss of service availability or integrity of data - the degree of impact will vary in severity according to circumstances. A source actor seeking this type of impact is likely to be driven by anti-establishment, political and/or economic motivations.

    d. Reputation – damage to reputation is a compounding factor cutting across a wide range of business activity and is difficult to quantify. The impact on the business can vary tremendously according to circumstances and can be catastrophic in some scenarios. In terms of online services, for example, the belief, rightly or wrongly, that HMG is unable to protect against attacks on its services could for example, lead to the UK becoming known as a ‘soft touch’ for cyber crime

    e. Public Confidence – any or all of the foregoing could lead to varying degrees of breakdown in public confidence regarding online services. The implications for whether HMG’s ICT Strategy (reference [b]) is ultimately deemed a success or not is considerable, with an attendant degree of political fallout inevitable either way.

Chapter 3 - Types of Attack

Key Principles

- Credential theft or compromise is a major concern as details can be used by the threat actor or sold on the black market to other criminals
- 'Man-in-the-Browser' attacks are of equal concern and lead to information gathering and/or session hijacking
- Mobile malware is increasingly used to attack online services

General

40. This Chapter builds on the vulnerabilities identified in paragraphs 37-38 as the main focus of attention for fraudulent purposes, namely authentication of credentials and validation and verification of identity. It does not make a case per se for TxM, but is included to highlight the extent and seriousness of attacks that TxM is designed to counter. Cyber criminals will seek illicit financial gain, either in the form of a direct attack on financial assets or in an effort to obtain information about the citizen to sell on to others. There are many different kinds of attack that are possible against online services, in part made easier as information is, of necessity, invariably sent across a range of different platforms. These include credential theft, phishing, session hijack or transaction hijack.

Credential Theft or Compromise

41. A credential is some kind of shared secret and/or hardware token and/or biometric that allows an individual to give repeated assurance that they are the same person who successfully completed a process of verification at some point in the past. Identity credentials are based on the user's ability to provide information or data to the system for authentication purposes. Theft or harvesting of credentials, the difference between the two sometimes being one of scale, is in essence the pre-cursor to an actual attack. There is a variety of ways in which credentials can be compromised or stolen. Some methods are common to other kinds of data theft while others are unique. Once stolen or compromised, credentials can be used either to masquerade as a legitimate user of a system, or they can be sold on the black market to other criminals.

42. Credential theft can result from malware running on the citizen's device or endpoint, i.e., PC, tablet, smartphone, and so on. Credential information (e.g. passwords, secrets) is collected by the malware and sent from the device to the criminal entity in question.

43. GPG 44 (reference [g]) lists a number of different attacks that could be used to compromise authentication credentials. Once again, these methods are by no means unique to credentials. Of these attacks, the 'Man-in-the-Browser' is of particular concern.

Man-in-the-Browser

44. This attack targets information exchanged between the user and the browser on the user's own device and occurs before that information is protected by a secure

tunnel between the browser and the online service provider's server. A victim's machine is infected with malware by a variety of means, some of which may not be apparent, even to a technically competent user. Following the infection, the malware waits until the victim browses to the targeted online service. The malware can then alter the page provided by the online service (this is commonly called a web inject attack) either to steal user details or hijack the user's session as described below.

45. Once infected in this way, the user's device can then be controlled by the attacker in two ways:

    a. Information Gathering – in the course of the user's engagement with the online service, the malware generates fraudulent forms designed to gather various information about the user, invariably credential related. The information is then sent to the attacker. Once in possession of such information, the attacker may log onto the online service from a separate computer using the stolen identity credentials and masquerade as the legitimate user for fraudulent purposes. Alternatively, the credentials may be sold on the black market for others to use.

    b. Session or Transaction Hijacking – this involves illegal transactions following a legitimate login. Once the user is authenticated the malware initiates a fraudulent transaction. The legitimate user knows nothing about the attack being perpetrated and may even be coaxed into inputting two-factor and out of band responses. For its part the service provider will register that a legitimate customer session has been authenticated and will need to rely on TxM to detect that individual transactions have been compromised (see Chapter 4).

46. The encryption of data between the user's browser and the online service's server offers no protection against this attack as the malware, in simple terms, operates between the keyboard and browser input.

Mobile Malware

47. Various methods seen in commercial online services seek to increase authentication strength by using a second factor of a Transactional Authentication Number (TAN) sent to a second device, eg. a smartphone. Attacks have been identified against these methods coordinating actions of malware injected into both smartphone and session device. For this reason, mobile based one-time passwords should no longer be considered as being fully effective out of band or alternative communication channels for the delivery of additional authentication information.

Chapter 4 - Controls and Organisational Structure

Key Principles

- Successful TxM requires a new culture of continual pro-active service monitoring and rapid change in response to developments
- The citizen has a role to play by doing what they can to keep their personal ICT devices free from malware
- Use of government-installed software or recommended products on customer machines is strongly discouraged
- While various elements of a TxM system may be outsourced, complete outsourcing of TxM will never be possible
- Engagement with a Security Operations Centre to rationalise and streamline a number of security related functions may be an option
- Assurance of controls is expected to involve comparison of an organisation's own metrics against market statistics and trends in respect of fraud committed online

General

48. The organisational elements detailed below and their specific controls in practice present a defence in depth approach whose purpose is to detect, analyse and return a risk score for online transactions. Many of these controls, especially those relating to behaviour (see below), will require continuous rule development and profile updating to remain effective.

49. A TxM system compares all aspects of a transaction event against data and rule sets previously recorded as the normal profile for a particular user. Any element of the transaction event which falls outside the profile then triggers an alert which raises the risk score of the transaction. This, in turn, should trigger a series of escalating responses aimed at confirming the event as legitimate. While allied to TxM, response and escalation are not an integral part of a TxM system.

50. To achieve this, all the constituent elements of the profile need to be correctly weighted and balanced in order to detect transaction events worthy of a real time response. Getting the balance right is vital; too many false alarms will indicate limited effectiveness and quickly lead to a lack of confidence in the capabilities of the system.

51. A contributory factor in striking the right balance is the organisational structure of the system. This Chapter outlines a typical structure, including the option of establishing a Security Operations Centre (SOC).

52. The continual, pro-active service monitoring and change elements required for a successful TxM system represent a substantially different approach to the way in which ICT services have been provided and operated in the past. This cultural change will involve intelligence data feeds, multiple transactional data feeds, data collection and analysis. This will result in a great deal of low-level, highly detailed data analysis by cyber experts with the delegated authority to make business

changes to the online service immediately. Internal controls, governance and service contracts will all need to support this way of working.

Controls

53. The controls deployed to detect and respond to possible attacks will depend on the capabilities and interactions, of and between, the various elements of the system. They also need to be proportionate to the risks posed to the online service.

Responsibilities of the Citizen

54. This GPG takes the view that the citizen has a role to play in helping to avoid the instance of fraud by keeping themselves safe online, particularly with regard to taking steps to keep their ICT devices as free as possible from malware. User education about the range of good online practices that can be adopted should be actively promoted by government Departments and Agencies as a relatively cheap means of helping to limit the incidence of fraud.

55. Departments and Agencies will decide for themselves exactly what is required in this respect but should regard the sorts of advice and guidance offered by the 'Get Safe Online' website (reference [i]) as the starting point. Departments and Agencies may also wish to consider requesting users to sign up to certain 'Terms and Conditions' (perhaps via the frequently seen 'click to agree' button) as a pre-requisite for access to the online service. Such a step will help to reinforce the message that online security must be taken seriously.

Government-installed Software

56. CESG advises strongly against online service providers recommending that customers use particular products (security products or otherwise), or providing customers with bespoke software, as a precondition for use of the service.

57. Apart from any additional running costs incurred, there are sensitivities to be borne in mind surrounding the nature of government – citizen interaction, not to mention the reputational damage and claims for liability that could result in the event of failure of such products.

Organisational Structure

58. As described earlier in this guidance, the purpose of a TxM system is to analyse data and detect fraudulent transactions online. Some of the processes involved in this might be facilitated within the HMG Department or Agency offering the online service, some might be outsourced to third parties.

59. The level of assurance that Departments and Agencies require in the course of a transaction will depend on a number of variables. These include, but are not limited to, risk appetite, the extent of outsourcing involved, the nature of the online business, the value of the transaction, its sensitivity, the presence of personal data, whether a particular Department participates in any SOC-based arrangements and the need to comply with any legal and regulatory requirements that may apply to the nature of the online service in question (see paragraph 17g.)

60. Whatever Departments and Agencies decide upon in this respect, it will never be possible to outsource TxM completely. Some elements of transactional analysis will be heavily dependent upon specific business rules, and this will be service specific. Moreover, Departments and Agencies must retain the means to vary the make-up of their TxM system flexibly and quickly in response to the dynamic nature of attacks which themselves are constantly evolving and changing in response to controls being applied.

61. Against this backdrop, therefore, the organisational structure below is defined by the respective functions required by TxM. Each of these is best viewed as an 'organisational entity' in recognition of the fact that their true identity lies somewhere between on the one hand, that of a virtual public-private organisation and, on the other, an organisation in its own right in cases where a particular process is run by only one body, be that the public or private sector.

Transaction Event Monitoring

62. This process focuses in real time on various technical aspects of the session interface and is intended to identify suspicious traffic between the citizen and the online service. The following are recommended as the minimum that HMG online services should monitor in this respect, from both a procedural and technology perspective.

    a. The same IP address authenticating as multiple users and conducting the same transaction each time.

    b. IP fingerprinting – works by building an IP profile or fingerprint of the machine(s) normally used by a customer and raising the risk rating of the transaction when the profile changes more than a configurable threshold. To be effective, the inputs used to produce an IP fingerprint need to be dynamically configurable in terms of their weightings from a risk perspective as some of the inputs could be a result of legitimate behaviour. A variety of information can be used to build the fingerprint.

Behavioural Monitoring

63. Behavioural monitoring encompasses a wide area of activity, including Root Cause Analysis (see below). The effectiveness of behavioural monitoring relies on continuous, simultaneous analysis of multiple strands of TxM related activity with numerous outputs being fed in near real time into the updating of various rule sets. The aim of all this activity is to maintain an up to date profile of what represents 'normal' activity. This in turn permits 'abnormal' activity to be detected and system responses to be triggered.

64. The number of TxM monitoring strands related to behaviour is many and varied and can be expected to grow as TxM technology develops. Principal among these are the following:

    a. Analysis of new business processes and online functionality in order to baseline normal system and customer behaviour.

    b. Offline analysis of historical transactions to identify patterns that might indicate automated attacks.

c. Maintaining situational awareness to identify emerging trends in attacks and techniques (see Intelligence Feed, below).

d. Utilizing historical transaction data to test new approaches to and methods of, detection.

e. Date and time a transaction occurs.

f. Geographical location.

Data Entry Monitoring

65. This is essentially the monitoring and comparison of data entry made by the citizen during a transaction against the same data provided at time of first registration with the online service provider. It also includes that same comparison being made in respect of data held by the IdPs and AtPs, all in order to detect either genuine inputting errors or attempted fraud. Note that IdPs and AtPs should only release data that they are required to under the terms of the contract with the online service provider; to do otherwise would infringe data protection principles.

Situational Awareness / Intelligence Feed

66. Any TxM system will require a constant feed of situational awareness updates or intelligence which it will assimilate and translate into requirements for fine tuning of the system. The source and nature of such feeds will depend on the system in question, but could, for example, come from the intelligence services, law enforcement bodies, other HMG Departments and Agencies, public sector bodies, or be purchased from a range of commercial suppliers of information services. No one source of information is likely to meet all the requirements of a particular Department or Agency, so organisations should plan to accommodate and make use of multiple inputs in this respect.

67. The information feeds required are typically likely to include, but not limited to, items such as problem IP addresses, bank account details, telephone numbers, threat assessments, situational awareness reports, market trends and developments, the latest virus signatures and details of reported online attacks.

68. Such information would typically be received and processed by a SOC for sharing amongst those Departments and Agencies running online services, but where such a body is absent Departments and Agencies should take steps to share such information with other online service providers for the benefit of them all.

69. It is worth noting that some commercial threat intelligence feeds may not be compliant with UK law, so while some commercial concerns may be happy to use them, HMG organisations should ensure that they obtain appropriate legal assurances beforehand regarding their use.

Root Cause Analysis

70. Root Cause Analysis (RCA) is initiated as a result of the following:

a. When a successful attack has been made.

b. An attempted attack has been made but averted through detection and response.

c. A detection / response sequence has proved to be a false alarm.

71. RCA can involve different procedures, the nature of which will be decided by the business. It is an in-depth analysis of all of the information metadata germane to any of the aforementioned scenarios a–c. As a minimum this should include specifics such as details of the event in question, attack vectors, participants (if identified), related situation reports, malware analysis and data mining to look for anomalous or similar behaviour to that noted.

72. The purpose of RCA is to enable the TxM system to learn from the event and feed updates and fine tuning adjustments into the profiling process accordingly. In other words, it contributes towards maintaining the definition of 'normal' user behaviour. Analysis and output need to take place as quickly as possible and be measured in terms of minutes rather than hours to maintain effectiveness of the TxM system.

Security Operations Centre (SOC)

73. The concept of a SOC is one of rationalising and streamlining a number of security operations or services centrally that would otherwise need to be replicated by Departments and Agencies. TxM is one such area of operations that typically could be offered by a SOC to Departments and Agencies engaged in online service transactions.

74. Depending on the sophistication and maturity of operations of both the online service provider and the SOC, the former may wish to allow the latter to run a large part of the online service on its behalf, even to the extent of permitting the latter to propose appropriate levels of short and long-term risk appetite, by virtue of their unique overview of the security landscape.

75. The decision to engage with a SOC, which services to draw upon and to what extent will be one for the business to make. In the absence of a SOC Departments and Agencies should seek to compensate for this by sharing knowledge and resources with partner organisations to maximise the effectiveness of TxM across a particular area of government.

System Testing

76. In addition to its live operations, all aspects of a TxM system should be reviewed and tested periodically in accordance with the agreed TxM policy. This is particularly important in the following circumstances:

a. After system patching has taken place.

b. Rule sets have been updated or fine-tuned.

c. New system functionalities or business processes have been instigated.

d. Configuration changes have been made.

Assurance of Controls

77. The issue of how one judges the effectiveness of a TxM, i.e. how well or otherwise the controls are working, will ultimately be one for the business to decide and include in its business case for a TxM system.

78. How the business decides to measure effectiveness will depend on the nature of their TxM requirements. In addition to all the usual statistical data such as the percentage of blocked attacks, assets compromised or lost, error detection rates, the issue at heart for most Departments and Agencies will be value for money; how much money has been kept out of the hands of fraudsters compared to the running costs involved? However, even this is not necessarily a straightforward question as value for money will also draw reputational risk into the equation.

79. Nevertheless, most Departments and Agencies will at least want an indication of how well their system is performing; in essence, where is the online service industry 'red line' for fraudulent transactions and do they fall above it or below?

80. A good place to start is a comparison of their own metrics against the latest market statistics and trends for fraud committed against online service providers. A SOC is likely to provide such information, but in its absence Departments and Agencies will either wish to commission their own research or fall back on whatever publications are available from government or the information security industry.

Chapter 5 - Response and Escalation

Key Principles

- Response and escalation are separate to TxM and likely to be governed within a different part of the online service provider's system
- The point at which to respond to activity flagged as suspicious and whether a potential attacker should be alerted to this fact are business decisions
- Exceeding a pre-determined level of trust should trigger an initial automated response followed by manual intervention as escalation occurs
- Clearly understood arrangements for delegated authority to act must be in place and provide for changes to be made to the online service immediately as required

General

81. Response and escalation are not a constituent part of a TxM system. In particular, they are likely to be governed within a different part of the online service provider's system. Nevertheless, the role of a TxM system is to provide data for a response service and this Chapter summarises.

82. The point at which to respond to activity flagged by the TxM system as possibly 'suspicious', the extent of that response and the timeliness required, is essentially a risk management decision for the business to make. A number of factors will come into play which will reflect the way in which the TxM system itself has been configured to respond.

83. In principle, the risk level of a given session should be altered immediately when TxM flags an alert to unusual activity. However, this should not be reflected in the external interface presented by the OSP to the user, in order to prevent any attacker learning about TxM thresholds from stress-testing a system. Not alerting an attacker in this way will also facilitate their actions being tracked with a view to learning more about their modus operandi and/or gathering evidence for a prosecution.

84. The various rule sets must be able to accommodate rapid change in order for the TxM system to remain effective. At its most fundamental level the TxM system will be indicating that there is an insufficient level of trust in either an individual transaction, or the client device/end point being used. From that point on, pre-determined business processes will be initiated resulting in the appropriate response.

Response Options

85. In its simplest form a response will involve some kind of intervention in the transaction event, the nature of which can be automated or manual. Response options should range from low level assurance checks (challenge – response with the citizen) to immediate suspension of the transaction. In certain high risk situations it may even be necessary to limit the effects of an attack by taking a service offline for a period of time. The TxM system should be sophisticated

enough to capture real time evidence of wrongdoing, enabling immediate notification of law enforcement authorities to be made.

Automated Intervention

86. This is the first level of response once the pre-determined level of trust has been exceeded. This provides for a timely response and is particularly appropriate given the relatively high number of transaction events that are likely to be taking place simultaneously and the fact that most detection errors will occur in the initial stages of a transaction.

87. A number of checks will be undertaken to ensure that the transaction event is acceptable, i.e. that it meets the requirements of the provider's policy. The service could confirm legitimate transactions with customers using pre-defined transaction contextualisation approaches or some method of out-of-band communication, e.g. pre-recorded telephone call requiring submission of additional information. (It should be noted that techniques using mobile phones to support one time password authentication can be compromised and therefore should not be considered fully out-of-band.)

Manual Intervention

88. This is the second level of response and takes place once automated interventions have been exhausted but the transaction still does not meet the provider's policy. At this point manual checks are undertaken to confirm the integrity and authenticity of the transaction before any transfer of value is made.

Delegated Authority to Act

89. The issue of who has authority to act in the event of an alert is vitally important and must form part of the TxM system's response planning. There must be a clearly understood and unequivocal process in existence; any uncertainty in this respect cannot be tolerated as any undue delay may mean the difference between successfully bringing an attack to a halt or not.

90. A swiftly executed response will inevitably require some measure of delegated authority whereby operational staff are empowered to make critical response decisions and system changes immediately as required in response to events and are supported by whatever out of normal working hours follow-on support arrangements are required. Staff charged with such responsibilities must, of course, receive the appropriate training and support to prepare them for the task.

91. Authority for staff to act in this way should be based upon and integrated with a proper business change process governing long term change.

References

[a] HMG Security Policy Framework, Tiers 1-3 available at www.cabinetoffice.gov.uk

[b] “Government ICT Strategy” – available at www.cabinetoffice.gov.uk

[c] Available at www.acpo.police.uk

[d] Available at www.fsa.gov.uk

[e] Information Commissioner’s Office, Privacy Impact Assessments. Available at: http://www.ico.gov.uk

[f] CESG Good Practice Guide No. 43, Requirements for Secure Delivery of online Public Services (RSDOPS) – latest issue available from the CESG website.

[g] CESG Good Practice Guide No. 44, Authentication Credentials in Support of HMG Online Services – latest issue available from the CESG website.

[h] CESG Good Practice Guide No. 45, Validating and Verifying the Identity of an Individual in support of HMG Online Services – latest issue available from the CESG website.

[i] See www.getsafeonline.org

Glossary

ACPO	Association of Chief Police Officers
AtP	Attribute Providers
GPG	CESG Good Practice Guide
IA	Information Assurance
ICT	Information and Communications Technology
IP	Internet Protocol
IdP	Identity Providers
MR	Mandatory Requirement (of the SPF)
OSP	Online Service Provider
RCA	Root Cause Analysis
RSDOPS	Requirements for Secure Delivery of Online Public Services
SMS	Short Messaging Service
SOC	Security Operations Centre
SPF	Security Policy Framework
TAN	Transactional Authentication Number
TxM	Transaction Monitoring

CESG provides advice and assistance on information security in support of UK Government. Unless otherwise stated, all material published on this website has been produced by CESG and is considered general guidance only. It is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate tailored advice.

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Email: enquiries@cesg.gsi.gov.uk