Business to Business Data Sharing using Trusted Computing

Stephen S. Khan

Technical Report
RHUL–MA–2010–07
31st March 2010

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

Business to Business Data Sharing using Trusted Computing

Stephen S Khan

Supervisor: John Austen

Information Security Group, Royal Holloway,
University of London, Egham, Surrey, U.K

Student Number: 100595943

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature:

Date:

Executive Summary

Businesses and Governments are seeking new ways to improve their products and services, make them cost effective and take advantage of global sourcing options.

This has been largely enabled by fast, stable communication networks sharing vast volumes of data to facilitate delivery of services to customers. Sharing has led to concerns over data protection and the risks the data faces in the new open business models called Digital Business Networks.

Sharing data with partners to meet business objectives requires trust from both parties. Trust is difficult to build which is why organisations use a number of different methods to establish trust such as contracts, audits, etc. These have inherent issues which cannot easily be addressed.

The current security landscape of controls, countermeasures and mitigation strategies have not changed significantly therefore new ways are being sought to deliver improved security. This need is increasing as organisations move towards new open de-perimeterised seamless business process models.

Trusted Computing using a Trusted Platform Module claims to offer higher security for platforms leading to better data assurance and lower risk levels as well as protecting platforms from malicious code.

This paper seeks to establish if Trusted Computing can offer lower risks and greater data assurance against platforms attacks when compared with current controls.

A detailed risk assessment was performed of risks to data on current platforms, and then a further comparator assessment was performed assuming Trusted Computing Trusted Platform Modules (TPM) controls were deployed.

This comparison suggests that Trusted Computing does indeed reduce the platform risks to data by up to 67%. However, due to the low adoption of the Trusted Computing TPM technology today, there are currently few applications using this new technology. This is expected to change as leading manufacturers of processor chips develop integrated functions within their processors, which will facilitate more applications to use the TPM in the medium to long term.

There are other challenges which need to be overcome before TPM usage becomes common place. This includes a Public Key Infrastructure with certificate authorities aiding the use of the TPM. Deployment of TPM will need to extend from mainly laptops today to servers before organisations can use them for their critical data.

The microprocessor manufacturers will also need to improve on isolation technologies to support commonly used virtualisation solutions. Operating system and application vendors will also need a standard method for software hash checks support proving the integrity of software.

Trusted Computing with TPM offers a great step forward in protecting data from platform attacks as the current protection mechanisms have not changed significantly over recent years and in the author's opinion are largely not effective against today's attack methods. The technology needs to mature on many fronts before applications are developed and organisations gain the confidence to use it. However in the author's opinion it is simply a matter of time before the required enablers are in place to allow wide spread adoption.

Acknowledgement

I would like to thank Royal Holloway and the lecturers for running such a great course. It has afforded me a personal development opportunity and an environment to develop deep friendships.

I would like thank my wife, children, family and friends for their support, encouragement and understanding in allowing me the time to pursue this master's degree without placing additional pressure on my limited time.

Table of Contents

List of Figures

List of Tables

List of Acronyms

AIK	Attestation Identity Key
BBC	British Broadcasting Corporation
BERR	Department for Business, Enterprise & Regulatory Reform
B2B	Business to Business
CE	Conformance credential
CRTM	Core Root of Trust Measurement
DBN	Digital Business Networks
DPA	Data Protection Act
EK	Endorsement Key
FDA	US Food and Drug Administration
GxP	Good Regulatory Practice
HIPPA	Health Insurance Portability and Accountability
KPI	Key Performance Indicators
PCR	Platform Configuration Registers
PE	Platform credential
PKI	Public Key Infrastructure
PII	Personal Identifiable Information
RTM	Root of Trust Measurement
RTS	Root of Trust Storage
SaaS	Software as a Service
SANS	SysAdmin, Audit, Network Security institute
SSL	Secure Sockets Layer
SRK	Storage Root Key
TCG	Trusted Computing Group
TLS	Transport Layer Security
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TPME	Trusted Platform Module Entity
VE	Validation Entity

1 Introduction

1.1 Context

Over recent years, the pharmaceutical industry has been going through an unprecedented level of change. This has been driven by the global competitive market for drugs with few new high market value drugs, patient expiration on existing drugs and research and development taking 10-15 years [1] on occasions. Regulatory requirements also make the drug development process longer before a drug can be released into the market.

This has put pressure on business operating models to reduce costs in order to maintain competitive advantage and pursue new cost effective operating models. The days when new compounds were researched and developed inside the business and marketed by internal teams are no longer viable.

Collaboration with business partners offers the opportunity to share costs, knowledge, information and expertise to develop and market drugs.

In the context of this paper, a Partner is defined as any entity from which the business buys service provision or is engaged in a business relationship.

These Partnerships are formed with many sectors including hospitals, doctors, IT service providers, research companies and universities both locally and globally.

Collaboration means sharing facilities and confidential business information including patient data, personal information, intellectual property, research information and price information. Given the time and resources taken to develop drugs, these data assets are of high value to businesses and their competitors. The aspects of data security are not always within control of the data controller or owner but instead the Partner organisation.

To allow seamless integration in these Partnerships, many businesses are driving towards de-perimeterisation [2] and the general direction advocated by the Jericho forum [3]. The idea that perimeter controls (such as firewalls, proxy's, routers, etc) will be complimentary to controls on the actual data is an important concept going forward.

The author suggests, despite the awareness and alarm over data loss, there seems to be a constant stream of data breaches as highlighted in the press [7], [8], [9], [10], and [11]. The issue will persist unless better controls are implemented.

Data loss can be attributed to human errors, deliberate acts or malicious activity and not forgetting criminals using vulnerabilities in software. These include but not limited to programmatic code [12] or applications installed with backdoors called root kits [13]. SANS a respected security research organisation highlights 25 of the top programming errors and information on how to fix those [70]. However, the same errors are continually present in applications as confirmed by the organisations weekly publication.

This highlights the need to have good control over all aspects of information security including people, technology and business processes. These controls should be implemented in an effective manner to establish trust in an organisations ability to look after data.

This paper explores if Trusted Computing can provide that additional level of data assurance and trust to allow organisations to build more confidence in sharing data when working with Partners.

This level of assurance will be determined and assessed by conducting a security risk assessment on the Trusted Platform Module used in implementations of Trusted Computing.

1.2 Objectives

The objectives of this paper are to:

1. Outline the context of data sharing and why organisations need to share data;

2. Outline business challenges in trying to establish trust in data sharing relationships;

3. Perform a risk assessment to establish if Trusted Computing controls can offer reduced risk and better data assurance on platforms processing sensitive data; and

4. Outline any challenges which may prevent Trusted Computing adoption

1.3 Scope

The scope of this study is to look at data sharing in business and governments through the use of a pharmaceutical organisation for setting context for the risk assessments. It is assumed that many of the challenges faced by pharmaceutical organisations are common to general business and governments.

The risk assessment will attempt to establish if a Trusted Platform Module used in Trusted Computing can offer improved platform security, lower risk and greater assurance for data integrity and confidentially.

The paper will put forward in the author's view, the challenges for Trusted Computing adoption.

1.4 Organisation

The report is broken down into the following chapters:

Chapter 1 – Sets out the context of the study, the objectives and scope.

Chapter 2 – This chapter sets the scene and discusses data sharing. Why data is shared, some of the drivers for data sharing as well as how data is shared. The author then explores some of the advantages and challenges with data sharing.

Chapter 3 – This chapter discusses trust and how organisations try and establish trust and the associated challenges in business relationships. Some of the commonly used methods to establish trust and their challenges are highlighted.

Chapter 4 - Explores the security landscape and outlines some of the drivers and requirements for data security. The author explores some of the challenges in meeting those requirements.

Chapter 5 – An overview of Trusted Computing is provided, focusing on the Trusted Platform Module (TPM) which aims to give the reader context for the risk assessment. A model for business to business data sharing is outlined using Trusted Computing. The author then explores in their view, some of the challenges for the adoption of Trusted Computing technology.

Chapter 6 – In this chapter, the risk assessment process is described along with the methodology for the assessments. A comparison of the risk profile with just best practice controls and the differences introduced with using TPM is considered and discussed.

Chapter 7 – The author's view of the conclusions that can be draw from the study.

Chapter 8 – References used during this study

Appendices – Appendix A-D contains some of the supporting data used during the generation of this paper.

Appendix E – Includes the completed Project Description Form.

2 Data Sharing in Business

2.1 Introduction

This chapter sets out the wider context of why businesses need to share information and the types of information that is often shared when providing services to each other and their customers. A range of different mechanisms can be employed to facilitate information sharing which is also discussed.

The Data Protection Act (DPA) and Human Rights Act (HRA) set out the legal obligations that different parties have to each other when they share information. This paper discusses the effectiveness of the legislation.

This paper centers on the challenges faced by pharmaceutical businesses and the pharmaceutical industry. However in the author's opinion these challenges are common across different industries and Governments and therefore the considerations put forward in this paper apply more broadly.

2.2 Information Challenges Faced by Businesses

Pharmaceutical businesses face a number of challenges including fewer new drugs in the pipeline, greater competition, high cost of research and development, maintaining regional sales forces, long development cycles and maintaining robust internal structures to meet legal and regulatory requirements [1].

Pharmaceutical businesses can be considered a collection of business processes that operate to manage information and data to deliver new and improved products to customers. Therefore the management of information and data is a fundamental imperative for pharmaceuticals and indeed any business.

To maintain an effective operation whilst meeting the challenges of shrinking markets, tougher competition and the difficult economic climate, businesses are driven to look for innovative ways to minimise operating costs and reduce time to market.

One approach to achieve these strategic goals is the use of global sourcing [2] which involves working with business partners in different geographies to provide complimentary expertise, services, and products. This allows businesses to focus on core value added business activities and outsource non-core activities.

Forrester, a leading research organisation, calls these collaborative alliances, Digital Business Networks [3]. Using Digital Business Networks as well as existing business to business partnerships allows companies to embrace change and take advantage of the Global Market Place [3]

For example, pharmaceutical businesses core focus is on the development of medical products and it employs Information Technology (IT) to facilitate this objective.

These new business models require seamless business processes to cross national and international boundaries whist sharing critical business data with outsourcing Partners [4]. This is facilitated by stable network connections and the internet whilst potentially relaxing existing security controls at the perimeter to allow applications to work.

In the author’s opinion, there is a perception that using business process outsourcers and data processing partnerships is similar to purchasing any other utility such as gas or electricity. This perception is reinforced by new models such as Software as a Service (SaaS) where business use software as and when needed. The author believes, this may not be suitable for all services, especially when considering cost in the context of the potential impact on quality and risk.

In the authors experience such arrangements mean relaxing of security controls or opening more communication paths to allow poorly or indeed badly developed applications to operate, which ultimately places additional risks on the organisation.

For example, Oracle (a commonly used data base management application product suite) requires a large network port range to be opened in the firewalls because different functions select different network ports at the time of use. Therefore firewalls and intrusion detection systems need to accommodate this following a waiver from senior management to accept the risk. This is directly at odds with generally accepted good practice for applications to be restricted to selected ports [71]

2.3 What Data is Shared

Pharmaceutical organisation share a wide range of information between business partners to enable inter-organisational business processes to operate for competitive advantage.

The types of information shared include:

- Drug research data
- Clinical trials data
- Human Resources information
- Finance information
- Payroll details
- Competitor / Market Analysis data
- Sales and Marketing data
- Financial Market Data

The value of this information varies and in many instances can be considered trade secrets. For example drug trial data is collected from a large number of parties over long periods of time (sometimes between 10-15 years), from doctors, hospitals and development companies, etc.

The collection of this data must comply with regulatory compliance which serves to protect the integrity of the data being collected in an auditable manner. This type of exercise is costly and is commercially sensitive.

It is important to protect this information from unauthorised access or disclosure. If this information became accessible to unauthorised parties, then the consequences to the business will be extremely negative. For example, loss of reputation, share value reduction, loss of customers and their perception etc. Reputations can take many years to build but can be lost very quickly.

Much of the information shared by pharmaceutical businesses map directly to other private sector organisations where medical data can be swapped for other product information. The Government however differs from private sector organisations in the information it shares.

In a report produced in July 2008 by Richard Thomas, Information Commissioner and Mark Walport, Director of the Welcome Trust [5], where they looked at data sharing in the Government and the public services. They highlighted three major areas where data sharing plays a critical role in delivering public services which are the following:

1. Law Enforcement and Public Protection
2. Service Delivery
3. Research and Statistics.

Unlike most of the information shared by pharmaceuticals and private sector organisations, most of the information shared by the government departments relates to Citizen Information or Personally Identifiable Information (PII).

The broadest category of shared Government information is that of Service Delivery (2), and encompasses a vast array of different services (and related information) from a large number of public bodies as indicated below.

- **Local authorities**: council tax, housing, democratic services, education, libraries, social services, waste management and, environmental services

- **Departments, Agencies and Non-Departmental Public Bodies**: policing, court services, prisons, probation, medical records, self assessment and tax records, etc.

Following the Gershon Review [59] the Government is seeking to reshape itself to introduce greater efficiencies. Shared services have been identified by the Cabinet Office as a strategic approach to delivering these efficiencies across the Government as identified in the Transformational Government white paper [58]. This initiative highlights the streamlining of public services and corporate services such as HR, finance and procurement and targets £1.3billon of savings per annum by a 20% efficiency improvement. The Government is sharing information in vast volumes and this is expected to increase.

The author, agrees that sharing information across Government will bring valued added services for citizens but at what cost? The introduction of shared databases such as ID Cards and DNA has many opponents as these are considered steps towards the 'big brother' state. Recent news articles highlighting loss of PII data by the Government whilst trying to share information has left the public even more skeptical and dubious of the Governments ability to manage this national asset.

In the author's opinion, more protection frameworks are needed or existing protection frameworks need to become more robust. Only when these are in place can the public be assured that their information is being appropriately looked after.

2.4 Data Protection and Human Rights Acts

In the general activities of commerce and Government, data will be collected, processed and potentially sold on, for example the electoral roll information [6]. When data is shared the parties involved should be aware of their legal obligations relating to collection, storage and processing.

The Human Rights Act asserts that individuals have the right for personal privacy. The Data Protection Act (DPA) is a general act and is based on self regulation. It places obligations on organisations and individuals in the management and handling of personal data with emphasis given to ensure personal privacy is maintained and protected with data being collected and processed for a specific purpose.

For example, the Data Protection Act [7] and the Human Rights Act 1998 article 8 [8] are of particular interest to processing of medical health data in pharmaceutical data processing. A business is in breach and liable with respect to a patients rights if due care is not taken when the patient data is processed, stored and distributed.

As discussed in the previous section, global relationships are driving the need for cross border commerce. In this regard, concern has been raised about the legal implications of collecting, processing and movement of data between European member states saying "s*haring data across and between organisations can be a complex process*" with no single regulatory advice for data sharing ([5a] – Thomas and Walport).

To provide enhanced protection, organisations often use specific contracts with data protection provisions between each other that develop and clarify the principles laid out within the Data Protection Act (DPA) [7].

Whilst protection may be available, not all companies handle data in a careful manner. In the Thomas and Walport report [5b], The British Computer Society said "t*he enforcement mechanisms for the DPA are insufficient: breaches that may cause considerable suffering for individuals, such as damaged credit reference histories, rarely result in any meaningful penalty for data controllers*".

This was further reinforced by Richard Thomas, the information commissioner, at the European RSA conference, that his office was currently investigating 30 serious cases of breach [9]. In the author's opinion this appears to be a very small number of cases given the vast array of businesses that the DPA applies to.

Given the restrictions in the DPA with respect to use of gathered data, following the report on data sharing [5],[5b], the Government sought to allow for greater sharing by introducing a clause into the Coroners and

Justice Bill (Clause 154) allowing for data to be marked for sharing [71]. However the Government recently announced in an open letter from Justice Minister Michael Willis that this clause will be removed.

A quote from a privacy campaign group conveys the broader social dimension and tension in this debate on data sharing [71]. This quote was in response to Coroners and Justice Bill (Clause 154) amendment.

According to Privacy International's Director, Simon Davies: "*this is an extraordinary U-turn but we cannot be led into a false sense of security. We congratulate the Government on its decision, but it was inevitable given how badly the clause have been drafted and how morally corrupt its outcome would have been. Nobody should be under the illusion that the Government has changed its colours with regard to its zeal for surveillance. This could be merely a blip, so we all have to remain vigilant for the next assault of privacy*."

It is the author's opinion that the legal authorities and the Government recognise that existing frameworks for sharing are not sufficient or robust enough to hold up in court of law if tested.

The author's view is that the Government and private sector businesses need to do far more to control data with respect to the DPA and the current breaches are a tip of the iceberg, i.e. there are more breaches than is reported. The author believes many private sector businesses may treat data protection as a 'tick the box' activity in partnering relationships. The author concurs with the report [5] that the information commissioner needs more powers to ensure the legislation is taken more seriously. In support of the legislation is the need for practical technical solutions to support the legislative obligations.

2.5 How is Data Shared?

Businesses have a wide range of methods available to facilitate data sharing depending on the differing requirements. The method employed is very important as the method of transfer will in many cases dictate the level of protection afforded to the data. For example, people send an email which is similar to sending letters in the post with one critical exception – the use of a transparent envelope.

The methods of communication employed are driven by volume of data involved, timeliness, quality, availability, privacy and cost considerations. Mechanisms include dedicated network links; use of a Wide Area Network (WAN); use of the Internet (which is by far the most common method) to the physical transport of media.

In pharmaceutical businesses, data exchanges can occur daily via high speed communication links to transport high volumes of data. For example data extracted as a result of a DNA scan as part of research and development.

However, regardless of the method of transportation when human beings are involved in the process, a mistake or error of judgment can lead to data breaches as can be seen here [20] [21] [22] [24] [25] [26] [27]. Education on security matters is very important if an organisation wants to maintain it security posture and risk profile.

2.6 Summary

Public and private sector organisations are looking for innovative ways of improving business operations and processes using Digital Business Networks to gain competitive advantage. These networks form a web of connections sharing a wide range of different types of data in vast volumes. The data includes Personally Identifiable Information (PII) to sensitive company information which may have taken years to gather, for example drug trial information. This data becomes distributed across multiple Partners and therefore needs to be protected in a consistent manner to maintain integrity and confidentially.

Protection is provided by the Data Protection Act [7] and the Human rights act [8]. Both are concerned with maintaining personal privacy and ensuring data is collected, processed and stored in a lawful way.

All organisations including Government are mandated to comply with the Data Protection Act but in a self regulatory manner i.e. they must sign up the act and are responsible for reporting breaches. As a result, there have been few reported cases of data breaches from the private sector.

Data protection is critical to pharmaceutical organisations because they are obligated to follow regulatory practices with any breach leading to potential closure of business operations.

The public wants efficient public services and cost savings but they are reluctant to trust organisations including the Government with personal information given the recent data breaches, such as the high profile data breaches in the public sector which suggests that Government in particular is not ready to share data in large volumes.

The author believes stronger powers should be given to the Information Commissioner to conduct spot checks, audits and conduct investigations in both public and private organisations with significant penalties for breaches.

Organisations for their part should ensure contracts include clear unambiguous written agreements on data protection with specific clauses, setting out the agreement on regular reviews of information security to be carried out as part of the relationship.

3 Managing Trust

3.1 Introduction

This chapter considers how trust is generated within business partnerships and the consequences of losing trust including exploring some of the human factors in these relationships.

Consideration is given to some of the methods available to build confidence and trust between partners as well as exploring some of the challenges and issues with those approaches.

3.2 Trust in Business Relationships

It was once said to the author "*Trust takes a lifetime to build but can be lost in a flash*". For example, a family member may be trusted to not steal your bank details and use it without your permission, but if they did would your trust in them to the same level as before?

With the banking crisis, pensioners have lost a huge proportion of their savings [12] when they entrusted their money management to large established banks only to find those organisations took advice from other established organisations without questioning the validity of what was being offered.

Given that trust is so fragile and fundamental requirement for humans, it is not a surprise trust levels cannot be maintained when things do not go as expected. Both the pensioners and the family member will think twice and have lower confidence in engaging in a similar situation.

Public trust and confidence in the current economic climate is very low given recent news events, for example the Northern Rock crisis [12] highlighted the effect a news story has on a bank when people started to queue to withdraw their money, the government had to intervene to restore order

Trust in the bank may have been founded on reputation, recommendation from a trusted source or from independent statistical information setting out past performance. Statistical information from independent parties instills more confidence within the receiver than statistics produced by public bodies, businesses and Government. This is confirmed by a report published by the Office of National Statistics [10], a quote from the report conveys this sentiment "*Participants emphasised that the independence of statistical services was one of the most important factors for ensuring confidence in statistics.*"

The principle of buyer be aware applies in all situations when dealing with banks, which in business would translate to *due diligence,* using some of the methods discussed later in this chapter.

Another story [13] reported an alleged problem with a drug produced by a pharmaceutical company which resulted in the news article stating "*Investors, doctors, patients and medical malpractice lawyers are watching closely what steps legislators and regulators will take*."

This may not sound very serious until consideration is given to the amount of money this drug produces for the business which was reported to be above $3 billon dollars. Should shareholders perceive this company as a bad investment and lose trust and start to sell their shares then this can have a significant impact on the organisations. Indeed, as a result of this article, the company's value on the stock market dropped by $1 billon dollars in four days and was continuing to slide. This highlights the importance of trust through brand loyalty, reputation and public perception.

Given the importance of trust to all organisations and its fragile nature, it is critical that businesses protect the trust that their business Partners and customers place in them. Establishing a common understanding in Partnerships and rules of engagement is critical to the success of the business and the Partnership.

There are many methods available that serve to highlight to existing and new business Partners and customers that confidence and trust can be given in working with an organisation. Some of the approaches available include:

- Contracts
- Accreditations such as BS ISO/IEC 27001.
- Audits
- Site visits and Inspections
- Review of Technical Controls
- Questionnaires
- Interviews
- Due Diligence
- Reviewing Internal Partner Processes such as Change Management, Incident Management and Problem Management.
- Information Security Heath Checks
- Risk Assessments
- Team Building Events
- Recommendations from other Companies
- Performance Reviews against Key Performance Indicators (KPI)

There numerous resources available where further information can be found, for example BS ISO/IEC 2005:2008, and BS ISO/IEC 27001 &

27002. This paper discusses a few of these in the following sections to outline some of the challenges.

3.3 Challenges to Establishing Trust

The methods listed in the previous section all help in the establishment of trust and assurance in a Partner and they in the business; given it is a two way relationship. Not all of the methods are deployed in every situation and the methods will not solve all problems but used in a collective way will go some way to establishing trust.

Businesses have many relationships with Partners to support their operational activities, so any management of these relationships has to manage factors such as locations, resources and skills to ensure the relationship runs smoothly.

At an open industry forum held in December 2008 in London to discuss "Outsourcing and Third Party Security Risks" [14] an attendee said "*We have 18,000 suppliers and share data with many of them*". This particular attendee was highlighting that it is not possible to check every partner on a regular or annual basis, so alternative approaches would be welcomed.

The author suggests a risk based approach to prioritise activities is employed to make use of limited resources.
The following sections review a few of the most commonly used approaches to establishing trust and some of the considerations in these methods to highlight potential issues where trust can be affected.

3.3.1 Contracts

This section discusses the key points in the contracting process and puts forward the author's views and experience with respect to challenges in managing a data sharing relationship. It is not intended to be a legal narrative.

Contracts set out the obligations, accountabilities and responsibilities (through express and implied terms, exemption clauses, outline of service levels, etc) between a business and its Partner. These clauses need to be understood by all parties and an agreement reached on escalation and dispute resolution mechanism in case something goes wrong. The contract is usually agreed between senior managers from the business and the partner.

In the author's view a number of problems creep in to the contract due to the process by which the contract is drafted and the importance placed on information and data security. These problems often surface when the relationship is strained and one party reaches for the contracts folder only to be surprised by the content and its implications.

At the time of drafting a contract is a critical focus when all parties are very keen and flexible in their dealings with each other. A discussion takes place between business managers who have a need that is addressed by the Partner and are keen to strike a deal.

Information security is often not considered unless an organisation is mature from an information security perspective and has the relevant resources. An appropriate information security specialist may be engaged however this is often seen as a low priority and often not regarded as a deal breaker should problems be identified.

The Partner will not spend money improving information security when the contract does not mandate for it to happen. Ultimately, should this be mandated, the costs would be incurred by the business through service charges.

Whilst contracts offer a means of establishing trust and control. Contracts are signed by senior managers however the operational aspects of the Partnership are managed and operated by staff who have limited or no visibility as to their responsibilities which can cause problems for the relationship.

The author asserts that in many cases the clauses are generic to a point that any breach of information security becomes unenforceable; in which case the parties accept the failure and hope they can improve the process in future.
Should the breach be very serious then both parties may resort to legal means to get a resolution, which will only sour the relationship and place both organisations into a position where trust is lost.

This brings into focus, who is taking the risk when a breach takes place. The author suggests that the business is taking the risk as it has a reputation and a brand value to protect. Therefore it can be argued that the business needs to take extra care in these relationships. Contracts may not always provide the redress to certain situations.

For example, in January 2009, a provider of outsourcing services was hit by a scandal of corporate fraud [66]. Businesses were not able to exit from this relationship in a controlled manner and had to obey the contracts in place. This sent shock waves through the corporate community who started to look at ways of managing this risk and therefore this undermined trust.

3.3.2 Accreditation to BS / ISO IEC27001:2005 & 27002:2005

The BS / ISO IEC27001:2005 & 27002:2005 standard is provided as guidance to businesses to measure their security practices and draw guidance on controls that need to be implemented. The standard offers categories of risk and controls which should be implemented as appropriate for the organisation.

Previously the standard was called BS7799. During this time, many organisations seeking to implement Information Security Management Systems (ISMS) found it difficult to interpret and apply the standard as it was set out in a blueprint form, whereas the current standard is more practically set out as guidance.

In the author's opinion, a business entering a Partnership should review the application of the generic controls to ensure they are justified and must be documented in the *statement of applicability* as it applies to the Partners business. Therefore when a partner claims compliance a complete review of the process and on going management practices should be conducted. The standard requires continual application by the Plan, Do, Check and Act cycle to ensure the standard is used as intended and is not a one time event.

Furthermore, checks should be made on the application of controls within standard. This does not refer solely to the technical controls on a data sharing relationship but sections 5-15 of 27002:2005 are of particular importance and should be used as a guide during reviews and audits.

The authors acknowledges that this is a good standard deployed in excellent ways by many businesses however for the purposes of due diligence, the author suggests an expedient way to check compliance may be to contact the company who carried out the accreditation review.

3.3.3 Audits

Audits are a helpful way to establish if a partner is doing what they have documented or agreed with the business. Audits are reliant on documented processes, procedures, local instructions, Service Level Agreements (SLA) and Operational Level Agreements (OLA) as well as industry best practices to which an audit is performed against. The implied view is that if something is not documented then it is not being performed. The author views this as rather short sighted, however it does help to define a baseline which reviews can be conducted against.

Businesses have internal audit functions to maintain compliance and ensure regulatory oversight. However this does not mean everything is reviewed and highlighted for remediation. When it comes to auditing a Partner, this may be done by site visits; questionnaires; interviews; inspection of processes and procedures. These are often carried out under heightened circumstances which are outside of day to day activity i.e. partners will be more alert and attentive during these inspections, so a business may not always see a true picture of the operation.

Consideration should be given to how often the audit will be carried out. In any Partnership, if this is done too often it will erode trust and mutual respect and too seldom may mean issues will turn into incidents. This must be managed appropriately and set out in a formal contract which will introduce an element of legitimacy to the process without making any parties feel uncomfortable as this will be agreed in advance.

The key issue here in the authors view, is that audits are essentially probing and recording activity a Partner may be providing over a short duration, possibly a week or two. Therefore it may not be possible to interview and talk with all staff to get their views. It is also normal when conversations are being conducted with operational staff; a request is made which allows the Partner to select the best person for the interview and not the other members who may not be appropriately trained.

The author recommends that to build long term mutual trust an audit should be conducted in a fair and collaborative manner. This assists in dispelling negative view of an audit but one must remember the audit in a Partner relationship is effectively the customer making a spot check so that everyone will be on their best behavior.

3.3.4 Review of Technical Controls

There are numerous security products on the market, ranging from risk management tools to end point protection. A US security research organisation (CERT) published a report [16] which surveyed 671 security executives and law enforcement officers who highlighted their top 10 most effective controls and their deployment (%):

1. Stateful Firewalls (82%)
2. Access Controls (79%)
3. Electronic Access Controls (78%)
4. Application Layer Firewalls (72%)
5. Host based Anti-virus (70%)
6. Password complexity (70%)
7. Encryption (69%)
8. Heuristics-based SPAM filtering (69%)
9. Network based Policy enforcement (68)
10. Network based anti-virus (65%)

The author suggests whilst these are very effective controls, they must be underpinned with effective processes and training for staff operating these controls. This means simply deploying the controls is not enough in itself unless processes are there to inform staff on how to respond and take action when something is spotted beyond expected activity.

Another issue with these controls is that they are often reliant on automatic alerting of events based on thresholds or signatures because appropriately trained staff often have limited time to review the large amount logs generated. Therefore a targeted attack by a skilled attacker will slip under the radar because the automated system may not have the ability to detect or respond.

There is a perception that deployed controls are capturing all security incidents which is leading to a higher level of confidence. The same report [16] has highlighted over confidence amongst the respondents although the survey suggested e-crime being consistently steady in 2007 against the previous year. A similar survey by BERR [17] suggests 87% of respondents are confident that they had caught all the significant security breaches.

The author is surprised by the level of confidence from respondents. On what basis have these judgments been made? The author believes the lack of incidents detected within the organisation is creating this false sense of security. There seems to be a misconception amongst technical security professionals that one can deploy a technology and it will provide total protection. What is not taken into consideration is that people and processes are the other two factors which need to integrate into the security program.

For example, insider attacks may be an issue, 67% of respondents were affected by an insider outlined in the Cert report [16]. However, the emphasis is still on the outsider being the attacker.

In an article published by the Jericho Forum [15], John Arnold, chief security architect, said "*Trust cannot be developed using technical security concepts alone; it must come from examining how humans create trust.*"

Although the list above seems to ticks all the boxes, the author would like to re-iterate that not everybody manages controls in the same manner; there may be Partners who simply deploy the technology. The author recalls a story by a SANS auditor, who when auditing a business asked an analyst if they had a firewall to which the reply was yes. When the SANS auditor asked to see it, he was taken to a cabinet where sure enough there was firewall but it was still in its box. This illustrates the how security professional or senior management may not take security threats seriously because nobody followed up to ensure the firewall was installed.

This conveys the need to ask the most appropriate questions at all times when visiting a Partner. In the data sharing relationship, there needs to be an oversight as to how these controls are being used and where they are being deployed. This will create a true picture of what the risks are to the data.

3.3.5 Penetration Testing Partner Systems

Penetration testing is a process where a vulnerability scanner will scan a particular host or network in order to find any issues with servers, routers, firewalls. Normally this is conducted on perimeter devices facing the internet. However, there is no reason why a penetration test cannot be conducted against internal systems (systems processing the business data).

A test performed with a quality tool or free tools run by an experienced penetration testers should give additional assurance of system soundness at a point in time. There are lots of commercial tools available for this type of testing.
New vulnerabilities are emerging on a regular basis, so the check can only be performed at point in time. This is similar to getting an MOT carried out on car; as soon as you leave the garage it could be invalid.
Penetration testing is good check for system vulnerabilities but it must be stressed that it’s only an indicator and should not be relied upon without further checks such as access controls mechanisms.

3.4 Summary

In this chapter, the author highlighted the need for establishing trust in a business relationship and some of the foundations which could be used to build that trust.

Managing trust is a difficult concept with businesses using contracts, audits, accreditations, technical controls etc to develop levels of trust.

Each mechanism has its difficulties which the organisation needs to be aware so that it can choose the most appropriate way to build trust with its partners.

For example, contracts may not have appropriate clauses for data protection; technical controls may not be managed appropriately allowing breaches to take place; accreditations may not include an appropriate scope leading to security weakness in organisational controls.

Trust needs to include clear lines of responsibility and accountability to be effective along with agreements on how to deal with issues when they arise.

Building trust is a fragile business and needs to be handled with due care and diligence because a failure may affect organisations internally and externally and trust is very difficult to regain once it is lost.

The author concludes, that trust is difficult to establish and maintain in these relationships and needs to be treated with care and thought.

4 Computer Security Landscape

4.1 Introduction

This chapter outlines the current situation surrounding computer security. In particular, what Government is doing to protect citizens, what challenges businesses face and how they are addressing the issues.

It also looks at some of the issues organisations face from the constant internet connection used by the employees including insider threats, e-crime, de-perimeterisation, software testing and development, recommended security controls and the legal framework available for addressing technology related crimes.

4.2 Changes in the Computer Security Landscape

4.2.1 Always Connected

Computers have become part of our everyday lives, from using them for keeping in touch with family and friends to selling goods on the internet. Whilst a home user may live without the use of a computer for while, businesses on the other hand reply on it for their survival. A business uses computers in its processes and serving its customers. Any disruption could cost an estimated £80K to £130K for large businesses and around £8k-15k for small businesses [17]. A 2008 survey by BERR, found “84% of companies relied heavily dependent on IT systems” and of those surveyed, “77% saw protecting customer data as very important” [17].
Governments and business see information as the key to economic and business success therefore ensuring measures are put in place to encourage and facilitate that strategy.

There are the usual data loss stories in the press [25], [26] ,[32] which bring this to the attention of the public and makes the public worry where their data is kept, who is protecting it and if they will become the victim of an e-crime such as identity theft. This current trend is set to continue according to the SANS top 10 trends [68]. These loses affect an organisations reputation and standing in a competitive market place.

Computers and information systems are not only targeted by criminals [31] and insiders [30] but also vulnerable from malicious code such as viruses, trojans, spyware and program flaws [32] including buffer overflows [34]. Secure coding practices [35] can help but they will not cure all the problems.

Given this and the belief that 34 million computers are installed with fake software [33],[32], it is no wonder that companies are seeking new ways to combat these problems before they become at risk of going out of business

4.2.2 The Insider Threat

The internet and the continued drive for better, faster, cheaper products and services has seen an explosion of companies (six out of seven large companies off shoring IT operations [17]) looking for better ways of managing business operation leading to insider threats from internal employees and partner employees based within the same physical location .

Businesses are deploying a range of tools and technologies such as database security products, personal firewalls, patch management systems, host intrusion prevention systems, endpoint data protection and desktop encryption to protect against insider and outsider threats as outlined in [30].

In the authors view, these tools cannot always be effective in prevention or detection by automated tools with reliance on signatures and behaviors. The logs generated daily by technical controls are very large. In addition, skills for analysis are stretched with analysts not having enough time to review all alerts because they have to deal with operational issues

An extract from the 2007 E-Crime Watch Survey [16] is provided below:

"*It is important that organisations are proactive in their approach to mitigating insider threats," says Dawn Cappelli, Senior Member of the Technical Staff at CERT. "Defense in depth isn't just about putting adequate technology in place, it's also about paying attention to your people and implementing policies and procedures to reduce the likelihood of an insider attack. Our research has shown that those very policies and practices that respondents are cutting back on are critical in mitigating insider threats.*"

This is further compounded with the knowledge that roughly the same numbers (insiders 34%, outsiders 37% [16]) are involved in e-crime however emphasis is still more focused on the outsider. This may be as the author suggests attributed to political and human resource management considerations i.e. one does not want to upset the workforce by accusing them of potential wrong doing. The 2007 E-Crime Watch Survey suggests 58% [16] of businesses are reliant on good policies covering employee terms and conditions in tackling insider crime but will this be effective in the long term as staff turnover increases? The author suggests that loyalty, contracted staff and short contracts make this method of control via policies ineffective as there is no incentives for a staff member follow them.

Insiders have access to local disks, USB drives, email, instant messaging and other mobile devices. Given that 36% of information theft is carried on mobile devices [16]; we can say this trend will continue at the current levels or even increase given the current state of employment practices.

The author also suggests, from a business perspective employee's could be targeted by competitors for their access to data and knowledge of a business.

This breeds the environment of insider attacks and develops motivation for the information security breaches and intellectual property theft.

4.2.3 E-Crime

The government is a large user of information systems as discussed in the data sharing chapter and clearly understands the risks posed by new business models; it too has been busy putting measures into place to protect national interests [61]

For example, the public are fully aware of internet card fraud... In 2008, it was reported £328m was lost from non card transactions

Extract from the article [61] "*Britons face a growing online threat from criminals, terrorists and hostile states, according to the UK's first cyber security strategy*"

Gordon Brown, – UK Prime Minister, wants the UK to lead the way on digital technologies and he wants every household to be connected to the internet. But he is aware that criminals will seek to exploit these situations that have currently amassed a £50bn industry and using it for organised crimes and terrorist's activities.

In light of this concern, the UK Governments is recognising the threats and opportunities that could affect the UK economy and now setup e-crime strategies [17] across the UK as well as national critical infrastructure protection programmes.

The Serious Organised Crime Agency [19] and the Home Office understand old crimes are being committed in new ways by criminals across all sectors and have led to the creation of an e-crime strategy [28].

With all these initiatives, the question is will they be effective? Initiatives need to be coordinated to be effective in tackling electronic crime. For example, information must be shared between groups in a sensitive manner taking into account individual privacy concerns. Any enforcement action needs to be measured and not sensationalised in the press.

There needs to collaboration to fight other forms of e-crime such as intellectual property theft and copyright etc.
The author also suggests assistance should be given to private companies in dealing with e-crimes as most of them are dealing with it internally (66% [16]). But they may not be following good practice or the correct legal framework which could open themselves up for litigation from employees or partners. According to 2007 E-Crime Watch Survey [16] 34% of them said they did not have enough evidence. Are they following correct evidence collection procedures?
For example, what steps would a business need to follow in the event an employee downloading inappropriate content or copyrighted material claiming their account was compromised?
A framework for processing these types of events would be useful suggests the author.

The author believes this highlights a greater issue around the lack of forensics expertise in businesses. This has to be addressed going forward, especially in large businesses where there are globally diverse operations and requirement is greater.

Forrester [60] suggests malicious code is on the decline and security directors have failed to adapt and still focus on viruses, worms and spy ware. The author disagrees as there are continual malicious code events being generated as reported [16]. The reason maybe related to the ineffective detection methods hence the security directors have not changed their focus. One can argue that security directors have become more reliant on technology due to resource pressures. One can also argue, the perceived outsider threat is more then the insider threat which would be at odds with the deployment of data loss protection tools.

4.2.4 De-perimeterisation

The emergence of new business models is driving the adoption of a de-perimeterisation business infrastructure where traditional controls compliment new controls on the data as advocated by the Jericho Forum [29].

The author suggests, there is a shift from perimeter security controls to more localised controls on the data itself; however, existing controls will remain in place for the foreseeable time.

New type of controls such as data security products (protecting databases), application firewalls (protecting applications) and more general end point protection products are being deployed to protect data in use and at rest.

However, this raises two issues with this new approach. Firstly, security directors are not getting enough funding and resources to enable this new of model working with appropriate staffing and tools. This in turn leads to stretched resources with the business benefiting from de-perimeterisation but not the considering the costs for the added flexibility.

4.2.5 Software Development and Testing

Software development has been trying to address errors in programmatic code by programmers but little progress has been made.

SANS highlights its top 10 coding errors [67] which led to the need to have systems patched on a regular basis. These errors can be used as a mechanism for exploiting systems. Once again, the author would like to highlight these errors types have been around for years which leads to asking the question. Why?

One explanation is that programs are filled with thousands of lines of code along with lack of security awareness amongst developers, lack of quality checks and pressure to develop products faster and faster.

So developers cannot be expected to know every usage of a piece of code, however training courses have emerged to help educate developers.

4.2.6 Security controls

The current level of crime inside and outside a business is not on the decline. What controls should be deployed? The author refers to SANS a respected security organisation, has recommended their 20 controls (these include controls relating network, platform and software vulnerabilities) which should be implemented to mitigate risks [67]. The author notes that we have not come very far as 18 of the recommended controls have been round for a sometime except Data Loss Protection and Application firewalls. This conveys the idea that organisations are protecting data and their web applications from harm.

These controls rely on signatures and behavioral type controls which could be circumvented by a skilled attacker or be missed by an inexperienced analyst, so training is important.

4.2.7 Legislation

The emergence of criminal activity also saw the emergence of three acts to give the courts more powers to deal with such offences. These acts are the Computer Misuse Act 1990 [62], Data Protection Act [63] and the Regulation of Investigatory Powers Act (1990) [64]. This means law enforcement now have a tools to deal with computer crimes although it must be noted these are complimentary to other laws such as i.e. copyright laws, fraud act, theft act, obscene publications act.
Although computer crimes laws can be applied to cases, it does not mean other laws cannot be applied. On occasions an existing law can be applied to bring a prosecution. However, as mentioned earlier, evidence must be collected in an appropriate manner to be admissible.

4.3 Summary

The security landscape has changed over the last few years as businesses look for new innovative ways of working. Threats can arise from insider or outsiders; in fact the differential between the two is small.
Organisations are engaging in collaborations across open networks like the internet which also has its threats. As a result, the controls landscape is changing from perimeter controls (de-perimeterisation) to more local controls on the data allowing many connections to the data to facilitate digital business networks and outsourcing.
Organisations are very aware of insider threats in these seamless models of business connectivity, so started to deploy all kinds of controls and placing reliance on automated tools for log management and intruder detection. Automation tools are not optimal suggests the author because attacks are only measured against known attacks or signatures / behavioral patterns.
To address insider threats from employees, organisations are using employment contract policies as a preventive measure to encourage staff not to engage in acts against the organisation.
Errors in software have not stopped despite awareness of the security flaws in programming practices. Some organisations have started to develop secure coding training courses to reduce the number of errors leading to security vulnerabilities.
Governments have recognised the threats to the public from e-crime and have setup a number of initiatives to compliment current laws in fighting e-crime.
Private businesses not having the resources of the Government but could do with assistance and support in developing forensics skills to aid appropriate handling of e-crimes within an organisation.

5 Trusted Computing

5.1 Introduction

This chapter provides an overview of trusted computing and the components of a Trusted Platform Module (TPM) as well as outlining why the TPM can be trusted. A model for B2B data exchange using trusted computing technology will be presented with an explanation of how trusted computing can help reduce risk. This will aid the reader in understanding this study and set context for the ensuing risk assessment.

5.2 Trusted Computing and it's Benefits

Graeme Proudler [39] outlines that it is safe to trust something when:

- (it can be unambiguously identified)
- and (it operates unhindered)
- and ([the user has first hand experience of consistent, good, behavior] or [the user trusts someone who has provided evidence / references for consistent, good, behavior])

Trusted Computing refers to a computer system for which an entity has some level of assurance that (part of or all of) the computer system is behaving as expected [39]. This is implemented by using the services of a hardware component (chip) called a Trusted Platform Module (TPM) which measures the software components on a computing platform using a range of cryptographic services.

The original specification for the TPM was developed by the Trusted Computing Platform Alliance as outlined by Pearson [36], the current specification for the TPM is being developed and maintained by the Trusted Computing Group (TCG) [37] whose members include major vendors in the computing technology market driving its adoption including Microsoft, Intel, HP, IBM, Sun Microsystems as well as others [38]. The goal is to improve trustworthiness on information systems including PC, Laptops, servers, networks, mobile and storage systems.

Trusted computing benefits include (as presented on the TCG website):

- Protect Business Critical Data and Systems
- Secure Authentication and Strong Protection of User IDs
- Establish Strong Machine Identity and Integrity
- Ensure Regulatory Compliance with Hardware-Based Security

- Reduce Total Cost of Ownership Through "Built In" Protection

The TPM chip is included on the motherboard of a platform along with the BIOS to form what is called the *Root of Trust* for all trusted functionality.

5.3 Overview of the Trusted Platform Module

This section sets out a simplified explanation of the services provided by a TPM within a Trusted Platform, and aims to support the discussion set out in the paper. For a detailed explanation of Trusted Computing refer Mitchell [11], Pearson [8], Challener [12], Eimear Gallery [39] – chapter 3.

A TPM has three critical functions called *Roots of Trust* which must behave as expected because their misbehavior cannot be detected and therefore these form the foundation and constant for the solution.

The Roots of Trust are embedded within the TPM and are responsible for reporting, gathering and storage of evidence about the trustworthiness of the platform software environment, and therefore must be trusted otherwise the whole TPM creditability and assurance in its measurements are not possible. These roots are explained below along with other TPM components relevant to this paper.

5.3.1 Key Functions of a TPM

This section introduces the key functions of a TPM which include:

- Core Root of Trust for Measurement (CTRM)
- Root of Trust for Measurement (RTM)
- Root of Trust for Storage (RTS)
- Root of Trust for Reporting (RTR)
- Platform Configuration Registers (PCR)
- Endorsement Key Pair (EK)
- Storage Root Keys (SRK)
- Attestation Identity Keys (AIK)
- Binding
- Sealing
- Migrateable Keys
- Non-Migratable Keys

Core Root of Trust for Measurement (CRTM)
This starts the boot process. This code is contained in the BIOS Boot Block and measures itself and the BIOS then stores the values into a PCR before passing control to the next piece of code.

Root of Trust for Measurement (RTM)
This is trusted to make reliable integrity measurement of software / firmware after a platform reset (maybe a partition as in a virtual machine or the platform itself i.e. a power cycle).

Root of Trust for Storage (RTS)
This is trusted to store integrity measurement recorded by the RTM into the Platform Configuration Registers (PCR).

Root of Trust for Reporting (RTR)
This is trusted to report the integrity metrics to a third party requesting to know the platform state / PCR values stored by the RTS, along with a log of the components on a platform. This log is referred to as the Stored Measurement log (SML) and stored outside of the TPM.

Platform Configuration Registers (PCR)
The registers inside the TPM are used to store integrity metrics provided by the RTM (20 bytes of data per register). These metrics are essentially hashed measurements of software components on a trusted platform. This is a critical function.

Endorsement Key Pair (EK)
This is unique for every TPM and serves the requirement - “it can be unambiguously identified “. This key pair is only used for encryption / decryption purposes and is critical in the creation of Attestation Identity Keys (AIK). The Private Key never leaves the TPM or revealed outside the TPM. This key pair is generated by the TPM manufacturer in commercial platforms.

Storage Root Keys (SRK)
This key is created when a TPM ownership process is invoked which requires physical presence and is separate from the EK. This key is used to protect other keys in the created by the TPM.
Physical presence is required when taking ownership of a TPM. It is a measure to stop rouge software taking ownership of a TPM by remote means. This key is used to protect other keys generated by the TPM.

Attestation Identity Keys (AIK)
These are identity key pairs created for different purposes and attest to belonging to a TPM but do not give away any TPM details. This is carried out using a Privacy Certificate Authority (P-CA) who signs the public key of an AIK after confirming the AIK came from a genuine TPM by verifying a series of TPM credentials.

Binding
By using a TPM Bind key, external data can be encrypted such that it can only be decrypted by another TPM with specific authorisation data.

Sealing
Sealing is a process of encrypting data to specific TPM PCR measurements. Conditions can be set so that the encrypted data cannot be decrypted unless those specific PCR measurements are present, i.e. the platform has to be in a particular configuration state.

Migrateable Keys
Migrateable Keys can be migrated away from a TPM assuming the correct authorisation data is available. This allows keys to be stored in a different location for safe keeping.

Non-Migratable Keys
Non-Migratable Keys cannot be migrated away from the TPM. An example could be the private endorsement key of the EK.

The are other components within the TPM such as I/O; Non-Volatile (NV) storage; Random Number generator; Opt-in, RSA Engine, SHA-1 Engine, Execution Engine and Key generation capabilities which are used to provide TPM services including the Roots of Trust.

5.3.2 The Authenticated Boot Process

The importance of the Root of Trust concept is critical to Trusted Computing and can be better understood during the authenticated boot process.
Figure 2 outlines the information flow and integrity measurement during an authenticated boot up of a platform containing a TPM. It shows how measurements are conducted and stored using a cryptographic hash function.

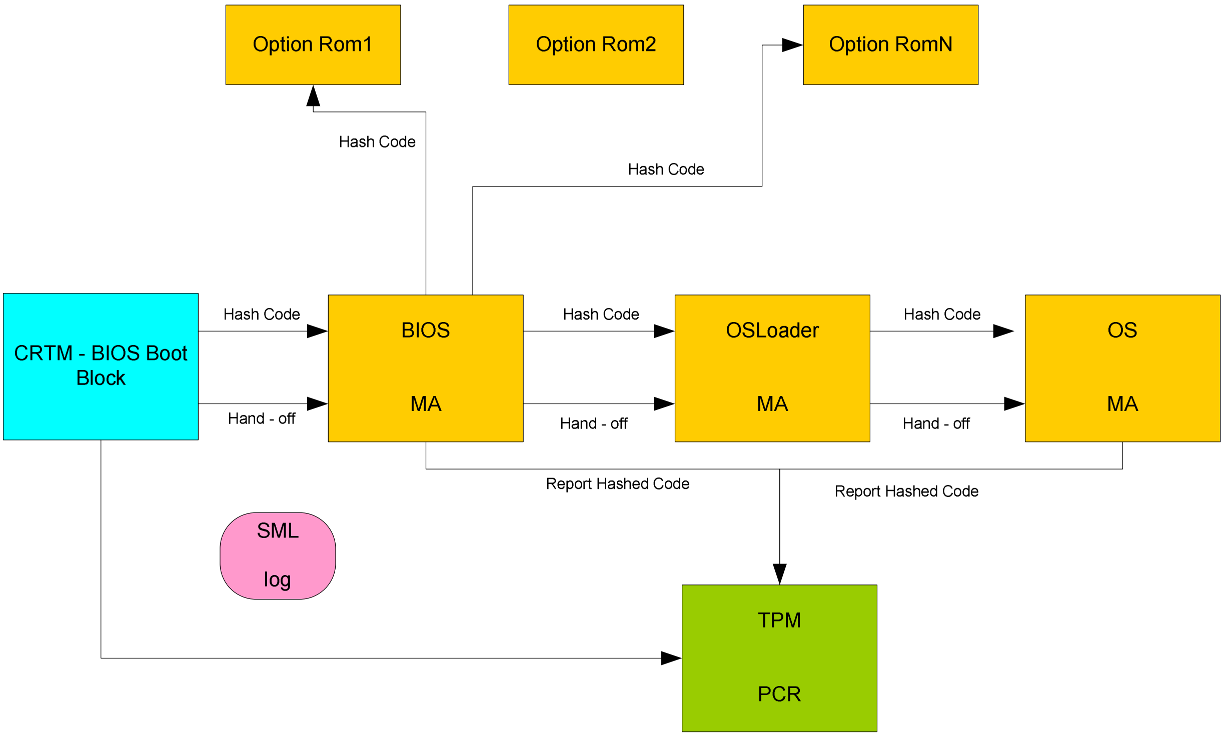

Figure 2: Authenticated Boot Process.
Source derived from: Royal Holloway - Trusted Computing Lecture Notes

In a PC, where the Core Root to Trust Module (CRTM) may be integrated into the part of the BIOS called the BIOS boot block (BBB), integrity metrics may be measured and recorded as follows:

- The BBB (the CRTM) starts the boot process, measures its own integrity and the integrity of the entire BIOS, and stores the details of the measured components in the Stored Measurement Log (SML), saving the integrity measurements (hash values of the component measured) in a TPM Platform Configuration Register (PCR);

- The BBB then passes control to the BIOS, which contains a Measurement Agent (MA) responsible for measuring the option ROMs, storing the details of the measured components in the SML and the integrity measurements in a TPM PCR;

- Control is then passed from the BIOS to the option ROMs, which carry out their normal operations and pass control back to the BIOS;

- The BIOS then measures the OS Loader, and stores the details of the measured component in the SML and the integrity measurement in a TPM PCR;

- Control is then passed to the OS loader, also containing an integrated MA, which carries out its normal functions and then measures the OS, stores the details of the measured component in the SML and the integrity measurements in a TPM PCR;

- Finally, control is passed to the OS.

The authenticated boot process ensures all components are measured and kept in PCR's so these measurements can be provided to a third party when requested. PCR values for software present on the system will also be recorded and released to third parties upon request. The third party then has assurance that only software outlined in the SML and PCR are present on a system and not some other code.

5.3.3 Isolated Operating Environment

Trusted Computing using a TPM allows for the operation of an isolated operating environment which can sit inside a host and process data without being affected by the remaining platform.

For example, a virtual machine running one application can be created purely for processing data and be protected from other environments physically on the same machine. These environments use the latest processor extensions to facilitate their operation. Integrity measurements stored in the PCR can be provided to a remote challenger for verification.

5.4 Why should a TPM be Trusted?

A TPM is manufactured in controlled and secure environments by manufacturers with strong brands to protect. The TPM is a security chip produced and distributed as something which should be trusted. Any adverse publicity would damage brands, present legal issues as well as affecting their reputations as businesses. The Trusted Computing Group (TCG) has developed a number of signed credentials and outlined a deployment process for all TPM manufactured to their specifications. In particular, there four credentials that vouch for the trustworthiness of a TPM:

1. **Trusted Platform Module Entity (TPME)** – This is usually the manufacturer of the TPM who signs the public key of the EK to confirm the TPM is genuine.

2. **Conformance Credential (CE)** – Guarantees the Trusted Platform design and the design of the TPM conforms to the TCG specifications.

3. **Platform Entity (PE)** – Gives assurances that a particular platform is an instantiation of a Trusted Platform design as described in the conformance credential and the platforms TPM is genuine. This is usually the original equipment manufacturer.

4. **Validation Entity (VE)** – Certifies integrity measurements of embedded data or code such that a challenger can use the measurements as means of validation of the programmes or data.

5.5 Establishing Trust on a Remote Host

This paper is concerned with data confidentially and integrity within B2B data processing relationship. The service user needs to be sure the remote partner is operating an environment which is approved by the service user. There is a need to obtain an integrity report which can be verified against known integrity measurements provided by a Validation Entity.

Figure 3 below outlines the communication exchange between two parties establishing a data processing relationship. The service user seeks to confirm that the service provider is using a specific configuration before sending any data for processing.

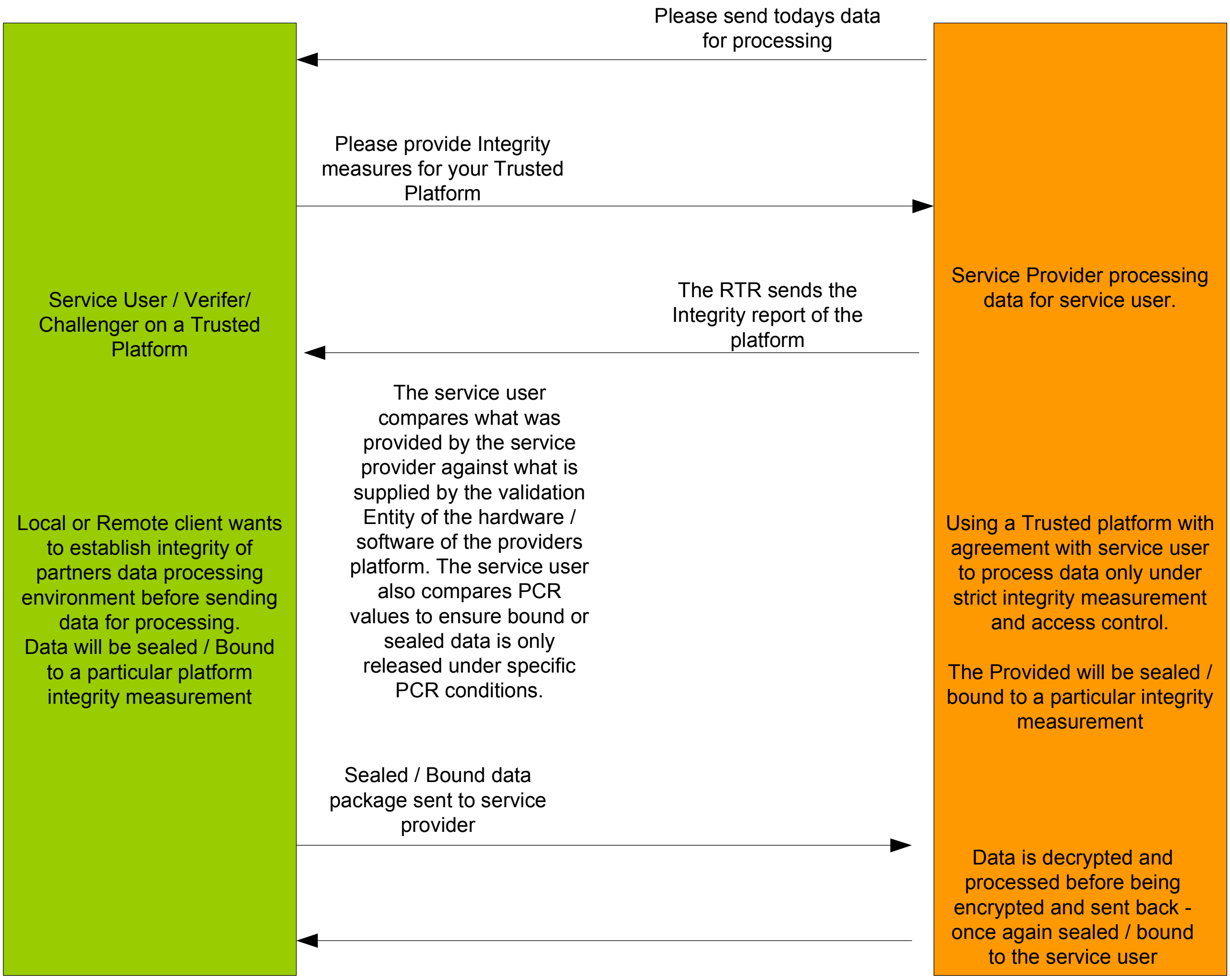
Please send todays data for processing
Please provide Integrity measures for your Trusted Platform
Service User / Verifer/ Challenger on a Trusted Platform
The RTR sends the Integrity report of the platform
Service Provider processing data for service user.
The service user compares what was provided by the service provider against what is supplied by the validation Entity of the hardware / software of the providers platform. The service user also compares PCR values to ensure bound or sealed data is only released under specific PCR conditions.
Local or Remote client wants to establish integrity of partners data processing environment before sending data for processing.
Data will be sealed / Bound to a particular platform integrity measurement
Using a Trusted platform with agreement with service user to process data only under strict integrity measurement and access control.
The Provided will be sealed / bound to a particular integrity measurement
Sealed / Bound data package sent to service provider
Data is decrypted and processed before being encrypted and sent back - once again sealed / bound to the service user

Figure 3: Communication exchanges in B2B data processing using Trusted Computing

The exchanges illustrated in Figure 3 can occur locally inside an internal network or over communication lines using secure protocols over open networks such as the internet via SSL/TLS making it widely applicable.

5.6 How does Trusted Computing Help

Many organisations including pharmaceuticals businesses, heath departments, hospitals, Governments often want to restrict or keep secret information from employees, competitors and Partners depending on the circumstances. However data can leak any numbers of ways including by removal media, email, taking screen grabs etc.

As an example, The Health Insurance Portability and Accountability (HIPAA) regulation makes it an offence to release medical records to an unauthorised person [13].

In a business to business data processing Partnering relationship, using trusted computing technologies an environment can be created on the partner site or internally locking the data to a particular platform state and even then only allow restricted access to the processing application.

Other applications of Trusted Computing include OS functions where unauthorised users would not be allowed to access data whilst the data is processed in the decrypted form. This would be achieved by the use of secure drivers which for example may not allow copying of memory locations to another location i.e. cut & paste in Windows. This however does not protect against somebody taking pictures of data from the screen using a mobile phone with a camera.

Trusted Computing allows for the creation of secure environments where the data owner sets pre-conditions as when and how their data will be accessed and by whom.

Having this level of control is clearly powerful and reduces if not eliminates activity as a result of malicious code, viruses, Trojans, bad applications, buffer overflows, basically vulnerabilities introduced by software mechanisms. The assumption is that the trusted software is free from bugs too. However, as the trusted software is expected to be small and specific in its function, it can be can validated by external parties or the validation entity. This is not the case for current commercial operating systems or software because of the size of the programs and vast array of functions.

5.7 Challenges to the Adoption of Trusted Computing

The author suggests there are many challenges to the wide spreadsheet adoption of Trusted Computing with the TPM. These challenges include.

- The TPM is a heavy user of public key cryptography and would need a robust Public Key Infrastructure (PKI) with all the associated challenges of deployment for using a TPM manufacturing and supply [64].

- The TPM relies very much on PCR configuration information relating to software which is on a platform. Currently there are no reliable mechanisms which can be deployed with a common standard to make such measurements.

  For example frequent patching will change PCR values and make attestation very difficult, not forgetting the unsealing of locked data. If a PCR value changed then all data locked data to that TPM with a non-migrateable key would be lost.

- Currently the Trusted Platforms do not come with a CRTM or the relevant conformance information which a user can build confidence upon. This makes it difficult to validate that a TPM is genuine.

- TPM are being deployed on laptops and desktops but not currently on servers which are where a corporate audience could utilise it form B2B applications.

  The author suggests this is a critical area for further work as servers generally hold the critical data in a corporate environment and are attacked from remote locations. This will happen more as businesses move towards the de-perimeterisation as advocated by the Jericho forum.

- TPM has a very limited number of commercial applications which take advantage of its services currently. Until manufacturers issue, credible conformance credentials, take up will be low. The author suggests few software vendors are looking to use the technology due to lack of market opportunity.

- Limited software development expertise is a constraint as is little knowledge amongst developers on how to build applications using TPM technology resulting in few applications exploiting the technology.

- The author believes that the public would be against the idea of using Trusted Computing because of the fear of being tracked by their computer usage, although people can be tracked by law enforcement and cookies already.

- The management overhead associated with TPM may prohibit take-up. For example, additional processes will be required to manage TPM failure, the safe protection of keys, ensuring TPM was used correctly by employee, releasing of data when employee leave a business, etc.

- TPM fundamentally requires two parties to operate using pre-agreed software stacks, which may mandate organisations use specific software to maintain conformance i.e. parties are locked into using specific software vendor.

- With the popular use of virtualisation (multiple virtual machines on a single platform), for TPM to work in this context, there is a need for more mature isolation technology from microprocessor manufacturers. This isolation technology has not left the lab with its full feature set as promised by processor manufacturers and is not ready for commercial use.

Other concerns relate to backward compatibility with TPM already released; development of open source software and commercial incentives for certification authorities to enter into the market.

5.8 Summary

Trusted Computing with TPM offers a great advancement in platform security if all of the features are established. It offers platform security against software based attacks from malicious code, Trojans, viruses, root kits as well as providing platform configuration information when requested. Its strength resides in its ability to measure components on a platform in a manner which cannot be circumvented by code running without the knowledge of the core root of trust supported by the CRTM, RTM, RTS, RTR and PCR.

The main reliance is on the measurements carried out and storage provided by the platform configuration registers during the authenticated boot process.

The TPM also offers a range of Cryptographic services used for generating identities; secure key storage, random number generation, symmetric and asymmetric services etc.

A trusted platform is trusted to behave as expected because its misbehaviour cannot be detected by any other components i.e. its core trust measurements are expected to be carried out and provide a genuine attestation of its configuration otherwise it cannot be trusted. Reliance is placed on these measurements by other TPM services such as sealing and binding.

Software running on a trusted platform is expected to be verified by a validation entity which vouches for the cryptographic value of the code and has the ability to be measured by a management agent so that its hash value can be recorded into a PCR.

The report B2B environment for data sharing relied on remote attestation which connects to a remote host and requests it’s configuration information before any data is sent for processing. This ability assured the service user the platform at a partner site was indeed running a secure configuration and it was safe for data to be sent for processing.

Although trusted computing offers a great step forward, it does have it draw backs on implementation and acceptance.

To be fully integrated commercially, it requires the use of public key infrastructure and associated services of certification authorities for the various credentials for the TPM and associated identities it generates.

Currently there are no such certification authorities to facilitate wide spread adaptation of the TPM.

TPM are currently only deployed onto desktop and laptop machines systems only, the author suggests the key area where a TPM needs to be deployed is on servers where organisations process and store their critical data.

Other issues include the lack of software with appropriate measurement agents and associated validation entities. As a result, there are few applications available which are able to use the TPM functionality. This maybe due to the lack of developer expertise too and generally knowledge is not widespread.

The TPM usage in the study relied on Microprocessor based isolation technology which is currently not available from CPU manufacturers. This again is still in the lab and not fully realised.

There are other issues too, including changes in PCR values due to patching; software changes and the lack of a CRTM on current processor boards.

It also has its objectors mainly due to privacy concerns because there is a view that users will be tracked and also software lock in concerns because vendors may require customers to use particular software.

The authors view is that the technology is not mature enough to be used in commercial environments where stability and low management overhead is important.

6 Impact of TPM on Organisational Risk

6.1 Introduction

The impact of introducing Trusted Platform Module (TPM) into a business to business data sharing environment is considered in this chapter. The approach to understand this impact is via a comparison of the risk profile before and after the introduction of TPM.

This chapter starts by providing an overview of the risk assessment methodology employed based on BS ISO 27005:2008 [46c]. Critically it also highlights the scope of the assessment to ensure a fair and balanced approach. To ensure an unbiased comparison by drawing information on information from different sources including SANS Institute (SysAdmin, Audit, Network, Security, established in 1989 as a cooperative research and educational organisation which also runs security courses globally. It is a not-for-profit organisation and is well respected within industry). The chapter concludes with a discussion of the findings.

6.2 Risk Management Methodology

A risk as defined by the Management of Risk used in UK government departments as “an uncertain event or set of events which could, should they occur, will have an effect on the achievement of objectives” [45]. The risk management methodology described below summarises the steps involved in identifying the risks, quantifying their impacts using industry specific information and evaluating the approach to treatment.

6.2.1 The Method

The method employed here is to develop the risk profiles based on BS27005:2008 [46]. Figure 4 below illustrates the risk management process used in BS ISO / IEC 27005:2008 to establish an Information Security Management System (ISMS).

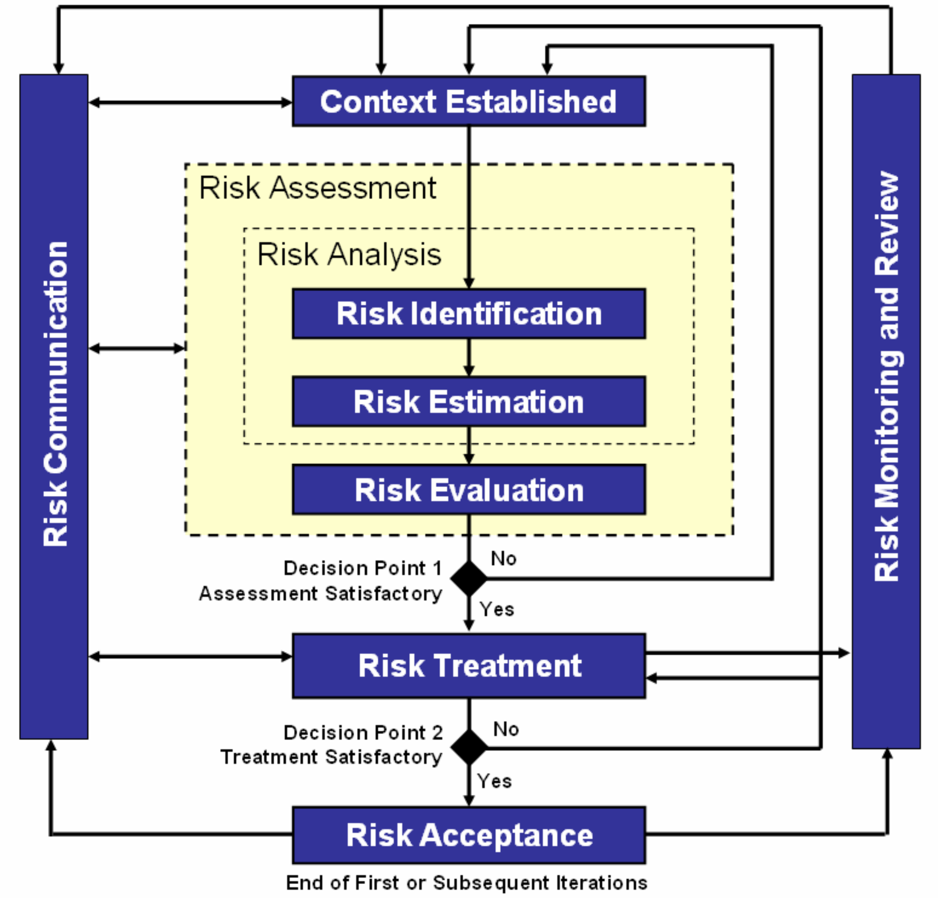

Figure 4: Information Security Risk Management Process
Source: BS ISO/IEC 27005:2008

Put simply, the method requires the context be defined (Context Established) and for the purposes of this paper is data sharing between businesses in the pharmaceutical industry as set out in previous chapters. Within this context, risks are identified (Risk Identification), i.e. what problems could come about that would compromise the business. Once the lists of risks are understood, estimates of their likelihood and possible impact are determined (Risk Estimation). Depending on the likelihood and possible impact, risks are evaluated (Risk Evaluation) to develop appropriate controls in response. The approach with each stage is described in more detail in the following subsections.

The overall process being used is well documented in [46c], however as this study is an evaluation of assurance. The author has limited the scope to Context Establishment, Risk Identification, Risk Estimation and Risk Evaluation and did not consider other elements included in the guidance [46c] such as Risk Monitoring and Review, Risk Communication, Risk Treatment and Risk Acceptance as the intention is not to establish as Information Security Management System.

6.2.2 Statement of Applicability

BS ISO/IEC 27005:2008 sets out eight types of threats as shown in the left of Figure 5 below and illustrates how the selection of the four high level risks was derived from this list of eight high level risk areas outlined in the standard.

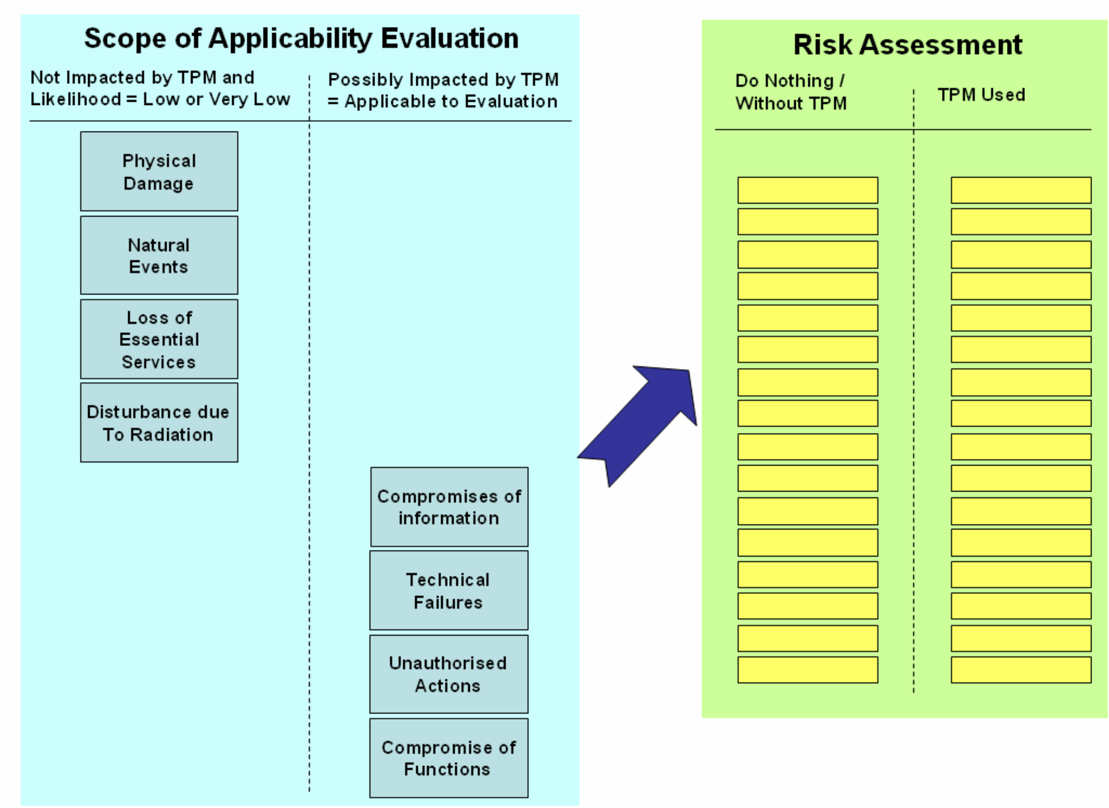
Scope of Applicability Evaluation
Not Impacted by TPM and Likelihood = Low or Very Low
Possibly Impacted by TPM = Applicable to Evaluation
Physical Damage
Natural Events
Loss of Essential Services
Disturbance due To Radiation
Compromises of information
Technical Failures
Unauthorised Actions
Compromise of Functions
Risk Assessment
Do Nothing / Without TPM
TPM Used

Figure 5: illustration of how the "Statement of Applicability" was used to select risks for this evaluation

A number of these risk types are related to major catastrophes or '*force majeure*', where the presence of TPM will have little or no impact on the outcome. The likelihood of these events are also low or very low albeit the impacts are high or very high and therefore these risk types have been excluded from the scope of applicability, i.e. Physical Damage, Natural Events, Loss of Essential Services and Disturbance due to Radiation.

The high level statement of applicability will include the following risk areas:

1. Compromise of Information;
2. Technical Failures;
3. Unauthorised Actions;
4. Compromise of Functions.

6.2.3 Risk Identification and Estimation

The risk types in the Statement of Applicability were expanded further into typical threats and risks as outlined in the 2007 e-Crime Survey [16], BS ISO/IEC 27005:2008 [46a] and the SANS Top 20 Programming errors [70].

The risks identified were used to build the risk register. This method was used by the author to establish a linkage between actual risks identified in practice as outlined in 2007 e-Crime survey [16], known established problems contributing to risks as outlined by SANS and the best practice risk considerations given in BS ISO/IEC 27005:2008. This can be seen in figure 1 below.

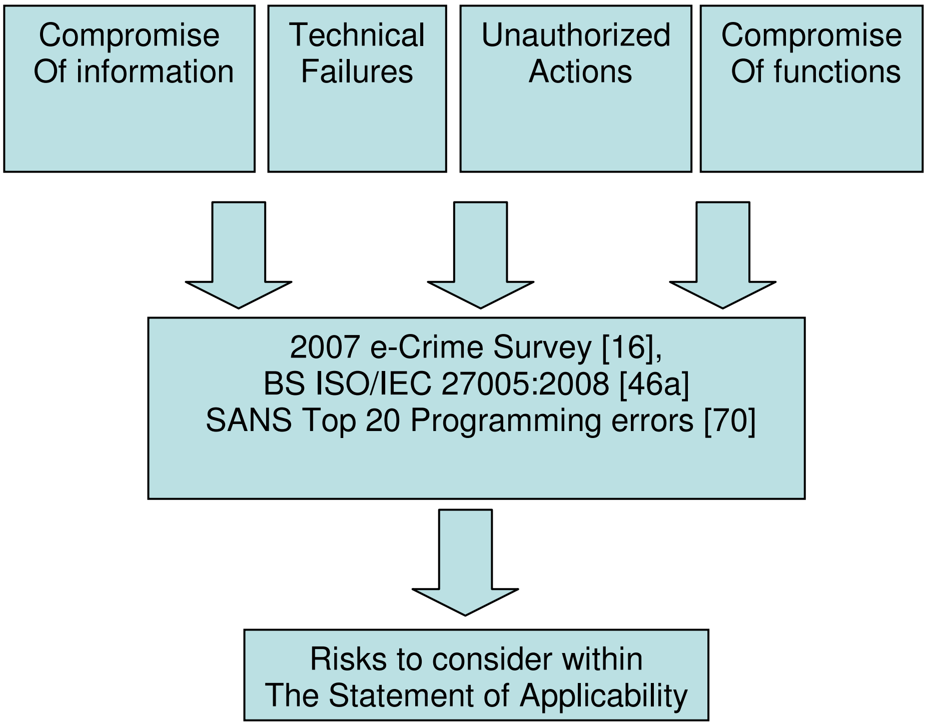
Compromise Of information
Technical Failures
Unauthorized Actions
Compromise Of functions
2007 e-Crime Survey [16],
BS ISO/IEC 27005:2008 [46a]
SANS Top 20 Programming errors [70]
Risks to consider within The Statement of Applicability

Figure 1: Steps in Identifying Risks

For the purposes of this evaluation of TPM, it is important that a fair sample of risks is considered to ensure an unbiased result.

These risks were recorded in the risk register taking guidance from industry best practice, specifically 2007 e-crime surveys [16] , BS ISO/IEC 27005:2008[46a] and SANS top 20 Programming errors [70].

The reason behind this two step approach by the author was to capture the areas where e-crime is most active and extract the most common risks associated with business to business transactions.
To score the risks, source materials [16], [70], [46c], Appendix A – Impact and Likelihood Matrix and Appendix B – Risk Impact Definitions were used. The impact and likelihood matrix and the risk impact

definitions set out the scoring scheme used to quantify likelihood and impact and aid in comparison between the two risk profiles. Both likelihood and impact have linear scoring which are multiplied to give a combined risk score.

An estimation of the likelihood and impacts is offered within the risk assessment. The important consideration here is the relative difference between the likelihood and impact before and after the introduction of TPM.

6.2.4 Risk Evaluation

The risk assessment evaluation firstly considers the controls that are typically employed as part of a risk treatment plan BS ISO/IEC 27005:2008 and other industry good practice i.e. SANS Top 20 Controls [67] to mitigate the identified risks.

This is followed up with an evaluation of how TPM can also mitigate these risks. The resulting two risk profiles are compared and the findings are discussed later in this chapter.

6.3 Risk Assessments: Without and With TPM

The risk register for the threats associated with the risk types identified within the statement of applicability and appropriate controls is included in Appendix C – Baseline Risk Register without TPM Controls. For the purposes of this evaluation, this register is used as the baseline from which a comparison is made. It should also be noted that this evaluation focuses on the security of the platform.

The risk register for the threats associated with the risk types identified within the statement of applicability and appropriate controls (***including TPM controls***) is included in. Appendix D – Risk Register with TPM Controls. It should be noted that TPM controls are taken into consideration as part of the assessment as well as layering on top of the SANS Top 20 controls.

The risks addressed by trusted computing are related to platforms and not network connectivity and it is assumed parties would use data sharing via dedicated network links. However, there is a stream of trusted computing which can be applied to secure network connectivity know as Trusted Network Connect (TNC).

6.4 Comparison of Risk Profile and Findings

Trusted Computing controls do reduce the overall risk profile. Table 5 below highlights the level of risk reduction after the deployment of Trusted Computing controls when compared to the baseline risk register. The Risk IDs refer back to the risk register and using the risk scoring scheme it can be seen that the risk levels reduce by between 33% and 67% by using Trusted Computing.

Risk ID's	Risk Reduction
2,3,6,7,18	67%
15,16	50%
1,4,5,14,19,20,21,22,23	33%
8,9,10,11,12,13,17	0%

Table 5: Risk Reduction Table

The TPM was most effective in reducing risk associated with *Compromise of Information* and *Unauthorised Actions* from the statement of applicability. It was less effective on "Compromise of Functions" due to the nature of the activity on a platform. Furthermore, it had no effect on preventing theft of media: theft of equipment or tampering of hardware which are related to physical attacks and made no difference.

Below is a discussion of how trusted computing controls were used to reduce the current risks:

1. **Sealed / Bound Data**
   TPM seals data to the platform, so any attempt to copy information from a Trusted Platform renders that data useless. It can be argued, that is offers no more protection than encrypting the data. The difference is that the current encryption methods do not set state information which is a prerequisite for access with TPM. This is reinforced by keys which may be non-migrateable and so never leave the TPM and therefore render the data useless even if the data was copied off.

   This control prevents data loss and protection of data on mobile devices as well as preventing access to data by malicious software. However, the author points out that if the TPM is damaged or inoperable then all data is lost unless there is a backup of keys which may not be the case in every event.

2. **Platform Integrity using Platform Configuration Registers (PCR)**
   These registers are critical in preventing and controlling access to data by users or programs. If the platform is running an un-validated piece of code or code is started on a system then the PCR registers values will defer from the conditions required to unseal the data, therefore the data will remain inaccessible and sealed.

   A known good configuration state provides assurance that malicious code, spyware, botnets, phishing attacks, backdoors and other hacking/malicious tools cannot be used to control the platform and gain access to the data. This may be possible with existing arrangements as operators may surf the internet and potentially become infected with malicious code.

   Regulatory bodies like this kind of control because access to data is controlled and not allowed without specific conditions being met. PCR were the most used control for reducing risk in the trusted computing risk assessment.

3. **Data Locked to Platform State**
   This control is a combination of (1) and (2) above and prevents data copied off onto remote / mobile devices from being accessible outside of the platform. This function could be used to offsite backups and prevent unauthorised access. If this offsite data was stolen, then it will be useless to a thief because the data is locked to a platform state.

4. **Software Integrity Checks**
   This prevents malicious or compromised software being installed and run on a host. The Validation Entity measurements would not match; therefore data would not be released for processing. This would prevent rogue software taking control of a host. For example if a host was compromised as a result of vulnerability, the additional / changed code to compromise the host would change the integrity metrics.

5. **Isolated Processing Environment**
   Using the TPM functions, an isolated environment can be implemented in which all data processing is carried out. This would not be accessible from other environments on the computing platform and only selected services and access is provided to allow for data processing. For example, the environment may not allow for any connections by mobile devices (memory sticks, USB drives etc) or allow the operator to run any other applications outside of what was required for data processing.

We can see from this risk assessment that using these measures improves host security protection by reducing the risk considerably. These measures give the businesses using the services, a higher level of confidence that their data is managed in a controlled environment, giving additional assurance outside of the regular business to business controls which rely on the third party Partner to behave in an expected manner.
Trusted Computing is particularly useful for pharmaceuticals environments, in the authors view because some systems must be maintained to standards outlined by what is called “Good Regulatory Practice” or GxP for short. The x is used to denote that good practices apply to different streams of drug development cycle, i.e. manufacturing, clinical trials etc.

Currently, an entire system must be managed with appropriate documentation kept for inspection by the regulators. This applies to software updates, patching, and physical hardware operations etc, basically anything which could be interpreted as affecting the integrity of the data stored on a system. As the reader can imagine, this takes a long time and is an expensive task performed by experienced staff on the entire system.

Trusted Computing would allow for GxP to be applied to the isolated data processing environment which has small number of applications installed and more importantly, all applications have an associated integrity measurement compared to an entire system which has a far greater number of applications and no integrity measurements.

This allows for controlled auditable activity to take place in more manageable and isolated environment leading to lower risks and better assurance for the data. In the context of the risk assessment, this is an important point to note.

For example, compliance checks can be made; particularly to demonstrate that information relating to drug trial was not modified or accessed by other parties affecting the integrity and confidentiality of data.

Using trusted controls allows partners to establish from a remote location, the integrity of a platform before allowing data to be transferred as opposed to asking the partner if the environment is safe for the transfer of data.

In the authors view, Trusted Computing is a great step forward for a number of reasons. For example, data assurance would seem to be greater because the business has some control over the processing environments. Currently there is reliance and trust placed on the partner to behave in good manner against the fear of loosing business. The author argues, this is not always the case because the partner is so interconnected with the business that contracts cannot be cancelled that easily.

Trusted Computing brings a level of control against software based attacks because any software not behaving as expected would prevent processing of data by simply relying on PCR integrity check of the software.

For example, non validated software cannot be used for information processing or used if the business does not mandate it. Therefore businesses can be assured that Partners are not using non validated software in their environments.

6.5 Summary

During this stage of the report, a risk assessment was performed following the methodology outlined in BS27005:2008 drawing on multiple sources to identify threats, risks and current e-crime activity (SANS, BS27005:2008 and e-crime survey).
The context of the risk assessment was for a pharmaceutical organisation which is processing sensitive competitive information after identifying, evaluating and estimating the risk associated with B2B data sharing.
The risk methodology was used to develop the statement of applicability choosing the most appropriate risks from eight categories down to four which were applicable to platform risks.
The four risk categories were:

1. Compromise of information
2. Technical failures
3. Unauthorised actions
4. Compromise of functions.

These categories were used to identify specific risks on which the two rounds of risk assessment was carried out.
One round was using current controls recommended by SANS Institute and another round assuming Trusted Computing controls were implemented.
The risk evaluation against likelihood and impact were calculated and recorded in the risk registers for each round.
The two risk registers were compared and analysed. The risk registers suggested that the TPM did indeed reduce the risks associated with B2B data sharing in a pharmaceutical organisation using Trusted Computing by as much as 67%. The assessment highlighted the TPM was most effective for compromise of information and unauthorised actions. However, it was less effective on compromise of functions.
The TPM reduced the risks by using the following of its functions:

1. Sealing and bounding data to the TPM prevented data loss and rendering any data copied off useless to the attacker because it was locked to the platform and its configuration information.
2. PCR helped to ensure no rouge software could compromise the data because the data was only released for processing under a particular platform state. PCR also helped with ensure only validated software was running on the platform.
3. Isolated environment within the processing host helped ensure no connectivity from other possible hostile environments were possible.

The TPM offered considerable risk reduction compared to current operating environments where data is processed giving high levels of confidence and data assurance to the business and the partner. The author also established that this kind of control would be very useful in GxP regulated environments where audit trails are of vital important to demonstrate data integrity.

7 Conclusions

This paper aimed to explore data sharing between organisations and in particular data sharing between pharmaceutical organisations and their partners.
It explored the need to share data, how organisations can build trust when sharing data and discussing some of the challenges.
It explored the current security landscape and some of the challenges facing information security today before performing a risk assessment on platform security using Trusted Computing with a Trusted Platform Module to establish if it will offer impressive levels of data assurance and aide in the development of trust between organisations.

Organisations and governments are sharing data to facilitate new business to business operating models to maintain competitive advantage, maintain control over operating costs and deliver services. Global sourcing deals means data is shared across multiple geographies by relaxing existing security controls to allow applications and data processing environments to work in the new de-perimeterised seamless business models.
This allows organisations to focus on core business activities. Pharmaceutical organisations share critical drug research information as well as business process information which is sensitive and valuable due to the time it takes for the information to be gathered and processed (sometimes up to 15 years).

Pharmaceuticals and the government must follow the data protection act and the human rights act to maintain confidential information. Pharmaceuticals must also maintain regulatory control over data by demonstrating compliance during a drug development cycle.
The public is skeptical on the ability of the government or private companies in looking after their personal information and maintaining privacy given the number of breaches reported in the press. The government recently withdrew a data marking amendment to the justice bill after receiving pressure from the privacy groups.

Data sharing is in existence and will continue to be but care is needed by all in the processing, collection and storage.
Building trust in these business partnerships and entrusting a partner with some of the organisations critical competitive information is very difficult but necessary for the success of an organisation. Trust is a fundamental human requirement and is very fragile with serious consequences when it is lost. This is even more so in business relationships because it can have dramatic effect on public confidence, perception, brand loyalty and not forgetting the legal issues which may arise out of data breach i.e. confidential information is released into the public domain or data on individuals status of health becomes know in public

Organisations use a number of methods to develop trust including contracts, accreditations, audits, review of technical controls, interviews, site visits and inspections etc.
One method in isolation does not offer a complete picture upon which to build trust. A collection of methods must be used to ensure trust established.

Each method has its flaws relating to people, processes and technology. For example, contract responsibilities, accountabilities may be not being communicated across the partner organisations, audit may overlook key areas or lack scope and technical controls may not be managed correctly. In the pharmaceutical environment these issues may lead to regulatory compliance problems with regulatory bodies holding organisations accountable for the problems of their partner.

Security management is further complicated by organisations need to be constantly connected to the internet and the partner networks following de-perimeterisation principles , so any disruption affects operations and costs money.
The threats from malicious code, viruses, trojans, and botnets are here to stay because there has been no remarkable improvement in protection or detection technology as attacks have become more sophisticated.

New sourcing and business partnership models have given rise to more motivation for insider and outsider attacks on organisations who have responded by concentrating data protection at the end point i.e. on the data itself. Once again this is important for pharmaceuticals where data integrity and confidentiality must be demonstrated to regulatory authorities.
The Government being a large sharer of data recognises the need for a connected economy and realised the need to protect the public and its infrastructure from criminals, hostile states and terrorist. The Government has setup e-crime strategies across the UK and internationally to tackle this growing threat.

The author suggests that as e-crime may take place within organisations, help is needed to drive expertise and good practice in computer forensics,
Data sharing is a essential for organisation which means e-crime will always remain and unfortunately security controls have not changed dramatically over recent years. This has left governments, individuals and private organisations feeling vulnerable to attacks. This highlights the need for effective security controls. Trusted Computing using a Trusted Platform Module aims to offer this control by claiming it can offer more platform security and data assurance.

To determine if this claim could be justified, two risk assessments were performed and compared against the context of a pharmaceutical environment. One assessment assumed the TPM was in use whilst the other did not.

The statement of applicability as outlined in BS 27005:2008 helped identify the generic risk areas from eight risk types down to four risk types. The risk types selected were Compromise of information; Technical failures; Unauthorised Actions; Compromise of functions.

To ensure the risks where selected in a fair and appropriate way, the author selected multiple sources to ensure practical real world risks and theoretical risks advocated by BS 27005:2008 were considered. The Industry recommended best practice controls were assumed to be in use against the selected risk types.

A comparison was made between the two risk registers and it was found that TPM reduced the risks by 33% to 67% across most of the risks. The TPM was most effective on risks associated with “Compromise of information” and “Unauthorised actions” which is very applicable to pharmaceutical GxP regulated environments because these two types of risks can invalidate drug research information or trial data. Furthermore the risks could allow a regulator to halt business operations if compliance can not be demonstrated.

The risk was reduced because the platform security had improved and there was no reliance on the partner’s controls or assurances regarding the platform as discussed in the challenges in managing trust.

Trusted Computing specification developed by the Trusted Computing Group (TCG) is used within a Trusted Platform Module (TPM) whilst offering greater levels of data security and data assurance has a number of challenges. In the context of this report and data sharing in a pharmaceutical environment, the top challenges are:

1. The lack of a Public Key Infrastructure (PKI) which can be used to build trust in the actual TPM itself i.e. a PKI which can be used by TPM manufacturers, platform designers and platform manufactures upon which the Pharmaceutical organisation can build confidence that a TPM is genuine and conforms to TCG specifications.
2. TPM are not deployed on servers so applications used for data processing cannot take advantage of TPM functionality.
3. Lack of an agreed standard by which application validation can take place or measurements provided by a validation entity so PCR values can be referenced.
4. The lack of a PKI for generation of identities but this may not be such as an issue because that could be run internally by the pharmaceutical organisation and its partner.
5. There is little expertise in application development or commercial drive in the developing applications which utilise TPM functions.
6. Virtual isolation technology has not matured to use TPM on server platforms.

7. In a pharmaceutical environments or any business environment, software patching is mandated to take place on a regular basis so the PCR values would need to be managed between the organisation and its partners which introduces complexities and operational overhead.
8. The TPM is a new technology and has not matured enough for use in a corporate environment because there is little understanding of what it would take to manage such an infrastructure.

This paper has met the initial objectives by outlining the need and drive to share data; the current security landscape; challenges for establishing trust and explored whether a TPM can offer greater levels of data assurance and platform security for a pharmaceutical organisation by way of a risk assessment.

In summary, the findings are such that a TPM can offer better security and data assurance whilst offering more information towards building trust in a partnership but it is not yet a mature technology which can be used for data processing.

This work has contributed to offering a risk based approach to confirming some of the accepted views in using TPM technology. It has also highlighted how the TPM offers another avenue in establishing trust between organisations because reliance is not solely placed on assurances from the partner that their environment is safe for data processing.
The work has also agreed with some of the challenges faced by trusted computing and its wider adoption. It has also confirmed that "Trust" is a very difficult concept to pin down and requires technology, processes and above all people to make it work.

The author concludes on a few suggestions as to where further work should be conducted for the adoption of Trusted Computing.
The new ideas such as trusted computing will be another control for the management of information security but there needs to be more work carried out in the following areas:

1. The development and acceptance of a PKI used in trusted computing approved by law makers, so it has legal acceptance on areas such as liabilities and accountability
2. Deployment of TPM onto servers needs higher priority from the platform manufacturers and designers.
3. Agreement on a mechanism for validating applications which takes into account the security patching cycles in organisations.
4. More awareness and training offered on TPM technology which seems to be only in research establishments.

The TPM opens the doors to an endless list of secure applications including Business to Business data sharing, Digital Rights Management (DRM) Applications, Secure Web Services, Digital Signatures, Secure P2P networks etc

In the authors view, Trusted Computing offers a long awaited security control for platform security which if not handled correctly will become another technology which never leaves the research lab. At this time, the author cannot think of any other security technology with as much promise as Trusted Computing.

8 References

[1] - http://www.forrester.com/Research/Document/0,7211,54046,00.html
Pharmaceutical Industry Trends Drive EA

[2] -
http://www.forrester.com/Research/Document/0,7211,45250,00.html?src=54046pdf - Business Realities Drive IT Globalisation

[3] - http://www.forrester.com/Research/Document/0,7211,38314,00.html
Digital Business Networks

[4] - http://www.forrester.com/Research/Document/0,7211,54068,00.html
EMEA IT Outsourcing Deals: 2008 Review

[5] – http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf
Data Sharing Review – Richard Thomas and Mark Walport – pages 13-21.
July 2008.

[5a] – http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf
Data Sharing Review – Richard Thomas and Mark Walport – pages 22-26.
July 2008

[5b] – http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf
Data Sharing Review – Richard Thomas and Mark Walport – pages 49.
July 2008

[6] -
http://www.forrester.com/rb/Research/wave%26trade%3B_uk_database_marketing_service_providers%2C_q2/q/id/47325/t/2
The Forrester Wave: UK Database Marketing Service Providers, Q2 2009 – May 2009.

[7] - http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
Data Protection Act 1998

[8] – http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_3
The Human Rights Act 1998

[9] -
http://www.ico.gov.uk/upload/documents/pressreleases/2008/rsa_speech_oct08_final.pdf
Speech to RSA Conference Europe on data breaches
Richard Thomas, Information Commissioner – 29 October 2008

[10] - http://www.ons.gov.uk/about-statistics/development-programmes/public-confidence/project/public-confidence-in-british-official-statistics.pdf
Public Confidence in British Official Statistics
Maryanne Kelly
United Kingdom Office for National Statistics
28 February 2005

[11] - http://news.bbc.co.uk/1/hi/business/8184695.stm
Top firms' pension funds plummet

[12] - http://www.bbc.co.uk/blogs/thereporters/robertpeston/2007/10/the_rock_and_me.html -- The Rock and me – Robert Peston – BBC news.

[13] - http://www.newsobserver.com/print/friday/business/story/579584.html
GSK's Avandia problem may grow

[14] - http://www.tif.co.uk/
The corporate IT Forum

[15] - http://www.opengroup.org/jericho/newsletters/NWW8_managingtrust.pdf
Managing trust in our digital world

[16] - http://www.cert.org/archive/pdf/ecrimesummary07.pdf
2007 E-Crime Watch Survey – by Cert.

[17] - http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf
Department for Business, Enterprise & Regulatory Reform (BERR) – 2008 Information Security Breaches Survey.

[18] - http://www.crimereduction.homeoffice.gov.uk/internet02.htm
The E-crime Strategy

[19] -http://www.soca.gov.uk/assessPublications/OrganisedCrimeReview.html
Serious organised crime review

[20] - http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf
"Airport Insecurity: The case of missing or lost laptops", Ponemon Institute, 30 June 2008.

[21] BBC, "Defence minister's laptop stolen", 4 June 2000.
http://news.bbc.co.uk/1/hi/uk/776364.stm

[22] "MoD loses 600 laptops", BBC News, 13 January 2002.
http://news.bbc.co.uk/1/hi/uk/1757792.stm
Page 72

[23] “The Federal Bureau of Investigation’s Control Over Weapons And Laptop
Computers Follow-Up Audit” report, February 2007, Pg iv.
http://www.usdoj.gov/oig/reports/FBI/a0718/final.pdf

[24] The Guardian, “Personal details of every child in UK lost by Revenue & Customs”,
Deborah Summers, 20 November 2007.
http://www.guardian.co.uk/politics/2007/nov/20/economy.personalfinancenews

[25] BBC, “Nine NHS trusts lose patient data”, 23 December 2007.
http://news.bbc.co.uk/1/hi/uk/7158019.stm

[26] BBC, “Millions of L-driver details lost”, 17 December 2007.
http://news.bbc.co.uk/1/hi/uk_politics/7147715.stm

[27] BBC, “Company loses data on criminals”, 21 August 2008.
http://news.bbc.co.uk/1/hi/uk/7575766.stm

[28] - http://www.met.police.uk/pceu/ACPOecrimestrategy.pdf
E-Crime strategy

[29] - http://www.opengroup.org/jericho/about.htm
Jericho Forum.

[30]- http://www.sei.cmu.edu/publications/documents/08.reports/08tr009.html
The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures

[31] - http://news.bbc.co.uk/1/hi/scotland/glasgow_and_west/6089736.stm
“The gangs are seeking customers' details. One in 10 of Glasgow's financial call centres has been infiltrated by criminal gangs, police believe.”

[32] -
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=11&issue=60
SANS NewsBites - Volume: XI, Issue: 60 – 31st July 2009.

[33] - Fake Security Software Steals $34 Million Monthly
http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=218800178

[34] – Buffer Overflow attacks – James C Foster – ISBN 932266067-4.

[35] – Secure coding principle and practices – Mark G Graff & Kenneth R Van Wyk – ISBN -0 – 596 – 00242 -4.

[36] – Trusted computing platforms – Siani Pearson – ISBN – 0-13-009220. - Chapter 1.

[37] - http://www.trustedcomputinggroup.org/

[38] - http://www.trustedcomputinggroup.org/about_tcg/tcg_members

[39] – Trusted Computing – Chris Mitchell – IEE professional applications of computing series 6 – ISBN -0 -86341-525-3.

[40] – A Practical guide to Trusted Computing – David Challenger, Kent Yoder, Rayan Catherman,David Stafford, Leendert Van Doorn.

[41] -
http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html
Understanding HIPAA Privacy

[42] - http://www.forrester.com/Research/Document/0,7211,54046,00.html - Pharmaceutical Industry Trends Drive EA - Henry Peyret

[43] http://www.rhul.ac.uk/mathematics/techreports Report - Management of Risks
Associated with De-perimeterisation - RHUL-MA-2009-07 - Kwok Keong, LEE

[44] - http://www.opengroup.org/jericho/

[45] – M-o-R – Management of Risk: Guidance for practitioners -2007 – ISBN -978-0-11-331038-8.

[46] - BS ISO/IEC 27005:2008 page 5.
Information Technology – Security Techniques – Information Security Risk Management.

[46a] – BS ISO/IEC 27005:2008 Annex C – page 39.
Information Technology – Security Techniques – Information Security Risk Management.

[46c] - BS ISO/IEC 27005:2008.
Information Technology – Security Techniques – Information Security Risk Management.

[47] - ISO/IEC 27001:2005(E)
Information technology — Security techniques — Information security Management systems — Requirements

[48] - http://news.bbc.co.uk/1/hi/scotland/glasgow_and_west/6089736.stm
The gangs are seeking customers' details
One in 10 of Glasgow's financial call centres has been infiltrated by criminal gangs, police believe.

[49] - BBC, “Company loses data on criminals”, 21 August 2008.
http://news.bbc.co.uk/1/hi/uk/7575766.stm

[50] - http://www.scmagazineuk.com/Credit-card-breaches-reported-at-two-companies-with-over-half-a-million-users-possibly-affected/article/140621/ - Dan Raywood July 27, 2009
Credit card breaches reported at two companies with over half a million users possibly affected

[51] - http://www.theregister.co.uk/2009/07/22/fsa_hsbc_data_loss/
Bank fined £3m for data loss

[52] - http://www.theregister.co.uk/2009/07/09/data_breach_survey/
UK data breach incidents on the rise

[53] - http://blogs.msdn.com/sdl/archive/2009/07/28/atl-ms09-035-and-the-sdl.aspx - Tiny typo blamed for massive IE security fail

[54] - Book “Subverting the Windows Kernel – Rootkits” – Greg Hoglund and James Butler. ISBN – 0-321-29431-9

[55] - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
Risk Management Guide for Information Technology Systems

[56] – Security in computing - Fourth edition – Charles P Pfleeger and Shari Lawrence Pfleeger – ISBN 0-13-239077-9 – Chapter 1.

[57] – Information Warfare and Security – Dorothy E Denning – ISBN – 0-201-43303-6 – Chapters 3,4,5,6,8,9 and 13.

[58] - http://www.cabinetoffice.gov.uk/cio/shared_services/ss_in_govt.aspx#1
Shared Services and Transformational Government

[59] - http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/media//879E2/efficiency_review120704.pdf
Releasing resources to the front line – Page 11 outlines the areas for effiency savings – Sir Peter Gershon, CBE.

[60] - It’s Time To Focus On Data Protection by Simon Yates
Forrester – 31st July 2008.

[61] - http://news.bbc.co.uk/1/hi/uk_politics/8118348.stm
Cyber-security strategy launched – 25th June 2009

[62] - http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1.htm
Computer Misuse Act 1990

[63] - http://www.ico.gov.uk/what_we_cover/data_protection.aspx
Data Protection Act - Your rights, responsibilities and obligations to data protection

[63 – http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1
Regulation of Investigatory Powers Act 2000

[64] - http://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-14.pdf
Challenges for Trusted Computing
S. Balfe, E. Gallery, C.J. Mitchell and K.G. Paterson

[65] - http://news.bbc.co.uk/1/hi/uk/7953401.stm
Thursday, 19 March 2009
Overseas credit card scam exposed

[66] - http://news.bbc.co.uk/1/hi/business/7818220.stm
8 January 2009 - Satyam scandal shocks India

[67]- http://www.sans.org/cag/guidelines.php
20 Critical Security Controls - Version 2.1
Version 2.1: August 10, 2009

[68]- http://www.sans.org/resources/10_security_trends.pdf
The Ten Most Important Security Trends of the Coming Year
SANS Institute 2006

[69] - http://www.apacs.org.uk/09_03_19.htm
2008 fraud figures announced by APACS
Fraud loss figures released today (19 March 2009) by APACS

[70] - http://www.sans.org/top25errors/?cat=top25
CWE/SANS TOP 25 Most Dangerous Programming Errors
Sans.org – 14-August 2009.

[71] - http://isc.sans.org/top10.html
Ports usage and associated vulnerabilities can be found here.

[72] - http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-563879
The government has announced that it will immediately abandon clause 154 of the Coroners and Justice Bill.

Appendix A – Impact and Likelihood Matrix

		Impact				
		Very Low (1)	**Low (2)**	**Medium (3)**	**High (4)**	**Very High (5)**
Likelihood	**Very Low 0-10% (1)**	1	2	3	4	5
	Low 11-20% (2)	2	4	6	8	10
	Medium 21-69% (3)	3	6	9	12	15
	High 70-89% (4)	4	8	12	16	20
	Very High 90-99% (5)	5	10	15	20	25

Table 1: Impact and Likelihood Matrix - used as the scoring of likelihood and impact for all risks identified in the risk register.

Appendix B – Risk Impact Definitions

Impact Definitions	
Magnitude	**Definition**
Very High	Exercise of the vulnerability - (1) may stop all company operations globally or (2) may result very high loss of life
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organisation's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organisation's mission, reputation, or interest; or (3) may result in human injury
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organisation's mission, reputation, or interest.
Very Low	Exercise of the vulnerability (1) Disruption to non critical business operations at single site

Table 2: Risk Impact Definitions
Source: Derived from NIST SP 800 30 [55]

Appendix C – Baseline Risk Register without TPM Controls

The risk register is provided in the table below. The assessment was conducted with the assumption that appropriate SANS top 20 controls were implemented however without Trusted Computing controls.

Table 3: Risk Register without TPM Controls

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Controls [SANS Top 20 Controls][67]
1	**Theft of Information + Theft of Intellectual Property**	[**Compromise of Information**] Theft of information and intellectual property developed over many years, sometimes up to 15 years, including drug trials, medical compounds, patient information, and confidential research useful for competitors etc. Impact: Loss of potential source of new business income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.	Medium	High	▪ Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers ▪ Secure Configurations for Network Devices such as Firewalls, Routers, and Switches ▪ Boundary Defence ▪ Maintenance, Monitoring, and Analysis of Security Audit Logs ▪ Application Software Security ▪ Controlled Use of Administrative Privileges ▪ Controlled Access Based on Need to Know ▪ Continuous Vulnerability Assessment and Remediation ▪ Account Monitoring and Control ▪ Malware Defences ▪ Limitation and Control of Network Ports, Protocols, and Services ▪ Wireless Device Control ▪ Data Loss Prevention ▪ Secure Network Engineering ▪ Penetration Tests and Red Team Exercises ▪ Incident Response Capability ▪ Data Recovery Capability ▪ Security Skills Assessment and Appropriate

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Controls [SANS Top 20 Controls][67]
					Training to Fill Gaps
2	**Virus, Worms or other malicious code + Spy-ware**	**[Unauthorised Actions]** Impaired business performance and potential corruption of sensitive data affecting integrity of information. Confidential information may be sent to third parties without knowledge. <u>Impact:</u> Loss of potential source of new business income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.	Medium	High	▪ Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers ▪ Secure Configurations for Network Devices such as Firewalls, Routers, and Switches ▪ Boundary Defence ▪ Maintenance, Monitoring, and Analysis of Security Audit Logs ▪ Application Software Security ▪ Controlled Use of Administrative Privileges ▪ Controlled Access Based on Need to Know ▪ Continuous Vulnerability Assessment and Remediation ▪ Account Monitoring and Control ▪ Malware Defences ▪ Limitation and Control of Network Ports, Protocols, and Services ▪ Secure Network Engineering ▪ Penetration Tests and Red Team Exercises ▪ Incident Response Capability ▪ Data Recovery Capability ▪ Security Skills Assessment and Appropriate Training to Fill Gaps
3	**Intentional exposure of private or sensitive information + Disclosure**	[**Compromise of Information**] Disclosure of information developed over many years, sometimes up to 15 years, including drug trials, medical compounds, patient information, and confidential research useful for competitors etc. <u>Impact:</u> Loss of potential source of new business	Medium	High	▪ Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers ▪ Secure Configurations for Network Devices such as Firewalls, Routers, and Switches ▪ Boundary Defence ▪ Maintenance, Monitoring, and Analysis of Security Audit Logs ▪ Application Software Security ▪ Controlled Use of Administrative Privileges ▪ Controlled Access Based on Need to Know ▪ Account Monitoring and Control

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Controls [SANS Top 20 Controls][67]
		income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.			▪ Malware Defences ▪ Limitation and Control of Network Ports, Protocols, and Services ▪ Wireless Device Control ▪ Data Loss Prevention ▪ Penetration Tests
4	**Unauthorised Access to/Use of Information Systems and Networks**	**[Unauthorised Actions]** Unauthorised access to sensitive information leading to information disclosure and regulatory violation. Unauthorised use of systems for illegal content download / distribution etc. Disclosure of unpublished material and leaks to press. Impact: Loss of potential source of new business income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.	Medium	High	▪ Inventory of Authorised and Unauthorised Devices ▪ Inventory of Authorised and Unauthorised Software ▪ Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers ▪ Secure Configurations for Network Devices such as Firewalls, Routers, and Switches ▪ Boundary Defence ▪ Maintenance, Monitoring, and Analysis of Security Audit Logs ▪ Application Software Security ▪ Controlled Use of Administrative Privileges ▪ Controlled Access Based on Need to Know ▪ Account Monitoring and Control ▪ Malware Defences ▪ Limitation and Control of Network Ports, Protocols, and Services ▪ Wireless Device Control ▪ Secure Network Engineering ▪ Penetration Tests
5	**Illegal Generation of Spam Email + Zombie Machines**	**[Compromise of Functions]** Compromise of systems leading illegal system use for generating SPAM or other automated activity. Compromised systems attacking other entities using business resources by	Medium	High	▪ All appropriate controls

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Controls [SANS Top 20 Controls][67]
		Botnets, Zombies. Impact: Loss of customer confidence, degraded operations, loss of reputation, Judicial proceedings, leak to press, loss of trust, and disruption to partner operations.			
6	**Remote Spying**	**[Compromise of Information]** Description / Impact	Medium	High	▪ All appropriate controls
7	**Eavesdropping**	**[Compromise of Information]** Description / Impact	Medium	High	▪ All appropriate controls
8	**Theft of Media or Documents**	**[Compromise of Information]** Description / Impact	Low	High	▪ All appropriate controls
9	**Theft of Equipment**	**[Compromise of Information]** Description / Impact	Low	High	▪ All appropriate controls
10	**Retrieval of Recycled or disguarded media**	**[Compromise of Information]** Description / Impact	Very Low	Medium	▪ All appropriate controls
11	**Data from untrustworthy sources**	**[Compromise of Information]** Description / Impact	Very Low	Medium	▪ All appropriate controls
12	**Tampering with hardware**	**[Compromise of Information]** Description / Impact	Low	Medium	▪ All appropriate controls
13	**Protection Detection**	**[Compromise of Information]** Description / Impact	Low	High	▪ All appropriate controls
14	**Denial of Service Attacks**	**[Unauthorised Actions]** Description / Impact	Medium	High	▪ All appropriate controls
15	**Phishing**	**[Unauthorised Actions]** Description /	Low	Medium	▪ All appropriate controls

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Controls [SANS Top 20 Controls][67]
		Impact			
16	**Sabotage**	**[Unauthorised Actions]** Description / Impact	Low	Medium	▪ All appropriate controls
17	**Unauthorised use of Equipment**	**[Unauthorised Actions]** Description / Impact	Low	High	▪ All appropriate controls
18	**Fraudulent copying of software + Use of counterfeit or copied software**	**[Unauthorised Actions]** Description / Impact	Medium	Medium	▪ All appropriate controls
19	**Corruption of data**	**[Unauthorised Actions]** Description / Impact	Medium	High	▪ All appropriate controls
20	**Illegal processing of data**	**[Unauthorised Actions]** Description / Impact	Medium	High	▪ All appropriate controls
21	**Key loggers**	**[Unauthorised Actions]** Description / Impact	Medium	High	▪ All appropriate controls
22	**Forging of Rights + Abuse of Rights**	**[Compromise of Functions]** Description / Impact	Medium	High	▪ All appropriate controls
23	**Denial of Actions**	**[Compromise of Functions]** Description / Impact	Medium	High	▪ All appropriate controls

Appendix D – Risk Register with TPM Controls

The risk register is provided in the table below. The assessment was conducted with the assumption that appropriate SANS top 20 controls were implemented as well as the Trusted Computing controls.

Table *4*: Risk Register *With* TPM Controls

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Trusted Computing Controls Deployed
1	**Theft of Information + Theft of Intellectual Property**	[**Compromise of Information**] Theft of information and intellectual property developed over many years, sometimes up to 15 years, including drug trials, medical compounds, patient information, and confidential research useful for competitors etc. Impact: Loss of potential source of new business income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.	Low	High	▪ Secure Storage ▪ Platform configuration validation ▪ Process Isolation ▪ Symmetric Cryptography ▪ Asymmetric Cryptography ▪ Platform Integrity measurements ▪ Conditional data release ▪ Protection of Cryptographic keys ▪ Protection from other execution environments
2	**Virus, Worms or other**	**[Unauthorised Actions]** Impaired business performance and potential corruption of	Very Low	High	▪ Secure Storage ▪ Platform configuration validation

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Trusted Computing Controls Deployed
	malicious code + Spy-ware	sensitive data affecting integrity of information. Confidential information may be sent to third parties without knowledge. Impact: Loss of potential source of new business income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.			▪ Process Isolation ▪ Remote attestation ▪ Symmetric Cryptography ▪ Asymmetric Cryptography ▪ Platform Integrity measurements ▪ Conditional data release ▪ Protection of Cryptographic keys ▪ Protection from other execution environments
3	**Intentional exposure of private or sensitive information + Disclosure**	[**Compromise of Information**] Disclosure of information developed over many years, sometimes up to 15 years, including drug trials, medical compounds, patient information, and confidential research useful for competitors etc. Impact: Loss of potential source of new business income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.	Very Low	High	▪ Secure Storage ▪ Platform configuration validation ▪ Process Isolation ▪ Remote attestation ▪ Symmetric Cryptography ▪ Asymmetric Cryptography ▪ Platform Integrity measurements ▪ Conditional data release ▪ Protection of Cryptographic keys ▪ Protection from other execution environments
4	**Unauthorised Access to/Use of Information**	**[Unauthorised Actions]** Unauthorised access to sensitive information leading to information disclosure and regulatory	Low	High	▪ Secure Storage ▪ Platform configuration validation ▪ Process Isolation

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Trusted Computing Controls Deployed
	Systems and Networks	violation. Unauthorised use of systems for illegal content download / distribution etc. Disclosure of unpublished material and leaks to press. Impact: Loss of potential source of new business income and competitive advantage, loss of patient for drugs, loss of reputation, regulatory fines and legal proceedings, business disruption, loss of customer confidence, affect on brand value and decline in share price.			▪ Remote attestation ▪ Symmetric Cryptography ▪ Asymmetric Cryptography ▪ Platform Integrity measurements ▪ Conditional data release ▪ Protection of Cryptographic keys ▪ Protection from other execution environments
5	**Illegal Generation of Spam Email + Zombie Machines**	**[Compromise of Functions]** Compromise of systems leading illegal system use for generating SPAM or other automated activity. Compromised systems attacking other entities using business resources by Botnets, Zombies. Impact: Loss of customer confidence, degraded operations, loss of reputation, Judicial proceedings, leak to press, loss of trust, and disruption to partner operations.	Low	High	▪ Secure Storage ▪ Platform configuration validation ▪ Process Isolation ▪ Remote attestation ▪ Symmetric Cryptography ▪ Asymmetric Cryptography ▪ Platform Integrity measurements ▪ Conditional data release ▪ Protection of Cryptographic keys ▪ Protection from other execution environments
6	**Remote Spying**	**[Compromise of Information]** Description / Impact	Very Low	High	▪ All appropriate controls
7	**Eavesdropping**	**[Compromise of Information]** Description / Impact	Very Low	High	▪ All appropriate controls

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Trusted Computing Controls Deployed
8	**Theft of Media or Documents**	**[Compromise of Information]** Description / Impact	Low	High	▪ All appropriate controls
9	**Theft of Equipment**	**[Compromise of Information]** Description / Impact	Low	High	▪ All appropriate controls
10	**Retrieval of Recycled or disguarded media**	**[Compromise of Information]** Description / Impact	Very Low	Medium	▪ All appropriate controls
11	**Data from untrustworthy sources**	**[Compromise of Information]** Description / Impact	Very Low	Medium	▪ All appropriate controls
12	**Tampering with hardware**	**[Compromise of Information]** Description / Impact	Low	Medium	▪ All appropriate controls
13	**Protection Detection**	**[Compromise of Information]** Description / Impact	Low	High	▪ All appropriate controls
14	**Denial of Service Attacks**	**[Unauthorised Actions]** Description / Impact	Medium	High	▪ All appropriate controls
15	**Phishing**	**[Unauthorised Actions]** Description / Impact	Low	Medium	▪ All appropriate controls
16	**Sabotage**	**[Unauthorised Actions]** Description / Impact	Low	Medium	▪ All appropriate controls
17	**Unauthorised use of Equipment**	**[Unauthorised Actions]** Description / Impact	Low	High	▪ All appropriate controls
18	**Fraudulent copying of software + Use of counterfeit or**	**[Unauthorised Actions]** Description / Impact	Very Low	Medium	▪ All appropriate controls

Risk ID	Risk	[Type] / Description / Impact	Likelihood	Impact	Trusted Computing Controls Deployed
	copied software				
19	**Corruption of data**	**[Unauthorised Actions]** Description / Impact	Low	High	▪ All appropriate controls
20	**Illegal processing of data**	**[Unauthorised Actions]** Description / Impact	Low	High	▪ All appropriate controls
21	**Key loggers**	**[Unauthorised Actions]** Description / Impact	Low	High	▪ All appropriate controls
22	**Forging of Rights + Abuse of Rights**	**[Compromise of Functions]** Description / Impact	Low	High	▪ All appropriate controls
23	**Denial of Actions**	**[Compromise of Functions]** Description / Impact	Low	High	▪ All appropriate controls

Appendix E – Project Description Form

MSc Information Security

One copy of this form (or a typed or computer-generated version) is to be completed by each project student and sent (by email) to the project supervisor **by the end of the second semester at the latest**. If the project supervisor is satisfied with the contents then they should sign the form for their own records and inform the student. The student should keep a copy of the final project description form. If the project starts to deviate significantly from the originally approved proposal then the student should discuss this with the project supervisor and, if necessary, complete a revised form.

TO BE COMPLETED BY THE PROJECT CANDIDATE

Name: Stephen S Khan

Contact email address(es): Stephen.S.Khan@gmail.com /
sk@skhan.co.uk

Provisional Title of Project:

1. Statement of Objectives

a. What do you intend to achieve?

1. To establish if Trusted Computing using a TPM provides an additonal level of data assurance on platforms compared to current controls.
2. Perform a security risk assessment on using Trusted Computing TPM controls.
3. Outline some of the challenges in establishing trust.

b. Why have you chosen the proposed project?

I have conducted risk assessements and due diligence on partners during the course of my career for many years. I always found controls around data protection to be very subjective until I came across Trusted Computing at Royal Holloway. Existing mechanisms didn't seem to be effective in establishing trust in business relationships.

I wanted to explore platform data assurance with Trusted Computing using a TPM.

2. Methods to be used

a. How do you intend to achieve the objectives listed above?

I propose to draw on my own experience and draw on other security risk management professionals working in the private and public sector. I used a number of methods including the following:

1. Search for documentation across multiple forums, working groups, conferences.
2. Material form Trusted Computing conference papers.
3. Materials published in OpenTC.net
4. Interviews with people involved Trusted computing and business to business risk management across different organisations in public and private sectors.
5. Source material from past Royal Holloway reports
6. Examination of course material on Trusted computing.
7. Books on Trusted Computing
8. Interview / Open discussion with Industry experts.

b. What is your strategy for getting started?

1. Review current information available from TCG and OpenTC website.

2. Review books on trusted computing.

3. Discussion with security risk management professional about establishing trust in business partnerships.

3. The work plan

Provide a rough schedule, showing any key milestones in the project.

4. June 09 – Review information and make notes.
5. Early July 09 – Conduct interviews with industry experts, government risk managers and private sector security risk managers.
6. Late July – Start to prepare report and review more source materials.
7. August 09 – Prepare report
8. Early September - Hand in report

4. Additional comments

Use this section to make extra comments on the proposal on matters not covered above (use extra space if necessary). Include details of any involvement of external organisations.

TO BE COMPLETED BY THE PROJECT SUPERVISOR

I approve the attached project plan.

Signed:

Name:

Date: