Data sharing using Trusted Platform Module

Organisations increasingly need to share information with partners, but this can open them up to new risks. **Stephen Khan** and **John Austen** explain how a Trusted Platform Module can help organisations gain more control and validate partner data processing environments.

Royal Holloway University of London
SearchSecurity.co.UK

THIS ARTICLE EXPLORES how a Trusted Platform Module (TPM) can help organisations gain more control and validate partner data processing environments. It also introduces and identifies TPM concepts, abilities and limitations. Risk assessments comparing results with and without a TPM are used to highlight the benefits of a TPM and are within the context of sharing clinical trial data although the principles can apply to any data sharing environment.

Many industries including the pharmaceutical industry have been experiencing an unprecedented level of change. This has put pressure on these businesses to pursue new operating models that are cost-effective in a globally competitive market.

Collaboration with business partners is often seen as key to business success as it offers the opportunity to share costs, knowledge, information and expertise in the development of products and services.

Pharmaceutical organisations may share a wide range of information with business partners and across internal business processes that seek to deliver competitive advantage.

Information shared includes:

- **Drug research data** – between research establishments and their partners such as hospitals. For example, case report data containing personally identifiable information about patients.
- **Clinical trials data** – between hospitals, doctors and independent research companies. For example, sampling of patient data whilst maintaining regulatory compliance.
- **Development of new drug compounds** – collaboration between small research companies and universities.
- **Human resources information** – payroll and personally identifiable information on employees for outsourced HR function.
- **Sales and marketing data** – information sent to remote sales forces.

For example, when a clinical trial takes place, information is collected and shared between different organisations relating to an individual. This information must be collected and processed in a controlled environment to maintain integrity of the operating environment and the integrity of the data itself whilst preventing data loss or contamination with other data being processed by the same partner for other clients.

In another example, when information is collected at doctors' surgeries or at hospital, there needs to be validation that the information is being collected using an approved computing

device i.e. a computer terminal connected to a measurement device that has not been tampered with or is not running an incorrect software version which could compromise the trial and invalidate any findings.

In many instances, the information can be considered trade secret. 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 research companies etc.

At present, a business will find it very difficult, if not impossible, to validate the computer processing environments of its partner organisations on a regular basis and therefore must accept the assurances from the partner and ultimately any potential risk to the data.

So why is this important? If data and information are an organisation's key assets, then the organisation needs assurance that its valuable data is not being copied, processed, transferred, or stored in locations either maliciously or intentionally without its consent.

TRUST IN BUSINESS RELATIONSHIPS

Sharing data with partners to meet business objectives requires trust between an organisation and its third party service provider.

To establish this relationship, organisations must ensure they consider the capability and motivation of the service provider. To assure their data is protected they seek compliance with their security risk standards and use a range of approaches to confirm compliance as set out below:

- Accreditations such as BS ISO/IEC 27001
- Audits
- Site visits and inspections
- Review of technical controls
- Interviews
- Reviewing internal partner processes such as change & incident management
- Risk assessments

Whilst the capability is important in terms of controls and processes, one must also consider the motivation of the service provider to protect the client's data assets. These assurances can be incorporated within contracts with specific clauses for data protection. Also, assurances can often be found through recommendations from their customers.

Establishing the capability and the motivation of the service provider can create its own problems. For example, technical controls may not be

managed appropriately allowing breaches to take place. In addition, accreditations may not include an appropriate scope which could lead to security weakness being overlooked.

TPM technology allows for the creation of processing environments with pre-determined conditions as to when data can be processed or released into this processing environment.

The service provider will be motivated to implement controls to prevent the misuse of client's data in order to protect its business reputation.

Instead, misuse may be attributed to factors including human errors, malicious code, unauthorised network connections and inappropriate use of computing resources such as data being copied into external storage devices [1, 3].

Given the sensitive nature of clinical trail data and the impact of the data being damaged, it is important to ensure processing environments are controlled in a manner that gives confidence to regulatory authorities such as the Food and Drug Administration in the USA that data integrity has not been compromised.

TPM technology allows for the creation of processing environments with pre-determined conditions as to when data can be processed or released into this processing environment. For example, if there is a non-validated piece of code, a system has not been patched to the correct level, or the system has been infected with malicious code, then the processing of the data will not be allowed.

Existing controls within information security do not provide this level of assurance.

COMPUTER SECURITY LANDSCAPE

Governments accept that criminals have created a £50bn e-crime industry that needs to be tackled, but current controls have not changed over many years, so a new approach is required.

Recent reports have suggested e-crime is set to continue with governments creating new strategies to combat this area of crime [2]. These strategies will help overcome public fears over data loss and being a victim of the digital economy, such as online credit card fraud.

This is compounded by more open business process models implemented by business to maintain competitive advantage and control costs whilst still protecting their reputation, brand value and standing in a competitive market place. It is also accepted that insiders and outsiders commit similar levels of damage via e-crime [4].

The security industry is always trying to play catch up by patching reported errors only after notification by vendors or the vulnerability becomes public. Common programming errors have been around for years, so criminals may discover vulnerabilities and not report them.

CONTINUE WITH CURRENT PRACTICES OR FIND A NEW TYPE OF CONTROL?

Given the situation that e-crime is set to continue and current controls are not totally effective, do we start to put more controls on the data? If so, what controls?

How do we control where business data can go? How do we (locally and/or remotely) control processing environments? Do we blindly trust our partners or indeed our internal staff to take care of our valuable critical business data? How can we control the rise of programming errors in software?

The answers to some of those questions may vary between organisations depending on their appetite for risk. However, the preference would always be to maintain control of business data.

The next section outlines a technology that gives a greater control over data than has previously been possible by the use of a TPM.

TRUSTED COMPUTING AND ITS BENEFITS

Trusted Computing refers to a computer system which gives a business some level of assurance that part of or all of the computer system is behaving as expected. This is implemented using the services of a hardware component (chip) called a TPM which measures the software components on a computing platform using a range of cryptographic services.

Trusted Computing benefits include (as presented on the Trusted Computing group website):

- Protecting business critical data and systems
- Establishing secure authentication and strong protection of user IDs
- Establishing strong machine identity and integrity
- Ensuring regulatory compliance with hardware-based security
- Reducing 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.

The roots of trust embedded within the TPM underpins information provided for reporting, gathering and storage of evidence about the trustworthiness of the platform software environment, and therefore it must be trusted otherwise the whole TPM creditability and assurance in its measurements are not possible.

WHAT IS A TPM AND WHAT ARE ITS FEATURES?

A TPM is a hardware chip embedded within the motherboard of a computing platform and implemented as part of the BIOS boot block.

What follows next is a simplified explanation of why a platform using a TPM should be trusted.

- During the initial power on stage, the BIOS boot block measures its own integrity and the integrity of the entire BIOS and stores hashed values of this measurement into a Platform Configuration Register (PCR) before passing control to the BIOS and allowing that to execute.
- The BIOS measures the Operating System (OS) loader (the next upstream block of code) and stores its integrity measurements into the PCR before passing control over to the OS loader which performs measurements on the next piece of upstream code (the OS).
- This continues until all of the platform's components have been loaded and the platform is ready for operation.
- A remote entity may request platform configuration measurements. This can be reported to the remote entity which it can compare to known values. For example, the platform is running a particular piece of software at a specific patch level. More importantly, the remote entity is informed of all the components running on the platform. This allows the remote entity to make decisions as to whether it trusts the platform.

In existing environments, can we tell exactly what is truly running on a platform? The authors suggest we cannot.

ISOLATED OPERATING ENVIRONMENT

A TPM could be used to measure the integrity of a platform running applications created purely for processing data for a specific purpose. This would mean any other applications running on that platform could be identified during boot-up.

WHY SHOULD A TPM BE TRUSTED?

A TPM is manufactured in controlled and secure environments by manufacturers who have strong brands to protect. The TPM is a security chip produced and distributed as something that should be trusted. Any adverse publicity would damage the brands and present legal issues as well as affecting their business reputations.

A TPM is manufactured in controlled and secure environments by manufacturers who have strong brands to protect.

ESTABLISHING TRUST ON A REMOTE HOST

This research was concerned with data confidentiality and integrity within business-to-business data processing relationships. The service user needs to be sure the remote partner is operating an environment that 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 software component suppliers.

The exchanges to establish trust on a remote host can occur locally inside an internal network or over communication lines using secure protocols such as the internet via SSL/TLS.

HOW DOES TRUSTED COMPUTING HELP?

Using TPM technology, parties in data processing relationships can request platform state information before using a processing environment.

Having this level of control is clearly powerful and eliminates or reduces all activity as a result of malicious code, viruses, Trojans, and bad applications. 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 validated by external parties. This is not the case for current commercial operating systems or software because of the size of the programs and vast array of functions.

IMPACT OF TPM ON ORGANISATIONAL RISK

Whilst it is widely believed a TPM would reduce risk to an organisation, to date there has been no formal risk assessment to confirm this idea. To

understand this, the author performed a risk assessment to make a comparison of the risk profile before and after the introduction of a TPM. The risk reduction is presented without any consideration of operational and business costs. The approach is purely to understand risk.

Once the list of risks is understood, estimates of their likelihood and possible impact can be determined (risk estimation).

The method employed was to develop the risk profiles based on BS ISO/IEC 27005.

The goal here is to understand risk in data sharing relationships between businesses. To give context and allow for risk analysis, a pharmaceutical business was chosen, although the findings can be applied to any organisation. Within this context, risks were identified (risk identification), i.e. what problems could compromise the business. Once the list of risks is understood, estimates of their likelihood and possible impact can be determined (risk estimation). Depending on the likelihood and possible impact, risks are evaluated (risk evaluation) to develop appropriate controls in response.

STATEMENT OF APPLICABILITY

BS ISO/IEC 27005: 2008 sets out eight types of threat. The authors selected four of these threat types for risk evaluation and estimation.

Excluded risk types are related to major catastrophes or 'force majeure', where the presence of a TPM will have little or no impact on the outcome. The likelihood of these events is also low or very low therefore these risk types have been excluded from the scope of applicability. This is reflected in Figure 1 (see page 9).

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

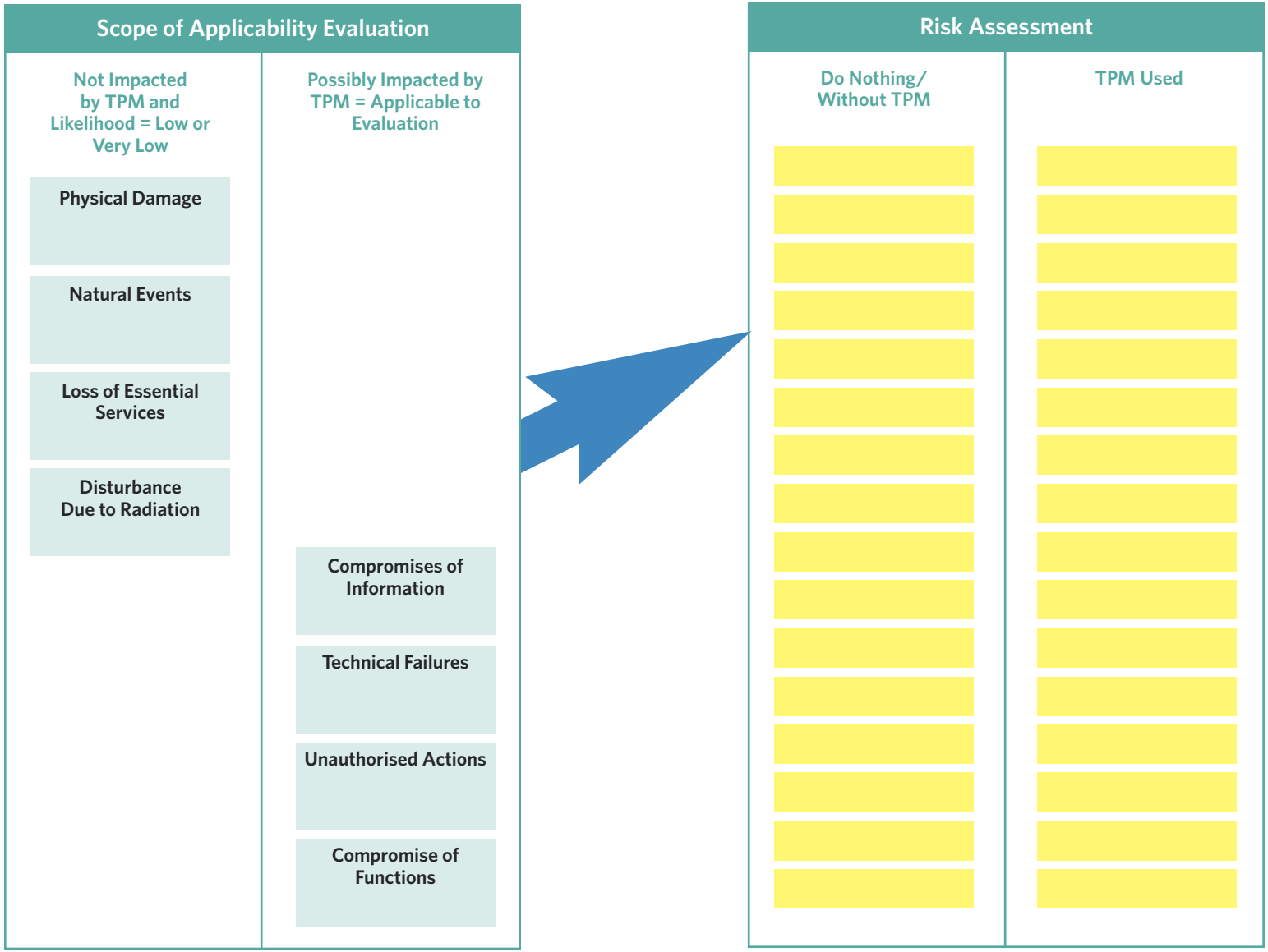
RISK EVALUATION AND ESTIMATION

The risk types in the statement of applicability were expanded further into typical threats and risks as outlined in the 2007 e-Crime Survey [4],

FIGURE 1

ILLUSTRATION OF HOW THE "STATEMENT OF APPLICABILITY" WAS USED TO SELECT RISKS FOR THIS EVALUATION

Source: Stephen Khan MSc dissertation 2009

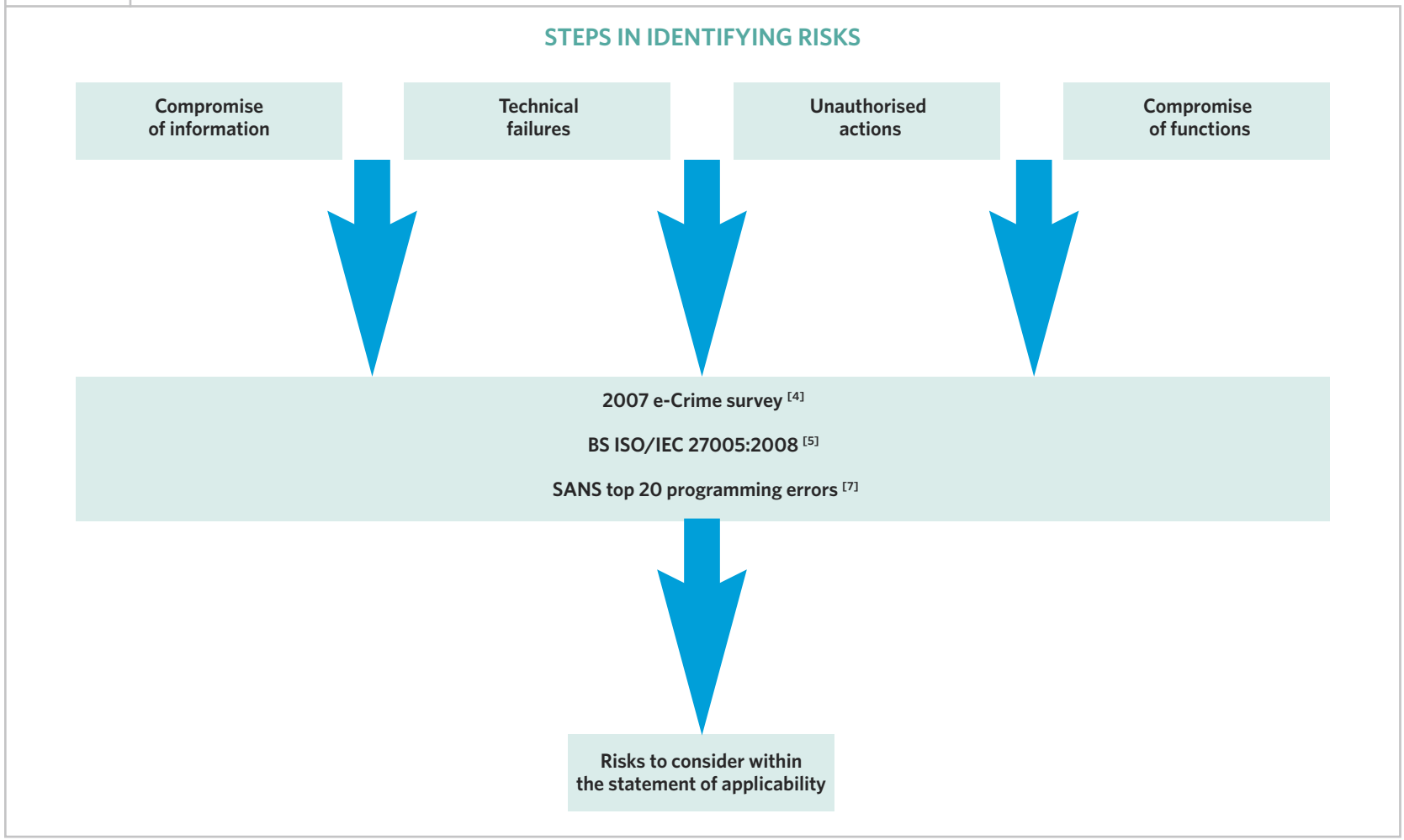


BS ISO/IEC 27005: 2008 [5] and the SANS Top 20 programming errors [7] by the author to establish a linkage between actual risks identified in practice and risks considered in BS ISO/IEC 27005: 2008.

This is shown in Figure 2, (see below).

The authors used this two-step approach to capture the areas where e-crime is most active and to extract the most common risks associated

FIGURE 2



with business-to-business transactions.

The context of this assessment revolves around a pharmaceutical company sending intellectual property in the form of clinical trail data to its service provider to process this data. The processed data will be used by the pharmaceutical

The context of this assessment revolves around a pharmaceutical company sending intellectual property in the form of clinical trail data to its service provider to process this data.

organisation to make decisions on further research or even stop that research stream. The drug development cycle can be 10-15 years, so this data becomes extremely valuable to competitors during the latter stages of this cycle. External bodies will need to establish that data integrity was maintained throughout the development cycle before allowing a drug to be released into the market. For example, if the clinical data has been tampered with or damaged it may cause adverse affects to patients.

To score the risks, source materials [4, 7, and 6] were used to build risk profiles (one with no TPM and the other with a TPM implemented).

RISK ASSESSMENTS WITH AND WITHOUT TPM

The first risk assessment considered all the risks from the statement of applicability and built up the baseline risk register with relevant scoring.

This was followed up with an evaluation of how a TPM can also mitigate these risks. The resulting two risk profiles are compared to establish the gap.

The important consideration here is the relative difference between the likelihood and impact before and after the introduction of a TPM.

In this paper, the overall risk reduction is shown using Trusted Computing from the baseline risk register. The risks addressed by Trusted Computing are related to platforms and not network connectivity, and it is assumed parties would use data sharing via secure connections.

COMPARISON OF RISK PROFILE AND FINDINGS

Trusted Computing controls did reduce the overall risk profile. Table 1 (page 12), highlights the

TABLE 1

RISK REDUCTION TABLE

Risk Areas	Risk reduction
Virus, worms or other malicious code + spy-ware; intentional exposure of private or sensitive information + disclosure; remote spying; eavesdropping; fraudulent copying of software + use of counterfeit or copied software	67%
Phishing; sabotage	50%
Theft of information + theft of intellectual property; unauthorised access to/use of information; illegal generation of spam email + zombie machines; corruption of data; illegal processing of data; key loggers; forging of rights + abuse of rights; denial of actions	33%
Theft of media or documents; theft of equipment; retrieval of recycled or disguarded media; data from untrustworthy sources; tampering with hardware; protection level detection; unauthorised use of equipment	0%

level of risk reduction after the deployment of Trusted Computing controls when compared to the baseline risk register of no TPM implementation. The risk areas represent specifics from the risk register. Comparing the two risk files allowed the calculation of risk reduction of between 33% and 67% by using Trusted Computing.

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 to the risk.

Below is a discussion of how Trusted Computing controls were used to reduce the current risks:

1. Platform integrity using Platform Configuration Registers (PCR)

These registers are critical in preventing and controlling access to data by user programs. If the platform is running an un-validated piece of code or code is started on a system, then the PCR register values will deviate from the conditions required to unseal the data and therefore the data will remain inaccessible.

The regulatory authorities in clinical trails often look for an audit of events, especially when it comes to ensuring the integrity of the data is maintained throughout a drug development cycle. At present, all activity on a computer system in such environments must be documented and logs captured to demonstrate this. With a TPM, the platform integrity can be captured, reducing auditing and system management overhead. The authors suggest these authorities would welcome this kind of control because access to data is controlled and not allowed without specific conditions being met.

2. Sealed / Bound Data

A TPM seals data to the platform, so any attempt to copy information from a trusted platform renders that data useless. It can be argued this offers no more protection than encrypting the data. However, modern encryption schemes do not allow data to be encrypted in such a way that it can only be decrypted by a computing platform in a particular state.

This control prevents data loss and protection of data on mobile devices as well as preventing access to data by malicious software.

3. Software integrity checks

Integrity checks on platform software prevent malicious or compromised software being installed and run on a host.

4. Controlled processing environment

Using the TPM functions, a controlled environment can be implemented in which all data processing is carried out. 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 is 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.

Trusted Computing is particularly useful for pharmaceutical environments in the author's 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 the 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. In essence, anything which could be interpreted as affecting the integrity of the data stored on a system. As the reader can imagine, this is time-consuming and expensive.

Trusted Computing would allow GxP to be applied to a controlled data processing environment which has a small number of applications installed. This allows for controlled auditable

activity to take place in a more manageable and isolated environment leading to lower risks and better assurance for the data.

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 a PCR integrity check of the software.

For example, validated software must be used by the service provider for information processing. Service users can be assured that partners are not using inappropriate software to process their data.

CHALLENGES TO THE ADOPTION OF TRUSTED COMPUTING

A control which offers risk reductions of up to 67% whilst offering higher levels of data assurance would be welcome in any organisation. 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.

The TPM was most effective on risks associated with "compromise of information" and "unauthorised actions". These controls are applicable to pharmaceutical GxP regulated environments because these two types of risks can invalidate drug research information or trial data.

Whilst the TPM offers greater security, the authors suggest there are many challenges to the wide spread adoption of Trusted Computing with the TPM. These challenges include:

- The TPM has a heavy reliance on public key cryptography internally within a TPM implementation and externally from TPM manufacturers. At the time of writing, manufactures are not generally issuing conformance certificates with each TPM. This makes it difficult to enforce liability chains should reliance be placed on a TPM.
- The TPM relies on software configuration measurements stored in a PCR. Currently there are no reliable mechanisms able to record the software measurements.
- Currently the trusted platforms do not come with a measurement firmware or the relevant conformance information upon which a user can build confidence. 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 is where a corporate audience could utilise it for business-to-business applications.
- Cost will be another consideration which has not been discussed during this risk assessment.

CONCLUSION

The authors suggest TPM on servers 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.

The TPM opens the doors to an endless list of secure applications including business- to-business data sharing, digital rights management applications, secure web services and secure peer-to-peer networks.

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 authors cannot think of any other security technology with as much promise as Trusted Computing. ■

ABOUT THE AUTHORS

Stephen Khan has extensive experience of information security within large scale mission critical business environments having held a number of information security roles. His current research interest is in cloud security focusing on what it means for a global enterprise in terms of risks, privacy, compliance and how the cloud changes overall enterprise security architecture.

John Austen is the Course Director for the Royal Holloway Diploma in Information Security. He was head of the Computer Crime Unit, New Scotland Yard, until September 1996. He was a career detective for 30 years, investigating the first major UK computer crime in 1976 and founding the Computer Crime Unit in 1984 - the first of its type in the world.

REFERENCES

[1] http://news.bbc.co.uk/1/hi/7104945.stm - Brown apologises for records loss

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

[3] http://www.scmagazineuk.com/employee-of-hsbc-steals-information-of-24000-customers/article/165579/ Employee of HSBC steals information of 24,000 customers

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

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

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

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