Trusted Information Sharing Network
for Critical Infrastructure Protection

# User-access management

## Summary Report for Chief Information Officers (CIOs) and Chief Security Officers (CSOs)

June 2008

# Introduction

In today's business environment, controlling access to information is essential to long-term competitive advantage. Access control is at the core of all information risk-management exercises, a principle corroborated by a Deloitte Global Security Survey in which 50 per cent of respondents listed access and identity management in the top initiatives pursued in 2007[1].

This report has been developed by the IT Security Expert Advisory Group (ITSEAG) which is part of the Trusted Information Sharing Network (TISN)[2] for critical infrastructure protection.

Responsibility for protecting the organisation's information assets is at the core of the role of the Chief Information Officer (CIO) and, as such, user-access management must be a critical area of focus for CIOs and Chief Security Officers (CSO).

The concept of '*Defence in Depth*' provides an approach to security that is integrated with the organisation's business processes and enterprise-wide risk-management capability.

User-access management supports this approach through ensuring that access is available to authorised users and denied to unauthorised users. This includes controls throughout the areas of:

- User provisioning and de-provisioning (people).
- Operational management of user-access (processes).
- Technical-access controls (technology).

The ITSEAG has released a series of papers on the topic of *Defence in Depth*, to provide guidance on how to effectively layer and integrate security controls to manage the organisation's information security risk.

This paper is part of a set of papers on *User-Access Management* and is a companion to the broader *Defence in Depth* papers which provide guidance on appropriate strategies for mapping and understanding the layers of information that need to be protected.

---

[1] Deloitte, *2007 Global Security Survey*
http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf

[2] TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of nine sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAG), and the Critical Infrastructure Advisory Council (CIAC - which is the peak body of TISN and oversees the IAAGs and the EAGs). More information on TISN can be sought from http://www.tisn.gov.au or by contacting cip@ag.gov.au. The ITSEAG is one of the EAGs within the TISN framework. The ITSEAG provides advice to the CIAC and the sector-based IAAGs on IT security issues as they relate to critical infrastructure protection. It is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. The ITSEAG Secretariat can be contacted on (02) 6271 7018.

The three *User-Access Management* reports are:

- **The full report** extends the core principles in the *Defence in Depth* report to the specific area of user-access management, providing practical implementation examples and specific focus area analysis on key topics within user-access management.
- **The CEO paper** is a summary of the full report designed to highlight to senior executives the importance of user-access management.
- **This Summary Report for CIOs & CSOs** is an extended summary which considers the requirements for effectively deploying user-access management.

## User-Access Management within Defence in Depth

The US National Institute of Standards and Technology (NIST) defines 'access' in an information systems context to be simply the ability to do something with a computer resource (eg, use, change or view)[3]. Given this definition of access, 'user-access management' therefore involves managing who can use, change or view information systems or data, and the circumstances in which such access is permissible.

In order to effectively implement user access management, understanding of the internal environment is key. A process of system and data categorisation and classification is required.

A broad set of business-level objectives for user-access management can be defined as follows[4]:

- Allow only authorised users to have access to information and resources.
- Restrict access to the least privileges required by these authorised users to fulfil their business role.
- Ensure access controls in systems correspond to risk management objectives.
- Log user-access and system use, and ensure auditability is maintained in line with the system's risk profile.

As detailed in the *Defence in Depth* report, the core principles of a successful Defence in Depth strategy are:

- Implement measures according to business risks.
- Use a layered approach such that the failure of a single control will not result in a full system compromise.
- Implement controls such that they serve to increase the cost of an attack.
- Implement personnel, procedural, technical and physical controls.

[3] US National Institute of Standards and Technology (NIST), *Special Publication 800-12*, http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter17.html
[4] Trusted Information Sharing Network (TISN), *Defence in Depth*, http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Publications_e-SecurityPublications, June 2008

# User-Access Management in the Defence in Depth Lifecycle

The full *User-Access Management* report is divided into four (4) main areas, following the lifecycle model for strategic implementation defined in the *Defence in Depth* paper, as applied to user-access management. These areas are:

- **Establishing context –** provides context for user-access management and introduces prerequisite controls necessary for the implementation of effective user-access management within the Defence in Depth framework.
- **Risk analysis –** utilises the risk-analysis methodology in the *Defence in Depth* paper to develop criteria for assessing internal and external risks and threat trends that determine the need for user-access management.
- **Implement user-access management –** provides guidelines for the implementation of a holistic approach to user-access management throughout people, process and technology disciplines.
- **Monitor and review –** analyses current and upcoming user-access management trends to ensure ongoing relevance of the user-access management approach.

# Implementing User-Access Management

A successful user-access management implementation will include the following key components and actions:

- **'Categorisation' and 'Classification' - Clearly categorise and value all data and processing resources, and enable the status of each resource to be correctly 'labelled'**
  Through effective understanding of information asset criticality, business use cases and role responsibility, your organisation can determine the relevance of data to roles (categorisation) as well as the sensitivity of data (classification) to support decision making regarding the allocation of an appropriate level of resources to the protection of its information systems.

- **'Least Privilege' - Provide the least amount of access necessary for a given user to complete their business role**
  Through providing the minimum level of access necessary for a user to complete their business role, your organisation minimises the opportunity for such access to be abused.

- **'Need to Know' - Provide access to systems and information only where there is a need for the recipient of such access to have it**
  Taking the concept of least privilege one step further, this principle states that even in situations where a user has necessary approvals to access a given resource, that access should not be executed unless there is a genuine need for the resource to be accessed by that user at that time.

- **'Controlled Access' - Define procedures to monitor, enable and disable access methods, and enforce security policy at all access points**
  Given a regularly changing access environment, your organisation must have defined and documented procedures for monitoring user-access, and processes for effectively and efficiently enabling and disabling access. Controls must be established across all available access points. These controls should have consistency and be relative to the risk posed by the given access point.

A number of featured controls have been included in the full report covering areas across governance, people, process and technology, with respect to User Access Management. These are:

- User roles and access requirements definition
- Staff commencement management
- Staff termination management
- User role change management
- Education and training
- User activity auditing
- Account and password policy
- Audit changes to controls
- Disable user access (upon departing the organisation)
- Privilege management
- Authenticate users
- Network-access control
- Host-access control
- Application-access control
- Data-access control
- Credential management
- Logging and detection
- Physical-access control

## Trends & Emerging Threats

Industry trends and emerging threats demanding consideration in the context of a user-access management strategy include:

- **Migration to browser-based web applications**. This poses a challenge for user-access management as approaches to authentication and access control need to be understood and implemented. Web application vulnerabilities may leave data and applications at risk of unauthorised access or tampering, and allow circumvention of access controls[5]. The risk of user identity theft at the client-end is also heightened.

- **Migration to web services**. The growing adoption of web services for connecting both internal and external systems presents a significant challenge for user-access management. These systems are often business critical, so the robustness of user-access controls around these web services is particularly important.

- **Use of genuine credentials with malicious intent**. The use of genuine user credentials for malicious purposes has been increasing in recent years. Such credentials are often obtained via a specifically targeted form of phishing attack called 'spear phishing'[6]. This type of attack makes it necessary to find ways to identify unauthorised access to valid user accounts.

- **Growing use of single sign-on technologies**. The growing adoption of single sign-on technologies presents a significant user-access management risk due to the convergence of identities and credentials. In some cases an attacker needs only to compromise one set of credentials to completely assume a user's identity across multiple information systems.

- **Federated identity and trust broker relationships**. Identity federation involves the assembly of identity information from multiple sources and the use of this information across different systems and organisations. Any failure of security controls within the organisation or system managing this process can directly result in unauthorised access to data or resources across a range of organisations.

- **Use of personal mobile devices & equipment**. The increased usage of devices such as smartphones, mp3 players and data storage devices within organisation-owned IT environments increases the difficulty of user-access management, as access to such devices is typically controlled by the user. Organisations looking

---

[5] Open Web Application Security Project (OWASP), *Top 10 2007*, 2007, http://www.owasp.org/index.php/Top_10_2007

[6] Microsoft, *Spear Phishing: Highly targeted scams*, September 2006, http://www.microsoft.com/protect/yourself/phishing/spear.mspx

to address risks proliferated by these devices have to ensure that the connected device's access to the organisation's network is appropriately limited.

## Questions to ask

*Are adequate resources allocated to appropriately deploy user-access management controls?*

Both the analysis and implementation phases of user-access management will require effort and expense. This will be related to the risks and strategies that the organisation has identified and the information environment that controls are to be deployed in. While long-term operational efficiencies may arise from an effective control structure, initially it will be necessary for resources to be allocated commensurate with the size and complexity of the organisation and criticality of its information to ongoing business operations.

*Do we understand our information environments well enough to assess their exposure to user-access-related risks?*

User-access management requires a good understanding of your organisation's information assets and systems, users of these systems and the necessary functions required by users to complete organisation-related tasks and operations. This knowledge is required to assess and design appropriate user-access management methods and controls.

*Do our existing policies and processes provide for ongoing monitoring and review of performance?*

Industry trends and emerging technologies rapidly change the landscape of identity and access management. It is crucial to ensure that user-access management controls are subject to regular monitoring and review to ensure adequate mitigation of emerging threats.

*Does your organisation support an organisational security framework incorporate user-access management that entails consideration of people, processes and technology?*

User-access management controls should be established across these dimensions of your organisation. A strong governance presence will aid the sustainability of user-access management efforts.

*Can we state that our organisation's asset and information accessibility strategies are aligned with the core principles of effective user-access management?*

Information security starts with the leadership of the information technology group. Ensuring alignment with the user-access management core principles will support effective and relevant controls.

## Conclusion

Information assets are among the most valuable assets for many organisations regardless of industry. Ensuring that authorised access is available when required and that unauthorised access is prevented is a key outcome of well-applied user-access management.

The use of the core principles described in this report, based on sound risk management processes along with the examination and implementation of the recommended controls, will ensure that the risk of unauthorised access is minimised and effective control of user-access is maintained.

It is noted that user-access management is only one control area within the full spectrum of information security and should be implemented in concert with complementary controls to provide for Defence in Depth.

## The Trusted Information Sharing Network

Further information, reports and resources are available at the TISN website (www.tisn.gov.au).

The Australian Government provides support to critical infrastructure organisations in maintaining a secure IT environment. Services and support available include:

- Computer Network Vulnerability Assessment (CNVA) Program
- http://www.tisn.gov.au/agd/WWW/TISNHome.nsf/Page/CIP_Projects
- Trusted Information Sharing Network (TISN)
- http://www.tisn.gov.au/
- SCADA Community of Interest - Secretariat - scada@dbcde.gov.au