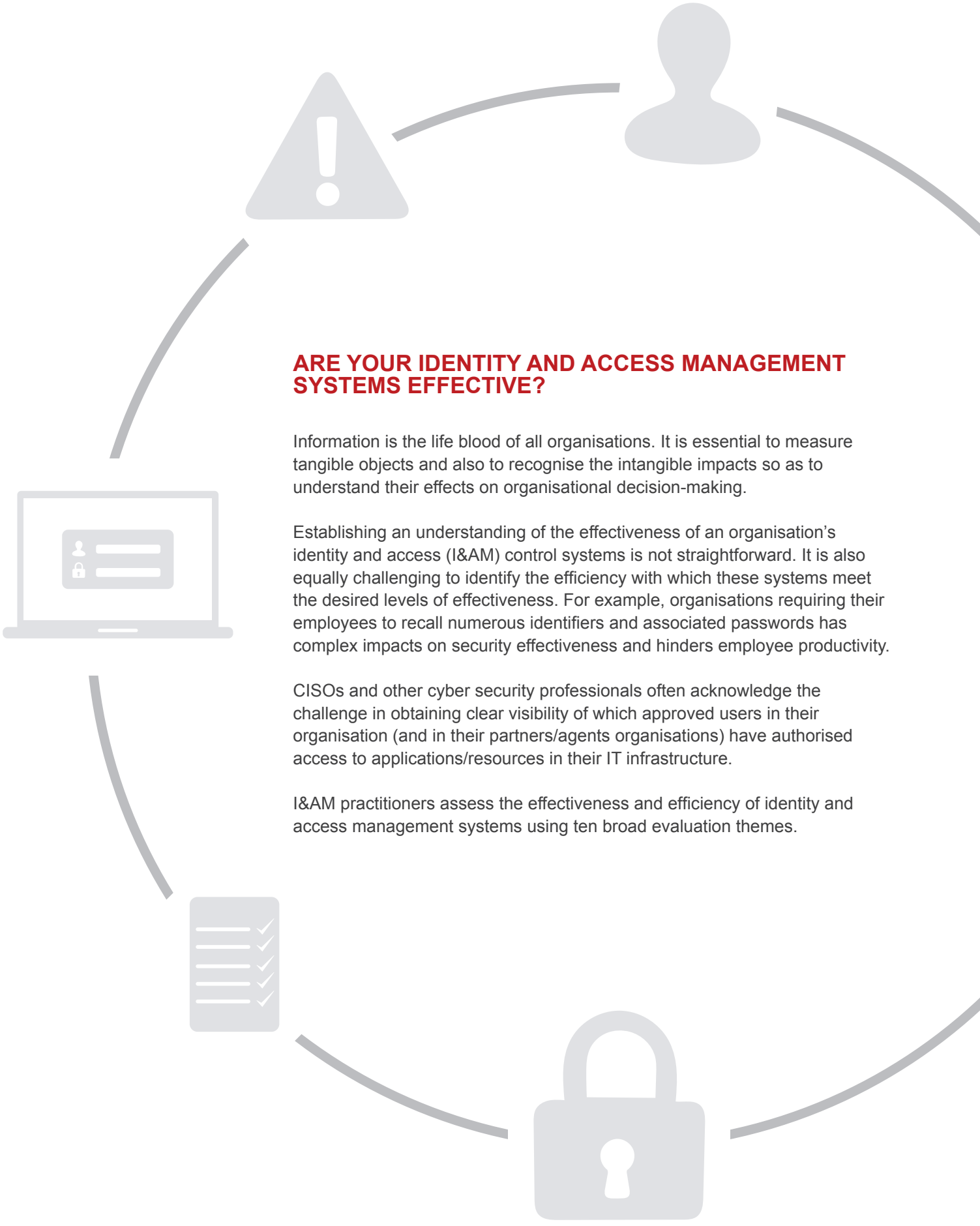
Are your identity and access management systems effective?

ilex International



ARE YOUR IDENTITY AND ACCESS MANAGEMENT SYSTEMS EFFECTIVE?

Information is the life blood of all organisations. It is essential to measure tangible objects and also to recognise the intangible impacts so as to understand their effects on organisational decision-making.

Establishing an understanding of the effectiveness of an organisation's identity and access (I&AM) control systems is not straightforward. It is also equally challenging to identify the efficiency with which these systems meet the desired levels of effectiveness. For example, organisations requiring their employees to recall numerous identifiers and associated passwords has complex impacts on security effectiveness and hinders employee productivity.

CISOs and other cyber security professionals often acknowledge the challenge in obtaining clear visibility of which approved users in their organisation (and in their partners/agents organisations) have authorised access to applications/resources in their IT infrastructure.

I&AM practitioners assess the effectiveness and efficiency of identity and access management systems using ten broad evaluation themes.

FUNCTIONAL REQUIREMENTS

This theme determines the extent to which an organisation's I&AM systems fulfil their functional requirements (e.g. supporting user enrolment, credential distribution etc.) to manage users' (e.g. employees, agents, customers etc.) access to applications/resources.

Functional requirements are derived from an understanding of several factors, including business operational requirements, the characteristics of the user communities and their devices, the applications/resources needing protection, and the technological and regulatory constraints of the operating environments. Political and stakeholders economic interests may also influence an organisation's functional requirements and also their performance requirements to mitigate identified risks to their assets.

PERFORMANCE REQUIREMENTS

Performance requirements relate principally to the accuracy and the speed of an organisation's I&AM systems to authenticate approved users. While biometric user authentication systems strive to meet tough imposter detection and genuine user authentication threshold rates, the true accuracy of some knowledge-based user authentication systems are often masked, i.e. passwords can be phished.

A requirements evaluation should determine acceptable and realistic accuracy/throughput rates, based upon the practical experience in the intended operational environments and the organisation's risk mitigation strategy. These rates should not be set by vendors that have not been corroborated. Empirical evidence suggests that, for some biometric authentication systems, insufficient thought has been given to setting acceptable performance in relation to risks. The inevitable result is that the performance of some biometric-user authentication systems often falls short of an organisation's expectations.

REGULATORY ALIGNMENT, INCLUDING PRIVACY PROTECTION

This theme is designed to assess the ability of an organisation's I&AM systems to demonstrate their compliance with data protection, privacy, social accessibility and discrimination legislation. Equally, this assessment needs to establish the degree to which deployed I&AM systems comply with an organisation's governance and security policies, or possibly international standards.

TECHNICAL RELIABILITY

This theme evaluates an organisation's I&AM system's assurance capabilities to resist attack and/or errors and to detect when its user authentication method has been compromised. An assessment needs to identify unauthorised user attempts in order to establish the resistance capabilities of its user authentication methods to defend against various types of attack, to ascertain the difficulty of producing artefact and/or credential data to circumvent the user authentication system.

Tests planned for an assurance assessment require substantiated data from audit logs which record the user access events and the corresponding administrative actions. The tests should take place during planned day-to-day activities and should additionally allow for unexpected events. Assurance testing should involve individuals from the intended user community in their operating environment in order to augment assurance test data produced under controlled conditions.

USABILITY OF THE USER AUTHENTICATION METHODS

This assessment theme is designed to assess the usability of the deployed I&AM system's user authentication method, particularly regarding the alignment of the user interaction dialogues with the users' everyday tasks.

The inadequacies of HCI security designs often dilute the effectiveness of preventative controls. Despite these usability design deficiencies, security effectiveness is improved by enabling users to make informed decisions from having a better understanding of a device's security operations.

Knowledge based authentication systems mainly attract user password management problems. Increasing the number of password attempts could help users' chances of recollection success. However, this strategy may marginally increase the opportunity of an external adversary obtaining that authentication data.

ACCESSIBILITY OF THE USER AUTHENTICATION METHODS

The criteria in this theme are designed to gage the extent to which the organisation's deployed user authentication methods exclude certain members of the user community.

An organisation's I&AM system's user authentication method may require individuals in the user community to possess specific technologies, sensory skills and/or cognitive skills. Equally, some individuals may fail to enrol for some biometric systems because they are unable to provide signals of sufficient quality, e.g. capturing fingerprint minutiae. Some customers may simply refuse to use an Internet Service and the associated I&AM system due to the unacceptability of some biometric modalities.

I&AM SYSTEM'S MANAGEABILITY

This theme is designed to assess an organisation's ability to manage the computer-application systems, networks, devices and other components\ technologies, during the anticipated lifetime of its deployed I&AM systems. The competencies of the personnel required to support the organisation's I&AM system's components may lead an organisation to seek cloud-based user authentication systems.

TECHNICAL AND NON-TECHNICAL VULNERABILITIES

This evaluation theme relates to the identification of deficiencies in the organisation's I&AM systems and the potential impact in the event that the organisation's I&AM systems are not able to function fully as designed.

This assessment includes the protection of the authentication data upon which user authentication takes place. Non-technical vulnerabilities include the likelihood of user error. Users' capabilities to memorise multiple or complex passwords may lead to undesired behaviour, i.e. saving passwords on devices for easy access.

Additional controls may need to be introduced to minimise the impact of the identified vulnerabilities. However, this invariably increases the expenditure required to mitigate the risks associated with user access control.

IDENTIFIED ISSUES

This theme is designed to evaluate the issues identified during an assessment of the organisation's operational usage of its I&AM systems. According to many security practitioners, all I&AM systems possess vulnerabilities, attract issues and incur costs.

Again, organisations may suffer additional costs in their attempt to reduce the impact of the issues associated with their deployed I&AM systems. The costs associated to mitigate residual risks and identified issues should be proportionate to the value of the assets which are to be protected.

STAKEHOLDERS' COSTS

This theme is designed to review the costs (both direct and indirect) of their I&AM systems to manage risks and to fulfil organisational objectives.

Direct costs relate to the expenditure (capital and operating) of the identity and access management systems themselves. These expenditures include software components, infrastructure costs (network, PKI etc.) and also support, including personnel costs. Indirect costs relate to the losses and recovery/compensation expenditure associated with access control security breaches. Lost productivity may also be construed as an indirect cost.

These cost elements are essential for decisions relating to the deployment of I&AM systems for risks mitigation versus costs considerations, or for security return on investment predictions.

CONCLUSION

Acquired data needs to be evaluated in an analytical framework in order to make sense of information collated from a variety of organisational perspectives, e.g. business activities, risks management, legal and regulatory compliance, IT operations etc. The qualitative data acquired assists in explaining quantitative data gathered during an evaluation.

CISOs need to produce substantiated information in order to describe events – past, present, and future – so their requests for investment in security controls can be supported adequately. The analytical insights gained from evaluating identity and access management systems need to provide intelligence on how and why events happen, the recommended actions, and predictions of impact as input into an organisation's strategy to manage business risks.

ABOUT ILEX INTERNATIONAL

Ilex International is a European Identity & Access Management (I&AM) software vendor. Founded in 1989 Ilex offers a comprehensive solution including identity management (identity, rights and role management) and access management (authentication, access control, SSO, identity federation and card management). The organisation invests heavily in R&D, providing state of the art technology and services to a large international customer base across finance, defence, healthcare, government and retail sectors.

ILEX INTERNATIONAL

info@ilex-international.com
www.ilex-international.com/en/