Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Mergers, Acquisitions and Machinery of Government Changes

First published: July 2019
Last updated: June 2022

Introduction

Major organisational change, such as mergers, acquisitions and Machinery of Government changes, presents significant and unique challenges to cyber security as they create upheaval and disruption to the normal flow of business. In short periods of time, new relationships need to be established, new business processes need to be integrated and systems need to be stood up, merged, relocated or decommissioned as capabilities are moved and consolidated.

Major organisational change also creates significant opportunities for malicious actors, such as:

- established relationships and business processes are replaced by new arrangements creating opportunities for social engineering attacks and other low sophistication techniques to cause significant harm
- different threat environments, risk appetites and security postures between organisations lead to assumptions about the quality and completeness of controls in mitigating security risks
- data can be disclosed to people without a need to know, stored in places without adequate protection or used in ways which exposes it to new, and previously unconsidered, security risks.

The compromise of one organisation prior to a merger can also be leveraged by malicious actors to compromise both organisations if data is exchanged or systems are connected.

The human factor

Malicious actors target organisations undergoing major organisational change because they know the disruption makes it easier for social engineering attacks to succeed. Staff inside an organisation undergoing major organisational change will need to quickly form effective relationships with a new set of colleagues, often while operating with significant uncertainty and time pressures.

During major organisational change, staff may find they are under pressure to accept the validity of requests for access, payment or data from people they don't know, and cannot easily verify the identity and authority of. Malicious actors use this pressure to increase the likelihood of successfully using techniques such as business email compromise.

This problem is further exacerbated if the organisations participating in major organisational change are geographically separated – even more so if the separation crosses national borders or cultural boundaries. To manage this security risk, organisations should:

- brief staff on human risks as soon as possible after major organisational change is announced

- remind staff to refuse requests for access, payment or data until they can verify a person's identity and authority
- put in place arrangements so that staff can readily verify the identity and authority of new colleagues
- organise introductions between staff to help them understand who they should be expecting to deal with.

These steps are effective provided staff are confident they will be supported if they refuse requests due to identity and authority concerns. It is key that management set the right tone and, through their own actions, demonstrate that they accept the small once-off inconveniences that may occur.

Understanding security postures

Understanding security postures between different organisations can be challenging. The key to coming to a quick and accurate understanding is sharing candid information as efficiently as possible.

An exchange of security testing results and cyber security incident registers, and working back from there, will often provide faster and more accurate insight into security postures than exchanging high level documents such as strategies, policies and risk assessments.

Organisations should also consider security testing after major organisational change to verify the security posture of combined systems.

Data migration

During major organisational change, data is often moved to align with a new operating model. Examples include:

- File system migration – Relocation of electronic folders containing documents, spreadsheets, reports, pictures etc.
- Data extract, transform and load – Structured data, such as that stored in a database, is extracted and then loaded into a new system. This can include data from line of business applications, email systems, payroll etc.

Managing security risks during data migration

Online data transfers

When data is migrated using online data transfers, organisations should:

- ensure the communications infrastructure used to conduct data transfers is appropriately secure for the sensitivity and classification of data being transferred
- use two trusted staff to oversee data transfers and verify that data is sent to the intended destination
- use an Australian Signals Directorate (ASD)-Approved Cryptographic Algorithm to generate a checksum prior to and after data transfers to ensure data has not been corrupted or modified in transit
- ensure data is appropriately secured at its destination, including any storage locations where it had to be temporarily staged.

Organisations may also wish to use cloud services as an intermediary for online data transfers. In such cases, organisations should:

- use cloud services that have been authorised for the sensitivity and classification of data being transferred
- limit access to only those staff and systems involved in data transfers.

Organisations should also consider that activities associated with online data transfers may present a cover for data exfiltration by malicious actors and, as such, should put in place any additional controls considered appropriate.

Finally, organisations are reminded that the *Privacy Act 1988* obligates them to take reasonable steps, such as those outlined above, to protect personal information in their possession.

Physical data transfers

When data is migrated using physical data transfers, organisations should:

- encrypt media using an ASD-Approved Cryptographic Algorithm
- transfer media from person to person using trusted staff
- protect media in an appropriately secure briefcase or container during transit.

In addition, the *Information Security Manual* (ISM) specifies controls relating to encryption of data at rest. Furthermore, protective security requirements within the Department of Home Affairs' *Protective Security Policy Framework* (PSPF) should be reviewed and applied as appropriate.

Organisations conducting physical data transfers should be mindful that media used for data transfers will likely retain a recoverable copy of data previously stored on it. This is particularly relevant if organisations do not use encryption. As such, media should be sanitised before being released for reuse or disposal. The ISM contains guidance on media use, sanitisation, destruction and disposal.

Preparing for security risks after data migration

Preserving file system permissions

When importing data into a new system, additional steps may need to be taken to preserve access control lists. In many cases, there will be no native support to move access control lists between different systems, such as between two Microsoft Windows servers in different domains. However, aftermarket tools and other processes are available to support this if needed.

New business rules

When importing data into a new system, it may be subject to a different set of business rules and organisations may unintentionally provide more access than required. Before importing data into an existing system, organisations should review system, security and data architectures to satisfy themselves that access remains in line with business rules and security principles, such as the need-to-know principle and the principle of least privilege.

Importing bad data

When importing data into a new system, reasonable steps should be taken to ensure data is free from malicious code. As such, organisations should scan imported data with two high quality antivirus products with up-to-date signatures. This should include scanning imported email boxes irrespective of whether they come in database format or not.

Different security contexts

When importing data into a new system, it may be exposed to a greater security risk if imported into a system with a lower security posture. As such, data custodians should ensure that their data will be protected with an equivalent or greater level of security following any data transfers. Alternatively, if there is to be an increase in security risk, this should be accepted by data custodians before any data transfers take place.

Organisations are reminded that the Privacy Act obligates them to take reasonable steps to protect personal information in their possession, including assessing the security posture of any other organisation they share such information with.

Decommissioning old data holdings

Once it has been confirmed that data has been transferred between organisations successfully, organisations may need to delete any historical copies. In such cases, organisations should be mindful of their need to retain official records in accordance with the legislation in their jurisdiction and should seek advice from their archives office.

Organisations are also reminded that the Privacy Act requires them to either destroy or de-identify personal information if they no longer have a valid reason to retain it. Organisations should review the *Australian Privacy Principles* and the Privacy Act for further information.

For specific advice on how to sanitise media and dispose of ICT assets, organisations should review guidance in the ISM. Organisations should also consider how they address their cloud holdings. For specific advice on how to sanitise cloud storage and compute, organisations should consult their cloud service provider's advice. Finally, for destruction of physical records, organisations should seek guidance from the PSPF.

System migration

Creating an exhaustive list of cyber security issues that may arise out of system migration is beyond the scope of this publication, however, organisations should consider the following high level issues.

Inheritance of technical debt and security risk

Organisations can find that they inherit a substantial amount of technical debt, and associated security risk, during major organisational change. To assist with identifying this, system patching and support levels can provide an insight into the attention and care paid to inherited systems by their previous owners. In doing so, organisations inheriting systems may also need to look beyond what is listed in inventories, or configuration management databases, as the greatest technical debt is often hidden in systems that are not properly monitored or listed in inventories. Use of a discovery capability, such as an automated vulnerability scanner, may help organisations build a more comprehensive picture of inherited systems, and their security postures, that need to be accommodated as part of system migration activities.

If organisations plan to join their systems with inherited systems, and one of the inherited systems has already been compromised, then lateral movement by malicious actors into newly connected systems can be trivial depending on the inherent trust built into underlying technologies. As such, organisations may have to consider how they will

develop reasonable assurances that inherited systems are not the subject of an active compromise. Alternatively, organisations may find it is easier and safer to build new versions of existing services from inherited systems in a new system, along with migrating users and data, than to try and 'lift and shift' services in an unknown state from an organisation with a lower security posture.

Cyber security governance

Organisations will need to determine who will become the system owner of inherited systems before authorising their operation in accordance with their organisation's cyber security framework, including the acceptance of any additional technical debt, and associated security risks, resulting from system migration activities.

Organisations may also need to consider whether existing security documentation needs to be reviewed and revised. For example, cyber security strategies, policies and procedures may need to be updated to align responsibilities and authority in the new organisational structure. Cyber security incident response plans may also need to be updated to reflect new contacts, teams and escalation points.

Cyber security incident response planning

Organisations may find themselves having to respond to cyber security incidents during or immediately after major organisational change. If this occurs, it will be highly beneficial if well developed relationships between cyber security incident response teams in each organisation are already in place. Organisations should consider how they can establish these relationships early in planning for major organisational change.

Ecosystem fit

Inherited systems are often complex, with ecosystems that may not be well understood by an organisation's technical workforce. As such, organisations inheriting systems as part of system migration activities should consider whether they have sufficient expertise and capacity to support new operating systems, databases, application servers, network technologies, cloud infrastructure and applications, including the languages, frameworks, application programming interfaces and cloud services used to support them.

Where organisations do not have sufficient expertise and capacity to support new systems, and their associated applications, they will need to consider how such capabilities can be acquired and put in place.

System availability

System migration planning, which typically focuses on issues related to business interruptions, should also consider any reduction in availability protection that may occur as part of system migration activities. For example, some organisations operate distributed denial-of-service mitigation measures, leveraging public cloud services, while others operate less capable on premise solutions. Organisations should consider only reducing the availability protection afforded to systems if security risks are well understood and accepted.

Identity and access control

Issues related to how identity is provisioned will typically be considered as part of system migration planning. For example, identity may be provided to an application internally (e.g. recorded in a connected database), provided via an external directory (e.g. a corporate active directory) or provided via a third party (e.g. a federated identity solution). In all cases, organisations need to consider that mechanisms that protect systems may not be integral to the system itself. For example, a multi-factor authentication solution may rely on integration through a corporate identity directory, which may not be moved as part of a major organisational change. To accommodate for these situations as best as possible, organisations should review system security documentation and previous configuration change

tickets, in addition to speaking to previous support staff, including any gateway and cyber security staff, to identify external controls which protect that system.

Conclusion

Cyber security is a critical consideration during any major organisational change. In order to manage associated security risks, organisations should focus attention on the following three areas:

- ensuring systems and data are well integrated into their new organisation
- ensuring equivalent or greater protection is afforded to systems and data in their new operating environment
- where possible, minimising the accumulation and compounding of technical debt due to the migration of systems and data.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

The *Protective Security Policy Framework* articulates the Federal Government's protective security policy and provides guidance to Commonwealth entities in areas including security governance, personnel security, physical security and information security.

For broader advice on Machinery of Government changes, Commonwealth entities should review the Department of Finance and Australian Public Service Commission's *Machinery of Government changes* guide.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate