Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Mergers, Acquisitions and Machinery of Government Changes

JULY 2019

Introduction

Major organisational change, such as mergers, acquisitions and Machinery of Government (MoG) changes, present significant and unique challenges to cyber security as they create significant 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 and decommissioned as capabilities are moved and consolidated.

Major organisational change creates significant opportunity for adversaries:

- Established relationships and business processes are replaced by new arrangements creating opportunities for adversaries to use social engineering and other low sophistication methods to cause significant harm.
- Different threat environments, risk appetites and security postures between organisations lead to assumptions about the quality and completeness of security controls in mitigating security risks.
- Systems can be misconfigured leaving them vulnerable to compromise.
- Data can be disclosed to people without a need to know, stored in places without adequate protection or used in ways which expose it to new, and previously unconsidered, security risks.
- Adversaries can leverage the compromise of one organisation prior to the merger to compromise both organisations if data is exchanged or systems are connected.

For broader advice on MoG changes, public sector organisations should review the MoG guide issued by the Australian Public Service Commission (APSC)[1].

The human factor

Adversaries target organisations undergoing major organisational change because they know the disruption makes it easier for social engineering attacks. 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 data, payment or access from people they don't know, and cannot easily verify the identity and authority of. Adversaries use this pressure to increase the likelihood of successfully using techniques such as business email compromise and CXO impersonation.

[1] https://www.apsc.gov.au/sites/default/files/machinery_of_government_guide_2019.docx

The 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. For public sector organisations, in line with the APSC's MoG guide, this should be part of providing early advice and assistance to staff[2].
- Remind all staff they should refuse requests for access, payment or data until they can verify the requestor's identity and authority. Identity should preferably be established in person or via telephone using contact details known to be correct.
- Put in place arrangements so that staff can readily verify the identity and authority of new colleagues and inform them of this mechanism in the initial brief (e.g. online organisation charts and valid email addresses). Staff should also be encouraged to use trusted third parties (e.g. a colleague they know who can verify another person) to help deal with ad hoc identification.
- Organise introductions between new staff as quickly as possible to help everyone understand who they should expect to be dealing 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.

Additional advice on people management for public sector organisations can be found in the APSC's MoG guide[3].

Understanding security postures

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

An exchange of security testing (e.g. penetration 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 policies, strategies 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 typical electronic folders containing documents, spreadsheets, reports, pictures etc.
- Data Extract, Transformation and Load – Strongly typed 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, personnel, payroll, etc.

[2] https://www.apsc.gov.au/machinery-government-mog-changes-executive-summary
[3] https://www.apsc.gov.au/machinery-government-mog-changes-people-management

Managing security risks during data migration

Where data is being migrated using online transfer, organisations should:

- Ensure the destination environment and the communications infrastructure used to conduct data transfers are appropriately secure (e.g. via the use of encryption) for the sensitivities and classifications of data being transferred.
- Use two trusted staff to oversee the transfer and verify that data is being sent to the intended destination. On significant data transfers the investment in an extra set of eyes to double check details is worthwhile.
- Use an Australian Signals Directorate (ASD) Approved Cryptographic Algorithm listed within the ***Australian Government Information Security Manual*** (ISM)[4] to generate a checksum prior to and after the transfer to ensure that data has not been corrupted or modified in transit.
- Ensure data is appropriately secured in its destination environment, including any storage where it is being temporarily staged.

Organisations should also consider that activities associated with legitimate data transfers may present a cover opportunity for data exfiltration by advanced adversaries and as such should put in place any additional security controls considered appropriate.

Using public cloud as an intermediary

Organisations may also wish to use public cloud storage as an intermediary in transferring data. In such cases, organisations should:

- use cloud storage from a vendor on the Government's ***Certified Cloud Services List***
- for private, sensitive or classified data, use an ASD Approved Cryptographic Algorithm to encrypt the data before it is transferred
- ensure the cloud storage has appropriate access controls and limits access to only those staff and systems involved in the data transfer.

For Commonwealth entities, the ISM specifies security controls relating to encryption (security control 1162) and use of public cloud for official and classified data (security control 1395). These security controls should be reviewed and applied as appropriate.

Organisations should only consider transferring unencrypted data to public cloud storage if that would be in line with their existing operating models.

Organisations are reminded that the ***Privacy Act 1988***[5] (the Privacy Act) obligates them to take reasonable steps, such as those outlined above, to protect private information in their possession.

Physical data transfers

For physical data transfers, organisations should:

- encrypt data using an ASD Approved Cryptographic Algorithm with key transferred via an alternate secure path
- transfer the media containing the data from person to person using trusted staff
- protect the media in an appropriately secure briefcase or container during transit.

[4] https://www.cyber.gov.au/ism
[5] https://www.legislation.gov.au/details/c2014c00076

For Commonwealth entities, the ISM specifies security controls relating to encryption of data at rest outside Security Zones (security controls 1161 and 0459). Furthermore, recommendations in the Attorney-General's Department's ***Protective Security Policy Framework*** (PSPF)[6] for official and classified data should be reviewed and applied as appropriate.

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

Preparing for security risks after data migration

Preserving file system permissions

When transferring file systems, organisations may need to take additional steps to preserve access control lists. In many cases there is no native support to move access control lists between different systems (such as between two Microsoft Windows servers in different domains). Aftermarket tools and other processes are available to support this requirement if needed.

New business rules

If data is imported 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 and data architecture, business rules, and security architecture with a view to the newly imported data and satisfy themselves that access remains in line with business rules and cyber security principles such as least possible privilege.

Importing bad data

An organisation importing file system data should take reasonable steps to ensure data is free from malicious software. Organisations should scan the 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.

Microsoft Office macro security

Organisations that have implemented Microsoft Office macro security, in line with the Essential Eight[7], may need to consider how they will vet and approve any macro enabled files which arrive as part of a data transfer.

Organisations which only permit vetted and approved macros to run will need to ensure that incoming staff understand the process for macro vetting and approval. The staff that vet macros should be prepared for a spike in workload in the short term, with a scaled increase in workload based on the size of the new organisation in the long term. Additional staff may need to be allocated to this role.

Organisations may also need to identify any critical macros that support key business functions so that review and enablement of these macros can be tasked as part of the data transfer activity to minimise interruption to business.

Different security context

Data that arrives as part of a data transfer may be exposed to a greater security risk if it is placed in an environment with a lower cyber security posture. Organisations should pay particular attention to high value assets including:

[6] https://www.protectivesecurity.gov.au
[7] https://www.cyber.gov.au/publications/essential-eight-explained

- sensitive data about people
- key intellectual property
- commercially sensitive data.

Before transferring data, the current custodian or owner should ensure that the data will be protected with an equivalent or greater level of security at the destination. Alternatively, if there is an increase in security risk, then this should be communicated to the current and new owners.

Organisations are reminded that the Privacy Act obligates them to take reasonable steps to protect private information in their possession, including assessing the security context of any partner or other organisation they share private 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 private information if they no longer have a valid reason to retain it. Organisations should review the ***Australian Privacy Principles***[8] 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 arise out of system migration is beyond the scope of this document. However, organisations should consider the following high level issues.

Cyber security basics

Are systems still under vendor support? Are systems patched and up-to-date? What systems are not being monitored or are not in the inventory?

Organisations can find that they inherit a substantial amount of technical debt and associated security risk during major organisational change. While a high level understanding of the number and type of different platforms and applications provides one view, looking at patch and support levels provides an insight into the attention and care paid to systems operated under business as usual arrangements.

Organisations inheriting systems may also need to look beyond what is reported in inventories or configuration management databases as the greatest technical debt is often hidden in systems that are not properly enrolled in monitoring and management systems.

Use of a discovery capability, such as an automated vulnerability scanner, may help organisations build a more complete picture of what they need to accommodate, including the security posture of systems in question.

[8] https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

Ecosystem fit

How will new systems be patched, backed up, monitored and managed?

Systems are often complex. In addition to the applications, systems also rely on operating system and application server platforms which may not be known inside an organisation's existing technical workforce.

Organisations should consider whether they have:

- Sufficient expertise to support applications, including developers familiar with the languages, frameworks, application programming interfaces and cloud services used to develop them.
- Existing capability to support the underlying operating system, database, application server, network technology, cloud infrastructure and other dependencies. Support should include:
    - expertise
    - compatible patching platform and capabilities
    - backup infrastructure
    - monitoring and configuration management (including log management and review).

Where organisations do not have sufficient capability, they will need to consider how that capability is put in place.

Cyber security governance

Organisations will need to consider who will become the new system owner of migrated systems. They will also need to consider who will accept the security risks before authorising the operation of the system in accordance with the organisation's cyber security framework, including any additional security risks and technical debt resulting from the migration.

Organisations may also need to consider whether existing security documentation needs to be reviewed and updated. For example, policies and Standard Operating Procedures may need to be updated to align responsibilities and authority into the new organisational structure. Incident Response Plans may also need to be updated to reflect new contacts, teams and escalation points.

Incident response

Organisations may find themselves having to respond to cyber security incidents during or after major organisational change as a result of dependencies between systems that cross organisational boundaries. If this occurs it will be highly beneficial if there is already well developed relationships between the operational cyber security teams in each organisation. Organisations should consider how they can establish these relationships early in planning and promote their use during the change.

Availability

Conventional systems migration planning will typically address issues related to business interruptions during major organisational change. However, organisations should consider any reduction in availability protection occurring as part of system migration. For example, some organisations operate significant distributed denial of service mitigation measures leveraging public cloud, while others may operate less capable on premise solutions. The protection afforded a system should only be reduced if the security risk is understood and accepted.

Organisations should also consider availability risks related to not being able to restore data. Organisations which cannot recover their data after a cyber security incident often fail. The Essential Eight provides additional advice on

backups, including the importance of offline, or non-rewritable and non-erasable, backups to prevent damage from ransomware and similar adversary tactics.

Joining networks

Joining networks provides adversaries with a significant opportunity to move laterally into a different organisation's environment should one network already be compromised. Organisations should take care to only permit the network services that are required through any organisation to organisation communication links.

If organisations plan to join environments, and one of those environments has already been compromised, then lateral movement into the other environment can be trivial depending on the inherent trust built into the underlying technology. If environments are to be joined, organisations may have to consider how they will develop reasonable assurances that neither environment is the subject of an active compromise. Organisations may find it is easier and safer to build new versions of existing services in a new network, and migrate users and data, than to try and 'lift and shift' servers which are in an unknown state and exist in an organisation with a low cyber security posture.

Organisations should consider the use of gateway technologies such as proxies as well as scanning and monitoring infrastructure for communications links between organisations. The ISM and the ***Strategies to Mitigate Cyber Security Incidents***[9] provides additional advice in this regard.

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 (identity is recorded in a connected database), via an external directory (such as a corporate active directory) or via a third party (such as a federated identity solution).

In all cases, organisations need to consider that mechanisms that protect systems are not always 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 being moved as part of major organisational change.

The greater concern however is not the security controls which are obvious (because they affect user experience and/or availability) but rather those that are unseen by the user, such as those that monitor and react when suspicious activity is detected. For example, monitoring to detect identity abuse which occurred in the previous owner's Security Operations Centre or security controls which relied on capabilities which are not part of the destination system's technology stack, for example, different end point security agents, gateway and proxy technologies.

To accommodate for these situations as best as possible, organisations should review:

- system security documentation
- tickets for configuration changes to the system over its operating life
- staff that support the system, including any gateway and cyber security staff, to identify external security controls which protect that system.

Conclusions

Cyber security is a critical consideration as part of major organisational change. To manage the increased security risks, organisations should focus attention on the following three areas:

- minimise the accumulation and compounding of technical debt

[9] https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents

- ensure data and systems are well integrated into the new organisation to ensure they are properly patched, supported and monitored
- understand the security controls which protected data and systems in their previous operating environment and ensure appropriate and ideally equivalent, or greater, protection is afforded in its new operating environment.

Further information

The ***Australian Government Information Security Manual*** assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

The ***Privacy Act 1988*** is the legislations that governs the collection, storage and disclosure of private information by Australian organisations. It can be found at https://www.legislation.gov.au/details/c2014c00076.

The ***Australian Privacy Principles*** are contained in the Privacy Act and outline how Australian organisations must handle, use and store private information. It can be found at https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles.

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. It can be found at https://www.protectivesecurity.gov.au.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).