Protecting Critical Infrastructure and Systems of National Significance

Consultation Paper

September 2020

Abstract

This consultation paper is in response to the Department of Home Affairs Critical Infrastructure Centre public request for submissions.

Dell Technologies

Dell Technologies provides the essential infrastructure for organisations to build their digital future, transform IT and protect their most important asset, information. Dell is a collective force of innovative capabilities, trusted globally, to provide technology solutions and services from the edge to core, to cloud.

We are an organisation that embraces risk, change and makes big, smart bets. From our forward-thinking investments in the future of IT to Dell's privatisation, to the Dell + EMC combination, Dell Technologies is defining change in the marketplace. Our unique structure as a family of businesses enables us to attract the very best talent to innovate like a startup while offering the trust, service and global scale of a large enterprise.

Executive Summary

Dell Technologies is a global provider of Data Protection solutions and services to organisations and government agencies across the global. We help entitles architect and maintain a data recovery strategy that can address a variety of incidents, including infrastructure failures, software failures, human failures, data corruption, insider threats and cyber related events. Recently, Dell has observed an escalation in the tactics, techniques and procedures employed by malicious threat actors seeking to extort funds from organisations. These techniques involve intent to compromise all data copies held by an organisation, including data backup system copies, that are used to recover from such events. These threat actors have realised to execute successful extortion campaigns, they need to paralyse an organisations data recovery capabilities. While we continue to educate the industry at large, it is clear organisations across Australia are not acting to mitigate these threats. On the contrary, we have seen many organisations throughout the United States strengthen their recovery capabilities to defend against such incidents. The extent of these incidents is not limited to our observations. In the latest Australian Cyber Security Centre Annual Cyber Threat Report (July 2019 to June 2020), the ASCS states "*ACSC has observed sophisticated cybercriminals conducting significant victim research on networks they have compromised prior to deploying ransomware. Cybercriminals will locate and target backups which have not been isolated from the network or internet, maximising the impact of their ransomware and increasing the likelihood of victims paying ransoms to them*".

The Strategies to Mitigate Cyber Security Incidents was published by the Australian Cyber Security Centre in 2017 and adopted by various organisations including the Australian Government. We believe these strategies should be reviewed considering the recent and emerging threat to data recovery systems, highlighted in the recent ACSC report. Specifically, we recommended additional controls are implemented to mitigate against these threats, particularly for organisations and governments supporting Australia's critical infrastructure. The remainder of this paper outlines the existing mitigating strategies that may be open to compromise, and proposed methods to further strengthen the mitigation strategy.

Mitigating Strategy to Limit the Extent of Cyber Security Incidents

The Australian Cyber Security Centre guidelines for mitigating Cyber Security incidents call for multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access on important (sensitive/high availability) data repository. In the

case where backup systems are classified important data repositories, the presence of multi-factor authentication does not prevent an insider with privileged access, from compromising the backup data repository. In a plausible worst-case scenario, the insider may have access to both production data repositories and backup data repositories, and could compromise both, rendering business-critical systems unrecoverable from backups.

To mitigate this threat, multi-step authentication should be required for backup data repositories. In a multi-step setting, a privileged user that attempts to execute destructive commands, such as wiping backup systems, will not be possible, without the involvement of a second independent authority. The second independent authority is required to approve the action using independent credentials that should not be known by the initiator or stored in a common database. In a typical setting, the second authority, along with their credentials, are designated and managed by the entity's security office.

In addition, data backup systems should employ write-once read many technologies that prevents a user with privileged access rights, from intentionally or unintentionally wiping copies of backup data prior to the data copies reaching their expiration period. This control should be enforced by the backup system housing the data, and the system should be hardened so that adversarial measures, such as turning back the system clock, cannot be used to circumvent the control.

These controls are designed to mitigate the scenario where backup data repositories are wiped intentionally or unintentionally by insiders with privileged access rights.

Mitigation Strategies to Recover Data and System Availability

The Australian Cyber Security Centre guidelines for mitigating Cyber Security incidents call for daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months, with test restoration performed initially, annually and when IT infrastructure changes occur.

Daily backups are essential to ensuring a recovery position is maintained for critical systems. However, a regular data backup is not immune to infection, as they are carbon copies of production data which is susceptible to malware and ransomware infection. In the event backup systems are used to recover from a major cyber event, one of the first actions an entity needs to perform is to forensically verify whether the backup copies are infected or compromised. This process of forensic verification can significantly increase the complexity and time necessary to recover IT systems. In the meantime, critical systems remain down for extended periods of time. Similarly, in the event a malicious threat actor conducts reconnaissance in the network for extended periods of time, it is conceivable all backup copies are compromised. This would further extend recovery times, as many backup copies would need to be forensically analysed to identify the extent of the compromised data, prior to then cleaning the copies and initiating critical system recovery.

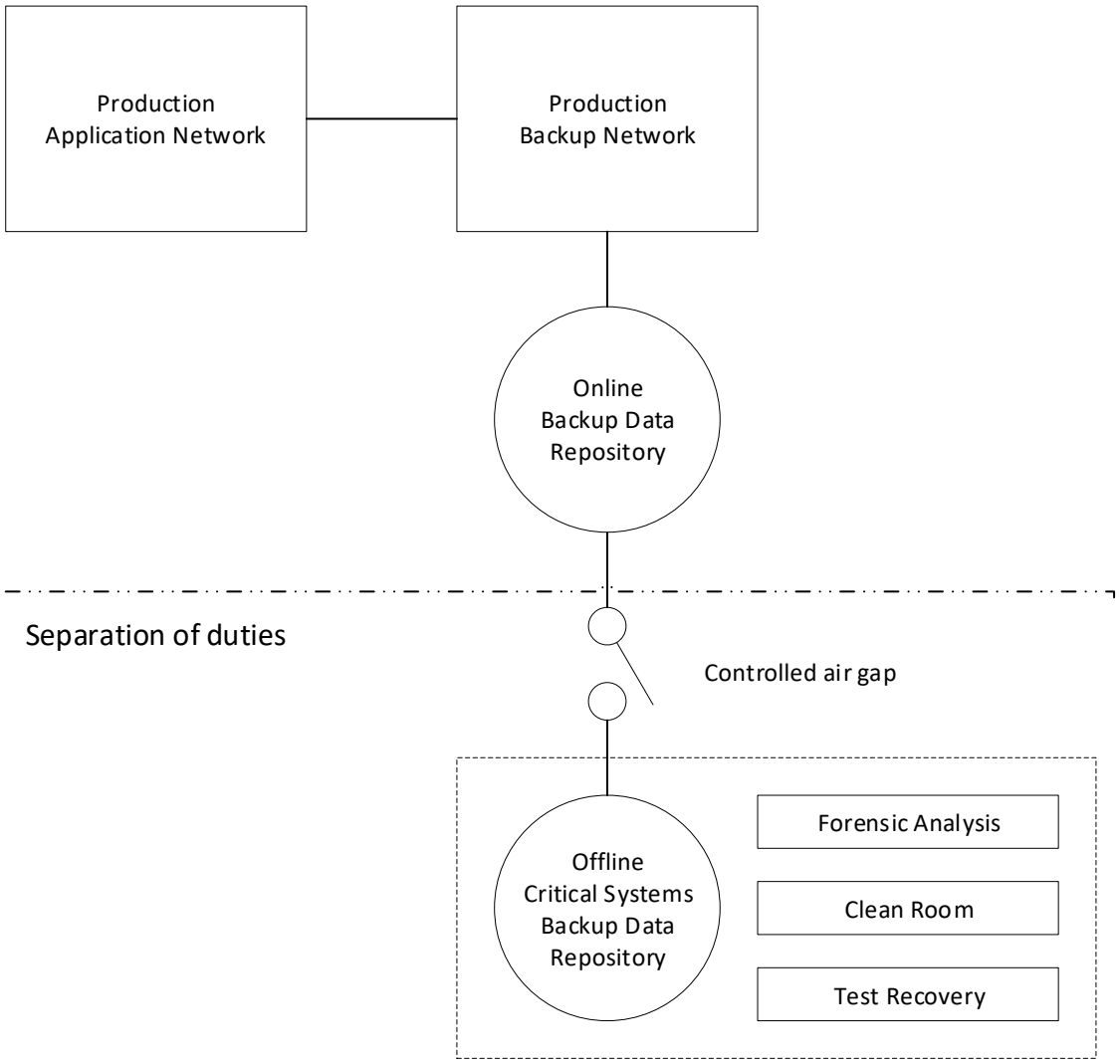
The current guidance also recommends full backup restoration is tested when the backups are first implemented, and each time fundamental information technology infrastructure changes. Partial restoration is recommended on a quarterly or more frequent basis. While these are sound guidelines, they often provide a false sense of security, that backups are recoverable, at any moment notice. The challenge is depending on manual processes to conduct verification tests does not scale when large volumes of data is involved. This often manifests itself in infrequent and partial testing, which is not

sufficient to identify compromised and infected backups and may leave entities exposed for prolonged periods of time.

Dell recommends a pro-active approach to backup copy verification that uses forensic methods to uncover suspicious patterns in backup copies. This active approach to forensic copy verification would rely on automated systems and methods that actively scan backup data to uncover suspicious patterns in backup copies and between backup copies. This control is designed to uncover compromised backup copies to avoid reinfection in the event of an incident, and to eliminate the reliance on manual processes which are susceptible to human error and complacency. Most importantly, this control is designed to maintain positive identification of backup copies that have been cleared of suspicious activity prior to a cyber incident, so that a moment's notice, data can be recovered. To implement these controls, Dell also recommend entities establish a tertiary backup copy that is isolated from regular backups, by a controlled air gap. This ensures the process of forensically verifying and cleaning backup copies does not interfere or contaminate regular backup and restoration activities, which need to remain online and accessible to deal with regular day-to-day incidents. In summary, these additional controls are designed to be pro-active in nature and rely on a tertiary backup copy that serves five primary purposes.

1. It provides a means to respond to a major incident in rapid succession, by disconnecting the critical systems backup data repository, and securing copies of all critical system data.
2. It allows the entity to address reinfection, whereby the tertiary backup copies can be used to conduct forensic analysis, and provide a clean room, in the even production data has been compromised and infiltrates the backup copies.
3. It allows the automated forensic verification of backup copies, without fear of spreading malware, due to restoration and verification activities.
4. It provides a tertiary backup copy that is offline majority of the time and reduces the attack surface by adversaries present in the network.
5. It provides complete separation of duties without impacting regular day-to-day backup and restoration activities.

The following diagram illustrates how an entity's existing backup environment may be adapted to comply with these controls.



Regulate versus Active Enforcement

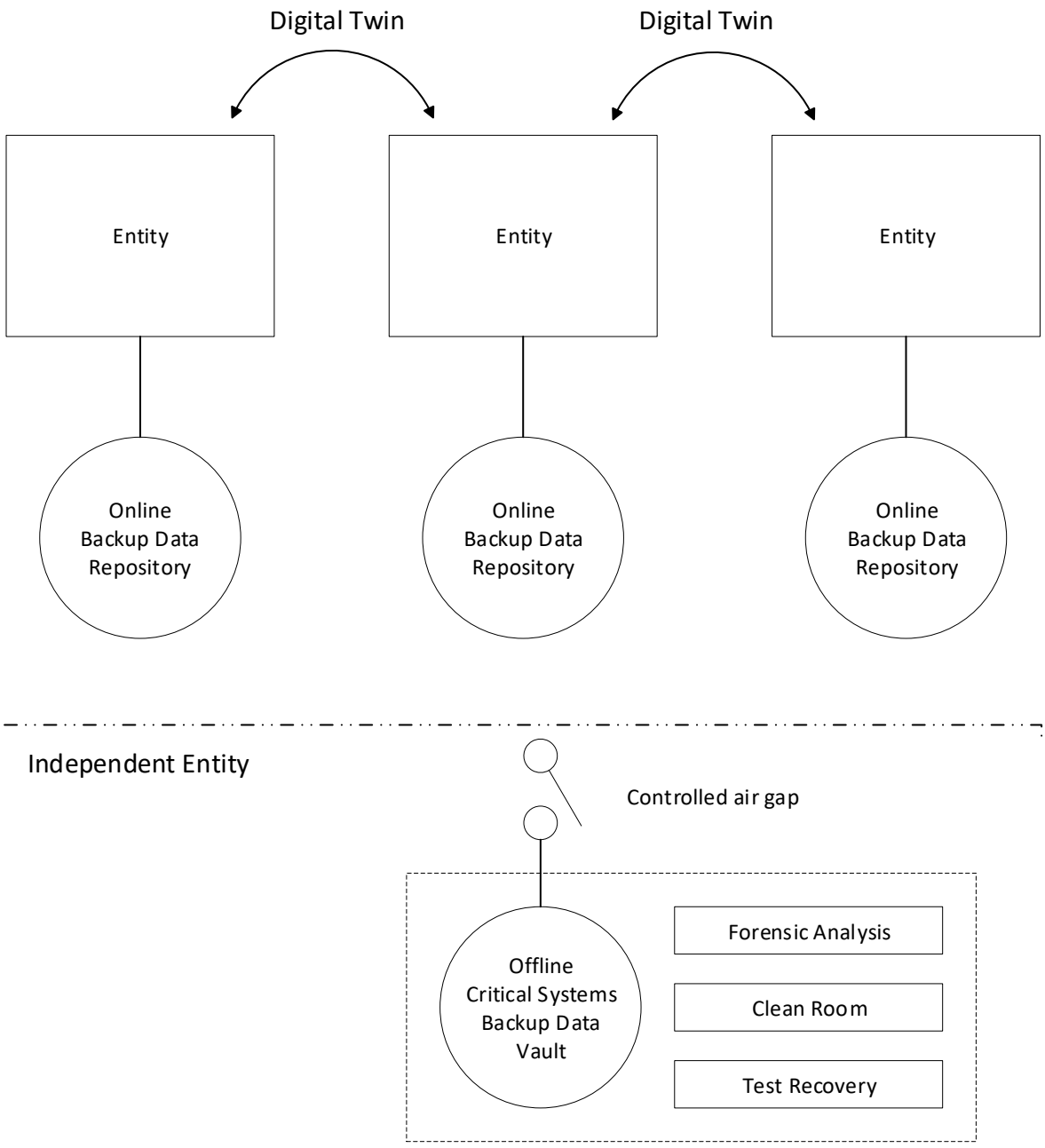
The final recommendation concerns the regulatory framework. The paper calls for a legislative framework that establishes an appropriate regulator for each sector, to work with the entities to co-design specific requirements and guidance to safeguard Australia's critical infrastructure. The regulatory model proposes a risk-based approach in developing and enforcing an entities security obligation through reporting, inspection and gradual enforcement powers. The paper also calls for enhanced Cyber Security obligations where there is a need to build an active partnership with the most important entities, to share near-real time information, to better understand and address threats.

Dell considers this approach passive enforcement. It relies on reporting, compliance and penalties to ensure entities comply with guidelines. We believe this approach may not be sufficient to protect Australia's critical infrastructure from the cyber threat landscape. The adversaries are growing in sophistication and it is unclear whether passive enforcement would provide a timely response to a major cyber incident. Similarly, we believe it is impractical to assume all cyber events can be detected and prevented using security controls and a regulated framework. As the government evaluates each sector's security obligations, we recommend they are evaluated on the assumption; a) critical systems

infrastructure will be compromised; and regular backup systems and data repositories will be targeted by adversaries. Given the current cyber threat landscape and what is at stake, Dell recommends the government consider active enforcement measures. Active enforcement measures would allow the government to entities data recovery facilities, under the plausible worst-case scenario. The plausible worst-case scenario is activated when an entities controls have been compromised and data supporting critical systems is rendered unrecoverable. In this setting, the government would establish a central entity that is responsible for maintains all applicable entity's "copy of last resort". The copy of last restore would be provided by a central data vaulting system. In establishing and managing the central vault, the government will have established active enforcement measures to assure data is protected and recoverable under the plausible worst-case scenario. The systems supporting the central vault would adopt all the controls and methods outlined in this paper. In addition, Dell recommends digital twins are established between similar entities, that allows critical IT systems to be recovered to the digital twin, in the event an entities critical system is unavailable for data recovery.

In summary, the establishment of a central data vault would allow the Australian Government to ensure the data supporting critical infrastructure, is actively protected and recoverable using a copy of last resort. By establishing a copy of last restore, the Australian Government will be able to actively verify the recovery posture of Australia's critical infrastructure, at a moment's notice.

The following diagram illustrates how a central data vault managed by a government entity, can be used to provide forensically verifiable copies of data supporting critical systems infrastructure.



Authors

Peter Marelas
CTO Data Protection Solutions, APJ
[redacted]

Melissa Osborne
CTO for Australia/NZ
[redacted]