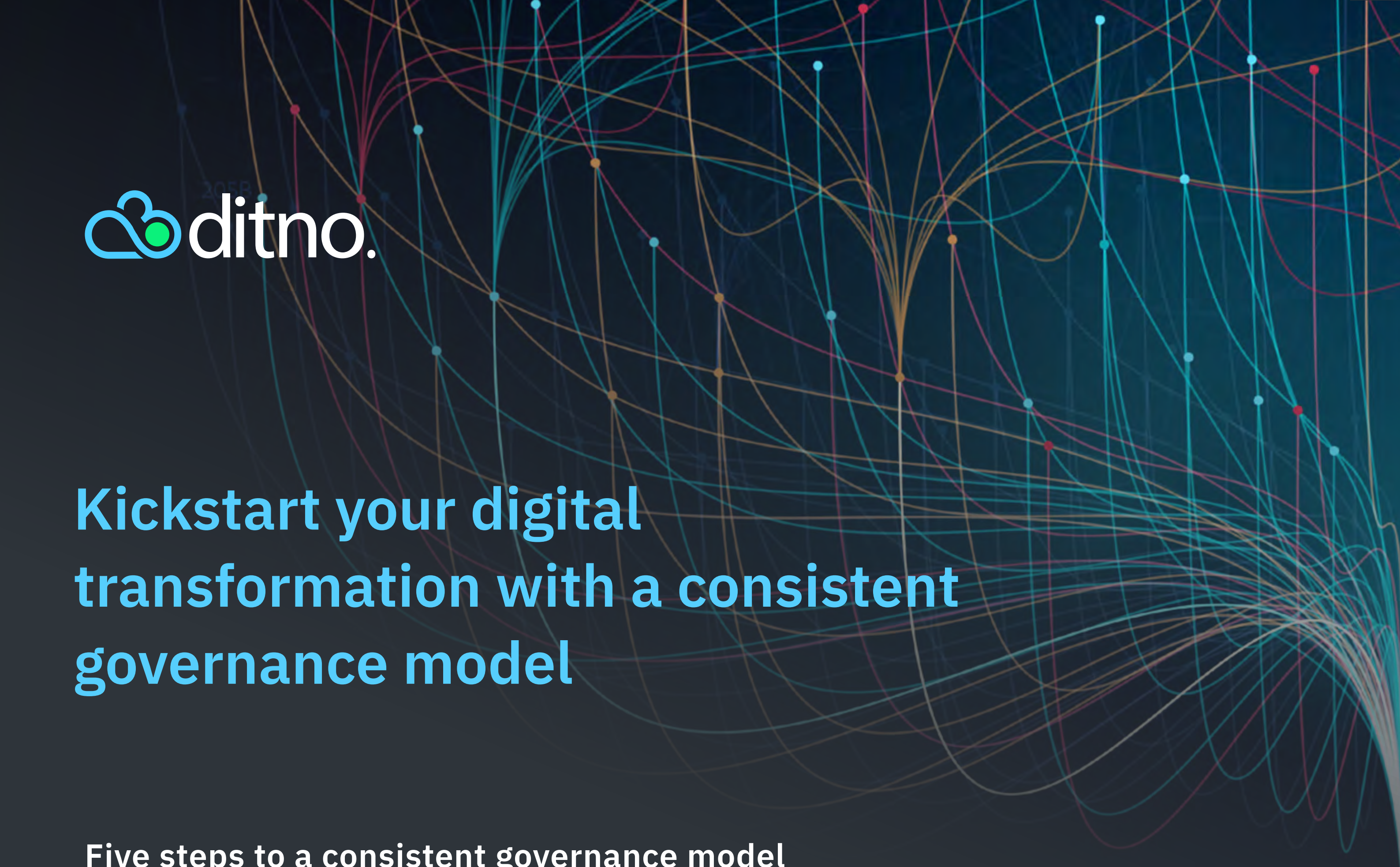

Kickstart your digital transformation with a consistent governance model

Five steps to a consistent governance model that will map to your transformation

Organisations are digitally transforming at an accelerated rate and in ways that many business leaders may never have envisaged before the events of the last 18 months. Unfortunately, the speed of transformation means that many organisations have overlooked the importance of security. If digital transformation is not underpinned by a robust cybersecurity model, then companies may not be able to fully maximise the potential benefits of their transformation and may be at risk of security breaches.

Just one cyber attack can bring a business to its knees in this era of increased online transactions and experiences. Australian Signals Directorate (ASD) Director-General Rachel Noble told a Senate committee that a single significant cyberattack against Australia could cost $30 billion and 160,000 or more jobs.[1] In just one high-profile attack recently, global meat processing company JBS Foods paid around $14 million to cybercriminals as part of a ransomware attack.[2]

Fortunately, there are measures businesses can take to reduce the risk of falling victim to these types of attacks. However, the effectiveness of any controls you implement will be dictated by your governance model.

The importance of a consistent governance model

A governance model refers to the sets of policies and procedures that are in place to dictate what can connect to the network, where the risk areas lie, and whether your network security solutions and controls align with those policies and procedures. Ensuring your cybersecurity controls align with your security policies is essential to make sure there are no gaps or non-compliant controls that could introduce risk.

A consistent network governance model is essential to ensure you can digitally transform with peace of mind, knowing that your network will remain secure even as it changes.

[1] - Parliamentary Joint Committee on Intelligence and Security - 11/06/2021 - Security Legislation Amendment (Critical Infrastructure Bill) 2020 and Security of Critical Infrastructure Act 2018

[2] - ABC RURAL, JBS Foods pays $14.2 million ransom to end cyber attack on its global operations

There are five steps to a consistent governance model that will map to your transformation:

1

Gain real-time visibility with network security software that provides a clear picture of the IT landscape

The IT landscape is becoming harder to protect as the perimeter edges continue to blur and endpoints continue to proliferate. Many point security solutions leave gaps and blind spots that cyberattackers can exploit.

It’s valuable to implement automated network security and network discovery tools that can shine a light on those dark corners, illuminating the environment so you can understand how to seal the gaps and limit the effectiveness of cyberattacks.

2

Enforce a zero trust approach

A zero trust network is one in which no user or device is trusted simply based on where or what it is; instead, continuous verification is required to prevent unauthorised access by previously trusted users. Zero trust leverages micro-segmentation, where virtual fences are built throughout the network, to prevent unauthorised users from accessing parts of the network they shouldn’t be in. This is particularly useful if trusted users’ identities or devices are compromised, which is an increasingly common risk in the modern, distributed network. It’s important to codify the zero trust approach into your governance model to ensure your controls continue to support zero trust.

3

Use machine learning to automate security controls to start building a zero trust network

Manually managing security controls leaves room for error, not to mention monopolising time and resources. Using machine learning, you can reduce the time and effort needed to discover and protect your most critical devices and IT services. Machine learning solutions can analyse the environment and suggest the most appropriate rules to protect your data. Using a machine learning approach to manage zero trust instead of a manual one can dramatically reduce costs and lower the risk of errors when building your cybersecurity posture.

4

Build a governance model that covers your on-premises and cloud-based networks, delivering continuous security and governance across all of your environments

As organisations digitally transform, they often find themselves straddling a hybrid environment comprised of on-premises and cloud-based networks. This can mean that security controls don't map to different environments; however, if you're not aware of this then you could proceed with your digital transformation in the mistaken belief that your data is protected when it's actually at risk.

Therefore, you should implement a governance model that covers your entire environment across on-premises and cloud to ensure that no gaps appear even as your digital transformation progresses and your environment evolves.

5

Maintain continuous improvement to ensure your environment remains compliant

As the threat landscape continues to evolve, and digital transformation projects continue to progress, the IT environment will undergo constant change. This means it's important not to become complacent but, instead, to maintain continuous improvement to ensure the environment remains compliant.

With the right network security policy management (NSPM) tool in place, compliance can be automated. The solution is configured according to the rules determined for the organisation's preferred security posture. It then reviews all security controls against those rules and determines if a change or addition is non-compliant. This gives you confidence that your security controls remain compliant and will protect your invaluable data even as you transform.

How ditno can help

Protecting your network both on-premises and in the cloud is essential to underpin your digital transformation. ditno offers powerful unified governance and network security policy management tools that can help organisations protect their systems and data as they transform.

To find out how ditno can help your business transform safely without compromising on speed and agility, contact the team today.

ditno.com
(02) 8011 4860
info@ditno.com

ditno.