A new approach to security and trust in government

Table of contents

Introduction

Governments across Australia and around the world are confronting new challenges of trust, security and confidence.

Their work is increasingly being transformed by a culture of connectedness fueled by new digital tools and platforms.

Governments must be more collaborative, mobile and responsive to citizens' needs. Responding to these challenges goes well beyond the important work of CIOs and CISOs in individual government departments.

It demands a sustained, consistent, whole-of-government strategic policy response that should engage the highest levels of agency and public sector leadership to determine the right mix of policy, design and architecture, investment and effective implementation.

Something interesting has happened to the network

Connectedness is the hallmark of a world in which success is increasingly a function of new combinations of information, assets and expertise that work across old divisions of structure, sector and geography.

And that means the network (the fabric of connections that links people, things and places, physical and virtual) has become the organisation.

What was previously an asset built inside the organisation and managed within a set of physical buildings and offices has, in effect, broken free. This is the shift that renowned historian, Niall Fergusson, has described, in a recent book, as a move in the constant battle between the "tower" (hierarchies) to the "square" (networks) or, earlier, what open software writer and theorist, Eric Raymond, proclaimed as the difference between the "cathedral" and the "bazaar".

The network is no longer confined inside the organisation. In a very real sense, an organisation's network has become the Internet, connecting people and ideas and things anywhere and everywhere, anytime and all the time.

Just like the work, people, devices and services it supports, which all need to be so much more mobile and flexible than they have ever been, the network has left the building. The two things – a more connected and collaborative way of working and the new architecture of networks – are completely interdependent, each feeding off and into the other.

And that brings new opportunities and new risks. And it demands a new response.

Nowhere is this more important than in government and across the public sector.

This paper explains what has happened to the network, why security and safety are now major strategic challenges for senior leadership and how organisations need to respond with solutions that are simple, flexible and robust in their design, procurement and management.

But the story starts not with the network or actually with technology at all, but with government itself.

The story of network security in government is changing because the story of government is changing. In fact, the two things are interdependent.

As the work of government, in fact all “public work” whoever is involved, becomes more open, collaborative and connected, the network tools and platforms on which that work relies become more critical.

Their security and reliability are now a major strategic issue for agency and whole-of-government leadership as new demands for digitally transformed policy, service and regulatory performance drive the search for reliable and robust network security.

But the challenge is that, in a world of cloud-enabled mobility, speed and flexibility, the network has “left the building”. A new response is required.

The story of government

There’s a big shift redefining the work of government and the public sector, which reflects a deeper evolution in the role and purpose of government itself in a more open and connected world.

Three attributes

Three attributes are increasingly coming to define the character of modern, effective government in Australia and around the world. These attributes, in turn, are being driven by trends whose combined effect is to reframe how government works and the tools and platforms on which it will increasingly rely.

The changing nature of public work: collaboration and co-creation

Coming up with solutions to the big challenges we face as communities and as a nation – growth and inclusion, jobs and investment, sustainability and responding effectively to climate change, new models of affordable and effective health and social care, more livable and innovative cities and regions – is no longer the job of government alone.

It’s arguable whether it ever was, but the truth now is that ideas like co-creation and collaboration are the hallmarks of the way we approach these big pieces of public work, that affect us all and shape the lives we live in common. Ideas and solutions come not from government alone, or from any single sector for that matter, but from more complex combinations of ideas, expertise and resources from across many different sectors.

That means there is a new premium on the ability to share information and expertise safely, quickly and reliably across new networks of communication and influence. In fact, we would argue that the more connected and collaborative public work becomes, including the work specifically of the public sector itself, the more important the underlying quality and security of the network becomes.

If people need to connect and collaborate more frequently, the networks on which they rely must be commensurately safe and secure. The network becomes an important source of trust and confidence that will determine the quality and impact of the work of public agencies and their partners.

Rescuing trust and legitimacy

We're becoming familiar with discussions about the alarming rate at which trust appears to be leaking from many of our institutions of government and the way we tackle some of our big public challenges.

Much of the work of the public sector, and of the "public purpose" sector more broadly if you include the contributions of companies, NGOs and entrepreneurs, has to have at least half an eye to rescuing a sense of trust and confidence in the work and integrity of government itself.

Into the foreseeable future, governments will have to address two separate but linked levels of capability and competence in all their work. One will be the extent to which problems are solved and policy solutions and service delivery outcomes make a positive difference in people's lives.

But even as governments and others combine in new forms of co-production to come up with new ways to create public value, their work has to contribute to restoring trust and legitimacy. Making sure information is shared safely and that issues of security and privacy are properly handled is of premium importance.

In fact, they become direct investments in a steady improvement in trust between people, communities and governments.

A new performance trifecta: safe, reliable, responsive

It's already true, and will become even more pronounced into the future, that the work of governments will increasingly be judged against a trifecta of concerns that reflect people's expectation of good government, done well.

One is safety. There will be diminishing margins of error for practices and behaviours in government, or across the more complex value chains of different actors who design and deliver policy and services, that might in any way compromise the safety and integrity of information, people and assets. The safety and security dimension of the work of governments and their partners has become a central test of competence. And competence is the wellspring of trust which then feeds gradually into rising levels of legitimacy for the work and interventions of government.

A second dimension is reliability which cuts two ways. One way is the reliability and predictability with which government translates creative new thinking and policy solutions into effective programs and services that improve people's lives.

The other way reliability matters is in the underlying systems and processes that governments and others rely on to get their work done.

Privacy breaches, compromises to the integrity of data platforms and systems, and not keeping people and information safe and secure as they become increasingly mobile and institutionally untethered, are all now major risks to good government.

Failure in any of these dimensions will be swiftly punished by a loss of confidence in government itself as well as poorer outcomes for people who will withdraw their trust.

It becomes a vicious downward spiral. Breaches in the cycle of reliability and capability to get work done well feeds further decline in trust which, in turn, will make people more suspicious than ever of government's competence.

And the third dimension of performance for the future of government and public work is responsiveness.

As they now do in other parts of their lives – travel, banking, shopping, entertainment, communications – people expect government to become more responsive to their shifting needs, priorities and expectations.

Together, these attributes are creating a new set of conditions for the work of government, and the contribution of the public sector. In particular, they are making big demands on reliable and safe connectedness which in turn is becoming a strategic policy and performance challenge in individual agencies and across government as a whole.

The changing work of government: four trends

Underneath the emerging attributes of modern government are four trends we think are having a particularly significant impact on government work and the way government works.

The digital transformation of government

At least rhetorically, if not always consistently in terms of investment, implementation and impact, governments across Australia are committed to some variation on the theme of digital transformation.

What that means is a commitment to the gradual replacement of the "analogue" platforms, processes and practices of government with digital capabilities that improve quality, engagement and productivity.

That ambition embraces everything from new web and digital capabilities, investment in new infrastructure, development of new skills and capabilities and, less obviously but very importantly, nurturing new leadership and operational skills, culture and capabilities across the public sector.

https://www.digital.nsw.gov.au/

https://www.dta.gov.au/

https://www.arnnet.com.au/article/634602/former-dta-chief-calls-govt-it-procurement-overhaul/

A common thread of the digital transformation ambition is what amounts to a major de-centering of the work of government, a growing recognition that the people, information and other resources needed to tackle policy and service delivery challenges are diverse and dispersed.

New connections are being nurtured between the "centre" of public service organisations and the public sector itself and their "edges" where experimentation and innovation tend to thrive.

The changing work of the public sector

A recent report into a major program of systemic reform in the finance and banking systems makes the point that "safety enables collaboration...without it, people hold back from participating they fail to take risks, admit mistakes or connect wholeheartedly with others".

Agency success will rely on a growing capability for staff to collaborate across the agency and often with people and experts outside the agency. That will require good systems and practices that keep data safe and provide an appropriate level of assurance for staff that a more open and collaborative culture doesn't mean any compromise in security standards. Quite the opposite.

The more frequently and extensively staff need to collaborate, the more they need to know the systems and processes that will keep data and other shared resources are reliable, safe and secure.

As people and organisations take their work out of the enterprise and into the cloud and the Internet itself, security strategy and safety functions must move with it.

Policy and service reform: data, design and delivery

A closely related and rapidly growing theme for many governments now is the dramatic rise of "big data" capabilities. This includes initiatives to aggregate, publish and use data for problem solving, innovation and improved policy development and service performance.

The NSW Data Analytics Centre (DAC) is a good example, which is being replicated in many other jurisdictions. The federal government's intent to bring forth a new data ownership regime, together with a more widespread and common identity method that, together, will empower users and citizens, is another important push into this space.

https://www.pmc.gov.au/public-data/data-integration-partnership-australia

Data has become a new and growing obsession for governments, recognising the potential for better policy and services from a more intense exploitation of the very significant stocks and flows of data which characterise much of the work of government.

Governments are now combining their interest in using data more creatively and purposefully for policy and delivery innovation with new techniques of design thinking that improves citizen experience and engagement.

Public value: trust and competence

Somewhere close to the heart of the agenda for better government is the need to improve levels of trust between government and citizens.

In a period of significant disruption in the relationship between government and citizens (think Trump and Brexit), governments are increasingly animated by the need to rebuild stocks of trust and legitimacy which have become dangerously eroded.

It is not too fanciful to argue that pretty much every aspect of public sector reform, including the push for "real" digital transformation, is being driven by the need to do something significant, and urgent, to turn around dramatically declining levels of trust in government.

Safe and reliable: a new approach

In common with many governments, the NSW Government faces significant challenges to secure the new contours of the network in a more crowded and complex cyberspace.

A recent report from the NSW Auditor General suggested that agencies are struggling in many dimensions of the new security environment.

The report found examples of "poor detection and response practices and procedures" and noted the lack of a "whole-of-government capability to detect and respond effectively to cyber security incidents." The significance of the security challenges was reinforced as the report noted the different domains in which they now play out – personal data, critical infrastructure, financial information and intellectual property."

The Auditor's recommendation was that the public sector needed to "significantly and quickly" improve its security performance.

https://www.audit.nsw.gov.au/publications/latest-reports/detecting-and-responding-to-cyber-security-incidents

https://www.itnews.com.au/news/nsw-govt-gets-an-f-for-cyber-security-486189

One commentary has drawn the conclusion that there is a relationship between the rate and intensity of digital transformation and the effectiveness and maturity of cybersecurity capability and performance. The review of the NSW Audit report also suggests that it isn't necessarily more spending that matters so much as how that investment in made. Investments in cybersecurity capacity have to reflect the shifting nature of the network itself.

The audit's findings suggest that although NSW is preparing for a secure digital environment at a whole-of-government level – with a Government Chief Information Security Officer (GCISO) appointed in 2017 and cyber security embedded as a priority area in the latest digital strategy. Efforts so far have not advanced beyond this initial strategic stage, with most individual agencies continuing to determine what is appropriate which invariably leads to inadequate, sometimes reactionary and often improvised approaches to cyber security.

For all digital leaders, latently implemented cyber security enablers and controls have the potential to stall or derail ongoing digital transformation efforts. This is because any weak security capabilities belonging to an individual agency makes cross-government information sharing risky, as connectivity between agency back offices hinges on the security of the entire ecosystem.

https://www.intermedium.com.au/article/does-rapid-digital-transformation-jeopardise-security

As the work of government becomes more connected and collaborative, it is making new demands on the safety and reliability of the networks that support its ambitions for trust and collaboration at the heart of better policy and improving services.

As the changing nature of the network becomes more central to the ability of agencies to deliver on their policy and service improvement ambitions, the security of the network becomes an increasingly important strategic challenge.

And responding to that challenge means understanding a little of the changing nature of security in new network configurations that have slipped many of the traditional and reassuring organisational boundaries within which “secure and reliable” used to be understood.

A quick tour of IT security: what you need to know (and no more)

It isn’t necessary for agency heads and the policy and service delivery leadership across government to understand the technical details of IT security.

But understanding the changing nature of security in a technology environment in which organisational performance is increasingly hostage to the wider world of the Internet and “anywhere, all the time” connectedness is now an inescapable leadership requirement.

The evolution of IT security

While the network was in the building – basically inside the limits of the organisation or enterprise – security was a relatively simple and straightforward business. A bit like keeping the building itself safe, the network could be configured and policed inside well established and clearly defined boundaries.

As mobility became the hallmark of the world of work, people needed the capacity to connect to their work and each other with ease, speed and security wherever they were and whenever they needed.

Security and safety became more complex. Not only did the business of keeping the “home” network safe become more difficult, as people demanded a capacity to “bring your own device” and connect on a rapidly proliferating array of devices and public and private networks. But increasingly the concept of the network was being stretched to follow the changing patterns of work and connection that new digital tools and platforms allowed and demanded.

And then the cloud arrived and, in effect, blurred the distinction between the core network and the other networks on which people needed to connect to the point where it became irrelevant. The new reality was that the network was wherever people needed to connect. Its contours stretched and moulded to the way people wanted and needed to work.

> “Information security is a complex system, made up of hardware, software, and wetware. Hardware primarily includes the computer systems that we use to support our environments. Software includes all of the code, databases, and applications that we use to secure the data. Wetware includes policy, procedure, training, and other aspects that rely on people. Information Security is part science, part art, and to some I am sure it seems like part mysticism. But it is not new.”

https://www.securityweek.com/evolution-information-security

And security had to respond, following these shifting patterns with new models of security and network integrity that felt less like defending a "fortress" and more like embedding security deep inside the network itself. As the network changed shape to keep pace with people's desire for robust connectedness, security needed adapt its shape and capabilities accordingly.

The Internet is the new network

Now we've reached the point at which the network is the Internet and the Internet is the network. Distinctions that made sense a few years ago when enterprises ran networks for work and everything else happened "outside" the network on the public Internet seem less and less relevant.

Now that so much of what we do digitally across virtually every dimension of lives – work, entertainment, shopping, politics and government – lives in and on the cloud, the architecture of connectedness has changed dramatically. Security and safety, the indispensable enabling conditions for confident and secure communication and collaboration, now have to be stitched tightly into the fabric of the way we connect. Security is no longer a function of which network you are on. It is a function of each and every moment of connection wherever and whenever it happens. The network happens when you want to connect.

Implications for procurement

These big evolutions of architecture and functionality in the network bring new challenges for designing and then procuring the requisite suite of cyber security capabilities that have become so central to the confidence with which enterprises – public, private, civic – and individuals can learn and work and play in the cloud.

Part of the challenge is that traditional procurement practices, which tend to focus on individual agencies and individual problems or solutions, are increasingly out of step with the nature of the contemporary security solutions that government needs.

More broadly, it's increasingly clear that the challenge goes well beyond any specific domain in technology and relates more generally to the way government procures technology solutions. The NSW Government's recent announcement of a new "marketplace" initiative for ICT procurement is promising. In particular, the new platform will take the friction out of connecting buyers and sellers by putting the problems to market and tapping into the innovation in the supply chain rather than approaching the market with prescribed requirements.

https://www.intermedium.com.au/article/nsw-tries-fresh-approach-procurement

There is more of a role in this domain than in others for a whole-of-government approach which sits above discrete solutions for different agencies or areas of policy. It is also increasingly true that the burst of invention that has witnessed so many new applications and services, hosted in and accelerated by the cloud, makes it easier to source globally trusted and tested solutions quickly, easily and cheaply.

The more dispersed the network of agencies and users (a defining characteristic of government networks for sure) the more important it is to have the capacity for a 'global', single view of information flows and their associated security risks. As the recent NSW Auditor General's report has shown (and it is far from the only recent example here and around the world), failure by government as a total enterprise to see, and act on, cybersecurity and information management threats leaves the work of government, and the performance of individual agencies, at risk of major failures or worse.

Cybersecurity should increasingly be made easily accessible and understandable through whole-of-government dashboards that "see" the cybersecurity performance of the entire system at any given time and, rather more importantly, what the response has been.

That capability doesn't exist today because the information comes from too many different sources; it simply can't be done by the current systems, with their multitude of management interfaces sitting in many different locations and agencies.

The good news, though, is that there is no need to discard all of those systems. Instead, the response should be to augment current solutions (which may mean replacing some parts of them) with a platform and associated tools that can provide a global view.

We have evolved from a time when people sat in an office and a security perimeter was established to protect the computer network - and those on it - from the outside world. Hardware gateways are not able to "stand guard" over all of the people who have access to government information, all of the time.

Today, the only way to provide comprehensive protection for users, no matter where they connect, is by moving security and access controls to the cloud.

This is a central challenge to which Zscaler provides an answer: why is security still so often sitting inside a building when the workers and information it protects are no longer there?

Zscaler™ – The global security cloud

Built 100% in the cloud, the Zscaler global platform delivers the entire gateway security stack as a service. By securely connecting users to their applications, regardless of device, location, or network, Zscaler is transforming enterprise security.

Zscaler security controls are built into a unified platform, so they communicate with each other to give you a cohesive picture of all the traffic that's moving across your network. Through a single interface, you can gain insight into every request — by user, location, and device around the world — in seconds.

The Zscaler security cloud protects all users, in the office or in the field, anywhere in the world. The Zscaler security cloud is always current with the latest security updates to keep you protected from rapidly evolving malware. With tens of thousands of new phishing sites arriving every day, appliances can't keep up. And Zscaler minimises costs and eliminates the complexity of patching, updating, and maintaining hardware and software.

Why the cloud offers better protection than appliances

Protecting users with consistent and enforceable policies requires much more than simple URL or web filtering. That's why thousands of organisations have already moved their IT security from appliances to security controls in the cloud. Here are some of the differences between appliance-based security and a cloud-delivered approach.

UBIQUITOUS | The cloud is always reachable from anywhere, any time, from any device.

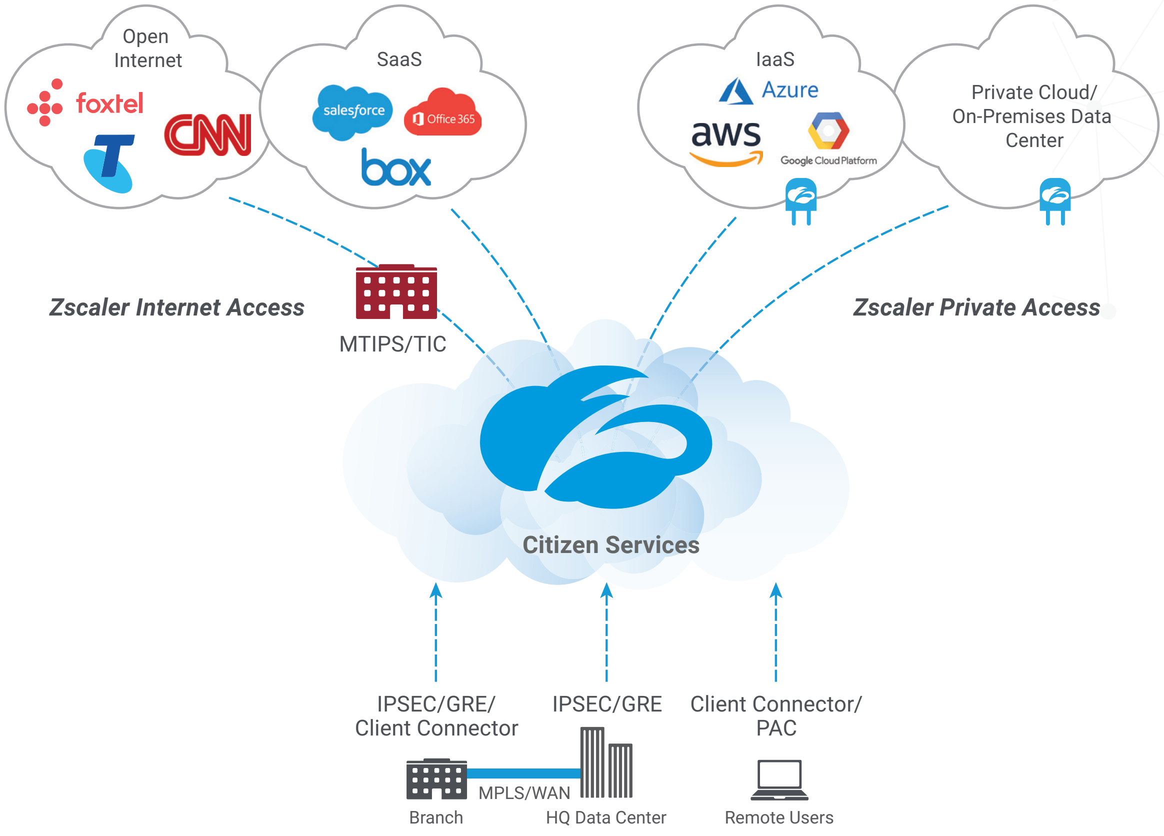
SCALABLE | You can add new features and thousands of users without breaking a sweat.

VISIBILE | All services talk to each other so you get full visibility of security for all users, everywhere.

COMPREHENSIVE | The cloud scans every byte coming and going, including SSL and CDN traffic.

INTELLIGENT | The cloud learns from every user and connection; any new threat is blocked for all.

Zscaler delivers the full security stack as a service



Secure, direct-to-cloud approach

ZSCALER INTERNET ACCESS™

The Outbound Gateway: fast, secure access to the open Internet and SaaS applications

- No hardware or software to purchase and manage
- Full inline content inspection
- Real-time threat correlation
- Cloud intelligence
- Uniform policies
- 60+ threat-sharing partnerships

ZSCALER PRIVATE ACCESS™

The Inbound Gateway: secure access to private, internal applications

- No more legacy VPN; the Internet becomes a secure network
- Users are never on your network; traffic moves through an encrypted tunnel
- Your apps are invisible, never exposed to the Internet
- Fast, secure access to internal apps on the cloud
- Simplified access and improved control; users can only see the applications to which they've been granted access

Conclusion: three ways to respond

An inescapable part of leadership in a digitally transformed public sector is the need to assure high levels of safety and security for all aspects of an agency's work and operations.

Assuring appropriately high levels of cybersecurity and safety is an increasingly central part of the strategic responsibilities of public sector leadership.

1. Build stronger strategic leadership awareness and understanding of security and network capability

Information security and cybersecurity have rapidly moved from the technical edge of organisations to their strategic centre. These are now significant threats, and opportunities if they are done well, for the mission and mandate of enterprises in government, business and civil society, large and small.

Reliability of 'business as usual' operations and innovation for new capabilities are increasingly dependent on safe and secure connections in a world where the Internet has become the network. Speed and confidence have become the new hallmarks of success in a connected world, whether it is for transactions, production and delivery capability or provisioning complex webs of relationship and interaction across the organisation and around the world.

Security and network capability are now the stuff of strategic business leadership.

2. Whole of government policy, architecture and procurement

For government, the more connected and collaborative nature of public work demands an approach to security and information management that is integrated and comprehensive. That means cybersecurity policy and procurement need to be designed, provisioned and monitored on a whole of government basis.

Individual agencies retain their responsibilities for leadership and management of security within their own domains.

But increasingly the tools and platforms they access need to be common and shared across the public sector. Costs will be lower; visibility and legibility of network security and data integrity will be higher and quicker and responses to threats and intrusion swifter and more effective.

3. Connect globally available platforms and tools

Finally, solutions should be procured from globally available and tested platforms and tools that improve speed of deployment and management and connect individual users into a network that can rapidly share experiences and expertise in the search for constantly improving cybersecurity design and performance.

About Zscaler
Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organisations transform into cloud-enabled operations.

Zscaler, Inc.
Level 35, Tower One
100 Barangaroo Avenue, Sydney 2000
+61 2 9225 7864
www.zscaler.com