

.....  
*Digital trust*

---

# *Securing your future in the digital world*



*Why is the digital world  
more dangerous than the  
old world?*

---

# Opportunity and danger

Digital technology is changing customer behaviour and business models at an exponential rate and creating extraordinary and unforeseen opportunities for growth and development.

Barely a month goes by without front page reports of a major security breach somewhere in the world.

Unsurprisingly, boards and senior management are becoming increasingly concerned about their cyber, or digital, security. A recent PwC survey reveals that 75% of CEOs now regard it as a serious threat to their business.

We understand their apprehension.

Our research reveals that over 60% of customers would stop using a company's products or services if an attack resulted in a known breach.

Why? It's a matter of trust.

In the digital space, your customers rely on you to protect their information and privacy. If your systems fail you, they will feel that you have failed them.

---

*“Digital security is not just a technology issue – it should be at the heart of an organisation's business strategy. Trust is a critical component that will enable companies to succeed in the digital economy. This trust is hard to build and is easily eroded.”*

*Peter Malan | PwC Digital Trust Lead*

---

Looking at digital security through the lens of trust means you are considering the wider business context in which you operate.

You are acknowledging the needs of your customers, suppliers and other key stakeholders.

You are taking into account the opportunities as well as the risks.



## 61%

of customers would stop using a company's product if there was a breach in their computer security.

## Going beyond best practice

We believe that, due to the rapid pace of change and increasing interconnectivity, traditional security models are no longer fit for purpose. The new mantra of digital security is ‘constancy’.

To build and maintain trust, we advise that you constantly:

- monitor and adjust your risk profile
- prioritise and protect where your ‘crown jewels’ reside
- review the digital landscape for emerging threats
- monitor the key risks within your digital boundaries as well as those from outside
- understand the effect of the digital environment on the fabric of your business and on your strategic plans.

## Where should you focus your attention

Our research globally and locally has identified the following key areas that support the development of digital trust.

1. **Third party supplier security.** Your data no longer resides within your four walls. It spans your interconnected business ecosystem. It remains imperative to manage information security risk within the supply chain.
2. **Cloud assurance.** Cloud technologies can reduce operating costs and increase flexibility. To realise these benefits, there is the need to manage your changing risk profile.
3. **Identity and access management.** The ability to effectively manage access to technology assets underpins digital trust. This is a base capability for organisations from which to leverage and achieve their digital objectives.
4. **Privacy and data protection.** With ongoing changes to privacy regulations, there is a significant opportunity to turn this cornerstone of trust into a competitive advantage.
5. **Resilience.** At the heart of operating in the digital world is 24/7/365. You need to assess the impact of entering the digital world on your end-to-end processes to ensure that resilience is built in from the outset.
6. **Data governance.** Data is increasingly becoming more valuable to organisations. How you govern and protect data is imperative for growth.

## Our approach

We can help design a strategic response to digital risk by establishing your current capability and then targeting those areas that require investment. We explore six key areas:

<b>1</b> <b>Prioritise</b> you can't secure everything	<b>2</b> <b>Crisis</b> it's not if, but when. It's how you handle it	<b>3</b> <b>Technology</b> make sure the basics are sound
<b>4</b> <b>Risk</b> seize the advantage	<b>5</b> <b>People</b> people matter	<b>6</b> <b>Connections</b> their risk is your risk

## When is the time to act

There will be trigger moments in your business that should prompt action and where we can help:

- When initiating a strategic business planning cycle that needs to pre-empt problems as opposed to fixing issues later.
- When there are changes to legislation and regulation.
- When you experience change in the form of new leadership, new markets, new acquisitions, new suppliers or new technology.
- When you need to respond pro-actively to emerging trends or developments in your market.



## How do you benefit

A well-managed digital security program will gain the trust of your customers and clients and give you the confidence to realise the full potential of the digital environment for your business.

This confidence comes in several forms:

**Confidence to take risks.** Assessing how digital interaction will impact your past, present and future.

**Confidence in your people.** Fostering secure behaviour by designing processes and systems that bear human vulnerability in mind.

**Confidence in your technology.** Understanding and mitigating the risks associated with evolving technology platforms.

**Confidence in your connections.** Building an agile risk management framework that keeps pace with growing networks and interconnectivity.

**Confidence in a crisis.** Protecting your digital assets, detecting intruders and minimising exposure when compromised.

**Confidence in your priorities.** Recognising key, intangible assets and aligning them with your priorities.

## Assess your digital trust profile

There are some critical questions we ask our clients to answer:

*Have you identified your risk profile and ensured your controls are 'right-sized'?*

*Is your digital security program aligned to your business strategy?*

*Do you know where your most valuable data is physically held? i.e. the 'crown jewels'?*

*What controls enforce third parties to handle your data appropriately?*

*With increasing connectivity, how are you managing access to your systems?*

*How do you know that those people accessing core systems are truly who they say they are?*

*If you are holding customer data, how are you managing their security and privacy expectations?*

*Are you meeting fast-changing regulatory requirements?*

*In the likelihood of a breach, what is your incident response plan to secure the business and rebuild trust?*

## How can we help

We provide a market leading end-to-end technology, risk and security offering to help you navigate the risks and capitalise on the opportunities in the digital age – building and maintaining trust.

We bring:

- Access to the largest network of global expertise and insights from helping leading organisations.
- A multidisciplinary offering to address the multifaceted and complex nature of digital risk and security.
- Innovation in our thinking and our tools to help you manage risk in the rapidly changing digital landscape.

## Further reading

Visit [takecontrol.pwc.com.au](http://takecontrol.pwc.com.au) to read case studies that highlight issues and benefits in the area of Digital Trust.

Read how a major financial services organisation is at the forefront of making sure all their suppliers can be trusted with their digital assets.

Suppliers are emerging as a major area of cyber risks for large organisations.

Understand how a company learns that when moving to the cloud, digital trust needs to be high on the agenda from the beginning. Customers are increasingly demanding seamless access to online services across all their devices.

They also want to know their sensitive information is protected and secure.

## The new trust dynamic



*Opportunity*



*Trust*



*Growth*

## Contact

**Peter Malan**

[peter.malan@au.pwc.com](mailto:peter.malan@au.pwc.com)

03 8603 0642

Share this topic

