WHAT ARE YOU DOING TO DRIVE DATA SECURITY?

TELSTRA'S FIVE KNOWS OF CYBER SECURITY

An IDC InfoBrief | February 2017

IDC Analyze the Future

Co-authored by

Executive Summary

Information Is An Asset – Manage It Carefully

Digital transformation (DX) is sweeping the workplace as organisations realign themselves to take full advantage of the digital economy. At the heart of this transformation is the information that organisations create, capture, store and analyse in order to be more efficient, effective and competitive in a data-driven world.

However, organisations are often challenged to have a method to value data in order to understand what matters and how it should be protected — both on- and off-premises.

To that end, global technology provider Telstra developed a security methodology for its internal use and is now extending it to other enterprises seeking to protect their networks and data. Telstra's *five knows of cyber security* addresses the key data management and security issues facing enterprises today.

This IDC Infobrief takes a closer look at how business leaders can apply this framework, incorporate it into their risk management processes, better understand how to protect the valuable data across their organisation against the onslaught of cyber threats, and manage the risk that digital transformation amplifies.

Armed with this tool, critical advice and practical guidance from Telstra's own implementation, organisations can embark on their data security program with confidence that it will provide a higher level of risk management around their data assets.

Know The Value Of Your Data

You need to know what value it has, not just for your organisation and customers but also the value to those who may wish to steal or change it.

What is the value of your data?

Self-discovery questions include:

- Do you understand that data does not only have an internal value and that most data also has value on the black market?
- Are you aware that different data types have different value to the organisation and to threat actors?
- Have you considered the costly effects of data loss: financial penalties, negative publicity, brand damage, leakage of confidential information to competitors, loss of competitive advantage, and becoming vulnerable to cyber crime?

How do you establish the value?

Use these tips from the field as a starting point:

- Empower the business to better manage information security risk using Telstra's *five knows of cyber security* which defines the topic in terms that business users can understand and relate to.
- Identify a working group across the organisation to get the business to take greater ownership of the issue.
- Identify the value of the asset so as to define how well it needs protecting.
- Focus on the most critical first, and build from there.

NO ORGANISATION IS IMMUNE TO POTENTIAL DATA THEFT OR LOSS.

IDC
Analyze the Future

Know Who Has Access To Your Data

You need to know who has access both within your organisation and externally, like who has "super user" admin rights in your organisation and amongst your trusted partners and vendors.

Who has access to your data?

Self-discovery questions include:

- Who (or what, e.g., printers, cameras or other network devices) has access to what data?
- Have you considered who has access to your data when it is shared with service providers and stored in the cloud?
- Do you include service and cloud providers, contractors, fourth parties (your vendors' third parties) as well as operational technology in your security monitoring "watchlist"?

How do you know who you can trust?

Use these tips from the field as a starting point:

- Does your organisation review or revalidate access to data as staff move around the organisation (providing staff with access to sensitive data that is not required to do their jobs can significantly increase your risk exposure in the event of a breach)?
- Also consider those outside your organisation who may have access to your data — don't just look internally.
- Ensure key service providers who have access to your data have undergone your security evaluation.
- Continuously evaluate your data — the review process is not just a one-time effort.

YOUR ORGANISATION IS RESPONSIBLE FOR YOUR DATA, REGARDLESS OF WHO IS MANAGING IT.

IDC
Analyze the Future

Know Where Your Data Is

You need to know where your data is stored. Is it with a service provider?
Have they provided your data to other third parties? Is it onshore, off-shore or in a cloud?

Where is data stored?

Self-discovery questions include:

- As part of the holistic approach to combating cyber security, have you ensured that this process encompasses all data, regardless it is on- or off-premises?
- Is data located in places it should not be?
- Is your organisation equipped to know the difference between a hack and normal user behavior?
- Are you including cloud and offsite vaulting in the overall process, as well as breach notification?

How to know where your data is located?

Use these tips from the field as a starting point:

- Decide if certain data needs to remain onsite, and if so, why.
- Empower the security team to assess current and new shortlisted service providers, and to create a risk profile.
- Contract with providers to ensure the policies of your organisation are met by these partnerships. Begin with what you control, establish the baseline, and then share the expectation across your ecosystem.
- Focus on the data, and where it is actually located, and less on the systems and where you "believe" it to be located.
- Trust levels and security posture can change, so the review process is not just a one-time effort.

DATA CAN BE IN A VARIETY OF LOCATIONS, BOTH STATIC AND MOBILE, AND NOT ALWAYS WHERE YOU EXPECT IT TO BE.

Know Who Is Protecting Your Data

You need to know who is protecting your valuable data. What operational security processes are in place? Where are they? Can you contact them if you need to?

What is your data management process?

Self-discovery questions include:

- Does your own team understand and adhere to the designated process for data security and management?
- Do your suppliers, partners and contractors also comply?
- How do you evaluate to show they know the process?
- How do you audit them?
- Many hacks and breaches are as a result of an insider. What are you doing to monitor and measure this?

How to protect your data?

Use these tips from the field as a starting point:

- If sensitive data is being stored on "shadow IT" systems, who is protecting it? Would your organisation know if it was lost or stolen?
- Ensure your policy can be implemented across the many devices and systems where this data may be stored.
- Ensure your business ecosystem of suppliers and partners understand how you value data, and encourage them to adopt a similar stance.
- Be sure you know what data is being managed by third parties, and they understand your values and principles of data integrity.

STRONG DATA MANAGEMENT HAS INHERENT BUSINESS VALUE, TIE THIS PROCESS BACK TO THE BUSINESS STAKEHOLDERS.

Know How Well Your Data Is Protected

You need to know what your security professionals are doing to protect your data 24/7. Is your data being adequately protected by your employees, business partners and third party vendors who have access to it?

What is a strong risk management process?

Self-discovery questions include:

- Do you have a systematic security methodology (like Telstra's *five knows of cyber security*) to embed into your overall risk assessment process?
- Do you have the right people, processes and technology in place? There is no 100% solution — adopt a defence-in-depth approach to security.
- Is security inherent within your organisation or is it an afterthought?

TELSTRA'S FIVE KNOWS OF CYBER SECURITY DRIVES ACCOUNTABILITY BACK TO THE BUSINESS AS THE RISK OWNERS, ESTABLISHING CLEAR PRIORITIES FOR THE I.T. AND SECURITY TEAMS.

How do you achieve this?

Use these tips from the field as a starting point:

- Understand that this is about "business risk".
- Don't expect IT to be mind readers; it's your data, and you should value it accordingly.
- "People" play a large part in the process. Relying entirely on technology is over-simplifying the issue.
- Being aware of the risk is better than having no knowledge that a risk exists. Ask IT to go beyond the obvious for thorough risk assessment.
- Don't try to do it all at once, and know when you have achieved adequate coverage.
- Focus on the most important data first, then apply this knowledge across the organisation.

An IDC Opinion

Information transformation (Information DX) has emerged as one of 5 key pillars of digital transformation, and research shows that organisations that are better able to manage their information and mine the best insights are better equipped to compete in this new digital age.

Ensuring the security of this data comes down to having a proven process.

Telstra's ***five knows of cyber security*** fills a void in the market as guidance to business users on where to focus efforts around data security.

Business users who are able to implement this type of process are more likely to avoid breaches and financial loss due to data mismanagement in this age of the data-driven economy.

WHAT ARE YOU DOING TO DRIVE DATA SECURITY?

Find out more about **Telstra’s Five Knows of Cyber Security**

Register for a cyber security health check at www.telstra.com/cybersecurity