The Five Knows of Cyber Security – The Salesforce Edition

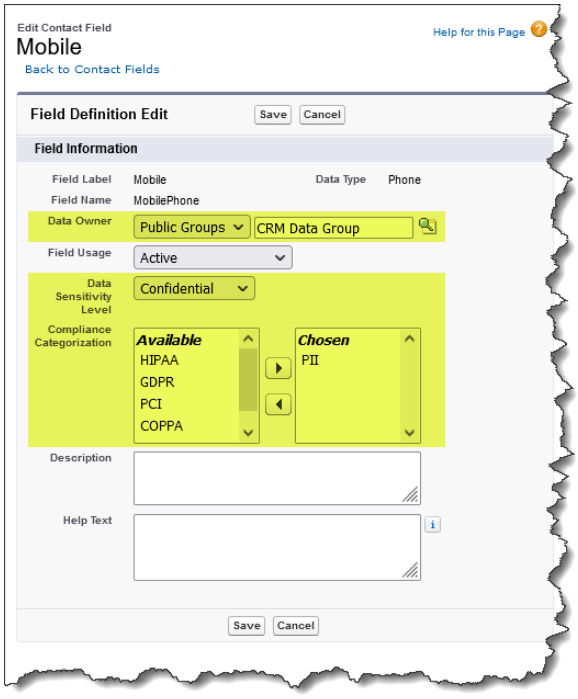
The 5 Knows of Cybersecurity were written in 2015 by Mike Burgess and Rachel Falk both from Telstra (now moved onto ASIO and the Cyber Security CRC respectively). This list of knows is the basis for all cyber security…

- Know the value of your data
- Know who has access to your data
- Know where your data is
- Know who is protecting your data
- Know how well your data is protected

These simple *knows* inspired this whitepaper and we will go through each of these from a Salesforce Core Services point of view and provide some insights…

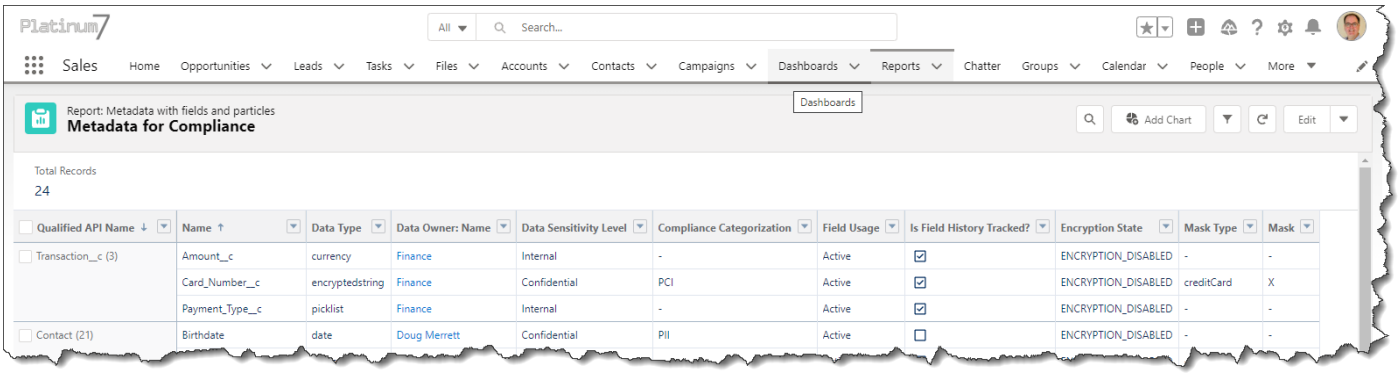
Know the value of your data

In this regard, most Salesforce customers are, in my opinion, not aware of the value of their data – either to them, their customers or to attackers… The first port of call here is to classify all the structured data (objects and fields) that is stored within Salesforce. This is pretty easy to do with Salesforce by using the inbuilt tools in the setup menu. The values for the *Data Owner* can be either a User or a Group. The *Data Sensitivity Level* and the *Compliance Categorisation* picklists are able to be customised to suit your requirements by going to the *Edit Compliance Categorization Picklist Values* on the *Data Classification Settings Setup* page.



Platinum7
PO Box 6143
Hawthorn West 3122
Australia
Phone: +61 404 005 435
Email: info@platinum7.com.au
Web: https://www.platinum7.com.au

After doing that, you can run a Compliance Metadata report to see all these details as well as encryption status (Standard or Platform Encryption) and History Tracking. The report is available via an unmanaged package I created and you can install it by clicking here for your Production org and here for a Sandbox.



Now comes the interesting part – how much data do you have in unstructured data? Where is it stored – Content, Files or Attachments? How do you audit them? This is a bit trickier as there is not an easy way to see all your unstructured data and will be the topic of a future whitepaper and blog.

Since you now have the data classified, the value of the data can be assessed. If you were hacked and this data was made public, what would be the ramifications? Are you liable to be penalised by regulators for a data breach? What about the news headlines?

Answering these questions can give the value to the company of your data — maybe not entirely in currency, it may also be intangible (reputation loss)...

EDIT: The following section was added 7th April 2023. It is here as I have been thinking about the value of data and how it diminishes over time.

Is the data you are holding providing value to your company? If it isn't, then why do you have it? An example of this could be that your company sells Widgets and you would like to keep track of the number of issues with each version of the Widget. So, you keep all the cases associated with a reference to the version of the Widget which allows you to do reports that say Widget X has an average of 201 issues per 1,000 sold and Widget Y has an average of 104 issues per 1,000 sold. Imagine now that you have been doing this for a while and have 10 years of data (Cases) stored in Salesforce. A lot of these customers have probably not had repeat contact with the company, however you still hold a lot of PII (personally identifiable information) on them: email, phone, address, etc. If you are not interacting with them, why do you have this data? Just do a summary of the data for the years 3 and older, keep that and delete those cases and any associated inactive contacts. This way you are minimising the data you are keeping and reducing your risk.

There have been three major breaches (Optus, Medibank and Latitude Finance) recently in Australia and two of these leaked PII data from customers who had not had any interactions with that organization for 10+ years. Why was the company holding onto that data?

For finance and telecommunications in Australia, there is a need to verify the customer and to do that you need to hand over a lot of PII: drivers licence, passport, credit card, council rates (tax), and bank statements for example. That is fine, however I believe that companies should archive this information from production systems very soon after approval/rejection and put it in a backup system that is highly protected and with minimal permitted access.

I believe it would be better if the government provided a service where the identity of a customer could be ascertained by the government service by asking for those ids and then send the company requesting the customer's identity an "transaction id" in the same way that credit card processing systems do to stop companies needing to hold payment card information. That way there would be a lot less sensitive PII being held by all these companies and therefore a lower risk to them of data breaches…

Know who has access to your data

Your employees have access to your Salesforce data to do their work, and if you have Experience Cloud (aka Communities) your partners and/or customers also have access. There is one special user in your Salesforce instance – the Guest User and this user is used by Salesforce for unauthenticated access to your instance. Unauthenticated access can be for public knowledgebases and the like. If this user is misconfigured, anyone on the net can access the data that this user has permission to see (or edit)… Salesforce has recently updated the default capabilities of this user, however you still need to check to see if your configuration is what you expect it should be.

You need to be very aware of "who can see what" when it comes to your users. There is an older, however still very relevant, Salesforce blog post about user access to data. There is a new (May 2023) set of recordings out from Salesforce on this. Your roles, profiles, permission sets and field level security settings control "who can see what" and you need to make sure these are set appropriately. Also, don't forget off-boarding employees who leave the company. The simple way is to freeze them first, then you can work out the changes of ownership for their data at your leisure.

A common misconception is that Salesforce Platform Encryption protects your data from your employees – it does not. All users in your org will always see data in plaintext via the UI or API if you are using Platform Encryption. The only people Platform Encryption protects your data from are a) hackers who have managed to get into the Oracle Database inside Salesforce's data centre [in my opinion, quite unlikely] and b) nefarious Salesforce Database Administrators [again, in my opinion, quite unlikely]. Even though the DBAs do have access to the Oracle Database underlying the Salesforce Application, they do not have access to your data in context – the Salesforce Data table contains bazillions™ of rows of data for all the customers who are sharing the same Salesforce instance as you (AP21 for example) and the data is not (easily) able to be reconstructed and connected back to you. For more information on this, please see one of my Dreamforce sessions on Multitenancy where I discuss the data structures (starts at 14m50s).

What about your development or consulting partners? Do you give them access to your Salesforce org and maybe sandboxes? Do you have production data in your sandbox? Sandboxes are a regularly forgotten

source of production data leakage. Salesforce has an add-on tool, Salesforce Data Mask, to assist in keeping this data safe.

Know where your data is

In the Telstra document, they are focussing on location of your data – that is not as important with Salesforce as all the Salesforce data centres have equivalent security levels. When you signed up to Salesforce, you were allocated a "region". Today, there are 7 regions: USA, UK, EMEA, APAC, Australia, Canada, and India, with more being announced all the time thanks to Salesforce's new deployment architecture – Hyperforce. When you are allocated a region, all your data will reside in that region – both production and failover. The APAC region is in Japan and anyone in APAC who does not specifically request an Australian or Indian instance will be hosted there.

In the Salesforce world, I would be more interested in understanding where your data is being stored outside Salesforce. What do I mean outside? Is it in your data warehouse? Where are the backups of your Salesforce data stored? Yes, Backups of your Salesforce data – you need to do this… Do you allow unfettered access to the API or are users able to export reports? All of these allow for your closely guarded data that was inside the very secure Salesforce data centre, managed with all your configured visibility settings to be left lying around with varying degrees of protection where the level of security is mostly trending towards zero. You may have access controls on your data warehouse, however these are usually quite broad and a data warehouse user more than likely has access to all your data…

How are you protecting your data when it is outside of Salesforce?

Again, another question, however the answer is very important to your data security. Spending time and effort to lock the front door is wasted if you leave the back door open.

Know who is protecting your data

This is an interesting one – who is protecting your data? Is it Salesforce? Is it your Security Operations Centre? Is it your Salesforce Administrators? Is it your Salesforce implementation partner? Is it no-one?

Yes, Salesforce protects your data when it is inside the Salesforce data centre, however there is a shared responsibility model when it comes to security. Salesforce provides features and capabilities to you for you to configure and maintain the security of your data – that is your part of the shared responsibility.

You need to have good policies and procedures in place to control your data security. All the things spoken about earlier are key – controlling data access in the org, securing data stored outside Salesforce, and understanding the value of the data. Not knowing who is protecting, or should be protecting, your data will most likely lead to preventable data loss.

In my opinion, the people who need to protect your data are your Salesforce Administrators as they should have all the skills needed to configure your Salesforce instance correctly, however they are not necessarily the best placed people to make the decisions on what these settings should be. This needs to come from the

company's security/compliance/risk team and if you don't have one, then you need the C-suite to step up and make these decisions as they are ultimately responsible and accountable for the company's data security.

If you have a relatively junior or uncertified Salesforce Administrator, you may require the assistance of a specialist. This is also true when it comes to configuring the Salesforce security add-on products: the Salesforce Shield suite of products – Platform Encryption, Event Monitoring and Field Audit Trail; Salesforce Data Mask; Salesforce Security Center and Salesforce Privacy Center.

Know how well your data is protected

Again, another interesting one – how well is your data protected?

From the Salesforce side, have you read the SOC2 report, ISO Statement of Applicability and the PCI Attestation of Compliance documentation? To read these documents need you to log into the Salesforce compliance portal with your production Salesforce login. If you do not have one, please reach out to your internal Salesforce Administrator as they can get these for you or you can speak with your Salesforce Sales representative who can request access for you.

From your side of the shared responsibility model, have you configured the multitude of Salesforce security settings appropriately? Have you created Salesforce Transaction Security policies to block data egress that is not compatible with your data protection policies? Are you storing the Event Monitoring logs so you can do forensic analysis on the usage in the, hopefully rare, occurance you need to do so?

That's a lot of questions, however the answers are generally found by studying the output of a thorough assessment of your current Salesforce environment – the org itself, the policies and procedures guiding the security of your data, compliance to those policies and procedures, the connected systems, your users, your partners, and your developers.

Platinum7 is able to provide an unbiased security assessment of your Salesforce org and the environment it runs within, and provide very granular and capable Transaction Security Policies, as well as Event Monitoring backup capabilities.

Please reach out to info@platinum7.com.au for more information or call +61 404 005 435.