Critical Third Party Applications: Risk and Handling

Flavio Gerbino
Defense Department, scip AG
flge@scip.ch
https://www.scip.ch

Marc Ruef (Editor)
Research Department, scip AG
maru@scip.ch
https://www.scip.ch

Keywords: Assessment, Detect, Fraud, Legal, Report, Request, Risk

1. Preface

This paper was written in 2013 as part of a research project at scip AG, Switzerland. It was initially published online at *https://www.scip.ch/en/?labs.20130117* and is available in English and German. Providing our clients with innovative research for the information technology of the future is an essential part of our company culture.

2. Introduction

Even though companies make considerable effort to deal with IT risks and their management there are security related topics that often get overlooked due to their nature. They appear to fly under the IT risk radar. One such topic is that of *critical third party applications* (C3PA).

From an internal point of view, a company focuses on the services its business is built around, their own infrastructure, networks and applications. During normal operations along those lines, companies access *C3PA*. Those are applications that are not proprietary to the company's IT resources. However, they're used to – among other things – handle financially and/or legally binding transactions. A prime example of a *C3PA* would be access to e-banking that is used to manage company accounts.

It is access to these *C3PA* that is done without much thought. Credentials are passed on among employees without second thought, informally and without any processes. This despite the fact that companies maintain a strict regime when it comes to the management of privileges as there are processes, controls, mechanisms et cetera in place that ensure the accountability and administration when account privileges are handed out.

Due to the fact that this application type is often overlooked, important adequate and recognized security principles that are usually respected by companies and enforced internally are not enforced in any kind of satisfactory way when it comes to *C3PA*.

Security mechanisms that tend to be overlooked include but are not limited to:

- The Principle of Least Privileges
- Need to Know Basis
- Segregation of Duties

Neglecting these crucial factors leads to a permanent high-risk situation and non-transparency regarding the use of *C3PA* in a company.

3. Question to Ask

When dealing with *C3PA* and their management, responsible parties need to ask themselves questions that help ensure a thorough process when implementing measures to manage *C3PA* and their security aspects.

- What is the company's definition of *critical third party application*?
- Which security risks are inherent in the *critical third party applications* in the company?
- Which risks are taken with *critical third party applications* during the company' normal operations?
- Which risks are taken when *critical third party applications* are ignored?
- What is the worst case scenario regarding *critical third party applications*?
- What established means and processes have been implemented already in order to ensure an adequately secure handling of *critical third party applications*?
- What possibilities are there for the analogue handling of functions normally performed by *critical third party applications* in order to minimise the latent risks?
- What risks regarding *critical third party applications* are purely fantasies, brought on by an exaggerated sense of precaution? Can they be ignored due to their complete lack of any relation to the business' operations?

4. Definition

Before any of these questions can be answered, *C3PA* need to be defined. This resulting definition needs to be limited to understanding.

Generally, *C3PA* are recognizable by the following functions

- They handle financially binding transactions. Prime example here is the e-banking access to a company account.
- Their function results in legally binding agreements
- They allow access to and editing of the company's reserves

In this context, the following type of application is considered to be a third party application:

- Application is hosted on a third party server
- A third party develops application

Even if an application is developed by a third party but hosted on an internal server, it is to be considered a third party application.

Following this definition *C3PA* have the power to generate financial contracts or collect data from external sources that is being processed in the financial context of the company. Critical third party applications are applications that can directly influence the financial success and the integrity of the company and impact its business.

5. Problem

The main problem in terms of these *C3PA* is the result of the way employees deal with them. Employees who are granted an account in a *C3PA* environment automatically receive high privileges of execution. If they misuse these privileges can lead to financial damage or a legal obligation that leads to financial damage.

The issuing of privileges can depend on external factors that can't be influenced by the company. For example: If a company has to rely on external parties to grant or deny access to an application and that process isn't bound to any kind of internal process the scenario that former employees retain their privileges even after their work contracts have expired. This enables them to initiate and perform critical transactions in the name of the company even after they are no longer part of the company.

Further, the uncoupling of company processes from privilege management leads to non-transparency regarding *C3PA*. Depending on the size of the company, it is close to impossible to accurately determine which and how many *C3PA* are deployed in what department of the company under whose authority and which processes and protection mechanisms may or may not have been implemented. This leads to risks.

6. Risks

The following risks describe scenarios that can come out of dealing with *C3PA*.

6.1. R1 – Slow and unnoticed but continuous drain of the company's money

Scenario: The attacker manages to gain money without the company noticing. In order to stay undetected and not to trigger any controls, he or she funnels money into his or her own account over a longer period of time. This flow of money is slow and continuous.

Comment: It is likely that established security, standards and controls in financial applications such as e-banking at least detect fraudulent transfer of money. Today's e-banking solutions and financial institutes are under constant pressure to protect themselves against even the most sophisticated threats. This is in their own interest. Gaps in security that have been discovered during previous attempts of fraud, regardless of their success, have been addressed. Among others, there have been confirmation mechanisms for transactions implemented. There are logs and reports that ensure non-repudiation and traceability.

6.2. R2 – Massive drain of company money or enormous financial obligation

Scenario: An attacker funnels a large sum of money into his or her own account or abuses his or her privileges to create a big, legally binding financial obligation for the company. This leads to lack of liquid funds and risks in terms of refinancing due to the fact that funds that are required short term are no longer available or can only be acquired at a high cost.

Comment: In order to conduct transactions and obligations in critical height, there are protection mechanisms in place so that business that exceeds a certain amount of money requires the approval or supervision of several people

6.3. R3 – Costly Long Term Obligations

Scenario: An attacker uses his or her privileges to enter into a long term legally binding agreement.

Comment: Employees in various areas of business have permission to place order or have access to license keys in order to acquire software and hardware, to perform upgrades or download programs. Often these permissions are not centrally handled by company procurement but, based on contracts, handled in a decentralised department and in autonomous areas.

6.4. R4 – Non-Transparency Regarding C3PA

Scenario: Due to non-transparency when handling privileges in *C3PA*, an incident such as the careless passing on of credentials leaves the integrity of the *C3PA* in regards to business operations vulnerable.

Comment: Incidents such as this one rarely get publicised, the most likely sequence upon an employee leaving the company is this: The employee leaves the company, his or her account remains active without consequence. There is no damage to the company. During the next routine check of accounts or when a successor to the employee starts working using the privileges, the old account gets noticed. This situation is dealt with and the account gets deleted. If an additional factor of authentication such as a token for e-banking has been given to the former employee has not returned it to the company.

There is no established and explicitly defined process, resulting in a conscious situation of neglect. However, this *laisser faire* attitude does not result in damage yet.

A worst-case scenario for each of the risks can look as follows:

Risk	Description	Affected Areas	Damage	Frequency
R1	Slow, continuous, unnoticed drain	CFO, Trading, Controlling, Pension fund, Treasury	High	50 years
R2	Massive drain of finances	CFO, Trading, Pension Fund, Treasury, Legal	**Catastrophic**	Irrelevant
R3	Costly long term obligations	Autonomous departments, Procurement, Legal	Low	20 years
R4	Non-Transparency leading to carelessness	All Areas	Irrelevant	10 years

Meanwhile it can be assumed that a manager in *C3PA* related areas will have established adequate processes to manage *C3PA* accounts. However, these might not be known or established throughout the entire company. This is because they are the most suited to recognise and mitigate risks in their own department. On the other hand, there is the distinct possibility of willingly or accidentally turning a blind eye on the obvious and occasionally turning a blind eye on the act of turning a blind eye.

Combining time and damage, the following matrix emerges:

	Damage			
Frequency	**Irrelevant**	**Low**	**High**	**Critical**
5 years	-	-	-	-
10 years	R4	-	-	-
20 years	-	R3	-	-
50 years	-	-	R1	-
Irrelevant (100 years)	-	-	-	-

7. Measures

It is time to have a look at possible, pragmatic measures and to classify them. These measures seek to lower or even eliminate the non-transparency regarding *C3PA* and to sustainably control the process of granting as well as removing access rights.

Measure	Description
M1	Accepting the status quo (do nothing)
M2	Declaring the principles when dealing with *C3PA* in corresponding policies
M3	*C3PA* self-declaration
M4	Addendum to employee file (HR Tools) specifying if employee has, based on their function, an account for a *C3PA*
M5	Addendum to employee termination process: Check if employee has access to *C3PA*
M6	Annual or periodical check of accounts with focus on *C3PA*: Request account list from operator of *C3PA* and check it for timeliness: Findings are being communicated and mitigated
M7	Random checks for *C3PA*, active pursuing of accounts
M8	Roll out reference model

8. Comments to Measures

- **M1 – Accepting the status quo (do nothing)**: Based on risk assessment and a damage history that shows very few actual cases of damage but a potentially relevant estimated number of potential damage, the argument could be made that the current status of non-transparency can be accepted without a problem without it resulting in a heightened risk of sustaining damage. Looking at the issue long term, it makes sense to at least address the issue of *C3PA*. If the decision to pursue measure M1 is made, it is to be seen as a postponing of the discussion rather than a final decision.
- **M2 – Declaring the principles when dealing with *C3PA* in corresponding policies**: It's typically easier to write rules than to implement them under normal operations conditions. Using measure M2, the goal is not an immediate lowering of the risk level but a signal that the problem with its risks is recognized in the company.
- **M3 – *C3PA* self-declaration**: Using the process of self-declaration, responsibility can be pinned on managers. All employees having access to a *C3PA* are to declare that fact to a position of management. Thus, upon an employee leaving the company or when random checks are executed, access to the *C3PA* can be removed. Short term, this seems like an efficient and pragmatic approach. Using an electronic form, users could declare their access themselves. This would most likely also raise awareness of the criticality of *C3PA*, because such a declaration would need to be widely communicated. However, there would be an estimated number of unreported accounts that could conceivably grant access to the most critical of *C3PA*.

- **M4 – Addendum to employee file (HR Tools) specifying if employee has, based on their function, an account for a *C3PA***: Access rights to *C3PA* are systematically catalogued in the base data of every employee. This results in an revision of every employee file, adding *C3PA* access where applicable. This seems like a systematic approach as well, but a small addendum to every employee's file might lead to considerable effort due to it being a change that reflects on the entire data structure of employee files, even if it's just the addition of one field.
- **M5 – Addendum to employee termination process: Check if employee has access to *C3PA***: Upon exit of an employee, he or she is asked if he or she has access to *C3PA*. In a less consistent form, this could take the form of random checks where some soon-to-be former employees are asked about *C3PA* and others aren't. Accounts will then be terminated, if they had one. This is a very pragmatic approach that – in combination with others – seems sensible.
- **M6 – Annual or periodical check of accounts with focus on *C3PA*: Request account list from operator of *C3PA* and check it for timeliness: Findings are being communicated and mitigated**: The operator of the *C3PA* is asked to send the company an account list on a periodical basis. This list is then cross-referenced with employee files and the accounts belonging to employees who have left the company are communicated and dealt with. This approach assumes that not only is the *C3PA* known but also its operator. Often, this is not the case, leading to an investigation into which *C3PA* are used and who they're operated by.
- **M7 – Random checks for *C3PA*, active pursuing of accounts**: One or several identified *C3PA* get investigated and findings are dealt with. This approach assumes that not only is the *C3PA* known but also its operator.
- **M8 – Roll out reference model**: Based on existing processes, a process for a characteristic *C3PA* is defined that is then applied to other *C3PA* as well. Based on this process, the owner has to apply the referential process to his or her *C3PA*. It's a distinct possibility that this application would be too extensive for many an application.

9. Effort and Benefit of Measures

The following table tries to show how the measures listed above are to be rated in terms of quality. The main goal is to give a brief overview focusing on practicability.

		Benefit		
Effort		Large	Medium	Small
	Small	M3, M5	M2, M7	M1
	Medium	-	M6, M8	-
	Large	M4	-	-

10. Summary

When looking at the situation of *C3PA* there are three measures that stick out that seem reasonable to pursue in order to have the best benefit with the least possible effort.

- M3 – *C3PA* self-declaration
- M5 – Addendum to employee termination process: Check if employee has access to *C3PA*
- M1 – Accepting the status quo (do nothing): Even though M1 isn't an option of action per se, it seems like a viable option regarding the likelihood of an incident. It would at least mean that the risk has been discussed and it has been decided to accept that risk as well as document it in the context of a transparent risk management.

Due to the fact that accurate information regarding *C3PA* isn't available without much effort, it's recommended to have departments using *C3PA* report their use and functionality. This could be part of the implementation of measures M3, M5.