

CISO - **Dave**

Account manager at The Salvage IT Support Company - **Tarquin**.

Dave: Hi, is that Tarquin? Listen mate, I think there's a problem.

Tarquin: What's up?

Dave: We've just failed our audit. Apparently there's an emerging threat as hackers have found a new way in by exposing our privileged identities. The auditor's pointed out that we're not controlling our privileged accounts. Can you take a look at this for me?

Tarquin: Right, leave it with me. I'll get back to you.

Tarquin hangs up and slightly adjusts his cravat. Turning to his colleague with a glint in his eye, he says, "We've got another one. That was Dave over at UK PLC. They've just failed their audit and he wants us to solve it. Looks like my bonus for thrashing my target's well and truly in the bag. I know this won't be covered by the contract because it never is and, while the negotiations are carrying on, we'll revert to an hourly rate. He's so short staffed he won't have time to do anything himself so he'll have to trust me."

Tarquin eventually stops laughing as he becomes totally absorbed watching his download of Money Never Sleeps for the eighth time that day.

Tarquin has Dave in a head-lock and both parties know it. Let's look at what Dave needs to ask, what Tarquin will say, and what Tarquin really means.

Dave: I've failed the audit – why?

Tarquin: Passing an audit isn't part of the contract.

Means: Here we go again! This is the call I've been waiting for - Operation Contract Negotiation in T minus 20 seconds.

Dave: Well, we have to fix this. What are we going to do?

Tarquin: We'll have to renegotiate the contract. Tell me what you want us to do.

Means: Get in!!!!

Dave: I want you to make sure we pass the next IT audit.

Tarquin: Any good auditor will tell you it's not about pass or fail, it's about the amount of risk you're exposed to. From that, you'll need to make an informed decision. So, what do you want to do?

Means: You haven't got a clue have you. You're talking about privileged identities, so you can't just leave things to chance because the risk is too great. You've got a hole that needs plugging and I'm just the man for the job – but I don't come cheap. The real question is, how much can I fleece you for?

Dave: I can't tell you how to mitigate this risk – isn't that your job?

Tarquin: We'll have to set up a temporary contract, at an hourly rate, to evaluate how to fix the problem.

Means: That means working out all the various permissions and how they're being used and with the size of UK PLC that's no small feat – if we're even able to do it. We're talking mega-bucks. It's about time the shareholders spread the wealth and sent a little my way.

Dave: Surely this is covered by the contract?

Tarquin: Unfortunately not. When we originally scoped everything out and agreed to take on the tools you were using, privileged identity management wasn't part of the scope of work. So, if you change our remit, or add new tools, then that changes our relationship and the contract.

Means: Of course it's not – only an idiot would make solving problems part of the contract. You really should have put more thought into SLAs. Instead, I was able to reel you in with an irresistible monthly fee. I knew the day would come that I'd be able to renegotiate and screw you for every penny.

Dave: Okay, the auditors have pinpointed our problem with privileged identities. Apparently we have no controls, so unauthorised people could gain access to sensitive company information. What can be done about that?

Tarquin: We can create some technology in-house. I can put a team together to start mapping all the necessary relationships.

Means: We can write ourselves a blank cheque.

Dave: Will that work?

Tarquin: Yes. As far as the auditor is concerned, he just needs to see that you are doing something about it.

Means: As far as the auditor goes, yes. As far as solving the problem goes, hell no. But it will be a while before you realise that, and by then I'll have bled you dry. You'll have invested so much money trying to solve the problem you won't be able to admit defeat. You'll roll over every time I say you need to put more bodies on it.

Dave: Don't you already have an accurate list of our privileged identities?

Tarquin: No – we've been following your processes and this isn't one of them.

Means: We did think that Sue was managing these but when she left, we discovered she hadn't been. You just can't get competent staff these days.

Dave: Isn't there existing technology to automate privileged identity management?

Tarquin: I'm pretty certain there isn't, but if you want to have a look feel free.

Means: Yes, but do I look stupid? Why would I automate manual tasks I can bill you for?

Dave: I don't have the resources to do product evaluations. Can you do that for me?

Tarquin: Yes.

Means: Of course not – why would I slit my own throat?

Dave: I've just been looking in this magazine and it talks about Lieberman Software who provides privileged identity management solutions – it sounds like this is exactly what we need. I'm going to give them a call.

Tarquin : Oh yeah, I've looked into that for you but I don't think it will work with your complicated infrastructure. Give them a call by all means...

Means: Damn, how did he find that out? Well, if I make it sound like it would be a mare to manage then hopefully he'll back off. He doesn't have the people or the resources to do much of anything in-house

because he's using all his budget keeping me in the good life to which I've become accustomed.

If Dave had just picked up the phone and given me a call I'd have been able to tell him that manually trying to manage his privileged accounts was just a money trap and wouldn't work. By automating the process, within a week his privileged identities could be under control and managed going forward – without a contract negotiation in sight.

There are many reasons why organisations, like Dave's, choose to outsource their IT security operations. The number one reason is to save money and reduce head count. There are some who do it to tap into specialised skills and services. However, equally as many are now discovering that the cost savings are quickly being eroded as the professional services aren't up to the challenge or come at a costly additional price.

Sometimes short-term cost cutting also cuts out the rich seams of experience and knowledge you have in your full time staff. Getting rid of them can sometimes cost you dearly in the long run and leave you at the mercy of an outside organisation which has as its main goal maximising its profits – the very reason you outsourced in the first place – to maximise your own profits! Welcome to the 21st Century's version of Catch 22. Milo Minderbinder would be proud.