Hello I'm Roger safety in today's Thursday, July 18 and you're listening to the information security news podcast brought to you by Northwestern University information technology payload of a summer cold so to try to make it through with no what serious coughing but FYI just in case Ray reminder is the summer patch Tuesday for Microsoft just happened there's been updates for Apple there's a new version chrome out there if you're running Oracle Oracle updates around basically anything you're running promenades and update so spend a little time to make sure you're grabbing the latest updates for all your favorite equipment keep it secure then there's a story here from Sands and the RSA talks about why helpdesk employees are of social engineering you know, target and we've talked about this before and why think is interesting about this particular story is not necessarily that helpdesk employees are our targets as a think that we all know that what think is interesting though is the way they talk about why and they suggest that perhaps it's because the performance is measured by the metrics that are new essentially how many calls do you answer how quickly did answer the calls and you know what your satisfaction is courteous or not and those kind of metrics make it you know kind of an incentive almost for the helpdesk employee to help you solve the problem even if the person trying to help solve the problem isn't necessarily the empty person this post we try and help you see one of you very careful about the stuff I will point out again the one thing you can do is make sure that your security questions and answers are strong and unique and one of the things within recommending is when it says for example you don't what was your first car don't put down Ford put down the grape fruit right you just have to know the answer to the question you don't have to answer actually answer the question that talk about some the golf them to cells essentially the sum to cells are small little repeaters network extenders basically for the cellular network so if you live in an apartment building and only build large the apartment building you might have you no notice that there was maybe a time when this perception for cell phones is bad part of the building and so the way to fix that his face instantly sold them to cells out there and these devices are available for all the different carrier sprinter AT&T whoever right and is estimated to be 50 million of them to are supposed to be in use by next year that's a lot another thing is you buy a device like this should put it on you network it you don't pay any attention to it typically practice nobody going around to see if this thing needs to be updated or anything like that you put in Islamists working its work in and unsellable that's fine right but the problem is if there's a security issue which there are security issues now whose could take care of this are people got well replaced these devices is is can you even upgrade him you know the answers probably no solicit problems can be around with this for a long time I think the problem with these things is there not secure in what they been able to demonstrate is people of been able to see that traffic going to the femto cell not necessarily does Travis: the cellular network traffic is going to defend itself and so the traffic or lessee of the text messages should know you please upload photos or captures all that I mean it it basically gives you a real good insight into what's going on on the cellular network now the sort one potential advantage to this is they got a pretty low range and also maybe it's Uno 50 feet minutes 100 feet think the quote that I saw was 40 feet to meet assumes little low but the guy think this problems compare around this for a long time and hope they do come up with a fix but even if they do you know it is just nobody paying attention these devices unless there some way to automatically push my out which doesn't sound like there is a big problem.
with us for long time I story that involves Kim Kardashian probably first time that we spoke about her on the podcast but the what the story is really about though is the hospital where Kim had her baby and what it turns out is some of the hospital employees were viewing Kim’s health records when she was in hospital notices this is a bad thing in hospital took action right there fired they fired some of these employees now for me this is good on two levels one you know something was done that was wrong in some action was taken was taken a relatively quick period of time upon that Padilla thing is the hospital is obviously logging these kinds of excesses and the hospital was paying attention to the logs think very often you even if you do log axis like this was paying attention the logs and so then months after the fact when another promised of is discovered they realize it’s been going out first bury long of a coated discovered a long time ago who just paid that the logs but nobody does so it's a real problem and he would say just because you have access to data doesn't mean that you should be looking at the data you should look at that data when you need to for your job not just because you can so if you're working in a hospital working in a Police Department any of these places you need to keep away from that data unless you need to see it back but nonetheless next-door here this is again about a hospital this is in the UK though they were fined 200,000 pounds that's about $300,000 because a hard drive that patient data was bought on eBay not normally be all for this except this particular case it seems like the hospital did nothing wrong and they gave their their equipment to a third party the third-party provided them with a certificate that said we’ve destroyed your hard drives and turns out that's not the case now if anything maybe the hospital excuse me is a fault because they didn't follow up they can actually physically see the hard drives being and destroyed but to me it seems like that's that's asking for too much in many cases I'm not sure this fine should be levied against hospital since it should been levied against the the company that was doing the work a while I'm none the UK animal goes on over there but it does seem to me like that if you take all the steps in a sign for service service provide you with certificate case that says were to do this and then they don't they're the ones who should be on the hook not you talk about RAM scrapers and these are point-of-sale RAM scrapers would talk about issues with point-of-sale terminals before these of those old devices should I swipe a credit card through when you're going to buy something at the store and occasionally these of turned out to be compromised and it looks like what really happens is because PCI requires that the data is encrypted in transit these RAM scrapers have been developed basically what they do is they look in memory they look for credit card numbers you know the stripe information things like that now what you do about this there's no way for you to actually tell if something's wrong writer menu lets face it you go to the store you run your credit card through machine how are you supposed to know that this is credit card terminals but compromised you can't buy do think it didn't require so was this means may be PCI needs to step up a little more and have requirements about what can be installed on there you know sanity checks to make sure maybe it's that you know of a checksum or something like that to make sure that things have been modified and low but something needs to be done to protect consumers here to store summary sent me this is called is this too much tea too much information Kim I excuse me again and basically what their story says is look if you're sharing something on the Internet it's forever and you really should ask yourself is this what really want everybody to know this with all probably seen stuff and maybe even posted stuff where
it's too much that stress can be around for a long time to really 110 years from now does somebody see you in that