All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Why does a 20 year old have access to TS/SCI and what do we do about it?

This is not the first time a young person has had authorized access to substantial amounts of top secret sensitive compartmented information (TS/SCI) and leaked it. How could this happen? It's easy to understand...

What do 20-year old people do in the military?

Among other things, they are in the field being shot at and shooting, driving armored vehicles, clearing buildings in hostile territory, jumping out of aircraft in the middle of the night, manning systems in nuclear submarines, and more. They also carry the bags of Generals, clean the printers in the data centers, dispose of the information placed in burn bags, and so forth.

Why do they need access?

They need access to relevant TS/SCI information because if they don't have it, they cannot do their jobs, killing others, not getting killed themselves, and generally doing the things they are supposed to do. If you are cleared to the appropriate level and your job requires access, you need access and you get access.

How do they get such a clearance?

Clearances are granted based on defined criteria, and those criteria do not include your age or how experienced you are. They are essentially a list of negative things that, if present, must be adjudicated, and if not present, provide no basis for denying you a clearance. The less you have done, the fewer people you know, the easier it is to get a clearance, because there are less things to check out about you. Older and more experienced makes it harder.

Why do they have need to know?

If you work in a data center, or if you are an aide to someone with a clearance and access, even if your job doesn't directly require that you have access, you have ancillary access, and this means you have to be cleared to do your job and this means, if you are cleared, you have need to know, and you have access. Sound backwards? Welcome to the security world.

What is this ancillary access and why do we need it?

If you carry the brief case of the person who has access, you are in possession of the classified material, and you cannot do that without the proper clearance. That because it is illegal to possess it without proper clearance and need to know. If you fix the printer that prints classified information, or maintain the computer that contains or processes classified information, you have access. That's because you could accidentally see the information, and thus you need a clearance and need to know or you break the law, and those who grant you access likely also break the law. We need this sort of access because that's how the law and the mechanisms we use operate.

How can they get it out of the classified areas?

They don't cavity search every person every time they leave a classified area. Nor can they reasonably do so. They must place trust in the people with access… they could memorize it.

What can we do about it (in many parts)?

I have many views in this regard, but they all come down to trust models and technological solutions. Technology solutions essentially use technology to prevent anything ever getting printed and reduce or eliminate the need for cleared people to do things with ancillary access.

- Removing ancillary access basically means the technology prevents such access and the content is only in devices that can adequately protect the content. No more paper classified briefings, no more printers in classified areas, etc. You carry a specially certified device that only operates in places where it is allowed, and so forth.
- Trust models are **NOT ZERO TRUST**! Did I mention we must trust people with access? I did. That's because they have access to do their jobs, and their jobs necessarily include actually knowing and using the classified information. You cannot know it and use it without knowing it and being able to use it. Unless we are cutting off all their tongues, they will be able to tell others, and even then there is writing and typing.

Why do we have to trust 20 year old people? Why not use more experienced people?

To do systems administration for a server in a data center, you need a modicum of knowledge and practice that can be gained by a 12 year old. By 16 you can be a talented master and get lots of certifications as well as bypass controls on most systems. It's not that hard.

In many large entities, employees are granted access to do such operations only after being in the company for 10-20 years and being part of a team of experienced IT folks who design, implement, operate, maintain, and manage IT systems and networks. They are typically 30+ years old and heavily embedded in the culture of the company, have group cohesion, know their fellow workers, and spend years together. That's because trust builds over time, is hard to gain, and is easily broken. Of course this is also changing... surprise... trust problems arise.

In government, they pay is low, retention is poor, and you can make twice as much after 5-10 years in by going elsewhere. You have to change jobs every few years, and that means that mundane tasks like operating computers are left to the least experienced folks who take on those jobs as soon as they are able to do so. Qualifications are "suitability" and clearance. If you are cleared and can pass the test you can get the job, if you are at the right pay grade for the work. By the time you are 10 years in, you will be out if you haven't moved beyond this.

Be careful what you ask for

Suppose we moved to a system that required 10 years of experience to gain TS/SCI access, requires actual bases for trust rather than a lack of reasons to distrust, limited access to only those with actual need to know, and got rid of ancillary access?

We have analog to this in the experience of a government department some years ago. They went beyond the simplicity of clearance and need to know to where people were making judgments. It was catastrophic in that they could no longer accomplish their mission and were doing psychological harm to their workers. So think carefully about how far you go overboard in this direction. Besides, are Generals really going to not have young aides and require colonels to carry their bags and take out the classified trash? I don't think so.

Conclusions

Now you know why and at a high level what we can do about it. I hope it helps...

