**The name is Smith. Richard Smith.**



When Richard Smith was fifteen years old, he hacked into his school’s computer network so he could download movies and games. Richard recalls that he had always been “captivated and mystified by the hacker” and admits that he was “a little bit devious and attracted to the idea of breaking rules”.

If subverting the IT controls in his school wasn’t devious enough, Richard naïvely downloaded a copy of a text called *The Anarchist’s Cookbook* through the school server. Perhaps it might have gone unnoticed by authorities in an earlier age, but this was shortly after the events of 9/11, and Richard remembers that the section titled *How to Blow up your School* “didn’t go down too well”.

The police were called, and Richard received some “very stern warnings”. As penance, he was put to work by his Principal in the school’s IT department. The intention was to embrace Richard’s obvious talent and put him in the right direction. And it might have done so, had the IT Manager not refused to let the astute schoolboy near the network. Instead, Richard spent a month cleaning dusty computer equipment and lamenting his punishment.

He studied the two available IT subjects at school, and built computers in his spare time, but for the most part found the classroom instruction and text books “quite dry and uninteresting”. So, when he was 17 and offered a job in the construction industry paying over $1000 a week, Richard didn’t hesitate. He remembers thinking: “I don’t need to go to university for three years; I can go straight to work and earn heaps of money.”

Though he now looks back at his choice “with some regret”, Richard also acknowledges that his career path may have been quite different had he made another decision as a teenager. Richard says that the IT industry today is a much different—and more exciting—landscape than it was ten years ago. Where he may have once been relegated to the IT Help Desk, Richard is now the very mystical thing he was so captivated by as a young, devious schoolboy. Richard Smith is now a hacker.

**Q&A**

**How did you get into the IT industry?**

I was a form worker doing carpentry work at Bond University. Due to the Global Financial Crisis, I was struggling with getting work and getting paid, not to mention the hard nature of the work. I remember observing the older tradesmen and how wrecked their war-torn bodies were; it was Summer, and we were all sweating our guts out. I was looking over the fence into the beautiful green Bond Uni campus at the nice shady pine trees, and I guess I was inspired. Prior to this, I had thought of pursuing a career as a dogman rigger working with cranes and using my brain a little bit more or possibly even something with computers. The economic downturn and instability with my job was the motivation I needed to make a change, so I enrolled in TAFE to pass the time until work picked back up. After completing my Certificate III, I was less inclined to get back to construction, so I completed a Diploma of Networking and then started a Bachelor of Information Technology. My thought process at the time was aiming to get into cyber security as I always had an interest in this area.

**What kind of work do you do?**

I am a Senior Consultant and Security Tester for KPMG. Penetration testing is a large part of my job and a very lucrative service our company provides. Usually this testing is a requirement of the end of year financial review. When conducting a penetration test, we will go to the organisation and test their security in terms of their IT environment—rather than their process of people—and look for vulnerabilities or “low hanging fruit”, as we call it. This exercise regularly has a time constraint in which we have to test their protocols, network, servers, and wi-fi, and look for weaknesses in order to break in and get domain administrator access. After the tests are complete, we write two reviews, one summarising the integrity of their security and risks aimed at either the board or audit committee, and the second for the IT manager of the team advising on fixes to made.

**Who do you interact with in your role?**

Internally within my company, we have Consultants; Senior Consultants; Managers executing a particular engagement; an Associate Director doing client relationships and making sure things are running smoothly; and a Partner at the firm who signs off and checks everything. We will typically have an Audit Committee or a Board of Executives that will engage us to do a particular piece of work, as most audit requests come from higher up the chain than the IT team. This being said, we spend a lot of time interacting with people less knowledgeable in IT such as the Chief Financial Officer, Chief Operating Office, Chief Information Officer, Chief Risk Officer and the Audit Committee, whose goal it is to protect the shareholders’ interests.

**Where do you spend most of your time?**

We have our office on Eagle Street in Brisbane City overlooking the river, which has an agile environment so you can sit wherever you want on the six different floors. We are encouraged to spend time with the client, however this isn’t always necessary as I can VPN to the Melbourne lab and test a client’s security from my loungeroom if I choose. The reason we use the Melbourne lab is so we can nominate an IP address that will be attempting intrusions, plus it has useful tools and processing power available. I work for a national team, so a lot of the engagements will be for example in say Gladstone, Melbourne, Sydney or even Lismore where I was last week, so this usually means getting on a plane and spending a week in a hotel.

**What part of your job do you find challenging?**

There are a couple of things I find challenging, one being when you have spent days trying to break into a network without succeeding, and you just have to try harder. There is actually a Certificate called the OSCP, which is a penetration testing exam where you are given 24 hours to hack into five different boxes and the motto is “*just try harder*”. That mentality relates to my job because you can’t just shrug and say you didn’t get in, because the client spends significant funds on hiring you, so you have to give them value for money. The other challenge I face is reporting, which involves mostly articulating the data you have obtained into a language the client can understand. Also, an obvious challenge is completing a thorough test and reporting on the engagement within the time allocated to the job.

**Has there been a moment in your career that you rate as most significant?**

The work I did in Sydney recently was an important moment in my career as an IT professional. My company’s relationship with the client had seen some damage and straight off the bat I experienced hostility with the client’s CIO. Until then, I had only assisted with client engagements, shadowing a senior colleague, and now I was left to make good of the bad situation. I was able to exploit numerous holes in their security, gain domain administrator, and demonstrate to the audit committee and the CIO the value of our company all on my own, which was a great feeling. I started with KPMG in the IT auditing division and it has been a slow transition for me working my way into the cyber security division and penetration testing. Not only the successful completion of this engagement but also the relationship management, has very much solidified my existence within this new position.

**How do you see the future of cybersecurity?**

This is an interesting question. Members of my team are a little bit concerned as the overall security presence is improving and Microsoft and its competitors are pushing things out that are making it easier to optimise security. Years ago, everyone would have their own third party security software but nowadays we are pretty much advising people to ditch that and just use int integrated OS security, so that’s good I suppose. We are actually testing system security mush less than we used to in exchange for testing the people and processes through what we call Red Team engagements; that being using methods like phishing, trying to get them to use a compromised USB or even physically break into a building. I hope it doesn’t go that way because I love this role, but at the same time the purpose of what we’re doing is to protect. It’s interesting that because of cryptocurrency and online trading, everyone wants to get into cybersecurity as well, but at the same time I think it will improve in leaps and bounds. For instance, we’re moving towards Azura Cloud, which is cloud-based servers instead of physical servers at a client’s premises, and the security is far more advanced than what is available in a localised server.

**Aside from what you do, what do you think the best role in IT is, all things considered?**

I’ve got a lot of friends who pursued the developer path; one is working for Telstra now and another for Suncorp, and they have great futures ahead based around their skills. If I had to put cybersecurity aside, I guess I wouldn’t go wrong getting into this side of things. I’ve found that you can really get a job anywhere if you specialise in software development. I’m actually really glad when I hear that kids are learning software development from quite a young age; they can be really creative and build something new and I do believe it is the second language of the future.

**What can the average user do to better protect themselves online and secure their information?**

It really depends what you are worried about. Disk encryption is a big one; Apple do it, Microsoft do it. Basically, this means that if your machine gets stolen, anything that is in it is safe—unless the thieves are extremely motivated, they won’t be able to access what is in there. You can go to the next level and add a PIN to your disk encryption, so when you first turn your computer on you put the PIN in, which hampers people because they don’t want to be bothered with that sort of thing. You can run a Password Manager; I have one on my own phone and work machine to protect my personal files.

**With regards to being a human in the modern world, how much security do we have?**

Google and bank websites are for the most part secure. The communication channel is encrypted, and you know you are talking to, say, the bank server. It is pretty rare with these large organisations for your information to be accessible.

However, every website you visit, every search you make, is monitorable. With DNS requests, those messages are getting sent out to a DNS server and they aren’t encrypted; they are plain text. Your Internet Service Provider can basically see everything you are doing. Cookies can also be used to connect the same person as looking at, say, ten different things. So, there is not as much anonymity on the internet as people might like to think.

I know that Malcolm Turnbull set up a metadata program and built data warehouses to actually monitor the online activity of Australians on the internet and stored this data constantly. In December last year, the Five Eyes organisation got together, and they were saying: look, WhatsApp and Facebook etc. are encrypted and we are losing our ability to do our intelligence work. This is not good. So, Australia turned around and said: well we are going to make legislation changes and force these organisations and give us a back door. I haven’t heard whether the organisations are complying, but the law was passed so chances are it is underway. Basically, the Government wants to be able to access Facebook and these other encrypted applications if they need to. It is said to be a matter of security, but of course, it also raises questions of ethics.

**What are your preferences for operating systems?**

I had always used Windows, but when I was at university, I thought I would ask the lecturers what they recommended. They suggested the MacBook, mostly due to usability for coding and because it ran on Unix. Combined also with the fact that Windows Vista and Windows 8 were pretty bad in terms of operating systems, I jumped across to Mac and stayed over there for years, but I am only just now coming back to Windows 10.

**Historically, Windows has been renowned for its lack of security compared to Apple – is this because most of the corporate environments are Windows, most of the hackers are targeting these systems?**

Yes, that, and because of the price point of Mac as well. I don’t want to say anything out of line, but people who are in the countries where the trends of attacks are statistically coming from, don’t have the money to afford Mac computers. Mac has also been such a small market share historically, so they haven’t been attacked. Because of the widespread usage of the Microsoft platform, they have borne the brunt of attacks, but fortunately this has meant that they now they have defenses to stand up against it.

**It has been said that sometimes the security problem is the user, rather than the system. To what extent is this true?**

Yes, we do find that often the people operating the technology can be the issue. In my line of work, once we have tested the technology enough and it isn’t so easy to get into, we begin testing the process and the people. We do what is called the Red Team exercises—much like a secret shopper—where we try to test physical security. So an example might be where we try to clone access cards; we will put cloning technology in a bag we are carrying and try to get next to someone in a line who has an access card hooked to themselves; we will brush up against them and get it to clone their card and use that to gain physical access to the building.

We also conduct social engineering tests, so we might try to talk our way into a company and test if the security guards will allow us to walk into the building. If I tailgate someone into an elevator or through a glass door that is letting me into their office, or if I was to sit in a meeting room for a week when I wasn’t mean to be there, would somebody actually raise the question and stop me? While this itself isn’t so much cybersecurity, the idea is to ‘hack the humans’ so I can then go and plug in a network tap that has a 4G sim card that connects to their network and gives me secure access to their infrastructure. Obviously, this needs to all be done within the boundaries of Statutory Law.

**In your opinion, how valuable is information as a resource in today’s world?**

Very valuable. The basis of my job is to protect and make sure that there are adequate controls around information. I’m not checking the security of these organisations for a vault; there isn’t money sitting on the premises. It is 100 percent that they have valuable information that needs to be protected, whether that is trade secrets or databases with confidential details. There are various reasons why it has to be kept secure, but it always comes back to the protection of information.

**What advice do you have for someone getting into the IT field?**

I think typically you are passionate about this stuff anyway if you are considering a career in IT; it isn’t something that you just decide to study one day. But it is constantly changing and evolving; I have done four and a half years of undergraduate study, and postgrad work, and I still just don’t stop. You have to continuously learn; technologies are constantly changing, and you can learn stuff one day that you have to let go of the next when something better comes out. You have to be prepared to be dynamic. It is like being in school for the rest of your life; if you have an issue with that, it might not be the right industry for you.