Sydney School of Entrepreneurship

Four things to know about

Cyber Security

for Startups

Developed with CyberCX

As part of Cyber123

If you're a start up, these four points will help you understand what you need to consider about cyber security. If you are interested in learning more on this topic, you can register through this link.

1. You need to shift left with cyber security

Whether you're developing the next big app, or providing a revolutionary B2B service, the earlier you think about cyber security and start integrating it into your planning, the easier and cheaper it will be for you.

"Shifting left" means moving security earlier in your development timeline. This increases your ability to stop issues before they become problems, which will reduce your costs and will help to protect your reputation.

2. The Supply Chain

Many start-ups rely on third-party services to handle aspects of their business, including advertising, customer management, IP, and communications. Have you considered what information you're sharing with these companies? Where are they storing that information? What is their cyber security like? Are they really protecting your data and your customers' data? If they're not, you're the one responsible for it from your customers' perspective.

If you want your product or service to be used by a large enterprise, you will be required to secure your systems from cyber attacks. Despite having good service and/or competitive prices, you are considered a risk to these larger enterprises, unless you can demonstrate a reduced risk level through good cyber security practices.

3. It doesn't have to be hard

People often see cyber security as something that's expensive, complicated, and requires expertise. The truth is it's easy to be more secure than you currently are.

Every business relies on people, processes, and technology and cyber security relies on improving all three areas. Having good processes in place and well-informed people following those processes will limit the amount of technology you need to implement to protect yourself.

There is a significant amount of free advice and education available from both the Australian government and private providers that entrepreneurs can take advantage of.

4. Be prepared - it's not 'if', it's 'when'

Good security means spending most of your efforts on preventing cyber attacks. However, you still need an action plan in the event that an attack is successful. How you respond to, and recover from, a cyber attack is just as important as the preventative measures you put in place.

Preparing by reducing your vulnerability to cyber attacks, and planning how you will respond if you do have a cyber breach are key to maximising your overall cybersecurity.

Register interest now in our course about cyber security for startups

Register your interest here!