

What is Cybersecurity?

Joshua I. James
Digital Forensic Investigation Research Group
University College Dublin
Belfield, Dublin 4
Ireland

April 4, 2013

Last week, a number of Korean organizations fell victim to cyber attacks. This has prompted discussions about cybersecurity in Korea, and while following this issue I've realized that Korea's main challenge appears to be understanding what cybersecurity actually is.

From many of the discussions, representatives from various organizations appear to believe that security is a force, much like the police or military. Cybersecurity, however, is not an organization. It is not something that can be prevented by a single group. Cybersecurity is a responsibility – a *mindset* – that each technology user must adopt. Everyone plays a part in the cybersecurity of Korea, and anyone not considering the security of their devices are putting not only themselves, but also their friends/family/workplace/bank/government/etc. in danger.

Indeed, organizations can play a part in helping to improve cybersecurity. Police investigations, for example, can lead to catching cyber criminals, and thus potentially reduce on-line crime. But Police cannot be everywhere, and are inherently reactionary. And unless citizens want the government protecting the people from themselves (via pre-incident monitoring to make sure you don't click on the 'wrong' link), then security of the country should be achieved through education of *everyone*.

The thing that every citizen, company and government entity needs to realize that your device probably *will* be compromised. So think of security as a function of time. With enough time, even the strongest security can be broken. So just give hackers less time. Change your passwords often, factory reset your phone and reformat your computers every 6 to 12 months, make sure your software is always up to date, use anti-viruses and firewalls on all your devices, and be very selective about software and websites you use. There is a lot of information available about on-line security¹, so there is really no reason not to understand and implement the basics. It doesn't take a lot of time, and it could end up saving you, or someone you love, a lot of inconvenience later.

Remember, cybercrime is not static. Security that worked yesterday may not work today. So securing devices should become a way of life, not a once-off effort.

¹For example, Google's tips for staying safe: www.google.com/intl/ko/goodtoknow
See also: www.kisa.or.kr and www.ctr.c.go.kr