Four things you should be doing to protect yourself from cyberattack

October 16 2015, by Robert Potter

Credit: AI-generated image (disclaimer)

It is easy to get lost in a sea of information when looking at cybersecurity issues. And hearing about hacks and cyberattacks as they happen is a surefire way to feel helpless and totally disempowered.

What follows is a sort of future shock, where we become fatalistic about

the problem. After all, 86% of organisations from around the world surveyed by PwC reported exploits of some aspect of their systems within a one year period. That represented an increase of 38% on the previous year.

However, once the situation comes into focus, the problem becomes much more manageable. There are a range of things that can we can easily implement to reduce the risk of an incident dramatically.

For example, Telstra estimates that 45% of security incidents are the result of staff clicking on malicious attachments or links within emails. Yet that is something that could be fairly easily fixed.

Confidence gap

There is currently a gap between our confidence in what we can do about security and the amount we can actually do about it. That gap is best filled by awareness.

Many organisations, such as the Australian Centre for Cyber Security, American Express and Distil Networks provide basic advice to help us cope with future shock and start thinking proactively about cybersecurity.

The Australia Signals Directorate (ASD) – one of our government intelligence agencies – also estimates that adhering to its Top Four Mitigation Strategies would prevent at least 85% of targeted cyberattacks.

So here are some of the top things you can do to protect yourself from cyberattacks:

1) Managed risk

First up, we need to acknowledge that there is no such thing as perfect security. That message might sound hopeless but it is true of all risk management; some risks simply cannot be completely mitigated.

However, there are prudent treatments that can make risk manageable. Viewing cybersecurity as a natural extension of traditional risk management is the basis of all other thinking on the subject, and a report by CERT Australia states that 61% of organisations do not have cybersecurity incidents in their risk register.

ASD also estimates that the vast majority of attacks are not very sophisticated and can be prevented by simple strategies. As such, think about cybersecurity as something that can managed, rather than cured.

2) Patching is vital

Patching is so important that ASD mentions it twice on its top four list. Cybersecurity journalist Brian Krebs say it three times: "update, update, update".

Update your software, phone and computer. As a rule, don't use Windows XP, as Microsoft is no longer providing security updates.

Updating ensures that known vulnerabilities are fixed and software companies employ highly qualified professionals to develop their patches. It is one of the few ways you can easily leverage the cybersecurity expertise of experts in the field.

3) Restricting access means restricting vulnerabilities

The simple rule is: don't have one gateway for everything. If all it takes to get into the core of a system is one password, then all it takes is one mistake for the gate to be opened.

Build administrator privileges into your system so that people can only use what they are meant to. For home businesses it could mean something as simple as having separate computers for home and work, or not giving administrator privileges to your default account.

It could also be as simple as having a content filter on employee internet access so they don't open the door when they accidentally click on malware.

4) Build permissions from the bottom up

Application whitelisting might sound complicated, but what it really means is "deny by default": it defines, in advance, what is allowed to run and ensures that nothing else will.

Most people think of computer security as restricting access, but whitelisting frames things in opposite terms and is therefore much more secure. Most operating systems contain whitelisting tools that are relatively easy to use. When used in conjunction with good advice, the result is a powerful tool to protect a network.

Simple things first

Following these basic rules covers the same ground as ASD's top four mitigation strategies and substantially lowers your vulnerability to cyberattack. If you want to delve deeper, there are more tips on the ASD site.

There are many debates that will follow on from this, such as: developing a national cybersecurity strategy; deciding if people should have to report an incident; the sort of insurance that should be available; what constitutes a proportionate response to an attack; and a whole range of others.

Each of those debates is underpinned by a basic set of information that needs to be implemented first. Future shock is something that can be overcome in this space, and there are relatively simple measures that can be put into place in order to make us more secure. Before embarking on anything complicated, we should at least get these things right.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation