With bugs in the system how safe is the internet?

May 1 2014, by Alastair Macgibbon

Popular web browser Internet Explorer the target for the latest security vulnerability. Credit: Flickr/Hash Milhan, CC BY

It seems hardly a week goes by without a major cyber security flaw exposed that could be exploited across millions of internet and mobile connected devices.

This week it was the Internet Explorer browser's turn with Microsoft warning of a vulnerability in the software that needs to be patched. Before that it was the Heartbleed vulnerability found in the Open SSL software used to encrypt communications between us and perhaps 60% of the world's websites.

NSW police warned this week that Eastern European gangs in Sydney have been busy conducting scaled skimming attacks against ATMs, stealing card data and PINs.

Before Christmas US retail giant Target lost control of millions of customer credit card details when point of sale devices were compromised after an attacker initially entered their corporate systems via an air conditioning and heating maintenance interface.

And diplomatic relations have been harmed – and cyber citizens infuriated – by mass data surveillance by governments exposed in files leaked by former NSA contractor Edward Snowden.

What does this tell us?

We increasingly rely upon complex software and hardware for our professional and personal lives. They run the critical systems upon which our society and economy depend and yet these connected devices are not as robust as we'd like to tell ourselves.

While some tech giants market themselves as the safer option, immune from cyber nasties, we should avoid falling for the hype: there but for the grace of God go they. In fact, it's more likely that they have been and are compromised, we just don't know of it yet.

For years Microsoft was lambasted as an unsafe operating system, when the reality was that criminals devoted considerable effort to breaking their product because it was on more computers and thus a bigger addressable market for those criminals.

Figures for March this year show Microsoft's Windows operating system has 91% of the market share compared to 8% on Apple's Mac with Linux users just 1.5%

As the mix of operating systems has become more complex, then exploits have become more common across the board. This is best illustrated by the growing list of malware specifically designed for Google's Android mobile operating system.

No time to act

We are learning that some vulnerabilities are in the wild for years before being exposed, leaving attackers ample time to conduct their business. These "zero day" (as in defenders have zero days to prepare against an attack) exploits were once considered to be theoretical only, but are now commonplace.

Despite dire warnings of the end of the internet as we know it, both the internet and its users are more resilient than we give them credit for, and in many respects it is business as usual online.

But that doesn't mean we should be complacent.

We know that computer crime is on the rise and criminals have access to hundreds of millions of stolen credit and debit card information. We know that they have control of millions of computers where they can extract our private data, use our computers as spam devices, or as part of large scale "botnet" armies that can launch denial of service attacks against critical systems. We know that huge amounts of corporate intellectual property has been plundered and transferred, lessening the economic viability of those companies.

We should be heartened by the fact that there are honest people working feverishly to protect us: security researchers and technicians who keep building better mouse traps.

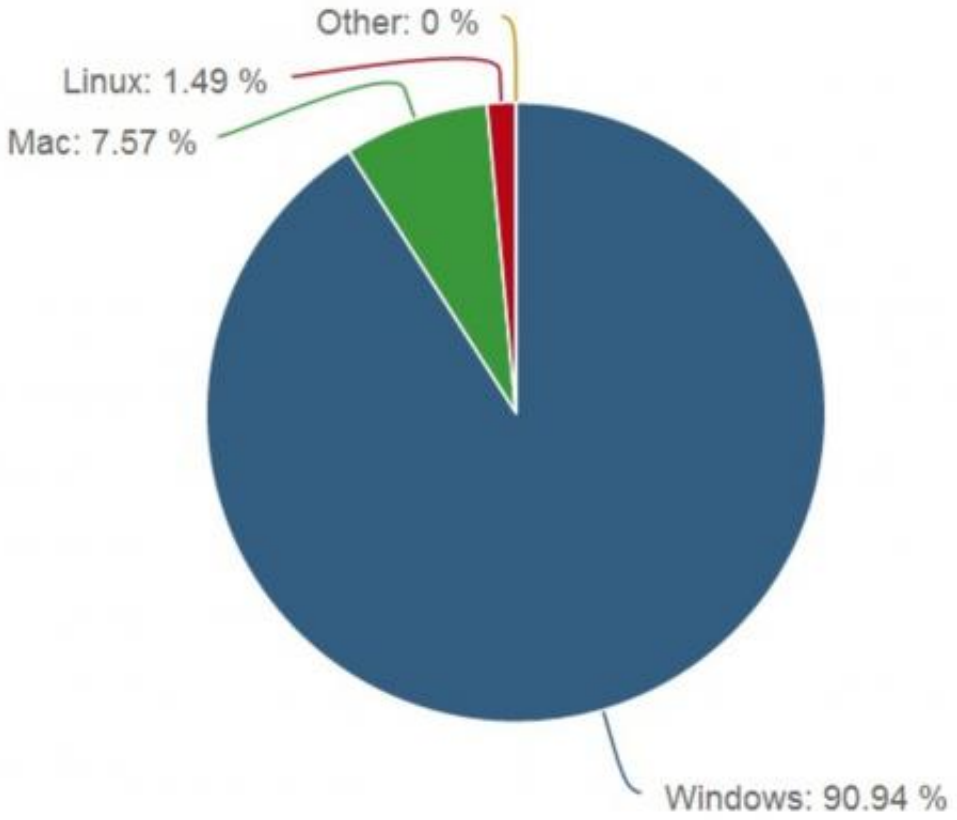
Police and regulators are doing what they can to track down cyber

criminals while educating end users and companies about how to be safer such as the federal government's Stay Smart Online campaign. There are many responsible companies investing in updating hardware and software.

Like so many social issues though this problem won't be fixed any time soon. Perhaps it never will. But it won't all come crashing down around us either, in spite of some media reporting.

Beware of fear fatigue

There is always the danger that people become complacent as more and more security threats are reported so it's important to be aware of the risks and take note of any advice.



Operating systems in use - March 2014. Credit: Net Market Share

Simply asking people to swap to alternate software or systems is not always the best as it assumes those other options are safe. As I said before, are they safer?

So what's the best advice on how to get by in this threat environment?

As end users, we need to make sure we have unique and hard to guess passwords, and change them often. We should patch our software with updates as often as they are available. We need to use security software where possible.

When it comes to using the internet we must be careful where we visit on the web and whose email and other messages we open: just like in the offline world there are safer places to visit and people to interact with.

But we must also demand more products that are fit for purpose, just as we do with the safety standards of physical consumer products.

We should expect companies to understand the value of the business they do with us, and of our data that they hold in trust. Boards and CEOs need to care about this as much as they do about their brand.

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

Source: The Conversation