We don't know the half of it

- Thursday 20 April 2017, 00:01
- by Michael Grey

Businesses need to secure themselves against rogue insiders as well as external cyber criminals. Gleb Stock/Shutterstock.com

The threat to companies from cyber attacks is bigger than we think and chief executives need to take it seriously

WAS some US military hacker responsible for a North Korean test missile exploding spectacularly just after its launch the other day? Is your chairman's smartphone busily transmitting confidential information to your overseas competitors in real time during your board meeting? As your containership makes its leisurely way across the ocean, is its entire bill of loading and stowage plans being scrutinised by a gang of e-enabled criminals based in your main discharge port? Or is some young nerd in his bedroom on the brink of taking out, with a few keystrokes, all the electronics on your huge cruiseship as it manoeuvres off a tricky berth?

I haven't the foggiest about the answers to any of these questions, but if an authoritative affirmative was appended to any one of them, we shouldn't perhaps be remotely surprised. The completely implausible scenario of just a few years ago is no longer categorised in the science-fiction department, but has moved firmly mainstream. We, as members of the public, don't know half of what is going on in this mysterious and confusing world of cyberspace.

With what high hopes we greeted the arrival of the internet, which was seen to be such a benison to mankind! I suppose there were cautious types who would have divided a piece of paper into columns of "opportunities" and "threats", but the list under the former would have hugely outnumbered that beneath the latter, at least for the first few years. Now, as we wonder whether we are being spied upon by our TV sets or "intelligent" refrigerators, and know for a fact that our location can be determined by the telephone in our pockets, that latter list is growing.

You get the occasional clue about the need to defend ourselves against cyber attacks. At a conference about future navigation just last year, I recall being amazed at the sheer volume of vulnerable equipment on the average modern merchant ship. Delegates heard about the colossal cost to navies to ensure that their warships' systems are not compromised electronically, which seemingly dwarf the sums being spent on military hardware in the first place.

We are beginning to appreciate some of the rudiments of the defensive strategies we need to adopt, in both business and as individuals. There is easily digestible, sensible advice being made available by BIMCO, and other market watchers, that lists the threats that menace our electronic and real-world safety. But it is a world that is moving very fast and dedicated, professional expertise is clearly called for if we are to be kept cyber-secure.

Andrew Fitzmaurice of Templar Securities is one of the authors of the UK government's national cyber security strategy and designs cyber security transformation programmes for governments and companies. He is ex-military and can give you a talk about cyber security that will scare you half to death as he elaborates on all the vulnerabilities you may not have thought of, as well as those that have been keeping you awake at night.

Speaking to the International Maritime Industries Forum the other day, he advocated greater awareness of the dangers of cyber attacks, encouraged coping strategies and emphasised that these were issues to be taken very seriously at the very top of any organisation. Nobody can opt out of the problem or consider that it is all within the competence of the IT department. This needed to be high on the agenda of every well-run business, he said, adding that the need to invest in people, processes and technology in this area was a "no-brainer".

Explosive growth

The internet knows no boundaries, it remains unregulated and is bound to grow exponentially. He cited the explosive growth in connectivity in huge populations like that of India, the need to tackle crime and build resilience in such an environment, noting that while the focus might zero in on criminals, "competitors, innocents (those making simple mistakes) and insiders" needed to be viewed very seriously, the latter being regarded by professionals as the biggest threat to the safety of businesses.

He emphasised simple password security and showed a short film which illustrated how a person with a pretty face and convincing manner can persuade a stranger to reveal their password. We watched a very professional video sales pitch for, of all things, the Dark Web, illustrating that serious, organised crime has stayed at the forefront of the technology and is now becoming what might be described as a third party managed service, available to unscrupulous people the world over. Things have moved on very fast from the corrupted database, ransomware or hard-luck stories from West Africa.

He left a lot of questions with his audience. Were there company insiders suffering midlife crises who could be suborned or bought by unscrupulous people? Was there confidence about the cyber safety of suppliers? Reminding us of the spy Edward Snowden, whose origins were in IT within a defence contractor, he asked: "Who watches the watchers?"

It would be quite easy to relapse into complete paranoia about an area in which all but the experts appear so helpless and vulnerable. "We don't know the half of it" was the old saying that kept sounding in my head as I nervously checked my smartphone at the end of the talk.

It is easy to criticise senior management for apparent incomprehension when the head of the IT department calls for all that extra investment in processes, people and technology. But it is also important that the expert can present this case in a manner that does not leave the chief executive utterly bewildered by meaningless jargon, something that is not altogether unknown.

Maybe we won't know what GCHQ or the FBI are monitoring, or the extent of President Trump's electronic capabilities, but just having sensible policies in place, aided by experts, would be a good start.

rjmgrey@dircon.co.uk
Article from Lloyd's List
https://www.lloydslist.com/ll/sector/ship-operations/article554038.ece
Published: Thursday 20 April 2017