Safety last

How to manage the computer-security threat

The incentives for software firms to take security seriously are too weak



COMPUTER security is a contradiction in terms. Consider the past year alone: cyberthieves stole $81m from the central bank of Bangladesh; the $4.8bn takeover of Yahoo, an internet firm, by Verizon, a telecoms firm, was nearly derailed by two enormous data breaches; and Russian hackers interfered in the American presidential election.

Away from the headlines, a black market in computerised extortion, hacking-for-hire and stolen digital goods is booming. The problem is about to get worse. Computers increasingly deal not just with abstract data like credit-card details and databases, but also with the real world of physical objects and vulnerable human bodies. A modern car is a computer on wheels; an aeroplane is a computer with wings. The arrival of the “Internet of Things” will see computers baked into everything from road signs and MRI scanners to prosthetics and insulin pumps. There is little evidence that these gadgets will be any more trustworthy than their desktop counterparts. Hackers have already proved that they can take remote control of connected cars and pacemakers.

It is tempting to believe that the security problem can be solved with yet more technical wizardry and a call for heightened vigilance. And it is certainly true that many firms still fail to take security seriously enough. That requires a kind of cultivated paranoia which does not come naturally to non-tech firms. Companies of all stripes should embrace initiatives like “bug bounty” programmes, whereby firms reward ethical hackers for discovering flaws so that they can be fixed before they are taken advantage of.

But there is no way to make computers completely safe. Software is hugely complex. Across its products, Google must manage around 2bn lines of source code—errors are inevitable. The average program has 14 separate vulnerabilities, each of them a potential point of illicit entry. Such weaknesses are compounded by the history of the internet, in which security was an afterthought (see article).

Leaving the windows open

This is not a counsel of despair. The risk from fraud, car accidents and the weather can never be eliminated completely either. But societies have developed ways of managing such risk—from government regulation to the use of legal liability and insurance to create incentives for safer behaviour.

Start with regulation. Governments’ first priority is to refrain from making the situation worse. Terrorist attacks, like the recent ones in St Petersburg and London, often spark calls for encryption to be weakened so that the security services can better monitor what individuals are up to. But it is impossible to weaken encryption for terrorists alone. The same protection that guards messaging programs like WhatsApp also guards bank transactions and online identities. Computer security is best served by encryption that is strong for everyone.

The next priority is setting basic product regulations. A lack of expertise will always hamper the ability of users of computers to protect themselves. So governments should promote “public health” for computing. They could insist that internet-connected gizmos be updated with fixes when flaws are found. They could force users to change default usernames and passwords. Reporting laws, already in force in some American states, can oblige companies to disclose when they or their products are hacked. That encourages them to fix a problem instead of burying it.

Go a bit slower and fix things

But setting minimum standards still gets you only so far. Users’ failure to protect themselves is just one instance of the general problem with computer security—that the incentives to take it seriously are too weak. Often, the harm from hackers is not to the owner of a compromised device. Think of botnets, networks of computers, from desktops to routers to “smart” light bulbs, that are infected with malware and attack other targets.

Most important, the software industry has for decades disclaimed liability for the harm when its products go wrong. Such an approach has its benefits. Silicon Valley’s fruitful “go fast and break things” style of innovation is possible only if firms have relatively free rein to put out new products while they still need perfecting. But this point will soon be moot. As computers spread to products covered by established liability arrangements, such as cars or domestic goods, the industry’s disclaimers will increasingly butt up against existing laws.

Firms should recognise that, if the courts do not force the liability issue, public opinion will. Many computer-security experts draw comparisons to the American car industry in the 1960s, which had ignored safety for decades. In 1965 Ralph Nader published “Unsafe at Any Speed”, a bestselling book that exposed and excoriated the industry’s lax attitude. The following year the government came down hard with rules on seat belts, headrests and the like. Now imagine the clamour for legislation after the first child fatality involving self-driving cars.

Fortunately, the small but growing market in cyber-security insurance offers a way to protect consumers while preserving the computing industry’s ability to innovate. A firm whose products do not work properly, or are repeatedly hacked, will find its premiums rising, prodding it to solve the problem. A firm that takes reasonable steps to make things safe, but which is compromised nevertheless, will have recourse to an insurance payout that will stop it from going bankrupt. It is here that some carve-outs from liability could perhaps be negotiated. Once again, there are precedents: when excessive claims against American light-aircraft firms threatened to bankrupt the industry in the 1980s, the government changed the law, limiting their liability for old products.

One reason computer security is so bad today is that few people were taking it seriously yesterday. When the internet was new, that was forgivable. Now that the consequences are known, and the risks posed by bugs and hacking are large and growing, there is no excuse for repeating the mistake. But changing attitudes and behaviour will require economic tools, not just technical ones.