The Economist

SPECIAL REPORT
CYBER-SECURITY
JULY 12th 2014

Defending the digital frontier

Defending the digital frontier

Companies, markets and countries are increasingly under attack from cyber-criminals, hacktivists and spies. They need to get much better at protecting themselves, says Martin Giles

THE TERM "CYBERSPACE" was coined by William Gibson, a science-fiction writer. He first used it in a short story in 1982, and expanded on it a couple of years later in a novel, "Neuromancer", whose main character, Henry Dorsett Case, is a troubled computer hacker and drug addict. In the book Mr Gibson describes cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators" and "a graphic representation of data abstracted from the banks of every computer in the human system."

His literary creation turned out to be remarkably prescient. Cyberspace has become shorthand for the computing devices, networks, fibre-optic cables, wireless links and other infrastructure that bring the internet to billions of people around the world. The myriad connections forged by these technologies have brought tremendous benefits to everyone who uses the web to tap into humanity's collective store of knowledge every day.

But there is a darker side to this extraordinary invention. Data breaches are becoming ever bigger and more common. Last year over 800m records were lost, mainly through such attacks (see chart 1, next page). Among the most prominent recent victims has been Target, whose chief executive, Gregg Steinhafel, stood down from his job in May, a few months after the giant American retailer revealed that online intruders had stolen millions of digital records about its customers, including credit- and debit-card details. Other well-known firms such as Adobe, a tech company, and eBay, an online marketplace, have also been hit.

The potential damage, though, extends well beyond such commercial incursions. Wider concerns have been raised by the revelations about the mass surveillance carried out by Western intelligence agencies made by Edward Snowden, a contractor to America's National Security Agency (NSA), as well as by the growing numbers of cyber-warriors being recruited by countries that see cyberspace as a new domain of war- ▸▸

CONTENTS

A list of sources is at **Economist.com/specialreports**

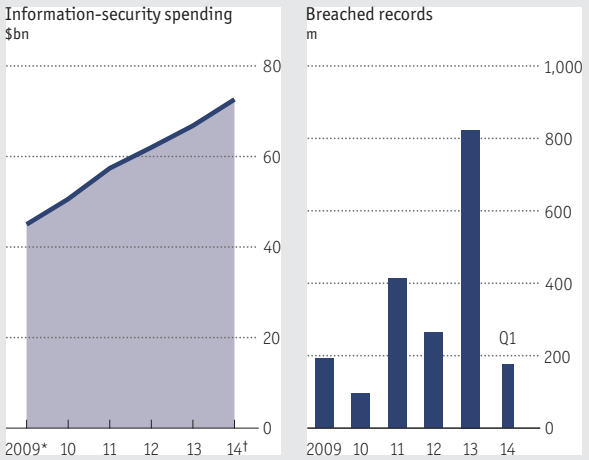
An audio interview with the author is at **Economist.com/audiovideo/specialreports**

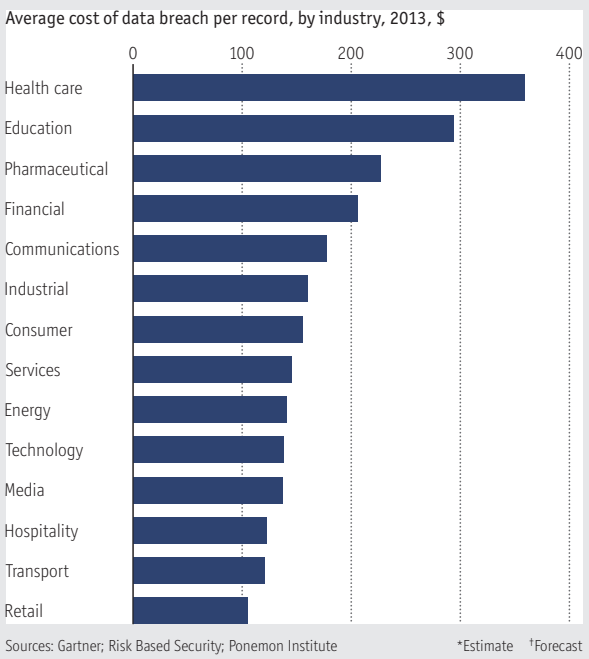
ACKNOWLEDGMENTS

Apart from those mentioned in the text, the author would like to thank the following for their help with preparing this report: Rohyt Belani, Dave Clemente, David DeWalt, Neil Gershenfeld, Ellen Giblin, Rajiv Gupta, Eugene Kaspersky, James Lewis, Jarno Limnell, Alain Louchez, Marc Maiffret, Barmak Meftah, Brent Rowe, Phyllis Schneck and Paul Swarbrick.

A world of insecurity 1

Worldwide





Sources: Gartner; Risk Based Security; Ponemon Institute *Estimate †Forecast

fare. America's president, Barack Obama, said in a White House press release earlier this year that cyberthreats "pose one of the gravest national-security dangers" the country is facing.

Securing cyberspace is hard because the architecture of the internet was designed to promote connectivity, not security. Its founders focused on getting it to work and did not worry much about threats because the network was affiliated with America's military. As hackers turned up, layers of security, from antivirus programs to firewalls, were added to try to keep them at bay. Gartner, a research firm, reckons that last year organisations around the globe spent $67 billion on information security.

On the whole, these defences have worked reasonably well. For all the talk about the risk of a "cyber 9/11" or a "cyber-geddon", the internet has proved remarkably resilient. Hundreds of millions of people turn on their computers every day and bank online, shop at virtual stores, swap gossip and photos with their friends on social networks and send all kinds of sensitive data over the web without ill effect. Companies and governments are shifting ever more services online.

But the task is becoming harder. Cyber-security, which involves protecting both data and people, is facing multiple threats, notably cybercrime and online industrial espionage, both of which are growing rapidly. A recent estimate by the Centre for Strategic and International Studies (CSIS), a think-tank, puts the annual global cost of digital crime and intellectual-property theft at $445 billion—a sum roughly equivalent to the GDP of a smallish rich European country such as Austria.

To add to the worries, there is also the risk of cyber-sabotage. Terrorists or agents of hostile powers could mount attacks on companies and systems that control vital parts of an economy, including power stations, electrical grids and communications networks. Such attacks are hard to pull off, but not impossible. One precedent is the destruction in 2010 of centrifuges at a nuclear facility in Iran by a computer program known as Stuxnet, the handiwork of American and Israeli software experts.

In another high-profile sabotage incident, in 2012, a computer virus known as Shamoon wiped the hard drives of tens of thousands of computers at Saudi Aramco, a Saudi Arabian oil and natural-gas giant, and left a picture of a burning American flag on the screens of the stricken devices. The assault is widely thought to have been carried out by Iran.

Look for the crooks and spooks

But such events are rare. The biggest day-to-day threats faced by companies and government agencies come from crooks and spooks hoping to steal financial data and trade secrets, so this special report will focus mainly on cybercrime and cyber-espionage. Smarter, better-organised hackers are making life tougher for the cyber-defenders, but the report will argue that even so a number of things can be done to keep everyone safer than they are now.

One is to ensure that organisations get the basics of cyber-security right. All too often breaches are caused by simple blunders, such as failing to separate systems containing sensitive data from those that do not need access to them. Companies also need to get better at anticipating where attacks may be coming from and at adapting their defences swiftly in response to new threats. Technology can help, as can industry initiatives that allow firms to share intelligence about risks with each other.

This report will also argue that there is a need to provide incentives to improve cyber-security, be they carrots or sticks. One idea is to encourage internet-service providers (ISPs), or the companies that manage internet connections, to shoulder more responsibility for identifying and helping to clean up computers infected with malicious software (malware). Another is to find ways to ensure that software developers produce code with fewer flaws in it so that hackers have fewer security holes to exploit.

An additional reason for getting tech companies to give a higher priority to security is that cyberspace is about to undergo another massive change. Over the next few years billions of new devices, from cars to household appliances and medical equipment, will be fitted with tiny computers that connect them to the web and make them more useful. Dubbed "the internet of things", this is already making it possible, for example, to control home appliances using smartphone apps and to monitor medical devices remotely.

But unless these systems have adequate security protection, the internet of things could easily become the internet of new things to be hacked. Plenty of people are eager to take advantage of any weaknesses they may spot. Hacking used to be about geeky college kids tapping away in their bedrooms to annoy their elders. It has grown up with a vengeance. ■

Cybercrime

Hackers Inc

Cyber-attackers have multiplied and become far more professional

AT 2PM ON March 20th 2013 the hard drives of tens of thousands of computers in South Korea were suddenly wiped clean in a massive cyber-attack. The main targets were banks and news agencies. At first the assault looked like a case of cyber-vandalism. But as they probed deeper, the computer sleuths investigating it came to a different conclusion.

The operation, which they dubbed "Dark Seoul", had been carefully planned. The hackers had found their way into the targets' systems a couple of months earlier and inserted the software needed to wipe drives. Just before the attack they added the code needed to trigger it. Looking at the methods the intruders used, the investigators from McAfee, a cyber-security firm, thought that the attack might have been carried out by a group of hackers known for targeting South Korean military information.

But they could not be sure. Tracing the exact source of an attack can be next to impossible if the assailants want to cover their tracks. Over the past decade or so various techniques have been developed to mask the location of web users. For example, a technology known as Tor anonymises internet connections by bouncing data around the globe, encrypting and re-encrypting them until their original sender can no longer be traced.

Conversely, some hackers are only too happy to let the world know what they have been up to. Groups such as Anonymous and LulzSec hack for fun ("lulz" in web jargon) or to draw attention to an issue, typically by defacing websites or launching distributed-denial-of-service (DDoS) attacks, which involve sending huge amounts of traffic to websites to knock them offline. Anonymous also has a track record of leaking e-mails and other material from some of its targets.

Criminal hackers are responsible for by far the largest number of attacks in cyberspace and have become arguably the biggest threat facing companies. Some groups have organised them- ▸▸

Zero-day game

Wielding a controversial cyber-weapon

"HOW DO YOU protect what you want to exploit?" asks Scott Charney, an executive at Microsoft. He highlights a dilemma. Intelligence agencies look for programming mistakes in software so they can use them to spy on terrorists and other targets. But if they leave open these security holes, known in tech jargon as "vulnerabilities", they run the risk that hostile hackers will also find and exploit them.

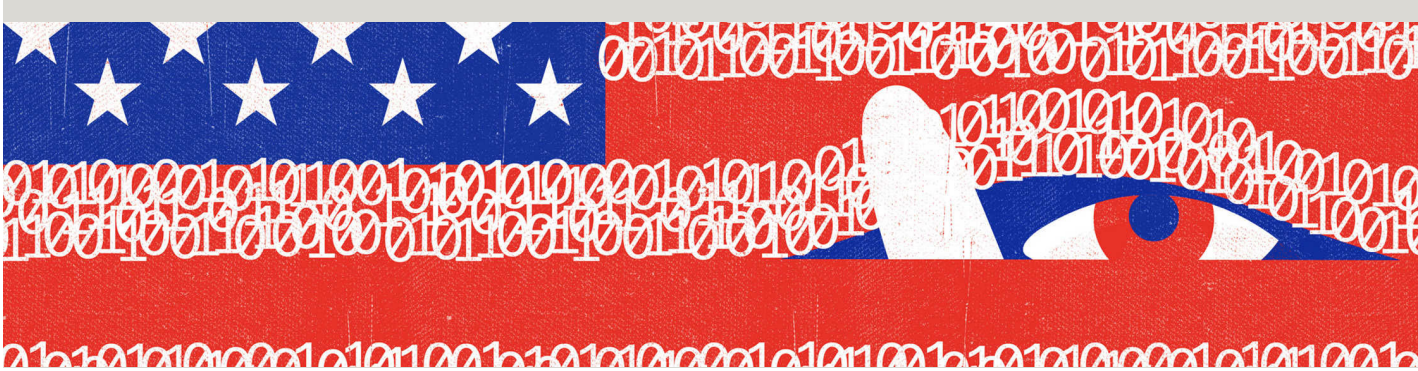
Academics, security researchers and teams from software firms unearth hundreds of vulnerabilities each year. One recent discovery was the Heartbleed bug, a flaw in a widely used encryption system. Software-makers encourage anyone who finds a flaw to let them know immediately so they can issue "patches" for their programs before hackers can take advantage of them. That is how most vulnerabilities are dealt with. Some firms even run "bug bounty" schemes that reward people for pointing out flaws.

But there will always be "zero-days", or brand new vulnerabilities that software makers do not know about and for which no patch yet exists. Hackers who can get their hands on the source code of a program can use various tools to try to find holes in it. Another technique is "fuzzing", which involves pushing random data into the inputs of a program. If it crashes or signals an anomaly, that indicates a bug is present which may offer a way in.

Zero-days are rare, and can often be used for some time before someone else spots them. Two researchers at Symantec, a cyber-security firm, studied 18 zero-days found by the firm's software in 2008-10 and concluded that the flaws remained undetected for an average of ten months.

The use of such vulnerabilities by Western intelligence agencies has sparked a debate about the wisdom of stockpiling digital weapons that weaken the security of cyberspace. But zero-days may occasionally be needed to uncover information crucial to national security, so a few have to be kept to hand. In America, a report by a presidential panel to review cyber-security after Edward Snowden's revelations, published last December, urged the government not in any way to "subvert, undermine, weaken or make vulnerable" generally available commercial software, and to fix zero-day vulnerabilities quickly, with rare exceptions.

In April Michael Daniel, the White House's adviser on cyber-security, announced that the NSA's future policy on exploiting zero-days would have a "bias" towards disclosing them unless there was a clear need to retain them on national-security or law-enforcement grounds. But what might constitute such a need was left unsaid.



selves so thoroughly that they resemble mini-multinationals. Earlier this year a joint operation by police from a number of countries brought down the cybercrime ring behind a piece of malware called Blackshades, which had infected more than half a million computers in over 100 countries. The police found that the group was paying salaries to its staff and had hired a marketing director to tout its software to hackers. It even maintained a customer-support team.

Such organised hacking empires are becoming more common. "Crime has changed dramatically as a result of the internet," says Andy Archibald, the head of Britain's National Cyber Crime Unit. Criminal hackers are involved in two broad sets of scams. In the first, they help carry out traditional crimes. Last year police in the Netherlands and Belgium broke up a drug-smuggling ring that had hired a couple of computer experts to beef up its logistics. The gang hid drugs in legitimate shipments of goods destined for the port of Antwerp, using the hackers to break into the IT systems of shipping companies at the port and steal the security codes for the containers so the crooks could haul them away before their owners arrived.

Economies of scale

The second type of crime takes place entirely online. In June American authorities issued charges against the Russian mastermind behind the GameOver Zeus botnet, a sophisticated piece of malware that steals login details for people's bank accounts from infected computers and uses them to drain cash from their accounts. The FBI puts the losses at over $100m. "Robbing one person at a time using a knife or gun doesn't scale well. But now one person can rob millions at the click of a button," says Marc Goodman of the Future Crimes Institute.

In the past year or so police have scored some other notable victories against digital crooks. These include the arrest of the man behind Silk Road, a notorious online bazaar that sold guns, drugs and stolen credit-card records, and a raid on servers hosting Cryptolocker, a "ransomware" program which encrypts computer files, decrypting them only on payment of a ransom.

Cybercrimes often involve multiple jurisdictions, which makes investigations complicated and time-consuming. And good cybersleuths are hard to find, because the sort of people who are up to the job are also much in demand by companies, which usually offer higher pay. Mr Archibald says he is trying to get more private firms to send him computer-savvy employees on secondment.

Crooks are generally after money. The motives of state-sponsored or state-tolerated hackers are harder to categorise, ranging from a wish to cause chaos to pilfering industrial secrets. The Syrian Electronic Army, for example, generates publicity by defacing the websites of media companies. Last year it hijacked the Twitter account of the Associated Press and posted a tweet falsely claiming that the White House had been bombed.

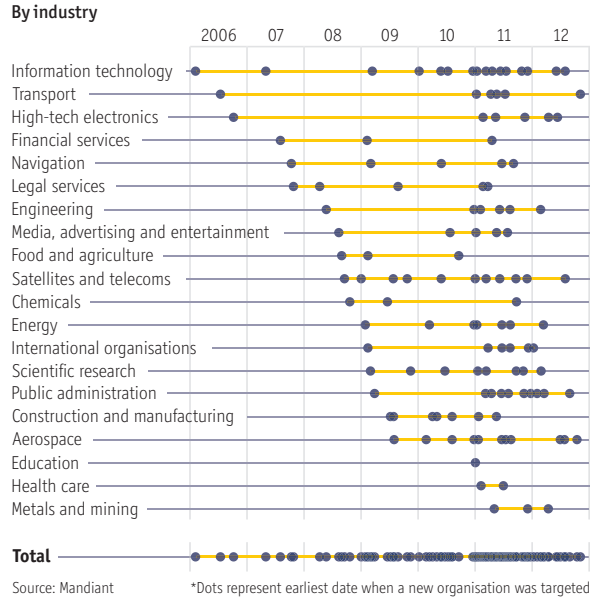
Other groups that have caught security people's attention include Operation Hangover, based in India and focused on Pakistani targets, and the Elderwood Group, a Chinese hacker outfit that was behind a series of attacks in 2009 on American tech companies such as Google. Such groups have become collectively known by a new acronym, APTs, or advanced persistent threats. "These hackers are smart and they wage long-term campaigns," says Mike Fey, McAfee's chief technology officer.

Unlike criminals, who typically scatter malware far and wide to infect as many targets as possible, APT groups concentrate on specific targets. They often use "spear-phishing" attacks, trying to trick people into divulging passwords and other sensitive information, to get access to networks. And once inside, they sometimes lie low for weeks or months before striking.

Government spies typically use the same tactics, so it can be hard to tell the difference between state-run spying and the private sort. When Mandiant, a cyber-security firm, published a report last year about China's industrial-espionage activities, it labelled it "APT1". The report claimed that Chinese hackers from Unit 61398, a Shanghai-based arm of the People's Liberation Army, had broken into dozens of corporate networks over a number of years, paying special attention to industries such as technology and aerospace that China sees as strategic (see chart 2). In May America's Justice Department indicted five Chinese hackers from the unit in absentia for attacks on the networks of some American firms and a trade union.

From China with malice 2

Organisations targeted by one Chinese group of hackers*



Source: Mandiant

*Dots represent earliest date when a new organisation was targeted

Cybercrimes often involve multiple jurisdictions, which makes investigations complicated and time-consuming. And good cybersleuths are hard to find

China is not the only country involved in extensive cyber-espionage. Edward Snowden's leaks have shown that America's NSA ran surveillance programmes that collected information direct from the servers of big tech firms, including Microsoft and Facebook, and that it eavesdropped on executives at Huawei, a large Chinese telecoms firm. American officials like to claim that the NSA's spying is not designed to be of direct benefit to American firms, though it has certainly sought intelligence on issues such as trade negotiations that are likely to be helpful to all American companies.

Blocking sophisticated and highly targeted attacks is extremely difficult. Defenders are like the batsmen in a cricket game who must deflect every ball heading for the stumps; hackers just need to knock off the bails once to win. But the defence would greatly improve its chances by getting a few basic things right. ■

Business

Digital disease control

Basic security hygiene goes a long way

SAFEGUARDING CYBER-SECURITY is a bit like trying to keep an infectious disease at bay. Nasty software can spread swiftly to large populations, so it has to be identified quickly and information passed on immediately to ensure that others can protect themselves. Ideally, organisations should avoid catching an infection in the first place—but that requires them to get better at basic security hygiene.

The story of the hackers who hit the bull's eye at Target is revealing. They are thought to have broken into the computers of a heating, ventilation and air-conditioning firm that was a supplier to Target and had access to login details for the retailer's systems. Once inside, the hackers were able to install malware on Target's point-of-sale system that captured credit- and debit-card details at tills before the data were encrypted. This scam affected some 40m customers.

The debacle showed up several flaws in Target's security that the company has since fixed. It has strengthened internal firewalls to make it harder for hackers to move across its network if they find a way in. It has also developed "whitelisting" rules for its point-of-sale system, which will flag up any attempt to install software that has not been pre-approved. And it has reinforced security around passwords used by its staff and contractors.

At eBay, cyber-attackers were able to get their hands on the login details of some employees and used these to gain access to a database containing encrypted customer passwords and other non-financial data. The firm asked all its 145m users to change their passwords as a precaution, but says it has seen no evidence of any spike in fraudulent activity. It also reassured customers that their financial and credit-card data were held in encrypted form in databases not affected by the attack.

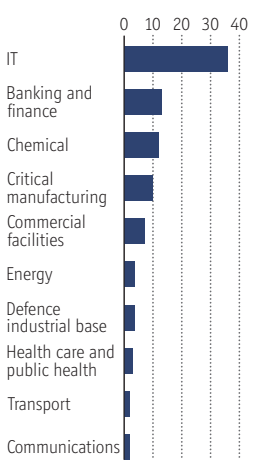
Both of these cases highlight the need to think carefully about how data are stored and who has access to them. They also demonstrate the importance of encryption. When Mr Snowden addresses conference audiences (which he does via video link from Russia), he often reminds them that strong encryption can frustrate even the NSA. That is why a number of technology companies, including Microsoft, Yahoo and Google, are now encrypting far more of the data that flow across their networks, and between themselves and their customers.

Educating employees about security risks is equally important. In particular, they need to be aware of the danger of spear-phishing attacks, which often use false e-mail addresses and websites. Kaspersky Lab, a cyber-security firm, found that globally an average of 102,000 people a day were hit by phishing attacks in the year to April 2013. Security software has got better at weeding out suspect mail, but hackers are constantly trying new tactics.

Whom can you trust? 3

Intellectual-property theft in America by insiders

By industry, % of total



Source: Carnegie Mellon CERT

Your birthday won't do

Their job would be made harder if people picked more robust passwords. Verizon, a telecoms company, studied 621 data breaches in 2012 in which 44m records were lost and found that in four out of five cases where hackers had struck they had been able to guess passwords easily—or had stolen them. There has long been talk of using biometric identifiers such as fingerprints or face-recognition technology to add an extra layer of security, but these have yet to catch on widely.

And even if they were to become more widespread, they would not protect firms from rogue staff. As Mr Snowden has shown, insiders bent on leaking sensitive data can cause huge damage. This can involve large sums of money. A study by researchers at Carnegie Mellon University of 103 cases of intellectual-property theft by corporate insiders in America between 2001 and 2013 found that almost half involved losses of more than $1m. Many were in the IT and financial-services industries (see chart 3). Insiders sometimes turn to this kind of crime after becoming disgruntled with an employer. "An insider threat is a thousand times worse than a hacker threat because it is so hard to defend against," says Chris Hadnagy, a security expert.

Technology can help. Darktrace, a British startup, is one of several firms touting continuous network monitoring software. This uses complex algorithms and mathematical models to map what normal daily behaviour on a network looks like and then flags up anomalies, such as a computer that suddenly starts downloading unusually large data files. The technology can also help spot hackers at work inside a system. Andrew France, Darktrace's boss, says firms need "immune systems" that can automatically react to any intrusion.

This is becoming even more important as skilled hackers are getting better at covering their tracks. In the APT cases Mandiant was asked to work on last year, the security firm found that the median time hackers were able to operate inside systems before being discovered was 229 days. The known record was held by a group of digital ninjas who dodged detection for over six

years. And these numbers cover only cases in which intruders were eventually spotted, so the real damage done may be much worse than they suggest.

To catch hackers early and create defences to keep them out, some companies are systematically studying the habits of highly organised groups. "You need to try and get ahead of threats, not just react to them," says Phil Venables, the chief information-security officer (CISO) of Goldman Sachs, a big American investment bank. Goldman has built a threat-management centre staffed by ex-spooks who scan cyberspace for anything that could pose a risk to the bank and then tweak its defences accordingly.

Facebook, a prime target for hackers and spammers, has built ThreatData, a computer system that sucks in vast amounts of information about threats from a wide range of sources, including lists of malicious websites. Details of these sites are automatically fed into a blacklist used to protect Facebook.com and the firm's corporate network. Joe Sullivan, the social network's CISO, says threats are now changing so fast that an instant response is essential.

If precautions have failed, it is still worth trying to zap a threat at an early stage. After the Target debacle a group of retailers including Nike, Gap and Target itself set up an Information Sharing and Analysis Centre, or ISAC, with an operations centre that will share information about cyberthreats among its members.

Big banks in America have been doing this for some time; indeed, the retailers' ISAC is modelled after the financial-services version, FS-ISAC, which was set up in 1999. The finance group now has 4,700 members and in recent years has helped co-ordinate banks' defences against massive DDOS attacks. Bill Nelson, who heads it, says it is spending $4.5m on building a platform that will allow banks using it to adapt their defences almost instantly to intelligence about new threats.

The British government has taken this idea even further. James Quinault, the head of the Office of Cyber Security and Information Assurance, which leads the government's strategic thinking on cyber-security issues, says it has created an electronic platform, or "social network for defenders", that lets its 450-plus members share threat information. The group includes companies from a wide range of industries including defence, financial services, energy and pharmaceuticals. The idea is to make it as diverse as possible so data about threats travel fast across the country's industrial base. The network also has a group of spooks and industry experts who spot intelligence that could be useful to firms in other sectors and pass it on, having first obtained permission.

Sharing information is extremely helpful, but some large companies are now assuming that truly determined hackers cannot be kept out. So they are putting more emphasis on building resilience—the ability to bounce back fast in the event of a breach. It is essential to have a well-conceived recovery plan and to test it regularly, says Ed Powers of Deloitte, a consulting firm. In financial services, where a problem at one company could easily trigger a system-wide crisis, regulators are urging banks and other firms to consider resilience across markets.

A war game run last July by America's securities industry, Quantum Dawn 2, simulated a widespread attack by hackers intent on stealing large amounts of money and disrupting the stockmarket. As part of the game, the assailants corrupted the source code of a popular equities software program, hacked a system that let them issue fraudulent press releases and mounted DDOS attacks on government networks. Among the lessons learnt from the exercise was that business and tech people need

Crashing the system

How to protect critical infrastructure from cyber-attacks

IN THE HIGH desert some 50 miles west of Idaho Falls, the terrain is so rugged that the vehicle in which your correspondent was touring the facilities at Idaho National Laboratory (INL) ended up with two shredded tyres. Originally set up in the 1940s to test naval artillery, the high-security government lab now worries about weapons of a different kind. Some of its elite engineers help protect power grids, telecoms networks and other critical infrastructure in America against cyber-attacks and other threats.

The lab boasts its own 61-mile (98km) electrical grid and seven substations. It also has a wireless network and an explosives test bed. These can all be used by government agencies and businesses to run experiments that would be hard or impossible to conduct in an operational setting. "There are not many places in the world where you can crash a power system without incident," says Ron Fisher, who oversees the Department of Homeland Security's programme office at the lab.

The tour covers the site of a 2006 experiment that subsequently got a lot of attention. Known as the Aurora test, it demonstrated how it was possible to launch a cyber-attack on a big diesel generator by exploiting a weakness in a supervisory control and data acquisition (SCADA) system. Such systems are used to monitor and control physical equipment in everything from power stations to water-treatment plants. In a video of the attack on YouTube, bits can be seen flying off the generator, followed by black smoke.

Teams from the INL and other engineers have since been advising utilities on how to secure SCADA systems. Many of these were designed to work in obscurity on closed networks, so have only lightweight security defences. But utilities and other companies have been hooking them up to the web in order to improve efficiency. This has made them visible to search engines such as SHODAN, which trawls the internet looking for devices that have been connected to it. SHODAN was designed for security researchers, but a malicious hacker could use it to find a target.

The worry is that a terrorist may break into a control system and use it to bring down a power grid or damage an oil pipeline. This is much harder to do than it sounds, which explains why so far America has seen no power outages triggered by a cyber-attack. Squirrels and fallen branches have done more damage.

Nevertheless, the case of Stuxnet shows what is possible. In 2010 the malicious code was used to attack the system that controlled centrifuges for enriching uranium at Iran's nuclear facility in Natanz, causing them to spin out of control. To pull this off, however, the masterminds behind Stuxnet had to find a way to smuggle the code into the facility, possibly on a USB stick, because the system had been kept isolated from the internet.

As more control systems are connected to the web, more vulnerabilities will inevitably appear. Already security researchers are discovering flaws in things such as communications protocols that govern the flow of data between utilities' SCADA systems and the remote substations they control. Hence talk about defence-in-depth strategies, which ensure that vital areas are covered by a number of back-up systems. Multiple bulwarks greatly increase the cost of security, but that may be a price the companies have to pay.

to work more closely together, and that they need to get better at judging whether an attack could spark a systemic crisis.

Such exercises are helpful to improve cyber-defences, but not nearly as helpful as a much simpler remedy: to put in place a set of basic precautions. The Australian Signals Directorate, the equivalent of Britain's Government Communications Headquarters (GCHQ), says that at least 85% of targeted breaches it sees could be prevented by just four measures: whitelisting software applications; regularly patching widely used software such as PDF viewers, web browsers and Microsoft Office; doing the same for operating systems; and restricting administrator privileges (granting control over a system) to those who really need them to do their job. So why do companies so often fail to adopt them? Economics provides some of the answers. ■

Market failures

Not my problem

Providing incentives for good behaviour

HEATHER ADKINS, GOOGLE'S security chief, has what she calls a "monthly patch day", when she updates the software running on all of the electronic devices in her home. If everybody were like Ms Adkins, cyber-security would be much less of a problem. But even with the best of intentions, people forget to update software, install antivirus programs and so on.

The problem is that by weakening their own defences, they do not just make themselves more vulnerable to being hacked; they may also cause harm to other web users by making it possible, say, for an intruder surreptitiously to take over their device and use it to attack other computers. The same holds true in the corporate world. Target spent a fortune each year on cyber-security, but was attacked via a heating and air-conditioning supplier whose defences were apparently not robust enough to keep hackers out.

Companies are often reluctant to admit that they have been hacked. This may make sense for them because disclosure could lay them open to litigation and put their customers off doing business with them, but it increases the risk that other companies which could have learned from their experience will be attacked in the same way. All these are examples of what economists call negative externalities, which come about when individuals or firms do not incur the full cost of their decisions.

There is a market failure in cyber-security, made worse by the trouble firms have in getting reliable information about the threats they face

Another reason for slip-ups is the way computer code is produced. Companies that make software have an incentive to ship it as fast as they can to get ahead of their rivals, and then patch any flaws as and when they are discovered. But fixes are not always delivered swiftly, which means customers' systems are left vulnerable to hackers.

Such cases suggest that there is a market failure in cyber-security. Solutions being suggested or tried include increasing transparency about data losses; helping consumers and firms to make more informed decisions about cyber-security; shedding more light on how internet-service providers (ISPs) tackle malware infections they spot on customers' computers; and using liability laws to force software companies to produce safer code.

On transparency, America has led the way. Almost all American states now have data-breach laws that require firms to reveal any loss of sensitive customer information. In Europe telecoms firms have been obliged to notify customers of breaches for some time now, and there are plans to extend reporting to a wider range of industries. A draft European Union directive approved by the European Parliament would require firms in other critical-infrastructure industries, such as power companies, to report breaches to the authorities.

The sky is the limit

Breach laws have encouraged insurance companies to offer coverage against potential losses. This is helpful because they are in a position to gather and share information about best practices across a wide range of companies. Mike Donovan of Beazley, a cyber-insurer, says that his firm advises companies on defensive tactics, but also on how to minimise the damage if something goes wrong.

Tyler Moore of Southern Methodist University suggests that the American government should create a cyber-equivalent of the National Transportation Safety Board, which investigates serious accidents and shares information about them. He says such a body could look into all breaches that cost over, say, $50m and make sure the lessons are shared widely.

But insurers are likely to remain wary of taking on broader risks because the costs associated with a serious cyber-incident could be astronomic. "Insurers can deal with acts of God, but not acts of Anonymous or acts of Iran," says Allan Friedman, a cyber-security researcher at George Washington University. This explains why the overall cyber-insurance market is still small: one recent estimate puts it at $2 billion.

Governments are weighing in, too, not least by supporting private-sector efforts to clean up "botnets", or networks of compromised computers controlled by hackers. These networks, which are prevalent in countries such as America and China (see chart 4, next page), can be used to launch DDOS attacks and spread malware. In Germany an initiative called Bot-Frei, which helps people clean up their infected computers, received government support to get started, though it is now self-financing. The American government has also worked closely with private firms such as Microsoft to bring down large botnets.

Another strategy involves issuing standards to encourage improved security. In February America's National Institute of Standards and Technology published a set of voluntary guidelines for companies in critical-infrastructure sectors such as energy and transport. And last month Britain launched a scheme called "cyber-essentials" under which firms can apply for a certificate showing they comply with certain minimum security standards. Applicants undergo an external audit and, if successful, are awarded a badge which they can use on marketing materials. Whether governments are best placed to set minimum standards is debatable, but they have certainly raised awareness of cyber-security as an issue that needs attention.

They could also help to get more information into the pub-

lic domain. Mr Moore, Ross Anderson, a professor of security engineering at Cambridge University, and other researchers have argued persuasively that collecting and publishing data about the quantity of spam and other bad traffic handled by ISPs could encourage the worst performers to do more to tackle the problem, thus improving overall security.

Another debate has revolved around getting software companies to produce code with fewer flaws in it. One idea is to make them liable for damage caused when, say, hackers exploit a weakness in a software program. Most software companies currently insist customers accept end-user licensing agreements that specifically protect firms from legal claims unless local laws prohibit such exclusions.

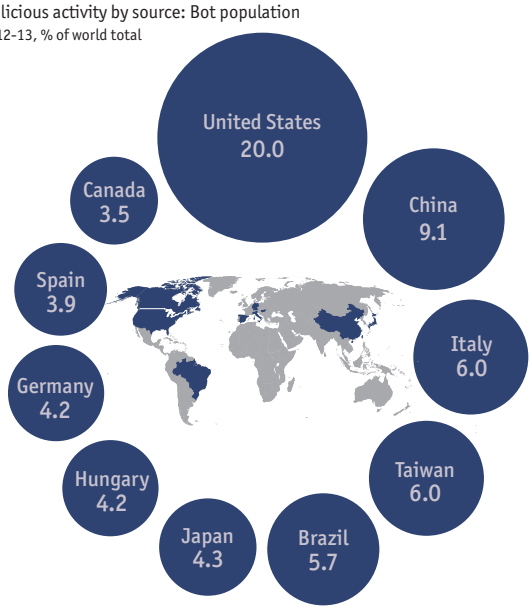
The snag is that imposing blanket liability could have a chilling effect on innovation. "Companies that are selling millions of copies of programs might take fright at the potential exposure and leave the business," cautions Brad Templeton of the Electronic Frontier Foundation, a consumer-rights group. Paul Rosenzweig of Red Branch Consulting suggests that strict liability be applied only to firms which produce software that cannot be patched if a security flaw is found. There is quite a lot of that sort of code around.

Mr Anderson reckons that the software industry is bound to come under pressure to produce more secure code, just as in the 1970s the car industry was forced to improve the safety of vehicles after campaigns mounted by consumer activists such as Ralph Nader. This process could take time, but the move to link all kinds of household devices to the internet is likely to be a watershed moment.

Europe already has laws requiring device manufacturers to certify that their products are safe for use. Mr Anderson thinks that, as part of this process, firms should also be required to self-certify that the software in them is designed to be secure and can be patched swiftly if a flaw is found. "You want to be sure that your connected TV cannot be recruited into a botnet," he says. There are already signs that hackers are finding ways to exploit devices around the home. ■

Danger spots 4

Malicious activity by source: Bot population
2012-13, % of world total



Source: Symantec

The internet of things

Home, hacked home

The perils of connected devices

ONE NIGHT IN April a couple in Ohio was woken by the sound of a man shouting, "Wake up, baby!" When the husband went to investigate, he found the noise was coming from a web-connected camera they had set up to monitor their young daughter while she slept. As he entered her bedroom, the camera rotated to face him and a string of obscenities poured forth.

The webcam was made by a company called Foscam, and last year a family in Houston had a similar experience with one of their products. After that episode, Foscam urged users to upgrade the software on their devices and to make sure they had changed the factory-issued password. The couple in Ohio had not done so. The problem arose even though Foscam had taken all the right steps in response to the initial breach, which shows how hard it is to protect devices hooked up to the internet.

There will soon be a great many more of them. Cisco, a tech company, reckons that by the end of this decade there could be some 50 billion things with web connections (see chart 5, next page). Among them will be lots of consumer gear, from cameras to cars, fridges and televisions.

Smart or foolish?

This new network is already turning out to be very useful. Smart cars are able to read e-mails and text messages to drivers on the move; smart fridges carefully manage the energy they use; smart medical devices allow doctors to monitor patients from afar; and smart screens in the home display all kinds of useful information. Entire cities in South Korea are already rushing to link their infrastructure to the web to make it more efficient and improve services.

But security experts are sounding the alarm. "There is a big difference between the internet of things and other security issues," says Joshua Corman of I Am The Cavalry, a group of security specialists trying to promote greater awareness of emerging risks to public safety. "If my PC is hit by a cyber-attack, it is a nuisance; if my car is attacked, it could kill me." ▸▸

This may smack of scaremongering, but researchers have already demonstrated that some vehicles are vulnerable to cyber-attacks. Modern cars are essentially a collection of computers on wheels, packed with many microcontrollers that govern their engines, brakes and so forth. Researchers such as Chris Valasek and Mathew Solnik have shown that it is possible to hack into these systems and take over a vehicle.

Their experiments, which include steering wheels suddenly being wrenched to one side and engines being switched off without warning, have caught the attention of carmakers. The techniques used to hack the vehicles' controls are sophisticated, and many require physical access to the engine, so for the moment this is unlikely to happen to your car. But technology moves fast: at an event in Singapore earlier this year two researchers showed off a car-hacking tool the size of a smartphone that cost less than $25 to build.

Some medical devices, including several types of insulin pump, have also been hacked in public demonstrations. Jay Radcliffe, a security researcher who happens to be diabetic, made headlines a few years ago when he discovered that his computerised insulin pump could be attacked by remotely entering the wireless-communications system that controlled it. A malicious hacker could have changed the amount of insulin being administered. In a recent blog post, Mr Radcliffe gave warning that emerging medical technology is often ill-equipped to deal with threats arising in an interconnected world.

Other researchers agree. "There are just super simple flaws in some medical devices," says Billy Rios of Qualys, a cyber-security firm. Last year he and a colleague found "back doors" into various bits of medical equipment. These are passwords used by technicians from firms that sell the devices to update the software that runs them. A hacker with a back door could use it to, say, adjust an x-ray machine so that it administers a far higher dosage than its display shows. Mr Rios took his findings to regulators and worked with them and with the companies involved to fix the flaws.

It all sounds rather worrying, but so far there has been no known case of a cyber-attack in which a car has been forced off the road or a medical device misappropriated. Mr Rios accepts that some people think his research is designed to drum up sales for the cyber-security industry, but he insists that the risks are real.

Many items, including mundane things like light bulbs and door locks, are being hooked up to the internet by putting tiny computers into them and adding wireless connectivity. The problem is that these computers do not have enough processing power to handle antivirus and other defences found on a PC. The margins on them are wafer-thin, so manufacturers have little scope for spending on security. And the systems are being produced in vast quantities, so hackers finding a flaw in one will be able to get into many others too.

This is already happening with some home wireless routers. Earlier this year Team Cymru, an American cyber-security firm, found a network of 300,000 compromised routers in various countries, including America, India, Italy and Vietnam. In 2012 crooks in Brazil took control of 4.5m routers, using the stolen information to plunder a large number of bank accounts.

Watch that fridge

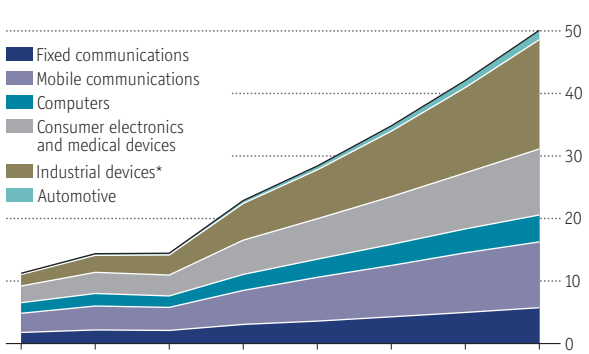
A lot more devices with little computers inside them will end up in people's homes, often connected to one another via home-automation systems. That will make them tempting targets for cyber-attackers. In January Proofpoint, a security firm, claimed it had found evidence that a group of compromised devices, including home routers, televisions and a refrigerator, had been commandeered by hackers and were being used to pump out spam. That is annoying enough, but what if a tech-savvy arsonist were to find a way of, say, taking control of home boilers and turn them up so much that they burst into flames? Mr Rios has already found tens of thousands of corporate heating, air-conditioning and ventilation systems online, many with vulnerabilities in their software that a hacker could exploit.

Some companies are now trying to build security into their products from the start. Broadcom, a chipmaker, recently unveiled a microchip specially designed for web-connected devices that has encryption capabilities baked into it, and Cisco has launched a competition offering prizes for the best ideas for securing the internet of things. But many firms plunging into this market are small startups which may not have much experience of cyber-security.

Mr Corman worries that it may take a catastrophic event to get makers to focus on the need for better security in connected devices. But optimists believe that pressure from customers will be enough to force their hand. ■

The 50 billion question 5

Worldwide number of internet-connected devices, forecast, bn



Source: Cisco

*Includes military and aerospace

Remedies

Prevention is better than cure

More vigilance and better defences can make cyberspace a lot safer

CYBERSPACE WILL NEVER be completely secure. The threats posed by what Sir David Omand, an academic and former head of Britain's GCHQ intelligence agency, calls "the cesspit of modernity"—online crime, espionage, sabotage and subversion—are not going to disappear. Nor is the temptation for governments to treat the internet as a new combat zone, alongside land, sea, air and space.

In 1996 John Perry Barlow, a cyber-libertarian, issued a "Declaration of the Independence of Cyberspace" addressed to governments, insisting: "You have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear." He turned out to be wrong. Governments have shown in a variety of ways—from the theft of industrial secrets by Chinese spies to the mass surveillance conducted by Western ones—that they are determined to make cyberspace their own.

Political leaders are fond of saying that they want their citizens to benefit from the huge opportunities that a secure and reliable internet can offer, and that they are determined to protect them from crime and terrorism online. Yet they do not hesitate to use the web for their own purposes, be it by exploiting vulnerabilities in software or launching cyber-weapons such as Stuxnet, without worrying too much about the collateral damage done to companies and individuals. Some of the trends pinpointed in this special report, including the rise of organised crime on the internet and the imminent arrival of the internet of things, will only increase concerns about a widening security gap.

A plain man's guide

So what can be done? The first thing is to change the tone of the debate about cyber-security, which is typically peppered with military metaphors. These tend to suggest that companies and individuals are powerless to help themselves, giving governments latitude to infringe their citizens' privacy. "The internet is the most transformative innovation since Gutenberg and the printing press," says Jason Healey of the Atlantic Council, an American think-tank. "Yet we're treating it as a war zone."

Bruce Schneier, a security expert, has suggested that crime-fighting is a better analogy than warfare. This is a useful idea. Police are needed to go after criminals, but people can help prevent crimes in the first place by taking sensible precautions. And although extraordinary powers of investigation and arrest are sometimes needed to apprehend wrongdoers, they are subject to robust legal protections for citizens.

Applied to cyberspace, this means that, far from being powerless against hackers, companies can do a lot to help themselves. Simply ensuring that only approved programs can run on their systems, regularly patching all software, educating employees about cyber-risks and constantly monitoring networks would help keep most intruders out. Yet too many companies fail to do these things, or do them consistently.

Tackling cybercrime often requires international co-operation. In recent years this has been getting better, partly thanks to agreements such as the Council of Europe's Convention on Cybercrime, whose members assist each other in international investigations. More resources for crime-fighting outfits, including teams on secondment from the private sector, would clear out more crooks.

That still leaves the job of dealing with the most sophisticated hackers, whose motives often have nothing to do with money. Getting broader agreement on norms of behaviour in cyberspace is crucial, but it will not be easy. Forging a consensus on what bits of critical infrastructure should be off-limits to a cyber-attack would be an excellent start.

Making sure that fewer bugs crop up in software in the first place would also be helpful, particularly as the internet of things is about to take off and opportunities for breaches will multiply manifold. The best method would be for companies to come up with robust proposals of their own for securing the new connected devices. In March a group of firms including Cisco, IBM and GE set up the Industrial Internet Consortium, which among other things will look at innovative approaches to security in web-connected industrial gear. Something similar is needed in the consumer field.

Far from being powerless against hackers, companies can do a lot to help themselves

The internet has turned out to be one of the biggest forces for progress in the history of mankind. Having started life as a gathering place for a small bunch of geeks and academics in the early 1970s, it is now at the heart of the global economy. Mr Gibson's "consensual hallucination" has become a worldwide success story. It must be kept in good working order. ■

Offer to readers

Reprints of this special report are available. A minimum order of five copies is required. Please contact: Jill Kaletha at Foster Printing
Tel +00(1) 219 879 9144
e-mail: jillk@fosterprinting.com

Corporate offer

Corporate orders of 100 copies or more are available. We also offer a customisation service. Please contact us to discuss your requirements.
Tel +44 (0)20 7576 8148
e-mail: rights@economist.com

For more information on how to order special reports, reprints or any copyright queries you may have, please contact:

The Rights and Syndication Department
20 Cabot Square
London E14 4QW
Tel +44 (0)20 7576 8148
Fax +44 (0)20 7576 8492
e-mail: rights@economist.com
www.economist.com/rights

Future special reports

Advertising and technology September 13th
The world economy October 4th
Iran October 25th
The Pacific Rim November 15th

Previous special reports and a list of forthcoming ones can be found online: **economist.com/specialreports**