Economist.com OPINION

Digital security

How to worry wisely

Oct 24th 2002
From The Economist print edition

Securing computer systems is important, but not for the reasons you might think

VIRUSES that spread by e-mail. Hackers who deface websites. Theft of credit-card details and customer lists. Follow the subject of computer security too closely, and you might be forgiven for never wanting to touch a keyboard again. Industry experts, government officials and technology firms issue endless alerts, fixes and guidelines, call for more spending on security, and even give dark warnings of cyber-terrorists poised to wreak havoc with a few clicks of a mouse. Just this week, mysterious online attackers tried to paralyse the Internet by flooding crucial "root server" computers with bogus traffic. Something must be done, and quickly.

Oh, really? Most people who use computers have probably experienced nothing more sinister than an occasional virus. Typing your credit-card number into a web page, once considered an act of near insanity, has become routine. Has the website of the company you work for been defaced recently? No, we didn't think so. Attacks similar to the one that occurred this week happen quite often, and nobody notices.

The truth, of course, lies somewhere between these two extremes, as our survey on the subject argues in this week's issue. Those in the security industry, like environmentalists, have an incentive to overstate the risks; meanwhile, to the untrained eye at least, nothing much seems to be wrong. So, is the subject of digital security cause for more widespread concern? It is—but not for the reasons that you might think.

It is tempting, for example, to dismiss the sudden emphasis being placed on digital security as a knee-jerk reaction to last year's terrorist attacks. But it is actually part of a much longer-term trend, as the Internet struggles to transform itself from a toy to a grown-up utility, as reliable as gas, water or electricity. There is clearly a long way still to go. As people become increasingly reliant on computers and networks, however, in both their personal and business lives, it becomes more important to make them secure. As for cyberterrorism, it is possible, but unlikely: truck bombs and hoax telephone calls can cause more disruption, far more cheaply and visibly. The security of the Internet needs to be improved, then, but for rather more mundane reasons than the cyber-Cassandras suggest.

The security problems that most people are aware of, and that they are most likely to worry about, are attacks by malicious hackers and viruses. These threats are certainly worth worrying about—a bit. But the reality for most organisations is that attacks by insiders, and the theft of intellectual property by disgruntled employees in particular, do much more damage. Hackers and viruses get disproportionate attention because they can be highly visible, and because there are lots of vendors offering apparently simple fixes. Insider attacks are usually hushed up, and are harder to detect and prevent. Putting the right policies and processes in place to improve internal security is mainly a management problem, not a technical one. So again, there is cause for concern, but the nature of the problem and the solution are widely misunderstood.

Have a coffee instead

So is the answer for everyone to start spending huge sums on security technology and training? Not necessarily. Most companies, according to a popular industry statistic, spend more on coffee than on digital security. Yet the real problem may be that the spending is in the wrong places. Security involves balancing costs and risks, and only a proper risk assessment can determine which assets are worth protecting, given the cost of doing so. Such decisions should fall not to the specialists in the systems department, but to senior executives. They need to pay more attention, though not necessarily more money.

It would be no bad thing if people worried a bit more about digital security. As long as they worry about the right things.

Economist.com

RESEARCH TOOLS
SURVEYS

Securing the cloud

Oct 24th 2002
From The Economist print edition

Digital security, once the province of geeks, is now everyone's concern. But there is much more to the problem—or the solution—than mere technology, says Tom Standage

WHEN the world's richest man decides it is time for his company to change direction, it is worth asking why. Only rarely does Bill Gates send an e-mail memo to the thousands of employees at Microsoft, the world's largest software company, of which he is chairman. He famously sent such a memo in December 1995, in which he announced that Microsoft had to become “hardcore” about the Internet. In January this year Mr Gates sent another round-robin. Its subject? The importance of computer security.

Until recently, most people were either unaware of computer security or regarded it as unimportant. That used to be broadly true, except in a few specialised areas—such as banking, aerospace and military applications—that rely on computers and networks being hard to break into and not going wrong. But now consumers, companies and governments around the world are sitting up and taking notice. Why?

The obvious answer seems to be that last year's terrorist attacks in America have heightened awareness of security in all its forms. But the deeper reason is that a long-term cultural shift is under way. Digital security has been growing in importance for years as more and more aspects of business and personal life have come to depend on computers. Computing, in short, is in the midst of a transition from an optional tool to a ubiquitous utility. And people expect utilities to be reliable. One definition of a utility, indeed, is a service that is so reliable that people notice it only when it does not work. Telephone service (on fixed lines, at least), electricity, gas and water supplies all meet this definition. Computing clearly does not, at least not yet.

One of the many prerequisites for computing to become a utility is adequate security. It is dangerous to entrust your company, your personal information or indeed your life to a system that is full of security holes. As a result, the problem of securing computers and networks, which used to matter only to a handful of system administrators, has become of far more widespread concern.

Computers are increasingly relied upon; they are also increasingly connected to each other, thanks to the Internet. Linking millions of computers together in a single, cloud-like global network brings great benefits of cost and convenience. Dotcoms may have come and gone, but e-mail has become a vital business tool for many people and an important social tool for an even larger group. Being able to access your e-mail from any web browser on earth is tremendously useful and liberating, as both business travellers and backpacking tourists will attest. Corporate billing, payroll and inventory-tracking systems are delivered as services accessible through web browsers. Online shop fronts make it fast and convenient to buy products from the other side of the world.

The price of openness

The flip side of easy connectivity and remote access, however, is the heightened risk of a security breach. Bruce Schneier, a security expert, points out that when you open a shop on the street, both customers and shoplifters can enter. "You can't have one without the other," he says. "It's the same on the Internet." And as music, movies, tax returns, photographs and phone calls now routinely whizz around in digital form, the shift from traditional to digital formats has reached a critical point, says Whitfield Diffie, a security guru at Sun Microsystems: "We can no longer continue this migration without basic security."

The September 11th attacks, then, reinforced an existing trend. Government officials, led by Richard Clarke, America's cyber-security tsar, gave warning of the possibility that terrorists might mount an "electronic Pearl Harbour" attack, breaking into the systems that control critical telecommunications, electricity and utility infrastructure, and paralysing America from afar with a few clicks of a mouse. Most security experts are sceptical, but after spending years trying to get people to take security seriously, they are willing to play along. Scott Charney, a former chief of computer crime at the Department of Justice and now Microsoft's chief security strategist, says Mr Clarke's scare-mongering is "not always helpful, but he has raised awareness."

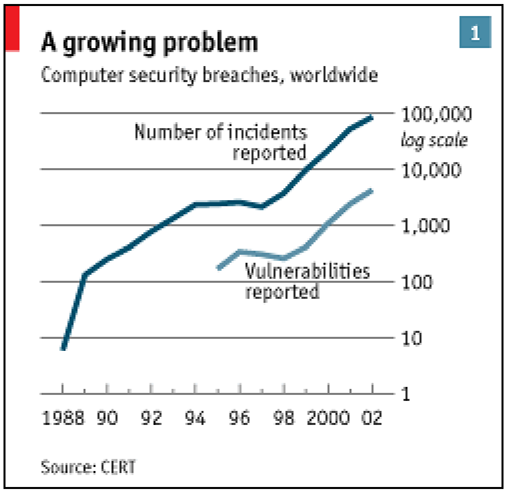
The terrorist attacks certainly prompted companies to acknowledge their dependence on (and the vulnerability of) their networks, and emphasised the importance of disaster-recovery and back-up systems. A survey of information-technology managers and chief information officers, carried out by Morgan Stanley after the attacks, found that security software had jumped from fifth priority or lower to become their first priority. "It's moved up to the top of the list," says Tony Scott, chief technology officer at General Motors. "It's on everybody's radar now."

The growing emphasis on security over the past year or two has been driven by a combination of factors, and has shown up in a variety of ways. Chris Byrnes, an analyst at Meta Group, a consultancy, notes that the proportion of his firm's clients (mostly large multinational companies) with dedicated computer-security teams has risen from 20% to 40% in the past two years. He expects the figure to reach 60-70% within the next two years. Previously, he says, it was financial-services firms that were most serious about security, but now firms in manufacturing, retailing and other areas are following suit.

One important factor is regulation. Mr Byrnes points to the change made to American audit standards in 1999, requiring companies to ensure that information used to prepare public accounts is adequately secured. This has been widely interpreted, with the backing of the White House's critical-infrastructure assurance office, to mean that a company's entire network must be secure.

Similarly, the April 2003 deadline for protecting patients' medical information under the Health Insurance Portability and Accountability Act (HIPAA) has prompted health-care providers, pharmaceutical companies and insurers to re-evaluate and overhaul the security of their computers and networks. In one recent case, Eli Lilly, a drug maker, was accused of violating its own online privacy policy after it accidentally revealed the e-mail addresses of 669 patients who were taking Prozac, an anti-depressant. The company settled out of court with America's Federal Trade Commission and agreed to improve its security procedures. But once HIPAA's privacy regulations come into force, companies that fail to meet regulatory standards will face stiff financial penalties. The same sort of thing is happening in financial services, where security is being beefed up prior to the introduction of the Basel II bank-capital regulations.

The growth of high-profile security breaches has also underlined the need to improve security. The number of incidents reported to Carnegie Mellon's computer emergency response team (CERT), including virus outbreaks and unauthorised system intrusions, has shot up in recent years (see chart 1) as the Internet has grown. The "Love Bug", a virus that spreads by e-mailing copies of itself to everyone in an infected computer's address book, was front-page news when it struck in May 2000. Many companies, and even Britain's Parliament, shut down their mail servers to prevent it from spreading.


A growing problem

Computer security breaches, worldwide

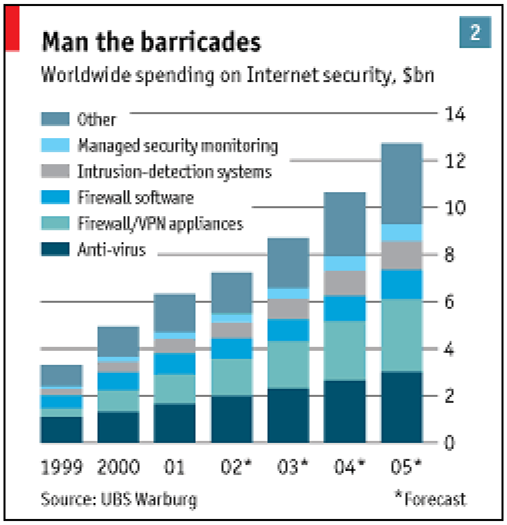
Source: CERT

There have been a number of increasingly potent viruses since then, including Sircam, Code Red and Nimda, all of which affected hundreds of thousands of machines. The latest, called Bugbear, struck only this month. Viruses are merely one of the more visible kinds of security problem, but given the disruption they can cause, and the widespread media coverage they generate, such outbreaks prompt people to take security more seriously.

Fear, sex and coffee

Spending on security technology grew by 28% in 2001 compared with the year before, according to Jordan Klein, an analyst at UBS Warburg. Mr Klein predicts that spending will continue to grow strongly over the next few years, from around $6 billion in 2001 to $13 billion in 2005 (see chart 2). A survey carried out by Meta Group in August found that although only 24% of firms had increased their technology budgets in 2002, 73% had increased their spending on security, so security spending is growing at the expense of other technology spending. This makes it a rare bright spot amid the gloom in the technology industry.

Steven Hofmeyr of Company 51, a security start-up based in Silicon Valley, says his company is pushing at a wide-open door: there is no need to convince anyone of the need for security technology. Indeed, Nick Sturiale of Sevin Rosen, a venture-capital fund, suggests that security is already an overcrowded and overfunded sector. “Security is now the Pavlovian word that draws the drool from VCs' mouths,” he says. Security vendors are really selling fear, he says, and fear and sex are “the two great sales pitches that make people buy irrationally”.



Man the barricades

Worldwide spending on Internet security, $bn

Source: UBS Warburg

*Forecast

So, a bonanza for security-technology firms? Not necessarily. The sudden interest in security does not always translate into support from senior management and larger budgets. A recent report from Vista Research, a consultancy, predicts that: “While the need to protect digital assets is well established, companies will pay lip service to the need to invest in this area and then largely drag their feet when it comes to capital spending on security.”

Even where security spending is increasing, it is from a very low base. Meta Group's survey found that most companies spend less than 3% of their technology budgets on security. Technology budgets, in turn, are typically set at around 3% of revenues. Since 3% of 3% is 0.09%, most firms spend more on coffee than on computer security, according to a popular industry statistic. The purse strings loosen only when companies suffer a serious security breach themselves, see one of their rivals come under attack or are told by auditors that lax security could mean they are compromising due diligence.

Jobs on plates

Mr Byrnes notes another factor that is impeding growth of the security market: a shortage of senior specialists. For much of the past year, he says, “There was more security budget than ability to spend it.” John Schwarz, president of Symantec, a security firm, puts the number of unfilled security jobs at 75,000 in America alone. As a result, the security boom widely expected last year has yet to materialise. But Mr Hofmeyr reckons that the increase in security spending is just starting to kick in.

Given the new interest in security, established technology firms, which have seen revenues plunge as firms slash technology spending in other areas, are understandably keen to jump on the bandwagon alongside specialist security vendors. Sun's advertisements boast: “We make the net secure.” Oracle, the world's second-largest software firm, has launched a high-profile campaign trumpeting (to guffaws from security experts) that its database software is “unbreakable”. Whether or not this is true, Oracle clearly regards security as a convenient stick with which to bash its larger arch-rival, Microsoft, whose products are notoriously insecure—hence Mr Gates's memo.

It suits vendors to present security as a technological problem that can be easily fixed with more technology—preferably theirs. But expecting fancy technology alone to solve the problem is just one of three dangerous misconceptions about digital security. Improving security means implementing appropriate policies, removing perverse incentives and managing risks, not just buying clever hardware and software. There are no quick fixes. This survey will argue that digital security depends as much—if not more—on human cultural factors as it does on technology. Implementing security is a management as well as a technical problem. Technology is necessary, but not sufficient.

A second, related misperception is that security can be left to the specialists in the systems department. It cannot. It requires the co-operation and support of senior management. Deciding which assets need the most protection, and determining the appropriate balance between cost and risk, are strategic decisions that only senior management should make. Furthermore, security almost inevitably involves inconvenience. Without a clear signal from upstairs, users will tend to regard security measures as nuisances that prevent them from doing their jobs, and find ways to get around them.

Unfortunately, says Mr Charney, senior executives often find computer security too complex. "Fire they understand," he says, because they have direct personal experience of it and know that you have to buy insurance and install sensors and sprinklers. Computer security is different. Senior executives do not understand the threats or the technologies. "It seems magical to them," says Mr Charney. Worse, it's a moving target, making budgeting difficult.

A third common misperception concerns the nature of the threat. Even senior managers who are aware of the problem tend to worry about the wrong things, such as virus outbreaks and malicious hackers. They overlook the bigger problems associated with internal security, disgruntled ex-employees, network links to supposedly trustworthy customers and suppliers, theft of laptop or handheld computers and insecure wireless access points set up by employees. That is not surprising: viruses and hackers tend to get a lot of publicity, whereas internal security breaches are hushed up and the threats associated with new technologies are often overlooked. But it sets the wrong priorities.

Detective stories

A final, minor, misperception is that computer security is terribly boring. In fact, it turns out to be one of the more interesting aspects of the technology industry. The war stories told by security consultants and computer-crime specialists are far more riveting than discussion of the pros and cons of customer-relationship management systems. So there really is no excuse for avoiding the subject.

Anyone who has not done so already should take an interest in computer security. Unfortunately there is no single right answer to the problem. What is appropriate for a bank, for example, would be overkill for a small company. Technology is merely part of the answer, but it has an important role to play, so that is where this survey will start.

Economist.com RESEARCH TOOLS SURVEYS

Tools of the trade

Oct 24th 2002
From The Economist print edition

How a box of technological tricks can improve (but not guarantee) your security

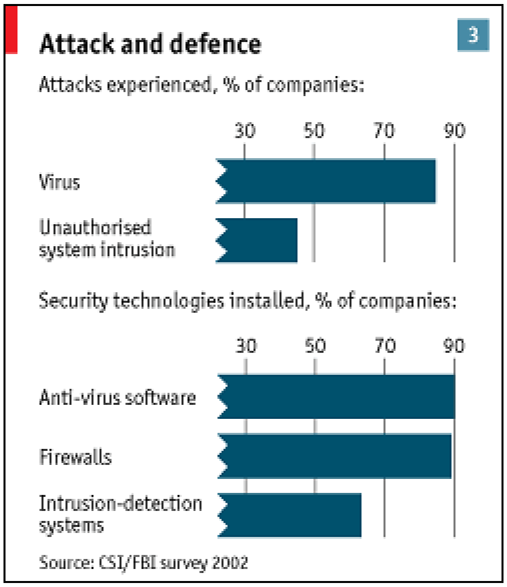
ASK a non-specialist about computer security, and he will probably mention viruses and attacks by malicious hackers, if only because they are so much more visible than other security problems. Take viruses first. Like their biological counterparts, computer viruses are nasty strings of code that exploit their hosts to replicate themselves and cause trouble. Until a few years ago, viruses merely infected files on a single computer. Eventually, an infected file would be moved, typically on a floppy disk, to another machine where the virus could spread. Modern viruses, however, are far more insidious, because they can jump from one computer to another across the Internet, most often by e-mail. (Since self-propagating programs are technically known as worms, such viruses are sometimes called worm-virus hybrids.)

Recent high-profile examples include Sircam, which struck in July 2001 and generated much comment because as well as e-mailing copies of itself to everyone in an infected PC's address book, like previous viruses, it also enclosed random documents from the infected machine's hard disk with each message. Users thus unwittingly sent half-finished screenplays, unsent letters and private diary jottings to their friends, sometimes with embarrassing results. Code Red, which also struck that month, was a worm that exploited a security vulnerability in Microsoft's web-server software to spread from one server to another. Infected servers were programmed to flood the White House website with traffic for a week.

Patching it up

The weakness that Code Red exploited had been discovered in June, and Microsoft had issued a software "patch" to correct it. But software patches are issued all the time, and keeping up with new patches and deciding which to install is more than many system administrators can manage. Within a week of Code Red's appearance, 300,000 computers were infected with it. Sometimes it defaced infected web servers with the message "Hacked by Chinese!", which suggested a political motivation, but the identities and motives of virus writers can rarely be determined for sure. Similarly, Nimda, a particularly vigorous virus/worm which struck on September 18th 2001, was initially assumed to have some connection with the previous week's terrorist attacks, though this now seems unlikely.

Viruses are extremely widespread, which is more than can be said for meaningful statistics about them. The annual survey carried out by the Computer Security Institute (CSI) in San Francisco, in conjunction with the Federal Bureau of Investigation's local computer-intrusion squad, is generally regarded as one of the more authoritative sources of information about computer security. According to the most recent CSI/FBI report, published in April 2002, 85% of respondents (mainly large American companies and government agencies) encountered computer viruses during 2001 (see chart 3). Quantifying the damage done by viruses, however, is extremely difficult. Certainly, cutting off e-mail or Internet connections can seriously hamper a company's ability to do business. In severe cases every single computer in an office or school may need to be disinfected, which can take days.


Attack and defence

Source: CSI/FBI survey 2002

Yet assigning costs to outbreaks is guesswork at best. Computer Economics, a consultancy, puts the worldwide costs imposed by viruses in 2001 at $13.2 billion. But few outside the marketing departments of anti-virus-software vendors take such figures seriously. Critics point out that if most companies are themselves unable to quantify the cost of cleaning up viruses in their systems, it is hard to see how anyone else can. Far easier to quantify is the surge in sales of anti-virus software that follows each outbreak. Following the Code Red and Nimda strikes, for example, anti-virus sales at Symantec, a leading security-software firm, in the last quarter of 2001 were 53% up on a year earlier.

Anti-virus software works by scanning files, e-mail messages and network traffic for the distinguishing characteristics, or "signatures", of known viruses. There is no general way to distinguish a virus from a non-malicious piece of code. Both are, after all, just computer programs, and whether a particular program is malicious or not is often a matter of opinion. So it is only after a virus has infected its first victims and has started to spread that its signature can be determined by human analysts, and that other machines can be inoculated against it by having their database of signatures updated. Inevitably, the result is an arms race between the mysterious folk who write viruses (largely for fun, it seems, and to win the kudos of their peers) and makers of anti-virus software. Some viruses, including a recent one called Klez, even attempt to disable anti-virus software on machines they infect, or spread by posing as anti-virus updates.

Viruses are a nuisance, but the coverage they receive is disproportionate to the danger they pose. Some vendors of anti-virus software, particularly the smaller ones, fuel the hysteria by sending out jargon-filled warnings by e-mail at every opportunity. From a technical point of view, protecting a computer or network against viruses is tedious but relatively simple, however: it involves installing anti-virus software on individual machines and keeping it up to date. Virus-scanning software that sits on mail servers and scans e-mail messages before they are delivered can provide an extra defensive layer.

Dealing with intrusions by malicious hackers is an altogether more complex problem. (The word “hacker” merely means a clever programmer, but is commonly applied to those who use their skills to malicious ends.) Computers are such complex systems that there are endless ways for unauthorised users to attempt to gain access. Attackers very often use the same security flaws that worms and viruses exploit; such worms and viruses can be seen as an automated form of malicious hacking.

Having gained access to a machine, an attacker can deface web pages (if the machine is a web server), copy information (if the machine stores user information, financial data or other documents), use the machine as a base from which to attack other machines, or install “Trojan horse” software to provide easy access in future or to enable the machine to be remotely controlled over the Internet. Savvy attackers cover their tracks using special software known as a “root kit”, which conceals the evidence of their activities and makes unauthorised use difficult to detect.

As with viruses, meaningful figures for unauthorised intrusions are hard to find. Many attacks go unnoticed or unreported. But the CSI/FBI survey gives some flavour of the scale of the problem. Of the 503 large companies and government agencies that participated in the survey, 40% detected system intrusions during 2001, and 20% reported theft of proprietary information. Of the companies that were attacked, 70% reported vandalism of their websites. But it is dangerous to lump all attacks together. Just as there is a difference between a graffiti-spraying youth and a criminal mastermind, there is a world of difference between vandalising a web page and large-scale financial fraud or theft of intellectual property.

The principal tool for keeping unwanted intruders out of computers or networks is the firewall. As its name suggests, a firewall is a device that sits between one network (typically the Internet) and another (such as a closed corporate network), enforcing a set of rules about what can travel to and fro. For example, web pages might be allowed inside the firewall, but files might not be allowed to go outside.

Walls have ears

Firewalls are no panacea, however, and may give users a false sense of security. To be effective, they must be properly configured, and must be regularly updated as new threats and vulnerabilities are discovered. “What kind of firewall you have matters far less than how you configure it,” says Bill Murray of TruSecure, a security consultancy. There are dozens of competing firewall products on the market, but most of them come in two main forms: as software, which can be installed on a machine to regulate traffic, and as hardware, in the form of appliances that plug in between two networks and regulate the flow of traffic between them.

The leader in the field, with 40% of the market, is Check Point Software of Ramat Gan, Israel. Four years ago, says Jerry Ungerman, Check Point's president, people thought the firewall market was almost saturated, because most firms had one, but the market has continued to grow. The notion that each company simply needs one firewall, between its internal network and the Internet, is now outmoded. Companies often have many separate links to the Internet, want to wall off parts of their internal networks from each other, or choose to install firewall software on every server. Some of Check Point's clients, says Mr Ungerman, have over 1,000 firewalls installed. The advent of fixed broadband connections means that home users, who often leave their computers switched on around the clock, now need firewalls too if they are to protect their machines from intruders. Even mobile phones and hand-held computers, he predicts, will have firewalls built into them.

Firewalls have their uses, but there are many kinds of attacks they cannot prevent. An attacker may be able to bypass the firewall, or exploit a vulnerability by sending traffic that the firewall regards as legitimate. Many attacks involve sending artfully formulated requests to web servers, causing them to do things that would not normally be allowed, says Geoff Davies of i-Sec, a British security consultancy. To show how easily this can be done, he types a string of database commands into the search field of an online travel agent, and instead of a table of flight departures and arrivals, the website comes up with a table of information about its users. (Mr Davies carried out this demonstration, called an “SQL insertion” attack, on a dummy server specially set up for the purpose, but it is a widespread vulnerability on real websites.) To a firewall, such an attack may look just like a legitimate use of the web server.

Halt! Who goes there?

An alternative is the “intrusion-detection system” (IDS), which monitors patterns of behaviour on a network or an individual computer and sounds an alarm if something looks fishy. Some kinds of detection systems monitor network traffic, looking for unusual activity, such as messages passing to and from a Trojan horse on the network; others sit on computers, looking for unusual patterns of access, such as attempts to retrieve password files.

Compared with anti-virus software and firewalls, detection is a relatively immature technology, and many people believe it is more trouble than it is worth. The difficulty is tuning an IDS correctly, so that it spots mischievous behaviour reliably without sounding too many false alarms. An IDS may end up like the boy who cried wolf—when a genuine attack occurs after too many false alarms, nobody pays any attention. And even when it is properly tuned, people may not know how to stop the problem when an IDS sounds the alarm. All too often the response is, “We just got hacked—what do we do?”, says Chris King of Meta Group.

Other tools in the security toolbox include encryption, the mathematical scrambling of data so that only the intended recipient can read them, and the related technique of cryptographic authentication to verify that people are who they claim they are. These tools can be integrated into an e-mail system, for example, using encryption to ensure that messages cannot be read in transit, and authentication to ensure that each message really did come from its apparent sender. The same techniques can also be used to send information (such as credit-card details) to and from websites securely.

Another popular use of encryption and authentication is the “virtual private network” (VPN), which allows authenticated users to establish secure communications channels over the Internet to a closed network. VPNs are widely used to knit a company's networks in different parts of the world together securely across the Internet, and to allow travelling employees to gain secure access to the company network from wherever they are.

There is still plenty of room for innovation in security technology, and there are dozens of start-ups working in the field. Company 51 of San Mateo, California, has devised an “intrusion-prevention system”, based on the workings of the human immune system. When an attack is detected, the attacker is promptly disconnected. Cenzic, also based in Silicon Valley, has devised a novel approach to security testing called “fault injection”. Greg Hoglund, the company's co-founder, says most testing of security software is akin to testing a car by driving it on a straight, flat road. Just as cars are crash-tested, Cenzic's software, called Hailstorm, stress-tests software by bombarding it with attacks.

Blame it on the bugs

A typical network, then, is secured using a multi-layered combination of security technologies. But these fancy measures merely treat the effects of poor security. A parallel effort is being made to deal with one of its main causes: badly written software. According to @Stake, a security consultancy based in Cambridge, Massachusetts, 70% of security defects are due to flaws in software design. Code Red, for example, exploited a “bug”, or coding error, in the way Microsoft's web-server software handles non-Roman characters. Buggy software tends to be insecure. So by taking a firmer stand against bugs and making their programs more reliable, software firms can also improve security.

Microsoft is now making a particular effort to improve its reputation for shoddy security. New bugs and vulnerabilities in its products are found weekly. This does not necessarily mean that Microsoft's software is particularly badly written, but has much to do with its ubiquity. Microsoft has a monopoly in desktop operating systems, after all, and a near-monopoly in web browsers and office productivity software. Find a hole in Internet Explorer, Microsoft's web browser, for example, and you are capable of attacking the vast majority of the world's PCs. Find a hole in Netscape's rival web browser, which is far less widely used, and you will be able to attack fewer than 10% of them.

Now that the threat to Microsoft of dismemberment by America's Department of Justice has receded, the company's poor reputation in security looks like its single biggest problem. Last year, following the Code Red and Nimda outbreaks, both of which exploited security flaws in Microsoft products, John Pescatore at Gartner, an influential consultancy firm, suggested that companies that wanted to avoid further security problems should stop using Microsoft's software. Bill Gates responded by issuing his company-wide memo in January on “trustworthy computing”.

Microsoft is pulling out all the stops to reduce the number of security vulnerabilities in its products. “There was a sea change in the way our customers were thinking,” says Pierre de Vries, Microsoft's director of advanced product development. The company, he says, realised that it had “a real problem” even before Mr Pescatore's report. Earlier this year, the 8,500 programmers in the company's Windows division were given new security training, after which they spent two months combing their code for potential vulnerabilities. New tools devised by the company's research division, called “Prefix” and “Prefast”, are used to scan for possible problems. And when coding errors are found, they are not only fixed but an effort is now made to find out how they slipped through the net in the first place.

The work the programmers are doing now will not be reflected in the company's products for a year or two, but Microsoft has also tightened security in other ways. The latest version of its web-server software, for example, arrives with most options switched off by default. Customers have to decide which options they want to use, and make a conscious choice to switch them on. This reduces their exposure to problems in parts of the software they were not using anyway. But some customers complained about having to work out which options they did and did not need, says Mr de Vries. One of them even asked for a button to turn everything on. The cost of improved security, it seems, is often a reduction in convenience.

This kind of thing goes against the grain for Microsoft. Traditionally, its products have had all the bells and whistles (such as the infamous talking paper clip - see article) turned on by default, to make it more likely that users will discover and use new features. Microsoft is also renowned for encouraging users to upgrade for extra features. But priorities have changed. As Mr Gates wrote to his workforce, "When we face a choice between adding features and resolving security issues, we need to choose security."

Microsoft's policy of tight integration between its products, which both enhances ease of use and discourages the use of rival software makers' products, also conflicts with the need for security. Because Microsoft's programs are all linked, a flaw in one of them can be used to gain access to others. Many viruses, for example, exploit holes in Microsoft's mail or browser software to infect the underlying Windows operating system.

Many observers believe that Microsoft's new-found concern over security is mere window-dressing. The Windows operating system is the largest piece of software ever written, so implementing security retrospectively is a daunting task. Mary Ann Davidson, chief security officer at Oracle, contends that American federal agencies are "really angry" with Microsoft over the insecurity of its products. Oracle, whose flagship database software grew out of a consulting contract for the Central Intelligence Agency, has many black-suited "professional paranoids" among its customers, so the company has security awareness far more deeply ingrained in its corporate culture, she says. But what of Oracle's advertising claims that its own software is "unbreakable"? Perfect security is impossible, she concedes; the campaign "is about being fanatical about security."

Need to know

A key test of a company's commitment to security is the speed with which it responds to vulnerabilities. The difficulty, says Steve Lipner, Microsoft's director of security assurance, is that when a new vulnerability is discovered, customers want a patch immediately, but they also want the patch to be properly tested, which takes time. Furthermore, issuing a separate patch for every vulnerability makes life harder for systems administrators, so Microsoft now prefers to group several patches together. But that lays it open to the charge that it is not responding fast enough. Once a vulnerability has been announced, attackers will start trying to exploit it immediately. According to Mr Davies, some big websites get attacked as little as 40 minutes after the publication of a new vulnerability. But the patch may not be available for weeks.

Mr Lipner says he would prefer researchers who find flaws to report them to Microsoft, but not to publicise them until a patch is available. The trouble is that software makers have little incentive to fix patches that nobody knows about, so many security researchers advocate making vulnerabilities public as soon as they are found. Admittedly, this alerts potential attackers, but they may already have known about them anyway. Proponents of this “full disclosure” approach argue that its benefits outweigh the risks. “Sunlight is the best disinfectant,” says Mr Diffie at Sun Microsystems.

Will software makers ever come up with products that are free of security vulnerabilities? It seems very unlikely, but even if they did, there would still be plenty of systems that remained unpatched or incorrectly configured, and thus vulnerable to attack. No matter how clever the technology, there is always scope for human error. Security is like a chain, and the weakest link is usually a human.

Economist.com RESEARCH TOOLS SURVEYS

The weakest link

Oct 24th 2002
From The Economist print edition

If only computer security did not have to involve people

THE stereotype of the malicious hacker is a pale-skinned young man, hunched over a keyboard in a darkened room, who prefers the company of computers to that of people. But the most successful attackers are garrulous types who can talk their way into, and out of, almost any situation. In the words of Mr Schneier, the security guru, "Amateurs hack systems, professionals hack people."

Kevin Mitnick, perhaps the most notorious hacker of recent years, relied heavily on human vulnerabilities to get into the computer systems of American government agencies and technology companies including Fujitsu, Motorola and Sun Microsystems. Testifying before a Senate panel on government computer security in 2000, after spending nearly five years in jail, Mr Mitnick explained that:

When I would try to get into these systems, the first line of attack would be what I call a social engineering attack, which really means trying to manipulate somebody over the phone through deception. I was so successful in that line of attack that I rarely had to go towards a technical attack. The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain.

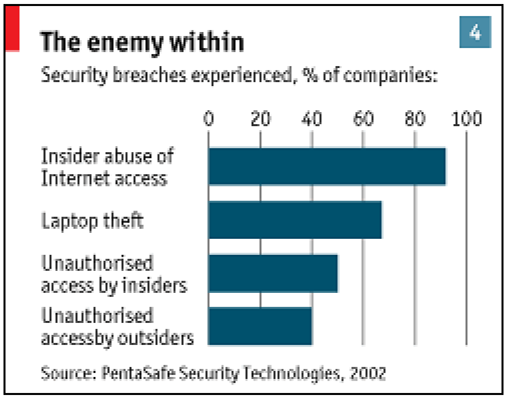
Human failings, in other words, can undermine even the cleverest security measures. In one survey, carried out by PentaSafe Security, two-thirds of commuters at London's Victoria Station were happy to reveal their computer password in return for a ballpoint pen. Another survey found that nearly half of British office workers used their own name, the name of a family member or that of a pet as their password. Other common failings include writing passwords down on sticky notes attached to the computer's monitor, or on whiteboards nearby; leaving machines logged on while out at lunch; and leaving laptop computers containing confidential information unsecured in public places.

Unless they avoid such elementary mistakes, a firm's own employees may pose the largest single risk to security. Not even technical staff who should know better are immune to social engineering. According to Meta Group, the most common way for intruders to gain access to company systems is not technical, but simply involves finding out the full name and username of an employee (easily deduced from an e-mail message), calling the help desk posing as that employee, and pretending to have forgotten the password.

Simple measures, such as encouraging employees to log out during lunch hours and to choose sensible passwords, can dramatically enhance security at very little cost. Passwords should be at least six and ideally eight characters long, and contain a mixture of numbers, letters and punctuation marks. Dictionary words and personal information should not be used as passwords. Users should have a different password on each system, and they should never reveal their passwords to anyone, including systems managers.

Yet a seminal paper published as long ago as 1979 by Ken Thomson and Robert Morris found that nearly a fifth of users chose passwords consisting of no more than three characters, and that a third used dictionary words. (Robert Morris, the chief scientist at America's National Computer Security Centre, was subsequently upstaged by his son, also called Robert, who released the first Internet worm in 1988 and crashed thousands of computers. Ironically, the worm exploited badly chosen passwords.) But back in 1979, only a small fraction of a typical company's workforce used computers on a daily basis. Now that almost everybody uses them, the potential for trouble is much greater.

A few precautions also go a long way when it comes to stopping the spread of viruses. Many viruses travel inside e-mail messages, but require the user to double-click them in order to start propagating. So they pose as games, utilities, anti-virus updates or even as nude photographs of well-known tennis players. The curious user double-clicks, nothing seems to happen, and the user thinks no more about it, but the virus has started to spread. Educating users not to double-click on dubious attachments is a simple but effective counter-measure against viruses.


The enemy within

Security breaches experienced, % of companies:

Source: PentaSafe Security Technologies, 2002

If correctly handled, a management-based, rather than a solely technology-based, approach to security can be highly cost-effective. The danger, says Peter Horst of TruSecure, is that: "People buy a hunk of shining technology, wipe their brow and say, 'Great, I've taken care of it,' when they might have been better off saving money and doing something simple in terms of policy and process." Probably the best example of how expensive, glamorous security technology can easily be undermined by poor procedures is biometric systems (see article).

A sensible and balanced approach, then, involves not only security technology but also a well-defined set of security policies which users understand and keep to. This approach is promoted by the Human Firewall Council, a group which argues that users themselves have an important role to play in maintaining security. Steve Kahan, its president, draws an analogy with neighbourhood-watch schemes. The idea, he says, is “to make security everyone's business”, and to have a clear security policy that governs what is and is not allowed. That policy should then be implemented both by guiding the behaviour of users and by the appropriate configuration of firewalls, anti-virus software and so forth, in much the same way that a combination of neighbourly vigilance, alarms and door locks is used to combat burglars in the real world. But, says Mr Kahan, surveys show that half of all office workers never receive any security training at all.

One way to disseminate and enforce security policy is to add yet another layer of security software, as demonstrated by PentaSafe Security, one of the backers of the Human Firewall Council. Its software can ensure that users are familiar with a company's security policy by popping messages and quiz-like questions up on the screen when they log on. According to PentaSafe's figures, 73% of companies never require employees to re-read security policies after they begin their employment, and two-thirds of companies do not track whether their employees have read the policy in the first place.

David Spinks, European director of security at EDS, a computer-services firm, says all EDS employees have to take a regular on-screen test to ensure they understand the company's policy on passwords, viruses and network security. Choice of technology, he says, matters far less than managing both technology and users properly: “The key to having a firewall isn't the firewall, but how the policies are set, monitored, managed and kept up to date.” Two companies can use exactly the same product, he notes, and one can be secure while the other is insecure. It is effective management that makes the difference.

The dismal science of security

But there are other, more subtle ways in which management and security interact. “More than anything else, information security is about work flow,” says Ross Anderson of Cambridge University's Computer Laboratory. The way to improve security, he says, is to think about people and processes rather than to buy a shiny new box. Mr Anderson is one of a growing number of computer scientists who are applying ideas from economic theory to information security. Insecurity, he says, “is often due to perverse incentives, rather than to the lack of suitable technical protection mechanisms.” The person or company best placed to protect a system may, for example, be insufficiently motivated to do so, because the costs of failure fall on others. Such problems, Mr Anderson argues, are best examined using economic concepts, such as externalities, asymmetric information, adverse selection and moral hazard.

A classic example is that of fraud involving cash dispensers (automated teller machines). Mr Anderson investigated a number of cases of “phantom withdrawals”, which customers said they never made, at British banks. He concluded that almost every time the security technology was working correctly, and that misconfiguration or mismanagement of the machines by the banks was to blame for the error. In Britain, it is customers, not banks, that are liable when phantom withdrawals are made, so the banks had little incentive to improve matters. In America, by contrast, it is the banks that are liable, so they have more of an incentive to train staff properly and install additional anti-fraud measures, such as cameras.

Similar examples abound on the Internet. Suppose an attacker breaks into company A's computers and uses them to overload company B's computers with bogus traffic, thus keeping out legitimate users. Company B has suffered, in part, because of the insecurity of company A's systems. But short of a lawsuit from company B, company A has no incentive to fix the problem. Some examples of this sort of thing have already started to appear. In one case, a Texas judge issued a restraining order against three companies whose computers were being used by intruders to attack another firm's systems. The three companies were forced to disconnect from the Internet until they could demonstrate that the vulnerabilities exploited by the attackers had been fixed.

Economic and legal measures will, predicts Mr Schneier, play an increasing role in compensating for perverse incentives that foster insecurity. Just as chief financial officers are legally required to sign statements declaring that company accounts are accurate, he speculates that, at least in certain industries, chief security officers might eventually have to sign security declarations. Similarly, product-liability lawsuits against software companies whose products are insecure would almost certainly discourage software makers from cutting corners on security.

The enemy within

Incompetence and indifference are one thing; misconduct is another. Although external attacks get more attention in the media, notes a recent report from Vista Research, a consultancy, “the bulk of computer-security-related crime remains internal.” Mr Anderson puts it a different way: the threat of hackers, he says, is “something that the security manager waves in your face to get the budget to deal with internal fraud.” Vista estimates that 70% of security breaches that involve losses above $100,000 are perpetrated internally, often by disgruntled employees.

Attacks by insiders are potentially far costlier than external ones. The CSI/FBI survey, albeit using a small sample size, found that an insider attack against a large company caused an average of $2.7m-worth of damage, whereas the average external attack cost $57,000. A survey carried out by Oracle found that British companies believe malicious attacks by insiders pose more of a threat than external ones.

Defences against external attacks may not be much use against insiders. For a start, such people are likely to be inside the firewall (although companies are increasingly using internal firewalls between departments). And to an intrusion-detection system, an insider attack looks very different from an external one; by one estimate, an IDS has less than a 40% chance of distinguishing an insider attack from legitimate use of the network. One option is to use an analysis and visualisation tool, such as that made by SilentRunner. It represents network activity graphically to help security staff spot unusual behaviour—perhaps a large number of file transfers in a department where lay-offs have just been announced.

An alternative approach when fraud is suspected is to use “honeypots”—decoy servers that lure attackers and collect evidence so that people who are up to no good can be identified. In one case cited by Recourse Technologies, a security firm that is now part of Symantec, a large financial firm discovered that its payroll systems had been compromised. Two dozen honeypots were set up, with names such as “payroll server”, which caught the company's chief operating officer as he was trying to manipulate another executive's payroll record. He confessed to attempted fraud and resigned.

But the difficulty of combating insider attacks with technical means demonstrates that security is mainly a people problem. Indeed, the root cause of an insider attack may be poor management. An employee may resent being demoted or passed over for promotion, or feel underpaid or undervalued. Better management is a far more promising way to deal with these kinds of problems than technology.

The best way to prevent criminal activity by insiders is to make it difficult. “One of the key things you need is a separation of duties, so that no one individual runs everything,” says Mr Spinks. Another simple measure is to ensure that all employees go on holiday at some point, to prevent them from maintaining tainted systems or procedures. Access privileges to company systems need to match employees' job descriptions so that, for example, only people in the personnel department can access employee records. When employees leave the company or their roles change, their access privileges must be revoked or altered immediately. And clear rules are needed to make sure that security staff know what to do if they detect abuse by senior managers. Better internal security procedures to deal with malicious insiders should also help to protect against external attacks, says Bill Murray of TruSecure.

One of the biggest threats to security, however, may be technological progress itself, as organisations embrace new technologies without taking the associated risks into account. To maintain and improve security, you need more than just the right blend of technology, policy and procedure. You also need to keep your eye on the ball as new technologies and new threats emerge.

Economist.com

RESEARCH TOOLS
SURVEYS

Biometric fact and fiction

Oct 24th 2002
From The Economist print edition

Body-scanning technology has its drawbacks

YOU'VE seen them in spy films and science-fiction movies: eye-scanners, fingerprint readers, facial-recognition systems. Such body-scanning or "biometric" systems, which can make sure that somebody really is who he claims to be, are touted as the ultimate in security technology. Systems protected by passwords are unlocked by something you know (the password), which others can find out. Systems protected by keys or their high-tech equivalents, smart cards, are unlocked by something you have (the key), which others can steal. But systems protected by biometrics can be unlocked only by a bodily characteristic (such as a fingerprint) that no one can take from you. Your body is your password.

Eye-scanning biometric technology played a prominent part in a recent science-fiction movie, "Minority Report". Its star, Tom Cruise, played a policeman accused of a crime who goes on the run. In the movie's futuristic setting, eye scanners are used to ensure that only legitimate users can access computer systems. Mr Cruise's character has eye transplants to conceal his identity, but also keeps his old eyeballs so that he can continue to log on to the police network.

That excursion into a fictional future highlights two real problems. The first is that the technology is not as secure as its proponents claim. Scanners that read fingerprints, the most widely used form of biometrics, proved easy to defeat in experiments carried out by Tsutomu Matsumoto, a security researcher at Yokohama National University. Mr Matsumoto was able to fool them around 80% of the time using fingers made of moulded gelatin. He was also able to take a photograph of a latent fingerprint (from a wine glass, for example) and use it to make a gelatin finger that fooled scanners 80% of the time as well. One advantage of gelatin is that having got past the guards, an intruder can eat the evidence.

Facial recognition, in which a computer analyses images from a digital camera and compares them with a "watch list" of known faces, is unreliable too. A study carried out at America's Defence Department found that instead of the claimed 90% accuracy rate, such systems correctly identified people only 51% of the time. Since the September 11th attacks, the technology has been tested at a number of American airports, but in one trial it was found that face-scanners could be fooled by people who turned their heads slightly. Recalibrating the system to allow looser matches caused a flood of false positives (where someone is wrongly identified as being on the watch list).

Identix, a leading supplier of facial-recognition systems, claims that its equipment's accuracy rate can be as high as 99%. But Mr Schneier, the security expert, says that even with an accuracy rate of 99.99%, and assuming that one in 10m fliers is a suspect whose face is on the watch list, there will still be 1,000 false alarms for every suspect identified. And most terrorists are not on watch lists. Face-scanning may reassure people and may have a deterrent effect, but these meagre benefits do not justify the costs.

The second and more important problem is that biometric technology, even when it works, strengthens only one link in the security chain. Its effectiveness is easily undermined by failures of process or policy. Tom Cruise's character in “Minority Report” is still able to get into the police computer network while on the run because someone has neglected to revoke his access privileges. This simple failure of process is all too common in real life. Another such real-world failure involves the use of hand-geometry scanners in airports. Each person's hand is supposed to be scanned separately, but often the first person in a group goes through the door and then holds it open.

In short, biometrics are no panacea. The additional security they provide rarely justifies the cost. And in high-risk environments such as banks or jails, other measures are still needed.

Economist.com RESEARCH TOOLS SURVEYS

When the door is always open

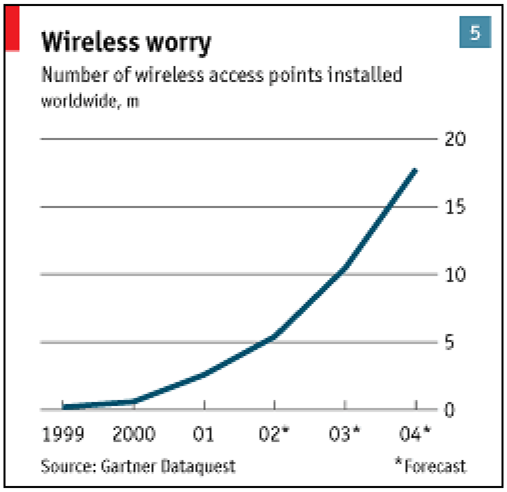
Oct 24th 2002
From The Economist print edition

The more that companies open up and interconnect their networks, the bigger the risk of security problems

NOT long ago, at the height of the dotcom boom, you could chart the rise and fall of companies by looking at the garish artwork sprayed on the walls of loft buildings in San Francisco's Multimedia Gulch district. But now, thanks to wireless technology, there is a better way. Driving around the city on a warm night a few weeks ago, Bill Cockayne, a Silicon Valley veteran, opens his car's sunroof. His friend Nathan Schmidt posts what looks like a small fluorescent tube through the open roof and plugs it into a laptop computer. “Metro/Risk”, says the computer in a clipped female voice as the car makes its way through North Beach. “Admin network. BCG.” Then a robotic male voice booms out: “Microsoft WLAN. Archangel. Whistler. Rongi.”

These are the names of computer networks in offices and homes that have been fitted with wireless access-points, which can provide Internet access to users within range (typically, within 100 metres or so). Mr Schmidt's computer is configured so that open access-points, which can often be used by anyone within range, have their names spoken by a female voice; closed ones, for which a password is required, are read out by a male voice. Most of them are open. Mr Cockayne pulls over, and Mr Schmidt connects to a nearby access-point and calls up *The Economist*'s web page.

This kind of wireless networking, using the so-called Wi-Fi protocol, has become immensely popular over the past two years, the technology crash notwithstanding (see chart 5). Many companies and individuals leave their access-points open deliberately to enable passers-by to share their Internet connections. Open a laptop in New York, San Francisco, Seattle or many other large cities around the world and you may well be able to get online free. But although Wi-Fi is liberating for users, it can cause security problems.



Adding an access-point to a network costs less than $200 and is very simple—so simple, in fact, that “rogue” access-points have started to sprout on corporate networks without the knowledge of management. A survey by *Computerworld*, an industry magazine, found that 30% of American companies had identified rogue access-points on their networks. And if these are left open, they provide a back door past the firewall into the company's network. Rob Clyde, chief technology officer at Symantec, says that half of the chief executives at a recent round-table event cited Wi-Fi as a top security concern.

This is just one example of how a new technology can bring security problems in its wake. There are plenty of others. Some firms are opening up their networks through online business-to-business exchanges, for example, where they list what they want to buy or sell and invite bids. Everything from paper clips to car components is bought or sold in this way. There is widespread agreement that “web services”, in which companies open up their core business processes directly to other firms over the Internet, will become increasingly important in the next few years. But by opening its systems to outsiders, a company may also attract unwanted visitors, or attacks from nosy competitors.

Joint ventures, in which two firms collaborate and share information, can also cause problems. A recent report by Vista Research cites the example of an American car maker that established a joint venture with a Japanese firm and opened up its network to allow in employees of its Japanese partner. But the design of the American firm's network allowed access only on an “all or nothing” basis, so the Japanese firm's employees ended up with access to everything.

Handheld computers are another problem. They are often used to store sensitive data such as passwords, bank details and calendars. “The calendar is a fundamental loophole,” says Doug Dedo of Microsoft's mobile devices division, because it may contain entries such as “meeting with company X re merger”. Another problem associated with handheld computers is that their users carry them into the office and plug them into their computers, bypassing anti-virus systems and firewalls. A virus-infected document stored on a handheld computer could then start spreading. Similarly, peer-to-peer file-swapping networks such as Gnutella, instant-messaging services that zap messages and files across the Internet, and web-based e-mail systems such as Hotmail all provide new routes into a company's network that can be exploited by attackers.

There are plenty of technical fixes available. Handheld scanners can be used to track down rogue access-points, and legitimate access-points can be secured against outsiders by using virtual-private-network (VPN) software. A lot of work is being done to ensure that web services are secure, including, improbably, a joint initiative by rivals Microsoft and IBM. Anti-virus and firewall software exists for handheld computers, which can also be password-protected. And firewalls can be configured to prevent unauthorised use of peer-to-peer and instant-messaging services.

All these threats arise from a common factor: the distinction between the "public" parts of a company's network (such as the web servers where its home page resides) and the private core (which is accessible only to employees) is quickly eroding. "The cultural and technological trend is towards more porous companies," says Gene Hodges, president of Network Associates, a large security-software firm. As firms connect with their suppliers and customers, "the more you open up, the more you are exposed."

Airports, not castles

The classic notion of perimeter security, in short, is fast becoming obsolete. Alan Henricks, chief executive of Cenzic, says the shift is "from keeping people out to bringing people in in a trusted fashion". Nand Mulchandani, co-founder of Oblix, another security firm, puts it more colourfully: the "big walls, moat and crocodiles" approach of the past few years, he says, is now outdated.

The latest thinking is that rather than seeing their networks as castles, large organisations should regard them as airports. People go in and out all the time, some areas are more secure than others, and as people pass from one area to another they have to present their credentials: tickets, boarding passes or passports. Apply this approach to computer security, and instead of an "exclusive" model in which you try to prevent people from doing things they shouldn't, you have an "inclusive" model that lays down who can do what, and only lets certain people do certain things.

In the old days, says Tony Scott, chief technology officer at General Motors, computer systems were used only internally, and managing who was allowed to do what was simple. But with the recent proliferation of systems, and a greater reliance on suppliers and outsourcing, the number of users who may need access to a company's systems has grown rapidly. "On top of that, most modern companies now have their actual business processes deeply embedded in their systems," he says. Indeed, their business processes are the systems. According to Mr Scott, "All these forces working together create a huge problem. Who is accessing these systems, and how can I manage it?"

One outfit offering solutions to this identity-management problem is Silicon-Valley-based Oblix. Its software sits between users and a company's existing software systems (accounts, inventory, e-mail, and so on). Using a big database that includes information on who can do what, it makes sure that users can do only the things they are meant to do.

It sounds obvious, but it has two advantages: it means users need to log in only once, rather than into lots of separate systems; and it centralises and simplifies the management of user privileges. For example, a division manager who hires or fires an employee can instantly update that employee's access privileges, rather than having to ask the systems department to make changes to a number of separate systems.

Responsibility for security can thus be devolved to managers and form part of their everyday management duties. Management is all-important, says Mr Mulchandani, because if your eyeball reader correctly identifies a sacked employee but his access privileges have not been revoked, you have a security failure on your hands. Oblix's software is used by a number of large firms including General Motors, Boeing and Pfizer. Identity-management systems are also available from other vendors, including Novell, IBM and ActivCard, whose smart-card-based offering is used by America's armed forces. The technique does not do away with the need for traditional security measures, but it provides an additional line of defence, particularly for large organisations that have to deal with a lot of users.

More importantly, identity management is an example of how technology can be used to align security procedures with business processes. Security thus becomes the servant of management. Security decisions must ultimately be taken by managers, not technical staff. The big decision, and the most difficult to make, is how much time and money to spend on security in the first place.

Economist.com
RESEARCH TOOLS
SURVEYS

Putting it all together

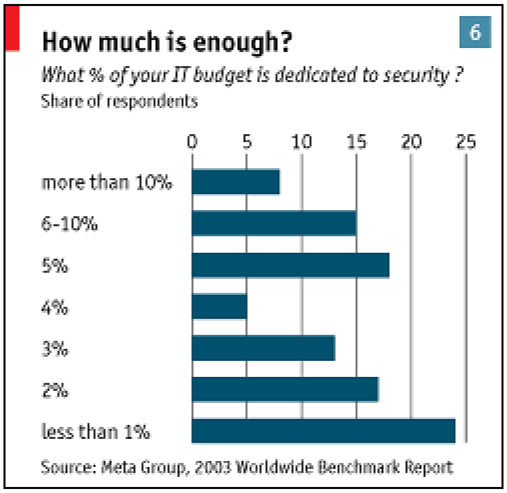
Oct 24th 2002
From The Economist print edition

Security spending is a matter of balancing risks and benefits

TOTAL computer security is impossible. No matter how much money you spend on fancy technology, how many training courses your staff attend or how many consultants you employ, you will still be vulnerable. Spending more, and spending wisely, can reduce your exposure, but it can never eliminate it altogether. So how much money and time does it make sense to spend on security? And what is the best way to spend them?

There are no simple answers. It is all a matter of striking an appropriate balance between cost and risk—and what is appropriate for one organisation might be wrong for another. Computer security, when you get down to it, is really about risk management. Before you can take any decisions about security spending, policy or management, the first thing you have to do is make a hard-headed risk assessment.

First, try to imagine all of the possible ways in which security could be breached. This is called "threat modelling", and is more difficult than it seems. Mr Schneier, the security guru, illustrates this point by asking people to imagine trying to eat at a pancake restaurant without paying. The obvious options are to grab the pancakes and run, or to pay with a fake credit card or counterfeit cash. But a would-be thief could devise more creative attacks.



Source: Meta Group, 2003 Worldwide Benchmark Report

He could, for example, invent some story to persuade another customer who had already paid for his meal to leave, and then eat his pancakes. He could impersonate a cook, a waiter, a manager, a celebrity or even the restaurant owner, all of whom might be entitled to free pancakes. He might forge a coupon for free pancakes. Or he might set off the fire alarm and grab some pancakes amid the ensuing chaos. Clearly, keeping an eye on the pancakes and securing the restaurant's payment system is not enough. Threat modelling alerts you to the whole range of possible attacks.

The next step is to determine how much to worry about each kind of attack. This involves estimating the expected loss associated with it, and the expected number of incidents per year. Multiply the two together, and the result is the "annual loss expectancy", which tells you how seriously to take the risk. Some incidents might cause massive losses, but be very rare; others will be more common, but involve smaller losses.

The final step is to work out the cost of defending against that attack. There are various ways to handle risk: mitigation (in the form of preventive technology and policies), outsourcing (passing the risk to someone else) and insurance (transferring the remaining risk to an insurer).

Suppose you are concerned about the risk of your website being attacked. You can mitigate that risk by installing a firewall. You can outsource it by paying a web-hosting firm to maintain the website on your behalf, including looking after security for you. And you can buy an insurance policy that, in the event of an attack, will pay for the cost of cleaning things up and compensate you for the loss of revenue. There are costs associated with each of these courses of action. To determine whether a particular security measure is appropriate, you have to compare the expected loss from each attack with the cost of the defence against it.

Firewalls make sense for large e-commerce websites, for example, because the cost of buying and maintaining a firewall is small compared with the revenue that would be lost if the site were shut down by an intruder, however briefly. But installing biometric eye-scanners at every turnstile on a city's public-transport system would be overkill, because fare-dodging can be mitigated with far cheaper technology. By contrast, in high-security environments such as military facilities or intelligence organisations, where a security breach would have serious consequences, the use of expensive security technology may be justified. In some situations, however, the right response may be to do nothing at all.

Standards stuff

That different organisations have different security needs is explicitly recognised in the ISO 17799, an international standard for "best practices in information security" that was introduced by the International Organisation for Standardisation in 2000. Risk analysis is a basic requirement of the standard, as is the establishment of a security policy. But, says Geoff Davies of i-Sec, a British security consultancy, "an industrial firm and a bank with ISO 17799 certification will have totally different systems." The standard does not specify particular technological or procedural approaches to security, but concentrates on broadly defined ends rather than specific means.The standard's flexibility is controversial, however. Critics believe future versions of the standard should be more prescriptive and more specific about what constitutes "best practice". Still, even in its current form, ISO 17799 is better than nothing. Many multinational companies have already embraced it to demonstrate their commitment to security. And in several Asian countries, companies that want to do business with the government electronically must conform to the standard.

Just as different organisations require different levels of protection, they will also respond to an attack in different ways. A large company, for example, may find it useful to have a dedicated security-response team. Scott Charney at Microsoft says that when an attack occurs, one of the things the team has to decide is whether to give priority to remediation or to investigation. Blocking the attack will alert the attacker, which may make collecting evidence against him difficult; but allowing the attacker to continue so that he can be identified may cause damage. Which is more appropriate depends on the context. In a military setting, tracking down the attacker is crucial; for a dotcom under attack by a teenager, blocking the attack makes more sense. Another difficult choice, says Mr Charney, is whether to bring in the police. Internal investigations allow an organisation to maintain control and keep things quiet, but law-enforcement agencies have broader powers.

For small and medium-sized companies, a sensible choice may be “managed security monitoring” (MSM). Firms that offer this service install “sentry” software and machines on clients' networks which relay a stream of messages to a central secure operations centre. Human operators watch for anomalous behaviour and raise the alarm if they detect anything suspicious. Using highly trained specialists to look out for trouble has the advantage that each operator can watch many networks at once, and can thus spot trends that would otherwise go unnoticed.

Risk analysis, and balancing cost and risk, is something the insurance industry has been doing for centuries. The industry is now showing increased interest in offering cover for computer-related risks. In the past, computer risks were included in general insurance policies, but were specifically excluded in the run-up to the year 2000 to avoid “millennium bug” liabilities. Now insurers are offering new products to protect companies against new risks. Because of the Internet, “the landscape has changed,” says David O'Neill, vice-president of e-Business Solutions at Zurich North America, which acts as a matchmaker between customers and underwriters. Greater connectivity means firms are now exposed to risks that were never contemplated by traditional insurance policies, he says.

Mr O'Neill can arrange insurance against a range of risks, including data theft, virus attacks or intrusions by malicious hackers, and loss of income owing to a security breach or network failure. Companies can also take out insurance against having to pay damages if confidential financial or medical data are accidentally or maliciously released. Because no two networks or businesses are alike, each policy is prepared individually.

Such cyber-insurance is, however, still very much in its infancy. The main problem is that the complexity of computer networks makes it very difficult to quantify risk accurately. By comparison, working out the likelihood that a 45-year-old smoker will have a heart attack in the next 12 months is a piece of cake. One reason for the lack of data, says Mr Charney, is that most security breaches are not detected or reported. But this will change. “When a company asks for $1m in damages after a virus outbreak, the insurer will say, ‘Prove it',” he explains. “Firms will have to substantiate it, and we will get some data.”

Mr Schneier predicts that insurance companies will start to specify what kinds of computer equipment companies should use, or charge lower premiums to insure more secure operating systems or hardware. Already, firms that use the monitoring service provided by his company, Counterpane Internet Security, enjoy a 20-40% reduction in their premiums for cyber-insurance. But Mr Anderson at Cambridge University thinks the need for cyber-insurance is overblown. “Insurers are having a hard time, so they are turning e-risks into a new pot of gold,” he says.

Wrong department

Most organisations already have the expertise required to handle computer security in a sensible way. Usually, however, this risk-management expertise is found not in the systems department but in the finance department. “Chief information officers, chief financial officers and other executives already know how to do risk analysis,” says Mr Davies. The systems department, on the other hand, does not; instead, it tends to be seduced by siren songs about technological fixes.

This survey has consistently argued that enthusiasm for technological solutions can go too far. In two areas in particular, security technology could end up doing more harm than good. First, some measures introduced in the name of improving security may have the side-effect of needlessly infringing civil liberties. Face-scanning systems at airports are a good example. They are almost useless at spotting terrorists, but civil-rights advocates worry about “function creep”, in which such systems are installed for one purpose and then used for another.

Similarly, new legislation has been proposed that would allow far more widespread wire-tapping and interception of Internet communications to combat terrorism. But would it actually improve security? “Broad surveillance is generally the sign of a badly designed system of security,” says Mr Schneier. He notes that the failure to predict the September 11th attacks was one of data sharing and interpretation, not data collection. Too much eavesdropping might actually exacerbate the problem, because there would be more data to sift. It would be better to step up intelligence gathering by humans.

The second area where security technology could do more harm than good is in the world of business. Technology introduced to improve security often seems to have the side-effect of reinforcing the market dominance of the firm pushing it. “Information-security technologies are more and more used in struggles between one company and another,” says Mr Anderson. “Vendors will build in things that they claim are security mechanisms but are actually there for anti-competitive reasons.”

One current, and highly controversial, example is Palladium, Microsoft's proposed technology for fencing off secure areas inside a computer. It might be very useful for stopping viruses; but it might also enable Microsoft to gain control of the standard for the delivery of digital music and movies.

Security, in sum, depends on balancing cost and risk through the appropriate use of both technology and policy. The tricky part is defining what “appropriate” means in a particular context. It will always be a balancing act. Too little can be dangerous and costly—but so can too much.

Economist.com

RESEARCH TOOLS
SURVEYS

The mouse that might roar

Oct 24th 2002
From The Economist print edition

Cyber-terrorism is possible, but not very likely

IT IS a devastating prospect. Terrorists electronically break into the computers that control the water supply of a large American city, open and close valves to contaminate the water with untreated sewage or toxic chemicals, and then release it in a devastating flood. As the emergency services struggle to respond, the terrorists strike again, shutting down the telephone network and electrical power grid with just a few mouse clicks. Businesses are paralysed, hospitals are overwhelmed and roads are gridlocked as people try to flee.

This kind of scenario is invoked by doom-mongers who insist that stepping up physical security since the September 11th attacks is not enough. Road-blocks and soldiers around power stations cannot prevent digital terrorism. “Until we secure our cyber-infrastructure, a few keystrokes and an Internet connection is all one needs to disable the economy and endanger lives,” Lamar Smith, a Texas congressman, told a judiciary committee in February. He ended with his catchphrase: “A mouse can be just as dangerous as a bullet or a bomb.” Is he right?

It is true that utility companies and other operators of critical infrastructure are increasingly connected to the Internet. But just because an electricity company's customers can pay their bills online, it does not necessarily follow that the company's critical control systems are vulnerable to attack. Control systems are usually kept entirely separate from other systems, for good reason. They tend to be obscure, old-fashioned systems that are incompatible with Internet technology anyhow. Even authorised users require specialist knowledge to operate them. And telecoms firms, hospitals and businesses usually have contingency plans to deal with power failures or flooding.

A simulation carried out in August by the United States Naval War College in conjunction with Gartner, a consultancy, concluded that an “electronic Pearl Harbour” attack on America's critical infrastructure could indeed cause serious disruption, but would first need five years of preparation and $200m of funding. There are far simpler and less costly ways to attack critical infrastructure, from hoax phone calls to truck bombs and hijacked airliners.

On September 18th Richard Clarke, America's cyber-security tsar, unveiled his long-awaited blueprint for securing critical infrastructure from digital attacks. It was a bit of a damp squib, making no firm recommendations and proposing no new regulation or legislation. But its lily-livered approach might, in fact, be the right one. When a risk has been overstated, inaction may be the best policy.

It is difficult to avoid comparisons with the “millennium bug” and the predictions of widespread computer chaos arising from the change of date to the year 2000. Then, as now, the alarm was sounded by technology vendors and consultants, who stood to gain from scaremongering. But Ross Anderson, a computer scientist at Cambridge University, prefers to draw an analogy with the environmental lobby. Like eco-warriors, he observes, those in the security industry—be they vendors trying to boost sales, academics chasing grants, or politicians looking for bigger budgets—have a built-in incentive to overstate the risks.