POINT OF VIEW

Achieving Network Security

An AT&T survey and white paper in cooperation with the Economist Intelligence Unit

Executive Summary

The aim of good network security used to be simple–fortify and protect. Now there's a competing business imperative–partner and share. According to a new global survey of 237 senior executives conducted by the Economist Intelligence Unit for AT&T, the goals that many businesses have, from holding customer data to sharing supply-chain data, often entail greater vulnerability to security threats. As a result, security is no longer a straight cost–it is now an enabler of business.

Yet despite heightened interest and spending in network security, the subject remains shrouded. Good data on the prevalence and cost of security attacks are scarce; too much focus tends to be given to external threats when the dangers lurking inside the organisation are arguably even greater.

The answer is to assess, outsource and educate. Risk assessment is the first stage in any corporate security policy, if one is to balance the cost and risk of disasters with the cost of preparedness and prevention. Outsourcing network security to a managed security services provider gives companies a way to partner with outside experts to design and manage complex and labour-intensive security solutions. Educating employees addresses the critical weak point in most security systems–people.

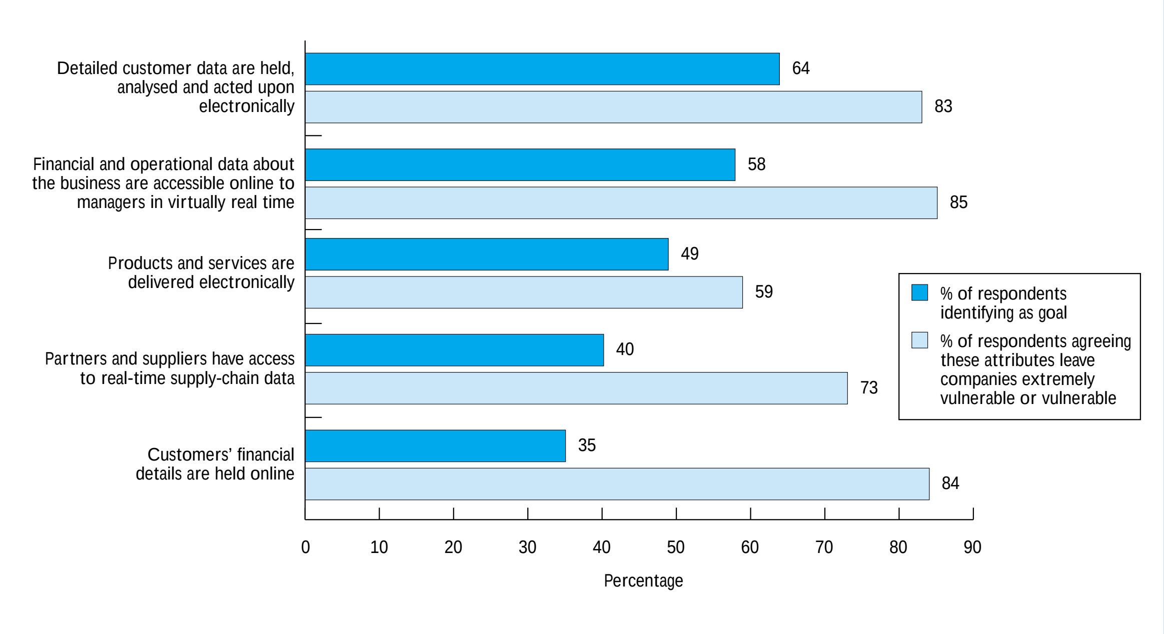
In the third in a series of four thought-leadership articles written by AT&T in co-operation with the Economist Intelligence Unit on the future of networking, we examine network security and some of its challenges. The Economist Intelligence Unit conducted the survey and held a series of interviews with analysts and executives to better understand the dynamics of network security. The fourth and final paper in the series will look at customer relationship management.

Imagine a network that is 100% secure. Sounds appealing. Now imagine a business that doesn't allow anyone outside the organisation to access its data. Less attractive. That, in a nutshell, is the real security challenge for business today–to balance the risks of a security event with the costs of inaccessibility.

The changing nature of the business environment–in which enterprises are using the Internet to extend access to their networks for employees, customers, partners and suppliers–turns security expenditure from a straight cost into a business enabler. When networks were closed and proprietary, security had the narrow focus of fortifying the business. The CEO and the IT director may have clashed over costs but their goals were fundamentally the same.

Now, according to a special global survey of 237 senior executives, the goals that preoccupy business leaders often entail greater vulnerability to security threats. The security challenge facing today's companies is no longer to keep people out, but to let the right people in.

Which of the following technology-related goals does your company have? And how vulnerable do they leave firms to breaches in electronic security?



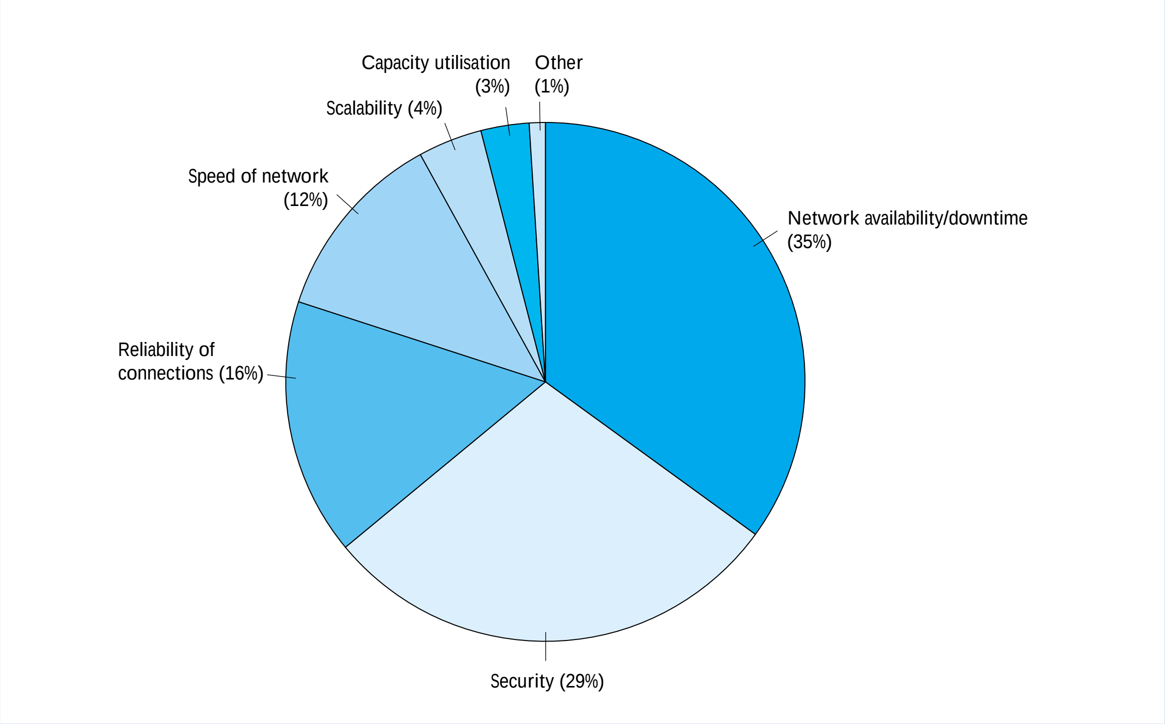
Source: AT&T/Economist Intelligence Unit survey, March-April 2003

Robert Coles, partner and service leader for the consultancy KPMG in London, calls this shift in security "de-perimeterisation, where the goal is to allow organisations to communicate more effectively and more safely with their public and partners". The core security issue today isn't blocking access but rather understanding who is on the other end of a communication link and determining what level and duration of access, if any, should be granted. Our survey group underlines this point–executives expect significant increases in the deployment of identity verification tools for both internal and external threats.

How bad is it?

Striking a balance between accessibility and protection isn't easy. The impact of network security violations can be extremely serious. Aside from the loss of valuable company information, company documents may be altered or illicit transactions carried out in the company's name. Sensitive customer information can also be stolen, resulting in serious damage to a company's reputation. And networks and hardware can also be damaged, leaving a business without functioning key processes. Survey respondents identified security as the second most important performance attribute of their networks after network availability.

What network performance attribute is most important to your business?



Source: AT&T/Economist Intelligence Unit survey, March-April 2003

Spending on security is rising as a result. According to a study done by international IT consultancy The Meta Group, while only 24% of firms increased their overall IT budgets in 2002, 73% increased their spending on security.

But impressive as this growth is, Meta Group's survey reveals that the total spent on security as a percentage of IT spending remains a remarkably low 3%. "All too often," says Meta's vice-president and service director Chris Byrnes, "executives only increase their focus and spending on security after a damaging attack."

That may be because it remains extremely difficult to assess the precise scale and impact of the threat. Figures from the 2003 CSI/FBI Computer Crime and Security Survey[1] show that only 30% of survey respondents reported security incidents to law enforcement authorities. The threat of competitive pressures, reputational risk, and even potential liability continue to keep a public veil over the realities of IT-related losses.

Greater transparency is likely as new laws and regulations requiring verification of data loss come onstream. In California, for instance, Senate Bill 1386 now requires companies to report any loss of personal information directly to affected customers. These greater risks of public exposure will, in turn, "lead to increased focus and spending on security," says Mr Byrnes. But in the meantime, many firms are flailing in the dark.

[1] The survey, conducted by the Computer Security Institute (CSI), a membership organisation serving and training IT security professionals, with the participation of the San Francisco Federal Bureau of Investigation (FBI), is the world's longest-running survey of information security. The survey is based on the responses of only 530 US corporations, government agencies, medical institutions and universities. According to CSI, the results do not represent anything near the total level of attacks and losses worldwide, but are nonetheless interesting for representing the types and costs of IT security attacks.

Assess, outsource, educate

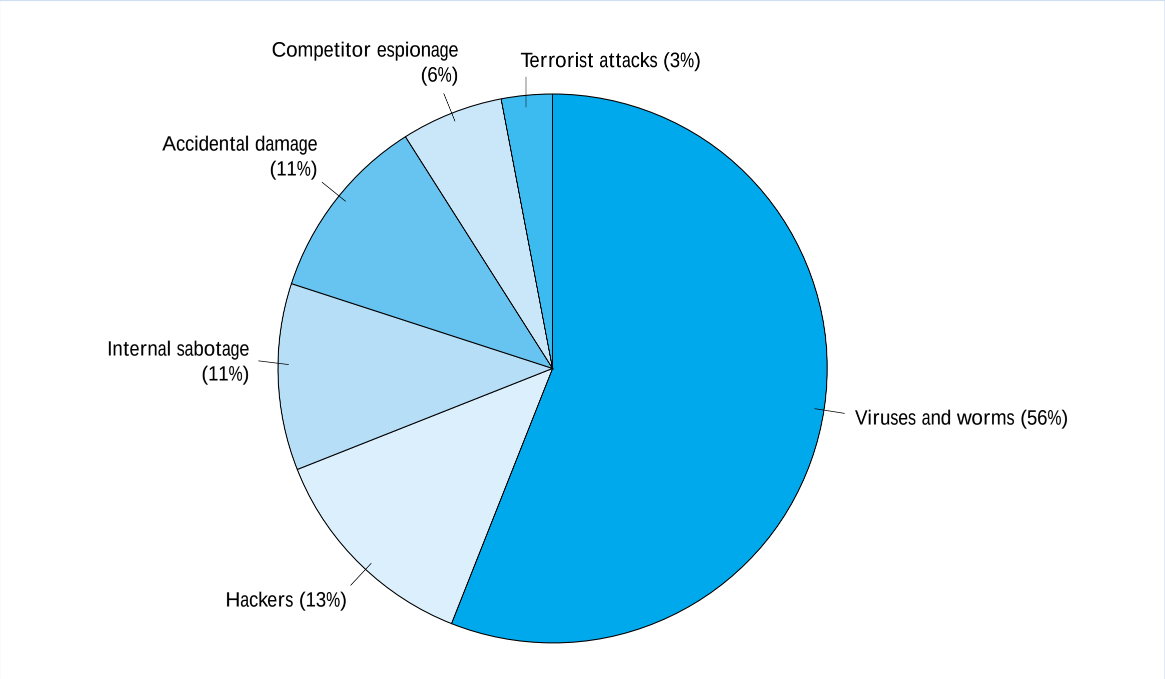
Faced with a situation in which the potential damage of a security event is extremely high, the nature of the threat is difficult to gauge, and the demands of the business point towards opening networks up rather than sealing them, three principles stand out:

- Assess the risk of a security event properly
- Harness the expertise of outsiders
- Focus on policies rather than technology

Risk analysis is the starting point in any security plan development. For Laura Koetzle, senior analyst with Forrester Research, it is all about striking an educated balance between the cost of security and the risk of loss. So what is right for one small manufacturing company will be very different from the security needs of an online financial institution. Without such analysis, says Ms Koetzle, "you are probably spending too much on security, or spending it on the wrong things".

Certainly, the relative insouciance of survey respondents about internal sabotage is misplaced. By some distance, viruses and worms are perceived as the most significant threat by our survey group, but the 2003 CSI/FBI survey indicates that virus incidents and insider abuse of network access actually rank together as the most cited forms of attack. Moreover, for the first time since 1999, the severity and cost of external attacks have actually ticked downward. Some 56% of respondents to the 2003 CSI/FBI survey reported unauthorised access of some sort, slightly lower than the average of 59% over the previous seven years.

Which do you regard as the most significant electronic security threat to your company now?



Source: AT&T/Economist Intelligence Unit survey, March-April 2003

According to Meta Group's Mr Byrnes, management's "dirty little secret is that while they say risk analysis is important, it is not always done. And when it is, it's not done very well." Mr Byrnes is confident that risk analysis will get better, but "it's going to mean documenting meaningful information about actual loss in order to perform more precise analysis."

In the meantime, companies face the daunting challenge of remaining as up-to-date as possible on security threats and technology solutions, while keeping spending under control. The answer lies in a breakthrough in the business model of security. Today, like the network itself, state-of-the-art security is increasingly available on an outsourced basis from so-called "managed services" providers. Companies can hand off management of all or part of their security programme to outside partners–in effect, letting experts sweat the details such as 24-hour monitoring, scanning, incident response and network maintenance.

Like all IT outsourcing, managed security services afford increased control over security spending while, at the same time, providing access to deep skills without the need to recruit and train dedicated staff. Market growth expectations certainly underscore the appeal of managed security services. Forrester Research predicts that spending on services in Europe will surge at a compound annual growth rate (CAGR) of 37% from 2003 to 2008[2], while in the US, Forrester pegs CAGR growth at 47.9% annually between 2002 and 2006[3].

Why would anybody want to hand over something as proprietary as security to an outsider?
Like all partnering, it comes down to focus, skills, and resource allocation. "Managed services represent a rationalisation of security architectures," says Forrester's Ms Koetzle. "As companies better quantify risks and returns, firms will seize on the cost savings and increased expertise that managed services provide."

As pointed out in Networking and Business Strategy, the first paper in this series, outsourcing doesn't just move salaries and equipment off the balance sheet. It also transfers R&D costs. That's because a managed services model allows a company to leverage the ever-increasing expertise of a service provider.

Technology Tools

Technology may not be the whole answer to security worries, but it's still essential. The most popular line of security defence for the majority of survey respondents is a "firewall," or a combination of hardware and software tools that prevents inappropriate outside connections to company resources.

As larger numbers of users log into networks, companies need to know who is accessing specific applications–and that the person really is who they say they are. One of the most commonly used techniques is so-called token authentication. At login, users must provide something they know (a password or PIN) and

[2] Europe's Managed IT Security Market Takes Off, May 2003, Forrester Research Inc.
[3] IT Security's Awkward Adolescence, August 2002, Forrester Research, Inc.

something they possess (an authenticator). Such "two-factor" protection schemes provide much more reliable authentication than static passwords. The double-whammy of a secret password and constantly changing token code makes it much harder for hackers to gain access to authentication credentials.

Token authentication is just one of the tools gaining favour as a means of protecting networks. So-called Intrusion Detection Systems help identify attacks by flagging suspicious connections and other traffic anomalies. A growing category of Intrusion Prediction Systems can prevent attacks before they occur. Network Scanning tools let companies test their own networks-and those of their partners–for security holes and identify necessary fixes to security infrastructure. Data encryption, using a growing variety of techniques, makes it impossible for eavesdroppers to decipher electronic communications. And biometrics promises more personal authentication strategies, where fingerprints, for instance, could be used to validate users logging on to networks.

Ultimately, however, responsibility for security will migrate more and more to the network itself. According to Ed Amoroso, AT&T's chief information security officer, layering firewalls and intrusion detection systems on top of an insecure foundation doesn't really solve security problems. "You still may not pick up anything but the most trivial security attack," he says. By contrast, moving security mechanisms to the network level allows data to be gathered and correlated that not only help analyse information after an attack but also help predict and prevent future attacks.

In the next three to four years, predicts Dr Amoroso, a growing number of companies will embrace the notion of "holistic" security, where the network is designed from the ground up for security and even monitors itself for vulnerabilities. Such a network would include "network" and "application" firewalls that cut across the network as opposed to just surrounding its edges. This holistic design would also focus on maximising the network's tolerance for failure: a good network should not come down entirely because of one attack.

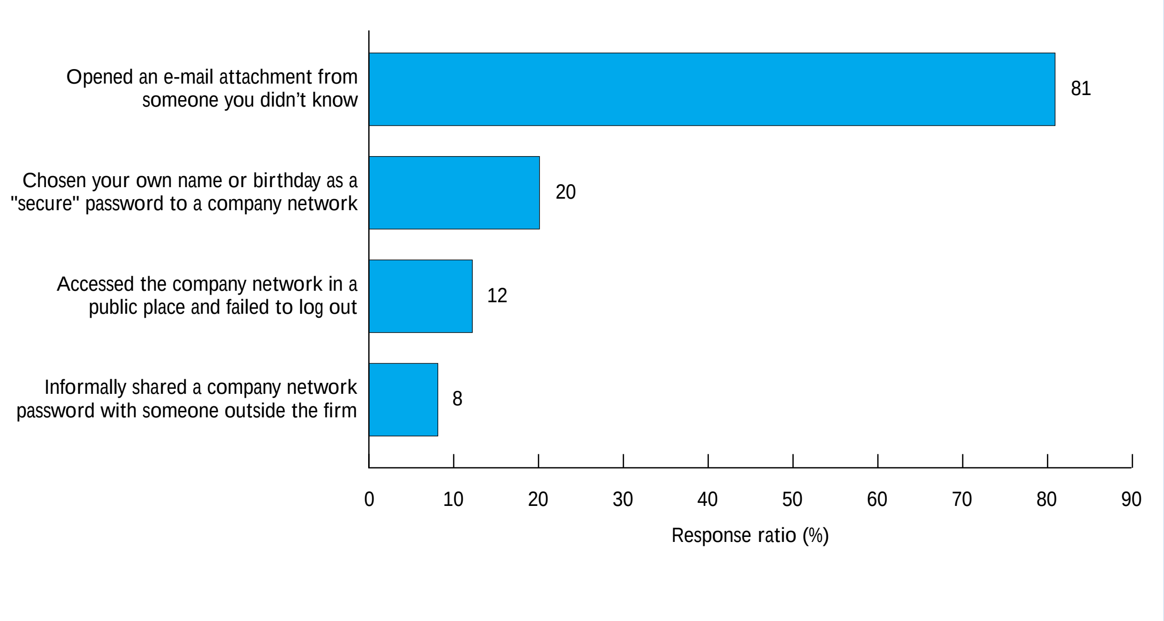
People problems

Managed security providers cannot resolve every threat, however. Indeed, arguably the biggest source of security breaches has nothing to do with installing and managing technology. The greatest weakness in the corporate security infrastructure is us.

Kevin Mitnick, a notorious US hacker, did not use technology to break into networks–he coaxed people into telling him information that let him march right in. The second annual survey of office scruples conducted by the organisers of Infosecurity Europe, the largest security conference in Europe, found that an astonishing 90% of office workers using London's Waterloo Station gave away their computer password to a surveyor in exchange for a cheap pen. "No amount of technology will be successful in protecting an organisation if employees are naïve, poorly trained or are not made aware of the impact of security violations," says Tamar Beck, director of Infosecurity Europe.

The survey respondents for this article reinforce the point–even at the most senior level, people make mistakes.

How many of the following security mistakes have you made in the last year? Check as many as apply.



Source: AT&T/Economist Intelligence Unit survey, March-April 2003

One way around the problem is to reduce reliance on human decisions. "Policy-based access control" mechanisms are just one of the technologies that companies now use to minimise the mistakes employees can make. One common tool, for instance, prevents employees from logging into the network if their anti-virus software is out of date. Network-enforced mechanisms such as this–while they don't eliminate the danger of human error or attack–harness smart technology to minimise risks.

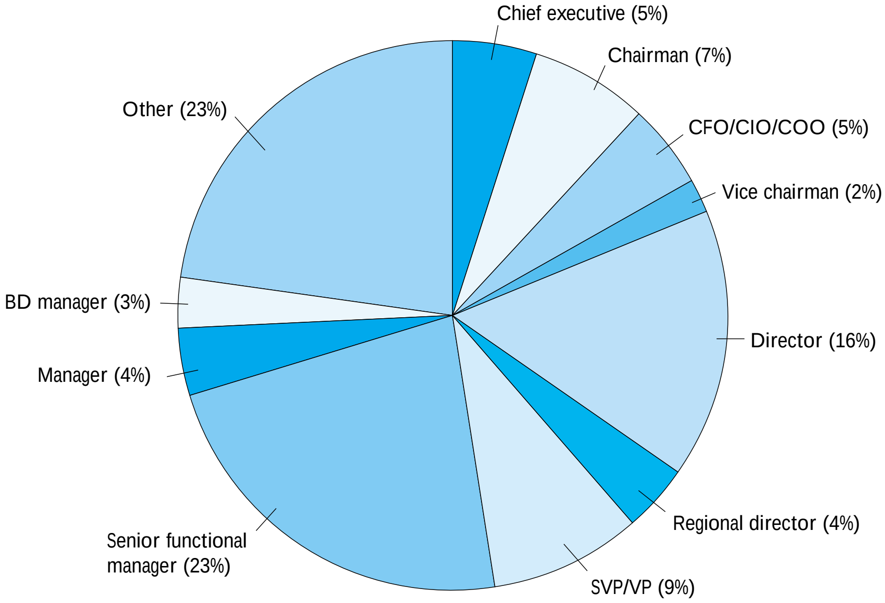
But the lesson is clear. Meta Group's Mr Byrnes estimates that "30% of IT security relates to technology, and 70% relates to people and practices". According to Forrester's Ms Koetzle: "Technology alone can't address one of the most difficult aspects of any security programme, the human element. In the end, it is usually people who make the simple mistakes–or commit the crimes–that lead to most security breakdowns."

Appendix: Survey Results

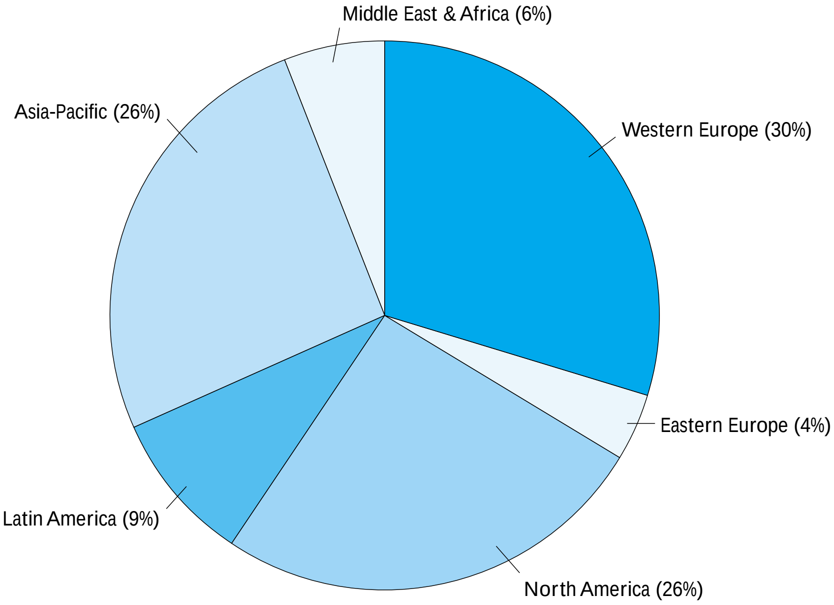
237 executives worldwide participated in an online survey on network security for this white paper. Our thanks are due to everyone who participated.

Respondent demographics

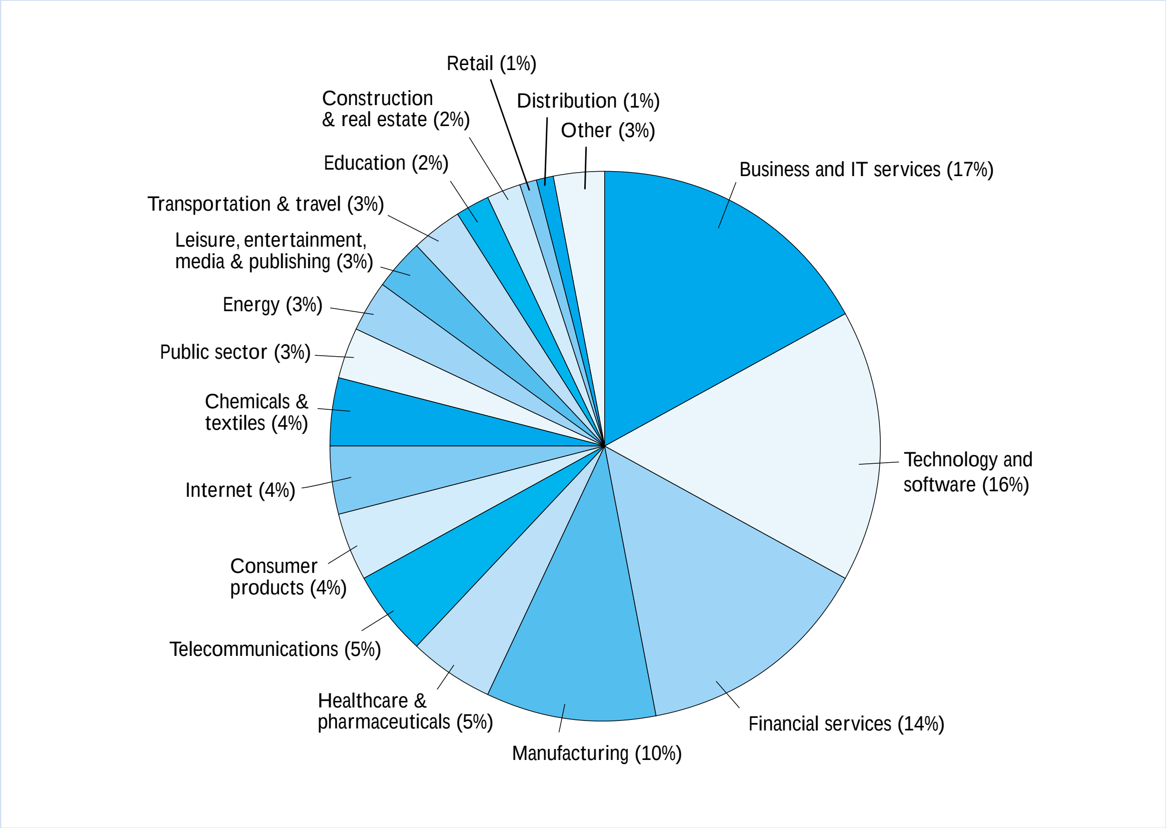
Job title



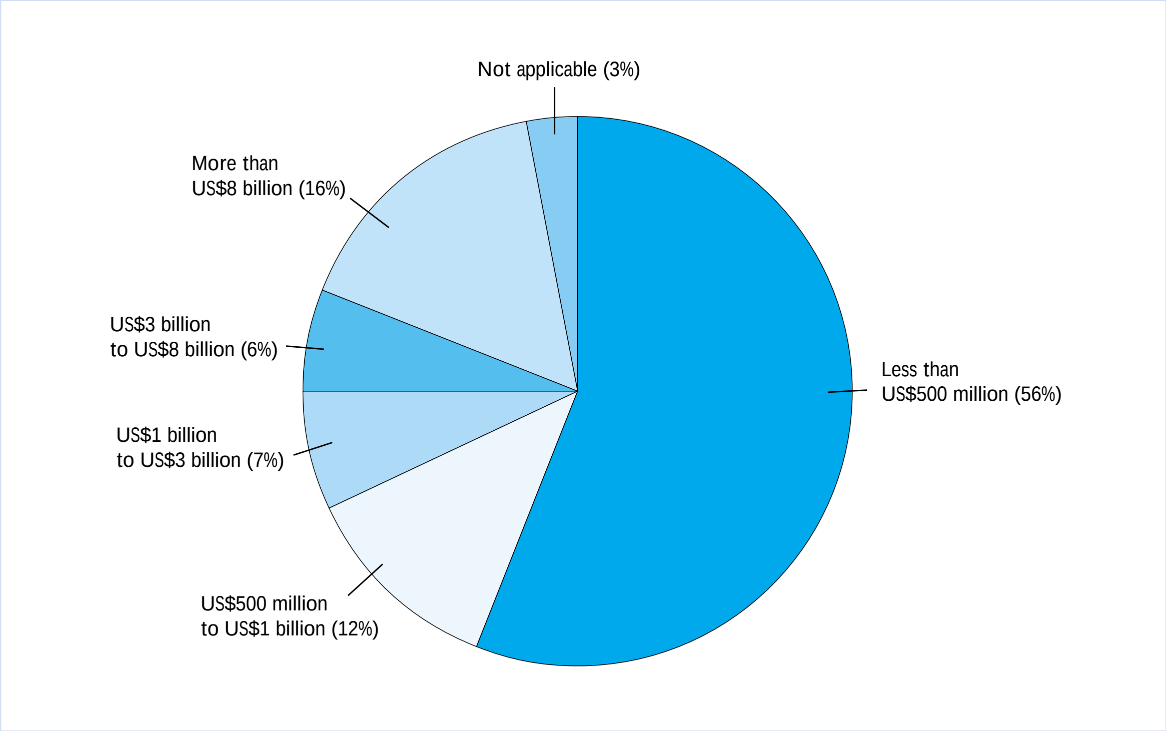
Geographical region



Industry

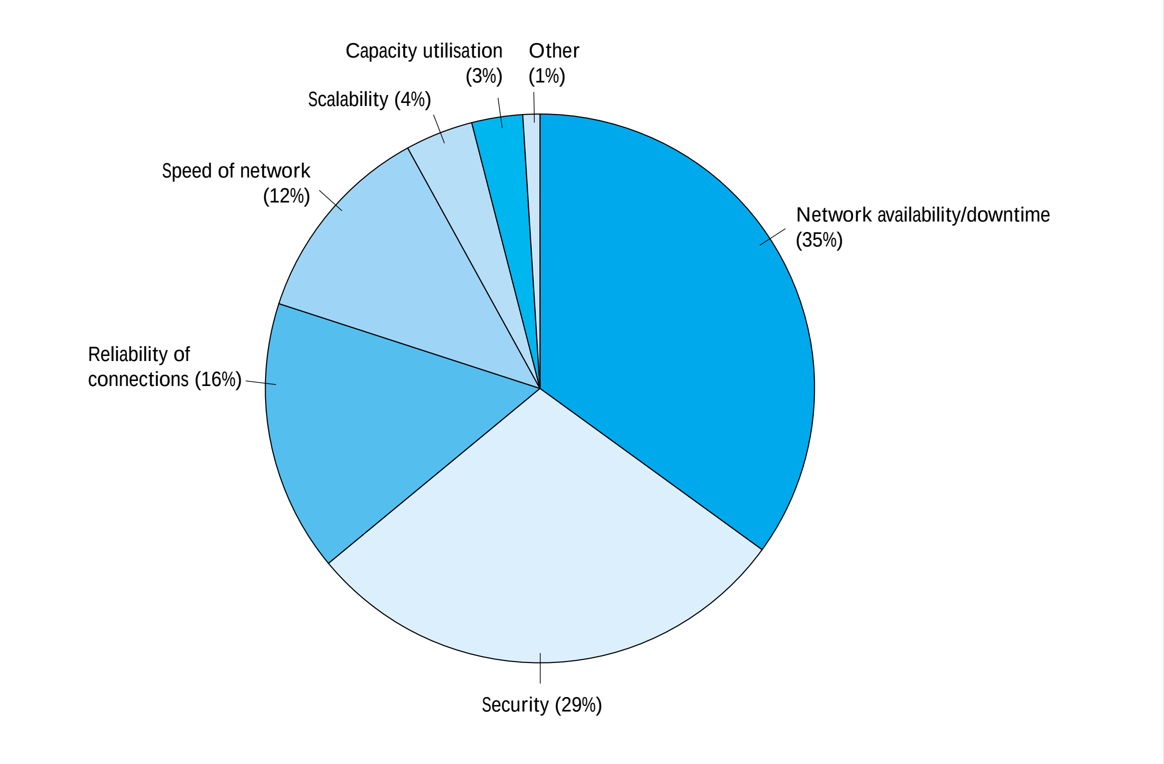


Annual revenues (US$, 2001)

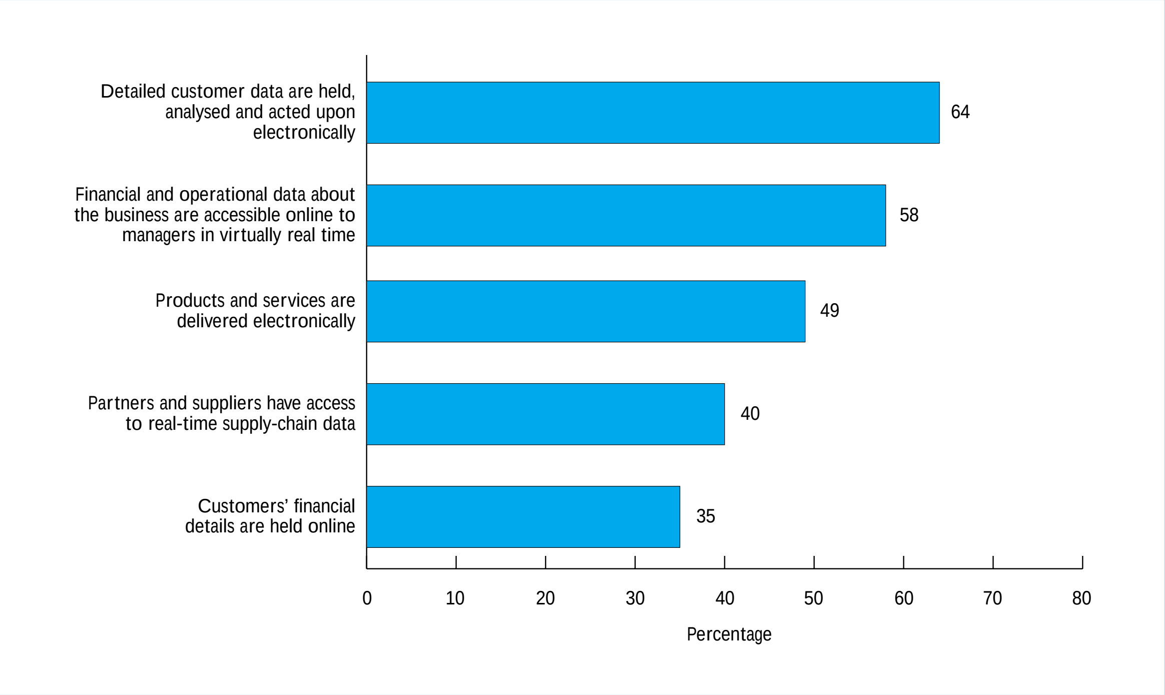


Survey questions

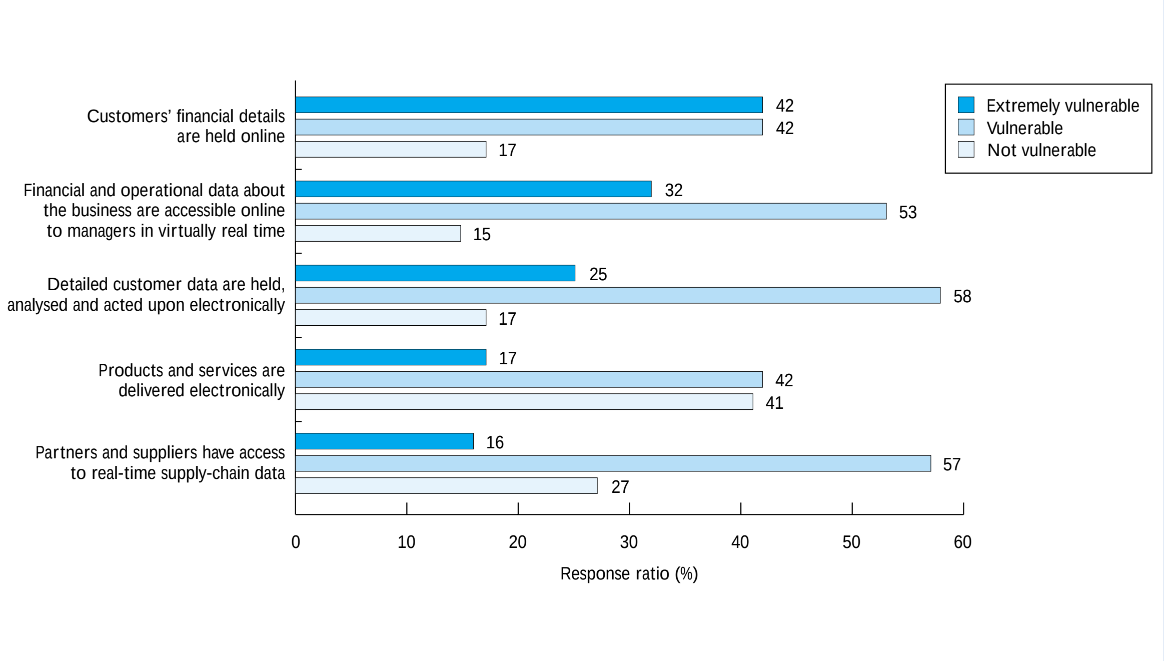
What network performance attribute is most important to your business?



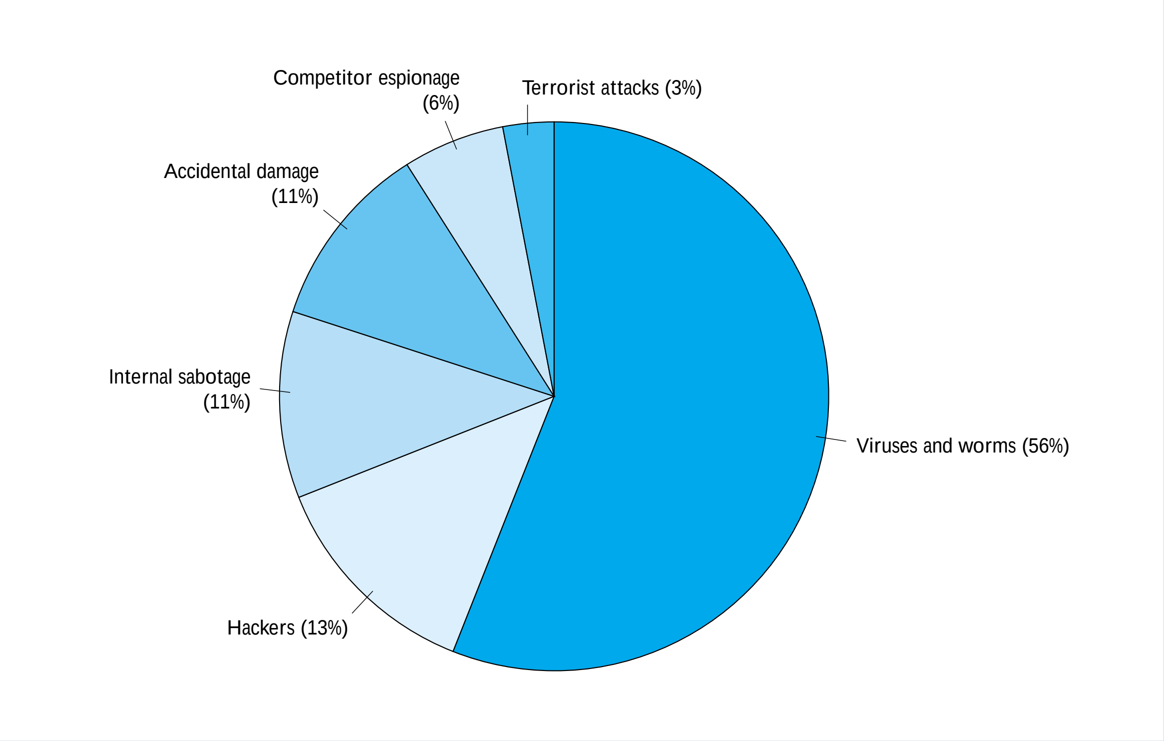
Which of the following technology-related goals does your company have? Check as many as apply.



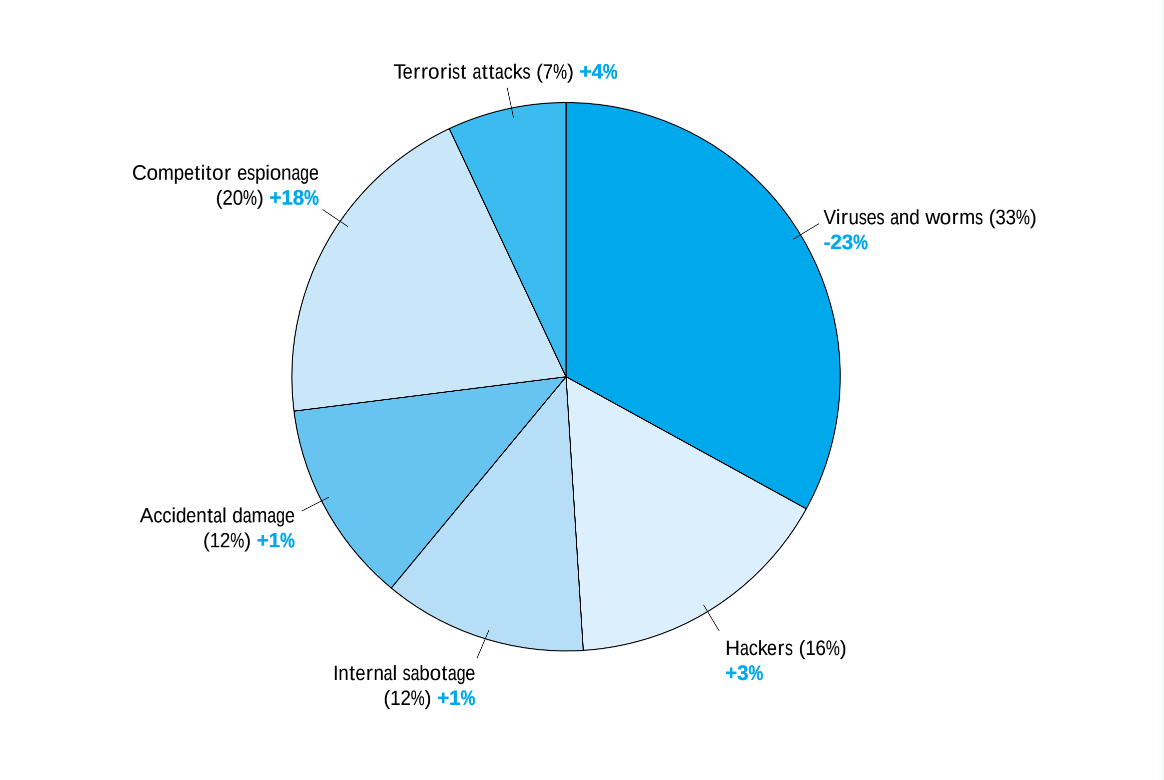
How vulnerable do the following corporate attributes leave firms to breaches in electronic security, in your view?



Which do you regard as the most significant electronic security threat to your company now?

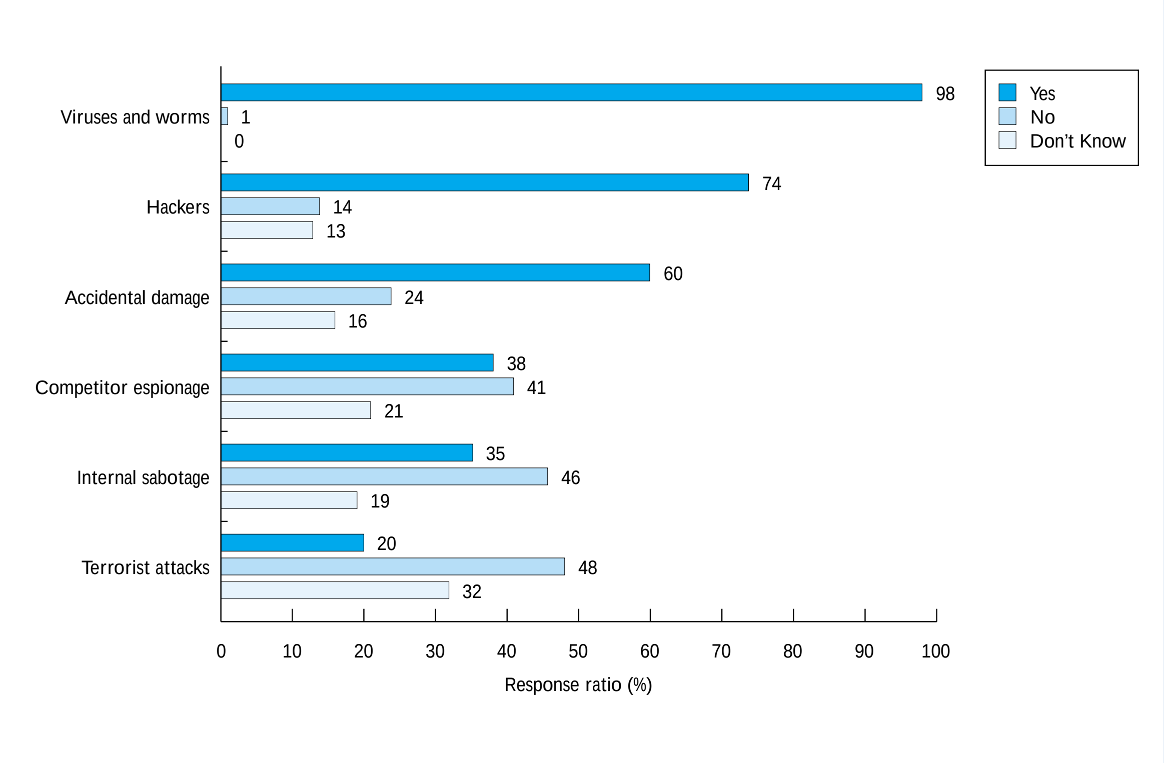


Which do you believe will be the most significant electronic security threat to your company in two years' time?

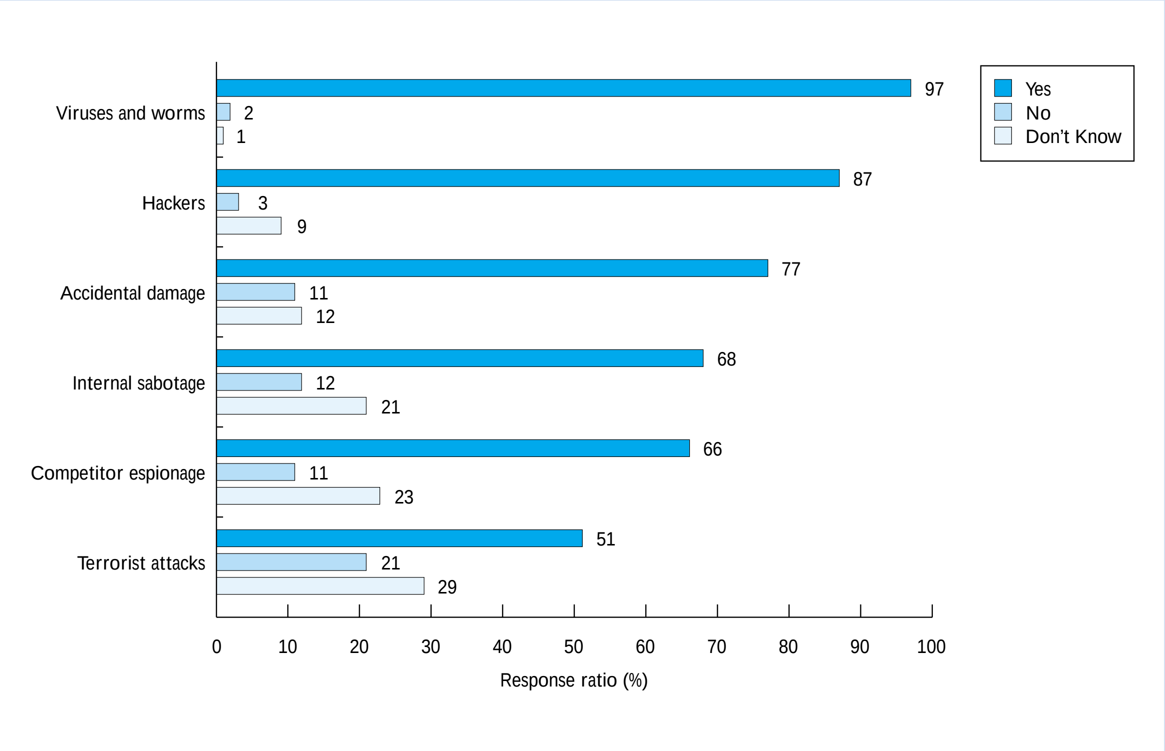


% in blue denotes the change in perception compared with 2 years previous.

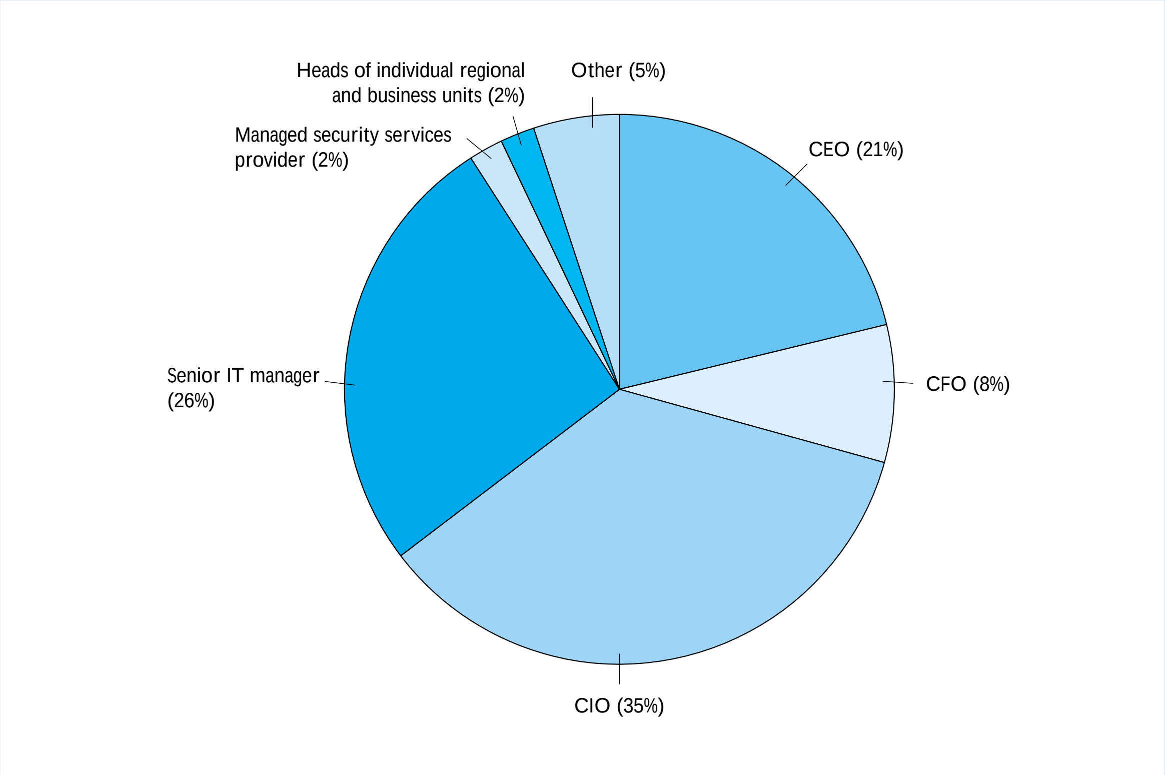
Has your organisation already installed technology to cope with the following electronic security threats?



In two years' time, will your organisation have installed technology to cope with the following electronic security threats?

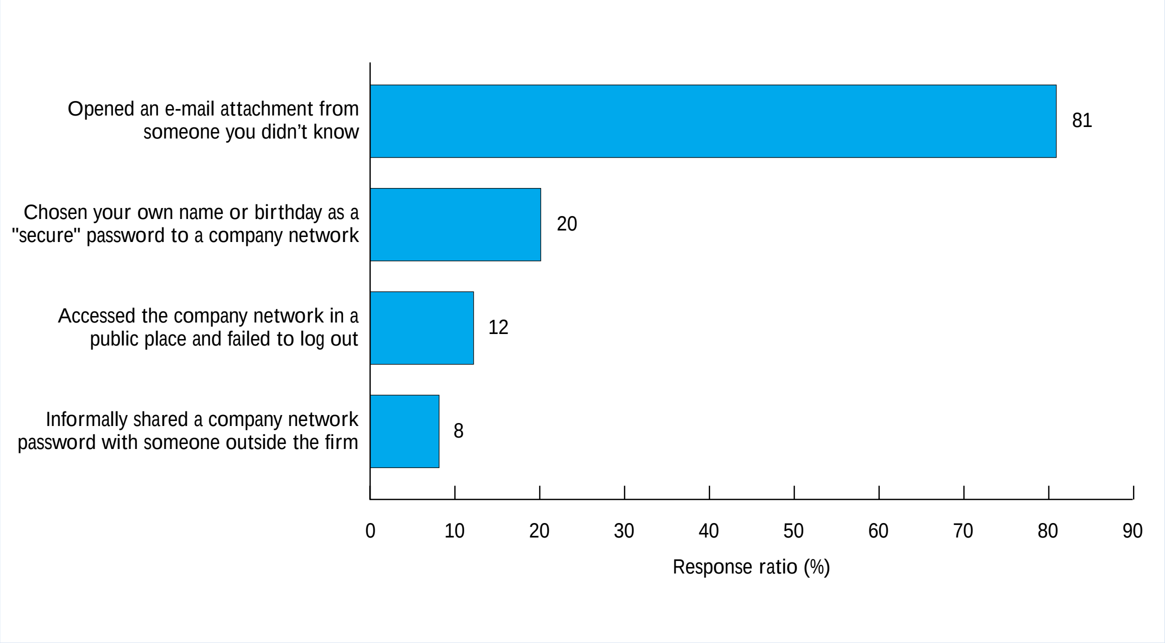


Who is in charge of decisions regarding electronic security policies at your firm?

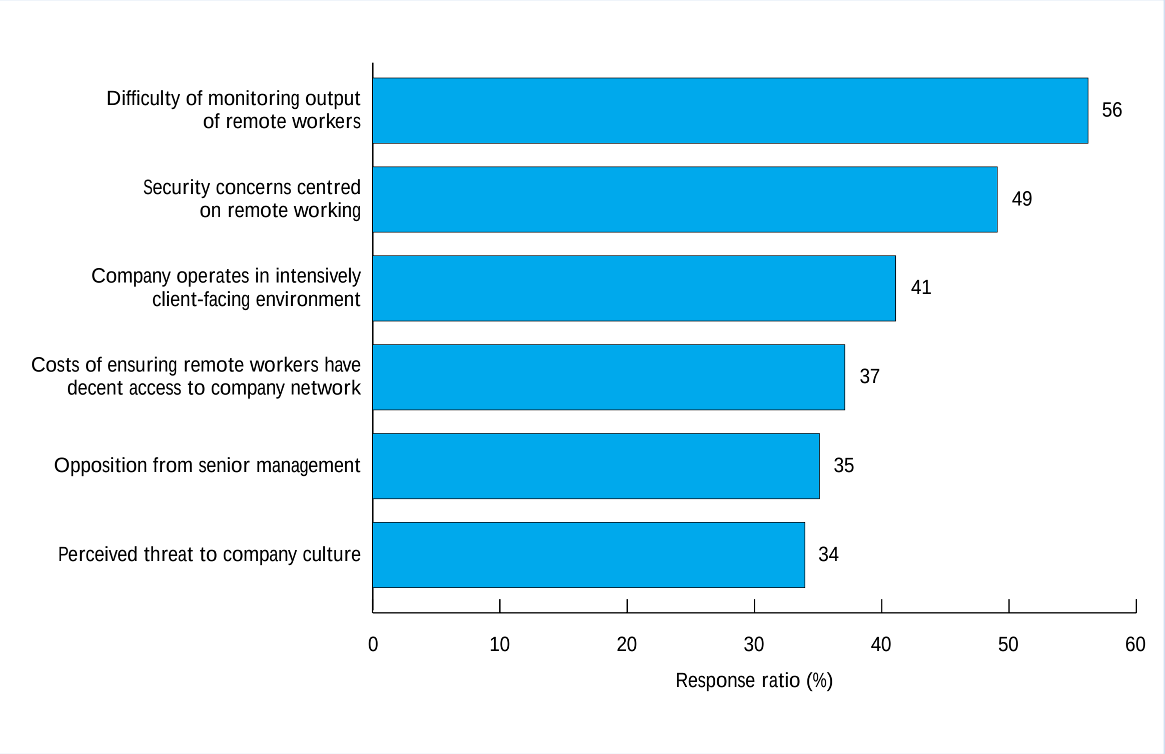


POINT OF VIEW

How many of the following security mistakes have you made in the last year? Check as many as apply.



What are the main obstacles to implementing remote working in your company? Check up to three obstacles.



To learn more about AT&T Services, contact your local AT&T representative, or visit our web site at **www.att.com/emea**

www.att.com/emea

ATT-WP-003
09/2003