E-commerce demanding strong network security

More people than ever are buying goods over the Internet. December 2005 was the first Christmas that the volume of online trade had a real impact on high street retailers. However, e-commerce strength is fragile; the public remains concerned about the security of online transactions.

One online retailer said that a denial of service attack would be equivalent to its high street stores being forced to shut.

Secure e-commerce depends on trust in the networks that carry confidential information, including credit card details. Technology offers benefits for businesses and customers, but without secure controls the benefits will not be realised.

80% of UK businesses now have a web-site; among large firms the figure is 93%. Most web-sites accept orders online (up to 73% overall, based on 2004 data). Most of these use payment service providers; only 13% of web-sites overall (but two-thirds of those for very large companies) take financial transactions online.

Is protecting customer information an important driver of security expenditure?

The increasing volumes of online business are raising the priority given to protection of customer data. Nine-tenths of firms considered this important or very important, the strongest justification for security expenditure.

Protection of customer information is underpinned by controls and accurate data. Nine-tenths of UK businesses also recognise the importance of data integrity. In contrast, in only three-fifths is security spend driven by enabling business opportunities.

A manufacturer automated its links with its suppliers. In the process, it removed many of the manual controls it previously used. This brought efficiency benefits, but increased the need for accurate and reliable data.

Incidents disrupt business

Overall, the number of businesses suffering network security incidents is consistent with those observed in 2004. However, when breaches do occur, their impact is more significant.

A retailer's web-site was compromised. As a result customers were unable to access the site for three days and orders were lost.

How many UK businesses' networks were attacked by an outsider in the last year?

<table>
<thead>
<tr>
<th>ISBS 2006 - large businesses</th>
<th>ISBS 2006 - overall</th>
<th>ISBS 2004 - overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>1%</td>
<td>2%</td>
<td>4%</td>
</tr>
<tr>
<td>22%</td>
<td>26%</td>
<td>2%</td>
</tr>
<tr>
<td>74%</td>
<td>83%</td>
<td>9%</td>
</tr>
</tbody>
</table>

The number of attacks is rising; over a quarter of firms affected by attempts to break into their networks said they suffered at least one significant attempt every day. Telecoms providers are particular targets; two-fifths experienced attacks, and more than half of these had several significant attacks a day.

Network security attacks were the cause of 7% of the worst security incidents of the year. Roughly half of these were described as serious. Three-fifths resulted in loss of Internet connectivity, and a quarter caused more than a day’s business disruption. One in ten led to customer complaints. Network security breaches did not, however, tend to cost much to fix; only 5% spent more than £1,000.

A manufacturer noticed heavy network traffic caused by an attack on its firewall. As a result, it had to shut down its service for several hours.

A concern is the rise in the number of companies reporting an attack on their Internet or telecommunications traffic. The businesses attacked tend to be those that take financial transactions online.
Transmissions beyond the firewall often not protected

The vast majority of UK businesses protect their web-sites. Nine-tenths of firms with a web-site now have a firewall. Reassuringly, all the web-sites that accept financial transactions are behind a firewall.

Nearly two-thirds of UK businesses also deploy intrusion detection software; in 2004, only a quarter of businesses used this technology. The improved network defences are encouraging. However, as networks are used for increasingly important business functions, additional controls need to be deployed.

A sports outlet that recently started accepting orders through its web-site said it had led them to examine their network security for the first time.

Many businesses are not using encryption to protect the confidentiality and integrity of the information they process. Less than two-thirds of web-sites accepting financial transactions encrypt the data they receive. In contrast, every transactional web-site run by a very large respondent uses encryption.

Traditional network boundaries are extending as companies make increased use of wireless networking, and start to implement Voice over IP telephony.

What defences do UK businesses have in place over their wireless networks?

<table>
<thead>
<tr>
<th>Defences</th>
<th>2006 - large businesses</th>
<th>2006 - overall</th>
<th>2004 - overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure placement of access points</td>
<td>45%</td>
<td>43%</td>
<td>35%</td>
</tr>
<tr>
<td>SSID changed</td>
<td>29%</td>
<td>29%</td>
<td>29%</td>
</tr>
<tr>
<td>Encrypted signals</td>
<td>29%</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>MAC filtering</td>
<td>16%</td>
<td>16%</td>
<td>18%</td>
</tr>
<tr>
<td>No controls</td>
<td>5%</td>
<td>6%</td>
<td>12%</td>
</tr>
</tbody>
</table>

Controls over authorised wireless networks have improved. The number of unprotected networks has halved since 2004. However, there is no room for complacency. One in five firms has no controls. What is more, simply changing the Service Set Identifier (SSID) of the access point will not deter a competent attacker for long.

There are more wireless access points in public places than two years ago. While these may be helpful to some mobile workers, they also represent a threat.

UK businesses seem to recognise this threat; only 12% allow staff access to their systems from these ‘hotspots’. Of those allowing access, three-fifths encrypt the transmissions by use of techniques such as Virtual Private Networks (VPNs). More than one in five large businesses permits access. These firms are also more likely to protect data by encrypting their transmissions; six out of every seven of them do so.

Voice over IP - Security not considered

Rather like wireless networking two years ago, the attraction of Voice over IP (VoIP) telephony is rising. VoIP offers firms the opportunity to use their existing data network infrastructure, to reduce telecommunications overheads.

At present, relatively few small businesses use VoIP; overall fewer than one in ten. However, three-tenths of large businesses have adopted VoIP, and more firms are planning to use it over the next year.

Are UK businesses adopting Voice Over IP (VoIP) telephony?

Like wireless networking, VoIP offers limited security controls by default. Worryingly, few businesses are assessing the risks associated with use of the technology. Half of the businesses that have implemented VoIP did so without evaluating the security risks.

One organisation that had recently deployed VoIP conducted a penetration test. They were glad they had. The test found several important vulnerabilities which they were able to fix before they were exploited.

Businesses appear to recognise the benefits of VoIP. They would be wise to make sure they evaluate the associated security risks as well.

This report is printed on Mega Matt paper which is made from 50% recycled and 50% chlorine-free pulp from countries that operate strict reforestation policies.

Department of Trade and Industry. April 2006. URN 06/807.

Founded in 1975, Microsoft (Nasdaq “MSFT”) is the worldwide leader in software, services and solutions that help people and businesses realize their full potential. The security of customers’ computers and networks is a top priority, and Microsoft is committed to building software and services to better help protect customers and the industry.

For more information, see www.microsoft.com.