SECURITY SERVICES

Telcos get a look in

MARY LENNIGHAN

IN A TIME when the market is inundated with security providers, questions still remain over whether telecoms operators are best-placed to offer security solutions alongside network services.

According to a report published by the Yankee Group earlier this year, global revenues from managed security services are forecast to reach $3.7 billion by 2008, up from $1.5 billion in 2002 and $2.6 billion this year.

"Everyone is trying to get into [managed security]," says Nick Hutton, principal consultant at 360is, a security professional services provider. "It's a profitable, high-margin business for [the telcos]," he says, noting that those who succeed in building a volume business can make margins of 60%-80%.

But telecoms operators have a number of hurdles to surmount if they are to build profitable managed security businesses. Dealing with customers' bespoke security requirements requires a fundamental change in the way many telcos do business. Some have chosen to partner with security specialists. Telefónica resells McAfee security services, for example; while others like MCI and Cable & Wireless have swallowed up niche players to handle the security side of their business.

According to Lionel Lamy, research manager, European IT outsourcing and infrastructure services at IDC, the more bespoke business model of outsourcers and systems integrators gives them the slight edge over the telcos, which offer "more or less 100% standardised solutions." As a result, he says, telcos "will find [creating a volume business] difficult, but not impossible."

But telecoms operators certainly believe they are up to the challenge. "We always deliver standard solutions, but we customise them for every customer," says Martin Dipper, vice president, BT Infonet managed security services. Similarly, UK-based Energis employs a design consultant and creates a statement of requirements for each customer that it offers on top of its out-of-the-box solutions. "Every security solution we provide is a bespoke solution," says David McLinton, head of customer security at Energis' Security Professional Services division.

"Having the carrier take care of security at their end obviously means that although the garden gate is locked, your front door is open"

Energis has a managed security deal with UK retail giant Tesco, which forms part of a multi-million pound managed services contract, and is primarily dealing with customers of this scale at present. With smaller enterprises, McLinton acknowledges the need to "invest time and energy" to provide what they need.

Smaller customers use building block services, such as distributed denial of service (DDoS) protection, firewall and mail scanning, says Graham Starkins, head of Internet and security products at MCI Europe. For larger customers, "you can use those building blocks and add additional layers on top." Top-end customers need custom solutions, he adds.

But not everyone is convinced of the need for customised security solutions.

"I wouldn't say security is really that bespoke," says Greg Day, security analyst at McAfee. There are many standard solutions; only the specifics of the customer environment are bespoke, he adds.

A lot of AT&T customers have the same profile, says Joe Dauncey, lead security consultant, AT&T Business EMEA. Most need traditional firewall infrastructure, anti-virus and content filtering.

And all have to interface with the Internet, as well as their business partners. It adds up to a case for network-embedded security, say the operators.

"Security is not really an add-on. It needs to be built from the network up," says MCI's Starkins. "As we play in both the network-based and customer site-based security services area, we are able to architect and build the best solution to each area of security concern. This puts us in a stronger position than perhaps some MSSPs that are only able to build solutions in one area."

MCI completed the $105 million acquisition of US-based global network security specialist NetSec in February this year.

"It's a bit about not playing too far out of your box," says Starkins. MCI concentrates on its strengths—wide area network and perimeter security around that—while NetSec gets further into the customer's network, offering the equivalent security within the customer's LAN, he says.

And indeed, customers want "a clean pipe," where they know 100% of the traffic is "good traffic" and the telco deals with anything "bad," says Hutton at 360is.

However, he adds, there are a number of problems that prevent this from happening. "Having the carrier take care of security at their end obviously means that although the garden gate is locked, your front door is open," he says. Furthermore, "shared infrastructure and lack of strong enough compartmentalisation of one customer from another means that for many customers security in the network is not something they are comfortable enough with."

However, some security can be added to the network without these problems, including virus scanning, web proxies and DDOS protection. "But that is far from a completely clean feed," says Hutton.

But Dauncey at AT&T insists that network-based security is one area in which the telcos have the lead.

"In order to embed security into the network, you have to own and run the network," he says. "Managed security providers typically only own the security components, whereas the network providers are able to embed security components into the network infrastructure, which in turn underpins the IT infrastructure." For example, it's too late to deal with DDoS attacks with CPE, says Dauncey. You have to embed a DDoS

solution within the backbone. AT&T offers customers an Internet Protect service, which uses network data as its prime intelligence source, picking up traffic anomalies that could indicate security threats.

"The Logicas and EDSs are just coming from a different end," says Starkins at MCI. "They don't necessarily have a good story to tell in that area."

"There's continuing consolidation in the security market," says David Friedlander, a senior analyst at Forrester Research, who says there are hundreds of small security vendors and while lots of acquisitions have taken place, there are still lots of gaps that haven't been filled. "There's a need for more in-depth security management that reaches the endpoints and provides protection for roaming users," he says. "This could include managed client antivirus, client firewalls and secure VPN connectivity services."

"The telecoms providers may be in a good position to fill some of the gaps in the SME market, where they are closer to the customer," he says. "There's an opportunity to at least provide network security and mobile phone security services."

Colt Telecom's TotalPlus "virtual IT department" is a package of managed LAN services for SMEs that leans heavily on security features. Daryl Szebesta, senior director managed IT services, says more than 30% of customers take the full managed service.

Issues of equipment

One of the key hurdles facing carriers is the proliferation of legacy equipment and the reluctance of companies to throw away existing hardware and software. Ultimately, the customer wants someone to come in and manage what they already have, says Hutton at 360is. Firewalls and routers do not go out of date in three years.

Even once the operators have dealt with the existing equipment owned by the customer, they still have to ensure they can effectively manage the equipment.

Putting any box on a site increases the cost, notes Hutton, since the operator may have to go to that site to repair or upgrade equipment. In addition, this affects SLAs, since often the customer wants total availability of that box.

"There's no real solution to it," he says. For 24/7 coverage, the operator either charges more or tells the customer to buy two boxes. "The customer begins to understand where the cost lies in the service," he says. "It's really difficult to hit the low price point," he says, and that has nothing to do with the cost of the hardware.

In 110 countries, BT Infonet has a response time of 4-8 hours, says Dipper, but he adds, "We [also] have firewalls in Eritrea and Uganda." In these kinds of locations, BT Infonet tells customers to "bundle up on the hardware."

"The hardware's so cheap now," he adds.

The company sets SLAs accordingly. "It's not rocket science. If they have to be up 100% of the time, you put spare equipment there," says Dipper.

MCI has adopted a similar solution. Customers can buy two firewalls, for example, and keep one on "cold standby" in case the other fails. Or the customer can opt for MCI's high availability option, where two firewalls are run at the same time.

"It's the same proposition as network connectivity itself," says Starkins.

But while operators like MCI are taking on the security business by acquiring specialists like NetSec, not everyone is taking it this far.

"Everybody is partnering with everyone around security," says IDC's Lamy, adding that it's a question of perception: it is better for the telco to portray itself as having the right relationship with the right people, he says.

Forrester's Friedlander agrees, noting that "enterprise buyers are less likely to turn to telecoms than security providers."

Indeed, in September, McAfee announced its Clean Pipes consortium, putting together a group of global service providers to focus on the development of security solutions and to act as a channel to market for McAfee.

The group comprises Cable & Wireless, Telefónica, China Netcom, KPN and a number of unnamed operators, one of which is believed to be BT.

"It's a very logical method for us to go to the customer market," says Greg Day. "Customers are looking to simplify their environment." Day adds that every corporate customer the company talks to is saying "we are simplifying down the number of vendors." Customers won't just buy components any more.

IDC's Lamy agrees. Managed security is not purchased as a separate service as much as had been anticipated, he says. "People tend to bundle services."

A question of trust

Many of the issues facing telecoms operators in the managed security space centre on sociological, rather than technical, questions.

Most telcos don't have a deep trust relationship with the customer, says Hutton at 360is. "Security is a very intimate thing... telcos will only get good managed security deals with customers who trust them."

A key issue for the customer is "finding a vendor they trust," agrees Energis' McLinton. "Why would you trust your telco with security? They are two different mindsets."

Energis attempts to circumvent this problem through its specialist security division, Security Professional Services.

"You can't forget the consultancy side," agrees BT Infonet's Dipper. "They trust us with the day-to-day network," he says, adding that BT has its own sales force dedicated to security and also sends consultants out worldwide. ■

QUESTIONS MANAGED SECURITY SERVICE PROVIDERS SHOULD BE ASKING

1. Do you currently have a deep trust relationship with your target customers? If not then what is your plan for building one. Start early, it takes a long time.
2. Are your security engineers suitable for face-to-face meetings with customers? Many customers will want to see who is managing their security before awarding trust, this is a face-to-face process.
3. How will you supply & support security infrastructure that is off-net in countries where you have no physical operations?
4. What are your own redundancy and disaster recovery arrangements?
5. What staff screening/vetting will you be doing to assure the customer that your security engineers are suitable?
6. What are the procedures that govern how you will react when a security event is detected?
7. Where does your responsibility begin and end, what role does the customer play?
8. What are your own internal controls for access to customer confidential information?
9. Password storage, access to logs, access to customer contact details must all be properly controlled.
10. What is your change control and rollback regime? Knowing who made which customer equipment changes when and why is critical to dispute resolution, and there WILL be a dispute sooner or later.
11. How will you charge for extra services that are beyond the scope of the service description?
12. What will be your security SLA? Incident response times, frequency of reporting, uptime and availability of the service?

Source: 360is.com