Security For All

With the converged networks of the future, security will not only be built in, it will become one of the applications on the network. It behooves companies to pay closer and closer attention to cabling infrastructure issues.

By Martin Slofstra

Whether it is cabling professionals, IT departments or senior executives, network security has become everybody's business for it has never been more complicated. There are networks that are or need to be secure, protecting your network from hackers, viruses and worms, and other threats to your data.

There are also networks used for security, which may include video surveillance and are used to protect a premise or for detecting intruders.

And there are the people involved in the security in the organization, from cabling professionals, to IT departments, to telecom specialists, to those in business units. Everybody seems to have a stake in network security and everybody has a role to play.

And it is not hard to see why. In the days of converged networks, companies must rethink everything from their cabling infrastructure to their software systems.

"The fact is that all networks are converging on an IP platform," says Francis Richard, a structured cabling specialist at Cerco Cable Inc., a value-added distributor of cable products based in Montreal. Whether it is the Internet, Heating/Ventilation/Air Conditioning (HVAC), fire alarm or video surveillance systems, the convergence of all these previously separate applications is causing organizations to change how it perceives security from an IT-only issue to a company-wide concern. Sometimes this can create problems. An IT department, for example, may focus on different requirements than a facilities manager, and it behooves all organizations to view security requirements in the context of the overall business strategy, balancing present and future network needs with overall goals.

Richard notes that inter-departmental conflicts and IT may look at short-term solutions because the typical application lasts only a few years, and that tends to be their frame of reference. In other words, the application dictates the type of cabling that is used, and in some cases, a temporary solution is put in place.

Differing opinions

A cabling expert, however, may look at the infrastructure from a 10-to-20-year horizon, and that can create a difference in opinion.

In defense of the IT department, however, the application is only one part of the security equation. "There isn't necessarily one right or wrong answer," says Stephen Ibaraki, a Vancouver-based IT consultant and president of the Canadian Information Processing Society. Important questions need to be asked involving business domain, model and environment; applications and infrastructure; value of the information; risk analysis for a security breach; security processes and technology that are in

Without question, the cabling experts and the IT departments need to combine their efforts. The concept of security has migrated from upper layer security to include a real focus on physical layer security.

place including sufficient training, the triad of people, process, and technology; doing a more formal security assessment using one of the available tools such as MSAT; and much more, he says.

"At minimum, it's good to seek out a variety of opinions from the IT professional community which are a key source of security information," says Ibaraki.

Without question though, the cabling experts and the IT departments need to combine their efforts. The concept of security has migrated from upper layer security to include a real focus on physical layer security. Users are securing their data by first securing their cabling, and that is a good foundational place to start. Then they need to work their way up.

Enterprise security software is solving a lot of the problems, says Sam Curry, vice-president, product management, security management business unit at CA in Islandia, N.Y. (formerly Computer Associates). Whether it is managing all the threats to computer systems, or it is card access for managing who is coming and going, to identity management, auditing a network and generating statistics, all the tools an IT department needs to manage security are available.

Curry says organizations need to see network security in a wider context. "I have a network security problem is seldom the starting point, it's I need to improve my uptime or regulatory compliance," he says. Explaining it in those terms or as part of a business case — whether it is increasing your uptime or regulatory compliance — will have a better chance of getting everybody in the organization on board.

Security was once a separate function with IT working on it isolation, but regulatory compliance is the catalyst to getting on the business agenda.

Yet roadblocks also exist. Curry cautions a lack of interoperability between different vendors equipment could inhibit the user's ability to manage the security function although the advent of standards will make this work.

There is some question whether traditional enterprise-class security products can meet the demands of the largest IP networks in the world, and whether IP actually makes them more vulnerable than ever before.

"Is IP more secure than non-IP? The jury is still out on that," says CA's Curry. "IP is a simple redundant protocol with a tremendous upside. It's attractive because it's cheaper, it's everywhere and it's very simplistic. But that same ubiquity makes it subject to attacks everywhere. It's a trade-off."

According to results of a global survey conducted by the Economist Intelligence Unit and commissioned by AT&T of 395 executives across the world, 60% of Canadian executives and 52% of global executives believe having a converged network gives their companies better protection against IT security breaches. The technology also brings network defenses to new levels of sophistication and reliability, equipping organizations with incomparably better tools to protect the network than they were even in the late 1990s, the report states.

The report also alludes to another trend. More and more executives are paying attention to network security issues. "Without question, 9-11 catapulted the security issue to front and center for executives," says Steven Taylor, vice president of sales for AT&T Global Services Canada, and the effects will be lasting. Although Canadian organizations tend towards a business-as-usual stance, there is a global dimension to network security that cannot be overlooked. Most threats to the network, whether it is hacker activity or virus-writers, or freak weather conditions or a terrorist attack, can occur anywhere, and Canada is as vulnerable to these threats as any country.

Part of the problem may be a lack of clear definition of network security. The trend overwhelmingly has been to define computer security broadly, and service-providers often include business continuity and disaster recovery, and the capability to move to off-site back-up network as part of their offerings.

Executives seeking to get a good sense of how their networks stack up from a security perspective may want to consider getting "a full-blown security audit" which evaluates all the facilities, processes and the security tools it has its disposal.

Then there is also the issue of cost. While most organizations realize they must go to converged networks, it may require a large up front investment and there is always the issue of legacy systems which can pulling security professionals into two different directions. "For corporations trying to manage these concerns, security raises significant issues of resource allocation," says David Denault, general manager of AT&T Global Services Canada.

"The increasing number of applications running across the network drives cost,

Sunshine Village Ski and Snowboard Resort in Banff, National Park, Alta., has deployed an IP network that facilitates voice, data and video communications.

Photo courtesy of Sunshine Village Ski and Snowboard Resort

and security personnel require a high level of expertise and ongoing training."

Michael Murphy, vice-president and general manager of Symantec (Canada) Corp., a supplier of enterprise security software products, points out that companies have become much better at managing their security infrastructure.

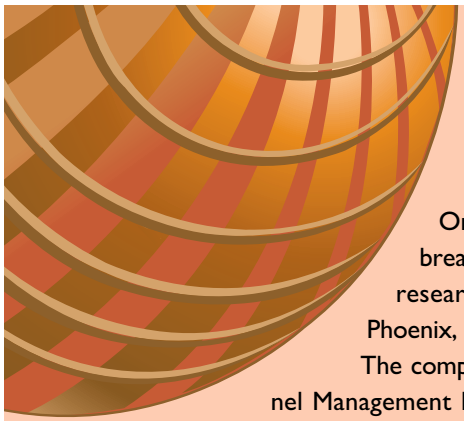
He acknowledges the high level of executive awarenessand lots of available product, but where organizations struggle is in the areas of implementation. "Corporations understand the risks, but they are also trying to do more with less. We have spent a lot on hardware and software and now we need to implement, which includes how to integrate it all and make it work together."

Meanwhile, networks continue to grow wildly. There is the core, there is the perimeter and remote locations, and today there is also wireless.

There has been a three-fold increase in the number of threats to systems since 2005, which is directly attributable to the proliferation of devices such as smart phones, personal digital assistants and handheld computers. And whereas the previous target was the operating system, the target is now the data that resides on these systems, much of which is private and confidential, says Murphy.

Corporations, however, that have bitten the bullet and made the necessary investments in properly secured converged networks may not see the benefits until later. Although the initial costs in equipment may be greater, as more and more standards come on board, the newer IP-based are more interoperable, and that alone can lead to enormous savings in manageability, says

There has been a three-fold increase in the number of threats to systems since 2005, which is directly attributable to the proliferation of devices such as smart phones, personal digital assistants and handheld computers.



TELEVERDE FINDS IT SECURITY CONCERNS RECOGNIZE NO BORDERS

Organizations in Canada and the U.S. express similar concerns about IT security breaches and rate security as a significant ongoing priority, according to separate research studies completed by Televerde, a marketing intelligence firm based in Phoenix, Ariz.

The company recently completed a Canadian survey on behalf of Quebec-based Channel Management International (CMI), then compared data from U.S. companies with similar demographics to compare and contrast the Canadian results.

All respondents were IT professionals with decision-making authority for new technology acquisitions.

Most significantly, the research identified the following common key areas of concern: protecting wireless devices used by employees within and outside of the enterprise that may threaten an organization's data; compliance with security regulations such as Sarbanes-Oxley, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), and the Health Insurance Portability and Accountability Act (HIPAA); spam filtering and control, among others; and Internet security, including virus protection.

Neither American nor Canadian companies feel confident in their attack response and prevention measures. One in four respondents expressed an immediate need to strengthen IT security, and none rated their ability to protect against external and internal threats as a strong point.

But IT decision-makers on both sides of the border are responding by making security issues a priority. More than 75% of participants plan to spend at least $75,000 for security technology investments in the next 12 months.

Richard from Cerco Cable.

Down the road, the savings become even more apparent. The benefits of digital and networked video mean that real-time or stored video surveillance images can be accessed wherever and whenever they are needed.

It is not just about security of the network anymore, it is also about using the network for security. Security systems now have the same flexibility and manageability of today's telephone and computer systems (LANs, WANs, Ethernet and Internet Protocol), and that has organizations rethinking how security systems can be deployed.

The future is now

Video surveillance, access control, alarm and paging systems, network authentication and physical security, once separate, can now all integrate with each other. Video is having a special role in these networks. With bandwidth now abundant and new advances in file compression techniques, more and more companies see an opportunity to add a capability for video to their networks.

Curiously, it is operators of ski resorts in Canada that are leading the way. Richard knows of one CEO at a Mont Tremblant-based ski resort who has the entire facility cabled for video, and he is able to use his laptop to "look into" the network from anywhere he has an Internet connection. Other ski resorts, meanwhile, are beginning to deliver complex multimedia applications. Sunshine Village Ski and Snowboard Resort in Banff National Park, Alta., for example, has deployed a comprehensive, IP network that facilitates voice, data and video communications. Applications include voice, point-of-sale, reservations and video surveillance, all on the same network.

"We've overbuilt our fiber to allow for the increase in traffic," says Tim Hodgkinson, Sunshine Village's supervisor

AT&T SURVEY EXAMINES SECURITY AWARENESS LEVEL OF CANADIAN EXECS

Security may be regarded by executives in Canada as the single most important attribute of their network, however, there is still some work to be done in terms of creating awareness, according to the results of AT&T Canada survey of 100 Canadian business executives regarding business continuity and security planning.

The report indicates 66% of respondents say business continuity is a priority, with 30% saying it has moved up to the priority list due to recent natural disasters or terrorist threats.

Despite the fact that 31% of respondents have suffered a natural or man-made disaster, a surprising 34% do not consider business continuity to be a priority. Additionally, only 9% of all surveyed executives are implementing business continuity globally.

While David Denault, president and general manager, AT&T Global Services Canada, describes some of the results as 'scary,'— a full one-quarter of IT executives do not have a business continuity/security plan, for example — the good news is that IT executives are beginning to take a more proactive stance.

When asked about the biggest issue around business continuity, security was at the top of the list. The survey indicates that 71% believe that viruses and worms are the most significant security threats followed by hackers at 43%.

As a result, three out of four executives indicated security is part of the company's business continuity plan.

Canadian end-users may lag in terms of overall awareness, but they are beginning to take a much more thorough look at their entire networks, Denault says.

"While peripheral defenses like firewalls, intrusion detection systems, anti-virus programs and spam filters play an important role, they are not enough," he says. "When you use the network itself as the first line of defense, you shift your posture from reactive to proactive."

Denault adds that a centralized approach to network security delivers greater cost efficiency and makes it easier to manage.

of information systems. Hodgkinson, who can usually be seen dressed in work boots and work pants, actually helped lay the cable himself.

He says he had a huge advantage for with no legacy system in place, he could go straight to state-of-the-art, building or what he calls a "Ferrari network."

Hodskinson stresses the importance of video communications (the network supports 35 cameras for monitoring and broadcasting various locations). While skiers can see how long the line-ups are or what the current ski conditions are by accessing the ski resort's Web site, the system can also be used for video surveillance and a variety of other security uses.

Sunshine's Web site can also be used for video surveillance.

With the converged networks of the future, security will not only be built in, it will become one of the applications on the network. It behooves companies to pay closer and closer attention to cabling infrastructure issues. And cable quality has become more important than ever, and cable professionals need to take note.

Structured cabling is at the heart of every security network. If the wrong cabling installation is chosen, the consequences can affect an organization's bottom line. With installations lasting from 10 to 20 years, planning for the future applications is essential.

And it is buyer beware. Signal strength (video needs a minimum of 200-250 MHz, but some manufacturers try to pass off cable that runs at only 100 MHz) Most good cables run at 500 MHz. "Always go to the high-performance cable and get a certified product. Even better get a certified installer if you want it done right," says Richard.

And at the end of the day, everybody has a stake in a good cabling infrastructure. Cabling people know how important it is to have a good solid cabling infrastructure; IT professionals know that it is much more time-consuming and inconvenient to change the cable infrastructure than to change the network equipment; business users are concerned about the medium used to transport the information and want the information gets to them faster; and, executives know they will soon be out of business if the network goes down. CNS

Martin Slofstra is a Brampton, Ont. freelance writer, who specializes in IT. He can be reached via e-mail at mslofstra@myway.com.