THE SWITCH E-BOOK






A GUIDE TO INSTALLING BROADBAND

www.primexfits.com/enclosures

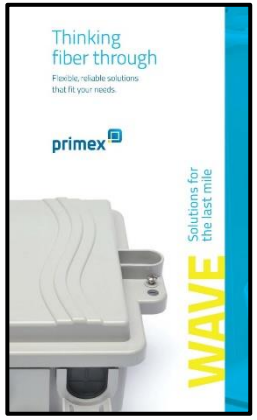
primex Fit everything. Together.

THE SWITCH E-BOOK

Contents

Resources

Product brochures



Social

Blog

THE SWITCH BLOG

E-Newsletter

primex THE SWITCH newsletter

Website

www.primexfits.com/enclosures

Contact page

www.primexfits.com/enclosures/contact

Toll Free Tel: 1 (877) 881-7875

primex Fit everything. Together.

The switch from legacy copper to fiber

Did you know our telephone network dates back more than 100 years? Often known as POTS (plain old telephone system), it's what the industry calls a "legacy technology."

Built on copper wires, the network was designed to carry telephone calls over long distances and was fully bi-directional. The downside? It was limited to a bandwidth of 300 to 3300 Hz.

POTS (plain old telephone system) was developed from the original phone system invented by Alexander Graham Bell in 1876.

As the system expanded, the telephone companies began to use fiber optic for the backbone of their networks, due to its greater capacity and speed. Because the fiber optic system is digital, this required equipment to convert the old POTS analog signal.

Once the Internet arrived there was demand to bring it into the home using the existing telephone network. This initially involved using modems that converted the digital signal to analog, but speeds were very slow and severely limited the usefulness of the Internet.

Later, ISDN and DSL technologies were introduced and used the Internet Protocol (IP) language.

Now demand has increased to the point where millions of subscribers are expecting TV, broadband, video, data and voice, all at the highest speeds possible. In response, the phone companies are pushing to eliminate POTS altogether and switch to an IP-based system.

What does this mean for the broadband industry?

The transition to IP means an all-digital process that is more conducive to using fiber. Fiber networks have the advantage of almost unlimited capacity. Copper is limited by the actual electrical conductivity of the wire, whereas fiber is simply transmitting a signal using light waves.

Fiber is much more reliable. The electrical conductance of copper can be affected by moisture and corrosion as well as from the wire being stretched, bent or broken. Fiber has a much greater pull strength and is not susceptible to the elements. However, it does require specialized connections and methods of routing and storage to maximize signal quality.

Fiber is also unlimited in the kind of signal it can send whether it be data, audio or video. It can easily adapt to changes in protocols and is not liable to interference from other sources.

It's not surprising that the telephone companies are pushing to abandon the old legacy copper system and move to all IP-based fiber optic networks. For example, after Hurricane Sandy the old copper infrastructure was destroyed by wind and flooding. It was mostly replaced with fiber, which will not be affected by salty air and less liable to damage from storms.

Drawbacks to switching systems

This switch, from legacy to fiber, means huge savings for telephone companies. Verizon recently converted seven of its central offices to fiber and found it can reduce its real estate space by 60% to 80%. On top of that, the telco estimates that fiber is 70% to 90% more reliable.

There are drawbacks from shifting away from the old system. Copper can do something fiber can't: it can conduct electricity.

With the old system, 48V DC is sent along the phone line so that in the case of power outages the phone can still connect to emergency services. With fiber there can also be problems connecting certain emergency calls and monitoring services including alarm systems and medical alert devices.

Another issue is that by switching systems the telephone companies are moving basic phone service out of the common carrier provisions of Title II that did not apply to Internet service. A recent FCC ruling said it should be covered, yet some phone companies plan to appeal the decision.

How multi-play solutions connect smart homes to the Internet of Things

If you follow tech news even casually, you've likely noticed a steady uptick in the number of articles about smart homes and multi-play. Well, maybe "uptick" isn't the right word, since it has actually been more of an explosion.

The key for service providers is multi-play, the ability to provide a number of different media services, such as Internet access, television, security monitoring and telephone service, over a single broadband connection.

ISPs need "last mile solutions" to deliver the bandwidth necessary for on-demand video, digital TV, high-speed Internet, wireless applications, and more. Whether a copper or a fiber installation is required, these solutions keep smart homes running smoothly, and to connect them to the so-called Internet of Things (IoT).

What exactly is a smart home?

It's simple, really: a smart home is one that contains a network of interconnected devices, which often gain emergent capabilities through their ability to interact. According to Wikipedia, "These additional capabilities can then be used to increase the quality of life inside the home in a variety of ways, such as automation of repetitive tasks, increased personal productivity, enhanced home security, and easier access to entertainment."

Customers may want to monitor their home security system using a smartphone or stream web content to every part of the house, it's all possible now (and will become even easier as we're able to move more data at greater speeds). In fact, this technology has become so ubiquitous, and so affordable, that home-automation hubs and do-it-yourself smart-home kits have become the stuff of holiday gift guides. Look for structured wiring enclosures to connect a state of the art smart home.

As a recent TechCrunch article put it, "Whether we're ready for it or not, we're rapidly evolving toward a world where just about everything will be connected." The U.S.-based tech research firm Gartner, Inc., says that by 2020, the number of IoT devices "will grow to 26 billion units installed in 2020 representing an almost 30-fold increase from 0.9 billion in 2009."

Needless to say, there is no shortage of companies hoping to take us there, from tiny startups with Indiegogo campaigns to major players including Apple, Google, Samsung, and Amazon.

What is the Internet of Things?

Many people are talking about the Internet of Things (IoT) as if it were the greatest thing to ever happen to the planet. The term was first used in 1999 by Kevin Ashton, a director at the Auto-ID Center at MIT. He described how the world of computers - up until that time - needed human beings to input data. But, with the development of connected devices, data could be collected without human intervention allowing computers to “know everything there was to know about things.”

According to Wikipedia, in 1982 programmers connected a vending machine to monitor how many cans of pop were available.

What is a thing?

Providing “things” with a unique identifier and the ability to transmit data is at the heart of the IoT. A “thing” could be any object that can be assigned an IP address and can be connected to the Internet, whether by using cabling or wireless technologies. One of the first examples was near the beginning of the Internet in the early 1980s when programmers at the Carnegie Melon University connected a vending machine so that they could monitor how many cans of Coke were available.

Recent developments have increased the potential of the IoT including the new Internet protocol IPv6. This features an extremely large address space that could potentially allow every single thing on the Earth down to the atomic level to have a unique ID. Other important factors are the expansion of access to broadband Internet and the decreased cost in getting connected. Also, as more and more devices are being connected, often referred to as becoming smart, their costs, as well as that of the associated technologies, are dropping.

Smart phones

Probably the most familiar smart device is the smart phone that has enabled huge numbers of people to access the Internet from anywhere they happen to be. They can now connect through high-speed wireless broadband connections or Wi-Fi if it is available. Cars too, are rapidly becoming smarter. For example they can know their service schedule, coordinate with the driver's calendar and arrange an appointment at the dealership as well as plan the best route to get there and avoid heavy traffic.

Entire homes have become smart. Starting with security monitoring, home automation has now evolved into control of thermostats and the ability to lock and unlock doors. Now there are smart appliances including fridges that can detect when supplies are getting low and order groceries. Alarm clocks could alert coffee makers to have that cup of brew ready in the morning. Other features of smart homes include smart TVs that can stream Internet content and send out ratings and viewing data.

Machine to machine

The Internet of Things expands far beyond the home. Machine to machine (M2M) communication has become widespread in manufacturing for monitoring inventory, optimizing labor, robotics and a host of other uses. There are a number of different technologies that make this work but usually it includes adding a sensor, transmitter and a receiver to devices. The sensor collects data which is transmitted to a central server. Once the data has been interpreted then commands can be sent to the machine to control its actions.

The expansion doesn't stop there. We're now talking about smart cities where everything is interconnected from traffic lights to smart electricity meters. These meters can communicate with the smart grid, a power grid that can allow two-way communications so that utilities can monitor their customers' electricity use as well as provide fault detection and system maintenance.

The worrying part about all this connectivity is the potential for security breaches. Apart from firewalls and antivirus software the actual physical network needs to be protected. Cabling, especially fiber that uses light to transmit data has advantages over wireless technologies that can be vulnerable to interception. Having a secure Internet connection using lockable enclosures throughout the network is essential.

What installers need to know about smart home hubs

The term “smart home” has been around for a while now. Initially, it described a residence that was wired throughout and connected to the Internet. Now, the word “smart” in smart home implies some kind of remote control, most likely from – take a guess – a smart phone.

For installers, this is an opportunity to integrate this new feature using enclosures for high speed cabling. This will save you headaches down the road if your client, or homeowner, decides to add the latest smart device. So, keep in mind that all kinds of devices are being marketed with the ability to be controlled with a smart phone.

Lighting

People have used timers on their lights for years especially as a deterrent to burglars. Now, all aspects can be controlled remotely including brightness and even color. What's more, some lighting can detect the presence of occupants in the room reducing energy waste.

Garage door opener

A wireless garage door opener was one of the first remote control devices to enter our homes. Ever misplace the remote or have it in a different car? Not to worry, most of us carry our smart phones at all times and can use them to open garage doors.

HVAC

All aspects of an HVAC system – heating, air conditioning and de-humidifying – can be controlled from a learning smart thermostat. Even if you don't have a whole house air conditioning system, standalone air conditioners and dehumidifiers are now available in smart versions.

Security

Security systems were an early adopter of smart technology. Remote monitoring was a service originally offered over regular phone lines but now connection through high speed data lines has allowed security companies to branch out into all aspects of home security. Integrating door locks as well as fire, smoke and CO2 detectors has been added along with moisture monitoring to detect water leakage. They can even be adapted to include hot tub or swimming pool heating and water quality monitoring.

Kitchen

In its early stages, smart appliances and gadgets for the busiest room in a household are rolling out. Wouldn't it be useful to cook and defrost food remotely? One idea that is taking off is the smart crockpot. This can be left on for hours but a smart feature allows users to adjust the temperature as needed.

Wiring a smart home

Many of these devices can run with just WiFi and a smart phone. The challenge, sometimes, is that there's a lack of consistent and optimal coverage throughout a house.

Hard wiring, along with a smart home hub, is the best option especially if you are dealing with a new build. In this scenario, you have a choice on where to locate the hub and what type of wiring to install. It makes sense while walls are open to put in as much wiring as possible in anticipation of connecting multiple devices in every room of the house, perhaps even the bathroom.

With this amount of wiring there is much debate as to what amount of future proofing makes sense. Some installers insist that with its lower price it makes sense to use Cat5e wiring as it can still handle gigabit speeds. It can be used for phones, data, television and media servers. There is also the option of Power Over Ethernet (POE), where the power needed to run something like a wireless access point or camera is supplied as well.

Which category cabling?

Others say it's worth paying the extra for Cat6, Cat7 and even fiber. One thing for certain is to consider future expansion and get a panel for your hub that is big enough and can handle enough capacity as more parts of the home become connected.

An optimal enclosure would be WiFi transparent to allow the installation of a wireless router. This way it can manage both your wired and wireless networks from a central location. Your ISP modem would provide the Internet connection and from there the data can be spread using distribution modules that allow easy access to connections.

Labelling cables at both ends will save time and frustration and general tidiness will make your smart home experience a delight.

7 New terms every broadband installer should know

As high-speed fiber crisscrosses North America there are still many last-mile challenges bringing it into buildings. Because of this, many new terms are being cited for iterations of the service.

With fiber able to deliver gigabit speeds over very long lengths and copper limited to higher bandwidths over only short lengths, the ultimate goal is to bring fiber into, or at least very close to the home or business. The general term for bringing broadband by fiber anywhere near to premises is **FTTx – fiber to the ... whatever**. But, beyond that, there are often confusing and conflicting terms being used.

Here's a primer on the current industry lingo used in cabling, telco, ISP and broadband conversations.

Fiber to the node or neighborhood (FTTN) refers to a termination somewhere distant or possibly miles from the final destination. The final mile in this case is usually pre-existing twisted pair copper or coaxial with connections made in a street cabinet. Hundreds of customers may be served, typically with DSL (digital subscriber line), and so speed and bandwidth will drop significantly from that of fiber optic.

Similarly, **FTTC** specifically refers to **fiber terminating in a cabinet** (or "to the curb") that is closer to the premises. This is perhaps less than 300 meters so that high-speed copper technologies that run over shorter loop lengths like the new G.Fast, can be used.

G.Fast upgrades DSL to higher frequencies and can handle gigabit speeds over distances up to 250 meters.

Getting progressively closer to the premises, the term **FTTdp** means **fiber to the distribution point**. The outside plant (OSP) may be next to the building itself and is the final connection point between the fiber and the building's network cabling.

Finally, we get to the near Utopian term we hear so much about: **FTTP**. This is where the fiber actually reaches the **premises** itself. There are two subcategories **FTTH – fiber to the home** and **FTTB – fiber to the building.**

With **FTTB,** the fiber connects to a panel either attached to, or inside a building, probably a multi-dwelling unit (MDU) or business building. From there it's distributed by the building's infrastructure, whether through Ethernet, WiFi or powerline networking. In a new build or greenfields, there's also the option of running fiber throughout the building.

FTTH brings the fiber right to the home and can be terminated in a simple cross-connect box or panel. From there, networking can consist of Ethernet or passive optical network (PON). Devices can be connected to the optical network using an optical network terminal (ONT).

The end result is **FTTD**, which is **fiber to the desktop**. This is the ultimate in speed with optical fiber running the full length of the network right up to the desktop.

4 Reasons to consider fiber to the home

With falling prices and increased demand, fiber to the home (FTTH) is becoming the new standard for data delivery for homes and businesses. Install and repair teams need a variety of enclosures for these in-demand systems.

According to Broadband Communities Magazine, FTTH deployments are increasing for several reasons. For starters, FTTH is attractive to new homebuyers. A marketing analyst interviewed by the magazine confirms:

> ***"Consumers are willing to pay a premium for fiber-connected housing both because FTTH allows them to work from home and because the in-home lifestyle is truly being transformed into an online-dominated experience."***

Another reason for the expected increase is that cable companies are planning to install FTTH, a service telcos have dominated for years.

Technicians installing fiber in new homes or multi-family dwellings (MDUs), should understand the main advantages it offers over traditional copper cabling solutions:

1. Greater capacity

Typically copper is limited to gigabit speed whereas fiber will handle at least 10 gigabit. This is becoming more of an issue as cloud computing demands shorter network response times.

2. Less signal degradation

Fiber can cover much greater distances without significant signal loss. This results in higher speed and dependability, and also reduces the amount of power needed to transmit data.

3. Stronger and more reliable

Fiber has a pull strength more than four times that of copper. Copper is very malleable and is susceptible to signal degradation due to being stretched, twisted or kinked. It requires insulation and shielding which are both vulnerable to damage

4. Secure and resistant to electrical noise

Fiber transmits light so it does not need shielding from electrical interference. It can be installed close to existing infrastructure such as transmission lines, cell phone repeaters or, on a smaller scale, WiFi hubs. Also, because of the use of light, it is more secure than copper as it is very difficult to tap into.

Choosing fiber enclosures for residential demarcation

Keep in mind that once the fiber reaches its destination point, the outside plant (OSP) near a home or business, connections need to be made to existing network cabling and this is where fiber becomes vulnerable.

As it transmits light instead of electricity the two pieces of optical fiber at any connection must be matched and the two cut faces (SC/APC) aligned perfectly in order to prevent any loss of signal at the splice or connection. Choosing the right enclosure is key to protecting the fiber.

Within the enclosure there is an Optical Network Terminal (ONT), which terminates the fiber then demultiplexes the signal into its component parts (voice telephone, television, and Internet). Often there is a fiber splice as well. There are two main types of fiber splices, fusion, where the two fibers are fused together, and mechanical, which is most often a temporary measure. The splice needs to be protected from the elements and from being damaged by being put into some kind of enclosure such as stackable splice trays and fiber transition outlets (FTO).

Other fiber management accessories like spools, clips and mounting brackets are essential for ensuring fiber protection within enclosures. Properly wrapping fiber around a spool maintains bend radius while clips and brackets keep the tangle at bay.

Fiber to the home is already here for many communities. If you don't already have it then it is on its way. Proper installation is the key to success when rolling out fiber to the home and a good enclosure is an important part of that.

What is gigabit Internet and how do you get it?

You may have heard the term gigabit Internet a lot lately, usually in connection with the rollout of fiber broadband across North America. Wondering what type of speed it refers to?

Simply put, it means Internet access running at speeds of 1000 megabits a second, or roughly 100 times what we've been used to in the past! This speed has become possible over fiber optic networks because it does not have the limitations of copper.

Previously, the choice for broadband was between copper-based digital subscriber line (or DSL) and cable broadband with cable being the faster of the two. DSL typically runs speeds up to 50 Mbps but premium cable in some areas is available with speeds up to 500 Mbps but with a high price tag.

Although fiber has been used for data backbones for years it's only recently been brought right into the premises. The term FTTP or fiber to the premises means exactly that but a term you may hear more often is FTTH or fiber to the home. At the very least ISPs are bringing fiber as close as possible with FTTN, referring to fiber to the neighborhood.

Sounds great, right? Well, yes, but installing fiber is expensive so getting it to individual homes is a challenge. The homes themselves also need to be retrofitted to accept fiber. Installers can look to new media enclosures available to streamline this process.

FTTH coming to a city near you

One of the pioneers of FTTH service is Google Fiber, which launched Gigabit Internet over fiber to Kansas City in 2012. Since then, they've aggressively expanded their network.

It's now available in Kansas City, Austin and Provo, with plans to expand to many more cities including Salt Lake City, San Diego, Phoenix, Atlanta, San Jose and Portland.

Other major players include AT&T, Century Link and Comcast. AT&T call their service GigaPower and is available in Atlanta, Austin, Chicago, Cupertino, Dallas, Fort Worth, Houston, Kansas City, Raleigh-Durham, Winston-Salem and most recently San Antonio. That puts them head to head with Google Fiber in some markets, which should be good for the consumer.

Comcast, who advertises their 2 Gbps service as Gigabit Pro, launched in Atlanta and is now available in many cities including Chicago, San Francisco Bay area, Houston, Miami, Portland and Seattle.

But fiber may not be the only way to deliver Gigabit. There is a new cable modem specification called DOCSIS 3.1 that supersedes the current DOCSIS 3.0. It has a minimum speed of 1 Gbps but may eventually be capable of 10 Gbps!

Comcast is field-testing the new technology and it may be a game changer as existing cable infrastructure will be able to deliver speeds comparable to fiber.

One of the big advantages to DOCSIS 3.1 is that cable companies won't have to upgrade a lot of their systems but then what about the telephone companies? These currently rely on DSL over twisted pair copper cabling but a new technology G.Fast is enabling Gigabit speeds over copper over short distances.

One way or another at the present rate of expansion you can expect Gigabit speeds near you soon.

Can copper cabling survive in a fiber world?

Two new technologies – G.fast and Cat8 – are improving copper cable options. This opens up new opportunities for telcos that have large amounts of legacy copper infrastructure, which currently cannot handle the speed and bandwidth that can be delivered by fiber.

Upgrading their existing copper is not only much cheaper than replacing with fiber, the increased speed will actually encourage the deployment of fiber networks.

G.Fast

The latest standard for twisted pair copper cabling is here and it may be a game-changer. Now undergoing testing and certification, it's expected to be available later this year.

The most exciting aspect of this technology is that the bottleneck created when fiber is brought to premises with copper cabling, will vanish. This will be a boon for fiber to the home (FTTH) installations. Many locations are difficult and expensive to reach with fiber but G.fast will deliver similar speeds over the last short distance of existing copper.

G.fast is a high-speed transmission technology for digital subscriber line (DSL) and expands on the current VDSL2 standard. Increasing the frequency spectrum from 30 MHz to 106 MHz, with a probable future increase to 212 MHz will enable gigabit speeds over loop lengths of up to 250 meters.

The technology will work in conjunction with fiber to the distribution point (FTTdp) – where an outside node is located within 250 meters of the premises. These will be the transition points between fiber and copper and would need specialized panels and transfer terminals located in a manhole, pole or cabinet or even as close as the building entrance.

G.fast will also save telcos money by using reverse power feed (RPF). This method is when the subscriber supplies the power to the distribution points instead of the telco and reduces overall cost to the service provider.

Category 8 cabling

The other new technology on the near horizon for BASE-T twisted pair copper is Cat8. This standard is still being defined and there are a number of competing solutions in the U.S. and Europe.

The intention would be to make Cat8 cabling very similar to shielded Cat6a or Cat7a cables with the same overall diameter and conductor size. Speed would be 40 GB per second with a bandwidth of 2 GHz – four times today's maximum of 500 MHz.

The most likely locations for large-scale installation of the new standard are data centers. There is solid support for the new standard to retain the RJ45 connector footprint, which would enable closely spaced connections and be less expensive that other options.

Lower cost will be a main feature of the new standard and as prices drop expect to see Cat8 become the new standard for multimedia infrastructure to handle demand for UHD (4K video) streaming. Along with all the current data types each Cat8 cable will be able to carry up to four services.

It's still too early to know the exact specifications of the new standard, but, as in previous cycles, early adopters are using expensive coax copper or fiber solutions for very high speed interconnects. Ultimately the new standard will become the mainstream solution and come in at much less cost.

Everything a broadband installer needs to know about streaming content

Have you ever installed broadband and a homeowner starts to quiz you on topics like streaming content? These days, consumers are turning to the Internet to satisfy all of their entertainment needs. With a dizzying amount of programming choices and just as many technical factors, today's broadband installer needs to understand streaming.

As high speed broadband Internet enters more homes it brings with it a whole new way to watch TV and listen to music. In the past, complete video or audio files were downloaded onto computers to be watched later. The download time was often quite lengthy and the file size, especially for video, was immense making storage an issue.

Increases in broadband speed have shortened the time it takes to download large files but have also enabled a better way to view or listen to content.

Receiving data in real time or streaming, as it's known, has many advantages over downloading files. Data is continually transmitted and can be accessed immediately, which means no waiting around for giant files to download. It is mostly used for video and audio but has also been adapted to streaming games and apps to devices with data limits like smartphones.

Streaming runs into problems on slow Internet connections or when there are interruptions in service. The data has to be able to stream fast enough to keep up with the speed of playback and span any short breaks in transmission. To avoid pauses in playback most programs use buffering where unused data that has already been received is stored until needed. But if the connection is too slow the buffer will empty and the dreaded "buffering" message will be displayed until the data flow catches up.

To get around these problems it is necessary to reduce the amount of data needed to send the stream. This is called compression, also known as bit-rate reduction. There are many types of compression but they all involve encoding the signal at the source and then decoding it at the receiving end. This reduces the number of bits of data needed but also requires more processing. So, the type of compression used is a trade-off between signal quality, size and time it takes to decode the signal.

The demand streaming has put on Internet connections have been steadily increasing with the quality of the content. Video resolutions have gone from the old standard 640 x 480 pixels to the new 4K or Ultra HD standard, which are 3840 x 2160 pixels. Even with compression and buffering this means conventional broadband may not be able to cope with multiple streams. Fiber to the home (FTTH) is one answer for customers but requires upgrading of equipment and enclosures.

Finding content to stream is easy. There are literally thousands of Internet radio stations webcasting every conceivable type of music or commentary. All that's needed for this is a web browser and some speakers. There's also music streaming services that allow you to choose the music you want to hear when you want to hear it. Examples include Spotify, which comes with either a free version that includes commercials or the subscription-only premium service, as well as the recently launched Apple Music, which works in conjunction with iTunes.

There are also many sources for video streaming that are free. YouTube is probably the best known but is geared to sharing fairly short videos uploaded by subscribers. To see full length movies and TV shows services like Netflix charge a monthly subscription for access to their huge catalog of videos as well as their own content.

Traditional broadcast TV stations are also getting in on the act. Many networks are now offering original TV shows in their entirety for streaming from their websites. There is usually no cost but you do have to put up with commercials, although they are much shorter than you would experience on conventional TV.

How secure is your Internet?

For millions of commercial and residential customers, their connection to the Internet is an essential service. So it would probably come as quite a shock to discover just how vulnerable their connection is. For most businesses, a loss of service could stop them being able to function. Residents could lose their phone service and the ability to work from home.

For years Internet security has meant protection against computer viruses, malware and malicious code on websites. Most computers today are protected by firewalls and anti-virus software but even some of the most sophisticated networks can be defeated by cyber attacks.

Just recently a number of universities across the U.K. lost their Internet connections when their network was brought down by a Distributed Denial of Service (DDoS) attack. Most people will remember other instances such as when Target was hacked and the Ashley Madison data breach.

The website Hackmageddon.com categorizes cyber attacks into cyber crime, hacktivism, cyber espionage and cyber warfare. The majority of cyber attacks are by criminals trying to obtain personal information such as credit card numbers and other banking information but the next most common is hackers often with some type of political agenda.

But it isn't just the virtual world that can be a threat. The actual physical connection can be damaged by weather, accident or deliberately. The entire Internet is mostly connected through cables whether by fiber or copper, which may be above ground, underground or beneath the sea.

Protecting fiber and cable

Some cables are extremely important. If you use a highway system as an analogy, then the major freeways would be called backbones. These backbones are usually high capacity fiber cables that carry thousands of Internet connections.

Other than weather-related issues most cable damage is caused by accident. The most common is from construction companies that don't check on the presence of underground cables before they dig. Because backbones are so important they are often buried underground and if damaged a huge number of customers may be affected.

Other culprits include squirrels who love to chew through the protective coating around fiber cable and vehicles that collide with utility poles bringing down overhead cabling. But not all damage is accidental.

Copper cable is quite valuable and thieves will steal large quantities of it. They sometimes mistakenly think fiber is valuable if cut into segments. Although a single fiber strand is capable of carrying a huge amount of data it does so through a pencil-thin cable that is relatively simple to cut.

Vandalism and sabotage account for some of the deliberate damage. It's important to protect the termination point of an Internet cable by installing it in a secure lockable enclosure that will also protect it from the elements. Burglars may also seek to cut the Internet cable as it often carries security signals as well as communications.

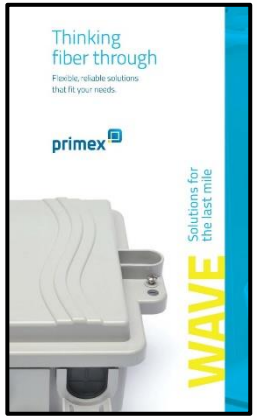
There has been concern lately about the presence of Russian submarines and spy ships in areas where there are vital undersea cables. If these cables were attacked it could cripple global Internet communication. With tensions building for some time, the worry is the Russians may sever cables at the most difficult-to-access locations. Meaning the damage could take quite some time to repair.

It's not just the Russians to worry about. Terrorist attacks could come in the form of cyber warfare or damaging critical infrastructure. Although a lot of effort is put into protecting data it may be surprising how poorly defended much of our essential cabling is.

Hopefully with that amount of risk governments will take more action to protect the Internet, both virtually and physically.

Resources

Product brochures



Social

Blog

THE SWITCH BLOG

E-Newsletter

primex THE SWITCH newsletter

Website

www.primexfits.com/enclosures

Contact page

www.primexfits.com/enclosures/contact

Toll Free Tel: 1 (877) 881-7875

primex Fit everything. Together.