Are your purchasing decisions placing your customers' networks at risk?

What happens when your customer gets less than the strong brand they paid for?

Cisco is committed to helping its customers receive quality products that are delivered with added value. When products are purchased on the secondary market, rather than through Cisco Authorised Distribution and resale Channels, Cisco cannot guarantee the source and quality of those products.

There have been many cases in Asia Pacific and around the world where companies have fallen victim to substandard, unauthorised market or counterfeit products. The following case studies will help you explain to your customers why they need to safeguard the integrity of their IT infrastructure by engaging only with a Distribution Partner they can trust.

Case study 1

Government department receives falsified equipment

A reseller purchased 40 units of 1841 Integrated Services Routers from a broker and resold them to a government department via an official government Request For Purchase (RFP).

A review of the serial numbers showed that the equipment was out of warranty and was sourced from several countries including the U.S., China and India.

The government department, however, was not satisfied with these findings, as on inspection the boxes were sealed and the equipment appeared to be new and unused.

Cisco traced the serial numbers to the original routers, two of which were installed in a client's network in Asia Pacific. Cisco Brand Protection team members photographed the serial numbers of the original routers and provided this evidence to the government department.

After further investigation, it was found that the 40 units of Cisco 1841 Integrated Services Routers had been illegally modified to a Security (K9) bundle, which is twice the price of the standard version.

It was also found that the broker had changed the serial numbers on the chassis with existing K9 serial numbers, modified the cookie (software that contains the serial numbers), upgraded the memory and the IOS software and the products were then repackaged with fake seals and Cisco tape.

The customer lodged a complaint with police and the case is being investigated by local authorities.

"When you buy a reputable brand, you should expect to get what you pay for and not fakes, second-hand items, third-party products, products with invalid warranties or software licenses, no service support entitlements or incorrect configurations."

Phil Wright, Director WW Cisco Brand Protection

Case study 2

Commercial customer is sold second hand switches as new

A commercial customer bought five Cisco Catalyst 3500 Series Switches from a broker at a very competitive price. The broker had assured the customer that the switches were new Cisco products in sealed Cisco boxes.

However, the customer became suspicious when he found dust inside the chassis and called Cisco Brand Protection. A serial number trace found some of the products to be 2-3 years old.

The customer returned the products to the broker and had them replaced with new Cisco products that were sourced from the Authorised Cisco Channel.

Case study 3

Broker uses online trading site to sell counterfeit equipment

After receiving spam emails offering new, genuine Cisco equipment at discounted prices, a Cisco Partner notified Cisco about the broker's online trading site.

Cisco's Brand Protection team investigated the broker's shop front which was hosted on a well known online trading site. They made a test purchase of the broker's Cisco branded equipment and found them to be counterfeit.

In conjunction with the local authorities, a search warrant was issued and 157 products were seized. The offender was sentenced to five years in prison and ordered to pay US$1.5 million in restitution.

Where do unauthorised products come from?

The Secondary Market

The sale of equipment to unauthorised Channels is carried out by 'brokers/resellers' who often source products from companies looking to dispose of old, defective and/or surplus equipment. These unauthorised resellers then sell the products to other resellers or directly to end users. During this process, an unscrupulous reseller may also mix counterfeit items into their shipments so that the customer ends up with a combination of legitimate, third-party or illegal products. In still other cases, these resellers may mix in defective, unsupportable, poorly refurbished and/or functionally obsolete products. It is not uncommon for products to change hands many times, thereby providing frequent opportunities for questionable and fake products to enter a network.

The Stolen and Unauthorised Market

The problem can be further compounded by the introduction of stolen or unauthorised market products. Illegal 'black' market products are those that have been stolen or are obtained unlawfully. Unauthorised market products are items intended by their manufacturer for one international market, but, instead, are exported and resold by territorial licensees or authorised Distributors into another market.

The Counterfeit Market

Counterfeit manufacturers often sell their products either directly or through a broker. Products are often marketed via online trading sites, their own Web site and via spam.

Unauthorised Distribution Channels – whether secondary, unauthorised market or stolen products – are frequently used to introduce the sale of counterfeit equipment.

- All 4 sales theatres affected
- CF Products sourced from Asia Pacific
- Sold in U.S./Canada, Europe, emerging markets
- Co-mingled with unauthorised market gear

Help your customers protect their IT infrastructure

- Source your equipment from an authorised Cisco Distributor.
- Make your customers aware of the benefits of buying only from a Cisco Partner. They can trust the integrity of the products you sell them and you can add value to the sale through your expertise and ongoing support and consultancy.
- Use the case studies in this brochure to highlight the negative impact of buying outside the authorised Cisco Channel.
- Encourage customers who have been approached by suspect brokers or offered suspect products to report the incident to **brandprotection-apac@cisco.com.**

Additional Assistance

If you need additional assistance explaining the risks faced by customers when they purchase equipment from the unauthorised market or that is suspected of being counterfeit or built with third-party components, please notify your Cisco contact or Cisco Brand Protection Office. Cisco helps its valued Cisco channel partners to sell against unauthorised market or counterfeit products.

If you would like to report suspicious products or activities you may do so via:

- Web: **www.cisco.com/go/brandprotection**
- Email: **brandprotection-apac@cisco.com**

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**