



Bringing it all together

# The challenges of securing complex global networks in a converged world

---



---

## Introduction

The immense complexity of modern networks and the nature of the threats and attacks make it impossible to secure them completely at all times. As the threats grow more severe, what is the most efficient and cost-effective way for companies to protect themselves?

This white paper explores the challenges modern businesses face in balancing the opportunity that the internet represents with the threats to security from network predators.

**The fluid and diverse nature of the threats and attacks, coupled with the increasing complexities of today's networks, makes complete protection impossible.**

## The evolving threat environment

Every year new technologies, products, even laws are introduced with the aim of improving network security. The overall situation has not improved, however, as the threats continue to keep up with, and sometimes outpace, the introduction of new forms of protection.

“The threat environment is changing – financially motivated, targeted attacks are increasing, and automated malware-generation kits allow simple creation of thousands of variants quickly – but our security processes and technologies haven't kept up.” (Gartner, December 2006)

BT considers that Gartner has identified what is probably the most significant shift in the threat environment in recent times. While many threats in the past have been motivated by a desire to cause damage and disruption, we are now witnessing an increasing shift to more sophisticated attacks by criminal gangs motivated by financial gain. These gangs have significantly more financial and technical resources at their disposal than a hacker operating alone. At the same time, the punishment for online crime is still comparatively lenient.

Although fewer than 10 per cent of the attacks on the internet are targeted against a single company, the financial impact on an individual business of a single successful targeted attack will be 50 to 100 times greater than the impact of a purely malicious worm or virus. By the end of 2007, Gartner predicts that 75 per cent of enterprises will be affected with financially motivated, targeted malware that evaded their traditional perimeter and host defences.

In addition to the financial implications of a security breach, the range of impacts on an organisation may include:

- Damage to a company's reputation, and potential legal implications that may result from any failure to protect customer information.
- Time wasted by employees in deleting spam or struggling with a slow network.
- Compromised assets, such as wasted bandwidth or damaged machines.

What companies need more than ever from their security providers is stability, and certainty – not the pursuit of some mythical preventative technology to enable threats to be avoided, but an acceptance of the situation as it exists, that security will always be relative, and that the paramount need of business is for adequate, effective security that optimally protects an organisation's electronic assets. All security devices are vulnerable to being sidelined by a resourceful attacker. The net result is that security products can't stop what they don't recognise as a threat.

**Technology in itself will never solve the problem of security; it must be harnessed to human vigilance and expertise.**

---

## Detection and response

The way forward not only includes effective products but also processes that recognise the value of electronic assets to a business. Just as detection and response underpin our physical security, they should also be essential elements of internet security. In the digital networked economy, companies need to take a proactive approach by continually investing in both static and proactive forms of protection, such as device monitoring and threat response. This will result in an effective layered approach to protecting an organisation's electronic assets.

**Point 1: It's critical to invest in network monitoring services.**

## Outsourcing monitoring

The key to a successful detection and response system is vigilance: attacks can happen at any time of the day, any day of the year. While it is possible for companies to build detection and response services for their own networks, it is rarely cost-effective. There are also the difficulties of recruiting and retaining the right people to oversee this process and of ensuring support across all geographic sites. To achieve economies of scale, outsourcing these services is a necessary consideration.

**Point 2: For economies of scale, companies should consider outsourcing network monitoring services.**

## Building protection within the network infrastructure

Organisations today must connect to the internet for a wide variety of reasons – to publicise their services, deal with customer sales and service enquiries, communicate via e-mail, and for e-commerce transactions and customer support. However, the internet is inherently an insecure and potentially hazardous medium, with threats from hackers, viruses, worms, Trojan horses, and internal threats such as employee sabotage. The impact of these threats on organisations can include: loss of productivity and revenue; loss of financially sensitive information; and damage to reputation.

Companies must assess the risk of threats being realised and then put the necessary barriers in place to protect themselves. Such barriers will always include an optimal mix of technology, people and processes. Any element on its own won't be sufficient to mitigate the risk posed by increasingly sophisticated attackers.

**Point 3: Companies must assess the risk of internet security threats, and then put the necessary barriers in place to protect themselves.**

## A multilayer approach

Although specific threats to security can be identified and categorised, the reality is that many threats are blended. For example, hackers may distribute Trojan software in a worm or virus in order to add a PC to a botnet (a collection of software robots) and use it to send spam. Failure to protect against one type of threat can result in the organisation being exposed to another. For instance, failure to prevent employees' illicit surfing can lead to their downloading spyware; or peer-to-peer software; or being exposed to sites hosting spyware-infected pages or downloads.

As the threat is both fluid and blended it is important to have a multilayer approach to protection. The exact form of protection will vary between sites, depending on their size, complexity of operating environment, and company electronic assets exposed to potential attacks. BT's view is that optimal flexibility is needed to respond to the demands for protection that each customer site or remote user places on technology and associated processes.

## Combating internal threats is as important as mitigating external attack risk

A growing proportion of both threats and actual attacks on an organisation's electronic assets comes not from external sources, but from inside an organisation. Employees, contractors and other staff who have access to a company facility or remote computer can inflict damage to an organisation's electronic assets if there are inadequate defences. Many "inside" attacks go unnoticed until the damage to the business has already been inflicted.

Proactive monitoring, event correlation and threat response, should be applied to security and non-security devices such as servers, desktop PCs, routers, etc. This allows both internal and external events considered to be "unusual" in nature to be reported and investigated immediately. Often such incidents involve access to servers either at unusual times or by unauthorised users. Without the proactive security monitoring of such non-security devices these events would not trigger any response. Thus an effective security posture should always highlight both internal and external threats, security and non-security devices.

**Point 4: The most effective approach may be to build capability and components from a number of vendors into a single cohesive solution.**

---

## BT advocates a layered approach to protection

Reflecting best security practices, BT creates multiple barriers to foil any potential attacks into the BT network. The essential elements of BT's defence-in-depth approach involve:

- Firewalls on the perimeter of the network (in best practice a dual-skin firewall solution with the firewalls sourced from different suppliers, so that both firewalls cannot be exploited in the same way)
- Intrusion detection systems (IDS) and Intrusion prevention systems (IPS) at strategic places in the network
- Monitoring, event correlation and threat response across an optimal range of security and non-security devices backed by skilled security analysts
- No "dial in" access to corporate network – remote access or wireless/mobile access is via strong authentication over VPN connection
- Anti-virus protection and proxy caching
- Network-based prevention against distributed denial of service (DDoS) attacks
- Vulnerability scanning and assessment tools
- Machine log storage for compliance and investigation purposes.

All of the above would be backed up by rigorous audit and test procedures.

## Viruses

BT adopts a dual approach to dealing with viruses – protection against desktop and server-borne viruses (essentially malware coming over the internet, or via USB tokens, Bluetooth devices or removable media), and protection against e-mail-borne viruses at its e-mail gateways. Isolated parts of the network have been rendered unavailable from time to time, but almost invariably as a result of authorised users importing malware and rogue code into the network.

## Dealing with attacks

BT's basic approach is to compartmentalise its internal domains so that it can isolate and contain the affected part of the business as quickly and effectively as possible. For example, if a problem is encountered in France, BT can temporarily shut down all or part of the French domain (maybe for an hour or more), identify the problem, fix it, or if it can't be fixed immediately, put in appropriate filters until a more permanent fix is available.

The implementation of all these counter-measures has helped ensure that BT's security management system is one of the most effective in operation today.

**Point 5: BT's basic approach is to compartmentalise its internal domains so that it can isolate and contain the affected part of the business as quickly and effectively as possible.**

## Centralised managed security services

With the roll-out of new global business-critical applications, organisations that trade globally using the internet have an increased dependency on web-based applications and business processes. This increases their vulnerability to online attack, but also offers an opportunity for IT consolidation and efficiencies. A single standard operating environment, such as a central logistics and tracking system replacing a number of local systems, offers reduced risk and points of vulnerability. It also reduces the opportunity for errors, offering improved service levels and business effectiveness. Without a central security policy and solution, growth can be hampered. It is slower to integrate partners and acquisitions. The cost of effective integration increases with the number of independent local applications and policies that are managed and/or adopted.

**Point 6: A centralised managed security environment provides a safe and secure corporate infrastructure that also maintains, manages and supports compliance against key regulatory requirements.**

---

## What is the most efficient and cost-effective way of securing the global network of the future?

### Defend and secure specific customer sites and networks in different ways

Technology will continue to evolve with advances in design and the increasingly complex demands of end-user customers. With the rapidly increasing range of customer devices running on TCP / IP and often exposed, either directly or indirectly, to the internet (Multiprotocol Label Switching [MPLS] routers, IP PBXs, etc.) the requirement to defend and secure specific customer sites and networks in different ways will be a key driver.

### Sophisticated layered defence for larger sites

Layered defence for larger sites (whether in the network infrastructure or premise-based or a combination of both) is becoming ever more sophisticated as devices designed to combat specific threats to specific devices or elements of a customer network continue to enter the market.

### Integrated devices required to protect smaller sites

Integrated devices under the unified threat management (UTM) banner now enable smaller sites to be more cost effectively protected against a range of threats while at the same time requiring managed security service providers (MSSPs) to manage and respond much more effectively than in the past when relatively simple firewalls were common.

### MSSPs evolve to provide a more holistic set of capabilities

Demands for proactive monitoring and response of security and non-security devices, often to guard against internal threats, are growing rapidly. Customers are increasingly viewing traditional perimeter security as the start-point not the end-point to protect vital electronic assets. Together with this increased monitoring requirement comes the need to store and retrieve machine log data for compliance and investigative needs. As a consequence, MSSPs will quickly need to evolve from the supply and management of traditional security appliances to providing a more holistic set of capabilities, including design and consulting services, which run across a customer's entire IT environment.

### Protecting complex distributed IT environments on static budgets

Customers continue to deploy increasingly sophisticated IT environments designed to automate and improve efficiency in key areas of their business. These environments can either be distributed across regions, countries or globally, and are much more exposed to the internet through the use of TCP / IP as their primary communications protocol. Such environments require much improved levels of protection and many more people to ensure an adequate level of defence than in the past. These requirements are set against budgetary environments that are often static despite the increasing risk profile that IT environments are generating.

### MSSPs become a necessary consideration

The business drivers outlined above are increasingly driving customers to re-define their traditional relationships with MSSPs. Small and mid-size organisations that have traditionally not had an MSSP relationship are looking to improve their defences by deploying sophisticated UTM devices which require management expertise only found in an MSSP. A different type of change is occurring higher up the market where large organisations that traditionally in-sourced most if not all of their IT security are looking at different business models both to take advantage of technological developments and to make tight budgets go further.

---

## Conclusion

Technology alone will never solve the problem of security. Technology must be harnessed to human vigilance and expertise. The key is detection and response, and therefore it is critical for companies to invest in network monitoring services. The most effective solutions integrate capability and components from a number of vendors.

To arrange their own security in the most cost-effective, flexible manner, companies should work in partnership with MSSPs who offer a holistic set of capabilities. These partnerships will be crucial in enabling businesses to protect complex distributed IT environments on static budgets.

BT practises a layered approach to protection, placing multiple barriers in the way of potential attacks into the BT network. A centralised and standardised managed security service, such as BT's Managed Security Service, provides a safe and secure corporate infrastructure that maintains and supports compliance against key regulatory requirements as well as offering greater control of budgets.

## About BT

BT is one of the world's leading providers of communications solutions and services operating in 170 countries. Its principal activities include networked IT services, local, national and international telecommunications services, and higher-value broadband and internet products and services. BT consists principally of four lines of business: BT Global Services, Openreach, BT Retail and BT Wholesale.

## About the Authors

### Mick Creane

Mick has over 25 years experience in the IT and communications field, during the last 15 of which he has increasingly focused on the areas of IT security and business continuity. He now heads the team which is responsible for shaping and developing BT's managed security and business continuity propositions on a global basis.

Prior to this, Mick headed the Security and Business Continuity practice within BT Consulting. During this time, he led teams which provided solutions to both detailed technical and business related security challenges facing clients across all sectors of business, ranging from UK government to global corporations.

Mick holds an MBA and is a CISSP and CLAS registered consultant

### Martin Smillie

Martin has been with BT for nearly 5 years and is a General Manager in BTGS's Global Professional Services Group.

He is currently responsible for building BT's advanced security services capability, primarily via acquisition. Recent examples include Counterpane and INS. Previously Martin was a Product Line GM responsible for BT's managed security services, high speed internet and remote access portfolios.

Prior to joining BT, Martin was Vice President for Broadband Services for KPNQwest in Amsterdam and Asia Pacific Product and Marketing Director for MCI (now Verizon Business). Martin is based in Amsterdam.

## Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

British Telecommunications plc 2007.  
Registered office: 81 Newgate Street, London EC1A 7AJ  
Registered in England No: 1800000

PHME 53075

