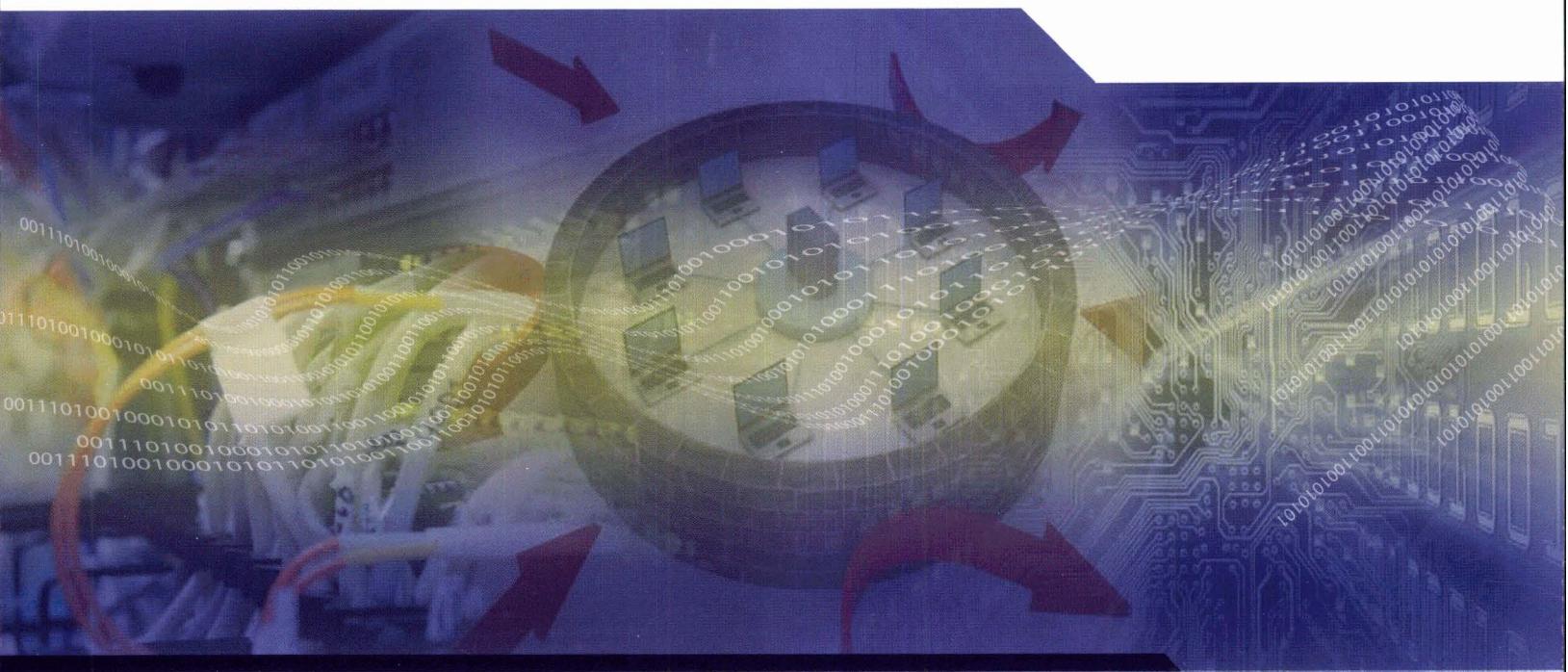


# THALES



[www.thalesgroup.com](http://www.thalesgroup.com)

Understanding cyber security is a challenge faced by all businesses and organisations around the world. New threats emerge on a daily basis and it can be difficult to understand what they are and where they come from, and most of all, what impact they can have on you and your organisation.

Thales has over 40 years' experience of delivering cyber security solutions to customers across a range of industries, including defence, security, government and commercial businesses.

This extensive experience has provided us with a detailed understanding of the issues you face and we have developed a clear methodology to help you become cyber aware, understand the depth and breadth of your cyber security issues, and recommend the best way forward to enable you to successfully manage your cyber security risks.

Whether you are looking to gain an initial understanding of your organisations' cyber security risks, or form a strategic partnership to guide you from the discovery stage through to being fully cyber aware and secure, Thales has the cyber solutions and experience to meet your requirements.

Thales - here to help you through the process of understanding how best to manage your cyber security, now and in the future.

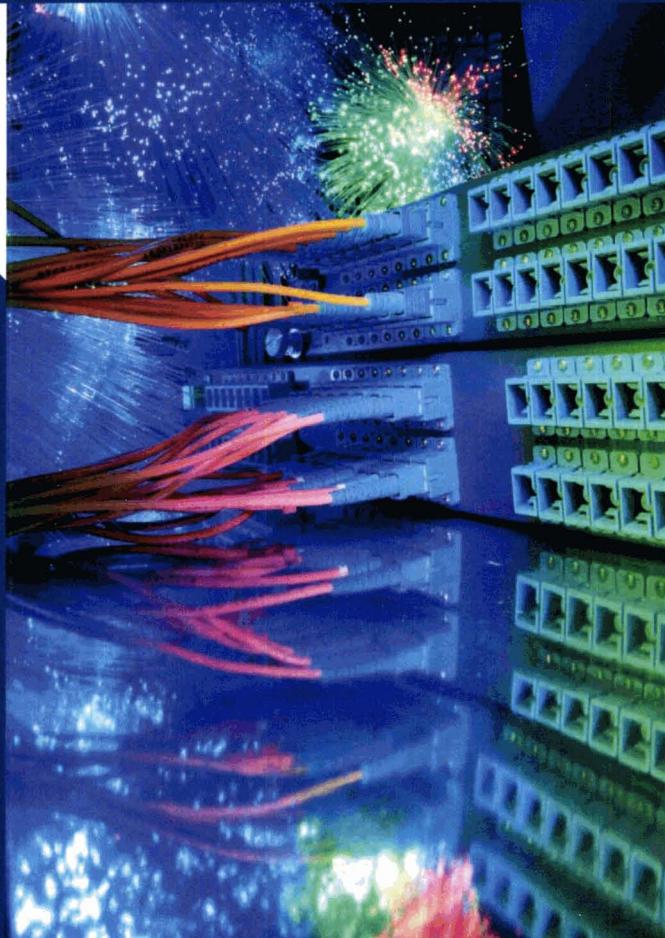
**Thales UK**  
2 Dashwood Lang Road  
The Bourne Business Park  
Addlestone, Nr Weybridge  
Surrey KT15 2NX  
Tel: +44 (0)1932 824 800  
[www.thalesgroup.com/uk](http://www.thalesgroup.com/uk)

**THALES**



# Vulnerability Assessment

## Global Cyber Solutions



In the digital age cyber space is a foundation for all of our daily activities. There are new threats emerging on a daily basis and it can sometimes be difficult to know which you are at risk from and how severe the impact of these threats could be.

At Thales, we have a detailed understanding of the cyber domain and the range of threats our customers face.

We have developed a methodology of helping you to understand your specific cyber domain, and how you can reduce the threats you face and become both cyber aware and cyber secure.

Our vulnerability assessment service will provide you with a detailed report on your vulnerabilities and a range of recommendations to help you overcome these issues. This low cost service will not only enable you to become cyber aware, but also give you a detailed understanding on cyber security and the elements included within it.

## The purpose

Undertake an exercise to determine the extent of vulnerability within an infrastructure or web application.

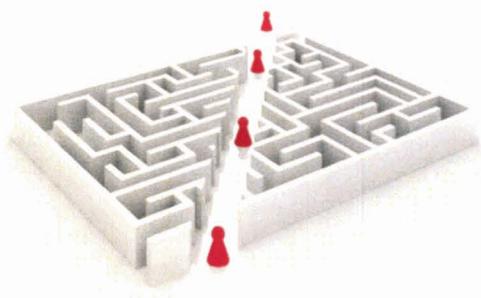
How we do it:

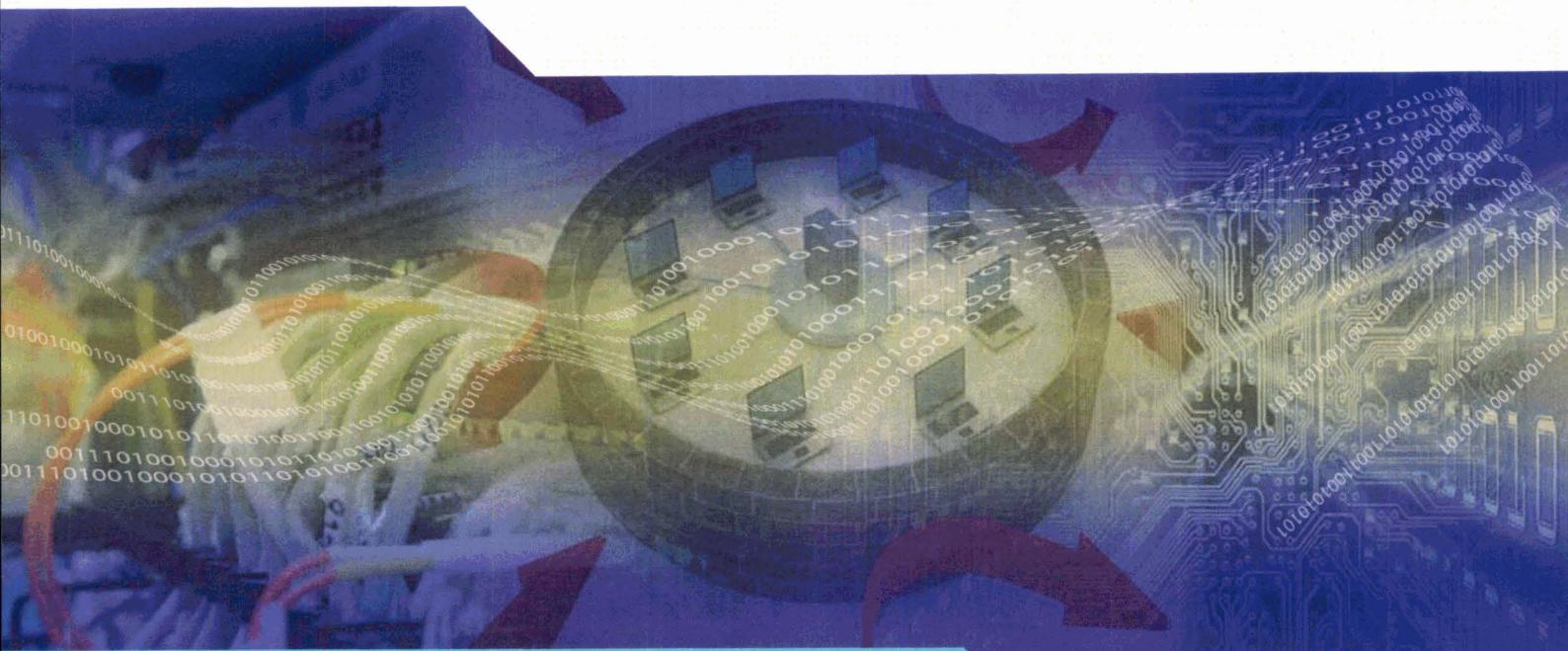
**Preliminary Assessment:** Prior to any work being undertaken our security consultants will work with your staff to determine the business objectives of the exercise and ascertain whether the vulnerability assessment is in response to a direct threat, security breach, or simply as a check to ensure systems are healthy and in good security order. Many organisations are required to meet stringent regulatory requirements surrounding their security and safety. Whatever the need or motivation we can tailor a service to suit your requirements.

**Proposal:** The preliminary work will result in delivery of a detailed proposal tailored to your individual needs.

**Vulnerability Assessment:** Using a combination of manual and automated tools and techniques, our highly skilled security consultants will undertake analysis of the target infrastructure or web application in order to determine the existence of and the extent of any vulnerabilities. The findings of the testing are mapped against good practice. All vulnerabilities are then categorised against a criteria of Criticality, Exploitability, Impact and Probability; this will illustrate the true risk levels and provide "in-context" advice as to how this could potentially impact your organisation.

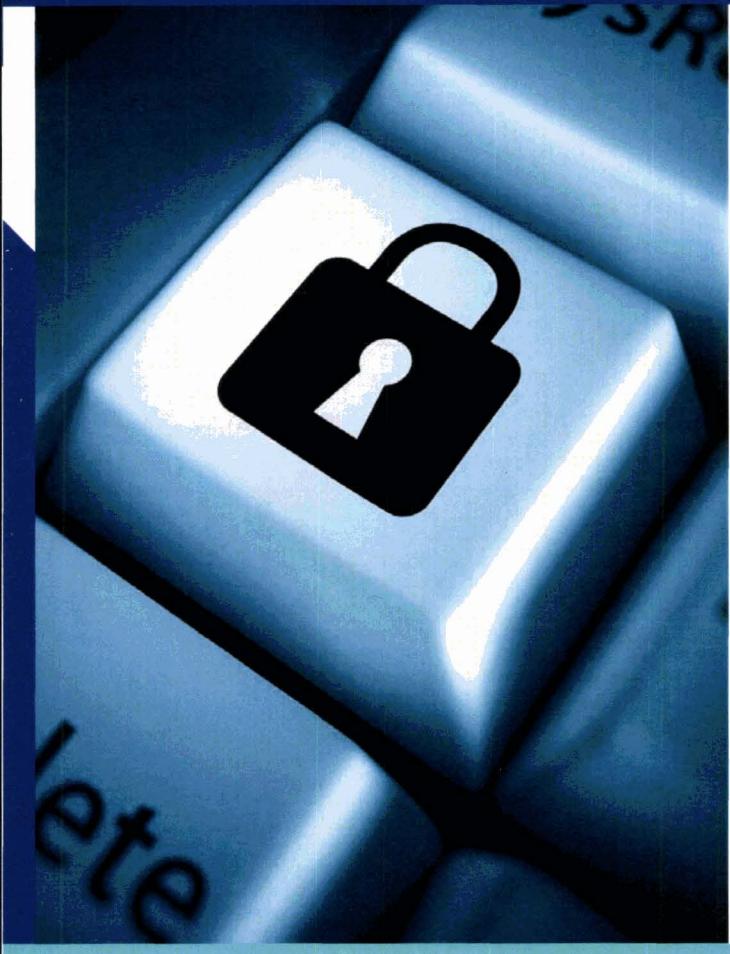
**Deliverable:** Reports are tailored to meet the needs of the Customers but in general we take pride in delivering high quality professional reports that outlines clearly the vulnerabilities identified during the assessment, their potential business impact and more importantly, recommends processes for remediation. The reports are designed to be relevant and readable at all levels from CIO board-level to the technical teams responsible for the IT Systems. We further aim to reduce technical jargon to a minimum whilst maintaining a high-quality and usable report. In addition, we are able to provide technical briefings and security awareness training to support the improvement of systems following on from the deliverable report.





## Holistic Auditing

### Global Cyber Solutions



Holistic Auditing – The 360° approach to security encompassing all factors rather than just the electronic security considerations.

This phase reviews all IT and Information Assets, the applicable threats and vulnerabilities. It considers the security of a business as a complete entity rather than just a series of disconnected elements.

This operates on the Thales doctrine: **HELP**

- Human
- Environmental
- Logical
- Physical

*Our holistic audits will help you to understand the cyber threat*

There are many factors that can impact on your level of cyber security. Many of these may not have previously been considered. These could include:

- Physical Security – Are your premises monitored by CCTV? Are there door access control mechanisms for potentially business sensitive areas? Are physical security measures circumvented for ease of use? Are your staff required to display company ID badges? Are unbadged visitors challenged?
- Personnel Security - Do your employees understand their role in Security? Are new starters subject to vetting, be that CRB, Credit Checking etc
- Procedural Security – What processes are in place to protect your security interests? Do employees sign and understand the computer usage policy? What measures are in place to monitor access to sensitive information? Are passwords changed when a breach is detected?

By identifying and considering the impact of vulnerabilities in these areas together the overall impact on security can be determined. We understand that security is not limited to any one single element and that cyber assurance should be considered in a holistic environment.

Holistic audits begin by engaging with you to determine your requirements and from them derive the best way forward. From this initial discussion we produce a proposal that is submitted to you for approval before the assignment commences. The proposal will outline your objectives, the methodology and actions to be undertaken by us to assist in meeting these objectives. At this point the deliverables and timescales are also defined for the work.

A variety of techniques are used to complete an audit dependant on the area being assessed. An audit requires significant effort in assessing policies, physical security measures and working directly with your team to determine how security is implemented in your organisation.

The outputs of a HA is a formal report that covers the vulnerabilities identified across all spheres, including their potential impact and associated risks to your business if they are not addressed.



**For more information contact us at: [cyber@uk.thalesgroup.com](mailto:cyber@uk.thalesgroup.com)**



# Cyber Security

## Global Cyber Solutions



---

Thales' cyber offering is structured around providing customers with a single point of contact to deal with all of their cyber security concerns.

At Thales, we recognise that as the cyber threat evolves rapidly it is often difficult for organisations to assess whether they are vulnerable and what they should do to protect themselves.

Thales recognises that each customer is at a different stage of maturity in managing their cyber security risk. To reflect this Thales has created a modular offering that will enable you to have access to a comprehensive cyber assurance service while only paying for the components that are pertinent to your business.

***Thales - committed to  
protecting your business  
from cyber attack***

## Consultancy

Our team of over 400 cyber security experts have extensive experience of working with defence, government and civil customers. We can quickly assess and understand issues pertinent to your business needs.

- Develop security strategies specific to your business operations
- Perform vulnerability and risk assessments to assess the risks to your business from cyber attack
- Recommend, design and implement improvements
- Deliver cyber and threat awareness training
- Change management

## Solutions

We are a world leader in providing modular, integrated cyber security solutions to meet your specific needs.

- Design and implement upgrades to the security of your existing business with minimal impact to your business operations.
- Pull through capabilities from the global Thales group and other key technology companies to deliver secure solutions that deliver tangible business benefits
- Use our world leading encryption product suite to protect your data

## Cyber Centre

Our Cyber Centre can be used for a range of activities including:

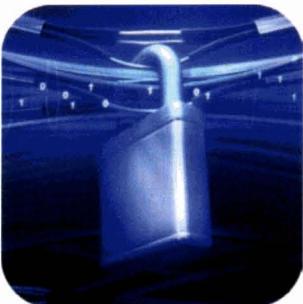
- *Performing Cyber Exercises* - testing whether you have the right recovery and incident procedures in place when an attack occurs
- *System Cyber Testing* – emulating and testing existing systems to establish areas most susceptible to attack
- *Solution design and testing* – using our engagement strategy across the cyber domain supply base to provide new integrated solutions that best suit the risk associated with your business whilst minimising cost and operational impact
- *Cyber Training Facility* – enables training of your employees on cyber issues and provides awareness of business impact

## Services

We have services to support your business in the implementation of security requirements in a cost effective way.

- Data and web hosting
- Security Operations Centres
- Network Operations Centres
- Data storage up to IL5

## *Thales - Simplifying Your Cyber Security*



[cyber@uk.thalesgroup.com](mailto:cyber@uk.thalesgroup.com)



Thales Copyright 2012 - The document is the property of Thales UK. Reproduction and distribution is strictly forbidden without prior written consent from Thales UK



## Cyber Domain Expertise

### Global Cyber Solutions



Threats to digital systems regularly change and evolve. Managing the way you assess, monitor and protect your business assets is key to maintaining business productivity and continuity. Loss or exposure of your information can be catastrophic in both financial and reputational terms.

Thales has a dedicated cyber security team within the UK that can assess your business needs and determine the most cost effective way of securing your information and reducing and managing the risks affecting your organisation.

Our structured, interactive security engineering approach, provided by our highly skilled cyber engineers, utilises governing information security legislation and regulations to ensure that a comprehensive, cost effective security solution is provided.

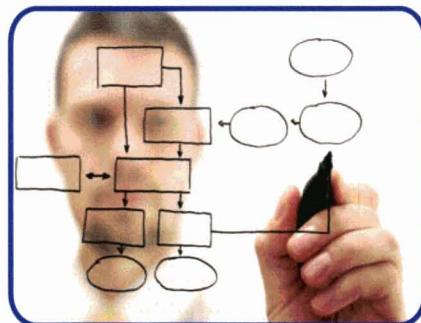
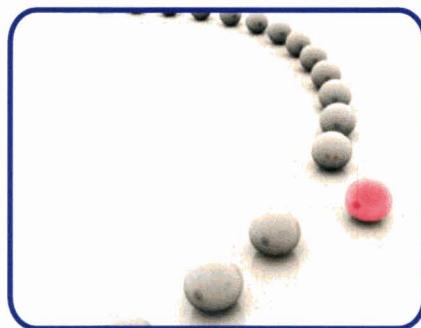
***Thales - providing your  
business with the expertise  
to solve your problems***

Thales has extensive experience in providing end-to-end security solutions to Government, CNI, finance and military organisations. Based on our proven expertise in delivering security solutions, and working within your industrial domain, we can provide a unique security service to meet your specific needs.

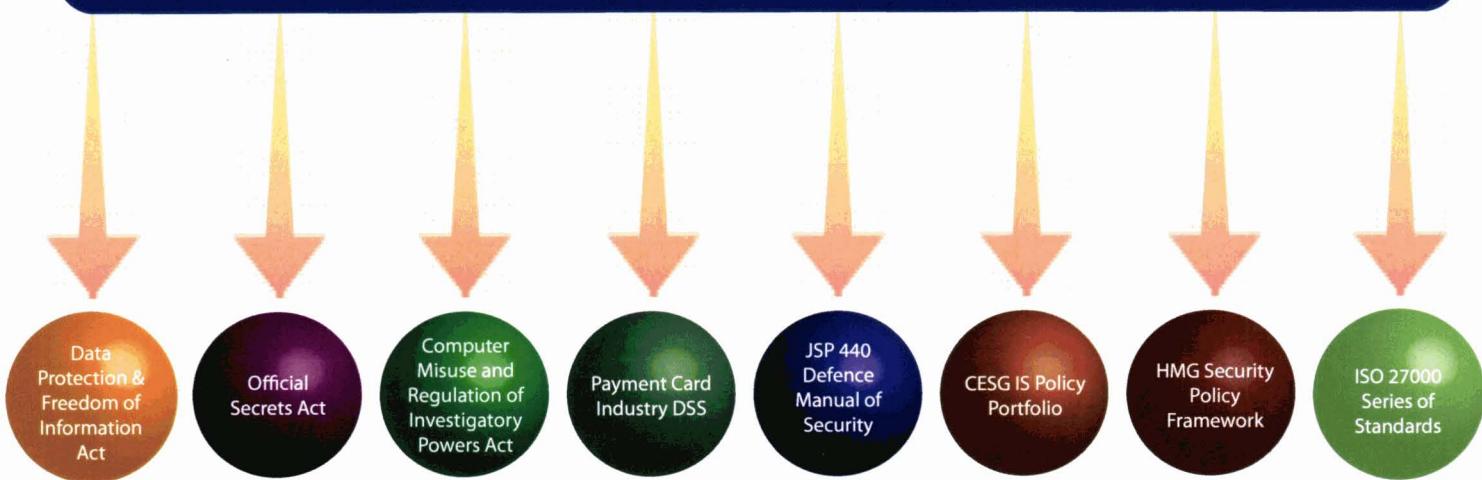
Backed by industry standard qualifications and certifications, including CLAS, CISSP and ISO27001 Lead Auditor, our cyber practitioners are perfectly placed to give up to the minute advice on the latest technologies and products whilst remaining vendor neutral.

Our wealth of experience in accreditation and evaluation processes will allow you to maximise benefit and efficiency from your relationship with CESG, the Defence Security Assurance Service (DSAS) and Central Sponsor for Information Assurance (CSIA), assisting you in achieving necessary accreditation for your security system.

Thales provides security based solutions tailored to your specific needs, using proven engineering principles. Our cyber consultants are able to provide subject matter expertise across a wide range of security domains, from risk assessment and mitigation, disaster recovery and cryptography, to physical security, infrastructure security and identity and access management.



### Our team of cyber domain experts have experience in:



For more information contact us at: [Cyber@uk.thalesgroup.com](mailto:Cyber@uk.thalesgroup.com)



# Penetration Testing

Global Cyber Solutions



Thales' range of Cyber Security solutions can help you become cyber aware so that you can fully understand the threats you face both now, and in the future. Our penetration testing goes one step further than our vulnerability assessments and will highlight how cyber threats against your organisation could be exploited.

Our penetration tests will demonstrate the real-life implications of potential security vulnerabilities in a controlled manner. This is applicable both to infrastructure and web applications. A penetration test typically simulates real-life threats posed to infrastructure or web applications.

*By helping you to understand  
how cyber threats can  
impact your organisation we  
can improve your cyber  
assurance*

*How its done:* As an extension of the Vulnerability Assessment, Penetration Testing goes one step further than just discovering the vulnerabilities; it seeks to demonstrate what could be leveraged by an attacker as a result of missing operating system patches, mis-configured web servers or web applications.

*Preliminary:* As for Vulnerability Assessments, all engagements begin with a customer meeting to determine the business drivers behind the penetration test. Is a new web application about to be launched do you want to determine whether it is secure or not, or maybe you are seeking to demonstrate your network security environment to a potential new client.

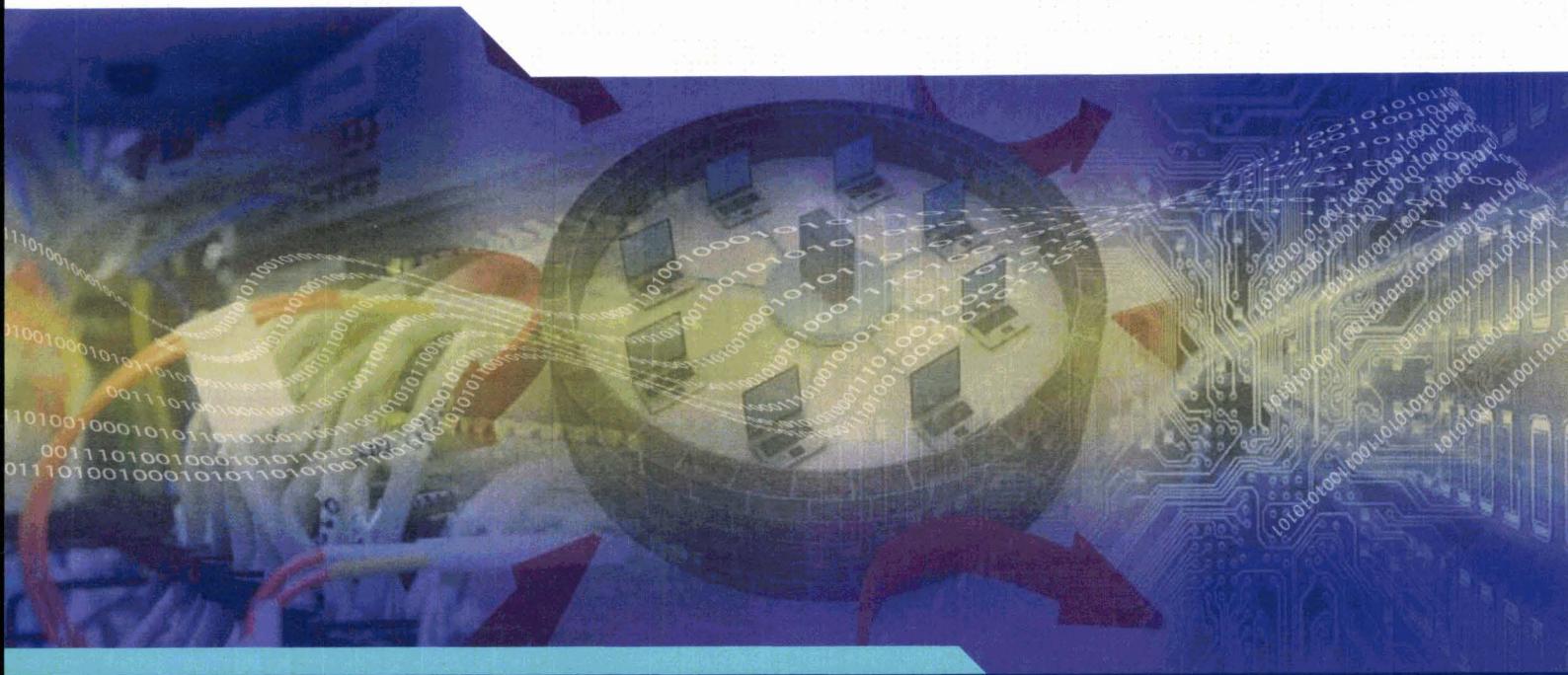
*Proposal:* This clearly identifies the business objectives of the testing, the scope of the testing whether it be the remote access portal, web application, network infrastructure and/or branch office environment, the permissible techniques and strategies for the security consultant to use. It will also provide you with a clear indication of the effort required to complete the assignment.

*Penetration Testing:* An extension of a basic Vulnerability Testing. The first step of a penetration test is to determine what vulnerabilities lie within a particular infrastructure or web application. Systematic testing allows for the easy identification of vulnerabilities that may be easily exploited or, yield the opportunity when perpetrators are attempting to compromise a network or application. From this, tested vulnerabilities are categorised against criticality and exploitability. Once the exploitable vulnerability points of entry are identified the security consultant will attempt to gain access to the system or web application in order to obtain evidence of compromise, this may be the result of a single vulnerability or by multiple interconnected vulnerabilities. This evidence is maintained as substantiated proof and will be documented in the final report.

*Deliverable:* Reports are tailored to your individual needs which will typically be a final report outlining the findings of the penetration test and include which vulnerabilities were identified, which were found to be exploitable and what evidence of the exploit is available. This will provide evidence of which system was compromised, and was retrieved in order to prove that access was obtained. The reports are designed to be relevant and readable at all levels from CIO to the technical teams responsible for the IT systems. The reports are designed to reduce technical jargon to a minimum while maintaining a high-quality and usable report.

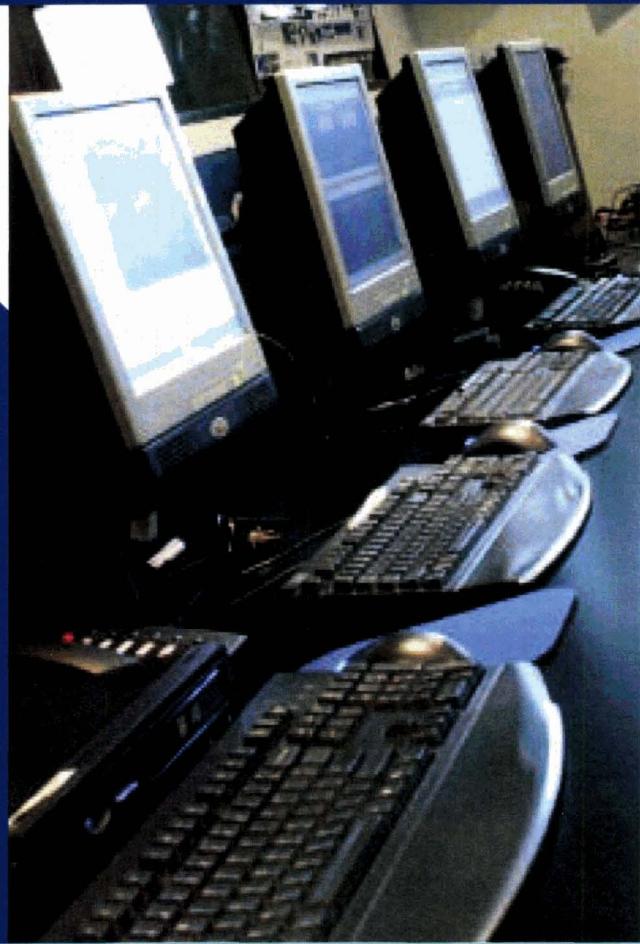


For more information contact us at: [cyber@uk.thalesgroup.com](mailto:cyber@uk.thalesgroup.com)



## Cyber Centre

Global Cyber Solutions



The modern business environment is reliant upon interconnected networks and communications.

This leaves businesses vulnerable to cyber attacks, whether this is interception of bank transactions, theft of intellectual property or other malicious and damaging attacks. Effective cyber security does not need to be expensive but does require a comprehensive approach.

At Thales we have developed a Cyber Integration and Innovation Centre where we integrate solutions that address customers' concerns; work with innovative companies to help develop solutions for tomorrow's problems and bring evolving technology to the market more effectively.

***The Thales Cyber Centre - combining Innovation and Integration to protect the UK's future***

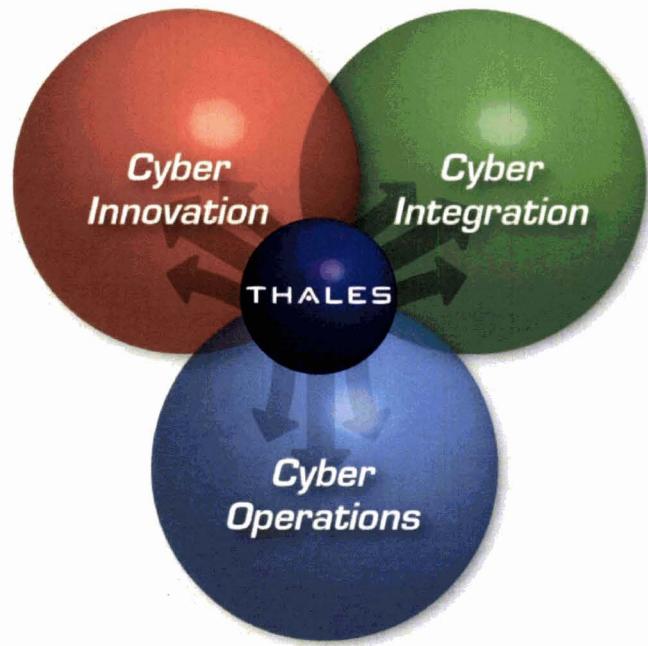
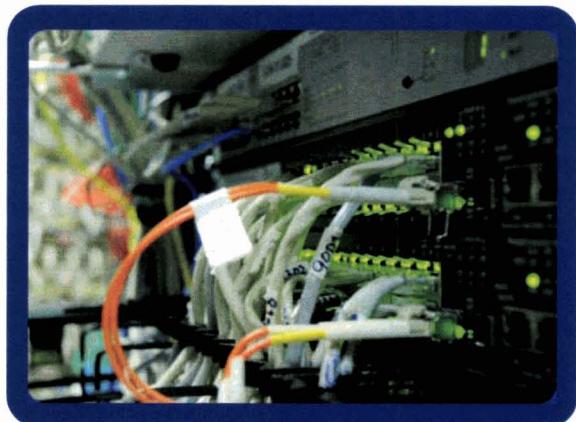
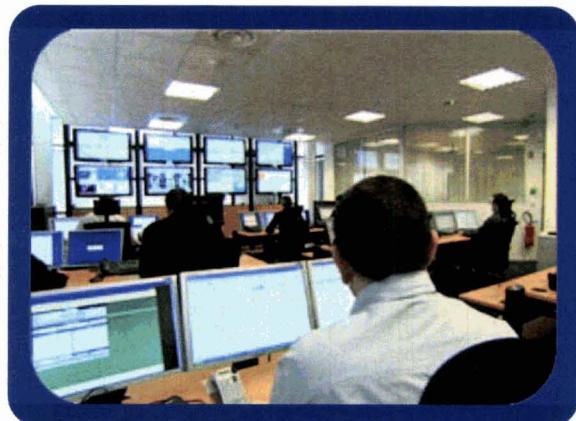
The Thales Cyber Integration and Innovation Centre has been developed to help customers understand the impact of cyber attacks upon business operations. Our cyber security experts provide customers with peace of mind that existing or new solutions are configured, operated and managed in a manner that provides maximum security.

The Cyber Centre can be used for a range of activities including:

- **Solution design and testing** – using our engagement strategy across the cyber domain supply base to provide new integrated solutions that best suit the risk associated with customers' businesses whilst minimising cost and operational impact
- **Cyber Innovation** – performing feasibility studies on emerging technologies to determine how they can best support evolving markets
- **Cyber Training and Awareness** – providing a facility that enables customer training on cyber issues and provides awareness of how it can impact business
- **Performing Integration Assessments** – testing the configuration of customer systems ensuring maximum return on their investment

Coupled with our own technologies and expertise the Cyber Centre and its team are committed to helping small and innovative companies. We can provide the platform to enable smaller companies to test and showcase their technologies in a replicated, real-time environment. This ensures that our customers have access to cutting edge innovation in cyber security, anticipating and addressing tomorrow's problems.

***Thales - Committed  
to protecting your business***

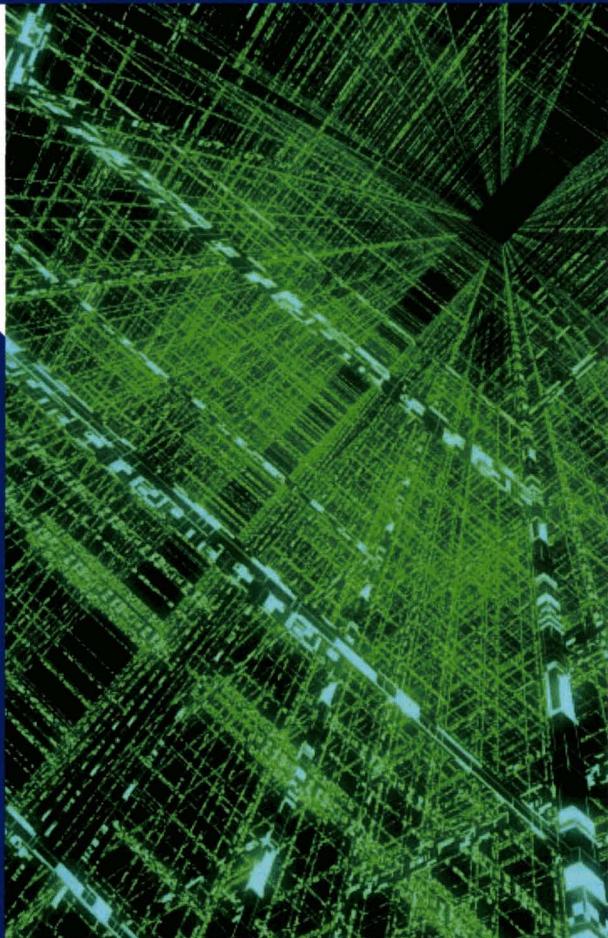


For more information contact us at: [cyber@uk.thalesgroup.com](mailto:cyber@uk.thalesgroup.com)



## Vulnerability Assessment

### Case Study - UK Utilities Business



At Thales we recognise that everything in cyber space is under threat from attack. Stored data, networks and data transfer systems are all high risk targets and the results from attack can be devastating to both business and the individual.

To counteract this threat we have developed a range of vulnerability assessment techniques designed to help reduce the impact of these threats and maintain the integrity of systems and data.

In our specialist, and accredited, Cyber Centre we can recreate a network environment in order to carry out rigorous testing and analysis to establish the level of security risk and then develop solutions to overcome these threats.

***Thales - protecting your  
networks, data and  
business assets***

## Customer Requirement

Undertake a vulnerability assessment of a control network for a UK utility company.



## The Process

Thales identified the business assets that were core targets and most vulnerable to attack.

VA techniques were employed to perform an assessment of active vulnerabilities.

## Recommendations

Thales provided recommendations that enabled the company to:

- Immediately resolve the identified vulnerabilities, by changing configurations of components
- Improve their processes and procedures
- Provide awareness for the staff to help the company undertake regular periodic testing of critical business assets and connected systems
- Recommendations for separating critical and non-critical networks with no impact to the business operations

## The Findings

Thales identified that whilst the configuration of the business assets were secure, connected network infrastructure had vulnerabilities which exposed the critical business assets to attack.

Vulnerabilities were identified in:

- Use of default passwords and usernames for 'non-critical' components that provided a path for attack to critical assets
- Missing patches
- Unprotected web pages to printer system, enabling interception
- Remote login pages available with minimal security

## Key Customer Benefits

This service provided the following benefits to the customer:

- For minimal cost the customer gained increased network resilience without any interruption or impact to their business operations. The increased resilience reduced the risk of disruption to the utility supply hence reducing the risk of fines from regulators
- Employees were made aware of cyber considerations and how to perform internal analysis, thus reducing the risk of future upgrades causing a vulnerability
- Increased awareness of cyber security for employees

For more information contact us at:

[cyber@uk.thalesgroup.com](mailto:cyber@uk.thalesgroup.com)