SECURE COMMUNICATIONS AND INFORMATION SYSTEMS

CVI

Cyber Vulnerability Investigation Whitepaper
Executive Summary

Businesses are spending an increasing amount of money on cyber security in all areas. The justifications for that spend is often made through complicated risk management activities performed by various departments and actors within the business. Therefore, despite an increasing amount of money spent it is often difficult to assess or quantify the effectiveness of it i.e. was the money well spent? It is a common refrain to hear that cyber security is really just risk management - you manage your security by managing the risk. By adopting this mind set there is a danger that risk management is seen merely as a compliancy activity undertaken by the IT department, and that once compliancy is achieved the cyber security risk to the business has been adequately managed.

A poor compliancy approach tends to look at the conceptual implementation of technical controls in isolation to the physical and procedural controls. It doesn’t take into account how the system will be operated in the real world and how physical/procedural vulnerabilities could be exploited in combination with technical vulnerabilities to cause a real-world impact to the business. Crucially, this creates a disconnect between those that implement risk mitigation and report compliancy to the board and the users who need to practically use the system in the real world to meet the business objectives.

Thales recognises that for business decision makers the critical question they need an answer to is ‘…do my security controls manage the vulnerabilities that could cause an unacceptable impact to my business’.

Business executives need to be actively engaged in the cyber security risk management process as they would with any other type of risk to their business. It is unreasonable to expect them to have an in-depth knowledge of the technical vulnerabilities, threat actors, and causal impacts, such as physical/procedural issues necessary to participate deeply in the risk management activities. They need to know the implications of cyber vulnerabilities and their impact on investment and profitability and take steps to mitigate them in a pragmatic and proportional manner.

This paper describes a bespoke Cyber Vulnerability Investigation (CVI) approach, which can be tailored to the business. It will carry out a socio-technical assessment to identify what could go wrong with their IT estate, what vulnerabilities (or combination of physical and technical vulnerabilities) could be exploited, and which would cause an unacceptable impact to the client’s business. This approach provides recommendations to address identified issues and provides evidence to:

- Support investment decisions and where necessary re-prioritise investment in line with the risk management objectives.
- Promote an understanding of the real current cyber security posture
- Support assurance activities
- Re-invigorate the cyber security risk management process, where necessary

By applying the CVI process, both on specific projects and within the general organisation, a clear link can be achieved between the business objectives and cyber security risks. This ensures that investment decisions related to control measures are proportional to the potential impacts, and critical vulnerabilities are consistently and effectively being managed.

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>2</td>
</tr>
<tr>
<td>It is inevitable that an organisation will be subjected to some form of cyber-attack</td>
<td>4</td>
</tr>
<tr>
<td>All organisations need to deal with the uncertainty</td>
<td>4</td>
</tr>
<tr>
<td>What is Thales Cyber Vulnerability Investigation?</td>
<td>6</td>
</tr>
<tr>
<td>Security Policies and Governance Module</td>
<td>7</td>
</tr>
<tr>
<td>Human Factor Analysis Module</td>
<td>8</td>
</tr>
<tr>
<td>Pentest Module</td>
<td>8</td>
</tr>
<tr>
<td>Internet Footprint Module</td>
<td>8</td>
</tr>
<tr>
<td>Information Assurance (IA) Module</td>
<td>10</td>
</tr>
<tr>
<td>Conclusion</td>
<td>11</td>
</tr>
<tr>
<td>Why Thales CVI?</td>
<td>11</td>
</tr>
</tbody>
</table>
**IT IS INEVITABLE THAT AN ORGANISATION WILL BE SUBJECT TO SOME FORM OF CYBER-ATTACK**

The recent National Cyber Security Centre launch report[^1] stated that the number of potential attackers will grow as the falling costs of technology make it more accessible. Internet usage will increase in the developing world and thus more states will develop their espionage and offensive cyber capabilities. The widespread adoption of technologies such as autonomous/unmanned systems and the internet of things will increase the number of exploitable vulnerabilities. An increasing dependency on information and communications technology to achieve efficiencies will mean that businesses will be more susceptible to potential attacks.

The increase use of technology will increase the opportunity to exploit technical vulnerabilities, however technology does not exist in isolation, it is installed in the real world and operated by people to create positive outcomes. Most successful attacks are based on the exploitation of a combination of technical and non-technical vulnerabilities:

- The lack of physical security provides the opportunity to a physical intruder to masquerade as a contractor and plant an unauthorised mechanism into the infrastructure to extract data
- An employee, who is an authorised user of the system may miss-use their privileged access to steal customer credentials and account details by writing them to a USB stick and then leaving the company premises

**ALL ORGANISATIONS NEED TO DEAL WITH THE UNCERTAINTY**

Whether it is a business that is worried about a change in the market that could cause it to fail, or unforeseen events which could disrupt the provision of critical national infrastructure, such as rail, air, nuclear power and water. All organisations rely on technology, systems and information to support their objectives; thus, they need to apply the same level of rigour to address the risk posed by the use of technology as they would regulatory, financial, strategic or operational risks. How that technology is actually used in practice may not be how it was designed to operate or should be operated. The effect of cyber risk is hardest felt when it has a direct unacceptable impact on an organisation’s activity.

- The observation that an internet facing firewall may have an exploitable vulnerability will not necessarily mean anything to decision maker. Their interest would increase if it was used in combination with other technical, physical or procedural vulnerabilities to disrupt or deny the use of a safety critical service. The potential disruption to the service may be measured in loss of revenue, but could also cause a regulatory and reputational damage, all of which could be an unacceptable impact to the business.
- The relaxation of media access controls between systems may facilitate the immediate need to exchange data, but combined with other physical and procedural weaknesses may cause the theft of sensitive data. The impact of this could be contravention of regulatory controls for protection of personal data, which results in a punitive fine with an unacceptable consequential loss in reputation and potential reduction in profitability.

In recent years, cyber security risk has started to take a more prominent position on business agendas. This has resulted in organisations adopting recognised standards and assurance schemes, such as the ISO 27001 series, Defence Cyber Protection Partnership and Cyber Essentials (plus) predominately to pre-qualify for a market and establish cyber credentials. Though these approaches promote a risk management regime, it has driven a compliancy culture delegated to the IT Department resulting in:

- Specialists staff motivated by high levels of security, who are overly cautious, leading to additional cost and complexity for users
- A disconnect between the assumptions made in the risk assessment and the reality of how the system is really used in its environment
- The compliancy assessment becomes the main objective, rather than active risk management at board level; thus, they will not understand and manage the overall risk exposure to the organisation
- Compliance not aligning with the rapidly evolving business environment or emerging threats with the adoption of new technology.
- Decisions about the implementation of controls without understanding the current business priorities and the amount of risk it is willing to tolerate
- The residual risk to the business not being escalated to an appropriate level as there is not a clear governance structure

The board should regularly review risks that may arise from the use of technology or systems that represent an unacceptable impact to the business. To ensure senior ownership and oversight, the risks resulting from attacks should be documented in the corporate risk register and regularly reviewed. For the board to carry out these activities effectively it needs to:

- Know what is important to it in terms of people, assets and information
- Know what the unacceptable impact is to those assets and how much risk it is willing to tolerate and provide clear direction to the organisation.
- Communicate to its staff how risk is to be escalated and how it is to be presented
- Constantly monitor cyber security risks as they would other business risks and incorporate it within their business change processes

The Thales Cyber Vulnerability Investigation (CVI) provides a mechanism to get under the bonnet of your business, focus on what is important to your business’s continued survival and get a clear understanding of whether you have the right structures and controls in place to manage your cyber risks. It can direct your efforts and investment to ensure that you continue to deliver improvements.

[^1]: The launch of the National Cyber Security Centre (NCSC) Report dated 14th Feb 17

---

[^1]: The launch of the National Cyber Security Centre (NCSC) Report dated 14th Feb 17
in your cyber security posture, rather than just deliver compliancy.

**WHAT IS THALES CYBER VULNERABILITY INVESTIGATION**

By providing a scalable and modular approach to delivering a Cyber Vulnerability Investigation (CVI), Thales UK will offer a comprehensive and cost-effective solution to organisations that require external Subject Matter Expertise (SME) support. The output report will provide sufficient, detailed information to enable the senior management to understand their cyber vulnerabilities, how these could cause unacceptable impacts to their business and make recommendations on the implementation of effective and proportional mitigations. The customer will be given an opportunity to review the report and comments will be noted and addressed to the customer’s satisfaction. In addition, our specialists will present their findings to the customer’s key stakeholders to facilitate the CVI business objective.

The Thales Cyber Vulnerability Investigation approach comprises an initial scoping stage, followed by a data collection and reporting stages as illustrated by Figure 1.

The scoping stage is initiated by a site visit, which may require follow-up meetings dependent on the size and scale of the requirement. It is designed to establish the business objectives of the CVI, understand the business, how it operates and the dependant services that it has reliance on. It will determine the value of the business assets and what constitutes an unacceptable impact to the business. It will also establish any constraints such as budget, geography or processes and agree the boundaries of the investigation in terms of physical locations, business organisations and system architectures. It is also used to identify key stakeholders, CVI modules and documentation that will be required for the data collection stage. Thus, the scoping stage will agree:

- The scope of the applicable CVI modules to address the customer’s business objectives.
- The priority of effort and areas of specific concern based on an understanding of the businesses critical assets/activities and unacceptable impacts to the business.
- Inputs required supporting the CVI, such as architectural diagrams, corporate policy and risk management documentation.
- The method for validating or simulating the impact of a vulnerability on the system.
- Site and network access levels.
- Timescales compatible with both the organisation and Thales UK SME availability.

The Thales UK point of contact to provide the interface between organisations “the customer friend” element of the co-ordination element of the task.

A formal Thales UK proposal of work.

The Data collection phase will initially implement an attack tree assessment based on the input agreed from the scoping phase. This will allow us to model the system to determine the combination of physical and cyber vulnerabilities that represent and exploitable attack paths that could have an unacceptable impact to the business, based on the value of the asset, whether that is information, process, equipment or people. The CVI will then implement the agreed CVI modules as illustrated in Figure 2. These modules will identify the true vulnerabilities to the business and compare that with the attack tree assessment. We will determine the effectiveness of existing controls and make recommendations on additional controls in proportion to the impact. This will enable positive results to be delivered to the customer no matter what the size or scope of their business.

**SECURITY POLICIES & GOVERNANCE MODULE**

Defining and communicating the organisation’s approach to risk management is crucial to ensuring that employees, subcontractors and service providers are aware how cyber risk is going to be managed. Without a clear governance structure, with defined escalation paths and decision points, the board won’t have confidence that its stated policies are being consistently applied across the business. Crucially the board will not have a realistic picture of the risks that they are exposed to, which could have an impact on their business.

The key aspect of this module is to not only to determine if the appropriate policy exists, but more importantly what is actually happening within the business. If the user of the system is unaware of the corporate security policy and their role, then they cannot contribute to the secure operation of the system or business. It might indicate weaknesses in the procedural area and governance regime that in combination with other vulnerabilities could be exploitable by a potential attacker. If a user doesn’t know the value of a particular asset or piece of information, then they may inadvertently transmit it out of the organisation to someone who shouldn’t have it.

The Security Policies and Governance Module is initially delivered by desktop review of the customer’s security policies, processes and procedures related to:

- Risk Management Strategy
- Incident management
- Business continuity
- Change management
- Supply Chain management of outsourced services

The key aspect of this module is to follow up the desk top review with interviews with various stakeholders to establish its effectiveness, specifically:

- Key security appointments identified within the organisation, such as IT Security Officer, Senior Information Risk Owner, Security Operation Centre Manager and IT Service Provider
- Users of the systems within the organisation
- Representatives from organisation that provide relevant services
HUMAN FACTOR ANALYSIS MODULE
The end user of a system or network provides a real-time and constant insider threat to the security of the enterprise. Technical controls are also dependent on the application of physical, personal, and procedural controls, which the user can circumvent. This circumvention is normally due to the impractical applicable of technical controls, which get in the way of the business process or a lack of awareness/knowledge of what is required by the user.

Thus, an educated, motivated, and focused user can be an enhancement to cyber security. By developing a culture of reporting incidents within a no blame environment, then an organisation can use their own staff to police their cyber security policy. This identifies weaknesses and allows resolutions to be put in place.

The Human Factor Module is delivered by interviewing via a question set the organisational personnel across a wide range of skills, posts and experience, or by the utilisation of several bespoke software tools assesses trends and HF patterns via CHEAT. This enables a comprehensive assessment of the organisation's security ethos and mindset at that point in time to be articulated, including:

- Security ethos and level of understanding across the staff
- The overall security culture of the staff and encourage a “note it – report it” approach
- Areas of weakness that would benefit from additional, periodic staff training or changes to induction processes

An assessment of the level of security culture is incorporated within the final report and areas of vulnerabilities are incorporated within the attack tree assessment to determine if they in combination with technical vulnerabilities could cause an unacceptable impact to the business.

PENTEST MODULE
Any critical vulnerability in an existing infrastructure could be exploited by either an internal or external attacker. By identifying these weaknesses and applying remediation, the business can maximise the effectiveness of their existing controls.

Rather than just sweeping the entire infrastructure for vulnerabilities to address a technical objective, our attack tree assessment will identify what aspects of the system/infrastructure are critical in terms of unacceptable impact to the business. Thus the focus of the penetration testing is addressing a specific business objective rather than a technical objective.

Thales UK has a team of PENTEST engineers who specialise in identifying weaknesses and vulnerabilities within networks conducted from multiple points of access (WiFi, network connections and server/administrator access options) via automated and manual scans.

The PENTEST Module identifies areas of weakness within the organisation including:

- Firewall configuration to ensure maximum protection is achieved
- Identifying port configuration to expose lockdown concerns or weaknesses
- Locating software conflicts (multiple versions of software, redundant software vulnerabilities)
- Provision of SME advice to the network management team
- Network and device “lock down” advice

Vulnerabilities can be assessed for their potential impact to the business and closed in coordination with the site system administrators on site, with a comprehensive set of findings and recommendations being included within the formal report.

INTERNET FOOTPRINT MODULE
Organisations are now required to have a digital presence on the internet, whether to promote and sell their goods or in the case of public bodies to provide information and services to the citizen. These potentially provide a source of information to facilitate an attack or provide sensitive data about individuals or organisations businesses activities. They identify potential targets for cohesion, bribery, or social engineering attacks either using on-line or face to face engagements masquerading as potential customers or partner organisations. In addition, the disclosure of information in the public domain could represent an unacceptable impact to an existing customer or business partner relationship.

Our attack tree assessment will determine the value of business information and what is considered an unacceptable disclosure by the business. By understanding your internet footprint, businesses can understand their existing exposure, what corrective action they

1The human element has been identified as contributing to 95% of all cyber incidents and 37% of data breaches.
2Cyber Human Error Assessment tool (CHEAT) is an example of such automation.
may need to take to reduce it and provide meaningful guidance to their staff and sub-contractors. Thales UK can provide open source internet monitoring investigations to enable an organisation to:

- Identify its internet footprint
- Provide a portfolio of sites that contain organisational information.
- List social media sites containing specific organisational references
- Identify any exposure of personal data (staff names, addresses et al)
- Links to 3rd parties or sub-contractors and their internet footprint
- Additional areas where the organisation could benefit from the wider exploitation of web services

A comprehensive report will be provided as an annex to the formal report articulating and highlighting the footprint identified by open source investigations.

**INFORMATION ASSURANCE (IA) MODULE**

Extant IT enterprise evolves overtime to accommodate the introduction of new systems and people naturally adapt processes to accommodate. The adoption of new technology, combined with other factors can introduce vulnerabilities that may be exploited. The IA Module identifies methods and scenarios which could be used to solicit sensitive data from the enterprise, modify data/software or disrupt and prevent the use of systems. Several skills and methods are used to identify areas of poor cyber hygiene, including:

- Physical area inspections to identify poor electronic practices such as shared passwords or accounts, passwords written within the workspace and poor equipment husbandry or accounting
- Electronic inspections to identify:
  - USB device usage and sharing via electronic logs
  - Missing or out date Anti-Virus (AV) definitions or engines
  - Unsuccessful log-on attempts
  - Unauthorised software usage and expired software versions
  - The manufacturers patching state for servers and end user devices
- Unauthorised Wi-Fi transmissions within secure or sterile areas
- Open or un-assured Wi-Fi access points within the organisation
- Desktop security architectural review to identify gaps and make recommendations proportional to the risks

On completion of the IA Module an on-site briefing will be provided to identify any critical vulnerability which could have an unacceptable impact to the business prior to the release of the formal CVI report. The formal CVI report will articulate the recommended remediation options proportional to the agreed impact to the business. Return visits to assess the progress in resolving identified IA vulnerabilities can be considered within an agreed resolution timeline.

### Conclusion

A compliancy ‘Box ticking’ regime leans to a control centric security approach, which will provide a false sense of security. Controls may not align to how the system is actually being used within the business by your employees. The application of a Cyber Vulnerability Investigation will actually look at how your system is used, determine what the real world unacceptable impacts are and whether your existing compliancy based controls are actually addressing your vulnerabilities.

The opportunity to implement a positive attitude towards security within your workforce represents the next level of maturity in Cyber Security. By enhancing your employee’s ability to implement good security practice you increase the number of personal, who are policing your Cyber policy and culturally you will create an environment/ethos where security is seen as a positive enabler.

Not only this, but at a board room level, the investigation can help business leaders make more informed, effective risk management and investment decisions, and reap the consequent operational and financial benefits.

**WHY THALES CVI?**

- It can be tailored to meet the business objectives, whether it be a bespoke project, department or wider organisational activity.
- It can be used as a benchmarking exercise to set priorities for remedial actions and support investment decisions.
- It can be used as an independent business assurance activity to support a key procurement decision.
- Thales Cyber Consulting has fully qualified CESG Certified Information Assurance Professionals (CCP) and Information Assurance specialists who have worked extensively with Government, MoD, Critical National Infrastructure and corporate organisations and can deliver whole life risk management strategies that will enhance the security of your systems and their information.

Our Security Practitioners have extensive experience working with Security governance policies and procedures, these include HMG Security Policy Framework (SPF), UK MoD Joint Service Publication 440 (JSP 440), ISO/IEC 27001, Nuclear Energy, rail and automotive industries.