Cyber Growth Partnership Industry Guidance

ASSESSING CYBER SECURITY EXPORT RISKS

Human Rights | National Security

techUK representing the future

HM Government

FOREWORD

“We want British companies to succeed and for the UK to take the lead on business and protecting human rights. The advice in this document is not designed to constrain growth but to help companies reduce reputational risk and increase their profitability in the long term. We firmly believe that the promotion of business and respect for human rights go hand in hand.”

The growth of the internet has had a profound effect on societies, economies, and states. It has stimulated the development of commercial and government services online, improved communication and enhanced access to information across the globe.

As we all know, cyber space is full of risks as well as opportunities. The UK's cyber security industry has responded effectively to the risks, protecting networks from attack, helping to detect cyber crime, and delivering growth for the UK economy. We have one of the strongest cyber security sectors in the world and we want to ensure its continued growth and vitality. The Government aims to foster £2bn of cyber security exports by 2016.

However, some of the technologies that have transformed our lives for the better can also be misused. The export of particular technologies to the wrong hands could lead to human rights abuses or undermine UK national security. The Government has a duty to protect human rights and uphold national security by helping UK companies understand and manage the risks associated with cyber security exports.

The Government therefore welcomes the publication of this guidance from techUK through the Cyber Growth Partnership. It aims to help companies assess the legal and reputational risks associated with the export of cyber security products. Companies should use this advice to enhance their existing due diligence processes.

We want British companies to succeed and for the UK to take the lead on business and protecting human rights. The advice in this document is not designed to constrain growth but to help companies reduce reputational risk and increase their profitability in the long term. We firmly believe that the promotion of business and respect for human rights go hand in hand.

Ed Vaizey, MP
Minister for Culture and the Digital Economy

INTRODUCTION

Rapid advances in technology have changed the way we work, communicate, socialise, learn and do business, and they have enabled greater enjoyment of many human rights.

Cyber security products and services are used around the world to strengthen the integrity of critical national infrastructures, prevent the theft of corporate and personal data, and tackle fraud.

The export of cyber security capabilities presents the UK with a significant economic opportunity. The UK Government has recognised this and is working with industry through the Cyber Growth Partnership to help companies realise this growth. To advance the reputation of UK companies and uphold international norms it is vital that this growth is achieved responsibly.

The UN Guiding Principles on Business and Human Rights state that all businesses have a responsibility to respect human rights. The UK national action plan, Good Business – Implementing the UN Guiding Principles on Business and Human Rights, sets out the Government's commitment to the Guiding Principles and its expectation that companies ensure they are respecting human rights in practice at home and overseas.

techUK has worked with the Cyber Growth Partnership to develop this guidance, which provides cyber security companies of all sizes with actionable advice designed to help them identify and manage the risks of exporting their products and services.

The Cyber Growth Partnership is a taskforce of members from government, industry and academia that works to help UK cyber security companies increase their access to overseas and domestic markets and to increase the talent pool available to them in the UK. It is co-chaired by the CEO of BT, Gavin Patterson, and the Minister of State for the Digital Industries, Ed Vaizey MP.

techUK would like to thank BT, Lockheed Martin and 3sdl for their generous support in sponsoring and supporting this guidance. We would also like to thank the many prime and SME companies who contributed to the development of this guidance throughout the consultation and review process.

techUK would like to thank the Institute for Human Rights and Business (IHRB) for facilitating industry consultation and input into the human rights section of this guidance and for its central role in the drafting and review of the guidance. IHRB focuses on corporate responsibility to respect human rights and played no role in drafting the section that deals with national security risks in Chapter 4.

Defining cyber security capabilities

In the context of this guidance, 'cyber security capabilities' are defined as including the categories of capability in figure 1 below. Products are set out in the coloured boxes; the grey boxes show the layers of supporting services, which companies may also provide to customers:[1]

Figure 1: Cyber Security capability categories

1 This model is an elaboration by Dr Andrew Rogoyski of a segmentation developed in the 'Cyber, Identity and Information Assurance Strategy', US Department of Defense, August 2009

CONTENTS

EXECUTIVE SUMMARY

What is this guidance for? This guidance provides detailed background information and a framework to help companies develop their due diligence processes, enabling them to identify and manage human rights and national security risks associated with the export of security cyber products and services.

Why do we need it?

The export of cyber security capabilities presents the UK with a significant economic opportunity. HM Government has recognised this and is working with industry through the Cyber Growth Partnership to help companies realise this growth.

Most often cyber security capabilities are used only to defend networks or disrupt criminal activity. However, some cyber products and services can enable surveillance and espionage, or disrupt, deny and degrade online services. If used inappropriately by the end user they may pose a risk to human rights, to UK national security and to the reputation and legal standing of the exporter.

When should my company assess the risks?

Risk assessment should be ongoing; however, key points of assessment include:

- The earliest stage of product design and development.
- Pre-sale when bidding for a new export deal, renegotiating an existing contract, upgrading a capability, or selling a product domestically to another company which intends to incorporate it into a wider (exportable) package.
- At the point of sale when considering the level of risk posed by the potential sale and the mitigation available to reduce identified risk.
- Post-sale to monitor the ongoing situation in the destination country.

What is the benefit of adopting this guidance?

Developing a comprehensive due diligence process will help companies to identify and address human rights and national security risks linked to the export of their products. This reduces the likelihood of a buyer being able to use your technology to help perpetrate human rights abuses. It also reduces the likelihood of reputational damage to your company.

How does it work?

The guidance provides background information on various human rights and national security risks. It explains which capabilities can be misused, lists potential mitigations and sets out a framework for risk assessment. The diagram below summarises the key stages of the assessment process. For each step the company will need to gather information and carefully consider the variables.

How does my company reach a decision?

As with any risk management process, someone will need to accept responsibility for making a decision on the basis of the information available. The decision maker will need to consider the following:

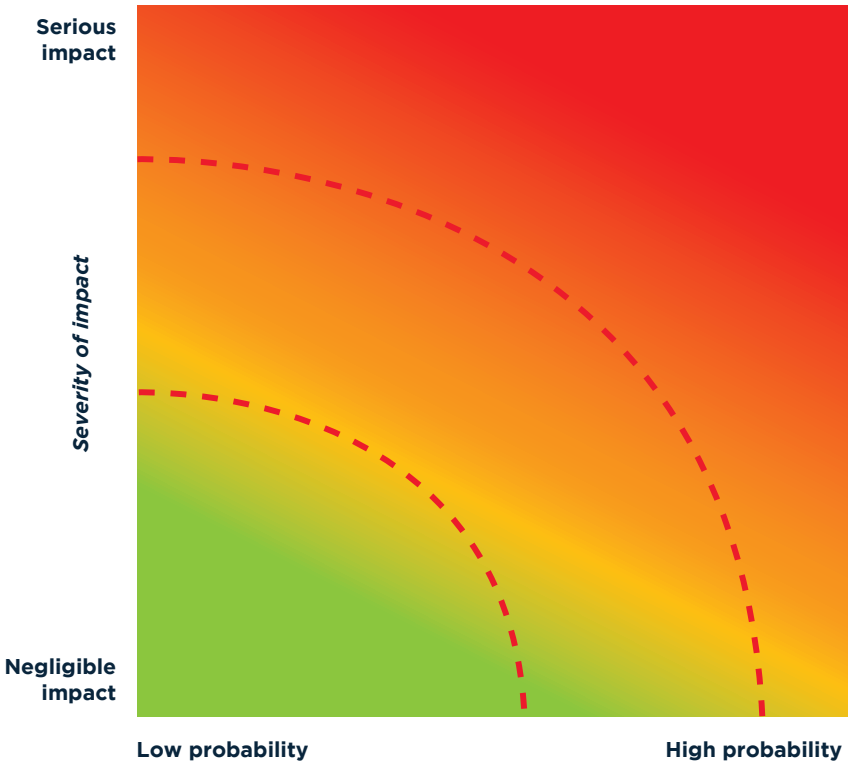
- What is the likelihood of an incident actually occurring?
- What is the potential impact?
- How strong and realistic are the proposed mitigations?
- Can the company defend itself effectively if something does go wrong?

N.B. For human rights risks the severity of the potential impact on an individual is a key consideration.

Recommendations

- Companies should adapt their own due diligence processes to reflect human rights and national security risks.
- Companies should stay alert to changes to the export licensing system and always check with the Export Control Organisation if in doubt.
- Cyber is a rapidly evolving area with numerous challenges; these can be tackled more effectively by working together. Companies should share lessons learned, especially viable mitigations through techUK so that this guidance can be updated to benefit all UK cyber companies.
- When support is required, companies should consult HM Government early on to allow government officials time to carry out their own due diligence process.

Determining the human rights risk



CHAPTER 1:

AIMS AND OBJECTIVES

1.1 Aim

Chapters one to three of this guidance are designed to help companies assess potential cyber security export opportunities to ensure that they do not negatively impact on human rights.

1.2 What will this Guide do for my business?

There is a strong business case for respecting human rights, as set out by the UK Business and Human Rights Action Plan.[2]

- Reputation and brand value can be protected and enhanced;
- It reduces the risk of litigation for human rights abuses;
- Customer base can be protected and increased as consumers increasingly seek out firms with higher ethical standards;
- It helps to attract and retain high-quality staff, contributes to lower staff turnover and increases employee motivation;
- Risks to operational continuity resulting from conflict inside the company itself or with the local community can be reduced;
- It appeals to institutional investors, including pension funds, who are increasingly taking ethical factors into account in their investment decisions;
- Potential government and business partners are keen to partner with companies that are concerned with avoiding human rights risks.

1.3 What will I learn from this Guide?

This Guide will help companies answer the following four questions:

1. Why are human rights relevant to my company?
2. What are my company's responsibilities?
3. What capabilities are of concern?
4. How can my company assess and address human rights risks?

This Guide is focused on identifying and assessing risk as set out in the UN Guiding Principles on Business and Human Rights,[3] unanimously agreed by governments at the UN Human Rights Council in 2011. The Guiding Principles set out a series of steps for businesses to take to ensure that they respect human rights in practice and for governments to ensure that they protect people against human rights abuses involving businesses. They also set out recommendations for both governments and businesses on providing remedy for human rights harms.

The UK Government supports the approach of the UN Guiding Principles and was the first government to publish a national action plan. This lays out the government's expectation of UK companies and the steps it will take to ensure they respect human rights wherever they operate.

This Guide has been designed to be useful to companies of all sizes, with varying types of ownership and structure. Wherever possible, attention is given to approaches that may be more appropriate for smaller companies in the sector.

2 HMG, Good Business Implementing the UN Guiding Principles on Business and Human Rights https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/236901/BHR_Action_Plan_-_final_online_version_1_.pdf
3 http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

1.4 How does this Guide fit with legal requirements on my business?

This Guide is not legally binding. It aims to provide advice to help your company address the risks posed by exporting cyber capabilities that are not subject to sanctions or export control, but may have negative impacts on human rights.

Undertaking human rights due diligence should help your company to reduce the risk of legal claims for alleged human rights abuses by helping you to demonstrate that you took reasonable steps to avoid causing or contributing to the harm. However, companies should not assume that due diligence alone will fully absolve them from legal liability or reputational damage. This guide is also not a substitute for expert legal advice.

Companies must abide by the national laws of the states in which they operate. Some of these laws will mandate companies to act in a way that protects human rights. The UN Guiding Principles on Business and Human Rights are not legally binding. However, they are increasingly being referred to in contracts, legislation and other international standards that make them binding in some circumstances.

Some export destinations and capabilities are subject to legal constraints through trade sanctions and embargoes or the UK's licensing regime (for further information please see chapter three). This guidance is designed to help firms make decisions about exports that are not subject to these legal frameworks.

Further Resources on the UN Guiding Principles on Business and Human Rights:

UN Guiding Principles on Business and Human Rights
http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

UN Office of the High Commissioner for Human Rights (OHCHR) The Corporate Responsibility To Respect Human Rights: An Interpretive Guide
http://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf

European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights
http://www.ihrb.org/publications/reports/human-rights-guides.html

CHAPTER 2:

WHY ARE HUMAN RIGHTS RELEVANT TO MY COMPANY?

2.1 Why should my company be concerned and what are our responsibilities?

Cyber security capabilities have many positive impacts on societies but there are also occasions where the same technologies are used by customers to infringe human rights.

Your company has a responsibility to respect human rights. This means it should avoid infringing on the human rights of others and should address negative human rights impacts that it causes or contributes to. It should also seek to identify, prevent and mitigate negative human rights impacts directly linked to its operations, products or services by its business relationships, for example its resellers, distributors and joint venture partners.

The responsibility to respect human rights applies to all companies, regardless of their size, ownership or structure. However, how a company meets this responsibility is likely to vary depending on these factors. For example, small and medium-sized enterprises are likely to have more informal processes and less capacity to address human rights issues. Therefore they may require more advice and support in implementing this guidance. techUK recognises this and will support smaller businesses by providing support through its Cyber Connect programme to identify best practice and lessons learnt in implementing human rights responsibilities.

There is now a greater expectation on companies to answer to the company board, shareholders and investors, consumers and the media as to how they are assessing and monitoring risks to human rights. Companies that have been implicated in human rights abuses have been subject to government investigations, fines, loss of support from home governments and loss of good reputation.

My Business and Human Rights:
A Guide to Human Rights for SMEs
http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/human-rights-sme-guide-final_en.pdf

2.2. Which human rights are relevant?

Your company has a responsibility to respect all the rights set out in the International Bill of Rights[4] and the International Labour Organisation Declaration on the Fundamental Principles and Rights at Work.[5]

Table 1 overleaf sets out a brief definition of some of the rights most likely to be relevant to the export of cyber capabilities.

4 The International Bill of Human Rights is comprised of the Universal Declaration of Human Rights (http://www.un.org/en/documents/udhr/), the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights (http://www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx).
5 http://www.ilo.org/declaration/lang--en/index.htm

Table 1: Human rights potentially affected by the export of cyber security capabilities

These rights may be restricted by a government for legitimate reasons, including protecting the rights of other people or in the interests of national security. However, any restriction on these rights must be prescribed by law, legitimate, necessary and proportionate.

Human right	What this means
Right to privacy	No one should be subject to arbitrary or unlawful interference with their privacy, family, home or correspondence, or to unlawful attacks on their honour or reputation. Everyone has the right to be protected by the law from such attacks.
Freedom of expression	Everyone has the right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds freely. The right to free expression protects opinions that may shock, offend, or disturb. Freedom of the press is especially important.
Freedom of association and assembly	Everyone has the right to freedom of association with others, and the right to peaceful assembly. This could involve forming a trade union or organising and taking part in a peaceful protest.

These rights must be protected from arbitrary or unlawful deprivation or interference by the State. The State may act only according to clear rules and processes set down in the law.

Human right	What this means
Right to life	Everyone has the right to life. The state has a positive duty to protect the right to life of all people within its jurisdiction. International human rights law makes clear that 'no one shall be arbitrarily deprived of his (her) life'. Limitations to the right to life are spelled out in greater detail in international instruments, for example imposing the death penalty in exceptional cases in accordance with the law of that country, killings in armed conflict situations, and the use of reasonable force by law enforcement agents in self-defence or defence of others.
Freedom from arbitrary arrest and detention and right to a fair trial	Everyone has the right to liberty and security of the person. No one shall be subject to arbitrary arrest and detention. Any arrest or detention must be carried out according to the law and the person has the right to a fair trial.

These rights can never be limited or restricted in any circumstances.

Human right	What this means
Freedom from torture, inhuman and degrading treatment	No one shall be subject to torture or to cruel, inhuman or degrading treatment or punishment.

Equality and non-discrimination should always be considered.
Everyone has the right to equal enjoyment of their human rights. States must not discriminate against people on any grounds, including, but not only: race, sex, sexual orientation, age, disability.

Gamma International – sale of Finfisher to the Bahraini Government

Background

During the Egyptian Revolution of 2011, activists stormed the abandoned headquarters of the State Security Investigations service (SSI). Among the items seized by activists were documents relating to the government's intention to buy a German software package called Finfisher, which was being sold by the UK-based company, Gamma International. Civil society groups began to investigate the capabilities of the portfolio of products that make up the Finfisher suite, and where else it had been sold. One product in particular, FinSpy, is intrusion software that is capable of monitoring Skype calls, emails and collecting passwords. Finfisher has since been found to have infected the computers of pro-democracy activists and human rights lawyers in Bahrain and Ethiopia, and has been found in 34 other countries.

Consequences for the company

Following extensive media attention in the UK and US,[6] Privacy International, a UK-based NGO, submitted a complaint against Gamma International to the Organisation for Economic Co-operation and Development (OECD) UK National Contact Point for a violation of the OECD guidelines. This complaint concerned the export of surveillance equipment to the Bahraini authorities who allegedly used it to monitor pro-democracy activists, some of whom were detained and tortured. It has been accepted and is currently being investigated.[7] Privacy International also submitted a complaint to HM Revenue and Customs (HMRC) to investigate Gamma's potential breach of UK export laws. The government found that due to its encryption capabilities, Finfisher should be subject to export controls.[8] Privacy International then filed a complaint to the National Crime Agency alleging that Finfisher was used to gain remote access to electronic devices owned by Bahraini activists living in the UK. It argued that by assisting the Bahraini government, Gamma is liable as an accessory to unlawful interception under the Regulation of Investigatory Powers Act (2000).[9]

6 http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher
http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html
7 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/208112/bis-13-947-complaint-from-privacy-international-and-others-against-gamma-international-uk-ltd.pdf
8 https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma
9 https://www.privacyinternational.org/news/press-releases/privacy-international-files-criminal-complaint-on-behalf-of-bahraini-activists

Table 2: Mapping Human Rights Risks in Technology Exports

Table 2 sets out a non-exhaustive list of some of the negative impacts that may arise from uses not intended by the seller. These are based on the capabilities specified in the UK Cyber Export Strategy (as shown in the introduction to this guidance) and illustrated with real-life examples.[10]

Capability	Intended usage	Potential negative human rights impact	Examples
Surveillance and Reconnaissance E.g. Deep Packet Inspection • Inspecting content • Modify content • Part of keyword filtering E.g. Malware • Spyware • Keyloggers • Trojan horses • Password sniffing E.g. Lawful Interception	*To observe, capture and explore behaviours and identities of people and platforms on computer networks* Technology developed to take samples of network traffic and inspect inside the packets (as opposed to shallow packet inspection which just analyses packet headers to determine the content). This assists identification of traffic content in order to detect spam or malware. Software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Often intentionally hidden by its creator but examples of overt malware exist. Companies supplying telecommunications infrastructure are often required by law to provide the technical means for communications to be intercepted for the purposes of supporting law enforcement.	All products potentially impact on the right to privacy, if not used lawfully, legitimately and proportionately. Depending on how the state authorities use the data they acquire these products may also impact on: • Freedom of expression. • Freedom of association and assembly. • Right not to be discriminated against. • Right not to be arbitrarily arrested or detained. • Right to a fair trial. • Freedom from torture, inhuman and degrading treatment. • Right to life.	A company provided the former Libyan government with surveillance technology that allowed it to intercept communications and process and analyse the data. The company also provided support and expertise in using this technology. This technology was used by the government to monitor opposition activists who were subsequently arrested, detained and tortured. It was also used to reinforce repression against the wider population.[11] A company provided intrusion software capable of monitoring Skype calls, emails and collecting passwords that has been found to have infected the computers of activists in Bahrain. A complaint has been submitted to the UK OECD National Contact Point to review.[12] A criminal complaint has also been submitted to the National Cyber Crime Unit regarding intrusion software sold to the government of Bahrain, which has allegedly been used to access the computers of Bahraini activists living in the UK.[13]

10 UKTI (2013) Cyber Security: The UK's Approach to Exports, p7 http://www.gchq.gov.uk/press_and_media/news_and_features/Documents/Cyber_Security-the_UKs_approach_to_exports.pdf
11 Amesys and Libya, see http://www.fidh.org/en/north-africa-middle-east/libya/Opening-of-a-judicial-inquiry
12 https://www.privacyinternational.org/blog/oecd-complaint-against-gamma-international-accepted-for-further-investigation
13 https://www.privacyinternational.org/news/blog/bahraini-government-with-help-from-finfisher-tracks-activists-living-in-uk

Capability	Intended usage	Potential negative human rights impact	Examples
Analytics and Big Data	*To acquire, store, retrieve, analyse and visualise very large and complex databases.* Allows analysis of data from a variety of sources, including closed sources, to reveal patterns, correlations and other useful information. It supplements conventional business intelligence mechanisms and enables organisations to improve their services. In the commercial sector these techniques are used to measure consumer trending and for market analysis (e.g. Tesco Clubcard).	As Surveillance (opposite).	In principle the correlation of different data sets can (re)identify an individual and provide information about them that is even more private than the data they consented to share, such as their religion, ethnicity or sexual orientation. This can be achieved by combining data from closed and open sources. The Iranian government used social media and a crowdsourcing website to identify protestors and dissidents. Pictures of individuals were posted on the site and users offered rewards to identify them.[14]
Social Media Analysis	To capture and analyse social network activity, to establish digital profiles, understand influence, monitor trends and observe sentiment. Increasingly, the private sector analyses social trends and public opinion by analysing open-source social media systems such as Twitter, LinkedIn and Facebook, where data is public, or within a corporation such as Google or Yahoo via web searches or email to support advertising capabilities.		*In principle, social media analysis could be used to violate privacy, for example by configuring the analysis to search for people of a particular ethnic group or government critics.*
Forensics	*To extract identities, behaviours and data from secured data and devices, often to evidential standards.* Digital forensics technologies allow the retrieval and investigation of data on networks, computers and mobile devices to provide evidence of a crime, determine intent, attribute evidence to suspects, identify/evaluate sources, and confirm/ authenticate statements, documents and alibis. It includes the technology and techniques required to seize, forensically image, analyse and report on data.	As Surveillance (opposite).	In principle such technology could be used to recover personal data from members of society who are not under legitimate criminal investigation.

14 Iran, http://online.wsj.com/news/articles/SB125978649644673331

Capability	Intended usage	Potential negative human rights impact	Examples
Information Operations	To protect, defend and mitigate against attacks utilising surveillance and management systems. This includes techniques employed to detect hostile or malicious activity on networks, which may be used to determine an appropriate response. The response may include the network manager or automated systems making and implementing decisions on security policy or applying configuration changes to remote network components. These systems could identify particular traffic types or malware and automatically block, divert or delete traffic.	• Right to privacy. • Freedom of expression, including the right to seek, receive and impart information. • Freedom of association.	In principle this technology could be abused in a similar way to surveillance tools, providing access to private data and enabling end users to make decisions which could breach human rights.
Security Management E.g. CERT-UK incident handling team E.g. Expertise in the development of effective security policies E.g. Training and delivery of Security Architects Blue/red teams E.g. Blocking/ filtering technology • IP address filter • URL filter • Web proxy • Content filtering • Firewalls	To integrate effective and agile security management across an organisation. Responsible for acting as hub and co-ordination point to respond to cyber security events. Good security policies are the first line of defence for any company or government. They set out how a network should be defended and how to respond to incidents. Good security architects are highly valuable and enable an organisation to set up and secure a network. Blue/Red teaming is an ideal way to independently (but safely) test system security by attacking it and reporting (similar to pen testing). Used to prevent access to illegal material (e.g. child abuse images), allow age-appropriate restrictions, restrict inappropriate use (e.g. in schools/libraries) and block malware deployment and/or command and control systems.	• Freedom of expression, including right to seek, receive and impart information. • Freedom of association.	In 2009 a provider of internet filtering software was informed that ISPs in Yemen were using its URL filtering software to block internet content banned by the Yemeni government, such as political opposition and independent news sites. The company has a clear anti-censorship policy which states that it does not knowingly sell filtering technology to governments or ISPs that are engaged in any sort of government-imposed censorship. When it discovered that its product was being used in this way it took action to identify the specific product subscriptions that were being used by Yemeni ISPS and to block updated database downloads to these subscriptions.[15]

15 https://community.websense.com/blogs/websense-features/archive/2009/08/17/websense-issues-statement-on-use-of-its-url-filtering-technology-by-isps-in-yemen.aspx

Capability	Intended usage	Potential negative human rights impact	Examples
Identity and Authentication E.g. ID tokens Swipe cards Biometrics (inc passports)	To capture, store and manage identity information, providing authentication for access and privileges. An organisation uses ID management to verify the credentials of employees or contractors and control physical and ICT accesses. Public bodies require this technology for passports and ID cards. Technology will include ID capture technology such as biometric readers or token readers and backend infrastructure.	Potentially as Surveillance (page 14).	ID management systems typically contain personally identifiable information, potentially including biometric information. In principle these could be used to access personal biometric data such as fingerprints or eye-iris scans and arbitrarily monitor people's movements.
Transaction Protection E.g. Encryption	To provide end-to-end security for each information transaction across variable trust environments. Cryptographic products enable security and privacy for transactions.	Negligible risk.	Not applicable
Trusted Platforms E.g. TPMs, Trusted Boot Secure I/O Secure Partitions and sandboxing	To ensure integrity of hardware systems/ services. Technology developed with the purpose of enabling confidence in the platforms through secure configuration, measurements and testing against known and expected states (attestation). Also designed to ensure IT environment has partitions of known security for processing securely or sandboxing untrusted functions such as internet browsing.	Negligible risk.	Not applicable

CHAPTER 3:

HOW CAN MY COMPANY ASSESS AND ADDRESS HUMAN RIGHTS RISKS?

3.1. What are my company's responsibilities?

The UN Guiding Principles on Business and Human Rights say that in order to know and be able to demonstrate that your company is respecting human rights in practice it should:

- Develop a human rights policy.
- Assess its actual and potential human rights impacts.
- Integrate the findings and act to prevent or mitigate negative impacts.
- Track how effectively risks are addressed.
- Communicate how risks are addressed.
- Work to remedy negative impacts it has caused or contributed to.

This guide is focused on assessing and addressing human rights risks, covered by the second two points. This is referred to as 'human rights due diligence'.

3.2. Developing a human rights policy

A human rights policy commitment publicly sets out that the company recognises its corporate responsibility to respect human rights. It should recognise that this involves respecting all internationally recognised human rights, but may highlight the rights especially relevant to its field of work. Its development should be informed by relevant internal and if appropriate external expertise.

The policy commitment provides the basis by which a company can develop human rights due diligence processes and communicate its expectations about behaviour and actions both internally and externally.

The policy should be approved by senior management and be publicly available.

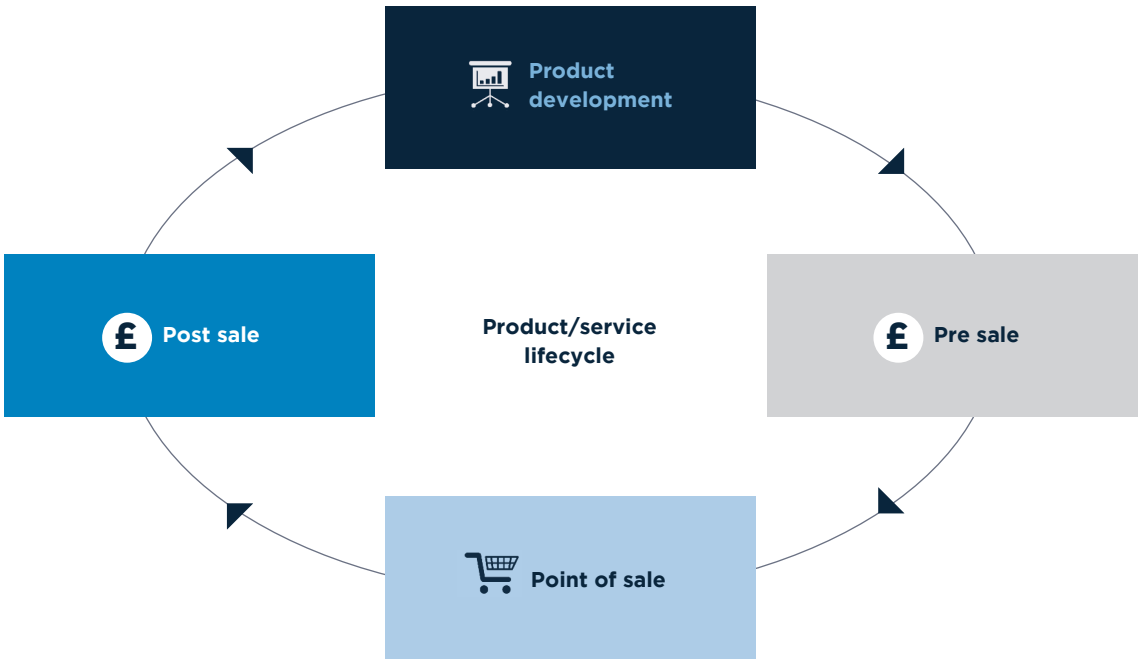
3.3. Human rights due diligence – assessing and addressing human rights risks

Human rights due diligence requires companies to take into account the whole lifecycle of its products and services – 'the product life cycle'. It should start at the earliest stages of capability design and continue through pre-contract assessment, the sale itself and post-sale review. It is about ongoing processes, not one-off events such as an impact assessment at the launch of a new technology, or an annual report. Risks change, particularly if new, unintended uses of the technology become known, so the risk assessment processes need to keep up to speed with changes.[16]

This section explores the assessment procedures and mitigation measures that companies can take at each stage of the cycle. Its core focus is on assessing human rights risks at the pre-sale and point-of-sale stages.

16 See chapter on 'Understanding Human Rights Due Diligence' in the European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (p16)

Figure 2: The product/service lifecycle



Product development

Engaging in human rights due diligence at the earliest stages of research, development and design can help companies identify and limit risks associated with exporting cyber security products and any associated services. If risks are identified at this stage, features could be designed to limit the risk of misuse.

It is crucial to involve engineers and developers in these conversations as they bring the technical expertise needed to assess the capabilities of a company's products, services and technologies. They are also best placed to advise on how potential adverse human rights impacts may be prevented or mitigated through appropriate design modification.

Further resources for assessing risks at the product development stage

Consider consulting with confidential advisory services such as the SURVEILLE Advisory Service. The service is free and includes advice on specific questions or issues to help with research project proposals, and feedback on work in progress. http://surveilleadvisoryservice.eu

Pre-sale scrutiny

When deciding whether to make a sale, a company needs to:

- Filter the deal – to identify any export controls or sanctions and to assess the level of risk involved in export.
- Conduct a further risk assessment if necessary.
- Identify potential mitigations where particular risks are identified.
- Have a final decision point at the end of the process where representatives with appropriate responsibility decide whether or not to proceed.

Filtering the deal

Assessing the proposed deal using a filter such as the example overleaf enables a company to establish whether the deal is legally permissible; if it is required to obtain legal documents such as an exports licence; if it is expected to undertake a full risk assessment process or if the deal can go ahead without one.

Figure 3: Example filter companies can apply to a deal

Countries subject to trade sanctions and embargoes

Some countries are subject to complete trade sanctions for dual use technologies under UK law. Other markets are subject to partial restrictions, which may affect the export of cyber security products. Both these categories are subject to change and firms are required to keep up to date with developments. Companies can find an up-to-date list of countries for which there are export bans or restrictions on the Government's website: https://www.gov.uk/current-arms-embargoes-and-other-restrictions.

Capabilities that require an export licence

Firms are required to keep up to date with UK Export Control laws and regulations, particularly the UK Strategic Export Control List, which forms the basis of determining whether any product, software or technology is controlled and therefore requires an export licence. Firms should also keep up to date with revisions to the Wassenaar Arrangement and European Dual Use Regulations, as well as other multilateral control systems. Resources to help your company do this can be found in the box opposite.

The Wassenaar Arrangement is a multilateral export control regime under which the export of dual-use technologies and conventional arms is regulated. It aims to promote regional and international stability by agreeing responsible and transparent export practices which member states incorporate into their national laws. The Wassenaar Arrangement mostly covers conventional arms but it also includes information security, electronics, computers and telecommunications products.[17] It has recently been updated to include two cyber security capabilities:

1. Complex surveillance tools which enable unauthorised access to computer systems.

2. Tools for extracting message content and metadata from a carrier class IP network and using that data to map the relational networks of individuals or groups.

Further resources on up-to-date export controls information

HM Government Department for Business, Innovation and Skills. Export Control Organisation
www.gov.uk/government/organisations/export-control-organisation

HM Government Notices to exporters:
http://blogs.bis.gov.uk/exportcontrol/

HM Government Overseas Security and Justice Assessment Process
www.gov.uk/government/publications/overseas-security-and-justice-assistance-osja-guidance

Wassenaar Arrangement:
www.wassenaar.org/index.html

Countries not of concern

Some countries are considered to be safe to export cyber security capabilities for end use in that country, without further human rights due diligence, provided the capability itself is not covered by export controls. These countries are: EU nations, Australia, Canada, Japan, New Zealand, Norway, Switzerland and the United States. For sales to customers and/or end users in any other country firms should carry out a proper due diligence process informed by the process set out below.

Human rights due diligence

Companies are expected to carry out their own human rights due diligence to establish the risk connected to the potential sale.

Risk assessment process

Companies need to follow a risk assessment process that covers the 5 Ps:

- Products and services it is planning to export.
- Places it wants to export to and the people that could be impacted.
- Purchasers and their intended use of the products.
- Partners, the business partners and sales agents the company would be working with in-country.

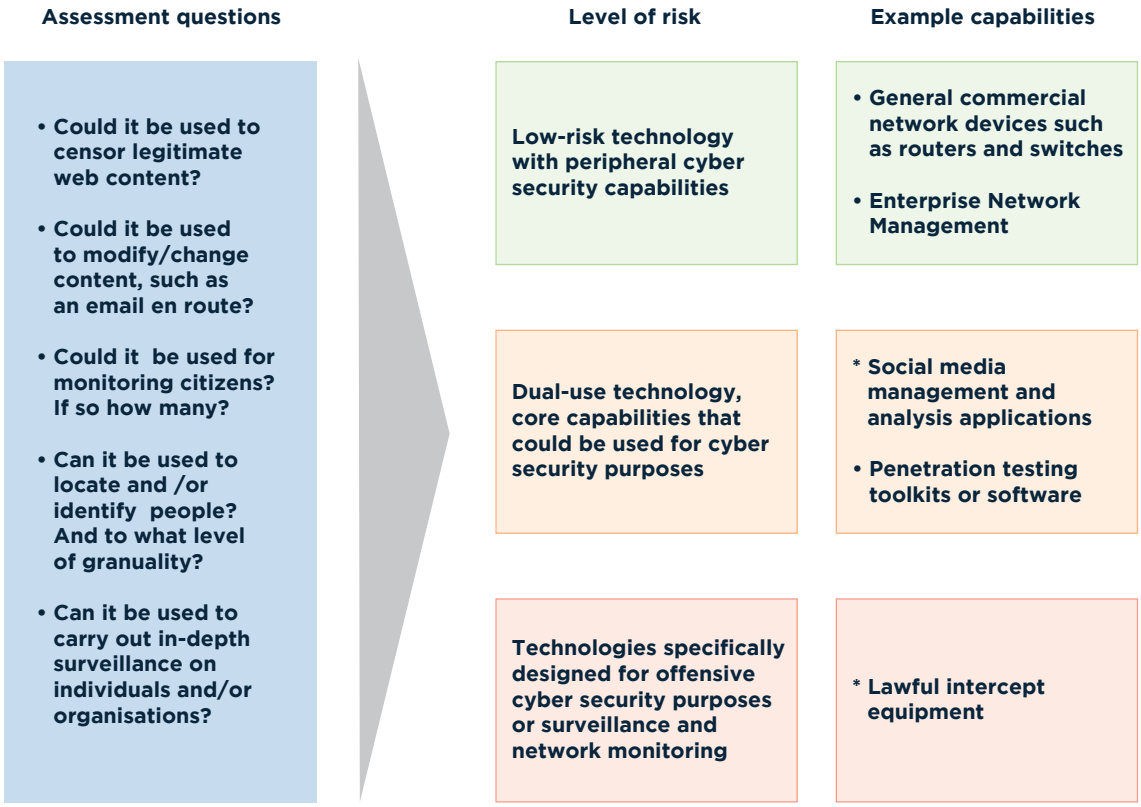
Products and services

It is important that companies understand the potential uses and misuses of their technology.

Companies need to map the capabilities of the products and services that they wish to export and use the result to answer questions such as the ones overleaf. This should not be seen as an exhaustive list. Companies should get product designers and engineers involved in the process to make sure it is thorough.

17 http://www.wassenaar.org/controllists/index.html

Figure 4: Assessing the risk of products and services



This process should help companies ascertain the risk related to the capability they are seeking to export. Once this has been established it is important for companies to make enquiries about the country where their customer is located.

Further resources on assessing products and services

Have other companies experienced similar issues? Check the UN Global Compact Human Rights Dilemmas Forum http://human-rights.unglobalcompact.org and the Business and Human Rights Resource Centre http://www.business-humanrights.org

Citizen Lab reports: https://citizenlab.org/publications/

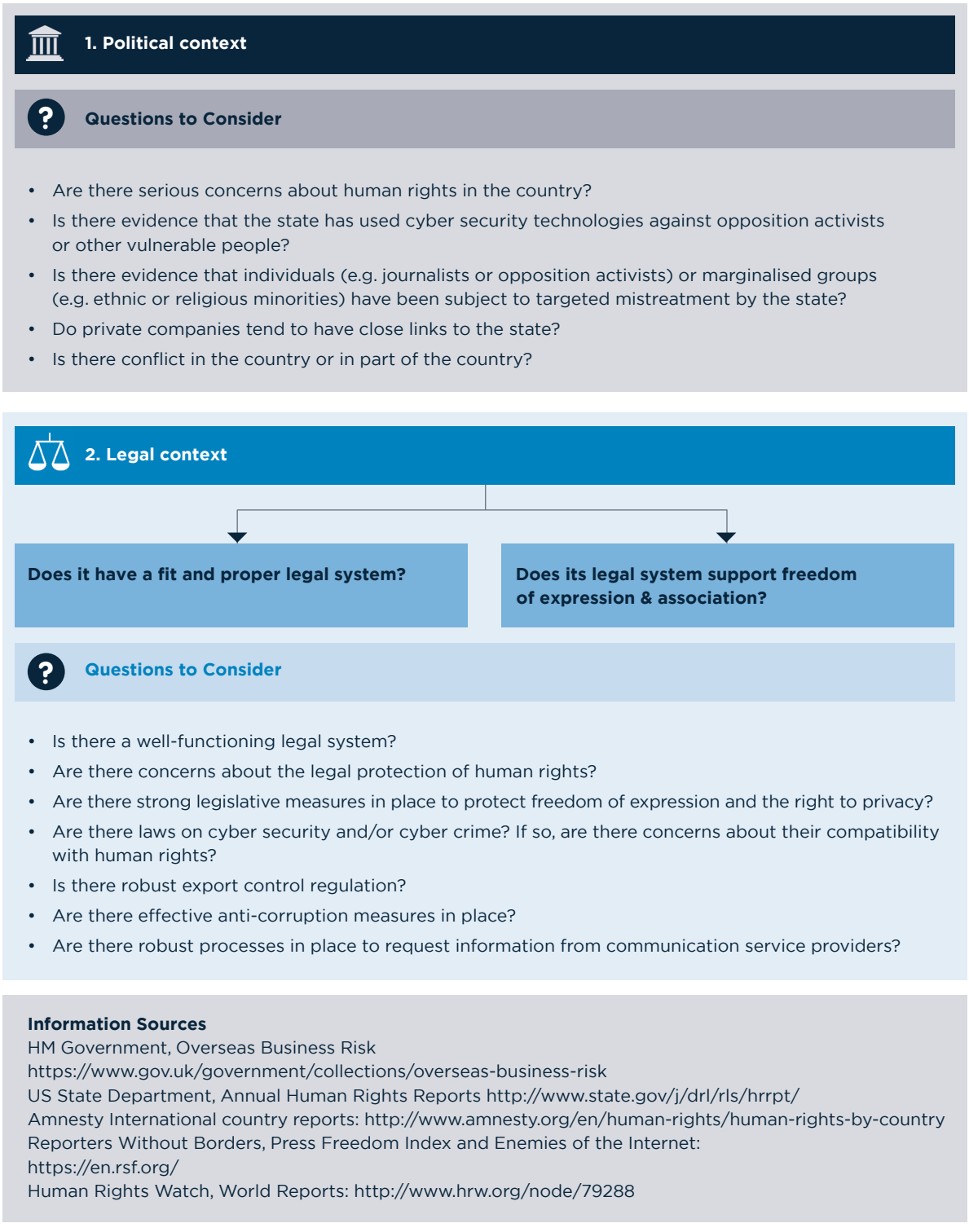
People and places – where are the countries of concern and who could be at risk?

Companies need to assess the political and security situation within the country they wish to export to, as well as the strength of its legal framework, namely whether it upholds international human rights standards and whether its application is consistent and transparent. This will help to reach a judgement about the level of risk that a capability may be misused and the strength of the checks and balances in place to prevent this.

In this assessment it is important to consider evidence of discrimination against individuals or groups, for example people who oppose the government, such as journalists, lawyers and human rights defenders and marginalised groups such as ethnic or religious minorities, LGBT and indigenous people. Capabilities may be sought by governments to monitor, track or take action against such groups.

Figure 5 gives examples of questions that could be used to assess the respect for and protection of human rights within different countries and the resources available to help companies answer such questions.

Figure 5: Identifying countries and end users of concern



Purchaser (or end user)

Whether the potential customer is a government or commercial entity, companies need to have a robust 'know your customer' screening process in place to establish the identity of the end user and their intended use of the product. Companies who already have such procedures need to make sure they are suitable for flagging potential signs that the buyer is trying to obscure the true customer or purpose of the purchase.

Figure 6: Know your customer checklist

Information to verify the final customer's identity and location

Assurance checklist	Warning signs to look out for
Has the prospective customer supplied you with the information you need to verify their identity?	Are you selling into a customs-free zone?
Have you checked the company's registration and VAT details?	Is the customer buying through a logistics agent?
Has the end user been cross-referenced against any internal denied customer list?	Is the customer reluctant to supply you with the credentials you are seeking from them?
Does the product destination match the company address?	Is the customer asking to pay large orders in cash which would usually require financing?
Have you verified the existence of the customer's premises either through in-country personnel or an online search?	Has the customer been linked to unauthorised dealings with embargoed countries or persons?
Have you checked to make sure the company has a functioning website?	Is the shipping route requested unusual?
	Has the customer requested an unusual degree of security for shipping the product?

Customer's stated requirements and intended use of product

Assurance checklist	Warning signs to look out for
Has your customer clearly defined their need for the product?	Has the customer been linked to the repression of human rights or to supplying services to organisations which have?
Is it clear what the product will be used for and who will use it?	Has the customer offered unusually favourable terms of purchase?
Do the product capabilities requested fit the customer's line of business and technical capability?	Has the customer refused installation, training or maintenance packages?
Have the end users and end use been designated in the contract?	Is the order out of kilter with the customer's business requirements?
Does the contract allow your company to withdraw services or cease support if contractual assurances are violated?	Has the customer requested unusual customisation of the product which doesn't fit with its stated end use?

Partners

The reputation of any business partners involved in the sale should also be investigated as their actions could adversely affect your company's reputation or operations. Taking steps to prevent and mitigate against negative human rights impacts linked to your company by your business relationships is also a key part of the corporate responsibility to respect human rights.

If your partner is a government or a state-owned company you should reflect on the questions asked in the 'Places' section. Governments in countries where there are significant human rights concerns are likely to pose higher risks.

Companies should apply similar 'know your customer' approaches to agreements with resellers and distributors, particularly where those business partners operate in or sell to customers in states that have a poor human rights record.

Figure 7: Resellers and distributors checklist

Assurance checklist for re-sellers and distributors

Are your company and products being accurately represented?

Does the reseller/distributor have a public policy commitment on respecting human rights? If so, is it broadly equivalent to your own?

If not are they willing to uphold your human rights policy?

Is the reseller providing the information your company needs in order to conduct a robust 'know your customer' approach? (See opposite.)

Warning signs to look out for

Does the reseller have close links to organisations / governments that are linked to human rights abuses?

Is the reseller on any relevant company or government 'blacklists'?

Is the reseller withholding information about the end user?

Is the reseller unwilling to sign and support end user statements?

Is the reseller/distributor linked to any credible allegations of involvement in human rights abuses?

Similarly, if a company plans to embark on a joint venture to make a sale it needs to take into the account the reputation of its business partner. Relevant factors in deciding to enter a joint venture can include:

Figure 8: Joint Venture Partners checklist

Assurance checklist for Joint Venture Partners

Does your potential partner have a public policy commitment to respect human rights? If so, is it broadly similar to your own?

If not, is it willing to adopt your human rights policy for the purposes of the JV?

Does the firm have its own human rights due diligence processes?

Is it willing to include provisions regarding human rights in the joint venture agreement?

Is the partner willing to let you take the lead and responsibility for ensuring respect for human rights in the JV?

Is the partner willing to collaborate in building capacity to respect human rights?

Further resources on 'Purchasers' and 'Partners'

Electronic Frontier Foundation (EFF), Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes https://www.eff.org/document/human-rights-and-technology-sales

At the sales stage

Mitigation

If the risk assessment has flagged up potential concerns, but the company wants to go ahead with the sale, it should consider placing conditions on the sale of its products or services or modifying the capability of its products to mitigate identified risks. Examples of potential technical and contractual mitigations are shown in figure 9 below.

Figure 9: Potential mitigation options

Technical mitigations	• Narrow the capability, e.g. Restrict the number of interceptions permitted simultaneously or switch off capability that's not needed. • Ensure that the technology has strong permission controls built into it for example by assigning encryption keys to legal authorities so that capabilities can only be used with legal permission • Keep any customisation requests, on-going service and upgrade requests and other arrangements.
Contractual mitigations	• Make sure the approved uses of the product or service is stated in the contract or as part of a separate "end user agreement". Companies could consider using an End User Undertaking form (part of the licensing process for controlled technology) and adapting it for human rights issues. • Representations and warranties from the customer that the product or services will only be used as intended, with a specification of the intended use, end-user and location of use. This may include a specific representation that the product or service will not be used to infringe on human rights. • Point the customer to the company's human rights policy, setting out the conditions under which they will do business. • Restrictions on re-sale or relocation without notice or approval by the company • A clause that permits the seller to make ad hoc inspections of it's buyers use of the product • A statement that if the product is misused, any warranties/licence will be void and no on-going maintenance will be provided. Companies could also undertake to inform UK Government (through UKTI) of the breach. • Any specific monitoring or reporting that must be done on the use of the product or service • At contract renewal time, take the opportunity to incorporate human rights safeguards into newly negotiated contracts. • In contracts with resellers and distributors, it will be important to include provisions for the reseller or distributor to conduct their own "know your customer" due diligence, and to provide for the voiding of any warranties if re-sale/distribution occurs without such due diligence having occurred. Companies may need to consider selling directly if such risks cannot be effectively managed through contractual language and monitoring. • All contracts should state that the sale is subject to UK laws and regulations.
Other mitigations	• Representation: Seek Government assistance with local contacts to obtain greater assurance about end-use.

Further resources available:

The Department for Business Innovation and Skills provides a template for End User Undertakings: www.gov.uk/government/publications/end-user-undertaking-euu-form

Wassenaar Arrangement End-User Assurances Commonly Used Consolidated Indicative List: http://www.wassenaar.org/publicdocuments/docs/End-user_assurances_as_updated_at_the_December_2005_PLM.pdf

Decision point

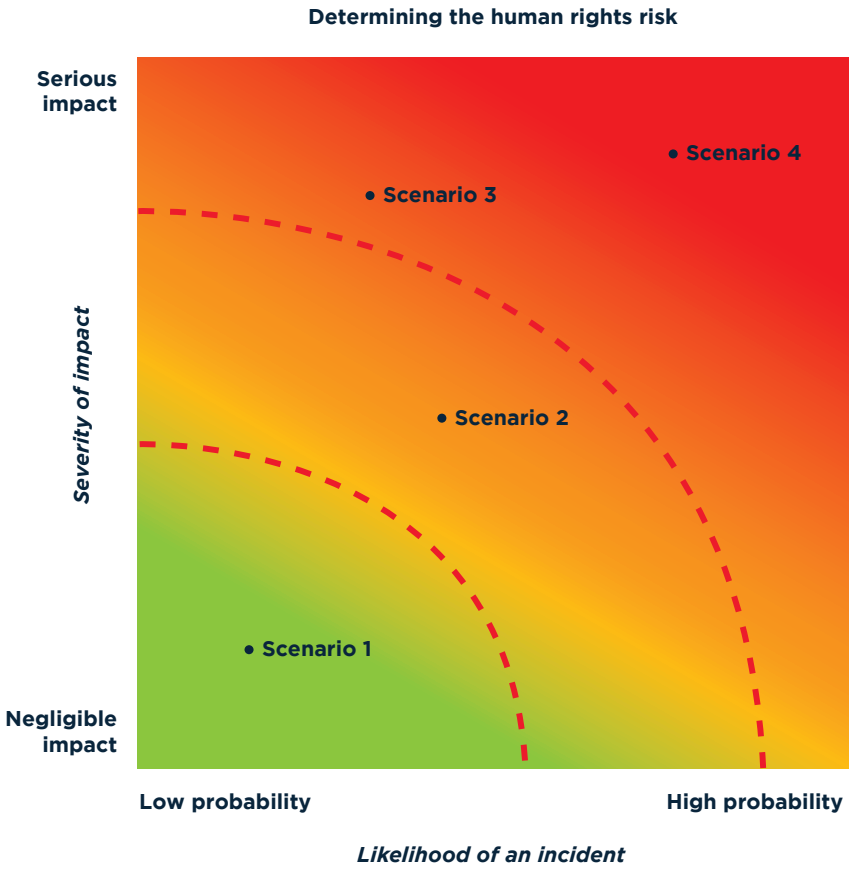
Many companies will already have pre-contract sign-off procedures / new business approval processes, which can be adapted and then used to weigh any human rights risks identified in the pre-sale stage against the opportunity expected to result from the sale. These need to include a formal decision point where a nominated individual takes responsibility for the company's action based on the information gathered. The decision process needs to be flexible to take into account both the probability of the risk occurring and the severity of the likely consequences. The severity of the potential negative human rights impact is a key consideration.

The decision maker should ensure that the risks identified in relation to products, places, people, purchasers and partners are all fully considered and reflected in the decision-making process. The following questions may help to assess the information gathered:

- Legality: Is the export of this capability legal?
- Probability: What is the probability of an identified risk actually occurring?
- Severity: What is the severity of the likely consequences?
- Moderation: How strong and realistic are the proposed mitigations?
- Morale: How do employees feel about the deal?
- Reputation: Can the company defend itself effectively if something does go wrong?

The huge variation of export destinations, purchasers and technologies makes it impractical for this guide to recommend specific responses. Instead it offers some illustrative examples of the type of decision process a company may wish to consider according to the level of risk it has identified with the potential sale.

Figure 10: Risk assessment matrix



Scenario 1 Country A: A company is considering the sale of a low-risk technology such as an Enterprise Network Management package to a government agency in an EU member state. The country has an advanced economy and highly developed civil and political rights. International human rights norms are codified in domestic law and enforced. Corruption levels are very low.

Decision process: The product poses a very low risk to human rights and the country and purchaser have been identified as being safe customers. In this case it would be appropriate for the sale director in charge of the contract to proceed with the export once they have carried out checks on the buyer.

Scenario 2 Country B: A company is assessing a potential export agreement with a small stable country with a prosperous economy driven mostly by the export of natural resources. The country is an absolute monarchy. Though politically stable, there are human rights concerns regarding the treatment of migrants and the breadth of the right to freedom of expression. A state-owned company has recognised the vulnerability of some of its key infrastructure to cyber attack and wishes to purchase firewall solutions. The country is not a member of the Wassenaar Arrangement but has its own stringent export laws.

Decision process: The product does not pose a serious risk to human rights, but it could be used to filter or block internet access. Given the lack of political freedom and freedom of expression in the country, the company should conduct a due diligence assessment in line with this guidance. Particular care should be given to assessing the buyer and to potential mitigations. This could include building approved end use clauses into the contract and a prohibition on reselling to any other organisation within the destination country. The sale should also be reviewed and signed off by a senior member of the company's compliance or risk management team.

Scenario 3 Country C: The energy and resources government department in a large notionally democratic country with substantial revenue from natural resources wishes to purchase social media monitoring software. Government agencies have been accused of perpetrating human rights abuses, with political corruption seen as endemic. There is, however, a large and active civil society and press.

Decision process: Having carried out its due diligence, the company will have identified serious concerns about the government's human rights record, although this would have to be weighed against the low potential for the capability to be used to carry out violations, especially by this particular purchaser. There may, however, be considerable reputational risks to the company from doing business with such a government. Given this, a company would be advised to seek authorisation from its Chief Risk or Compliance Officer or equivalent before deciding whether to go ahead with the deal. The company should build mitigations into the contract such as clauses around the approved end use of the product and a prohibition on reselling to any other institutions within the country in question.

Scenario 4 Country C: The police force in Country C has approached a supplier of digital forensics capabilities following, they say, a spate of cyber attacks against a number of corporations working in the country's extractive industry.

Decision process: A due diligence assessment carried out in line with this guidance would identify risks with the product, the place and the purchaser. This should raise serious concerns about the likelihood of harmful misuse and the legal and reputational consequences of going ahead with the sale. The company may well decide to refuse the sale in this scenario.

3.4 Post-sale stage – review

Risks may arise in the post-sales stage because: the situation in the destination country changes; there are personnel changes at government ministries which bring a different point of view about security; or the product is found to have been misused (such as filtering software being used to censor legitimate content). It is therefore important that companies remain alert to changes in markets where they have a footprint. Ongoing due diligence will help uncover any misuse of the product and enable a company to act quickly if a situation changes in-country. Any significant changes to political or legal conditions in the destination country, serious concerns about the behaviours of the customer or the use to which they are putting a product should trigger a reassessment of the contract using the processes set out in this guidance.

It will be easier for companies to react to changes if they have built opportunities in the contract to allow modifications to the products (where technically viable), services or contractual conditions to deal with new situations. This could be particularly effective when linked to ongoing support or warranty from the seller or where effective use of a product or service depends upon it receiving regular updates. Software and hardware licence management and renewal remain potential opportunities to assess post-sale usage and to mitigate risk.

Having a mechanism to feed back experiences of sales into the pre-sale risk assessment process can be used to refine and improve decision making.

Resources to help keep track of changes in destination countries:

Global Voices. A respected online resource that curates, verifies and translates news stories from 167 countries into 30 languages. Search by region and country: www.globalvoicesonline.org

Amnesty International. Searchable by region and country: http://amnesty.org/en/news

Human Rights Watch online news page, searchable by region: www.hrw.org

Blue Coat – Syrian Government use of internet filtering technology

Background:
In 2011, researchers found evidence that technology sold by San Francisco-based company Blue Coat was being used in Syria. This technology allowed internet filtering, website blocking, and monitoring internet users. It is believed this technology was used to track opponents of the regime who were subsequently arrested.

Consequences for the company:
As sanctions against the export of US technology to Syria were in place, the State Department launched an investigation. Blue Coat claimed they had sold the 13 devices found to a distribution partner in Dubai, which they believed was destined to a department of the Iraqi government.[18] After a lengthy investigation into the company, Blue Coat was cleared of knowingly selling the products to Syria in 2013 and blame was placed on a distribution partner based in Dubai. The distribution partner Computerlinks FZCO was fined £2.8 million, the statutory maximum for the unlawful export and re-export to Syria.[19] In a press statement released on the day of the verdict, the Undersecretary for Industry and Security at the US Department of Commerce said: 'Today's settlement reflects the serious consequences that result when companies evade U.S. export controls. It is the result of an aggressive investigation and prosecution by the Bureau of Industry and Security into the unlawful diversion of U.S. technology to Syria... It is vital that we keep technology that can repress the Syrian people out of the hands of the Syrian government.'[20]

Action by the company:
Blue Coat said they have now taken action to prevent Syrian-based devices from receiving software updates.[21] Research by NGO Citizen Lab in 2012 suggested Blue Coat devices in Syria were no longer 'phoning home' to Blue Coat servers in the USA. Citizen Lab also found that 'many Blue Coat Systems domains were being blocked in Syria, perhaps to prevent existing devices from receiving updates'.[22]

3.5 A note on remedy

Despite a company's best efforts, the complexity of operations and business relationships involved in export deals can lead to negative impacts on human rights occurring as the result of a sale. Companies need to be prepared for these situations so they can respond quickly and effectively. Where a company has caused or contributed to an adverse human rights impact (as indicated in the case studies throughout this document), they are responsible for remedying the harm. Where they are only linked to the harm through a business relationship, a company is not expected to provide a remedy itself, though may be expected to play a role in doing so, in particular using leverage to prevent or mitigate the risk of the impacts continuing or recurring.

Remedy can take a variety of different forms, including apologies, restitution, rehabilitation, financial and non-financial compensation and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition. A company should at least be able to prevent repetition of harm but it may well be expected and appropriate to do more, depending on the circumstances.

For more information on building a systematic approach to remediation, see the European Commission ICT Section Guide on Implementing the UN Guiding Principles on Business and Human Rights, Part VI.

18 Citizen Lab (2013) Mapping Global Censorship and Surveillance Tools https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/
19 http://online.wsj.com/news/articles/SB10001424052970203687504577001911398596328
20 http://www.techweekeurope.co.uk/news/blue-coat-partner-fined-surveillance-syria-114548
http://www.bis.doc.gov/index.php/2011-09-12-20-18-59/2011-09-13-16-43-06/102-about-bis/newsroom/press-releases/press-releases-2013
21 http://online.wsj.com/news/articles/SB10001424127887323336104578503292583322474
22 Citizen Lab (2013) Mapping Global Censorship and Surveillance Tools https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

CHAPTER 4:

NATIONAL SECURITY RISKS

In addition to the human rights risks covered in chapter three, there are certain cyber security products, services or capabilities that could pose a threat to the UK's national security, including its defence and security interests, critical national infrastructure and prosperity. The export of this technology could increase the risk of a direct attack against the UK's interests or increase the UK's vulnerability by exposing how it might defend such an attack.

Whilst the guidance in chapters one to three is based on a clear, internationally agreed framework for identifying and addressing human rights risks (the UNGPs), there is currently no similar framework to help companies identify and address potential national security risks. This is a new area in terms of business risk management. This chapter aims to help companies start thinking about the potential national security risks of their products and services by setting out some questions to ask and signposting where to go for further information.

The risks linked to products of concern are usually managed through the export licensing process, but this system is inadequate for cyber due to the novel dual/multi-use nature of the products and the potential for re-engineering. Some new products have been added to the control lists, but a significant number are not covered by the system. HM Government is keen, therefore, for companies to consider the national security risks posed by cyber products/services as part of their due diligence process.

4.1 Why should my company be concerned?

If the UK's national security interests are compromised by a successful attack there may be profound knock-on effects, not only to the UK but also to the company responsible for exporting the technology. The consequences might include negative impacts on the company's profitability, security and reputation.

The abuse of certain cyber security products and services could also have a negative impact on the security and integrity of other countries, including allies. This might not directly impact on a company, but it could still suffer reputational damage if it is found to be involved in supplying the capability to a party responsible for hostile cyber activity.

4.2 What are the risks?

Companies should adopt a risk assessment process that covers a range of factors. The following categories, which are examples, are similar to those used in chapter three, although the questions are different.

4.3 Products and services

Is the product/service (or components thereof) subject to export controls? If in doubt: check.

Could it have any of the following potential end uses?	Consider the potential use of the capability:	What are the potential impacts?
Espionage: Capabilities designed to retrieve another country's or company's protected information without sanction.	• Could the capability be used against the UK and/or its allies? • How might the intelligence gained be exploited?	• **UK national security:** - Defence and security. - Critical national infrastructure. - Economic well-being. And: • Prolonging or provoking **conflict** and internal or regional **instability**. • Risk of **diversion** to another end user and/or support for **terrorism** or **crime**. • Undermining **economies,** supporting **corruption** or seriously hampering the **sustainable development** of the recipient country.
Disruption: Capabilities designed to disrupt, deny or denigrate the functioning of, or confidence in, an online or real-world service.	• Could the capability be used against the UK and/or its allies? • How might the user exploit the capability to affect the delivery of services and/or information with what impact and on whom?	
Defence: Capabilities designed to defend networks and data from scrutiny.	• Could the capability defend activities or organisations that present a threat to the UK or wider international security? (E.g. illicit nuclear programmes, the communications of terrorist groups or regimes of concern)	

4.4 Places and purchasers

If a product/service clearly poses a risk then the company should consider the situation in the destination country.

- Is the destination country subject to sanctions or embargoes?
- Are there ongoing disputes or tensions between the destination country and the UK?
- Does the destination country have close links with countries which pose a concern?
- Does the destination country have the capability to re-engineer products?
- Is the purchaser known to the company and is the stated end use credible?
- To what extent does the destination country respect the rule of law and comply with international regulations?

There are many resources available to help companies make informed judgements about foreign countries, including news and Government travel advice websites.

Further resources for assessing country-related risks include:

- FCO Overseas Business Risk: www.gov.uk/government/collections/overseas-business-risk
  Note: HMG will not advise on whether a company should do business in a particular market.
- US State Department Country Reports: www.state.gov/countries/
  Additionally, some consultancies may offer tailored advice on country risks, sanctions and licensing issues

4.5 How can my company manage national security risks?

Companies can use the following methodology:

- Involve technical experts at an early stage;
- Identify any legal issues (e.g. export controls or sanctions);
- Conduct an assessment for products/services which do pose a risk;
- Consider potential mitigations;
- Assign responsibility for a final decision to the appropriate authority.

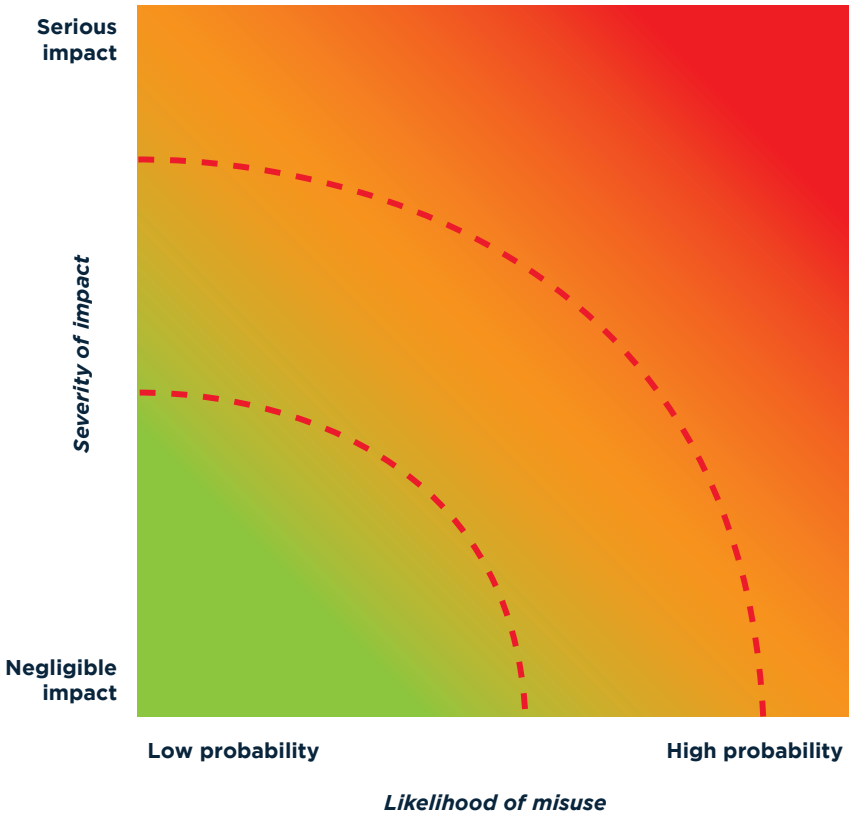
4.6 Making a decision

Having assessed the available information about a capability that clearly poses a potential national security risk, the company should come to a decision on whether or not to proceed with an export.

If the company is still unsure (especially for serious-impact/low-probability cases) then it should contact the International Cyber Policy Unit in the Foreign & Commonwealth Office.

Email:
cyberexportsandassistance@fco.gsi.gov.uk

Figure 11: Risk assessment matrix



Further resources

Key international human rights standards for companies:

The Universal Declaration on Human Rights
http://www.un.org/en/documents/udhr/

The International Covenant on Civil and Political Rights (ICCPR)
http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

The International Covenant on Economic, Social and Cultural Rights (ICESCR)
http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx

International Labour Organisation's Declaration on Fundamental Principles and Rights at Work
http://www.ilo.org/declaration/lang--en/index.htm

Practical guidance for companies:

European Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights
http://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf

UN Global Compact: How To Develop a Human Rights Policy: A Guide For Business
http://www.ohchr.org/Documents/Publications/DevelopHumanRightsPolicy_en.pdf

Examples of human rights policies:

BT: http://www.btplc.com/TheWayWeWork/Relationships/Humanrights/index.htm

Ericsson Code of Business Ethics:
http://www.ericsson.com/res/thecompany/docs/corporate-responsibility/cobe/ericsson-cobe-2014-en.pdf

Intel Human Rights Principles:
http://www.intel.co.uk/content/www/uk/en/policy/policy-human-rights.html

Microsoft Human Rights Statement 2013:
http://www.microsoft.com/en-gb/download/details.aspx?id=41958

TeliaSonera: http://www.teliasonera.com/en/sustainability/human-rights/

Other Sector Examples of Company Human Rights Policies:

http://www.business-humanrights.org/Documents/Policies

Assessing human rights impacts:

HM Government Department for Business, Innovation and Skills. Export Control Organisation:
www.gov.uk/government/organisations/export-control-organisation

UK Government Overseas Security and Justice Assessment Process:
www.gov.uk/government/publications/overseas-security-and-justice-assistance-osja-guidance

Wassenaar Arrangement: www.wassenaar.org/index.html

Assessing products and services:

Citizen Lab reports: https://citizenlab.org/publications/

Coalition Against Unlawful Surveillance Exports (CAUSE) http://www.globalcause.net/

New America Foundation / Open Technology Institute / Privacy International / Digitale GesellSchaft, Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/uncontrolled_surveillance_march_2014.pdf

Additional UN resources on identifying potentially vulnerable groups or individuals:

Convention on the Elimination of All Forms of Discrimination against Women
http://www.ohchr.org/EN/ProfessionalInterest/Pages/CEDAW.aspx

International Convention on the Elimination of All Forms of Racial Discrimination
http://www.ohchr.org/EN/ProfessionalInterest/Pages/CERD.aspx

Convention on the Rights of Persons with Disabilities
http://www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx

Declaration on Human Rights Defenders
http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx

Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities
http://www.un.org/documents/ga/res/47/a47r135.htm

Declaration on the Rights of Indigenous People
http://www.un.org/esa/socdev/unpfii/documents/DRIPS_en.pdf

International Convention for the Protection of All Persons from Enforced Disappearance
http://www.ohchr.org/EN/HRBodies/CED/Pages/ConventionCED.aspx

UNESCO: UN Plan of Action on the Safety of Journalists and the Issue of Impunity
http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/UN_plan_on_Safety_Journalists_EN.pdf

Identifying places:

The Danish Institute for Human Rights, Decision Map: Doing Business in High Risk Areas
http://www.humanrightsbusiness.org/files/Publications/doing_business_in_highrisk_human_rights_environments__180210.pdf

The Danish Institute for Human Rights, Human Rights and Business Country Guide:
http://hrbcountryguide.org/

Human Rights Watch, They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia
http://www.hrw.org/reports/2014/03/25/they-know-everything-we-do

The Institute for Human Rights and Business, From Red Flags to Green Flags
http://www.ihrb.org/pdf/from_red_to_green_flags/complete_report.pdf

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow.

More than 850 companies are members of techUK. Collectively they employ more than 500,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

techUK

10 St Bride Street, London EC4A 4AD
techUK.org | @techUK | #techUK