Unit 1 - The Understanding of Cyber Security and Online Threats

Overview

The candidate can understand the range and variety of threats, analyse and understand the way these threats are deployed and propagate and be able to evaluate some of their impacts. In the course of their investigations they will look at the types of threat and analyse their purpose and what or who they are designed to affect. They will try to understand the underlying mechanisms used by the attacking materials and people to better understand how to defend against them. They evaluate the threats in terms of their overall impact and disruption and produce a report on their findings to demonstrate a good understanding.

A work activity will typically be 'non-routine or unfamiliar' because the task or context is likely to require some preparation, clarification or research to separate the components and to identify what factors need to be considered. For example, time available, audience needs, accessibility of source, types of content, message and meaning, before an approach can be planned; and the techniques required will involve a number of steps and at times be non-routine or unfamiliar.

Example of context – carrying out a security audit for a local charity.

Assessor's guide to interpreting the criteria

General Information

RQF general description for Level 2 qualifications

- Achievement at RQF level 2 (EQF Level 3) reflects the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks and address straightforward problems. It includes taking responsibility for completing tasks and procedures and exercising autonomy and judgement subject to overall direction or guidance.
- Use understanding of facts, procedures and ideas to complete well-defined tasks and address straightforward problems. Interpret relevant information and ideas. Be aware of the types of information that are relevant to the area of study or work.
- Complete well-defined, generally routine tasks and address straightforward problems. Select and use relevant skills and procedures. Identify, gather and use relevant information to inform actions. Identify how effective actions have been.
- Take responsibility for completing tasks and procedures subject to direction or guidance as needed.

Requirements

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

- Standards must be confirmed by a trained Gold Level Assessor or higher.
- Assessors must at a minimum record assessment judgements as entries in the on-line mark book on the INGOTs.org certification site.
- The work in the unit is recommended in order for candidates to have covered enough depth and breadth in the topic to successfully carry out their controlled assessment and take the external exam.
- When the candidate has covered as much of ths material as necessary to complete the controlled assessment element, they may be introduced to the topic
- This unit should take an average level 2 learner 35 hours of work to complete.

Assessment Method

Understanding of these learning objectives will be demonstrated through answering questions related to key ideas and concepts in the terminal examination as well as practical application of their understanding through the controlled assessment.

Expansion of the assessment criteria

1. Understand the range and variety of cyber threats

1.1 I can explain the basic nature of a cyber threat

Learners should be able to explain a cyber threat using examples

Additional information and guidance
There is a great deal of debate about what cyber threats are and the range and extent of the threats. At the very simplest level it is something that is facilitated through computer networks, the networks carry traffic through “cyberspace”. So any threat delivered by computers to other computers is a cyber threat. The threats can also range in the extent of their damage. Some cyber threats are just a nuisance as they may disrupt a website or push pop up messages at you while browsing. Other threats are for more serious, such as the disruption of a country’s key infrastructure as happened to Iran in 2010. The more computers come online and carry out vital functions, the more attractive they are to criminals who want to use access to those computers or networks of computers to cause problems or extort money.

Learners should be able to write their own understanding of some of these threats and the impact they have in order to show they have a good feel for their nature. Various events and their explanation [1] can help with the overall understanding.

1.2 I can can list some of the more common threats

Learners should be able to list a number of basic threats

Additional information and guidance
Most of the threats to computers and systems are well documented and there is always some issue in the news related to cybercrime.

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

Learners should be able to make a list of a number of the most commonly occurring threats, such as:

- Fraud and financial crime
- Terrorist related
- Extortion
- Warfare
- Viruses/malware
- Denial of Service
- Spam, phishing etc
- Obscenity
- Harassment/trolling/bullying
- Trafficking

1.3 I can explain the main features of threats to individuals

Learners should be able to explain how some of the above threats affect their victims

Additional information and guidance
The type of threat used will determine how much damage it causes to individuals and the nature of the damage. In the case of cyberbullying that occurs at schools, it is generally focused on one or two people and the damage is psychological as the victims feel oppressed and frightened to interact with others. There are documented cases where this has lead to suicide. With crimes related to fraud or extortion the damage is both psychological and financial. Psychological because the people affected no longer feel safe online and feel violated. The financial costs will vary depending on the ability of the attacked person to pay. In addition the reputational damage a company may suffer has a direct impact on the earnings, share price and volume of customers as happened during the TalkTalk breach. Some threats to individuals cause them little or no direct harm at all. The use of botnets is an example here. The end users have little or no idea that their computer is part of a huge network of other computers that are being used to attack other networks. The end user might notice an increase in Internet traffic, but probably not enough to realise they are infected. In 2010 a Spanish team found 13 million computers being used as part of a botnet.

1.4 I can explain the main features of threats to companies

Learners should be able to explain some company based threats.

Additional information and guidance
As companies have significantly more resources and wealth, the nature and scale of the attacks is significant. To some extent, the cost to these companies is not born by one person, so the emotional and psychological damage may be less, though someone will always be held accountable for the damage.

There are daily examples of threats to companies in the news for learners to analyse and explain. An example of a recent UK one was the attack on the telephone and Internet company TalkTalk in 2016.

http://www.bbc.co.uk/news/uk-34611857 [2]

The attack of their system and the subsequent bad publicity caused their shares to drop 10%. This amounted to a loss of £60 million. Companies can not afford to lose their reputation in the public domain so will often pay money to cyber criminals just to make sure it never hits the news. This means they are more likely to suffer fraud and extortion attacks as a result.

Learners can give some examples of threats to companies and say why they are specifically bad for companies compared to individuals.

1.5 I can summarise the variety of threats for an audience

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

Learners should be able to demonstrate their understanding by presenting their findings

Additional information and guidance
To demonstrate their clear understanding of the types of threats and the problems they cause to individuals and companies or society, learners should produce a short presentation. This can take several forms: as a leaflet for people to read, perhaps as a leaflet in the library, a presentation using presentation software, a multimedia display, an advert or drama or a blog post to name a few. This process will help learners summarise the main points and show some clarity of understanding.

2.Analyse and detail the types of threat currently in operation

2.1 I can describe the motivations of people behind threats

Learners should be able to demonstrate they understand what motivates people to attack systems

Additional information and guidance
The type of target combined with the vector of the attack will likely be a guide to what the motivation is by the person or group the attack. Increasingly, there are coordinated attacks that are on an international scale. In early 2017 it was commented that the state of Russia may have been involved in trying to alter the outcome of the US Presidential elections. The motivation here is a complex one.

The outcome of Donald Trump winning the election was presumably seen as favourable to the Russian state operatives. In some cases, the motivation is greed of some sort. When criminals engage in malicious cyber activity into commercial retailers or other large organisations in order to blackmail them, they just want to get money. The threat to companies is so great that they will invariably pay large amounts in order to avoid disruption to their services or damage to their reputation. The gambling industry is a good example of this. If the criminals can hide their location, it makes it easier for them to break in without being traced back to their origin.

Learners need to describe in their own words what sort of motivations they have found in their research, or what their own interpretation of the motivations is. Much of the motivation will be emotion based: greed, despair, frustration, excitement, revenge, etc.

This can be defined but learning about the types of threat actors who carry out attacks as below:

Attacker	Level of Skill	Motivation	Example Victim	Potential Impact
Advanced Persistent Threat (APT) / Nation State Actor	Very High	Ideology	Military Secrets	Very High
Industrial Espionage	High	Profit / disruption	Competitors	High
Organised Cybercrime	High-Medium	Money	Banking or bank customers	High to Med
Hacktivist	Varies	Ideology	Causes not in line with their views i.e. large corporations	Med - High
Insider Threat	Med to Low (typically)	Revenge	Own Company	Very High
Script	Low	Curiosity /	Minecraft	Low

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

Attacker	Level of Skill	Motivation	Example Victim	Potential Impact
Kiddies		respect of peers	servers	

Some terms for learners to research are:

- The Activist
- The Getaway
- The Insider
- The Mule
- The Nation State Actor
- The Professional

2.2 I can analyse the main threats in terms of the mechanisms they use

Learners should be able to research and comment on some of the ways threats are carried out

Additional information and guidance
One of the easiest ways for cyber criminals to get into a company's system is through the general decency of human nature which they shamelessly exploit. This is known as social engineering. There are many cases where criminals will phone up various junior people in a company and pretend to be someone from the IT department and try to get access by tricking people out of their own login details. If people can get into an organisation physically, they can then pretend to be someone such as a computer maintenance technician and trick people out of their logins. Once they have these logins they can then begin to penetrate other aspects of the system.

Other mechanisms of attack will be:

- DDoS (Distributed Denial of Service
- CPM (Cross Platform malware)
- Phishing
- Spearphishing
- Waterhole attack
- XSS Cross site scripting
- SQL Injection attack

Learners can research and define these types of attack and keep a note of them in terms of what they might be able to do to stop or prevent them.

2.3 I can describe how the features of threats make them operate

Learners should be able to describe the threats they have researched

Additional information and guidance
Learners need to describe how the items in 2.2 function and show they understand some of the main ways they are used. Each one works in a different way and has different delivery mechanisms as well as outcomes. A DDoS attack, for example, will cause the system to go slow or stop and this will cause the customers some annoyance and disruption which will damage the company's reputation. There is a real danger companies that lose their reputation will soon go out of business, so the company will do anything to prevent this and will often pay ransoms to hackers to stop the DDoS attacks. If the DDoS attack is designed to stop a company altogether, then they will not care about payment or financial incentives and will just try to destroy a company.

Alternatively, a phishing attack relies on the poor training of internal personal and the gullibility of staff. The delivery is usually via an email that delivers a file with a payload that can infect a system

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

or by enticing a victim to click on a malicious link. It only works if someone clicks on the link to activate the code.

The level of phishing attacks is increasing significantly as the following graphic from Wikipedia shows.

Total number of unique phishing reports (campaigns) received, according to APWG[71]

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244	173063
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787	268126
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683	327814
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187	335965
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897	412392
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020	313517
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979	284445
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195	320081
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489	491399
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661	68270	66217	62765	704178
2015	49608	55795	115808	142099	149616	125757	142155	146439	106421	194499	105233	80548	1413978
2016	99384	229315	229265	121028	96490	98006	93160	66166	69925	89232	118928	69533	1380432

This only shows the ones reported, so it is likely even higher than this suggests.

2.4 I can describe how attacks on companies are designed to work

Learners should be able to describe in their own words what attacks are expected to achieve

Additional information and guidance
This criterion is related to others in this unit in that the activities of the company and perhaps the motivation of the attacker will determine the reason and design behind the attacks. Security aware companies may employ a professional to run a simulated attack on their systems. These hackers are known as white hats who work within the law and only with prior authorisation. Some hackers conduct attacks might to bring attention to the company's lack of good security. If they are not authorised to do so they are breaking the law however their motivation is not malicious. These are known as grey hat hackers. . At the other extreme the attack will be to extort money from a company. These are known as black hat hackers. The "hats" come from traditional cowboy movies where typically the sheriff has a white hat and the "baddie" has a black hat.

The way the attacks work will therefore vary and understanding the motivation is key. In most cases the attacks are designed to steal information or gain some level of control or deeper access to the network. If the attackers can get in with some nominal rights, these may then be escalated and different parts of the network a weaknesses exploit or security misconfiguration can be identified.

In describing the form of attack, learners should pick one as an example, perhaps from the press, and explain how it worked and some of the stages. Some of the detail may not be revealed for other security reasons, but they should be able to convey some sense of which type of attack could have achieved a given effect.

2.5 I can describe threats in terms of their hierarchy of damage

Learners should be able to describe some damage caused by different threats

Additional information and guidance
Some of the detail on this criterion may be addressed in other criteria above, but will need fleshing out somewhat. One of the aspects here is that damage may not necessarily be the most obvious

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

one, such as physical damage to a computing network.

Some of the real damage might occur to the well-being of the employees. As with a burglary that occurs on a home, it is the thought that someone came in to your house and looked around and took something. As with other criteria here, there is a scale of damage that can be described. Some companies that suffer the theft of customer data may lose so many customers that they have to close down, this is clearly significant for the company itself. Other companies may lose a percentage of their income, as was the case with TalkTalk who had a breach of customer data and were fined heavily by the Information Commissioner's Office (ICO). Some attacks may not have a clearly defined financial impact , such as the leak of information from the US government.

Learners can cite a number of examples from their own research to show the range and scale of different attacks with some of their own commentary on the damage, implied or otherwise. Learners may also be taught industry standard metrics used to asses the risk and impact of a vulnerability. The most frequently used of which is the Common Vulnerability and Scoring System CVSS.

https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator [3]

It is not anticipated that learners will develop an in depth understanding of the system however a basic understanding will allow them to quantify in numeric terms the risk associated with a vulnerability which for example may be used remotely, without authentication and requires little skill which would achieve total compromise of a system VS a vulnerability which is complex, requires skill and only gains limited access.

3.Evaluate the impact of threats on various individuals and organisations

3.1 I can evaluate the impact on the economy of cyber threats

Learners should be able to offer some basic evaluations of cyber threats

Additional information and guidance
How much money is lost from the economy because of cyber crime? Can we really know as many companies may not report the attacks because it will impact on their image and their image is everything. Is it possible to give a value to the threats? The UK government commissioned a report in May 2016 which showed some of the financial costs of security breaches.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/fil... [4]

The following infographic from this report shows some of the range of financial damage.

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

Using this information, we can see that there is an average cost of £36,500. If there are something like 1,000 large companies, though there will be considerably more, this means a loss of £36.5 million.

However, the Cabinet Office estimates the total amount to be £27 billion.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/fil... [5]

In April 2017, both Google and Facebook were subject to an attack of “CEO Fraud” and lost $100 million.

http://www.bbc.co.uk/news/technology-39744007 [6]

3.2 I can determine the level of threat to my home environment

Learners should be able to analyse and comment on their own security exposure.

Additional information and guidance
A quick look at any home router log file will show that your own system is under constant attack from individuals or more likely bots. Equally, you will no doubt have a full and constantly reloading spam folder. Most systems are useful for attackers to be used for DDoS attacks on other systems as there is probably little real commercial criminal value in gaining full control of home based system. The only real financial gain in this derives from attaching the device to a botnet which is subsequently rented out to other criminals. The types of threats will most likely be these attacks, but also there will be a deluge of spam, phishing and other malware attacks. If learners can show some statistics on the nature and volume of these attacks, it would be useful to compare and contrast with others in the group. The speed and reliability of Internet connections only increases these attacks.

If learners run their own email server from home, they will no doubt see similar images to the one below.

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

```
<fweg@yahoo.com.tw>: Relay access denied; from=<txmgsc@yahoo.com.tw> to=<fweg@yahoo.com.tw>
 <r_r7574@yahoo.com.tw>: Relay access denied; from=<bbztonkmasz@yahoo.com.tw> to=<r_r7574@ya
ija@yahoo.com.tw>: Relay access denied; from=<jhlobolfzu@ms96.url.com.tw> to=<tadija@yahoo.c

.1 <t56084528@yahoo.com.tw>: Relay access denied; from=<ycnoxhgzmzisa@pchome.com.tw> to=<t56
<foolfish86@yahoo.com.tw>: Relay access denied; from=<txmgsc@yahoo.com.tw> to=<foolfish86@ya
ky_805@yahoo.com.tw>: Relay access denied; from=<jhlobolfzu@ms96.url.com.tw> to=<vicky_805@y
a507@yahoo.com.tw>: Relay access denied; from=<jxbiwja@yahoo.com.tw> to=<hsa507@yahoo.com.tw
.1 <itqe@yahoo.com.tw>: Relay access denied; from=<ucdcyrbij@pcome.com.tw> to=<itqe@yahoo.co
pjv@yahoo.com.tw>: Relay access denied; from=<kjhwwpnvzkyt@hotmail.com> to=<2pjv@yahoo.com.t
<cxyx@yahoo.com.tw>: Relay access denied; from=<txmgsc@yahoo.com.tw> to=<cxyx@yahoo.com.tw>
1 <alan69614@yahoo.com.tw>: Relay access denied; from=<kbsfc@yahoo.com.tw> to=<alan69614@yah
252658@yahoo.com.tw>: Relay access denied; from=<jhlobolfzu@ms96.url.com.tw> to=<v22252658@y
1 <ydfm@yahoo.com.tw>: Relay access denied; from=<osmxrucr@yahoo.com.hk> to=<ydfm@yahoo.com.
```

Most of the email here, as can be seen from the addresses, are from Taiwan and Hong Kong, although all purporting to be Yahoo. On this particular home broadband system, there are on average 20-30 attacks per second, that is 1.7-2.5 million per day!

3.3 I can determine the threat to a website in a safe and controlled environment

Learners should be able to analyse and comment on the threat levels to their own institution

Additional information and guidance
The network team may be sensitive to some aspects of their system's security, but should be willing to at least discuss and explain some of the threats they have to deal with and give some examples.

Learners can then make notes on this presentation towards their own summary report for 3.5 below.

Additionally, this outcome may be supported by practical work depending on the technical capabilities of the institution and confidence of the in the instructor. The OWASP organisation maintains a list of intentionally vulnerable web applications here:

https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project [7]

These applications may be used on a local network or on a VPN (Virtual Private Network). The Advantage to this being that the application is kept isolated on either a physical or virtual network segment. This avoids both the danger of running such an application on the public internet and the danger involved in potentially breaching the Computer Misuse Act. It should be noted that these applications should never be run on the open internet or even within a local network without segregation.

In practical terms centers may use several light computers such as Raspberry Pis connected via Ethernet to a local unmanaged router. One Pi would then be able to serve the application while other is connected and running a security distribution of Linux such as Kali would be able to test the security of the application interfacing with it via IP address. https://www.kali.org [8] This method requires some physical hardware to be purchased.

Another option would be to virtualise both the website and the testing distribution using Virtual Box or VMware player. https://www.virtualbox.org/ [9]

https://www.vmware.com/go/downloadplayer [10]

Both machines would then be virtualised within a "host" machine and would only connect with each other via local IP address. This method requires a host on which virtualisation software to be installed which has 4-6Gb of ram in order to run a further two "guest" machines.

A third option would be to partner with a company or use a section of the institution's network to run the virtual systems. Connection to the system would be via an encrypted tunnel meaning that malicious traffic was not being sent in plain through the institution's network and over the public internet.

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

So called “online” vulnerable applications should be avoided.

3.4 I can determine the threat to a server in a safe and controlled environment

Learners should be able to summarise threats that affect a local business

Additional information and guidance
As with the above criterion, it may be difficult for a local company to reveal some of the more sensitive side of their security processes, but should be willing to engage with a local school or college.

If engagement with a local business is not possible, assessors should extrapolate types and levels of threats from government based national data for learners to use in their reports.

Similarly to outcome 3.3 a practical element may be introduced by running an intentionally vulnerable server. The technical process to achieving this is exactly the same as the advice given in 3.3. Examples of vulnerable servers are Windows 2003 (now free) without any security patches applied and Metasploitable Linux.

http://sourceforge.net/projects/metasploitable/files/Metasploitable2/ [11]

3.5 I can produce a presentation or report on my findings

Learners should be able to create and present their findings and recommendations

Additional information and guidance
All of the above exercises will produce broadly similar details, but also very divergent ones. The learners should be able to use their understanding of digital forensics and cyber threats to produce a report to highlight some of the issues in their area. These will vary
depending on the location of the centre and surrounding companies, but should give learners a broad overview of local cyber threats as well as data that they can scrutinise for local anomalies and patterns. The report will also be an opportunity for them to begin exploring some of the ways they can work towards addressing these threats.

Source URL: https://theingots.org/community/sil2u70x

Links
[1] http://www.bbc.co.uk/iplayer/episode/b08vfzm0/horizon-2017-cyber-attack-the-day-the-nhs-stopped
[2] http://www.bbc.co.uk/news/uk-34611857
[3] https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator
[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] http://www.bbc.co.uk/news/technology-39744007
[7] https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project
[8] https://www.kali.org
[9] https://www.virtualbox.org/
[10] https://www.vmware.com/go/downloadplayer
[11] http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');