**Unit 6: Cyber Security Analysis**

Lens email: len@specialistshub.co.uk

# **Portfolio 1**

Think about your company/organisation or at home. The computer systems you or they use are continuously under threat. Look at what it is you use in and around the home: routers, Mobile devices, Internet of Things (Alexa, Google products, Ring doorbells, etc.). If you are doing this as part of a business, look at network infrastructure, physical security, etc.

What vulnerabilities do you think exist?

What can you do about it?

**BT modem/router:**

**Out of date hardware:**

I have had my router for just over 1 year from the time when my contract began with BT. Although I suspect the router to have been new at the time when it was installed in my house, there is no date on the hardware and it could just be a refurbished piece of kit. If this was the case and it was more than 5 years old then using a device that is more than five years could mean it is no longer supported with automatic updates which would offer no guarantee that security risks could be fixed and protected against current threats.

To protect my family network, I will therefore be calling BT to clarify the age of my modem.

**Weak Default Passwords:**

When I logged into my modem setup for the first time just now, the default password set on the router was ‘dpdad6ti’. Containing only 8 characters, all of which are lower case and without any special characters, this was a pretty weak password.

I have just changed the password and made it much longer and more complex.

**Local Network Vulnerability:**

If a potential cyber attacker was in the vicinity of my home network and he managed to crack my Wireless Password to gain access to my network, then we could fall victim to a Man-in-The-Middle attack where the attacker would control all communications between the client and server and he could direct us maliciously how he pleased.

**Cordless Landline House Phone**

**Eavesdropping on our telephone conversations:**

I have a digital cordless phone, but will also discuss analog which was the earliest cordless technology.

**Analog:** Of the two, Analog is the easiest to intercept by anyone with a radio scanner making it possible to eavesdrop on conversations within a one-mile radius.

The best way for somebody with an analog phone to protect themselves would be to upgrade to Digital.

**Digital:**

Digital Enhanced Cordless Telecommunications (DECT) standard is used by many cordless phone makers and is much more secure than Analog, but it does also have vulnerabilities if a hacker is able to crack the manufacturer’s encryption implementation by using software and specialized hardware that was intended for auditors and security researchers and can be used to intercept and decode conversations on certain DECT cordless phones.

I feel pretty secure against DECT hacking due to the need for the necessary expensive specialized expensive radio hardware and the fact that we would not be considered a high value target for hackers to exploit.

If, however, we were a high value target, then it would be best to use an encrypted VOIP service such as Kryptos which uses a combination of AES-256 and RSA encryption.

**Ring Doorbell**

**No encryption:** The data that travels between the Ring device and its application may not be encrypted, making it vulnerable to threats and would put all devices connected to the network (laptops, phones, tablets etc... at risk.

**Ways to protect:**

### Update Passwords with complex unique password.

### Enable Two-Step Verification

### Add a Shared User – to access our Ring in case of emergencies, but without sharing login information with them.

### Monitor and Delete Old Footage

### Do Not Share Footage

### Invest in a robust and reliable Antivirus Solution and keep updates with the latest software.

**Laptops & Mobile Phones:**

Besides the obvious vulnerabilities and the many ways to reduce the threats, already covered in Unit 4 with Bob, our devices contain cameras and speakers making it possible for hackers to spy on us and eavesdrop on our conversations.

Good antivirus software to make it tough for hackers to gain access to our devices and cover any cameras when not in use.

**Portfolio 2 – Threat Intelligence**

# **Task 1**

Research a number of sources of threat intelligence (at least 3).

1. The Spamhaus Project: a European non-profit organization that tracks cyber threats and provides real time threat intelligence. They have developed blocklists for known spammers and malware distributors which they provide to ISP’s, email SP’s and organizations.
2. Google Alerts: a feature that comes free with Gmail that can be used to create a user’s threat intelligence alerts by allowing the user to set up alerts based on keywords or phrases that will look at all the websites indexed by google & return relevant links to the user by email, so if the user sets up an alert focused on cyber threats and security, they will receive relevant news and stay informed with the requested information sent to them regularly.
3. VirusTotal: ‘The google of cybersecurity’ (ref - securitymadesimple.org’), where you can input files, URL’s or IP addresses into the search bar and it will scan them to see if they have been associated with any type of malicious behavior. They don’t provide any in depth threat intelligence, but is a great first point of reference for checking suspicious items.
4. Netacea Bot Management: Mitigating automated threats to medium to enterprise businesses, providing protection against malicious bots across an organization’s website, mobile apps and API’s, by distinguishing between automated bots and humans t prioritize genuine users.

# **Task 2**

Identify which threat actors and threats/attacks are of most risk to you/your organization. What would be their motive?

1. Organized Cyber Criminals: make money by stealing data belonging to organizations. Cybercrime is of great appeal to them because it offers less risk to them than physical theft i.e. bank robbery enabling them to hide their identities whilst performing ransomware and business email compromise attacks typically via phishing emails.
2. Insider Threats: Employees who turn against their employers taking advantage of their privileged insider access to systems and networks. This could also be caused by an innocent employee mistake.
3. Lone Wolf Hackers: wants to hack computers because they can, usually young people who have acquired hacking tools built by more talented hackers. There are also more capable and talented lone wolf hackers and both pose a serious threat to organizations and regular recreational internet users.
4. Hacktivists: Hackers with a cause e.g. attack the government.

# **Task 3**

Identify if there are any new or emerging threats which may be of risk to you/your organization

1. Phishing Threats becoming more personalized: The company I work for loveholidays.com had a recent phishing email sent by [HR@loveholidays.com](mailto:HR@loveholidays.com) which is not an email belong to anyone in our company, but all our emails end @loveholidays.com.
2. I had a text message last week from PayPal saying that I’d had a suspicious transaction for $100 and to click the link to verify if it was genuine – or something along those lines. Anyway, I suspected it to be a scam and checked my PayPal and bank accounts to confirm my suspicion, but it was very authentic and could easily fool many recipients.
3. Attacks on the healthcare and civil service sectors: due to more employees working from home many organizations have relaxed their firewall settings.
4. Cloud security: there is a need to improve cloud security as apparently most don’t provide secure encryption.
5. New cars that are connected to the internet: could be fatal if a hacker gains access and complete control to your vehicle whilst driving.
6. IoT: can be used by cyber attackers for DDOS attacks and would more than likely go unnoticed. They are also a weak entry point for an attacker to a home network.

**Portfolio 3 – Future Trends**

# **Task 1**

Use the following list:

1. Educational technology
2. Information technology
3. Nanotechnology
4. Biotechnology
5. Cognitive science
6. Psychotechnology
7. Robotics
8. Artificial intelligence
9. Internet of Things and Edge Computing
10. Quantum computing  
      
       
      
    Choose three items on the list and answer the following questions for each topic:
11. Why is it good?
12. What could go wrong?
13. Why would it be bad?
14. Ethical?
15. Moral?
16. What is YOUR conclusion?

Your portfolio can be presented back in word or PowerPoint

**Artificial intelligence**

1. **Why is it good?**

AI could offer superior faultless performance to humans. Besides improved accuracy, AI doesn’t forget, get tired, sick, go on holiday or need money. It can work 365/24/7. It also has beneficial uses for people with disabilities such as blind people to help them to communicate with others using voice assisted AI.

1. **What could go wrong?**

It is easy to see why large firms who can afford it would opt for AI employees over humans, so in certain industries such as aviation, manufacturing AI poses a significant risk of job losses to humans.

AI could be used by large criminal organizations for enhanced cybercrime, exploiting vulnerabilities much faster than human hackers. A pilot-less aircraft could be compromised mid-flight to and manipulated to devasting effect.

Another potentially to devasting use would be if control over Autonomous weapons got into the wrong hands. We could see AI wars taking humans out of the equation, but at risk of huge casualties.

1. **Why would it be bad?**

Job losses, collapsed economies, huge human casualties. AI could become so intelligent that it develops itself and humans may be deemed as obsolete.

1. **Ethical?**

One ethical issue posed by AI could be privacy and data protection as AI could generate personal data without the consent of the individual.

AI can also be biased due to incorrect assumptions in the machine learning process. Incomplete data could lead to mistakes e.g. Wrongly assuming a man cooking to be female because the AI assumes cooking to be a female activity. I read an article (see link below) where AI could not recognize a dark-skinned face due to the system being trained to recognize mostly white men.

1. **Moral?**

As AI become more intelligent one would hope that it will be developed to have good moral judgement to be able to recognize the emotional repercussions of its decisions and actions with strict accountability measures in place for any poorly judged situations.

1. **What is YOUR conclusion?**

It’s easy to see why CEO’s would adopt AI to vastly improve productivity and efficiency, sadly to the detriment of their front-line staff. I personally would feel very uneasy about boarding a pilotless aircraft and it would be even more depressing if the cabin crew were also AI robots, no matter how realistic! Certain experiences and situations are enhanced with the human touch. Maybe the increase in AI in our everyday lives will make us appreciate each other more, rather than constantly absorbed in our mobile phones not present in the moment.

**Nanotechnology**

1. **Why is it good?**

The manipulation and manufacture of materials and devices on the scale of atoms may make it possible to manufacture lighter, stronger and programmable materials that require less energy to produce than conventional materials. They may produce less waste to manufacture and offer greater fuel efficiency to transportation ie aircraft, ships etc..

Other possible beneficial uses:

* Nanocoating of surfaces to make them more resistant to damage and radiation.
* Nanoscale electronic devices with unprecedented processing powers which could be used as biological sensors for protection, healthcare and the environment.

The potential for improvements in health, safety, quality of life and to protect the environment are vast.

1. **What could go wrong?**

Worryingly Nanoparticles can get into the body not just through the lungs and digestive system, but also through the skin and increase the risk of cancer.

1. **Why would it be bad?**

The human body has built up a natural immunity to most natural and manufactured toxins, but with no natural immunity to Nanotechnology this could lead to many more cases of the more severe illnesses ie cancer.

1. **Ethical?**

There isn’t enough public awareness of nanotech for us to be able to trust it. How do we know which of our everyday products contain it and has it been clinically trialed enough to justify the risks?

1. **Moral?**

Educating society about the benefits and risks is important to gain public trust, and to give us a choice and opportunity to protect ourselves.

1. **What is YOUR conclusion?**

If it’s used for good then there are significant benefits to health, natural resources and in turn the environment, but if it’s abused then it could cause unprecedented harm to us. I would have felt much more confident in its use for good 2 years ago than I do now where we are not as confident about who we can trust!

**Psychotechnology**

1. **Why is it good?**

Psychologists use a wide range of tools to study human behavior in various situations to better understand, predict or control human thought processes and emotions which could be used to improve mental health, behavior and intelligence, to enable human beings to operate to their full potential or maybe even to find new ways to use our brains. I’ve always wanted to be able to change channels on the tv using mind control! One day this could actually be possible.

1. **What could go wrong?**

The human brain and mind are very fragile and should therefore be handled with the greatest of care to avoid permanent damage. We are human beings and many believe created by God, but if we were to be psychologically enhanced by technology then are we still human or are we evolving into Cyborgs? Could a Cyborg give birth naturally to a Cyborg baby one day? In my opinion that is doubtful.

1. **Why would it be bad?**

As human beings we always want more, it is human nature to never be quite satisfied with what we have, hence the constant evolution of newer technologies. We only use about 10% of our brains, so if psychotechnology so being human we won’t stop until we have humans operating at 100% and no doubt at that point a new boundary will be set! This enhancement however will only be a privilege enjoyed by the top percentiles, so this will create huge divide between the knows and the know nots!

1. **Ethical?**

Over the course of the past 3 million years many types of Homo Genus have inhabited the earth, many different genus occupying the same areas at the same type e.g. Homo sapiens have only been the sole occupants of earth for the past 40,000 years which is the time when Neandertals, who were physically stringer than us, but less intelligent, are believed to have become extinct. It is believed that we are the reason behind their extinction. Is psychotechnology the next big step in evolving some homo sapiens into a superior human kind and in turn what would that mean to the homo sapiens who do not have the opportunity or desire to enhance their mental state or intelligence?

Just like our Neandertal relatives could homo sapiens one day be deemed obsolete?!

1. **Moral?**

As psychotechnology develops, hopefully is will continue to be used for good. Like all technologies if it’s abused then the repercussions could be catastrophic. Mass brain washing to Ingnite divisions is one area of concern.

1. **What is YOUR conclusion?**

It is essential that we use psychotechnology to enhance our positive traits and reduce the negatives! It is a scary thought that it could be misused to enhance a lack of empathy and other psychopathic traits that could lead to our own extinction!

If used for good, then it’s a very exciting possibility! Who wouldn’t want to be able to have a photographic memory, learn and master a new skill or language as quickly as a computer downloads a piece of software!?

My only hope is that in the process we will retain our identity as equal human beings!