Virtual Engagement Lesson Guide:

Making Better Decisions
with Threat Intelligence

Introduction

Lesson summary
In *Making Better Decisions with Threat Intelligence* pupils act as cyber security decision makers protecting a pharmaceutical company. This introduces some of the basics of *threat intelligence*.

Pupils are posed with a series of different scenarios, tabletop style. They have to prioritise their resources and staff to protect the company from cyber attack.

Who is this for?
Anyone working in technology with a familiarity with the basics of cyber security will be able to run this session. Background knowledge in threat intelligence, risk management, or incident response is useful and will let you add value, but is not required.

This lesson plan is an example of a high-quality cyber security activity suitable for high school age students. It's suitable for any classes who've covered the basics of cyber security, such as malware, or what constitutes a cyber attack. It is ideal for all studying the National Progression Award in Cyber Security. It has been designed for remote delivery but is also suitable for an in person volunteer visit.

How to use this lesson plan
1) Read through the lesson plan alongside the accompanying slides
2) Customise the slides to reflect what you do
3) Look at the sample responses to some common questions (Page 9)
4) Practice delivering the lesson, perhaps with a colleague or two
5) Engage with the classroom!

Daniel Devine
Digital Skills Education
April 2023

Lesson Plan

	Making Better Decisions with Threat Intelligence Session Volunteer: Teacher: Class Year/Level: Sample Slides: https://docs.google.com/presentation/d/1LMAYYq1Pch8Zoyc-To9mrFT64GEToKC5wp5TUh6L6-s/edit?usp=sharing
Maximum 5 minutes	**Introduction** Give a short, 2-3 slide, presentation on the area and what you do. Think about what context the learners might need for the activity - in this case being prepared for a cyber attack, and collecting intelligence. Make sure to include: • Your name and how you'd like to be addressed • Where you are calling from • What your role is (a brief description of what you do) • Who you work for and what the company does "Hello, I'm Christina Greenhalgh. Today you can call me Chris. I'm joining you today from our office in Jedburgh. I am a security analyst at Medium Security Corp. I make sure that businesses can keep running by helping them prepare for and protect against cyber attacks." "Today you're going to use your knowledge of cyber security to make recommendations that will keep a company secure. Our activity is based on a real-life job role, a security analyst or manager." "You're also going to get the chance to ask me any questions about my role as a cyber security analyst working at Medium Security Corp." See slides 2-5 for inspiration. You may adapt these to match your role.

Maximum 5 minutes	**Some basics - What is a cyber attack** "A couple of questions for you..." "What is a cyber attack?" A malicious attempt to steal data or damage someone's computer system. Things like sending viruses, or trying to guess passwords would count. "How do you know if one is going to happen?" You don't ever know for sure. It's really difficult to tell. But there is a whole career about this. **What is threat intelligence?** "It's called threat intelligence. It's about understanding the enemy, understanding the risks." "Threat intelligence is a branch of cyber security about understanding the wider context of cyber attacks, how likely things are to happen, and how bad it would be if they did happen." "The aim is to use that information to stop or reduce cyber attacks or data breaches." **Different types of threat intelligence** "There's different types of threat intelligence. Technical, strategic, and tactical." "You don't need to remember these different types, but you might find it interesting." "Technical threat intelligence usually is something you can 'fix'. Often it will be things like 'a vulnerability has been found and patched' - basically there's a bug that a cyber criminal could exploit, but a fix is available. What you'd do next is tell the IT team to go and do that update." "Strategic are less specific, some research might say "phishing attacks are expected to rise". It doesn't say what they'll look like, but you can still do something about it like arranging more staff training." "Tactical threat intelligence is very specific. These pieces of intelligence come from places like GCHQ, the CIA, and other intelligence agencies. They will warn specific companies or governments about specific threats. Maybe there's a hacker group who are targeting certain people. If you know you might be a target, you can step up your resources and defences."

Maximum 5 minutes	**Bearsden-Bio** "Now it's your turn! You are going to make some decisions using some intelligence!" "You are responsible for the day-to-day running of the security team at a pharmaceutical factory, Bearsden-Bio." **Situation** "Here's the situation" "They are a small team, and have to carefully prioritise how they protect their data, networks, and operations." "Your task is to decide what the team should and shouldn't work on, while keeping everything secure." **What's important to management** "The Bearsden-Bio board, that's the big bosses, have decided on their top 3 risks: 1) Production stops - We need to keep the factory running and making drugs 2) Theft of confidential information - We need to protect our secret formulas 3) Reputational damage - We must maintain our reputation for safety and reliability "You'll need to bear in mind these priorities when you're making decisions."
Maximum 10 minutes	**Round 1 - Resource Prioritisation** "Okay, time to make some decisions." "You have a small security team, so you need to carefully prioritise your time." Give the following instructions. Depending on the class, you may choose to have them complete the activity in groups.

	"It's up to you, individually (or in groups), to make some decisions to choose how we spend our time. 1. Take a piece of paper, and write down these 6 different tasks. 2. Write numbers beside each one, the bigger the number, the more important you think it is and the more time you'll spend on it. Everything needs to add up to 100." **Testing our decisions** "Let's find out what the results are of your decisions" "Cyber threats are unpredictable, so we're going to use random number generators" If you have dice, then you can use them. If not, use one online. **Simulation** "Oh no! The company has been targeted by some amateur cyber criminals. They sent phishing emails to lots of staff to trick them into sharing their passwords." "We're going to see if the decisions you made will have protected us against this attack." Ask the class to follow the instructions. Get some feedback from some pupils, did they survive the attack? How did they choose their points?
Maximum 5 minutes	**Round 2 - With Threat Intelligence** "I've just received some intelligence." "This is what tactical threat intelligence often looks like. It's a short report with some advice." Read the notice from the slide. **Prioritisation** "It's your turn to make some decisions again."

	"Now that we've received some intelligence, you might want to reconsider your decisions." "Take your piece of paper, and redistribute your 100 points." Get feedback from some pupils. How did they choose their points? Did they do anything different this time? Why?
Maximum 10 minutes	**Round 3 - With additional threat intelligence** "We've received some new intelligence." Read the notice from the slide. **Prioritisation** "You might want to reconsider your decisions again!" "Take your piece of paper, and redistribute your 100 points." Get feedback from some pupils. How did they choose their points? Did they do anything different this time? Why? **Simulation** "Let's do a simulation now." "We need to test all of our defences." "Follow the instructions to see how you have fared." It is recommended that you walk through this process with an example pupil, before letting the rest of the class assess their decisions.

At least 10 minutes	**Summary** "It's difficult to manage limited resources to keep an organisation protected against cyber threats." "Threat intelligence is a really important tool used to make better decisions." **Next Steps** Add your own website here, maybe you have some initiatives or programmes to recommend? **Q&A** You should hold a Q&A for the remaining time of your engagement. Aim to hold 10 minutes for this. If you're running behind, skip a round, not Q&A time. By keeping Q&A till the end the pupils will understand more about what you do, and how data is secured in industry. This will assist them in asking deeper and more insightful questions. We've gathered some frequently asked questions, along with sample answers on the next page.

Frequently Asked Questions

Is being a cyber security analyst a good job?
"Yes, working in cyber security as an analyst is a great job with fantastic opportunities for the future. People with knowledge in cyber security are in high demand and salaries are high. A university graduate can expect to earn between £25,000 and £30,000 [prospects.ac.uk] straight after university which is above the UK average of £24,217 [HESA Graduate Outcomes 2020].

For example, at the time of writing (January 2022), ScottishPower are looking for new cyber security graduates in the Glasgow area and will pay you a starting salary of £28,400. This is almost the average salary in the UK overall (£29,600) [uk.jobted.com/salary] when you are just starting the job!"

What school subjects should I take?
"People in cyber security have a wide range of backgrounds. However, computing is probably the most important along with maths and physics. You should try to take these subjects as far as you can (Higher and Advanced Highers)."

Where can I study cyber security?
There are different options to study cyber security at many colleges and universities in Scotland. There are apprenticeships for school leavers, HNC and HND college courses, and BSc and MSc university degrees. Below are some examples:

- College
    - Edinburgh College – HND Cyber Security and Forensics
      Requires 3 Highers or above and that you are comfortable with a computer. No previous programming knowledge is required. This course grants access to the third year of a BSc at Edinburgh Napier University on completion. (https://www.edinburghcollege.ac.uk/courses/browse/cyber-security-hnd-benghons-cyber-security-and-forensics-cr1cseka21)
    - Forth Valley College - HNC Cyber Security
      Requires 2 Highers, and 5 N5s. One of your subjects must be computing related.
      (https://www.forthvalley.ac.uk/courses/computing/hnc-cyber-security)
- Apprenticeship
    - QA - Information Cyber Security SCQF 8 Technical Apprenticeship
      Anyone can apply, but you'll need to demonstrate some knowledge and willingness to learn in cyber security.

(https://www.qa.com/course-catalogue/courses/information-cyber-security-scqf-8-apprenticeship-programme-scotland-qaacsl68s/)
    - Glasgow Caledonian University - BSc (Hons) Graduate Apprenticeship
      Requires 4 Highers at BBBB. Your time is blended between an employer, and the university.
      (https://www.gcu.ac.uk/study/courses/details/index.php/P03224/Graduate_Apprenticeship_Cyber_Security/)
- University Undergraduate
    - Abertay University - BSc (Hons) Cyber Security
      Highers ABBB including Mathematics at B.
      (https://www.abertay.ac.uk/course-search/undergraduate/cybersecurity/)
    - Edinburgh Napier University - BSc (Hons) Cyber Security and Forensics
      Highers BBBB to include Maths or Physics.
      (https://www.napier.ac.uk/courses/beng-hons-cybersecurity-and-forensics-undergraduate-fulltime)
    - Heriot Watt University - BSc (Hons) Computer Science (Cyber Security)
      Highers ABBB (including Mathematics).
      (https://www.hw.ac.uk/uk/study/undergraduate/computer-science-cyber-security.htm)

Next Steps

Visit the Digital World Website
https://www.digitalworld.net/cyber-security/learning-opportunities
The Digital World website will let you explore the different areas of cyber security available. You can find up to date information on where you can study, and other learning opportunities and resources.

Play Cyber Skills Live activities
https://cyberskillslesson.com/
Some good activities to start are:

> *How To Steal A Pizza - In this interactive lesson, you'll step into the shoes of a cyber security consultant. Your job is to help this business defend against cyber attacks*
> Defend The Power Stations - *Step into the shoes of a cyber security defence team to defend against a live cyber attack. Your challenge is to defend Scotland's Power Stations from a Denial of Service attack.*

We also run activities live!
Our interactive lessons don't need any technical knowledge. By taking part, learners develop digital skills while learning about cyber security topics. Over 150,000 learners have already taken part live! You can register your interest here - https://cyberskillslesson.com/

Acknowledgements

Authors
Daniel Devine
Craig Steele
digitalskillseducation.com

Thanks to
Mike Smith
Boclair Academy
Debbie McCutcheon