Keeping The Lights On

Lesson Guide

DIGITAL SKILLS EDUCATION

DIGITAL WORLD SHAPE IT

Virtual Engagement Lesson Guide:

Keeping The Lights On

Data Security

Introduction

Lesson summary
In *Keeping The Lights On* pupils act as cyber security analysts and engineers protecting the electricity grid. This introduces some of the basics of *data security.*

Pupils are posed with four different scenarios, tabletop style. They have to identify the best practical mitigations and approaches to protecting critical national infrastructure 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 distributed systems, industrial computing, or the energy sector 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 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 10)
4) Practice delivering the lesson, perhaps with a colleague or two
5) Engage with the classroom!

Daniel Devine
Digital Skills Education
January 2022

Lesson Plan

	Keeping The Lights On - Data Security Volunteer Session Volunteer: Teacher: Class Year/Level: Sample Slides: https://docs.google.com/presentation/d/1in3HyfAx_7cfGTji_AMp3y0vyBc9gd5KIvS-cxKCc6Q/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 introducing how data is used, and why it's important it is protected, in the energy sector. 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 Eleanor Dee . Today you can call me Ellie. I'm joining you today from our office in Kinross. I am a security engineer at Big Grid Industries. I make sure that electricity is available 24/7 for homes and businesses by ensuring the electricity network is protected against cyber attacks." "Today you're going to use your knowledge of data security to make recommendations that will keep our energy company and its data secure. Our activity is based on a real-life job role, a security engineer or architect." "You're also going to get the chance to ask me any questions about my role as a cyber security engineer working at Big Grid Industries." See slides 4-8 for inspiration. You may adapt these to match your role.

Main Activity Keeping The Lights On

Maximum 5 minutes	**Setting The Scene** "We're going to do an activity together about data security in our industry." "For us, keeping the lights on, keeping electricity available to everyone, is essential. We all rely on electricity, and society would quickly break down if we lost it." "We're going to do a tabletop exercise together, something that real cyber security teams do on a regular basis." **Tabletop Exercise** "Tabletop exercises are meant to help organisations consider different risk scenarios and prepare for potential cyber threats." "Bringing everyone together to discuss different scenarios, and talk about what could be done to mitigate, or reduce the risk." "Security teams do this type of exercise often. It's all about communication." **A Smart Grid** "Before we start working through the tabletop scenarios, here's what we're protecting." The electricity grid used to be quite simple, and operated using mechanical switches. Someone would have to drive to a substation, and pull a lever to change the flow of electricity. That made sense because we only had a few power stations and the electricity was predictable." "Nowadays, there's so many different places where electricity is generated. We still have big power stations, but there's also wind farms, solar farms, and customers with solar panels. The amount of electricity is much more variable depending on the weather so we have to control it. It's not possible to drive around and operate things manually. We need remote control and computer systems to make the grid 'smart'." "A smart grid is much more susceptible to cyber attacks because there's so many different computers, and in so many different locations. It's a really big problem to keep it secure." **What are we protecting?**

	"It's not just computers we need to think about. There's the computers and servers in the control room, but we have loads of different types of smart devices on our electricity network." "These devices are things like switches to turn electricity supplies on or off, or to redirect where the electricity is going. There's devices which measure the flow of electricity. There's also lots of what we call protection equipment which can turn off the power if a fault is detected. This is really important for everyone's safety." **Instructions** "You're representing the data security team." "Let's walk through some scenarios." "Use your knowledge of data security to make recommendations that will keep our energy company and its data secure"
Maximum 5 minutes	**Scenario 1** **"*Ofgem* is sending our staff malware that is known to target control systems. It looks like a press release."** "A suspicious email account, pretending to be the regulator Ofgem, is sending emails to everyone in the staff directory." "The emails contain a file titled "press release", but actually contains a virus that targets our control systems." "Take a look at this list of common security measures. What security measures would help stop the malware from getting into the control system?" 1. Ask pupils to write down ideas in pairs. 2. Ask the teacher to set a timer for two minutes so they know when it's time to feed back and listen to you again. 3. Take an idea from each pair and discuss together 4. Do you have any experience with this kind of problem? Share it with the class! Definite yes: • Network Segmentation • Antimalware Software • Firewalls But also, importantly for phishing: Staff Training/Culture

Maximum 10 minutes	**Scenario 2** **“A laptop used to remotely access the control room has been stolen”** “One of the laptops which is used by engineers to remotely access the control room has been stolen. We don’t know who stole it, why they stole it, or where it is now.” Pose the question, “*Why might someone steal the laptop?*” to the learners. Answers and things to talk about may include: • To disrupt the electricity network • Steal trade secrets • To sell to an organised crime group • To damage the reputation of the company (competitor) “Take a look at this list of common security measures. What security measures would help stop the thief from being able to access sensitive data?” 1. Ask pupils to write down ideas in pairs. 2. Ask the teacher to set a timer for two minutes so they know when it’s time to feed back and listen to you again. 3. Take an idea from each pair and discuss together 4. Do you have any experience with this kind of problem? Share it with the class! Definite yes: • Data encryption • Strong Passwords • 2FA • Device Encryption Also, to recover: • Backups Or, to stop the theft happening in the first place: • Keycard Access • Security Culture • Policy (must be physically protected at all times - eg. in a locked house)

Maximum 5 minutes	**Scenario 3** **“An unrecognised person has been seen on CCTV inside the data centre. The keycard log shows them as an ex-employee.”** “CCTV inside the data centre, where our most important data is stored, has captured someone inside. We checked the keycard log, and their pass is supposedly owned by an ex-employee.” “Take a look at this list of common security measures. What security measures would help stop the intruder from being able to access data?” 1. Ask pupils to write down ideas in pairs. 2. Ask the teacher to set a timer for two minutes so they know when it’s time to feed back and listen to you again. 3. Take an idea from each pair and discuss together 4. Do you have any experience with this kind of problem? Share it with the class! Definite yes: • Keycard Access • Data Encryption • Port Locking • Strong Passwords • 2FA • Device Encryption But also, importantly for phishing: Staff Security Culture (challenging people)

Maximum 5 minutes	**Scenario 4** **“A substation was left unlocked and a cyber criminal has entered.”** “We’ve heard that a cyber criminal has managed to get into one of our substations, apparently it was left unlocked!” “Take a look at this list of common security measures. What security measures would help stop the criminal from being able to plug in their laptop and access the whole network?” 1. Ask pupils to write down ideas in pairs. 2. Ask the teacher to set a timer for two minutes so they know when it’s time to feed back and listen to you again. 3. Take an idea from each pair and discuss together 4. Do you have any experience with this kind of problem? Share it with the class! Definite yes: • Network Segmentation • Port Locking • Firewalls

Questions and Answers

At least 10 minutes	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 scenario, 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 engineer or analyst a good job?
"Yes, working in cyber security as an engineer or 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
Fay Sears
Victoria Breeze
SSE
Johnstone High School
Debbie McCutcheon