BUSINESS LESSON

MANAGING SECURITY AND IT INTEGRATION

TEACHER'S NOTES

CREATED BY
ESLDEBATES.COM

Managing Security and IT Integration

https://www.esldebates.com/business-managing-security-and-it-integration/

Vocab matching answers

1. f
2. i
3. g
4. a
5. h
6. b
7. l
8. c
9. j
10. k
11. d
12. e

Video Answers.

1. He works for Vorstand Baramundi Software AG.
2. In recent years, he has seen a rise in the number of cyber-attacks in both IT and OT.
3. When he talks about cyber-attacks, he means the theft of data, sabotage, and espionage.
4. The damages caused by these attacks amount to approximately 55 billion euros per year in Germany.
5. The focus of the attacks is on OT or production. 36 percent of the attacks take place in this area.
6. When they talk about Industry 4.0, they make reference to new business models, new opportunities, and increased efficiency. It is a current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things, cloud computing, and cognitive computing. Industry 4.0 is commonly referred to as the fourth industrial revolution.
7. They can be vertical or horizontal. Vertical means that systems that were previously isolated are now connected in a network –being vulnerable to attack. Horizontal means the attack works cross-company and triggers a domino effect; an attack can spread to other areas and to other companies.
8. He mentions four steps: cataloging (software and hardware analysis), analysis (the system analyses the weak spots), securing (removing the insecure elements from the network), and making sure the new firmware and software is as secure as possible.
9. In OT, the primary protection goal is the safeguarding of production.
10. In IT, the principal protection aim is the protection of data.

Warmer questions

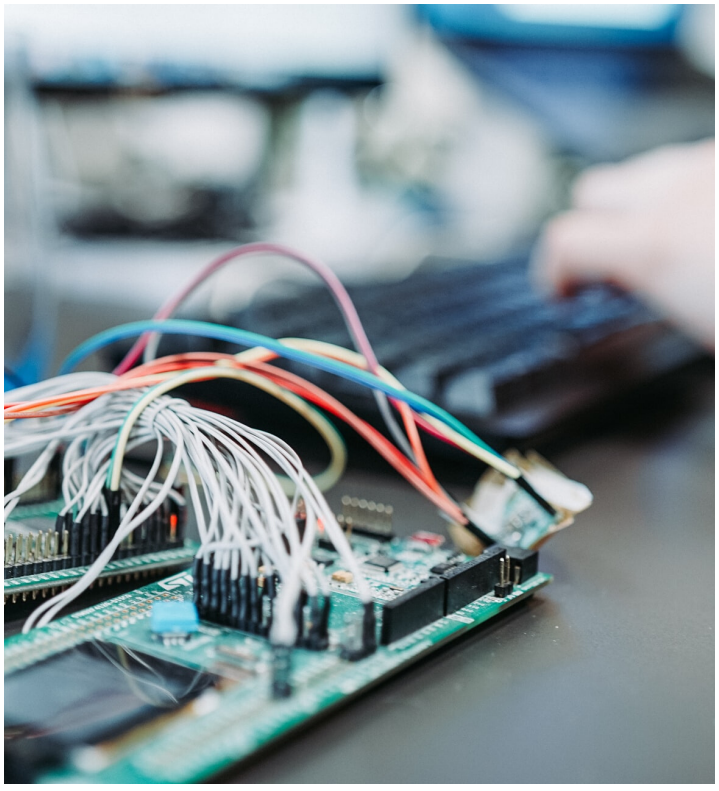
- What are the biggest risks in IT today?
- Are there any well-known incidents of IT risks in public life today?
- Have computer systems become too integrated and complex?
- Are industry computer systems modern and making positive improvements?

Reading section

Open door security policy

In today's digital world, security management is a wide-ranging topic that embraces many activities related to controlling and protecting access to a system and network resources.

Nowadays, office networks are primarily concerned with data security, while the major concern for industrial automation networks is uptime. Industrial control systems (ICS) security was considerably simpler before the web. Organisations were predominantly concerned with physically protecting their systems behind gates. But once the Internet appeared, the threat of connectivity-enabled attacks –with no physical access needed– became increasingly possible.



Companies are accordingly dedicating resources to protecting their ICS assets against intentional or accidental security threats. Defending these systems is now part of the industrial safety programs. The ICS networks and data acquisition systems (SCADA) that run today's modern society are a collection of devices designed to work together as a unified and homogenous system. In particular, the integration of automation, communications, and networking in industrial environments is today an integral part of what it is called the Internet of Things (IoT).

Information technology (IT) includes any use of computers, storage, networking devices and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data. And operational technology (OT), traditionally associated with manufacturing and industrial environments, includes ICS such as supervisory control and data acquisition systems.

When IT and OT systems work in harmony together, new efficiencies are discovered. Systems can be remotely monitored and managed, and organisations can obtain the same security benefits from administrative IT systems. Still, ICS security has plenty of challenges. Several of them owe their existence to the constant convergence of IT and OT. OT's upgrading through IT integration brings with it some security issues. Many operational technology systems were never designed for remote accessibility and, consequently, the risks of connectivity were not considered. Therefore, the vulnerabilities can leave organisations and critical infrastructure at risk of industrial espionage and sabotage.

In the UK, the most well-known act regarding cybercrime is the Computer Misuse Act 1990, which brings in three offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

This act has been amended twice in 2006 and 2015, introducing:

- 3ZA. Unauthorised acts causing, or creating risk of, serious damage.
- 3A. Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA.

Each of these offences carries a different potential prison sentence. Offence 1 and 3A has a potential sentence of 2 years imprisonment, offence 2 is five years imprisonment, 3 is 10 years. Offence 3ZA is the most serious crime covered by this Act and has a maximum sentence of life.

Questions to consider:

- Automation is, again, an important subject discussed in software protection. How to prevent massive leakage of sensitive information when all devices are interconnected?
- The smarter devices, the smarter attacks are possible. Will cyber-attacks ever stop?
- It is quite common to see hackers targeting other nation-states to where they live. Being that the UK has extradition relations with over 100 territories around the world, is the risk of extradition stopping British cybercriminals from attacking overseas?

Vocabulary matching

Using the words on the left match them to their real definitions.

Vocab Meaning	Meaning
1. IT	a. is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
2. OT	b. Susceptible to physical or emotional attack or harm.
3. Network	c. Deliberately destroy, damage, or obstruct (something), especially for political or military advantage.
4. The Internet of Things	d. Permanent software programmed into read-only memory.
5. Hacker	e. A means of protecting something from attack.
6. Vulnerable	f. Short for Information Technology. The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
7. Theft	g. A number of interconnected computers, machines, or operations.
8. Sabotage	h. A computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem.
9. Espionage	i. hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.
10. Software	j. The practice of spying or of using spies, typically by governments to obtain political and military information.
11. Firmware	k. The programs and other operating information used by a computer.
12. Defence	l. The action or crime of stealing.

Video: Managing Security and IT Integration

Barramundi is a German software company that develops end-user suites and mobile apps to provide security. They also have software that seeks to automate routine tasks (like checking for viruses) to benefits users.

Watch the video and then answer the questions below

1. Who is Dr Lars Lippert?
2. How vulnerable are companies right now?
3. What does Dr Lippert mean by cyber-attacks?
4. How much do these attacks cost per year?
5. What is the focus of the attacks?
6. What is Industry 4.0?How are the attack scenarios in the Industry 4.0?
7. What steps does Lipper mention in order to fix a weak point?What is the main goal of OT protection?
8. What is the primary objective of IT defence?

Benefits of IT/OT Convergence

- Cost reduction: By applying similar technology, standards, and governance principles for IT and OT, easy-to-convert synergies will be found in many organisations.
- Risk reduction: IT/OT convergence means security issues can be jointly addressed by IT and OT, leading to an integrated approach that provides enhanced security against intrusions from outside the company and to central security governance throughout the company.
- Enhanced performance: With the convergence of IT and OT, time and costs will be saved while allowing the smooth transition of newly-developed products into existing manufacturing operations.
- Produce anywhere: IT/OT integration will provide better transparency with regards to costs and cost structures and therefore lead to site efficiencies. The company will become more flexible, allowing for manufacturing to shift between locations.

The challenges concerning IT/OT

- Security Breaches. Access if often more limited, because greater access poses a more cybersecurity risk and possible service interruption.
- Limited Access. Connections to industrial automation networks can be limited to only those who categorically require access, and the level of access can be restricted based on each person's requirements. With such narrowly regulated access, certain security measures can be implemented which would not be practical for an office network.
- Size and Stability. Office networks, for example, tend to be very large when compared to industrial automation networks. A company is likely to have numerous PCs, tablets, and smartphones in traditional IT applications connected via Ethernet, intranet, and Wi-Fi networks.
- Software Updates. An item connected as a peripheral device typically communicates via an industry-standard protocol. Even if all components and networks are supplied by one vendor, any software change must be tested before its implemented. When components and networks are supplied by different vendors, there is more reason for caution.

Potential debating topics

- All data should be publicly available –this is the only possible way to stop data theft!

- We must defend our right to privacy and make every reasonable effort to ensure the security of our private information.

- Software protection companies must be stopped. Intuitive interface and automation will lead us to a disproportionate dependence on machines.

- Software protection companies are our allies and should not be stopped. They carry out daily security checks to guarantee the complete safety of our online transactions.

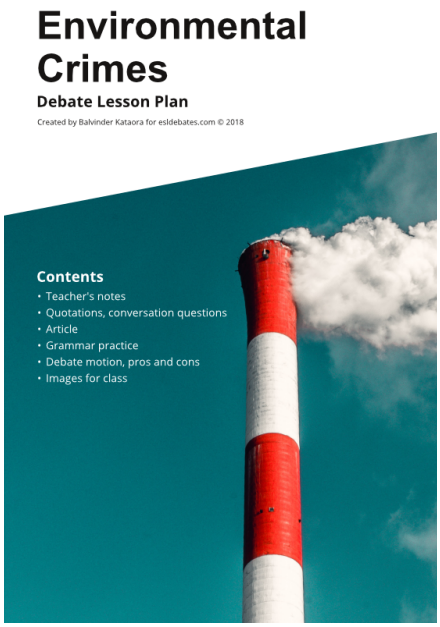
- Hackers are often different and misunderstood adolescents. They mean no harm. They should not be punished at all.

- Cybercriminals are anti-social individuals who should receive the maximum applicable penalty!

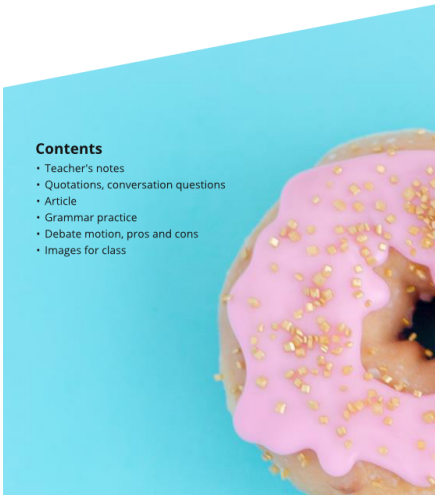
DEBATING PLANS

PREMIUM 30-PAGE DEBATING LESSONS ON DOZENS OF TOPICS

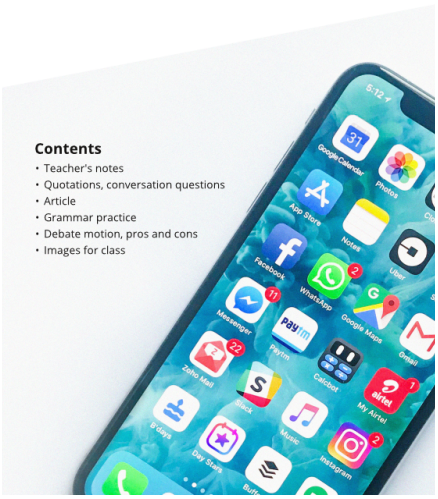
These lessons are extensive and includes a magazine-like introduction, a 2-page article, vocabulary section, grammar exercises, and images for discussion. To help students organize their debate, worksheets are included for appropriate language and pros and cons to get them started. In total these lesson plans offer 30 pages of activities and tasks for students.



Should natural features be given legal rights to protect them from pollution? This debate will target issues relating to how to legally protect the environment and criminalise pollution.



What are the best ways to tackle obesity? Some people advocate better food education, while others want to tax people to change their spending habits. Which is the most effective?



People are becoming increasingly concerned about social media. Discuss the main issues and find out what your students think and why.

WWW.ESLDEBATES.COM/SHOP