Industry Resource Links

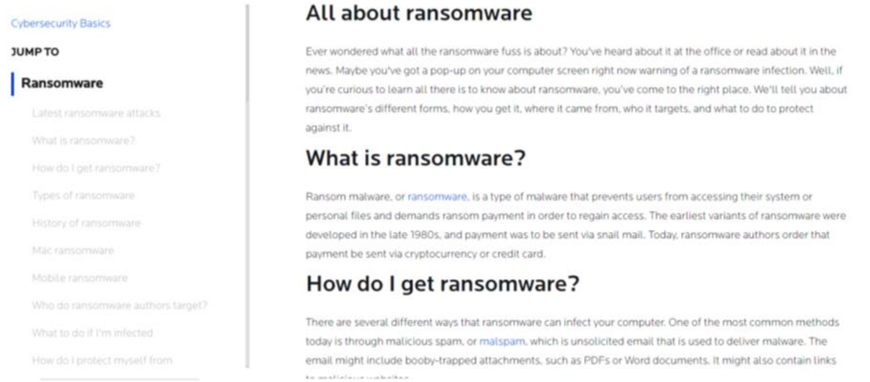
Topic: Security

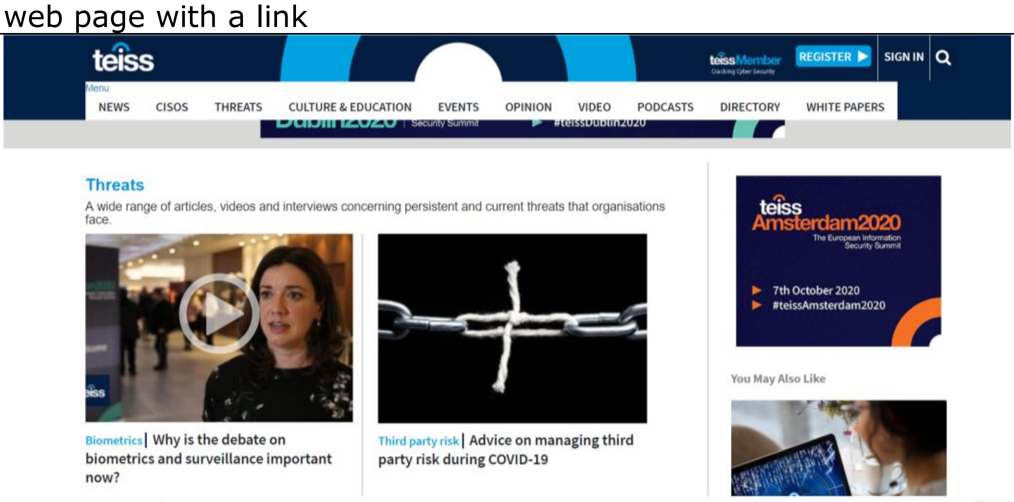
Industry Resource Links is a guide created by Pearson giving descriptions of, and links to, a variety of external stakeholder materials that are publicly available that you might find helpful in supporting your teaching and delivery of the Security Topic from the Core Component:

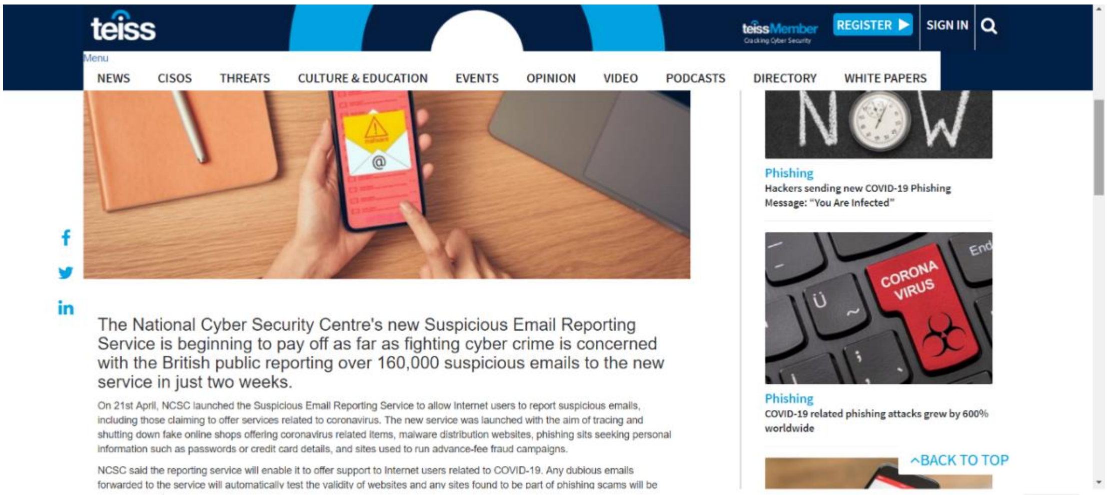
The links aim to show a selection of industries/employers that are high quality examples for the topics within the case study. Enabling your students to gain industry knowledge that is cutting edge and innovative, and supporting you in bringing the topic to life' within a classroom environment.

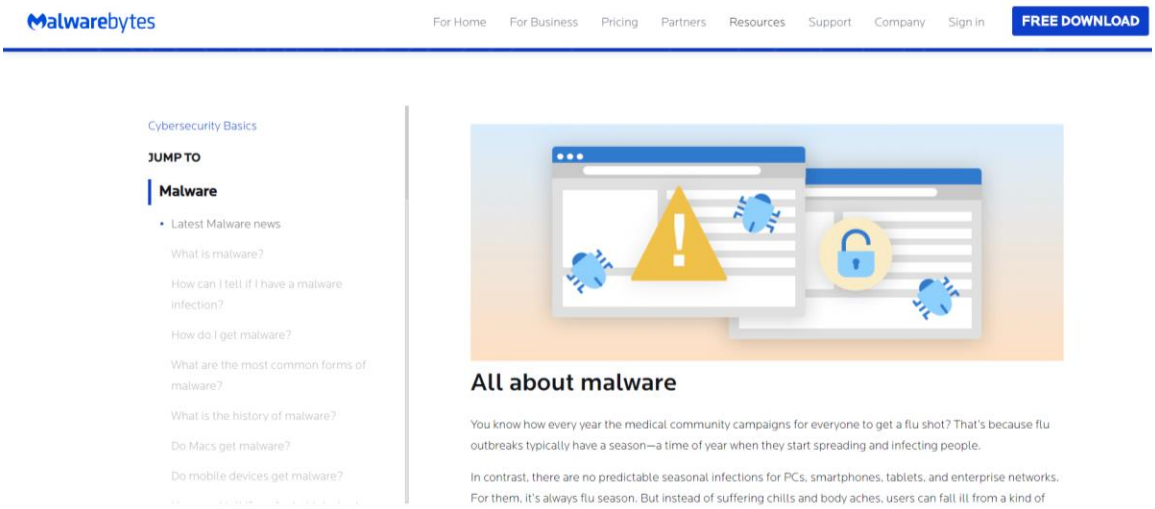
We leave it to you, as a professional educator, to decide if any of these resources are right for you and your students, and how best to use them.

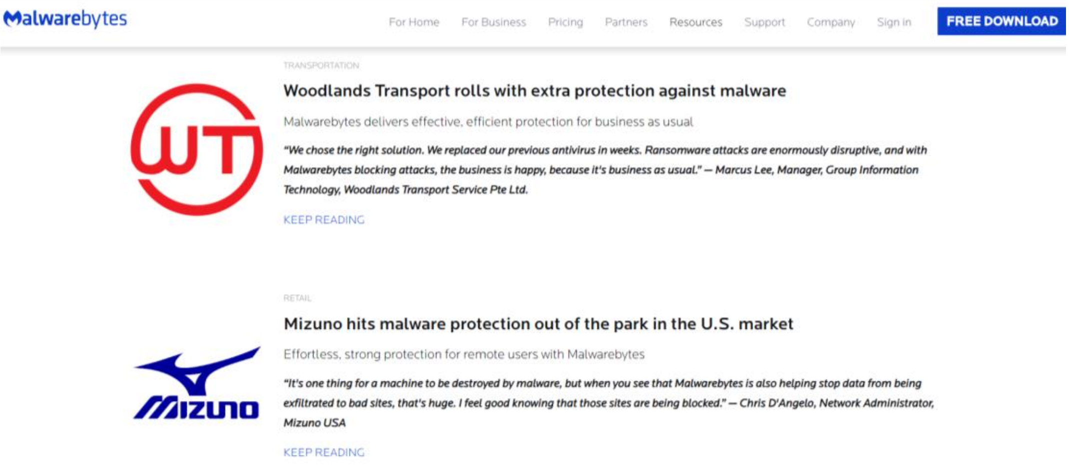
Pearson is not responsible for the content of any external internet sites. It is essential that you to preview each website before using it in class so as to ensure that the URL is still accurate, relevant and appropriate. We'd also suggest that you bookmark useful websites and consider enabling students to access them through the school/college intranet.

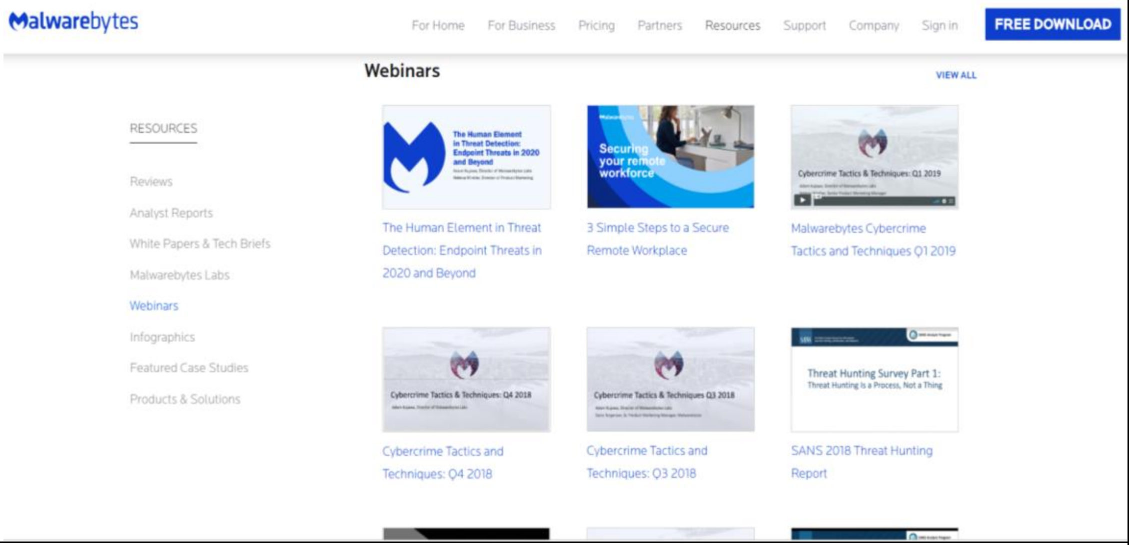
Title:	Cybersecurity Basics
Description	You've probably heard about Ransomware or read about it in the news. Maybe you've got a pop-up on your computer screen right now warning of a ransomware infection. This resource will tell you all about ransomware's different forms, how you get it, where it comes from, and what to do to protect against it.
Supports	8.1.3 Understand potential technical threats and vulnerabilities to systems, data and information
Cost	Free
Format	Website link
Screenshot	 Cybersecurity Basics JUMP TO Ransomware Latest ransomware attacks What is ransomware? How do I get ransomware? Types of ransomware History of ransomware Mac ransomware Mobile ransomware Who do ransomware authors target? What to do if I'm infected How do I protect myself from All about ransomware Ever wondered what all the ransomware fuss is about? You've heard about it at the office or read about it in the news. Maybe you've got a pop-up on your computer screen right now warning of a ransomware infection. Well, if you're curious to learn all there is to know about ransomware, you've come to the right place. We'll tell you about ransomware's different forms, how you get it, where it came from, who it targets, and what to do to protect against it. What is ransomware? Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card. How do I get ransomware? There are several different ways that ransomware can infect your computer. One of the most common methods today is through malicious spam, or malspam, which is unsolicited email that is used to deliver malware. The email might include booby-trapped attachments, such as PDFs or Word documents. It might also contain links to malicious websites.
Link	https://www.malwarebytes.com/ransomware/

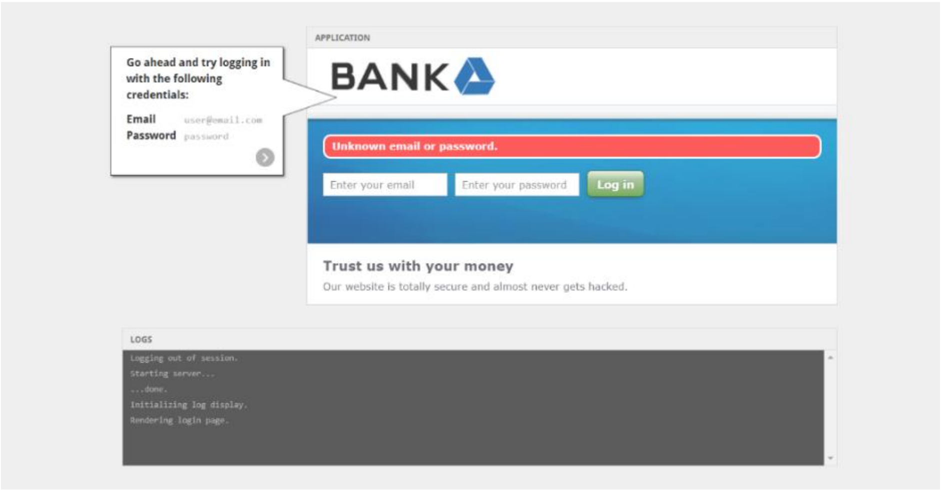
Title:	Teiss
Description	Has wide range of video articles on persistent and current cyber threats organisations face.
Supports	8.1.3 Understand potential technical threats and vulnerabilities to systems, data and information
Cost	Free
Format	web page with a link
Screenshot	 teiss teissMember REGISTER SIGN IN Menu NEWS CISOS THREATS CULTURE & EDUCATION EVENTS OPINION VIDEO PODCASTS DIRECTORY WHITE PAPERS Threats A wide range of articles, videos and interviews concerning persistent and current threats that organisations face. Biometrics| Why is the debate on biometrics and surveillance important now? Third party risk| Advice on managing third party risk during COVID-19 teiss Amsterdam2020 The European Information Security Summit ▶ 7th October 2020 ▶ #teissAmsterdam2020 You May Also Like
Link	https://www.teiss.co.uk/category/threats/

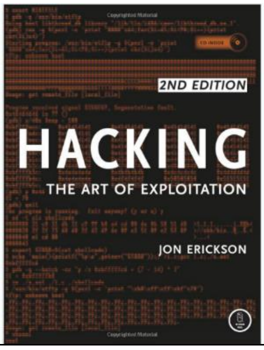
Title:	National Cyber Security Centre
Description	Article on suspicious email reporting service being rolled out in the UK and how it's using the public to fight cybercrime.
Supports	8.1.1 Understand the importance of maintaining privacy and confidentiality of an organisation's information 8.1.3 Understand potential technical threats and vulnerabilities to systems, data and information
Cost	Free
Format	Website Link
Screenshot	 teiss teissMember REGISTER SIGN IN Menu NEWS CISOS THREATS CULTURE & EDUCATION EVENTS OPINION VIDEO PODCASTS DIRECTORY WHITE PAPERS The National Cyber Security Centre's new Suspicious Email Reporting Service is beginning to pay off as far as fighting cyber crime is concerned with the British public reporting over 160,000 suspicious emails to the new service in just two weeks. On 21st April, NCSC launched the Suspicious Email Reporting Service to allow Internet users to report suspicious emails, including those claiming to offer services related to coronavirus. The new service was launched with the aim of tracing and shutting down fake online shops offering coronavirus related items, malware distribution websites, phishing sits seeking personal information such as passwords or credit card details, and sites used to run advance-fee fraud campaigns. NCSC said the reporting service will enable it to offer support to Internet users related to COVID-19. Any dubious emails forwarded to the service will automatically test the validity of websites and any sites found to be part of phishing scams will be Phishing Hackers sending new COVID-19 Phishing Message: "You Are Infected" Phishing COVID-19 related phishing attacks grew by 600% worldwide ^BACK TO TOP
Link	https://www.teiss.co.uk/public-flags-suspicious-emails-ncsc/

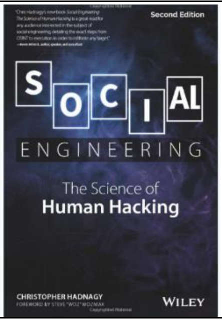
Title:	Malwarebytes
Description	Describes how malware infects your computer.
Supports	8.1.4 Understand potential physical vulnerabilities to systems, data and information
Cost	Free
Format	Web link
Screenshot	 Malwarebytes For Home For Business Pricing Partners Resources Support Company Sign in FREE DOWNLOAD Cybersecurity Basics JUMP TO Malware • Latest Malware news What is malware? How can I tell if I have a malware infection? How do I get malware? What are the most common forms of malware? What is the history of malware? Do Macs get malware? Do mobile devices get malware? All about malware You know how every year the medical community campaigns for everyone to get a flu shot? That's because flu outbreaks typically have a season—a time of year when they start spreading and infecting people. In contrast, there are no predictable seasonal infections for PCs, smartphones, tablets, and enterprise networks. For them, it's always flu season. But instead of suffering chills and body aches, users can fall ill from a kind of
Link	https://www.malwarebytes.com/malware/

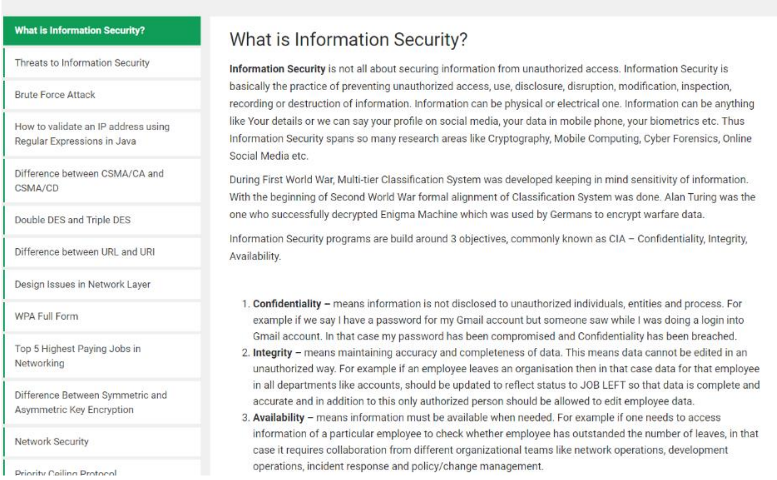
Title:	Malwarebytes
Description	Case Studies of 4 different organisations; Woodlands Transport, Mizuno, Pikes Peak and Spellman on how they implemented safeguarding measures against cyber threats.
Supports	8.1.2 Understand the potential impact on an organisation of failing to maintain privacy and confidentiality
Cost	Free
Format	Web Link then links to PDF Case studies
Screenshot	 Malwarebytes For Home For Business Pricing Partners Resources Support Company Sign in FREE DOWNLOAD TRANSPORTATION Woodlands Transport rolls with extra protection against malware Malwarebytes delivers effective, efficient protection for business as usual *"We chose the right solution. We replaced our previous antivirus in weeks. Ransomware attacks are enormously disruptive, and with Malwarebytes blocking attacks, the business is happy, because it's business as usual." — Marcus Lee, Manager, Group Information Technology, Woodlands Transport Service Pte Ltd.* KEEP READING RETAIL Mizuno hits malware protection out of the park in the U.S. market Effortless, strong protection for remote users with Malwarebytes *"It's one thing for a machine to be destroyed by malware, but when you see that Malwarebytes is also helping stop data from being exfiltrated to bad sites, that's huge. I feel good knowing that those sites are being blocked." — Chris D'Angelo, Network Administrator, Mizuno USA* KEEP READING
Link	https://resources.malwarebytes.com/casestudies/

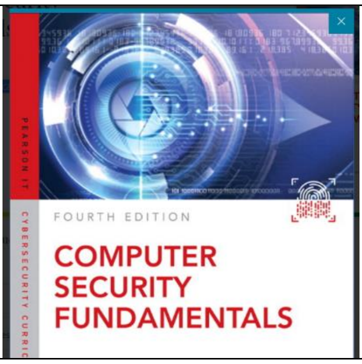
Title:	Malwarebytes
Description	A vast collection of resources including analyst reports, webinars and infographics on cybercrime, threats and malware products and solutions.
Supports	8.2.2 Understand the interrelationship between security, identity, confidentiality, integrity, availability, threat, vulnerability and risk management within a business context
Cost	Free
Format	Webinars
Screenshot	 Malwarebytes For Home For Business Pricing Partners Resources Support Company Sign in FREE DOWNLOAD VIEW ALL RESOURCES Reviews Analyst Reports White Papers & Tech Briefs Malwarebytes Labs Webinars Infographics Featured Case Studies Products & Solutions Webinars The Human Element in Threat Detection: Endpoint Threats in 2020 and Beyond 3 Simple Steps to a Secure Remote Workplace Malwarebytes Cybercrime Tactics and Techniques Q1 2019 Cybercrime Tactics and Techniques: Q4 2018 Cybercrime Tactics and Techniques: Q3 2018 SANS 2018 Threat Hunting Report
Link	https://resources.malwarebytes.com/#analyst-reports

Title:	SQL Injection demo
Description	Useful website that demonstrates how SQL injection works. The website is interactive and illustrates some of the basic concepts.
Supports	8.1.3 Understand potential technical threats and vulnerabilities to systems, data and information
Cost	Free
Format	Web link
Screenshot	 Go ahead and try logging in with the following credentials: Email user@email.com Password password Unknown email or password. Trust us with your money Our website is totally secure and almost never gets hacked. Logging out of session. Starting server... ...done. Initializing log display. Rendering login page.
Link	www.hacksplaining.com/exercises/sql-injection

Title:	Hacking: The Art of Exploitation (2nd Ed.) by Jon Erickson
Description	Look into the world of creative problem solving and exploitation. Rather than simply walking through how different exploits work, this book provides a holistic view of programming, network communications, and current hacking techniques.
Supports	8.1.4 Understand potential physical vulnerabilities to systems, data and information 8.2.2 Understand the interrelationship between security, identity, confidentiality, integrity, availability, threat, vulnerability and risk management within a business context
Cost	£23.29 (Kindle) / £31.56 (Paperback)
Format	Ebook or paperback
Screenshot	 2ND EDITION HACKING THE ART OF EXPLOITATION JON ERICKSON
Link	https://www.amazon.co.uk/Hacking-Art-Exploitation-Jon-Erickson/dp/1593271441

Title:	Social Engineering: The Science of Human Hacking.
Description	Looks at how cases both the creative genius and laziness of hackers. Why go through all the rigmarole and effort of breaking and climbing through a virtual window when you can walk through an open front door? This book looks at the vulnerabilities that exist within the human elements of a business and breaks down how you can recognize, anticipate, and prevent social engineering attacks.
Supports	8.1.4 Understand potential physical vulnerabilities to systems, data and information 8.2.3 Understand processes and procedures to mitigate threats and ensure security
Cost	£16.72 (Kindle) / £17.60 (Paperback)
Format	EBook or Paperback
Screenshot	 Second Edition SOCIAL ENGINEERING The Science of Human Hacking CHRISTOPHER HADNAGY WILEY
Link	https://www.amazon.co.uk/Social-Engineering-Science-Human-Hacking/dp/111943338X/

Title:	Geekforgeeks
Description	What is information security
Supports	8.1.5 Understand potential human threats and vulnerabilities to systems, data and information
Cost	Free
Format	Web link
Screenshot	 What is Information Security? Threats to Information Security Brute Force Attack How to validate an IP address using Regular Expressions in Java Difference between CSMA/CA and CSMA/CD Double DES and Triple DES Difference between URL and URI Design Issues in Network Layer WPA Full Form Top 5 Highest Paying Jobs in Networking Difference Between Symmetric and Asymmetric Key Encryption Network Security Priority Ceiling Protocol What is Information Security? **Information Security** is not all about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electrical one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc. During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of information. With the beginning of Second World War formal alignment of Classification System was done. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data. Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability. 1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached. 2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data. 3. **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.
Link	https://www.geeksforgeeks.org/threats-to-information-security/

Title:	Computer Security Fundamentals, 4th Edition
Description	Drawing on 20+ years of experience as a security instructor, consultant, and researcher, Easttom helps students take a proactive, realistic approach to assessing threats and implementing countermeasures
Supports	8.1.4 Understand potential physical vulnerabilities to systems, data and information 8.1.5 Understand potential human threats and vulnerabilities to systems, data and information 8.2.3 Understand processes and procedures to mitigate threats and ensure security
Cost	£30.62 (Kindle) / £34.20 (Paperback)
Format	Book
Screenshot	 PEARSON IT CYBERSECURITY CURRIC FOURTH EDITION COMPUTER SECURITY FUNDAMENTALS
Link	https://www.amazon.co.uk/Computer-Security-Fundamentals-Cybersecurity-Curriculum/dp/0135774772/