**Question 1**

Internal hacking takes place when a person or a group of people within an organization aims at accessing the computer systems without authority with the intention of exploiting organizational asserts or disrupting operations (Weiss & Solomon, 2016). Most of the internal hacking cases involve the hacker employing various skills, tools, and resources to launch a complex computer attack against their organization and potentially get rid of any evidence that could create awareness of the attack or its origin. Disgruntled, highly skilled employees including programmers and administrators, or technical users that could potentially benefit from the disruption of organizational operations may decide to start an internal hack against an organization via its computer systems (Weiss & Solomon, 2016). Organizations put in place different measures to protect themselves from internal attacks, including implementation of intrusion detection systems that would screen both internal and external hacking attempts. In addition, organizations log all forms of attacks and review the logs regularly (Weiss & Solomon, 2016).

One of the laws in the United Kingdom that are directed at addressing cybercrimes, including internal hacking, is the Computer Misuse Act 1990. This refers to a United Kingdom’s Act of Parliament that was partly introduced to respond to the decision made by the court in R v Gold & Schifreen (1988) (Fafinski, 2014). The Act has formed a model that has been emulated by other countries such as the Republic of Ireland and Canada in the development of their cyber security laws. The law presents three criminal offenses including “unauthorized access to computer material, unauthorized access with intent to commit or facilitate commission of further offenses, and unauthorized modification of computer material,” all of which hold different sentences (Fafinski, 2014). When it comes to the issue of internal hacking, section 1 of the CMA significantly applies.

With regards to the crime of unauthorized access to computer material, internal hackers are liable as they use a computer, including their computer or the company’s computer, to carry out a function that is aimed at securing access (Fafinski, 2014). This does not include the individual merely coming into physical contact with the computer. The law does not cover events in which an accused person engaged in 'computer eavesdropping', reading data on display or any other confidential data that is readily accessible on the computer. To prove that an offender violated this law, the plaintiff must show knowledge that any attempted access was unauthorized and that the attacker intended to access to data or programs on the organization’s computer (Fafinski, 2014). As such, mere reckless may not be sufficient to demonstrate an employee’s surpassing of his or her authority in accessing organizational computers with the intention of using certain programs or data safeguarded on them.

The case of DPP v Bignell [1998] is was highly criticized alongside the Computer Misuse Act 1990 due to the decision that was reached by the House of Lords. The case involved two police officers who made a request to the police national computer (PNC) for information that was to be used for their personal use, without the knowledge of the operator (DPP v Bignell, 1998). The police officers only had authorization to request such information for the purposes of policing only and did not inform the PNC operator that the information that they were requesting for was to be used for personal engagements. According to the decision of the Divisional Court, the two officers were within their limits ad had not committed an offense under Section 1 of the Computer Misuse Act (DPP v Bignell, 1998). This decision was affirmed by the House of Lords, with the Court stating that the officers’ role was merely to make a request to the operator to obtain information using a computer. The one involved in retrieving the information, the PNC operator, was within his authority to obtain such information. The operator was authorized to access the computer and the data on it in response to requests made through the correct channels by police officers (DPP v Bignell, 1998).

The decision by the House of Lords attracted significant criticism concerning the Act’s effectiveness in catching specific inside hackers. Generally, it is argued that the issue of authorization refers to both the ‘area of conduct’ as well as the conduct itself (Fafinski, 2014). However, in Bignell, the Court’s decision brought up questions concerning the extent and true nature of authority that the conduct of a defendant has. The case left unanswered what it means by making an ‘unauthorized’ access by insider hackers, who are required or permitted to access organizational computers for certain purposes. According to Section 17(5) of the Computer Misuse Act, if an accused person did not have an entitlement to gain access for the purposes in question and was not provided with consent with regard to the same then the access is unauthorized (Fafinski, 2014). Nevertheless, the deficiencies in the scope of this provision when the users hold some access rights were revealed in DPP v Bignell. As much as the police officers were authorized to request information that was to be used for policing purposes, they were not authorized to request information that was to be used for personal purposes. Thus, they violated the CMA as they surpassed their authority in causing another to access and pass on information to them for the wrong purposes.

**Question 2**

Ordinary shares, as the ones held by Orion plc., form the most common type of share that is issued to shareholders. Generally, these shares are considered as equity investments (Murray, 2016). They are suitable in cases where the shareholder seeks to exert a level of control over the organization through voting, to partake of earnings through dividends, and to contribute through the growth of the company through capital investments. On the other hand, preference shares include shares with which the shareholder does not have a right to exercise control over the company through voting and cannot take part in any earnings beyond a predetermined amount of dividend distribution, winding up, or redemption (Murray, 2016). These preference shares can present both debt and equity characteristics, informed by investments from different individuals having distinct interests and priorities to safeguard (Murray, 2016).

As Orion seeks to issue preference shares on top of the currently issues, it is important to understand the class rights that come with the new shares, as well as those that will be altered by the change. Prior to understanding the rights, it critical to acknowledge the requirements and objectives that may push investors towards acquiring or shifting to preference shares. Preference shares are commonly issued to parties that do not require or need voting rights and general participation in the management of a company (Murray, 2016). As such, unlike ordinary shares that provide the shareholder with the right to vote on issues concerning the organization, preference rights alienate the shareholder from the running of the organization, leaving them out as spectator beneficiaries. Moreover, this type of shares is issued to parties that seek medium risk and returns (Murray, 2016). In comparison to ordinary shareholders, those with preference shares are prioritized when it comes to receiving dividends. As such, in cases where the company experiences losses, the preference shareholders are the first to receive their fixed dividends, while ordinary shareholders are exposed to the full impact of the loss. Last but not least, preference shares are issues to parties that prefer equity investment exposure and a hybrid debt (Murray, 2016).

The law provides that preference shares rights ought to be expressly included in the articles or memorandum (Murray, 2016). Thus, preference shareholders are only entitled to the rights that are included in the articles or memorandum and no other rights. Any preference shares cannot be issued without indicating the rights of the shareholders in the articles or memorandum with respect to voting, non-cumulative and cumulative dividends, participation in profits and surplus assets, repayment of capital, and priority of payment of dividend and capital in relation to other shares (Murray, 2016). An important element of preference shares involves voting rights. The company’s articles are required to provide voting rights or indicate that preference shareholders do not hold voting rights. Preference shareholders are generally not issued with voting rights (Murray, 2016). However, they hold preferential rights with regards to their entitlement to dividends and hold the priority of being the first to receive payments in comparison to ordinary shareholders. Despite the fact that preference shareholders may not be provided with voting rights, they have the statutory right to vote under three circumstances, including on any resolution concerning the winding up of the company, on any decisions concerning the rights that are associated with such shares, and in cases where the preferential dividend goes unpaid for a period not exceeding twelve months from the due date or as it may be indicated within the articles (Murray, 2016).

Given the secure position in which preference shareholders are, they have no right to engage in voting in view of influencing the activities of the organization. Such a right is reserved for the ordinary shareholders (Murray, 2016). With an exception of the prementioned situations in which such holders are required to vote, preference shareholders can also gain voting rights by converting their shares into ordinary shares. The lack of voting rights prevents preference shareholders from directly influencing the distribution of authority among agents of the organization (Murray, 2016). While preference shareholders can be appointed as directors of their companies, most of them stay away from the organization and only take part in decisions that involve their dividends. The ordinary shareholders hold the exclusive rights of voting on important matters, including the appointment of organizational agents to represent the interests of shareholders (Murray, 2016). The directors of the organization receive express authority from the shareholders to represent them in strategizing and implementing the goals of the organization at managerial levels. Having a control over decisions such as the selection of directors and voting on other issues concerning the running of the organization places ordinary shareholders at an advantageous position of authority (Murray, 2016). Preference shareholders, on the other hand, have limited authority within the organization, especially when it comes to influencing decision making.

**References**

DPP v Bignell, 1 Cr App R8 (The House of Lords 1998).

Fafinski, S. (2014). Computer Misuse: Response, Regulation and the Law. New York: Routledge.

Murray, A. (2016). Information Technology Law: The Law and Society. Oxford: Oxford University Press.

Weiss, M., & Solomon, M. G. (2016). Auditing IT Infrastructures for Compliance. Burlington, MA: Jones & Bartlett Learning.