A K M Mominul Hasan
moon95e@yahoo.co.uk

MODULE 8 UNIT 2 Ongoing Project: Develop a cyber risk mitigation strategy

HARX CYB Module 8 Unit 2 Ongoing project

Learning outcome:

LO5: Develop a cyber risk mitigation strategy specific to your organization.

Name:

1. Instructions and guidelines (Read carefully)

Instructions

1. Insert your name and surname in the space provided above, as well as in the **file name.** Save the file as: **First name Surname M8 U2 Ongoing project** – **e.g. Zadie Smith M8 U2 Ongoing project**. **NB:** *Please ensure that you use the name that appears in your student profile on the Online Campus.*

2. Write all your answers in this document. There is an instruction that says, "Start writing here" under each question. Please type your answer there.

3. Submit your assignment in **Microsoft Word only**. No other file types will be accepted.

4. Do **not delete the plagiarism declaration** or the **assignment instructions and guidelines**. They must remain in your assignment when you submit.

PLEASE NOTE: Plagiarism cases will be investigated in line with the Terms and Conditions for Students.

IMPORTANT NOTICE: Please ensure that you have checked your course calendar for the due date for this assignment.

Guidelines

1. Make sure that you have carefully read and fully understood the questions before answering them. Answer the questions fully but concisely and as directly as possible. Follow all specific instructions for individual questions (e. g. "list", "in point form").

2. Answer all questions in your own words. Do not copy any text from the notes, readings or other sources. **The assignment must be your own work only.**

Plagiarism declaration
1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own. **2. This assignment is my own work.** **3. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as their own work.** **4. I acknowledge that copying someone else's assignment (or part of it) is wrong and declare that my assignments are my own work.**

2. Brief

This module focused on the importance of risk mitigation and the value companies can derive from implementing a risk mitigation strategy to improve organizational resilience and manage risks effectively. This assignment requires you to complete a cyber risk mitigation strategy for your organization.

As the notes made clear, a risk mitigation strategy helps an organization prioritize its risks so it can allocate resources efficiently. This final submission is an opportunity for you to reflect and condense all the knowledge you have gained over the duration of the course by incorporating feedback from your previous ongoing project submissions into a consolidated cyber risk mitigation strategy.

If you are completing your ongoing project on Sony, you are required to create a risk mitigation strategy that the organization should have followed in light of the 2014 hack.

Note:

All ongoing project submissions throughout the course need to focus on the same organization. Or, if you choose to focus on the case study of Sony, you will need to complete all your submissions on Sony.

It is highly recommended that you avoid disclosing any confidential information in your assignments. Although you are encouraged to draw on real-world experience during the course, you are urged to use pseudonyms (false names) and alter any sensitive details or data where necessary. You are responsible for ensuring that you do not disclose any information that is protected by confidentiality undertakings; all information is treated in accordance with our privacy policy.

Please read Section 4 of the Honor Code in the Orientation Module course handbook for more guidance.

Note:

- The published word count in each assignment is for satisfactory work – it is the amount of detail, analysis and nuance needed for a satisfactory score according to the rubric. If you exceed the published word count, you will not be penalized. The extra work can improve your grade – up to and including an exceptional score. Your grade is not dependent on the number of words you write. The word count is simply a benchmark for an average level of detail, analysis and nuance, and additional detail and nuance is needed to surpass a Satisfactory grade.

- You must not only include overall organizational context, but per-question context as well. This context allows the reader to understand what the organization does and which sector it is part of, as well as why each question is important to the organization.

3. Risk mitigation strategy

Introduction

Write a brief paragraph in which you provide a high-level overview of your organization's need for a risk mitigation strategy.

(Write approximately 150 words)

Start writing here:

As I have mentioned in my earlier Modules that my organization is the 13 Royal Signal Regiment in the British Army, it is only the Cyber Regiment within the British Armed Forces; this is very large and complex, and our Information Structure is bigger than any other IT organization in the UK.

In my organization, the most critical assets are our Data and Information, which includes official, official-sensitive, secret, and top-secret. Alongside this, all Military research, HR information, internal software development process, and classified agenda.

Without data, we (Army Cyber Regiment) can not carry out our daily cyber and military activities, on-going, and future mission. Everyone is responsible for using data and it has to follow the General Data Protection Regulation (GDPR), i.e. use fairly, lawfully, transparently, used for specified.

To share our resources and electronic communications, my organization using Local Area Network (LAN) and Wide Area Network (WAN), Military Classified Network (encrypted). However, my organization uses Military internet activities most of the time, and which is why the ISP (Internet Service Provider) relates to the Military internet and filters its connection layers to receive and send any data over the Military internet.

In order to maintain those, which I have mentioned above, we have some leadership roles like other non-military organizations in order to implement its Cybersecurity governance and carry out our daily business to keep fit British Army's Cybersecurity; similarly, we have our leaders who are responsible for this organization's Risk Mitigation Strategy.

Vision

Outline your organization's vision of what implementing a risk mitigation strategy will ideally achieve.

(Write approximately 150 words)

Start writing here:

We all know that Risk mitigation implementation is the process of executing risk mitigation actions within the organization. Similarly, we can follow a few strategies to avoid risk, i.e. Assume and accept risk, avoidance of risk, or transference of risk.

However, we have some leadership roles and they have some organizational vision like other non-military organizations in order to implement its Cybersecurity governance and carry out our daily business to keep fit British Army's Cybersecurity.

A Brigadier (1 star General) is the Chief Information Security Officer (CISO) and he is leading the Cyber regiment, as a whole. Additionally, our Officer in Command (OC) in the Cyber regiment is the Chief Information Officer (CIO) and the Second in Command (2IC) is Chief Security Officer (CSO) for our Cyber regiment. They are setting in the main roles in our Military Cyber Organization, and they are responsible for the governance and its implementation in order to achieve an ideal risk mitigation strategy for our Military Cyber organization.

Alongside this, the National Cyber Security Centre (NCSC), Government Communication Headquarters (GCHQ), Secret Intelligence Service (SIS), or MI6 are working together and sharing the governance which approved by the British Parliament, which is called "The UK Cyber Security Strategy Protecting and Promoting the UK in a digital world". All organizations, including my organization implementing its Annex A. It has four objectives, please see below:

a)Tackling cyber-crime and making the UK one of the most secure places in the world to do business.

b)Making the UK more resilient to cyber-attack and better able to protect our interests in cyberspace.

c)Helping to shape an open, vibrant, and stable cyberspace which the UK public can use safely and that supports open societies.

d)Building the UK's cross-cutting knowledge, skills, and capability to underpin all cybersecurity objectives.

[This paragraph idea and quote has taken from "The UK Cyber Security Strategy", which my organization (13 Royal Signal Regiment) implementing, and my own evaluation, (2021). Retrieved 9 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609611/uk-cyber-security-strategy-final.pdf]

Moreover, we are very careful that how our organizations can control, direct, and communicate our cyber security risk management activities. To do that all the leadership roles in my organization effectively coordinate the security activities of my organization; it enables the flow of security methodology and decision within my organization. However, we all are responsible for its implementation and decision-making at all levels in my organization.

Furthermore, my organization is one of the technical (Cyber) regiments in the British Army; therefore, my organization has to follow the Army Doctrine for its Land Operation and as well as Land Cyber Programme which was approved by the British Government. In my organization, all leadership roles follow the management processes when developing a cybersecurity governance plan.

Additionally, this Land Cyber program's aim is to cross-examine people with cyber and electromagnetic technology to exploit the opportunity and obtain a military advantage; also, this Cyber program stated as its priority "To offer electronic and cyber protection to operate in a hostile cyber and electromagnetic domain. To deepen our understanding, using enhanced electronic sensors and survey tools and by better contributing to the collection and exploitation of national intelligence." Therefore, our leadership roles in my organization are very keen to utilize its cybersecurity governance in order to uphold the distinct management process.

[The quote in this paragraph has taken from the Land Cyber Programme in order to evaluate my explanation, Land Cyber Programme. (2021). Retrieved 9 August 2021, from https://www.gov.uk/guidance/land-cyber-programme#programme-benefits]

As a Military Cyber organization, our leaders implement cyber security governance to helping my organization to control and communicate our cyber security risk management activities. However, for the governance and business objectives, general approaches for cyber security and risk management for my organization sometimes create confusion; predetermined security risk management plans, business process ideas, roles, and responsibilities are sometimes separated from the decision-making process for our daily business. This separation sometimes can lead to delay and misinterpretation in our cybersecurity decision-making process.

Therefore, our leadership roles prioritize the job or are committed to establish and implement cyber security governance plans to make effective risk mitigation strategies, which can fit in our daily business, and it can lead a good control and a good level of cyber security. By implementing Cyber security governance sufficiently, our leaders can achieve effective risk mitigation strategies, and they (leaders) can mitigate the cyber risk in order to secure Army's valuable assets and information from the hackers.

Strategic goals and objectives

List at least four strategic goals your organization must achieve to reduce its risks to an acceptable level. List at least two objectives under each strategic goal that explain what must be done to achieve the strategic goal.

Note: A thorough risk mitigation strategy should include associated action plans and milestones, but you are not required to detail these for the purposes of this submission.

(Write approximately 450 words)

Start writing here:

Nowadays, as the character of electronic warfare evolves, and the weapons used to fight those wars shift from the lethal weapon to the information age, digital and cyber capabilities are rapidly being used to ensure the nation's security and the safety of our Military Personnel in the country and overseas, and therefore, our organization has been set up some strategic goals and objective in order to reduce the risk.

I can say unequivocally, that my organization is more vulnerable than any other organization in the country because we are not only responsible for our tri-service (British Army, Royal Air Force, and Royal Navy) Cyberdefense but also, are responsible for Information Management (IM) for the Ministry of Defence (MoD), General Data Protection Regulation (GDPR) for the UK, and we have to maintain the Data Protection Act 2018 from the legal framework for protecting personal data and official data, which includes sensitive, official-sensitive, secret, and top-secret/ classified.

As I explained above, we are committed to protecting Defence information, knowledge, digital data, and therefore, we are a more vulnerable and potential target to threat actors. We selected Oracle Cloud Infrastructure (OCI) for improved agility and speed of its digital transformation, and Linux Operating system for our other defense activities but still, we are always under threat, and we experience at least 60 plus Cyber-attack every single day. Our National Cyber Security Centre (NCSC) and Government Communication Head Quarter

(GCHQ) are supporting us to design and implement secure cyberspace and to keep stability as a national Cyber force in order to protect the UK.

[This paragraph idea was taken from the Ministry of Defence IM management, and MoD reports, and my own explanation, reference given below.]

As a Military Cyber organization, to design and implement secure cyberspace, some firm strategies we have been put in place, i.e. creating a secure Ecosystem, creating an assurance Framework, implementing a Regulatory Framework, E-Governance service, and protecting our complex Information Structure (can not describe details due to the security purpose).

To protect our complex Information structure, my organization is very focused on the organization's cyber security awareness. To do this, my organization liaise with the National Cyber Security Centre (NSCS), and the Government Communication Headquarters (GCHQ) of the UK; additionally, the Defence Cyber School located at the Defence Academy of the United Kingdom conduct various types of cyber security awareness training to the Military Personnel in my organization.

Moreover, to achieve its goals and objective, and also, to make cyber security risk management effective, and governance implementation upfront, it is important to establish regular cyber security awareness training within my organization; therefore, all leaders in my organization establish clear lines of communication between those that are responsible and accountable for cyber security training.

In my organization, by conducting regular cyber awareness training, we develop and practice an effective culture and environment for our Cybersecurity and Cyber risk mitigation. Effective security culture and environment sometimes help to deal with complex Cyber incidents easily, as well as reduces the cyber risk management uncertainty. This security culture can be encouraging by ensuring that all Service Personnel in my organization understand the objectives and maintaining the priority of the business is most important within the organization, employing and appointing personnel who have Cybersecurity knowledge, risk management skills, and expertise. By doing all these, Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Security Officer (CSO) make sure that they can trust their employee and they can empower those people to implement the organization's governance, framework, and able to achieve strategic goals to reduce its risks to an acceptable level.

Metrics

List at least three metrics your organization will use to analyze the achievement of its goals/objectives. These metrics should be specific to the goals/objectives listed in the previous question.

(Write approximately 150 words)

Start writing here:

As I have mentioned above that my organization, by conducting regular cyber awareness training, develops and practices an effective culture and environment for our Cybersecurity and Cyber risk mitigation. In our Cyber risk mitigation strategy, we have included a few metrics for our organization to achieve its goals and objectives, i.e detect intrusion attempts, vulnerability patch response times, number of users broken out by application or data access levels.

Additionally, my organization always follows the British Army Doctrine *(one of the matrices and it is the Military classified strategy),* and the Doctrine introduced us to the Military Annual Training Test (MATTs), which is what we have to do every year before it expires, as a Cyber regiment we have to complete Cyber security awareness training via Defence Cyberschool. The Defence Academy conducts Cybersecurity awareness training and a full course every three months in a classroom consists of 30 – 40 students in the Defence Academy of the UK. This course is generally for my organization, which is Army's Cyber regiment, but sometimes, it allows a number of selected students from different security roles across the British Army, Royal Air Force, and Royal Navy.

By doing this Cyber course; and also, Military Annual Training Test (MATT), allows the leaders of my organization to measure the achievement of its Cyber strategic goals and objectives. Alongside this, Military Annual Training Test (MATT) allows the Service Personnel to perform their Cyber roles and give the ability with confidence to implement an effective Cybersecurity governance plan, Framework, E-Governance service, and protecting our complex Information Structure.

Note:

Include refined versions of your previous submissions in the sections below. Where relevant, incorporate any feedback from your Tutor, as well as additional knowledge gained during the course to improve on your previous submissions.

Threat actors and methods of attack

Integrate your submission from Module 2, in which you identified at least two threat actors to your organization, and described methods of attack these actors could use.

If you are using the Sony case, integrate the submission in which you identified the threat actor Sony faced in the 2014 hack and their method of attack, as well as at least one other threat actor Sony could face in the future and what method of attack they might use.

(Write approximately 550 words)

Start writing here:

As I have mentioned above, because of the nature of my organization, threat actors use common and sophisticated techniques in order to accomplish their mission; they use any suitable method for their attacks.

Because my organization is the Defence Cyber organization, therefore, Nation-State/ Advanced Persistent Threats (APTs), Cyber Criminals, Terrorists/ Hacktivists I consider to be the main threats against the individual of my organization, as well as the whole Ministry of Defence, and the UK.

Whilst our defence (my organization as well) and the UK is potentially under threat from many nations across the world, all the time, there are four main nation-states that are assessed as presenting the main threat to us. These are Russian, which is assessed as the most capable and greatest threat; China, North Korea, and Iran.

I am describing their motivations, the kind of tools and techniques they could use, please see below:

As I mentioned above, those threat actors are thought to be extremely capable, and they are continually active in the Cyber domain. Open-source reports suggest that there are a number of organizations state-sponsored that carry out operations in the Cybersphere against the UK and other nations. They have access to vast resources in order to carry out Cyber activity against the UK and other nations, i.e. it is suspect that Russia Cyber activities took place run-up to the 2016 US presidential election, the Sony Entertainment attack in 2014 and the NHS attack in 2017 by North Korea, Saudi Arabia oil company (Saudi Aramco) attack in 2012 by Iran.

Alongside this, Cybercriminals, and Terrorists/ Hacktivists use different methods and techniques in order to carry out their cyber-attacks, i.e. as per a US Department of Justice report, at least one Chinese national was successfully prosecuted for stealing plan for the F-35 Lightning II aircraft.

[This paragraph idea was taken from the Defence Gateway, Defence Learning Environment (DLE) and my own explanation, reference given below.]

Another technique they use is the phishing attack, most internet users in my organization with an email account may have come across Phishing emails, which at first, they may have suspected was a legitimate email from a company, friend, or family member. This attack uses many tactics and as people get savvier, the enemy (threat actors) get more creative. Threat actors trick someone into giving information by emailing but in reality that would allow someone else to take data or money out from them. This type of attack is very potential to my organization and could be compromised data.

Man In The Middle Attack (MITM) is another one, which can do great damage to my organization. These attacks come in a variety of forms, A MITM attack may simply refer to phishing, with threat actors in the middle of a transition between any employee of my organization and bank, or malicious actor in the middle of a sharing official-sensitive data between my organization and any Government body. The main aim of this attack is that they (threat actors) don't want to appear suspicious but want to attack our network structure.
If I explain about an Advanced Persistent Threat (APTs) is another method where a continual, sophisticated, and hidden hack takes place over a long period of time and remaining undetected, they can establish a backdoor process in order to continual access to the system. It does require a great deal of effort to plan, execute and maintain. It targeted high-value targets but not always nation-state. That is why there four countries and ATPs are assessed as providing the main threat to the UK and my organization.

Moreover, there are two kinds of Cyber-crime, those crimes that cyber facilitates, such as theft as a result of information gained from a phishing email, and Cybercrime itself, i.e. theft of data, identity, or money directly using Cyber power/ capability (Ransomware, Payment fraud). Sometimes this covers a great deal of non-technical criminal activities, i.e. Social Engineering. That is why Cybercriminal is one of the great threats to my organization.

In addition to this, Terrorist/ Hacktivists is another threat to my organization. Terrorists/ Hacktivists conduct serious violence against a person or damage to property, and their actions are designed to seriously interfere with or seriously disrupt an electronic system. They are creating a serious risk to the health and safety of the public of the UK and to my organization.

A Hacktivist, according to the Oxford English Dictionary, is: "A person who gain unauthorized access to computer files or networks in order to further social or political ends".

[This quotation is taken from Oxford English Spanish Dictionary in order to reinvigorate this assignment, HACKTIVIST | Definition of HACKTIVIST by Oxford Dictionary on Lexico.com also the meaning of HACKTIVIST. (2021). Retrieved 26 July 2021, from https://www.lexico.com/definition/hacktivist]

Terrorist/ Hacktivists are facilitated by hacker skills, as well as an often very-keen sense of how to use the internet to deliver their key message; they exploit social media to further their cause and often use the internet to release the information which is normally damaging their target, and that is why, as a cyber organization we are a potential target to them.

The main threat vector for my organization is Distributed Denial of Service attack (DDoS). This type of attack takes advantage of the specific capacity limits that apply to any medium and large network structure like my organization. The DDoS attack basically takes control of several hundred, several thousand machines and the attacker/ threat actor acts like a Cyber God and then he targets any network architecture or infrastructure like my

organization. Subsequently, he (threat actor) sends an extremely large number of requests to the victim resource, the threat actor then establishes a "zombie network" of computers that the threat actor has infected earlier. He (threat actor) has control of this big, infected network; therefore, he would be able to attack and infect our network by sending a huge scale of the attack, which can be overwhelming for my organization's web resources. That is why this attack is a very potential risk for our whole Information Structure.

Business critical assets

Integrate your submission from Module 3, in which you identified the assets that are most essential to your organization or Sony's ability to accomplish its mission. Describe what vulnerabilities there may be in the organization's systems, networks, and data that may put these assets at risk.

(Write approximately 550 words)

Start writing here:

In my organization the most critical assets are our Data and information, it's included official, official-sensitive, secret, and top-secret. Alongside this, all Military research, HR information, internal software development process, and classified agenda.

As we all know that Data are plain fact, but we have to maintain the Data Protection Act 2018 because it is the UK's implementation of the General Data Protection Regulation (GDPR).

"Data is our ammunition," said Major General Jonathan Cole, CIO and director of information at the British Army.

[speaking at New Statesman Media Group's CIO Town Hall Live forum in July 2020. TECHMONITOR. (2020, October 7). Https://Techmonitor.Ai/Tech-Leaders/Data-Cyber-Iot-British-Army. https://techmonitor.ai/tech-leaders/data-cyber-iot-british-army]

Without data, we (Army Cyber organization) can not carry out our daily cyber and military activities, on-going and future mission. Everyone is responsible for using data and it has to follow the GDPR as mentioned above, i.e. use fairly, lawfully, transparently, used for specified.

To share our resources and electronic communications, my organization using Local Area Network (LAN) and Wide Area Network (WAN). However, my organization uses Military internet activities most of the time, and which is why, the ISP (Internet Service Provider) relates to the Military internet, and it filters its connection layers to receive and send any data over the Military internet.

A LAN (Local Area Network) is consisting of a relatively small area, i.e. in our Camp, Garrison, Company HQ (headquarter). Alongside this, a WAN (Wide Area Network) is connected in larger geographic areas, i.e. London, the UK, Iraq, and Afghanistan. It is connected to transoceanic cabling or with a Military satellite in order to carry out our daily job, i.e Lockheed Martin satellite.

Data and Information are the most important part of my organization's information structure. Without these, we can not carry out our daily business and as well as the future mission to protect the UK from outside enemies. In general, data look useless but when these data are interpreted and processed; they become a very useful asset and we called it information, i.e. Covet plan for an operation against terrorist and terrorism activities, images, numbers, and sound.

[Those ideas on above have been taken from the British Army website. IMA (Information Management Assurance) and my own organization, which is the 13 Royal Signal Regiment and my own evaluation, references given below:]

Alongside this, my organization work on the Ministry of Defence Information Strategy (MODIS), which received a high-level endorsement and was scheduled for regular review, and we are also responsible for Ministry of Defence (MoD) Information Management (IM), which is another valuable subject for us as a Military Cyber organization.

Its executive summary stated "The Ministry of Defence (MOD) is a policy-making Department of State and the highest-level military headquarters in the UK, providing political control of all military operations. The Department has an annual budget of around £35 billion and employs approximately 280,000 military and civilian personnel."

[*Information Management Assessment Ministry of Defence March 2009, EXECUTIVE SUMMARY - Information Management Assessment. (2009). Https://Www.Nationalarchives.Gov.Uk/Documents/Mod-Ima-Report-Final.Pdf. https://www.nationalarchives.gov.uk/documents/mod-ima-report-final.pdf]*

Therefore, we as a Military Cyber organization always follow its methodology, Framework, and Risk Mitigation Strategies to protect our data and information.

As I mentioned above, data looks very plain and it's the raw material, which can be processed by any computing machine to be meaningful to the person who will receive it. It could be numbers, images, sound and also, it could be official, official-sensitive, secret and classified.

However, without our network structure (LAN, WAN) we couldn't be able to share our data, information, and all other resources.

Those data, information, and network structure in my organization are always potential targets to terrorists, hackers, and nation-state-sponsored cyber-attackers. They (hackers) are always ready to steal our data that has been

converted into a more useful or intelligible form; they steal numbers and words which can be stored in the computer's language.

Those attackers try to hack our system to steal our data, i.e. our plan, budget, employee names, operational activities, and very highly classified information. Those hackers use these data and information for their own purpose or sell in the black market. Otherwise, they keep it for future attacks on our organization or to the UK.

To protect our critical assets, network system, we always maintain our risk mitigation strategies and implement our cyber capability to ensure our highest value assets (Data and Information) have the most comprehensive security.

To do this, we have some top leadership roles to implement its Governance and Methodology; and also, we have a very large Security Operation Centre (SoC), which monitor our network activities 24/7 and 365 days; also, we have a Quick Reaction Force (QRF) as a backup cyber force in order to carry out our daily job if our critical system attacked by the attackers partially or as a whole.

Cybersecurity governance

Integrate the three questions from your submission in Module 4, in which you recommended a cybersecurity leadership plan, improvements to management processes, and a cybersecurity awareness training program.

(Write approximately 1,200 words)

Start writing here:

Management process when developing Cybersecurity in my Organization:

As I mentioned numerous times that my organization is one of the technical (Cyber) regiments in the British Army; therefore, my organization has to follow the Army Doctrine for its Land Operation and as well as Land Cyber Programme which was approved by the British Government. In my organization, all leadership roles follow the management processes when developing a cybersecurity governance plan.

Furthermore, this Land Cyber program's aim is to cross-examine people with cyber and electromagnetic technology to exploit the opportunity and obtain a military advantage; also, this Cyber program stated as its priority "To offer electronic and cyber protection to operate in a hostile cyber and electromagnetic domain. To deepen our understanding, using enhanced electronic sensors and survey tools and by better contributing to the collection and exploitation of national intelligence." Therefore, our leadership roles in my

organization are very keen to utilize its cybersecurity governance in order to uphold the distinct management process.

[The quote in this paragraph has taken from the Land Cyber Programme in order to evaluate my explanation, Land Cyber Programme. (2021). Retrieved 9 August 2021, from https://www.gov.uk/guidance/land-cyber-programme#programme-benefits]

Alongside this, our leaders implement cybersecurity governance to helping my organization to control and communicate our cybersecurity risk management activities. However, for the governance and business objectives, general approaches for cybersecurity and risk management for my organization sometimes create confusion; predetermined security risk management plans, business process ideas, roles, and responsibilities are sometimes separated from the decision-making process for our daily business. This separation sometimes can lead to delay and misinterpretation in our cybersecurity decision-making process.

Therefore, our leadership roles prioritize the job or are committed to establish and implement cybersecurity governance plans to make effective risk management decisions, which can fit in our daily business, and it can lead a good control and a good level of cybersecurity. By implementing Cybersecurity governance sufficiently, our leaders can achieve effective risk management, and they (leaders) can mitigate the cyber risk in order to secure Army's valuable assets and information from the hackers.

Based on my explanation above, the word "Governance" indicates that my organization or any other organization actively exercises control over the cyber risk it faces and gives some crystal-clear directions for the safety and security for running its daily business. To make this cybersecurity effective the governance needs that organizations invest risk management resources, and some good decision-makers, who the organization can trust, and my organization already has that. Those right people (leaders) need to be at the right places to enables sensible risk management decision-making to carry out its daily job.

In the end, when leadership roles implement good cybersecurity governance then we can see sufficient effective cybersecurity risk management; also, this is built on good, and effective decision making. However, the Chief Information Security Officer (CISO), Chief Information Officer (CIO), and Chief Security Officer (CSO) within my organization do not need to make all cyber risk management decisions by implementing the governance or methodology, as I mentioned earlier, cyber risk management decision making can take place at all levels within my organization; but sometimes, it delegates those people in my organization, who are Subject Matter Expert (SME), and solve the problem quicker than other.

I recommend a Cybersecurity awareness and training programme in my organization:

My organization is very focused on organization's cybersecurity awareness. To do this, my organization liaise with the National Cyber Security Centre (NSCS), and the Government Communication Headquarters (GCHQ) of the UK; additionally, the Defence Cyber School located at the Defence Academy of the United Kingdom conduct various types of cybersecurity awareness training to the Military Personnel in my organization.

Moreover, to make cybersecurity risk management effective, and governance implementation upfront, it is important to establish regular cybersecurity awareness training within my organization; therefore, all leaders in my organization establish clear lines of communication between those that are responsible and accountable for cybersecurity training.

In my organization, by conducting regular cyber awareness training, we develop and practice an effective culture and environment for our Cybersecurity and Cyber risk mitigation. Effective security culture and environment sometimes help to deal with complex Cyber incidents easily, as well as reduces the cyber risk management uncertainty. This security culture can be encouraging by ensuring that all Service Personnel in my organization understand the objectives and maintaining the priority of the business is most important within the organization, employing and appointing personnel who have Cybersecurity knowledge, risk management skills, and expertise. By doing all these, Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Security Officer (CSO) make sure that they can trust their employee and they can empower those people to implement the organization's governance and able to make a Cyber risk management decision.

Alongside this, the National Cyber Security Centre (NCSC) conducts a Cybersecurity online training via Defence Learning Environment (Military Education Site); also, they (NCSC) conduct 10 steps Cybersecurity engagement and training to our organization. The NCSC makes sure that every people in my organization practice good security and grow a positive Cybersecurity culture. The 10 steps Cybersecurity also will be used in my organization and NCSC's Cybersecurity toolkit for boards, especially the board members who may not properly train in Cybersecurity or Cyber risk management. The board toolkit helps frame discussion between the board and the technical experts and replaces the executive summary section of the original 10 steps.

The NCSC's 10 steps Cybersecurity stated below:

1)Risk Management
2) Engagement and training
3) Asset management

4) Architecture and configurations
5) Vulnerability management
6) Identity and access management
7) Data Security
8) Logging and monitoring
9) Incident Management
10) Supply Chain Security

[This paragraph idea and quote has taken from the NCSC's 10 steps Cybersecurity training, which they (NCSC) provide to my organization (13 Royal Signal regiment) each year and my own evaluation, Engagement and training. (2021). Retrieved 9 August 2021, from https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training]

Alongside this, my organization always follows the British Army Doctrine, and the Doctrine introduced us to the Military Annual Training Test (MATTs), which is what we have to do every year before it expires, as a Cyber regiment we have to complete Cybersecurity awareness training via Defence Cyberschool. The Defence Academy conducts Cybersecurity awareness training every three months in a classroom consists of 30 – 40 students in the Defence Academy of the UK.
This course is generally for my organization, which is Army's Cyber regiment, but sometimes, it allows a number of selected students from different security roles across the British Army, Royal Airforce, and Royal Navy.

By doing this course and Military Annual Training Test (MATT), it allows the Service Personnel and leaders to perform their Cyber roles and give the ability with confidence to implement an effective Cybersecurity governance plan.

Based on the explanation above, I have mentioned my recommendation; however, the leadership roles of my organization should consider the problems which may face my organization and decide which one should we deal with, and it will be good for our organization. This is very important because if those recommendations our leadership roles adopt and implement for the Cybersecurity governance, risk mitigation strategies, we can achieve a good level of security of our Cyberdefense, which will keep safe and secure our tri-service and the United Kingdom.

Protective technologies

In Module 5, you compiled a list of questions you would ask to understand the technologies implemented to protect your organization's critical systems, networks, and data. In this section, based on the questions you asked and by conducting any other additional research, identify technologies your organization can employ to protect its critical systems, networks, and data.

If you are using the Sony case, recommend protective technologies that could have addressed Sony's shortcomings in protecting their critical networks, systems, and data.

Note:

This question requires you to submit a paragraph consolidating the information you learned, and is not a resubmission of the questions you submitted in Module 5.

(Write approximately 650 words)

Start writing here:

As I have mentioned above that my organization is the 13 Royal Signal Regiment in the British Army, it is only the Cyber Regiment within the British Armed Forces; this is very large and complex, and our Information Structure is bigger than any other IT organization in the UK.

Also, I have mentioned above in my organization, the most critical assets are our Data and Information, which includes official, official-sensitive, secret, and top-secret. Alongside this, all Military research, HR information, internal software development process, and classified agenda.

Without data, we (Army Cyber Regiment) can not carry out our daily cyber and military activities, on-going, and future mission. Everyone is responsible for using data and it has to follow the General Data Protection Regulation (GDPR), i.e. use fairly, lawfully, transparently, used for specified.

To share our resources and electronic communications, my organization using Local Area Network (LAN) and Wide Area Network (WAN), Military Classified Network (encrypted). However, my organization uses Military internet activities most of the time, and which is why the ISP (Internet Service Provider) relates to the Military internet and filters its connection layers to receive and send any data over the Military internet.

Again, I am mentioning that a Brigadier (1 star General) is the Chief Information Security Officer (CISO), and he is leading the Army Cyber regiment, as a whole. Additionally, our Officer in Command (OC) in the Cyber regiment is the Chief Information Officer (CIO) and the Second in Command (2IC) is Chief Security Officer (CSO) for our Cyber regiment. They are setting in the main roles in our Military Cyber Organization, and they are responsible for the governance and its implementation.

In Module 5, I assembled 10 questions for them (CISO, CIO, CSO, and other leadership roles). However, now with those questions and context, I would

include that the technologies my organization can employ or implement to protect its critical systems, networks, and data.

Please see below:

Q1: Are we protecting our entire Information Structure well?

We can employ or implement: We implement ISO 27001 information classification, it's a process that organizations assess the data that they hold and the level of protection it should be given in order to protect our information structure.

As a Cyber regiment of the British Armed Forces, it is our duty to protect our whole Information Structure, as accurately as possible in order to protect the Tri-Service's (British Army, RAF, and RN) Data and Information.

[These ideas I have taken from Irwin, L., Irwin, L., Irwin, L., Irwin, L., Irwin, L., & Irwin, L. et al. (2021). Cyber Security Archives - IT Governance UK Blog. Retrieved 10 September 2021, from https://www.itgovernance.co.uk/blog/category/cyber-security and my own evaluation]

Q2: Can we identify and understand those critical assets that could impact our Confidentiality, Integrity, and Availability (CIA) and support our functions and operational roles?

We can employ or implement: Our leaders need to make sure that our all employees understand the security concept and can act accordingly; therefore, they (top roles) should conduct regular refreshment training for our employees.

As the most critical assets in our organization are Data and Information, it's included official, official-sensitive, secret, and top-secret. Therefore, we need to protect it at any cost, Cybersecurity wise alongside Physical security.

Q3: Is our Security Operation Centre (SoC) is operating well on a 24/7 basis?

We can employ or implement: In order to operate our SoC well, our leaders need to conduct a regular inspection that our SoC always reminds healthily, and they (top roles) can add a forensic team within the SoC team to do a further forensic investigation. Security Operation Centre is the first-line defense of our Cyberspace and that is why we need to make sure if anything suspicious is going on in our network that must be raised for an investigation

and act accordingly. Therefore, we need to put trained personnel in different roles as per its Cybersecurity requirement.

Q4: Is there any backup team ready for tackling any kind of incident or if our first-line defense (SoC) goes down?

We can employ or implement: In order to do this, our leaders need to make sure that the team is always fit to react if this kind of incident happened and they can do a refreshment drill on a regular basis.

As our organization is a Military Cyber organization; therefore, we need to make sure that there is a backup team like Cyber QRF (Quick Reaction Force) ready to deal with these kinds of incidence, i.e. safety-critical, mission-critical, and business-critical.

Q5: Is our network system secure to share our resources and electronic communications?

We can employ or implement: In order to carry out this, our technical expertise need to make sure that all functions and filter are incorrect places and performing accurately.

As our organization using Local Area Network (LAN) and Wide Area Network (WAN). Our organization uses Military internet activities most of the time, and which is why the ISP (Internet Service Provider) relates to the Military internet, and it filters its connection layers to receive and send any data over the Military internet. We need to make sure; everything is going well and secure in order to do our daily business.

Q6: Is there any extra feature do we need to add to our network system?

We can employ or implement: Our technical expertise needs to make sure that those extra features are up to date and working accurately in order to secure our critical assets.

As a Military Cyber regiment, a LAN (Local Area Network) is consisting of a relatively small area, i.e. in our Camp, Garrison, Company HQ (headquarter), but we still can include First Generation Firewalls (FGFW), IDS, and IPS in our network system in order to make an extra layer of Cybersecurity.

Alongside this, we use a WAN (Wide Area Network) is connected in larger geographic areas for our operation role in Iraq, and Afghanistan. Therefore, we need to make sure when it is connected to transoceanic cabling or with a

Military satellite in order to carry out our daily job, it is safe and secure, i.e Lockheed Martin satellite.

Q7: Are we maintaining our BOYD (Bring your own Device) policy accurately?

We can employ or implement: To do that responsible person in our organization should conduct a regular snap check or inspection to all employees.

A great example I can give, On 02 June 2021, the news came out that “UK Special Forces soldiers’ personal data was floating around What’s App in a leaked Army spreadsheet”. Though it was a different regiment; we need to make sure this kind of incident not taking place in our organization, and we are maintaining the BOYD policy accurately as per our governance.

[This quotation from, UK Special Forces soldiers' personal data was floating around WhatsApp in a leaked Army spreadsheet. (2021). Retrieved 14 August 2021, from https://www.theregister.com/2021/06/02/uk_special_forces_data_breach_whatsapp/]

Q8: Are we maintaining our Access Control List (ACL) well?

We can employ or implement: To do that our network engineers should check ACE and own rules on a regular basis.

As a Cyber organization, we can manage our own Access Control List, where we can make a list of Access Control Entries (ACE). We can set our own rules in our network system, and we can decide that whether we will allow or deny anything send from outside of our network.

Q9: Are we taking care of our role-based privilege and have divided our sections into different rooms?

We can employ or implement: To do that our Sys-Admin should keep an eye on all employee's access and should be proactive sometimes to check that everything is going well in my organization.

As our organization is the most sensitive organization within the Tri-Service and we deal with the most sensitive, secret, and top-secret data and information on a daily basis; therefore, we need to maintain the Role-Based

Access Control (RBAC). By doing this, we can restrict our network access based on the roles of each individual user within our Cyber organization.

Alongside this, by dividing our sections and put in a different room, users can work only in their perimeter and can not go to any other room or section if it is not necessary.

Q10: What have we done for overall Cybersecurity and Physical Security, as it is connected to each other?

We can employ or implement: To do that our leaders should implement our governance as accurately as possible and need to conduct a regular meeting to check that everything is in place to protect our critical assets, network, and data.

As I have mentioned, our organization is the first-line defense for our Cyberspace and also, for the Armed Forces of the United Kingdom; therefore, all Evil eyes are on our organization's Information Structure and its assets. That is why it is very crucial to have the highest Security standard for overall Cybersecurity as well as Physical security.

We need to make sure that we always (24/7, 365 days) have Armed Guards, and they are doing duty at the main Garrison gate, a single guard is watching our Cyber building entrance 24/7. Whenever we get IN and OUT to the main Cyber building we are signing IN and signing OUT the logbook. Without an access card, no one can not enter the actual Cyber Operational room, but physical security is something that is very important and sometimes overlooked.

Legal considerations

In Module 6, you compiled a list of questions you would direct towards an organization's senior management and general counsel in order to gauge the organization's legal risk mitigation strategy and the adequacy of their preparations. In this section, based on the questions you asked, and by conducting any other additional research, discuss the legal considerations your organization should take into account when compiling its risk mitigation strategy.

If you are using the Sony case, recommend steps that could have addressed Sony's shortcomings in protecting themselves from legal action.

Note:

This question requires you to submit a paragraph consolidating the information you learned, and is not a resubmission of the questions you submitted in Module 6.

(Write approximately 550 words)

Start writing here:

Nowadays, Cybersecurity is becoming a battlefield of legal risk; one incorrect step can ruin the organization's function and reputation. If something goes wrong and after a misstep, i.e., clint's data breach, it triggered a legal issue.

As in module 6, I assembled 10 questions for them (CISO, CIO, CSO, and other leadership roles). However, now with those questions and context, I would include that the legal considerations my organization should take into account when compiling its risk mitigation strategy.
Please see below:

Q1: How are we mitigating the litigation risks, are we avoiding three big issues for our organization, Breach of Contract lawsuit, Negligence Lawsuit, Regulatory Enforcement?

Considerations my organization should take: As a Cyber regiment of the British Armed Forces, we must understand our critical and valuable assets, which we need to protect, the risk of our organization, and risk management, as a whole. Alongside this, we must be a contract with everyone who is related to our Cyber regiment in order to secure our Cyberspace, and we need to look at any breach of contract.
The contract must specify the responsibility of each party; we need to be careful about a negligence lawsuit claims that a party failed to use responsible caution when providing services. We can avoid a Cybersecurity legal issue by maintaining the standard of care. In the end, we need to be the focus on Regulatory Enforcement.

Q2: Are we adopting and monitoring the UK law for our daily business in Cybersecurity, alongside our Military intense work?

Considerations my organization should take: The UK government published a plan for new Cybersecurity legislation on 21 April 2021, it relates to consumer Internet of Things (IoT) we need to make sure that we are adopting and monitoring the legislation alongside our Military instance work in order to keep safe our force and the country.

Q3: Are we looking after the privacy of our valuable asset, i.e. Data?

Considerations my organization should take: All the Evil eyes on our Information Structure, and as a British Army's Cyber regiment we have to be

very careful that there are no data breaches, if it is, then those attacks may impact our Military Personnel's data and privacy.

Q4: Are we mitigating the litigation risk for our organization?

Considerations my organization should take: This process will not prevent the legal action 100%, but it will help us to bring more clarity for legal action by any of our Personnel or victim of Cyber-attack. If we follow the 6 steps, it will help us to achieve our goal.

See below:

a) Select Framework
b) Obtain organizational commitment
c) Identify legal risks
d) Analyze legal risks
e) Evaluate legal risks
f) Communicate and advise

[This 6 steps idea I have taken from the Lextree site in order to reinvigorate my context and my own evaluation. Solutions, B. (2021). Lextree | Legal Technology | Berkman Solutions. Retrieved 21 August 2021, from https://www.berkmansolutions.com/]

Q5: Are we aware of our UK's legal rules and around the world?

Considerations my organization should take: As a Military Cyber organization, we need to understand and implement our laws, regulations, which are approved by the British Parliament, i.e. General Data Protection Regulation (GDPR) Act 2018. Alongside this, we need to be aware of other laws around the world, i.e. NIS, PCI DSS. These we need to apply to our organization in order to implement our daily Cyber business well.

Q6: How we are maintaining our GDPR as a Military Cyber organization in Great Britain?

Considerations my organization should take: As I mentioned earlier, the most critical assets in our organization are Data and Information. Without data, we (Army Cyber Regiment) cannot carry out our daily cyber and military activities, on-going, and future mission. Therefore, we need to maintain GDPR for our Military Personnel and ongoing missions' data collecting, processing, and storing.

Q7: If something goes wrong then what is our best Course of Action (CoA in Military language)?

Considerations my organization should take: As a Military Cyber regiment, we need to make sure that we have got enough resources, i.e. our Military Cyber Personnel, funding, and our high-ranking officer (top management) are

happy to recognize compliance efforts. Additionally, we need to estimate the potential cost of any incident that takes place to achieve more clarity.

Q8: Are we keeping our equipment secure, workable, and as well as reviewing Cybersecurity laws and regulations, and keeping them up to date?

Considerations my organization should take: First, as a Cyber regiment, we need to make sure that our sophisticated equipment for Cyber operations is secure, workable, and up to date. Alongside this, we (CISO, CIO, CSO) need to review our own (UK's) and International Cybersecurity law and regulation; we need to stay up to date, which we can apply to our current and future operations.

Q9: Are we insured with any company?

Considerations my organization should take: As a Cyber regiment, this should be our first thinking to mitigate litigation risk. Therefore, we need to make sure that we have adequate Cyber insurance as a part of our organization and cover the cost if there are any data breaches, privacy breaches, litigation, and penalties of our Military Personnel and others related to our Military Cyber regiment.

Q10: Are we taking our regular training in order to understand and manage our everyday job?

Considerations my organization should take: As a Military Cyber organization, we must follow the British Army's Doctrine; therefore, we need to complete MATT (Military Annual Training Test) every year. As a Cyber regiment, we need to make it mandatory that everyone across the tri-service (Army, RAF, and RN) is doing their Cyber training in order to appropriate handling and protection of sensitive data; also, they (Service Personnel) are aware of the information security, various attacks, i.e., phishing, vishing.

As well as selective higher roles from every regiment of our tri-service should conduct the Cyber course, and aware about risk mitigation for litigation from the Defence Academy United Kingdom.

In the end, I would like to mention to my CISO, CIO, and CSO that if we are covering and maintaining those, I have mentioned above then we can achieve clarity relates to litigation and mitigate our organizational risk.

References

[1] (2021). Retrieved 9 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609611/uk-cyber-security-strategy-final.pdf

[2] Armed Forces announce launch of Cyber Regiment in major modernisation. (2021). Retrieved 26 July 2021, from https://www.gov.uk/government/news/armed-forces-announce-launch-of-first-cyber-regiment-in-major-modernisation

[3] Those 10 Steps of Incident Response Plan ideas on above has taken from "The UK Cyber Security Strategy", which my organization (13 Royal Signal Regiment) implementing, Harvard University VPAL course materials, and my own evaluation, (2021). Retrieved 9 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[4] Network Security for Small Business - AccessEnforcer. (2021). Retrieved 21 August 2021, from https://www.calyptix.com/products/

[5] The overview of my organization and compiled 10 questions, those ideas I have been taken from the Harvard Course Materials, My learning experience thus far, British Army website. IMA (Information Management Assurance) and my own organization, which is the 13 Royal Signal Regiment and my own evaluation, references given below:

[6] speaking at New Statesman Media Group's CIO Town Hall Live forum in July 2020. TECHMONITOR. (2020, October 7). Https://Techmonitor.Ai/Tech-Leaders/Data-Cyber-Iot-British-Army. https://techmonitor.ai/tech-leaders/data-cyber-iot-british-army

[7] Land Cyber Programme. (2021). Retrieved 9 August 2021, from https://www.gov.uk/guidance/land-cyber-programme#programme-benefits

[8] Local Government Association. (2021). Retrieved 4 September 2021, from https://www.local.gov.uk/
[9] National Cyber Force Transforms country's cyber capabilities to protect UK. (2021). Retrieved 26 July 2021, from https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk

[10] Chapter 1: What is a Network? (n.d.). Https://Fcit.Usf.Edu/Network/Chap1/Chap1.Htm. Retrieved 1 August 2021, from https://fcit.usf.edu/network/chap1/chap1.htm

[11] Business Owners Policy Insurance | AmTrust Financial. (2021). Retrieved 21 August 2021, from https://amtrustfinancial.com/insurance-products/businessowners-policy

[12] Irwin, L., Irwin, L., Irwin, L., Irwin, L., Irwin, L., & Irwin, L. et al. (2021). Cyber Security Archives - IT Governance UK Blog. Retrieved 10 September 2021, from https://www.itgovernance.co.uk/blog/category/cyber-security and my own evaluation]

[13] Mayer Brown. (2021). Retrieved 21 August 2021, from https://www.mayerbrown.com/en

[14] Ministry of Defence. (2021, July 30). GOV.UK. https://www.gov.uk/government/organisations/ministry-of-defence

[15] National Cyber Force: defending the cyber domain. (2021). Retrieved 9 August 2021, from https://www.army-technology.com/features/national-cyber-force-defending-the-cyber-domain/

[16] NCSC (2021). Retrieved 26 July 2021, from https://www.ncsc.gov.uk/

[17] Thakur, D. (2020, August 10). What is the Difference between Data and Information ? Computer Notes. https://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information

[18] Engagement and training. (2021). Retrieved 9 August 2021, from https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training

[19] Sky News - Cyber security breaches hit unprecedented highs in UK defence industry. (2021). Retrieved 26 July 2021, from https://news.sky.com/story/cyber-security-breaches-hit-unprecedented-highs-in-uk-defence-industry-11903520

[20] Government Digital Service. (2015, September 16). Data protection. GOV.UK. https://www.gov.uk/data-protection

[21] Land Cyber Programme. (2021). Retrieved 9 August 2021, from https://www.gov.uk/guidance/land-cyber-programme#programme-benefits

[22] Ruffle, R. M. (2017, April 11). Critical Asset Identification (Part 1 of 20: CERT Best Practices to Mitigate Insider Threats Series). SEI Blog. https://insights.sei.cmu.edu/blog/critical-asset-identification-part-1-of-20-cert-best-practices-to-mitigate-insider-threats-series/

[23] The Ministry of Defence Selects Oracle Cloud Infrastructure for Improved Agility and Speed of its Digital Transformation. (2021). Retrieved 26 July 2021, from https://www.oracle.com/uk/news/announcement/defence-selects-oracle-cloud-infrastructure-2020-09-23.html

[24] Oracle - Ministry of Defence. Retrieved 1 August 2021, from https://www.oracle.com/uk/news/announcement/defence-selects-oracle-cloud-infrastructure-2020-09-23.html

[25] Salesforce Engineering. (2021). Retrieved 4 September 2021, from https://engineering.salesforce.com/

[26] The quotation taken from Oxford English Spanish Dictionary in order to reinvigorate this assignment, HACKTIVIST | Definition of HACKTIVIST by Oxford Dictionary on Lexico.com also meaning of HACKTIVIST. (2021). Retrieved 26 July 2021, from https://www.lexico.com/definition/hacktivist

[27] Ministry of Defence. (2021, July 30). GOV.UK. https://www.gov.uk/government/organisations/ministry-of-defence

[28] What is a DDoS Attack? - DDoS Meaning. (2021). Retrieved 26 July 2021, from https://www.kaspersky.co.uk/resource-center/threats/ddos-attacks

[29] British Army to be downsized but National Cyber Force is here to stay. (2021). Retrieved 26 July 2021, from https://www.teiss.co.uk/britain-more-focus-on-national-cyber-force/

[30] Defence Gateway – Defence Learning Environment - Access denied | helpdesk.defencegateway.mod.uk used Cloudflare to restrict access. (n.d.). Defence Gateway. Retrieved 26 July 2021, from https://helpdesk.defencegateway.mod.uk/index.php?/Knowledgebase/List/Index/49/dle

[31] (2021). Retrieved 10 September 2021, from https://www.indeed.com/career-advice

[32] (2021). Retrieved 4 September 2021, from https://www.itp.net/

[33] (2021). Retrieved 9 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web.pdf

[34] Be part of the science inside UK defence and security. (2021). Retrieved 26 July 2021, from https://www.gov.uk/government/news/governments-integrated-review-drives-dstls-recruitment-campaign

[35] Biggest Online Tutorials Library. (2021). Retrieved 10 September 2021, from https://www.tutorialspoint.com/index.htm

[36] Engagement and training. (2021). Retrieved 9 August 2021, from https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training

*[37] TechTarget - Global Network of Information Technology Websites and Contributors. (2021). Retrieved 10 September 2021, from https://www.techtarget.com/network?_gl=1*1rpfjgh*_ga*MTQzMTY4MjA2Ni4xNjMxMTMyNTI5*_ga_TQKE4GS5P9*MTYzMTEzMjUyOC4xLjEuMTYzMTEzMjc4NS4w&_ga=2.236605831.707933281631132529-1431682066.1631132529*

[38] (2021). Retrieved 21 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf

[39] Access denied | www.army.mod.uk used Cloudflare to restrict access. (n.d.-b). British Army, Royal Corps of Signals. Retrieved 1 August 2021, from https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-signals/

[40] (2021). Retrieved 4 September 2021, from https://www.ncsc.gov.uk/

[41] British Military Experiences 60-Plus Cyber Attacks Per Day. (2021). Retrieved 26 July 2021, from https://www.forces.net/news/british-military-experiences-over-60-cyber-attacks-day

[42] Ministry of Defence. (2021, July 30). GOV.UK. https://www.gov.uk/government/organisations/ministry-of-defence

[43] 2021 Security Outcomes Study. (2021). Retrieved 21 August 2021, from https://umbrella.cisco.com/info/2021-security-outcomes-study?utm_medium=search-paid&utm_source=google&utm_campaign=UMB_22Q1_UK_EN_GS_Nonbrand_Security&utm_term=pgm&utm_content=umb-fy21-q3-content-ebook-security-outcomes-study&_bt=524594963191&_bk=cybersecurity%20risks&_bm=p&_bn=g&_bg=121669317796&gclid=Cj0KCQjwpf2IBhDkARIsAGVo0D3m4ZH--91SD3OvKQIwaKXNq5CtZRjlyLvnzxYllcRH6_GSpHk_r3gaAmhXEALw_wcB

[44] Ruffle, R. M. (2017, April 11). Critical Asset Identification (Part 1 of 20: CERT Best Practices to Mitigate Insider Threats Series). SEI Blog. https://insights.sei.cmu.edu/blog/critical-asset-identification-part-1-of-20-cert-best-practices-to-mitigate-insider-threats-series/

[45] 1st Signal Brigade (United Kingdom) - Wikipedia. (2021). Retrieved 9 August 2021, from https://en.wikipedia.org/wiki/1st_Signal_Brigade_(United_Kingdom)

[46] Access denied | www.army.mod.uk used Cloudflare to restrict access. (n.d.-b). British Army, Royal Corps of Signals. Retrieved 1 August 2021, from https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-signals/

[47] Access denied | www.army.mod.uk used Cloudflare to restrict access. (n.d.-b). British Army, Royal Corps of Signals. Retrieved 1 August 2021, from https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-signals/

[48] Data protection. (2021). Retrieved 26 July 2021, from https://www.gov.uk/data-protection

[49] Cyber Primer (2nd Edition), British Army - Cyber Primer. (n.d.). Ministry of Defence. Retrieved 1 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf

[50] UK Special Forces soldiers' personal data was floating around WhatsApp in a leaked Army spreadsheet. (2021). Retrieved 14 August 2021, from https://www.theregister.com/2021/06/02/uk_special_forces_data_breach_whatsapp/

[51] Defence Gateway - Login. (2021, August 1). Defence Learning Environment. https://dle.ice.mod.gov.uk/Login.aspx?ReturnUrl=%2f%3fwa%3dwsignin1.0%26wtrealm%3dhttp%253a%252f%252fsso.defencegateway.mod.uk%252fadfs%252fservices%252ftrust%26wctx%3dbc08344d-417b-413d-a7ee-3c6dfbf1e09a%26wct%3d2021-08-01T21%253a04%253a22Z&wa=wsignin1.0&wtrealm=http%3a%2f%2fsso.defencegateway.mod.uk%2fadfs%2fservices%2ftrust&wctx=bc08344d-417b-413d-a7ee-3c6dfbf1e09a&wct=2021-08-01T21%3a04%3a22Z

[52] Association of Corporate Counsel (ACC). (2021). Retrieved 4 September 2021, from https://www.acc.com/

[53] Cyber Primer (2nd Edition), British Army - Cyber Primer. (n.d.). Ministry of Defence. Retrieved 1 August 2021, fromhttps://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf

[54] Defence Gateway – Defence Learning Environment - Access denied | helpdesk.defencegateway.mod.uk used Cloudflare to restrict access. (n.d.). Defence Gateway. Retrieved 26 July 2021, from https://helpdesk.defencegateway.mod.uk/index.php?/Knowledgebase/List/Index/49/dle

[55] Technology School | Defence Cyber School | Defence Academy of the UK. (2021). Retrieved 9 August 2021, from https://www.da.mod.uk/colleges-and-schools/technology-school/defence-cyber-school/

[56] Data protection. (2021). Retrieved 21 August 2021, from https://www.gov.uk/data-protection

[57] Cyber Primer (2nd Edition), British Army - Cyber Primer. (n.d.). Ministry of Defence. Retrieved 1 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf

[58] (2021). Retrieved 9 August 2021, from https://www.youtube.com/watch?v=udoyvUJk_TI&ab_channel=BritishArmy

[59] Defence Information, Knowledge, Digital and Data policy commitments. (2021). Retrieved 26 July 2021, from https://www.gov.uk/government/publications/jsp-441-defence-records-management-policy-and-procedures--2/defence-information-knowledge-digital-and-data-policy-commitments

[60] Information Infrastructure - an overview | ScienceDirect Topics. (n.d.). Https://Www.Sciencedirect.Com/Topics/Computer-Science/Information-Infrastructure. Retrieved 1 August 2021, from https://www.sciencedirect.com/topics/computer-science/information-infrastructure

[61] Electronic Warfare (EW), British Army - Access denied | www.army.mod.uk used Cloudflare to restrict access. (n.d.). British Army. Retrieved 1 August 2021, from https://www.army.mod.uk/news-and-events/news/2021/04/electronic-warfare/

[62] Information Management Assessment Ministry of Defence March 2009, EXECUTIVE SUMMARY - Information Management Assessment. (2009). Https://Www.Nationalarchives.Gov.Uk/Documents/Mod-Ima-Report-Final.Pdf. https://www.nationalarchives.gov.uk/documents/mod-ima-report-final.pdf

[63] Access denied | www.army.mod.uk used Cloudflare to restrict access. (n.d.-b). British Army, Royal Corps of Signals. Retrieved 1 August 2021, from https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-signals/

[64] Engagement and training. (2021). Retrieved 9 August 2021, from https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training

[65] Home | GCHQ. (2021). Retrieved 26 July 2021, from https://www.gchq-careers.co.uk/

[66] This paragraph idea and quote has taken from "The UK Cyber Security Strategy", which my organization (13 Royal Signal Regiment) implementing, and my own evaluation, (2021). Retrieved 9 August 2021, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[67] Engagement and training. (2021). Retrieved 9 August 2021, from https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training

[68] Access denied | www.army.mod.uk used Cloudflare to restrict access. (n.d.-b). British Army, Royal Corps of Signals. Retrieved 1 August 2021, from https://www.army.mod.uk/who-we-are/corps-regiments-and-units/royal-signals/

[69] Home - Leaf. (2021). Retrieved 4 September 2021, from https://leaf-it.com/

[70] MoD of the UK - Ministry of Defence. (2021). Retrieved 26 July 2021, from https://www.gov.uk/government/organisations/ministry-of-defence

[71] Risk management for cyber security. (2021). Retrieved 21 August 2021, from https://www.ncsc.gov.uk/collection/board-toolkit/risk-management-for-cyber-security

[72] Information Infrastructure - an overview | ScienceDirect Topics. (n.d.). Https://Www.Sciencedirect.Com/Topics/Computer-Science/Information-Infrastructure. Retrieved 1 August 2021, from https://www.sciencedirect.com/topics/computer-science/information-infrastructure

[73] Does the NIS implementation strategy effectively address cyber security risks in the UK?. (2021). Retrieved 9 August 2021, from https://ieeexplore.ieee.org/abstract/document/8884963
[9] Information Infrastructure - an overview | ScienceDirect Topics. (n.d.). Https://Www.Sciencedirect.Com/Topics/Computer-Science/Information-Infrastructure. Retrieved 1 August 2021, from https://www.sciencedirect.com/topics/computer-science/information-infrastructure

[74] National Archives (2021). Retrieved 26 July 2021, from https://www.nationalarchives.gov.uk/documents/information-management/mod-ima-report-final.pdf

[75] Ruffle, R. M. (2017, April 11). Critical Asset Identification (Part 1 of 20: CERT Best Practices to Mitigate Insider Threats Series). SEI Blog. https://insights.sei.cmu.edu/blog/critical-asset-identification-part-1-of-20-cert-best-practices-to-mitigate-insider-threats-series/

[76] Solutions, B. (2021). Lextree | Legal Technology | Berkman Solutions. Retrieved 21 August 2021, from https://www.berkmansolutions.com/

[77] Chakrabarty, T. (2020, August 29). What are the 3 principal types of critical. . . Online Class Notes. https://onlineclassnotes.com/what-are-three-principal-types-of-critical-system/
Cybersecurity & Technology News | Secure Futures | Kaspersky. (2021). Retrieved 4 September 2021, from https://www.kaspersky.com/blog/secure-futures-magazine/

Incident response plan (not required)

Note:

The incident response plan is a central part of an organization's cyber risk mitigation strategy. However, as you will not have an opportunity to revise your plan based on your Tutor's feedback in time for Module 8, you are **not** required to integrate it into your final risk mitigation strategy. Please consult the grading breakdown in the Orientation Module course handbook for more information.

Your ongoing project submission will be graded according to the following rubric:

4. Rubric

	Very poor	Poor	Satisfactory	Very good	Exceptional
Adherence to the brief *All sections in the template are completed.*	No submission, or student fails to address any element of the brief. (0)	Some key elements are not addressed. Most information provided is irrelevant. (5.5)	Student has adhered to most of the brief. Sufficient information is provided and is mostly relevant. (7)	Student has adhered to almost all elements of the brief. Almost all information is provided and is relevant. (8.5)	Student has fully adhered to the brief. All information provided is comprehensive and relevant. (10)
Introduction and vision *Student has clearly outlined the need for their risk mitigation strategy, and what it aims to achieve by implementing the strategy.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to clearly outline the need for the strategy or its long-term vision. There is no evidence that the student has used the content covered in the course to inform their response. (0)	Student shows an incomplete understanding of the need for their strategy, or its long-term vision. There is some evidence that the student has engaged with the content covered in the course but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of the need for their strategy, and its long-term vision. The student has clearly engaged with the content covered in the course, but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of the need for their strategy, and its long-term vision. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of the need for their strategy, and its long-term vision. The student has been able to critically apply their learning from the course. (10)

Strategic goals and objectives *Student has outlined at least four strategic goals that will reduce their organization's risks to an acceptable level. They have included at least two objectives that clearly explain what must be done to achieve each goal.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to clearly outline their strategy's goals and objectives. There is no evidence that the student has used the content covered in the course to inform their response. (0)	Student shows an incomplete understanding of their strategy's goals and objectives. There is some evidence that the student has engaged with the content covered in the course but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of their strategy's goals and objectives. The student has clearly engaged with the content covered in the course, but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of their strategy's goals and objectives. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of their strategy's goals and objectives. The student has been able to critically apply their learning from the course. (10)
Metrics *The student has listed at least three metrics their organization could use to measure the achievement of their goals, and the metrics are specific to the goals/objectives identified.* *Student has thought critically and incorporated*	No submission. OR Student fails to list three metrics their organization could use to measure cybersecurity. The metrics are not specific to the identified goals/objectives. There is no evidence that the student has used the content covered	Student shows an incomplete understanding of metrics their organization could use to measure its cybersecurity. The metrics lack relevance to the identified goals/objectives. There is some evidence that the student has engaged with the course content, but this	Student demonstrates satisfactory understanding of the metrics their organization could use to measure its cybersecurity and they are relevant to the goals and objectives identified. The student has clearly engaged with the course content but a	Student demonstrates a strong understanding of the metrics their organization should use, and they are specific to the goals/objectives identified. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of the metrics their organization can use, and they are specific to the goals/objectives identified. The student has been able to critically apply their learning from the course. (10)

learnings from the content.	in the course to inform their response. (0)	is not always accurately applied. (5.5)	more nuanced answer is required. (7)		
Cybersecurity threat actors *Student has identified at least two threat actors and described a scenario of an attack.* *In the case of Sony, student has accurately identified the threat actor and method of attack in the 2014 hack, as well as one other potential threat actor.* *Student has thought critically and incorporated learnings from the content and has applied this to their chosen organization.*	No submission. OR Student fails to list two threat actors that could attack their organization. They have not provided a possible method of an attack. There is no evidence that the student has used the course content to inform their response. (0)	Student shows an incomplete understanding of the threat actors who could attack their organization and the possible method of attack. There is some evidence that the student has engaged with the course content, but this is not always accurately applied. (5.5	Student demonstrates satisfactory understanding of the threat actors who could attack their organization and the possible method of attack. The student has clearly engaged with the course content but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of the threat actors who could attack their organization and the possible method of attack. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of the threat actors who could attack their organization and the possible method of attack. The student has been able to critically apply their learning from the course. (10)

Business critical assets *Student has identified the assets that are most essential to their organization, and described vulnerabilities these assets may be exposed to.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to identify the assets that are critical to their organization and accurately describe how these assets are vulnerable. There is no evidence that the student has used the course content to inform their response. (0)	Student shows an incomplete understanding of their organization's critical assets, and how they are vulnerable. There is some evidence that the student has engaged with the course content but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of their organization's critical assets, and how they are vulnerable. The student has clearly engaged with the course content but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of their organization's critical assets, and how they are vulnerable. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of their organization's critical assets, and how they are vulnerable. The student has been able to critically apply their learning from the course. (10)
Cybersecurity governance *Student has recommended cybersecurity leadership plan, improvements to management processes, and a cybersecurity awareness training program.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to recommend a cybersecurity leadership plan, improvements to management processes, and a cybersecurity awareness training program. There is no evidence that the student has used the course content to inform their response. (0)	Student shows an incomplete understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. There is some evidence that the student has engaged with the course content but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. The student has clearly engaged with the course content but a more nuanced	Student demonstrates a strong understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of cybersecurity leadership plans, management processes, and cybersecurity awareness training programs. The student has been able to critically apply their learning from the course. (10)

			answer is required. (7)		
Protective technologies *Student has accurately identified protective technologies that are, or should be, implemented to enhance their organization's cybersecurity.* *Student has thought critically and incorporated learnings from the content.*	No submission. OR Student fails to identify protective technologies that are, or should be, implemented to enhance their organization's cybersecurity. There is no evidence that the student has used the course content to inform their response. (0)	Student shows an incomplete understanding of the necessary protective technologies that are, or should be, implemented to enhance their cybersecurity. There is some evidence that the student has engaged with the content covered in the course but this is not always accurately applied. (5.5)	Student demonstrates satisfactory understanding of the technologies that are, or should be, implemented to enhance their cybersecurity. The student has clearly engaged with the course content but a more nuanced answer is required. (7)	Student demonstrates a strong understanding of the technologies that are, or should be, implemented to enhance their cybersecurity. The answer shows a strong grasp of the content. (8.5)	Student demonstrates a thorough and incisive understanding of the technologies that are, or should be, implemented to enhance their cybersecurity. The student has been able to critically apply their learning from the course. (10)
Legal considerations *Student has critically analyzed the legal considerations their organization should take into account.*	No submission. OR Student fails to critically analyze the legal considerations their organization should take into account. There is no evidence that	Student shows an incomplete understanding of legal considerations that their organization should take into account. There is some evidence that the student has	Student demonstrates satisfactory understanding of legal considerations that their organization should take into account. The student has clearly engaged with	Student demonstrates a strong understanding of the legal considerations their organization should take into account. The answer shows a strong	Student demonstrates a thorough and incisive understanding of the legal considerations their organization should take into account. The student has been able to critically apply

Student has thought critically and incorporated learnings from the content.	the student has used the course content to inform their response. (0)	engaged with the course content but this is not always accurately applied. (5.5)	the course content but a more nuanced answer is required. (7)	grasp of the content. (8.5)	their learning from the course. (10)
Application of course content to organizational context *The student has accurately applied the learnings from the course content to their own organization or Sony's unique context.*	No submission OR The student has not made use of their organization's unique organizational context and constraints to inform their response (0)	Student has demonstrated a limited understanding of their organization's unique context and constraints and context (5.5)	Student has demonstrated a satisfactory understanding of their organization's context and constraints, however a there is room for deeper engagement with its nuances. (7)	There is clear evidence that the student has thought about their organization's unique context and constraints, and catered for this in their strategy accordingly. (8.5)	There is strong evidence that the student has understood and thought carefully about their organization's unique context and constraints, and has provided considered recommendations in their strategy accordingly. (10)
Organization of writing *Answer should be structured clearly and logically.*	No submission or complete lack of logical structure. (0)	Answer has some logical structure, but not enough to justify a passing grade. (5.5)	Answer is structured fairly well in terms of logic and clarity. (7)	Answer is structured very well in terms of logic and clarity. (8.5)	Answer is structured exceptionally well in terms of logic and clarity. (10)

Total: 110 points