****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

Ali Gautreuax

**IHP4 Task 2: Ethics and Cybersecurity**

**IHP4 Task 2: Ethics and Cybersecurity**

**A1/A1a. Ethical Guidelines Related to Information Security**

One ethical guideline that is related to information security used by the EC Council is “Ensure all penetration testing actives are authorized and within legal limits.” The reason why this guideline is appropriate is because it was noted within the case study of TechFite that their Business Intelligence (BI) Unit actively participated in preformed unauthorized penetration test and scanning on various companies IP address. If TechFIte had adopted this guideline it would have helped because the organization and the employees would have known that using the Metasploit tool for penetrating and scanning unauthorized networks, will lead to lawsuits from the owners of the network’s that were accessed without permission along with Federal charges.

Another One ethical guideline that is related to information security used by ISACA is “Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security, and risk management.” This guideline is appropriate because TechFite never performed audit on their employee’s user accounts with their equipment allowing for Business Intelligence (BI) Unit have ability to create fake accounts that had full admin privileges could access departments that contain sensitive information. Had this guideline been put into practice then auditing would have taken place, which would have helped prevent the possibility of sensitive information being accessed by end users who didn’t have authorization to access and wouldn’t have been able to malicious software on their equipment to perform malicious activities.

**A2. Unethical Practices**

Carl Jaspers the head of Applications Division would continuously give glowing endorsements to the CISO (Chief Information Security Officer) of their employee IT Security Analyst Nadia Johnson, allowing her to gain raises for each review. It was also noted that Jaspers and Johnson had personal relationships with each other outside of work environment. Allowing for any issue that would come in reports that could be tied to Jaspers would easily be overlooked on purpose because of the relationship Johnson and Jasper have.

Jack Hudson a member of the BI Unit and an active member of Strategic and Competitive Intelligence Professionals actively participated in working with third parties to gain intelligence by preforming well known social engineering tactics having them harvest companies trash to be able get sensitive information. As member of the Strategic and Competitive Intelligence Professionals he is aware what is ethical and unethical.

**A3. Factors**

When Nadia Johnson was not properly reviewing the internal reports from the CISO, providing blanket summary statement of no abnormalities or issue where founded. This allowed for the individuals who were commenting malicious activity keep doing without any repercussions due to it being overlooked and the individuals not being held responsible for there actions.

By not making any attempt to create separation of client’s information of old and potential new clients. It allowed for malicious individuals to be able to perform insider trading deals with clients of potential new clients who have a competitor with current clients. By selling information that is disclosed within NDA’s potential new clients are required to fill out.

**B1. Information Security Policies**

Audit Policy is made to set account limits for a set of users of one or more resources. If this policy was in place appropriately it only appropriates users would have had access to full admin right within the network able make changes equipment appropriately. Unlike with the BI Unit who had full admin rights on there equipment where able to install Metasploit on their equipment and use it to gain unauthorized access into the various companies’ networks. This policy would drastically decreased threats to intellectual property because BI Unit wouldn’t have had the ability preform unauthorized scanning and penetration into networks.

Chinese Wall Policy are created to help stop the sharing of sensitive information form departments that are within a company. If this policy was in place, it would have helped with making sure that current clients that could have competitors that are potential clients of TechFite do not have access to the potential client’s sensitive information. Breaking up the grouping of clients putting every client and potential clients information into their own containers, help decrease the threats of intellectual property because not everyone will have access to the containers only certain employees would clients would only have access to their own container.

**B2. SATE Components**

The group that needs to manage this program is the Security team, but main oversight of it needs to be the CISO (Chief Information Security Officer) because they are highest position within the security team are going have most knowledge regarding external and internal security threats due to experience be able relay what needs to be talked about within the training.

As for who needs to take this training, every single person who is a part of TechFite, the reason for this because it does not matter whether you are in high level position or in a low-level position everyone has potential cause a security threat to the company needs to be aware of how to reduce the chance of that taking place.

**B2a. SATE Program Communication**

Emails should be sent out to all employees informing them that this training is required needs to be done, along with the email to all employee because not everyone reads there emails the department heads need to speak their employee inform of the training that it is required. If the training is not completed within the time frame and has not been completed, does not have vailed reason for not being completed, then possibility of termination needs to state within the email and passed along by the department heads.

**B2b. SATE Program Justification**

It was found that there was department who installed malicious software on their equipment and used it preform unauthorized penetration into various companies’ networks. If you are not a part of the Security and or a trained professional with pentesting certification and has been given authorization to be preforming pentesting, then that software should not be found on company equipment. Any unauthorized individuals from here on out, will be reported to authorities and will have legal consequences as they apply you will be immediately terminated form TechFite. This will help protect TechFite form any possible legal consequences that can come from unauthorized testing.

A potential client who decided to not go with are company, noticed that one of are current clients who there is competitor that produced a several similar products to what the disclosed in there NDA agreement when considering becoming a potential client. Let the employee know that insider trading is Illegal, and individuals found preforming will be punished according with possibility of termination. The information that is in are NDA agreements that we provided to are potential clients need to be upheld with upmost responsibility and is not shared with anyone outside of that client and agent that worked with beside the agent manager. This would be benefit TechFite because it helps with repairing their business reputation that has been damaged from the insider training that had taken place prior.

**C. Ethics Issues and Mitigation Summary for Management**

There where several ethical issues that have taken place that should been addressed appropriately but were not. An individual who is a head of department was importantly interacting with the Security Department, by buying them off with recommending glowing revies for creatin employee so that would gain raise when time came, inviting the employee to social gatherings outside of work providing them with gifts. This allowed for that employee to be indebted to feel need overlook malicious actives by the department head and individuals work with them in creating internal security threats. There needs to be separation of departments form the Security department beside required communication need to preform work, so that there is no further potential for the team and individuals of team to be bought off. The Security department also needs to start preforming proper steps for protecting the company form internal threats by setting up appropriate security policies. For instance, Auditing Policy needs to be in place so that no users of any department have access to admin rights if they have not been authorized to have it, along with make sure they not installing malicious software and or reaching out to third parties actively work providing services preforming malicious activities. Another example would be using the Chinese Wall Policy creating separation of information that way current and potential client’s information is gathered same place and has rules in place so specific individuals can access it only. Also need to have a Security training program awareness set up, so that individuals are aware of what potential security risk they could be causing how to avoid and prevent them for benefit of themselves and the company. It will be required by every individual within the company to take part in this training because everyone has potential to be a security risk. Starting out the training will be led by the CISO due to having most knowledge when comes to Security, they eventually distribute it to individuals with Security team but will keep watchful eye make sure proper topics are being covered. The process of how individuals will be notified through is with the companies email which each employee will have let them know that training is taking place and is required. Along with emails being sent to each of the department’s heads telling them that this training is required to speak to there employee letting them know there no excuse of not knowing about the training taking place. The training will cover important topics regarding security within the company, such as how to be protect against and help prevent and how to report on security incidents that individuals may notice. Making employee aware of social engineering tactics that bad actors actively use to gain sensitive information form them about the company for the social engineer’s benefit. Along with what is appropriate usage of company equipment, like what software is allowed to be installed on company equipment and using the companies’ electronical communications appropriately. This training will also make sure employees are aware of what will happen to their jobs if they do not follow appropriate procedures regarding the training and how could possibly lead them being terminated.

**References**

*Code of ethics: EC-Council*. EC. (2023, March 9). https://www.eccouncil.org/code-of-ethics/

Code of professional ethics: IS/it certifications. ISACA. (n.d.). <https://www.isaca.org/code-of-professional-ethics>

Annotate sources of any quoted, paraphrases or summarized content used. Delete this slide prior to submission if you have none to include. Delete the reference page/section if you do not have quoted, paraphrased, or summarized content.