

Reflective Review

During this module, I worked on a project relating to security and risk management. The goal was straightforward: identify and mitigate potential threats in our digital landscape. To help me reflect on my experience, I adopted the “What? So What? Now What?” model from Rolfe, Freshwater, and Jasper (2001). It provided a clear structure for my learning. In this review, I will cover four main areas:

1. Understanding the security and risk management process
2. My role in the team
3. My experience in the development group
4. How this impacted my professional and personal growth

1. Understanding the Security and Risk Management Process

What?

Initially, I recognized that the management of security and risk extends beyond mere technological considerations; it encompasses significant legal and ethical factors as well. In the context of this project, I conducted a risk assessment for a company named Pampered Pets as it progressed into the digital domain. I utilized methodologies such as FMEA (Failure Mode and Effects Analysis) and STRIDE, which assists in identifying potential threats. These analytical tools provided a comprehensive framework for assessing risks from various perspectives, including their probability of occurrence and potential severity.

So What?

A significant insight derived from my experience is that risk management is continually evolving rather than a singular task completed once. My initial assumption was that enumerating potential issues would be adequate. However, I quickly came to understand that new risks can emerge unexpectedly throughout any process. Thus, a successful approach to security management necessitates a degree of adaptability—consistently observing the operational environment and engaging with essential stakeholders. Additionally, I have come to appreciate that risk assessments should extend beyond basic technical solutions; fostering compliance and promoting user awareness are crucial components. This perspective is in alignment with the principles outlined in the University of Edinburgh’s Reflection Toolkit, which underscores the value of integrating varied viewpoints to effectively tackle intricate challenges.

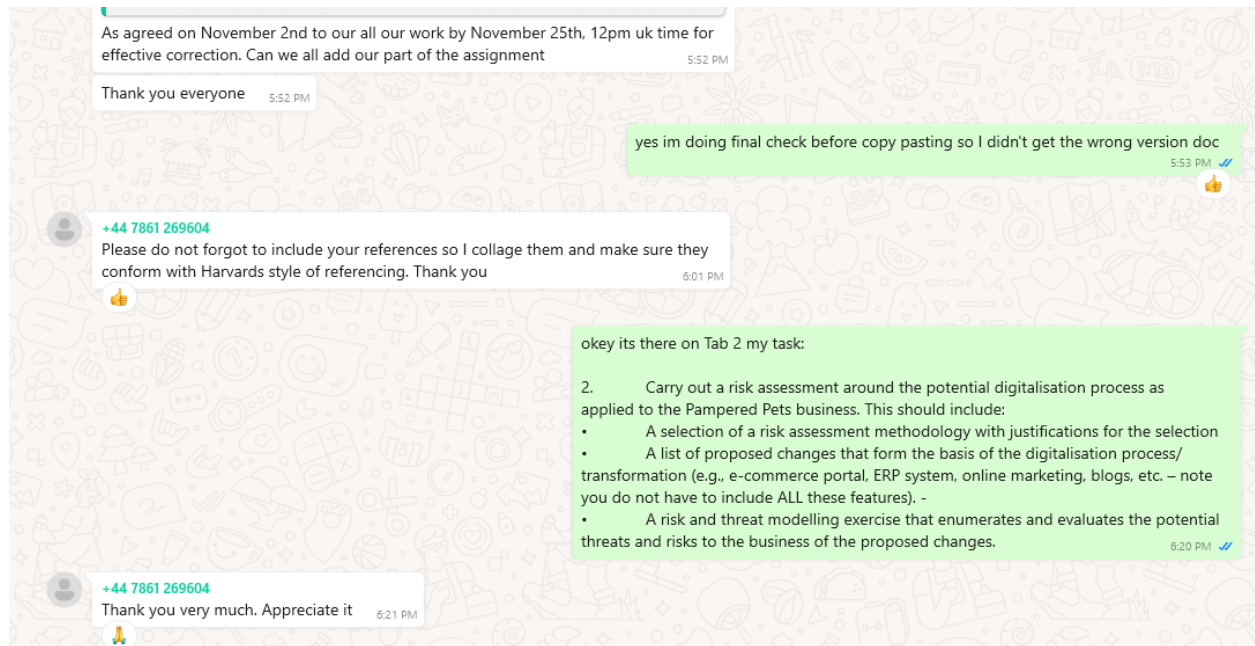
Now What?

Looking ahead, I intend to adopt a more proactive outlook in my risk assessments. I will consistently review emerging threats, seek feedback from my colleagues, and stay informed about reliable security developments. I plan to continue using FMEA and STRIDE, adapting these methods as necessary to handle new threats. Maintaining adaptability is essential when tackling the ever-evolving challenges in security.

2. My Role in the Team

What?

In my team, I chose to utilize FMEA and STRIDE and articulated their significance. I also recommended changes in sectors like e-commerce and online marketing. Furthermore, I developed a comprehensive plan for threat modeling. My primary duty encompassed identifying different risks and proposing appropriate solutions, including the implementation of penetration testing.



Identified Threats and Potential Mitigations					
STRIDE Category	Identified Threats	Likelihood	Impact	Priority	Potential Mitigations
Spoofing	Unauthorized access to the wireless network	high	Moderate	high	Secure Wi-Fi with WPA3 encryption and restrict access to authorized devices only.
Tampering	Alteration of warehouse inventory spreadsheets or transaction	medium	high	high	Use password-protected files and regular backups to prevent unauthorized changes
Repudiation	Lack of logs to track user actions, leading to disputes over errors	medium	moderate	medium	Implement basic logging systems on computers to track user activity and changes
Information Disclosure	Unencrypted emails exposing sensitive business or customer information	high	high	high	Enable <u>encryption</u> for all emails and sensitive data transmitted over the network.
Denial of Service (DoS)	Wireless network disruptions due to overuse or external attacks	low	high	medium	Set up network monitoring tools to detect and address abnormal traffic patterns.

So What?

Undertaking these tasks heightened my sense of accountability. I realised that the methods I chose needed to work not just theoretically but also in real-world settings. By frequently sharing my findings and remaining open to feedback, I was able to refine our assessments. This helped the team address both technical and business considerations, thus strengthening the overall project outcome.

Now What?

In future, I will continue promoting clear, data-informed approaches to risk assessment. Additionally, I aim to keep communication channels open within the team, as constructive feedback proved pivotal in enhancing our work.

3. Experience in the Development Team

What?

The composition of our team included members with a broad range of expertise spanning marketing and IT sectors. At the outset, we encountered difficulties in reconciling conflicting priorities, notably the tension between user experience and security considerations. Nevertheless, by implementing a structure of regular meetings and fostering open dialogue, we were able to define shared goals and delineate individual responsibilities clearly.

So What?

This experience reinforced the critical importance of effective communication. I discovered that breaking down complex security topics into accessible language enabled broader participation. Drawing on each member's strengths resulted in a more robust risk management plan. By the midpoint of the project, collaboration felt more natural, and everyone's contributions were valued, thereby boosting overall teamwork.

Moreover, I realised the impact of emotional intelligence in reconciling contrasting opinions. By fostering empathy and an open mind, we navigated disagreements in a constructive manner. Rolfe et al. (2001) point out that reflecting on such challenges is essential for continuous learning and growth.

Now What?

Building on these insights, I will strive to maintain transparent communication and create a supportive environment where everyone's voice can be heard. Whether I am leading or assisting, I aim to set clear objectives and enable team members to play an active role.

4. How This Project Helped Me Grow

What?

This project helped me be more flexible. In cybersecurity, things change fast. Plans that are too strict don't work well. My experience in customer support and working with data protection for governments and big companies gave me the confidence to link security work to bigger business goals.

So what?

Focusing on strong data protection and good communication with clients has helped me grow my skills. Working with important organizations in regulated fields showed me how crucial it is to be resilient, communicate clearly, and offer custom solutions. Handling urgent tasks and different risks taught me that putting the customer first is key to keeping trust and making sure everything runs smoothly.

Now what?

Going ahead, I'll work on communicating tricky security topics to different groups. I want to make sure clients, from government agencies to big companies, feel well-supported and up to date. Keeping strong ethics and putting user needs first will stay central to my work. This will help me provide solutions that protect important areas while keeping up with business needs.

Conclusion

This module and the related project have altered my understanding of security and risk management. I have come to view these areas as continuous and proactive responsibilities. My participation—especially in choosing methodologies and creating threat models—played a crucial role in defining the project's security strategy. Working with a diverse team enabled me to enhance my communication and teamwork skills. Furthermore, this experience has made me more adaptable and committed to ongoing education in cybersecurity. As I progress in my career, I feel better prepared to address the evolving challenges of information security.

References

- Rolfe, G., Freshwater, D., & Jasper, M. (2001). *Critical reflection in nursing and the helping professions: a user's guide*. Basingstoke: Palgrave Macmillan.
- The University of Edinburgh. (n.d.). *Reflection Toolkit*.
- UoEO. (n.d.). *Short Guide to Reflective Writing*.