**Unit 2 Seminar Preparation:**

The Scrum agile life cycle consists of several key stages, each aimed at delivering a product incrementally and iteratively. The stages are as follows:

1. **Product Backlog Creation**:
    - A prioritized list of features, enhancements, and bug fixes required for the product. It is maintained by the Product Owner.
2. **Sprint Planning**:
    - A meeting where the team selects items from the Product Backlog to work on during the upcoming sprint (typically 2-4 weeks long). The team defines the Sprint Goal and the work to be done.
3. **Sprint**:
    - A time-boxed period during which the team works on the selected backlog items. The goal is to deliver a potentially shippable product increment at the end of the sprint.
4. **Daily Standup (Daily Scrum)**:
    - A short, daily meeting where the team members discuss their progress, plans for the day, and any impediments they face. It helps keep the team synchronized and identifies any issues early.
5. **Sprint Review**:
    - A meeting held at the end of the sprint where the team demonstrates the work completed during the sprint to stakeholders. Feedback is gathered, and the Product Backlog is updated accordingly.

6. **Sprint Retrospective**:

    - A meeting held after the Sprint Review where the team reflects on the sprint's process, what went well, what could be improved, and how to make the next sprint more effective.

7. **Increment**:

    - The sum of all completed Product Backlog items during a sprint, including the increments of all previous sprints. The Increment must be in a usable condition, regardless of whether the Product Owner decides to release it.

| SCRUM STAGE | Recommended Security Processes (Based on Sharma & Bawa, 2020) |
|---|---|
| PRODUCT BACKLOG | - **Security Activity Selection**: Use empirical methods (e.g., AHP, PROMETHEE, ANN, Fuzzy Logic) to select appropriate security activities tailored to project needs.<br><br>- **Security Requirements**<br><br>- **Threat Modelling**<br><br>- **Incorporation of CLASP and Microsoft SDL Activities**: Include selected lightweight security activities from CLASP and Microsoft's SDL that do not compromise agility.<br><br>- **Stakeholder Requirement Analysis**: Consider the security needs of all stakeholders, including customers, team members, and project analysts. |

| | |
|---|---|
| **SPRINT PLANNING** | - **Integration of Selected Security Activities**: Integrate lightweight security activities into the sprint plan, ensuring they align with the agile nature of Scrum.<br><br>- **Security Prioritization**: Prioritize security tasks based on risk assessment and the frequency of use, as suggested by Microsoft's SDL. |
| **SPRINT** | - **Implementation of CLASP Activities**: Apply security activities from CLASP that can be performed independently and do not require a sequential approach.<br><br>- **Continuous Monitoring and Adjustment**: Dynamically adjust security activities based on real-time feedback and project requirements without hindering agility.<br><br>- **Automation of Security Processes**: Utilize automated tools to implement security activities, such as static code analysis, to maintain agility. |
| **DAILY STANDUP** | - **Security Status Updates**: Regularly update the team on the progress of security activities and any emerging security concerns. |
| **SPRINT REVIEW** | - **Review and Assessment of Security Features**: Evaluate the effectiveness and completeness of implemented security activities during the sprint.<br><br>- **Feedback Loop**: Collect feedback on security implementations and integrate it into future sprints. |
| **SPRINT RETROSPECTIVE** | - **Analysis of Security Practices**: Reflect on the security practices used during the sprint and identify areas for improvement.<br><br>- **Adjustments Based on Feedback**: Modify security activities based on retrospective analysis to improve future implementation. |

| | |
|---|---|
| **PRODUCT INCREMENT** | - **Comprehensive Security Evaluation**: Conduct a thorough review and evaluation of the integrated security activities and their impact on the product.<br><br>- **Documentation and Reporting**: Document all security activities, findings, and resolutions for future reference and compliance. |
| | - **Final Security Validation and Verification**: Perform final validation of security measures, including testing and review, ensuring all security requirements are met.<br><br>- **Secure Deployment Planning**: Plan and execute a secure deployment strategy, incorporating any necessary security configurations and hardening measures. |
| **POST RELEASE** | - **Ongoing Security Monitoring**: Establish continuous monitoring for potential security incidents and implement an incident response plan.<br><br>- **Security Patching and Maintenance**: Ensure a process for regular security updates and maintenance is in place to address any vulnerabilities that may arise.<br><br>- **User Security Training**: Provide training and awareness to end-users on security best practices and the importance of maintaining secure systems. |

**BLOG POST:**

The results presented here suggest that organizations can mitigate their cyberattack risks by ensuring that employees have appropriate training, understand establish security metrics, have general cybersecurity awareness, and become a part of a culture that embraces the benefits of cybersecurity. It is up to organizational leadership to set the tone when it comes to the culture of cybersecurity awareness. Investing in cybersecurity awareness and knowledge development is the

best way to create sustainable behavioral change (Pavlova, 2020). By placing employees into real-world situations with training and awareness programs organizations can gain valuable knowledge that helps them set up effective countermeasures to mitigate risk (Resnik & Finn, 2018). Most individuals want to do the right thing and perform their job duties well, but organizational leadership must place a focus on developing their employees the right way. Human behavior is a problem in cybersecurity that must be addressed and no matter how many safeguards are put into place those measures can always be compromised by human behavior (Scala et al., 2019).

**Managing Human Risk in Cybersecurity: Key Terms and Strategies**

In cybersecurity, human factors play a pivotal role in the overall security of an organisation. Drawing from the ISO/IEC Standard 27000 (2018), this blog post explores five key terms—Threat, Vulnerability, Threat, Attack and Performance—and how they relate to mitigating cybersecurity risks.

A **Threat** is an unwelcome incident which occurs when employee(s) accidentally or purposefully tries to breach security or access sensitive data (ISO/IEC 27000, 2018). As a solution, Elmrabit et al. (2020) proposed the Bayesian Network-based model, which predicts malicious threats before the organisation's security is compromised. This model helps identify potential attack paths and security breaches, thereby providing proactive threat management.

An **Attack** is one step further than a threat, where a user maliciously exploits a system's weaknesses to compromise the organisation (ISO/IEC 27000, 2018). Inside attacks are particularly challenging because they bypass external security measures. To prevent this, user activities need to be monitored, alongside the implementation of regular security audits and strong access controls (Fonseca-Herrera et al., 2021).

**Vulnerability** is when an organisation has systematic weaknesses, like poor training or policy gaps, making them exploitable (ISO/IEC 27000, 2018). Minimising these vulnerabilities includes conducting frequent assessments and security protocols (Sharma & Bawa, 2020). This will reduce the organisation's weaknesses and strengthen their safety against cybercriminals.

**Information Security** is the protection of an organisation's information from being accessed, edited or deleted by unauthorised users (ISO/IEC 27000, 2018). Fonseca-Herrera et al. (2021) proposed a recent model that alerts organisations of their information security status, and enables them to systematically incorporate strict policy adherence and regular employee training. Adopting these kind of models can safeguard systems from cyberattacks.

Finally, **Performance** is how well an organisation's security system is protecting their assets (ISO/IEC 27000, 2018). To ensure security performance is at its peak, companies need to regularly assess, review and update their security software (Fahrurozi et al., 2020). This requires diligent maintenance and ensures an organisation's security status remains strong.

By focusing on these key terms, organisations can better manage the human elements that contribute to cybersecurity risks.

**References:**

Elmarit, N., Yang, S., Yang, L., Zhou, H. (2020) Insider threat risk prediction based on Bayesian Network. *Computers & Security* 96: . DOI: https://doi.org/10.1016/j.cose.2020.101908

Fahrurozi, M., Tarigan, S., Alam Tanjung, M., & Mutijarsa, K. (2020) 'The Use of ISO/IEC 27005: 2018 for strengthening information security management (A case study at Data and Information Center of Ministry of Defence)', *12th International Conference on Information Technology and Electrical Engineering (ICITEE).* Yogyakarta, Indonesia, December. 86–91.

ISO/IEC 27000. (2018) Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 6 August 2024].

Fonseca-Herrera, O., Rojas, A., & Florez, H. (2021) A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science* 48(2): [no pagination].

Sharma, A, & Bawa, R. (2022) Identification and integration of security activities for secure agile development. *Springer* 14(2): 1117-1130. DOI: https://doi.org/10.1007/s41870-020-00446-4