# What Are Your Crown Jewels?

# Identification and Classification of Crown Jewels

# Assemble the Team

- **Key Stakeholders**
    - Involve representatives from IT, legal, finance, and business units.
- **CISO (Chief Information Security Officer)**
    - Leads the process and provides security expertise

# Define the Criteria

- **Business Impact**
  - Consider the consequences of losing confidentiality, integrity, or availability of an asset. (e.g., loss of revenue, reputational damage)
- **Regulatory Compliance**
  - Identify assets subject to specific regulations (e.g., HIPAA for healthcare data)
- **Intellectual Property (IP)**
  - Protect trade secrets, product designs, and other forms of IP

# Data Gathering and Mapping

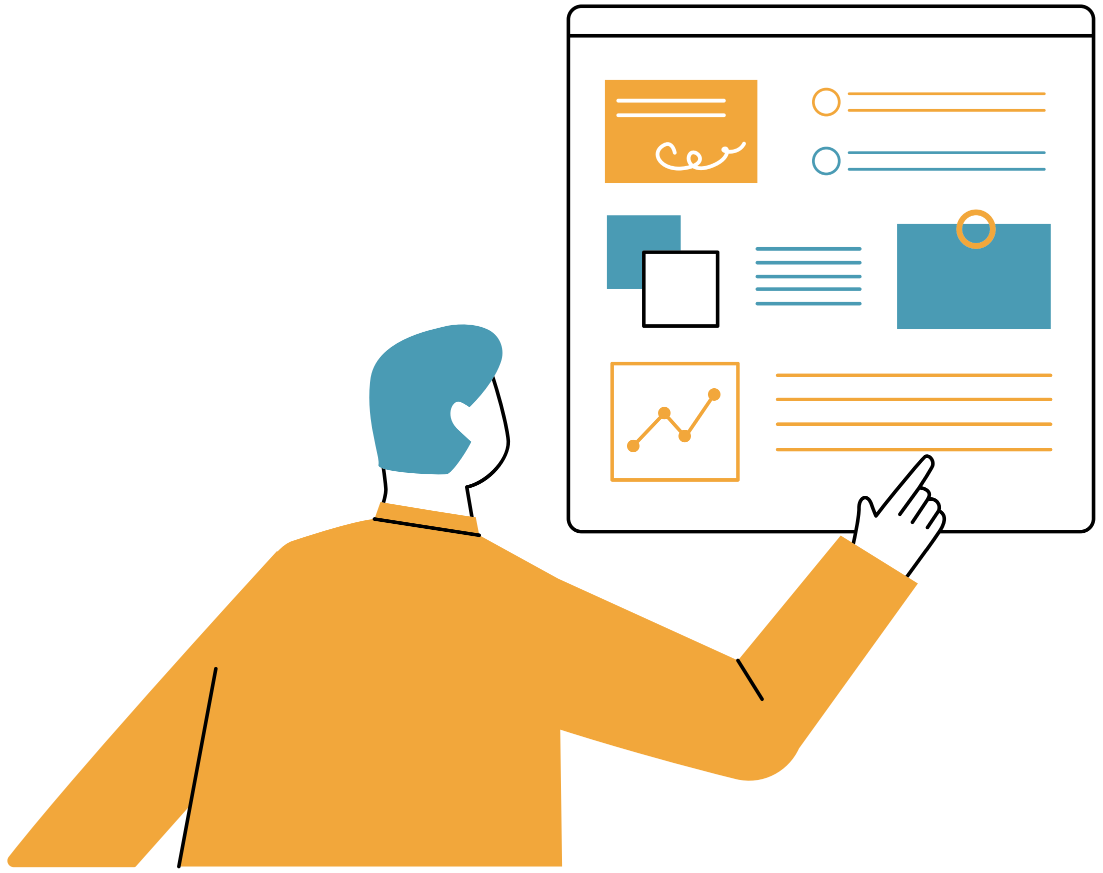
- **Inventory Assets**
  - Create a comprehensive list of all data, applications, systems, and infrastructure.
- **Data Lifecycle Mapping**
  - Understand how data flows through your organization, where it's stored, and who has access.

LSU

# Classification and Prioritization

- **Develop a Classification Scheme**
  - Categorize assets based on the defined criteria (e.g., High, Medium, Low)

- **Prioritize Crown Jewels**
  - Identify the assets with the highest impact if compromised



LSU

# Document and Maintain

- **Document Your Findings**
  - Create a formal report outlining the identified crown jewels and their classification.

- **Regular Reviews**
  - Schedule periodic reviews to update the classification based on changes in the business or regulatory

# Risk Assessment & Prioritization

# Seeing What Could Go Wrong

**Heading into the Danger Zone: Understanding Risk Assessment**

- We've identified our Crown Jewels - the vital assets that keep our business running smoothly. But just like any treasure, they need protection.
- In this section, we'll enter the world of Risk Assessment, where we explore potential threats to our Crown Jewels.

# What is a Risk?

**Identifying the Threats: Different Types of Risks:**

- A **risk** is any event that could negatively impact our Crown Jewels. These events can be:
  - **Accidental:** Hardware failure, human error, natural disasters
  - **Intentional:** Cyberattacks (hacking), theft, sabotage

- Risks can cause various problems for our business:
  - **Financial loss:** Data breaches, service disruptions
  - **Reputational damage:** Loss of customer trust, negative publicity
  - **Operational disruptions:** System outages, data loss

# Assessing Your Risks: Likelihood vs. Impact

**Prioritizing the Threats: The Risk Assessment Matrix**

- To understand the seriousness of a risk, we need to consider two factors:
  - **Likelihood:** How probable is it that the risk will occur (e.g., Daily power fluctuations vs. Targeted hacking attempt)
  - **Impact:** How severe would the consequences be if the risk did occur (e.g., Minor data loss vs. Complete system shutdown)

- A risk assessment matrix helps us visualize these factors and prioritize our concerns**.**
  - **High Impact, High Likelihood (Urgent):** These are the biggest threats - address them first! (e.g., Unsecured Wi-Fi network)
  - **High Impact, Low Likelihood (Prepare):** Be prepared for these potential threats. (e.g., Physical security breach)
  - **Low Impact, High Likelihood (Monitor):** Keep an eye on these less severe but frequent risks. (e.g., Accidental data deletion)
  - **Low Impact, Low Likelihood (Accept):** These pose minimal risk, so focus on the higher priorities. (e.g., Occasional printer malfunctions)

# Taking Action: Mitigate, Transfer, or Accept

**Defending Our Crown Jewels: Risk Mitigation Strategies**

- Once we've assessed our risks, it's time to take action and become cybersecurity champions! Here are some common approaches:
  - **Mitigate:** Reduce the likelihood or impact of a risk. (e.g., Implement strong passwords, data backups)
  - **Transfer:** Share the risk with another party (e.g., Purchase cyber insurance to cover some costs of a data breach).
  - **Accept:** Decide to live with the risk if the cost of mitigation is too high. (e.g., Accepting a low risk of occasional software glitches in a non-critical system)

- We'll prioritize our actions based on the severity of the risk. High-impact risks require strong mitigation strategies, while lower-risk situations might be addressed through a combination of approaches.

# Protection Strategies for Technology & Data

# Importance of Protection

- Technology and data are **critical assets** for organizations which is why they need to be protected
- Financial losses, reputational damages, and legal consequences can be **results of a data breach**
- In order to keep up the trust from customers **protection strategies are necessary**

# Key Threats

- Malware
- Phishing
- DDos Attack
- Zero-Day Exploits
- Social Engineering
- Insider Threats
- Data Breaches

# Protection Strategies

**A protection strategy should involve:**

- **Risk Assessment:** Identifying/assessing potential risks, vulnerabilities, and threats
- **Control Implementation:** To mitigate identified risks and to enhance security
- **Incident Response Plan:** To implement and develop procedures
- **Compliance and Governance:** To be compliant with laws, regulations, and standards
- **Training and Awareness:** To educate about risks and practices
- **Monitoring and Detection:** To detect potential risks and threats

# Key Protection Strategies

- **Encryption:** To prevent unauthorized access to sensitive data
- **Compliance Frameworks:** Ensure legal and regulatory compliance (HIPAA, GDPR, etc…)
- **Data Backup:** Regular backups ensure the availability of data in case of an incident
- **Access Controls:** To restrict unauthorized access to sensitive data
- **Regular Updates:** Keep software and operating systems up to date
- **Employee Training:** Provide training on security practices, develop and implement an Incident Response Plan

# Cybersecurity Measures & Incident Response

LSU

# The Importance

- We will delve into strategies and best practices to defend against cyber threats and mitigate damage during a cyber attack

- The focus will be on practice measures and effective incident response to ensure the security of your most critical assets

- By having an effect incident response plan you will be able to quickly get back on your feet after an attack and stop damages as soon as possible

LSU

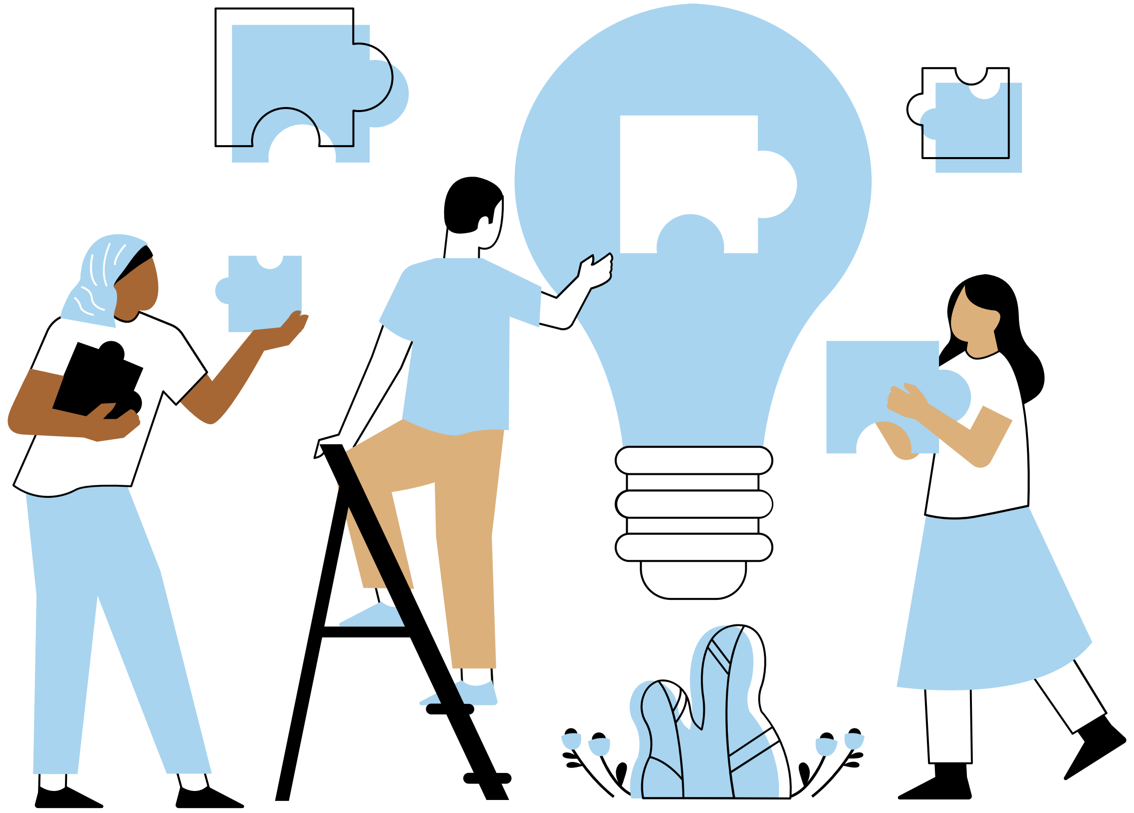
# Understanding Cybersecurity Measures

- Cybersecurity measures encompass a range of techniques and practices aimed at protecting systems, networks, and data from cyber threats
- Essential for preventing breaches and minimizing impact
- Different types of cyber security measures include
  - Network security
  - Endpoint security
  - Access controls
  - Encryptions
  - Security awareness training

# Cyber Security Measures

- **Network Security**
  - Involves implementing measures to protect the organization network infrastructure from unauthorized access, data breach, and other cyber threats
  - Ex. Implement firewalls, intrusion detection systems, intrusion prevention systems to monitor and control network traffic

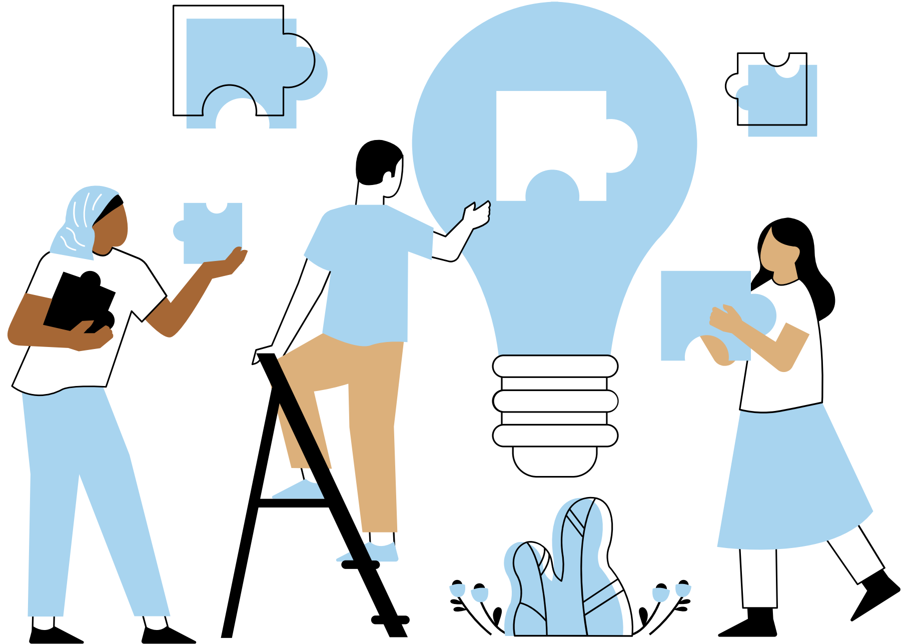
- **Endpoint Security**
  - Endpoint security focuses on securing individual devices such as computers, laptops, smartphones, and tablets from cyber threats
  - Ex. Deploy antivirus software, endpoint detection and response solutions, and mobile device management platforms to protect endpoints from malware, ransomeware, and other malicious activities



# Cyber Security Measures

- **Access Controls:**
  - This restricts and monitors access to sensitive data, systems, and resources to prevent unauthorized users from accessing or modifying them
  - Ex. Implement role-based access control, and multi-factor authentication to limit the risk of an authorized user gaining access to sensitive data

- **Encryption:**
  - Involves converting data into a secure format to prevent unauthorized access or interception by malicious parties
  - Ex. Encrypt sensitive data in rest or in transit by using encryption algorithms such as Advanced Standard and Transport Layer Security



# Security Awareness Training

- Security awareness training plays a crucial role in educating employees about cyber risks and best practices which can prevent a loss in your business

- Providing phishing awareness training to help employees recognize and report suspicious emails, and conduct simulated exercises to assess readiness

- Continuous training and reinforcement are essential to ensure employees remain aware of ever evolving cyber threats

# Proactive Monitoring

- Involves continuously monitoring networks, systems, and applications for signs of suspicious activity

- Tools such as intrusion detection systems (IDS), Security information and event management systems (SIEM), and endpoint detection and response solutions (EDR) are used for proactive monitoring

- Real time monitoring allows organizations to detect and respond to threats promptly, reducing the likelihood of successful attacks

# Incident Response Planning

- Involves developing a structured approach for responding to cybersecurity incidents
- This should outline roles and responsibilities, communication protocols, and containment/ eradication strategies
- An effective plan will coordinate their response efforts and minimize impact of security incident for a quick recovery

LSU

# Final Thoughts on IRP

- Proactive cybersecurity measures and effective incident response are essential for protecting Crown Jewels and mitigating cyber risks

- By implementing strong cybersecurity measures and developing a comprehensive incident response plan, organizations can strengthen their defenses against cyber threats.

- We encourage continued adaptation to emerging cyber threats to safeguard sensitive data and valuable assets