SRINIX COLLEGE OF ENGINEERING

Department of Computer Science & Engineering

We Represented the topic on

CYBERSECURITY: Your Imperative in the Digital Age

Presented By:-

Pabitra Nayak(Reg No.: 2421331053)
Suzen Ku. Mohanty(RegNo.:2421331063)
Sugith Saha (Reg No.: 2421331060)
Manish Ku. Panda (RegNo.:2301331056)
Papulu Maity(Reg No.: 2421331054)
Rupak Ku. Nayak (Reg No.:2421331058)

Guided By:

Mr. Mihir Kumar Behera
Asst.Professor,Dept of CSE
Srinix College Of Engineering

Overview of CyberSecurity:

- THE GLOBAL LANDSCAP
- COMMON CYBER ATTACK VECTORS
- OUR FIRST LINE OF DEFENSE
- SECURING NETWORKS AND DEVICES
- DATA PRIVACY AND COMPLAINCE
- INCIDENT RESPONDS
- HUMAN FACTORS
- EMERGINH THREAT
- BUILDING DIGITAL RESILIENCE
- CONCLUSION
- REFERENCES
- ANY QUESTION
- THANK YOU

The Global Threat Landscape: Understanding Who's Attacking and Why

- Cyber threats are no longer just an IT issue—they are a serious business risk.

Different attackers have different goals:

- **State-sponsored groups** try to steal information or disrupt important systems.
- **Cybercriminals** want money, often through ransom ware or stealing data.
- **Activists (activists)** aim to damage reputations or promote their beliefs.
- Understanding these different threats helps us build better protection.

Common Cyber Attack Vectors: Phishing, Malware, and Beyond

Phishing & Social Engineering

Deceptive emails or messages tricking users into revesling sensitive information or clicking mavicious links.

DDoS Attacks

Overwhelming & system with traffic to disrupt its normal operations, making services unavailable.

Malware & Ransomware

Haarmful softw&re designed to disrupt systems, steal data, or encrypt files until & ransom is paid.

Insider Threats

Malicious or negligent actions by current or former employees with access to sensitive systems.

OUR FIRST LINE OF DEFENS: STRONG PASSWORDS AND MULTI FACTOR AUTHENTICATION

Weak credentials are a primary entry point for cyber attackers. Strong, unique passwords for every account are fundamental. A combination of upper and lowercase letters, numbers, and symbols significantly increases security. Avoid using easily guessable information like birthdays or names. Password managers can help maintain complex, unique passwords without memorization.

Multi-Factor Authentication (MFA) adds a crucial second layer of security, requiring an additional verification step like a code from your phone or a biometric scan. This makes it significantly harder for unauthorized users to access accounts, even if they have your password.

Securing Networks & Devices: Firewalls, Antivirus, and Regular Updates

Firewall Protection

Acts as a barrier between your network and external threats, controlling incoming and outgoing network traffic.

Antivirus & Anti-Malware

Essential software that detects, prevents, and removes malicious software from your devices.

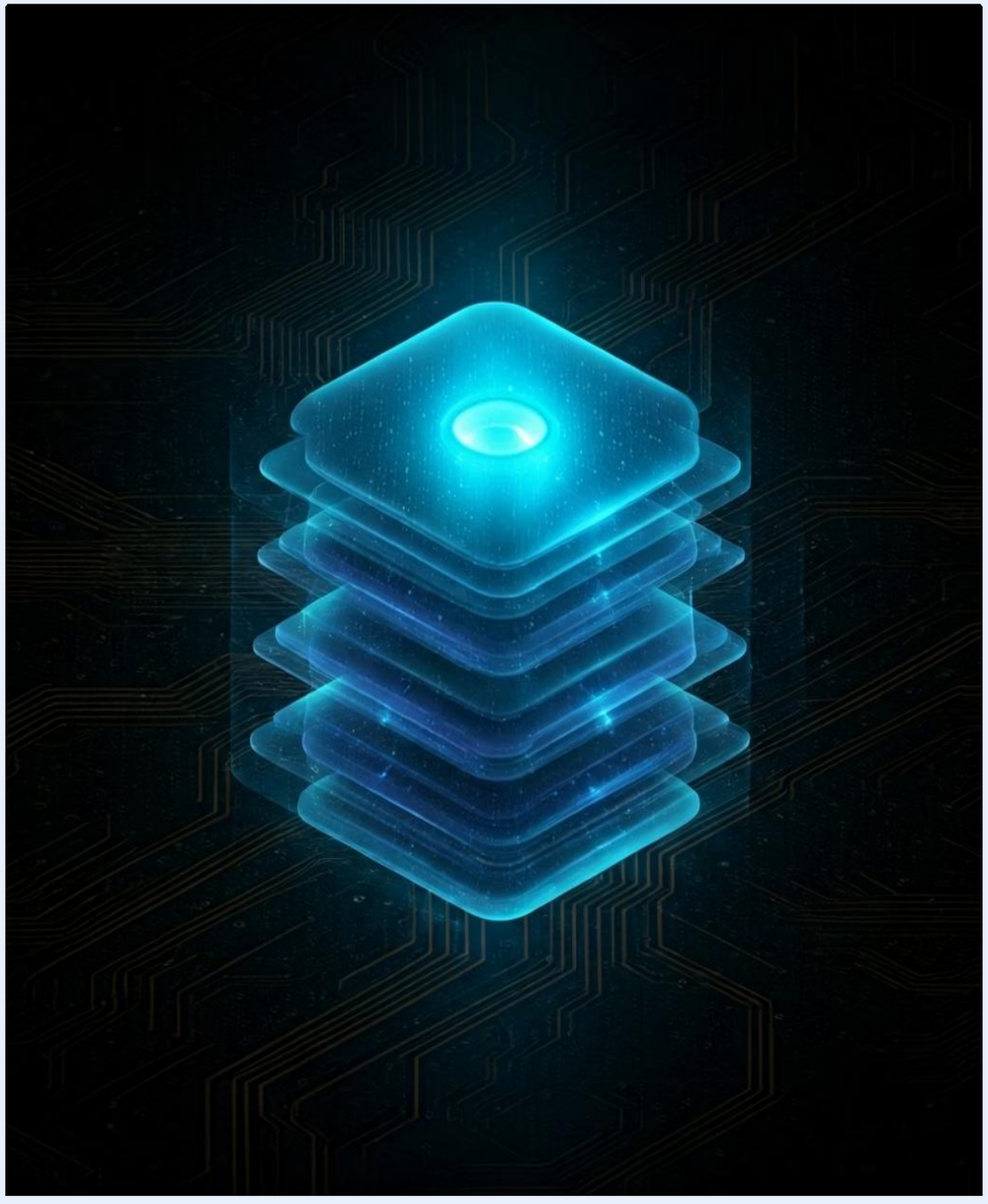
Regular Software Updates

Patching known vulnerabilities in operating systems and applications is crucial to prevent exploitation.

Network Segmentation

Dividing a network into smaller, isolated segments limits the spread of threats if a breach occurs.

DATA PRIVACY AND COMPLIANCE: PROTECTRING WHAT MATTERS MOST



Identify Sensitive Data: Know what data you collect, where it's stored, and who has access.

Access Controls: Implement strict permissions based on the principle of least privilege.

Encryption: Encrypt data both in transit and at rest to prevent unauthorized access.

Regulatory Compliance: Adhere to regulations like GDPR, CCPA, and HIPAA to avoid penalties and build trust.

Data Minimization: Collect and retain only the data necessary for your operations.

Incident Response: What To When a Breach Occurs

Preparation

Develop a detailed incident response plan, including roles, responsibilities, and communication protocols.

Identification

Detect the incident quickly, determine its scope, and isolate affected systems to prevent further damage.

Containment & Eradication

Stop the attack from spreading and remove the threat, ensuring all vulnerabilities are patched.

Recovery

Restore affected systems and data from backups, ensuring full operational capability.

The Human Factor: Building a Security-Conscious Culture

Employees are often the weakest link in cybersecurity, but they can also be your strongest defense. Regular and engaging security awareness training is paramount. Teach staff to recognize phishing attempts, understand password best practices, and report suspicious activities without fear of reprisal.

Foster a culture where security is everyone's responsibility, not just IT's. Encourage open communication about potential threats and reinforce the importance of vigilance through ongoing campaigns and simulated phishing exercises.

Emerging Threats: AI, IoT, and the Future of Cyber Warfare

Artificial Intelligence (AI)

AI can enhance both defenses and attacks. Malicious AI could generate sophisticated phishing, automate malware creation, and rapidly exploit vulnerabilities.

Internet of Things (IoT)

The proliferation of IoT devices creates vast new attack surfaces. Many IoT devices lack strong security, making them vulnerable to compromise and botnet information.

Building Digital Resilience: Key Takeaways and Your Next Steps

Prioritize Proactive Defense

Implement l&yered security me&sures, strong &authentic&tion, &nd regul&r upd&tes &s & found&tion.

Empower Your People

Invest in continuous security &w&reness tr&ining to tr&nsform employees into &ctive defenders.

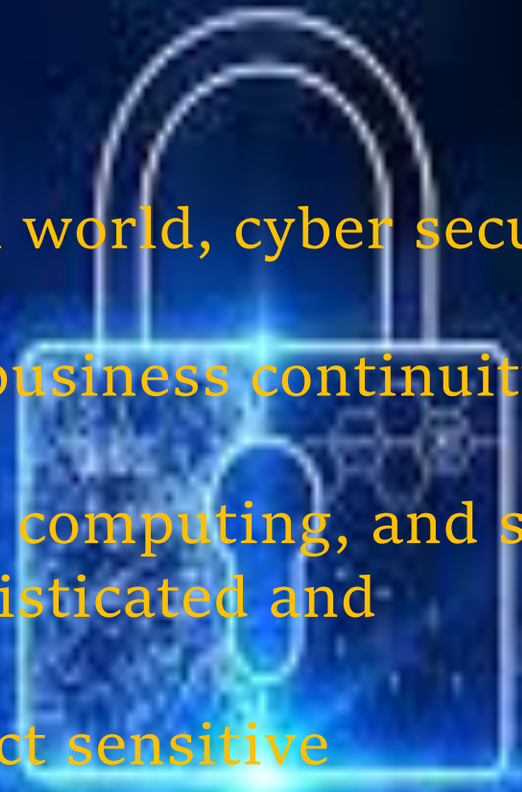
Plan for the Unthinkable

Develop & robust incident response pl&n to minimize d&m&ge &nd ensure swift recovery from bre&ches.

Stay Vigilant & Adapt

Continuously monitor the thre&t l&ndsc&pe &nd &d&pt your str&tegies to counter emerging cyber risks.

Conclusion :



- Cyber security In today's increasingly digital world, cyber security is not just a technical necessity
- t is a critical component of personal safety, business continuity, and national security.
- With the rapid growth of the internet, cloud computing, and smart devices, cyber threats have become more sophisticated and widespread.
- Effective cyber security measures help protect sensitive information, maintain trust, and ensure the smooth functioning of systems and services.

References:-

Include proper citations of :

- NIST (https://www.nist.gov/cyberframework)
- ISO (https://www.iso.org/isoiec-27001-information-security.html)
- Government CERTs
- Scholarly articles and whitepapers


WHEN?
HOW?
WHERE?
WHO?
WHAT?
WHEN?
WHAT?
WHERE?
WHERE?
WHAT?
When?
WHEN?
What?
HOW?
Where?
When?
WHERE?
ANY
WHERE?
What?
QUESTIONS?
What?
When?
When?
Why?
WHEN?
When?
Where?
WHAT?
When?
WHERE?
When?
When?
Why?
HOW?
WHAT?
When?
WHEN?
Why?
WHERE?
When?
Why?
HOW?
What?
Why?
HOW?


thank
you