NAME – Gaurav Kewalramani
Student Id – 14126543

Asset Register ->

Confidentiality Criteria (How sensitive or private is the data) - Confidentiality refers to protecting the data from unauthorized access or disclosure.

Scoring criteria
1 -> Data is non-sensitive, public, and has no repercussions if accessed by unauthorized parties (e.g., public info)

2 -> Low sensitivity; unauthorized access would cause minor harm (e.g., general training materials)

3 -> Moderately sensitive; unauthorized access may cause reputational damage or mild privacy concerns

4 -> Highly sensitive; includes identifiable information, but consequences of exposure are limited to specific users

5 -> Extremely sensitive; involves PII, financial data, or mission-critical intellectual property (e.g., student data)

Integrity Criteria (How critical is accuracy and consistency of the data) - Integrity ensures that data or systems are not tampered with or altered in unauthorized ways

1 -> Integrity is not a concern; minimal to no harm if data is altered (e.g., generic resource lists)

2 -> Low integrity requirements; errors in data would cause only slight inconvenience (e.g., training docs)

3 -> Medium-level impact; data alterations could lead to operational issues but not catastrophic failures

4 -> High-level impact; incorrect or altered data could result in significant harm, breaches of trust, or inefficiency

5 -> Critical-level impact; tampered data could endanger safety, disrupt operations, or cause regulatory/legal issues

Availability: This ensures that the information and systems are accessible and functional when needed. For SPYONU, this means ensuring that students, teachers, parents, and school management can always access the relevant applications (e.g., SSAP, SPAP, STAP) and that there is no downtime or disruption in critical school processes such as assessments, timetables, and communication systems.

5 -> Used for systems that must always be available to ensure operations (e.g., databases, communication systems, backup systems).

4 -> For systems that are important and require near-continuous availability (e.g., access logs, API integrations).

3 -> For systems that have a moderate need for availability but can tolerate some downtime (e.g., training materials, policies).

2 -> For systems that don't require constant availability and can afford downtime (e.g., behavioral data, social media data).

1 -> For systems where downtime does not impact operations significantly (e.g., some security protocols).

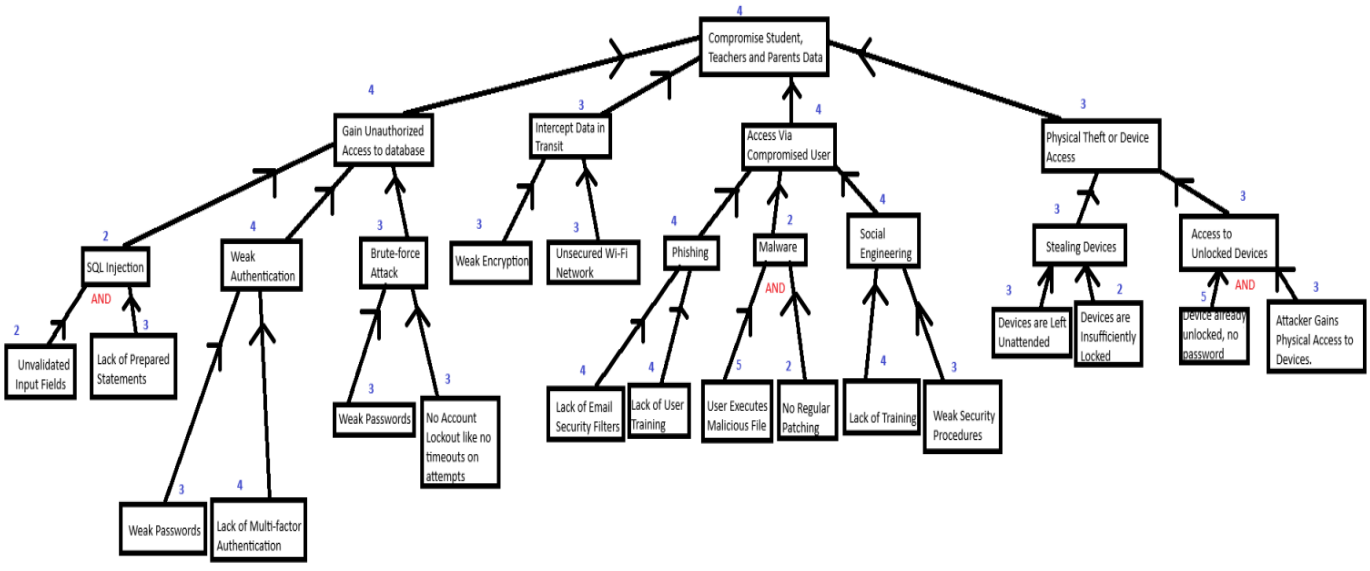
Asset	Description of the Assets (explaining Assets in depth)	Owner	C	I	A	Total
Student Data	Attendance, grades, behavioral records, dietary needs, financial details, and personal information.	Data Protection Officer (DPO) of the school	5	5	4	14
Teacher Data	PEDRP, lesson plans, personal identifiers, performance data, interaction records.	HR Manager of the school	4	5	4	13
Parent Contact Information	Parent/guardian details (phone, email, address, financial records for payment tracking).	Customer Service Manager of the school	5	4	3	12
School Financial Data	Payment data (school lunches, trips, fees), tied to parent accounts and banking/payment systems.	Finance Director of the school	5	5	4	14
SPYONU AI Algorithm	Core AI logic responsible for predictions, recommendations, mood analysis, etc.	CTO (Chief Technology Officer) of AI-City Software Limited	4	5	3	12
SPYONU Mobile Apps	Interfaces for students, parents, and teachers with extensive data interconnectivity.	Mobile App Development Lead of AI-City Software Limited	3	3	4	10
SPYONU Central Database	Main repository for all SPYONU data, including sensitive student/teacher/parent records and real-time interactions.	Database Administrator of AI-City Software Limited	5	5	4	14
Social Media Data	Data from Facebook, Instagram, TikTok, etc., analyzed for patterns like mood swings, risks of harm, and career advice.	Data Analyst Team Lead of AI-City Software Limited	3	3	4	10

Communication System	Internal and external messaging system between staff, parents, and students.	IT Network Administrator AI-City Software Limited	4	3	5	12
Backups	Stored copies of critical SPYONU data and configurations to ensure resilience against ransomware and data loss.	IT Security Manager of AI-City Software Limited	4	5	4	13
Access Logs	Logs recording every interaction with SPYONU's systems, detailing user actions, system changes, and data access.	Security Operations Manager of AI-City Software Limited	5	5	4	14
SPYONU System Data	Logs, application data, user activity data, etc., generated by the SPYONU system.	Data Manager AI-City Software Limited	5	5	5	15
Teacher Training Materials	Documents and resources to train teachers on using SPYONU.	Database Administrator of AI-City Software Limited	2	4	3	9
Student Training Materials	Resources for training students on using SPYONU.	Partially both school and AI city company is responsible but in this case I'll say the software company is more responsible for keeping the data	2	4	2	8
Parent Training Materials	Resources to guide parents in using SPYONU.	Partially both school and AI city company is responsible but in this case I'll say the software company is more responsible for keeping the data	2	4	2	8
Application Access Credentials	User credentials for accessing SPYONU (teachers, staff, parents).	Partially both school and AI city company is responsible but in this case I'll say the software company is more responsible for keeping the data	5	5	3	13

SPYONU API Integration Data	Data transferred between SPYONU and other systems or applications	Mobile App Development Lead of AI-City Software Limited	4	4	4	12
Student Behavioural Data	Data on student behaviour and emotional status.	Data Protection Officer (DPO) of the school	5	5	3	13
School Policies and Procedures	Documents outlining school rules, behaviour policies, and SPYONU usage.	Data Protection Officer (DPO) of the school	3	4	3	10
Security Protocols (e.g., VPN, Encryption)	Measures to protect data during transmission and storage.	IT Security Manager of AI-City Software Limited	5	5	5	15
Audit Logs	Detailed logs for auditing and compliance purposes.	IT Security Manager of AI-City Software Limited	5	5	4	14

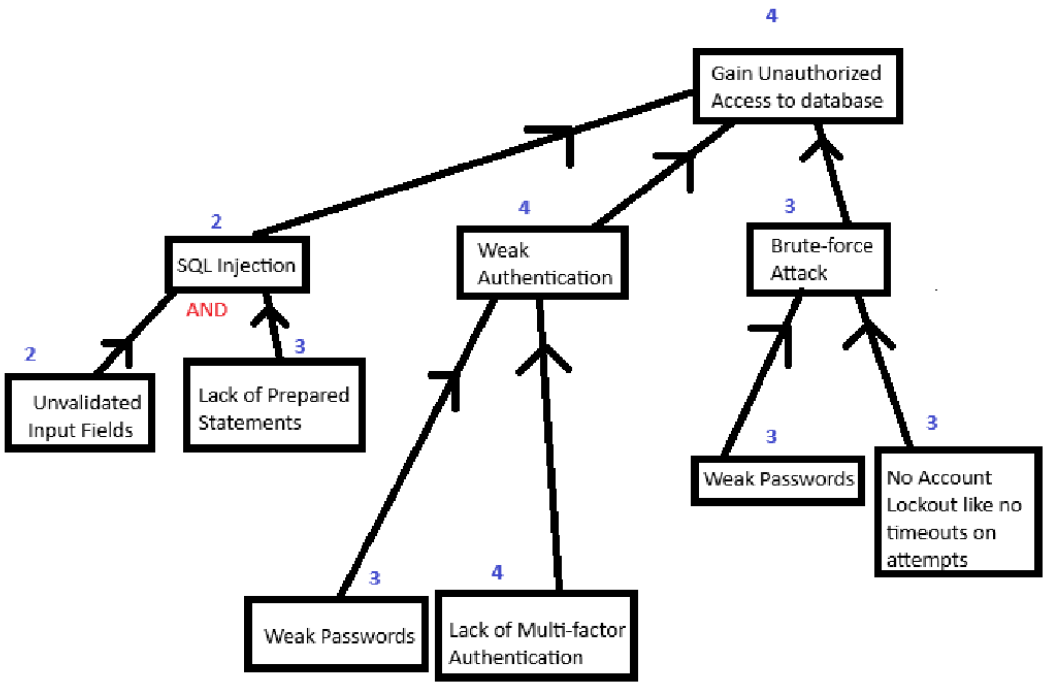
Attack Tree ->

Likely hood is numbered in blue I have made multiple tree, you can zoom it while marking assignment it will be more clearly visible, sorry for the trouble :)

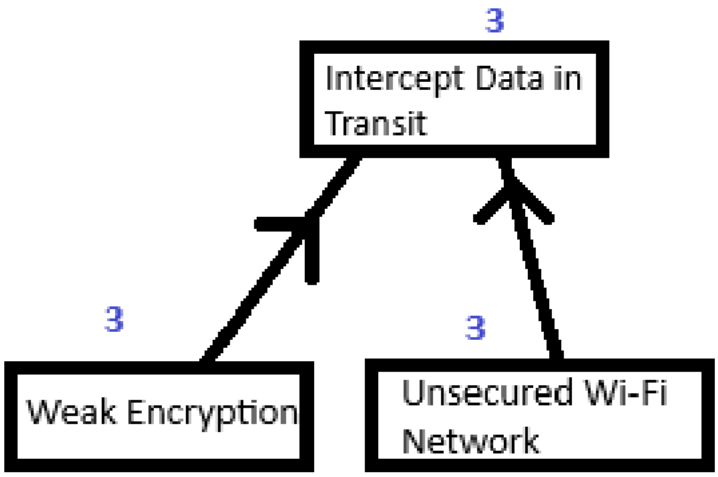


I'm also going to put each tree separately below,

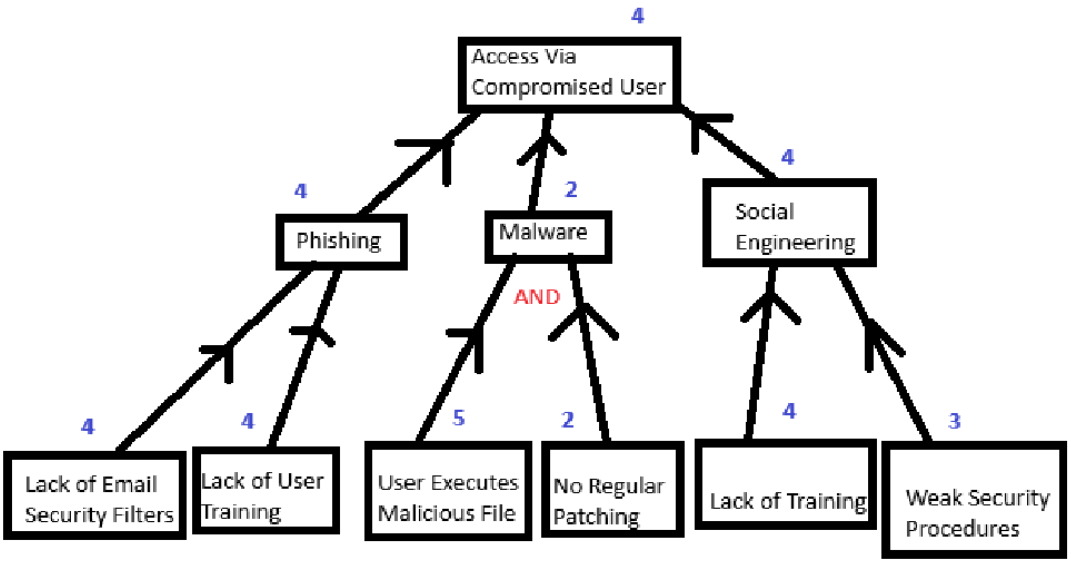
tree 1 -



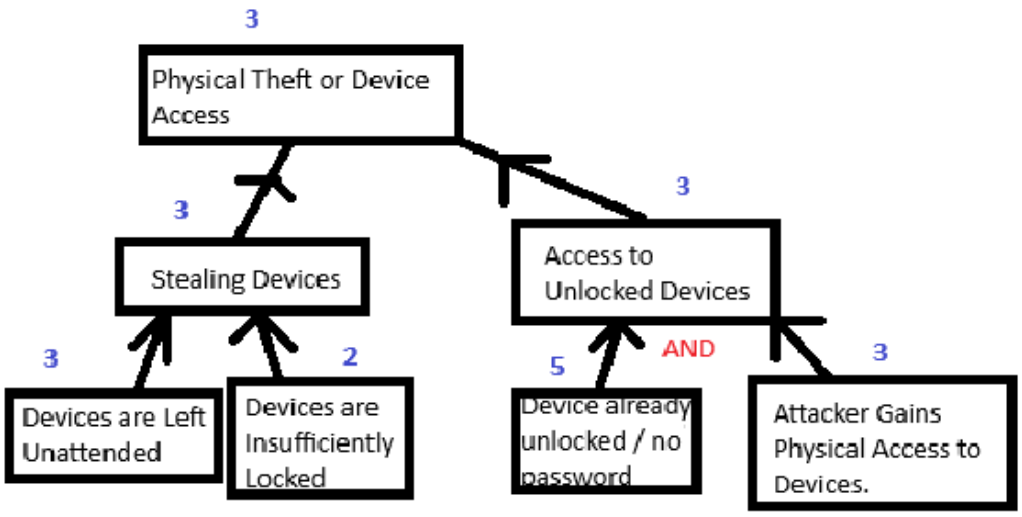
Tree 2 –



Tree 3 –


4
Access Via Compromised User
4
Phishing
2
Malware
4
Social Engineering
AND
4
Lack of Email Security Filters
4
Lack of User Training
5
User Executes Malicious File
2
No Regular Patching
4
Lack of Training
3
Weak Security Procedures

Tree 4 –


3
Physical Theft or Device Access
3
Stealing Devices
3
Access to Unlocked Devices
3
Devices are Left Unattended
2
Devices are Insufficiently Locked
5
AND
3
Device already unlocked / no password
Attacker Gains Physical Access to Devices.

Risk Treatment ->

converting and putting the excel sheet below, the excel sheet pdf came out really bad, REALLY BAD but I wasn't able to put 12 columns on word so have to use excel, If you want I can share excel file too.
I made risk treatment for the threads that made sense.

Please scroll down for the rest of the assignment. :)

Level	Description
Likelihood – 1	The likelihood of the attack happening
Likelihood – 2	The likelihood is low, but it's still a pos
Likelihood – 3	There is a moderate likelihood of the a
Likelihood – 4	The likelihood of the attack is high. It i
Likelihood – 5	The likelihood of the attack happening
Impact – 1	The consequences of the attack, if suc
Impact – 2	The consequences are noticeable but
Impact – 3	The impact is moderate. There would
Impact – 4	The impact is significant. The attack c
Impact – 5	The impact would be catastrophic. The

Attack Step	Information Asset	Attack Technique
Gain Unauthorized Access	Student, Parent and Teacher Data	SQL Injection
		Weak Authentication
		Brute-force Attack
Intercept Data in Transit	Student, Parent and Teacher Data	Weak Encryption
		Unsecured Wifi Network
Access via Compromised Us	Student, Parent and Teacher Data	Phishing
		Malware
		Social Engineering
Physical Theft or Device Acc	Student, Parent and Teacher Data	device stolen
		unlocked device Access
SQL Injection	Data Base.	unvalidated Input Fields
	Data Base.	lack of prepared Statements
Weak Authentication	account access	Weak Password
	account access	No Account lockout like no timeouts o
Phishing	device access	Lack of Email Security Filter
	device access	Lack of User Tracking
Malware	Device Acess	User Executes Malicious File
	Device Acess	No Regular Patching
Social Engineering	Device and account access	Lack of training
	Device and account access	Weak Security Procedure
Stealing Devices	Device and account access, with data	Devices Left Unattended
	Device and account access, with data	Devices are Insufficiently locked
Access to Unlocked devices	Device and account access, with data	Device already unlocked, no passwor
	Attacker Gains physical access to devices	

is extremely low, considered almost impossible under normal circumstances
sibility. The attack could happen with significant effort or specific conditions.
ıttack occurring. It may happen occasionally, but it's not extremely common.
s quite possible or frequent that this type of attack could occur.
is very high. It is almost certain to happen, or it's easy and cheap for an adversary to execute.
ccessful, would be minimal and unlikely to affect operations significantly.
not critical. There would be some disruption or damage, but it would be manageable.
be noticeable disruption, and some important assets or processes could be affected, but it wouldn't b
ould cause major disruptions, damage key assets, or have significant financial or reputational consec
e attack would result in a severe breach, major financial loss, or irreparable damage to critical operati

Likelihood (before)	Impact (before)	Risk (before)	Treatment Strategy	Action on Adversary
2	5	15	Secure code develop	Block SQL injection a
4	5	20	Enforce strong passv	Require multi-factor a
3	4	12	Implement account l	Lock accounts after f
3	4	12	Implement encryptio	Intercepting data bec
3	4	12	Enforce HTTPS for a	Prevent eavesdroppi
4	5	20	Conduct user awarer	Block phishing emails
2	5	10	Regular software pat	Prevent malware fron
4	5	20	User security training	Deceiving users becc
3	3	9	Encrypt data at rest,	Physical access to da
3	4	12	Secure physical stor	Data inaccessible wit
2	3	6	validate the input fiel	close logging in for sc
3	4	12	Use ORM (Object-R	block SQL injection
3	5	15	Enforce a strong pas	The attacker's ability
3	5	15	Implement account l	The attacker's ability
4	4	16	Activate email securi	Immediately identify a
			Implement real-time	During an attack, imn
5	5	25	Isolate the affected s	Once malware is dete
2	5	10	Immediately apply a	If an attack is exploiti
4	4	16	Initiate immediate av	If the attack involves
3	3	9	Immediately impleme	If weak security proce
3	5	15	Immediately enforce	If an unattended devi
2	5	10	Immediately enforce	If an attacker gains a
5	5	25	Immediately enforce	If a device is found ur
3	5	15	Implement strict phy	If an attacker gains pl

e catastrophic.
quences.
ons or reputation.

Control Mechanism	Likelihood (after)	Impact (after)	Risk (after)
Use prepared statements, input validation,	1	3	3
Implement password policies, multi-factor a	2	4	8
Account lockout, CAPTCHA, enforce strong	2	3	6
Enforce TLS/SSL for all data communicatio	1	4	4
SSL/TLS encryption, ensure all endpoints a	1	4	4
Anti-phishing tools, user awareness progra	2	3	6
Antivirus software, timely patch manageme	2	4	8
Security training, clear protocols for authen	2	3	6
Full disk encryption, strong password prote	1	3	3
Encryption, physical locks, device tracking	2	3	6
Use validation checkmarks	1	2	2
Use prepared statements, input validation,	2	2	4
Use password complexity rules, MFA, acco	2	2	4
Set up account lockout policies, CAPTCHA	2	3	6
ilter emails based on known phishing patter	2	3	6
Enable detailed logging and monitoring tool	1	2	2
onduct a post-incident review to improve de	3	3	9
If an attack is exploiting an unpatched vulne	1	2	2
Regularly assess and update the organizati	3	2	6
Establish clear procedures for reporting sec	2	2	4
Provide training and guidelines on securing	2	2	4
Regularly audit and monitor devices for cor	2	2	4
Conduct regular security audits and training	1	2	2
Develop and implement an incident respon	2	2	4

Test Plan for Assuring Effectiveness of Risk Treatments

The test plan will focus on validating the effectiveness of risk treatments through a series of security assessments, including penetration testing, vulnerability scanning, and audits. These methods will help identify weaknesses in the system and ensure that the implemented countermeasures address the identified risks.

1. **Penetration Testing**:

   Red Teaming: A dedicated team will simulate adversarial attacks to test the resilience of the system under real-world conditions. This will focus on common attack vectors such as unauthorized access to sensitive data, application vulnerabilities, and physical device theft.

   Blue Teaming: The internal security team will actively defend the system during the Red Team's simulated attacks, identifying gaps in detection and response capabilities.

   Purple Teaming: This approach will combine both Red and Blue teams, ensuring that lessons learned from the Red Team's attacks inform the Blue Team's defence mechanisms.

2. **Vulnerability Scanning**:

   Automated tools will be used to conduct vulnerability assessments across the infrastructure, applications, and networks. These scans will identify potential weaknesses such as outdated software, misconfigurations, or unpatched vulnerabilities.

3. **Audits**:

   Regular security audits will be conducted to review compliance with security policies, access controls, and the overall effectiveness of implemented controls. This will include reviewing logs, access controls, and adherence to security best practices.

Frequency: Penetration tests and vulnerability scans will be conducted quarterly, with audits being carried out on a bi-annual basis. Any findings will be addressed promptly to ensure continuous risk mitigation and system resilience.

By using these testing methods, we will ensure that our risk treatments remain effective and that the system can respond to emerging threats.

Guest Lectures ->

1. Paul Vlissidis –

Paul Vlissidis' guest lecture on "Red Pill or Blue Pill? (or how to make red teaming useful)," really resonated with me as it pushes past the comfort zone of compliance-based cybersecurity and dives into what true resilience looks like. His critique of standards like ISO27001 and PCI DSS struck a

chord—while they provide structure, they also encourage a "checkbox" mindset that ignores the evolving complexity of real-world threats. I found his emphasis on threat intelligence and frameworks like MITRE ATT&CK especially practical, as they offer a roadmap to better understand adversaries and strengthen defences. His insight that red and purple teaming, while effective, can overwhelm less mature organizations made me reflect on the importance of aligning strategy with organizational readiness. Personally, I admire how he challenges outdated norms and calls for a proactive, threat-informed security culture. That said, I think a deeper discussion on making these methods accessible to smaller enterprises facing resource constraints would have been helpful. Vlissidis doesn't just talk about cybersecurity; he offers a wake-up call to truly embrace adaptability, making this presentation both practical and thought-provoking. It's a message that I believe many leaders, myself included, need to hear and act upon.

2. Avi Shaked –

Avi Shaked's guest lecture on "Integrating Security into System Design: An Ontology-Driven, Conceptual Modelling Approach," offers a deeply technical yet thought-provoking perspective on embedding security into system architecture. By highlighting that security is inherently a systems design challenge, Shaked critiques traditional siloed methods and emphasizes the need for interdisciplinary integration. His TRADES framework which is a model-based, ontology-driven tool that brilliantly tackles complexity, providing a structured and scalable way to manage vulnerabilities while enhancing stakeholder collaboration. Particularly compelling is his focus on automating reasoning to make vulnerability management systematic and less error-prone. However, while the approach is rigorous, I wonder whether its accessibility to less resource-rich teams might be limited; scalability doesn't always equate to practicality for everyone. Personally, I appreciate the bold ambition to eliminate entire classes of vulnerabilities through foundational reengineering. it's a refreshing, proactive shift in thinking. Still, I'd love to see more real-world case studies demonstrating the framework's application beyond theoretical use. Overall, this work is an inspiring step forward in reimagining system design as inherently secure, offering actionable insights for the future of cybersecurity.

3. Ian Thornton –

Ian Thornton-Trump's guest lecture on "If You Think You Need a Lawyer, You Probably Need a Lawyer," offers a fascinating blend of cybersecurity pragmatism and legal awareness, wrapped in his unique, candid style. Thornton-Trump underscores the blurred lines between state actors and cybercriminals, the escalating sophistication of threats, and the critical need for businesses to focus on operational, strategic, and compliance risks. The highlights include actionable frameworks to deter, disrupt, degrade, and destroy cybercriminal activity, such as using MFA, zero-trust principles, and robust attack surface reduction strategies.

From my perspective, his insistence on validating controls through pen testing, maintaining evidence for liability protection, and addressing technical debt resonates powerfully. However, I wonder whether smaller businesses, often constrained by resources, can realistically implement his roadmap. His discussion on understanding shortfalls—accepting third-party validation for cost-efficiency—felt especially grounded and practical. Personally, I appreciated his sharp critiques of corporate indifference, especially his warning against misleading compliance narratives. Thornton-Trump's presentation is not just informative; it's a rallying cry for preparedness, delivering critical

cybersecurity wisdom with just the right amount of irreverence. It’s engaging, insightful, and unapologetically honest wake-up call for stakeholders.

4. Jon Noel –

In the guest lecture "Malware Evolution" by Jon Noel provides an insightful overview of the complex landscape of malware in 2024, focusing on its types, motives, and countermeasures. It introduces malware fundamentals such as viruses, worms, and trojans, explaining their modes of operation and impact. The narrative delves deeper into sophisticated threats like botnets, fileless malware, and AI-driven attacks, highlighting the growing role of artificial intelligence in enabling tailored phishing campaigns and optimizing ransomware execution. The exploitation of IoT devices as vulnerable entry points for network breaches also underscores the expanding attack surface. While detailing protection strategies, the text advocates for multi-layered defences like Zero Trust Network Access (ZTNA) and advanced AI/ML-driven solutions, critiquing the diminishing effectiveness of traditional signature-based tools.

Personally, I found the discussion on AI-driven threats both fascinating and alarming—it’s a reminder of how emerging technologies can be a double-edged sword. The fileless malware section also stood out; its stealthy nature poses a chilling challenge to modern cybersecurity. However, the document occasionally assumes a technically savvy audience, leaving some complex concepts underexplained. A stronger emphasis on actionable steps for individuals and organizations would have enhanced its practicality.