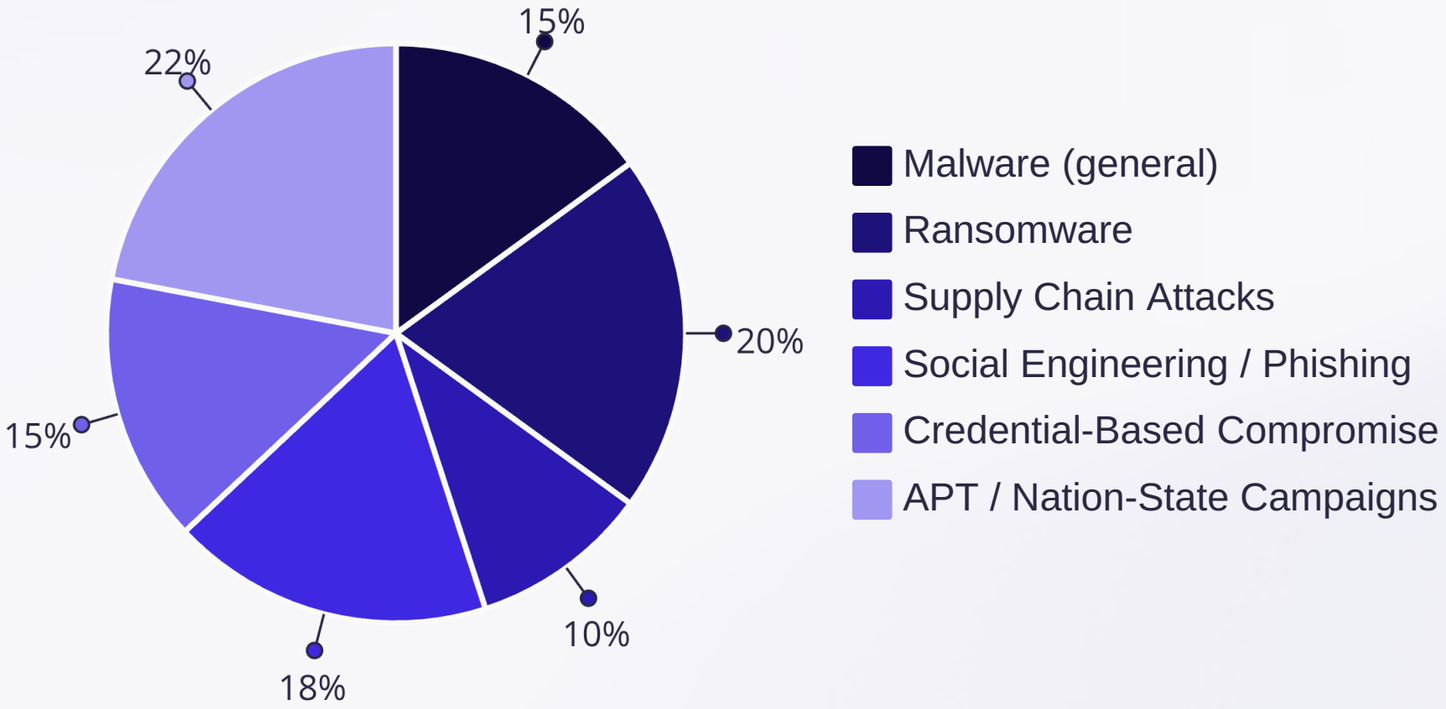
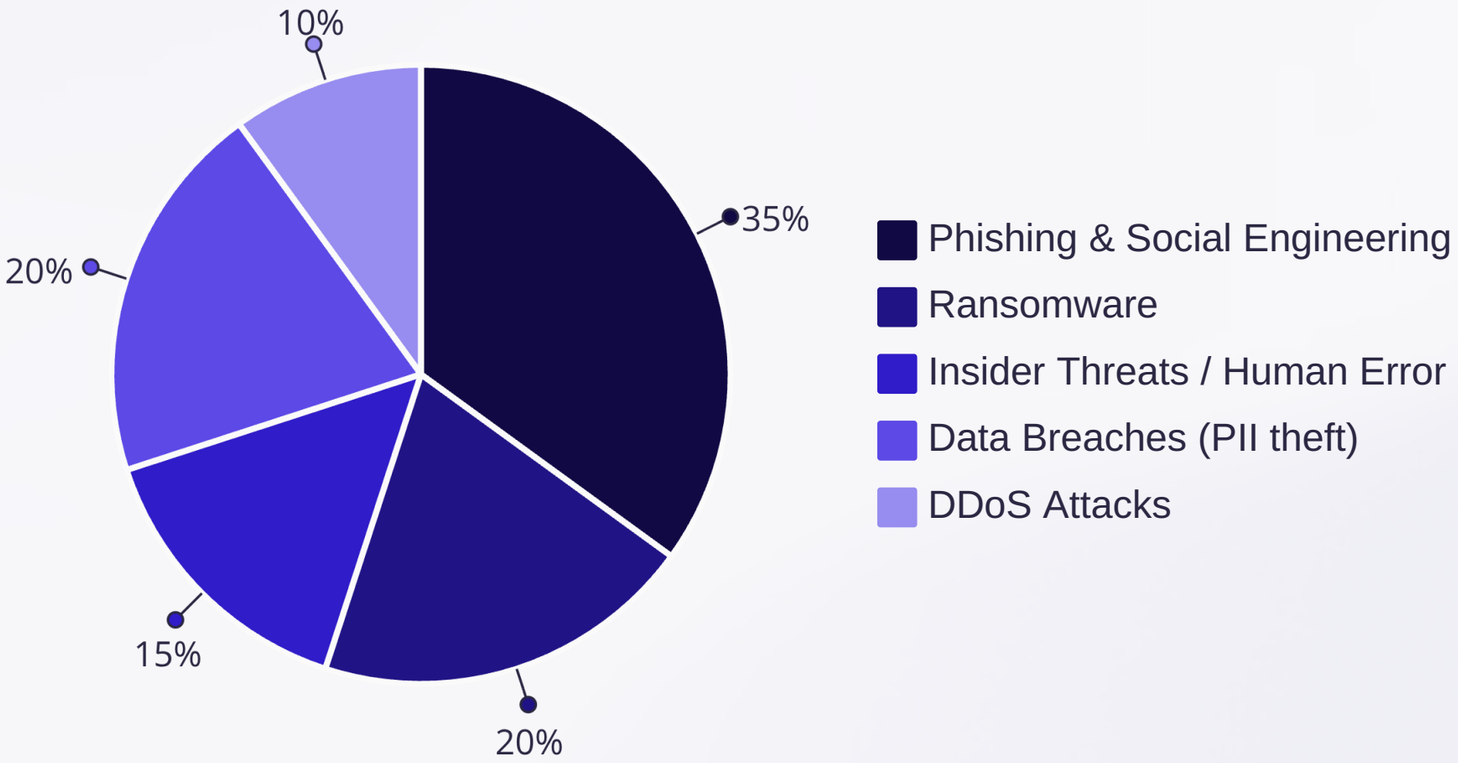
Cyber Threat Analysis across Industries

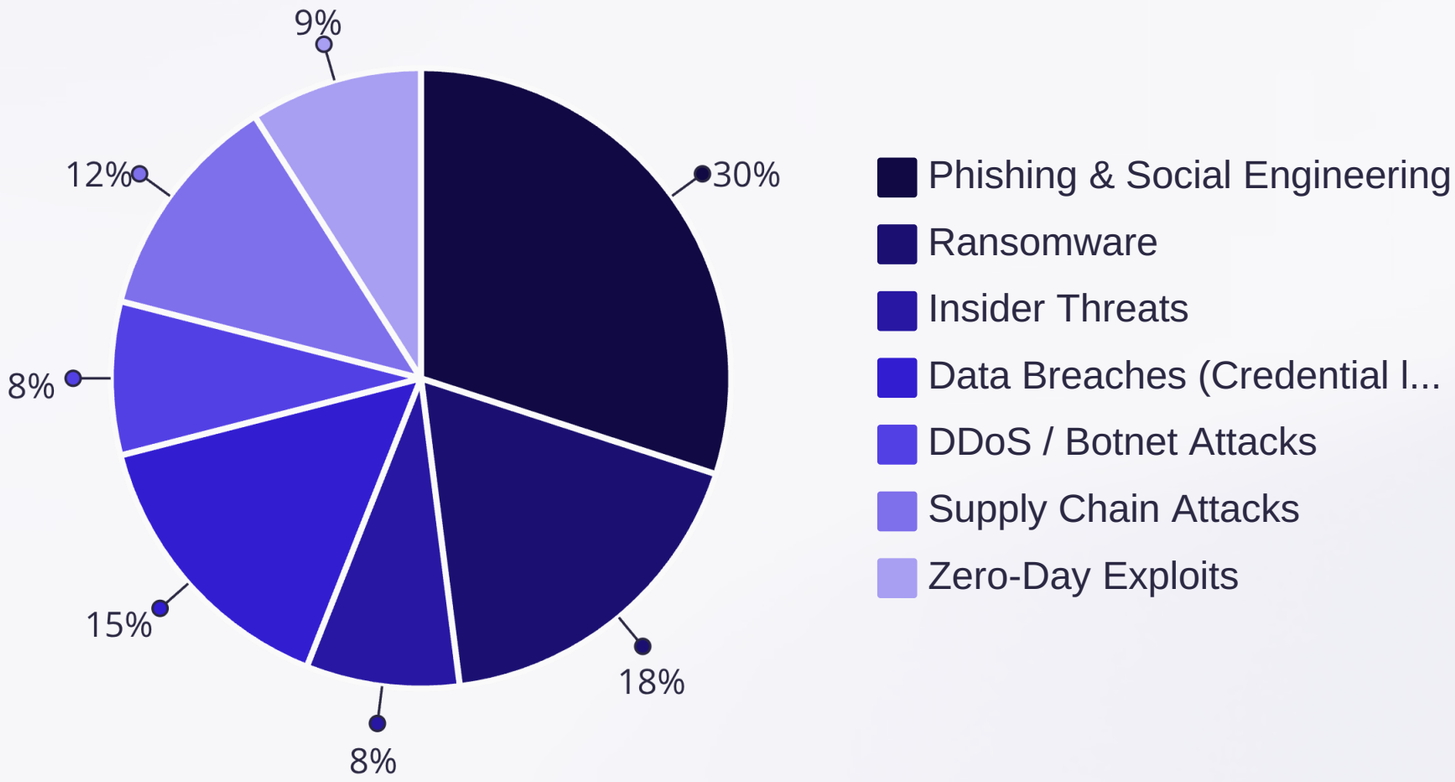
Cyber Threats in Manufacturing Industry(Percentage wise)



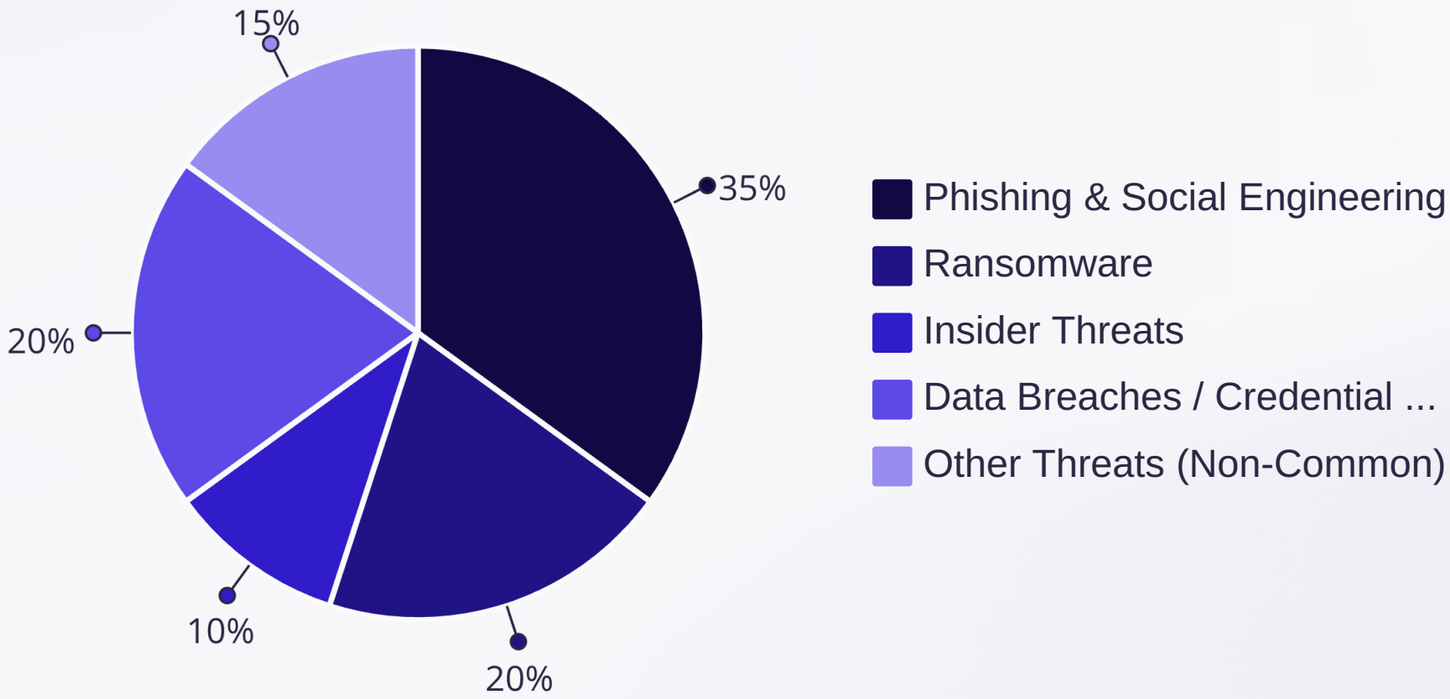
Cyber Threats in Education Industry(Percentage wise)



Cyber Threats in IT Industry(Percentage wise)



Common Threats Across All Three Industries



Common Threat Model

1. Scope

Applies to three industries: **Manufacturing, Education, IT**Covers **4 common threats**:

- Phishing & Social Engineering
- Ransomware
- Insider Threats
- Data Breaches / Credential Attacks

2. Assets at Risk

- Sensitive Data (IP, student records, customer data)
- Operational Systems (ICS/OT in manufacturing, IT servers, educational platforms)
- User Accounts & Credentials
- Financial Resources
- Business Continuity / Reputation

3. Threat Categories (STRIDE Mapping)

Threat Type	STRIDE Category	Attack Surface	Example Scenario
Phishing & Social Engineering	**Spoofing, Tampering, Information Disclosure**	Email, messaging apps, social media	Employee receives fake login email, discloses credentials
Ransomware	**Denial of Service, Tampering**	Endpoints, servers, backups	Malware encrypts manufacturing systems, halts production
Insider Threats	**Elevation of Privilege, Tampering, Information Disclosure**	Employees, contractors, privileged accounts	Insider leaks exam data, steals customer database
Data Breaches / Credential Attacks	**Information Disclosure, Spoofing**	Databases, cloud services, identity systems	Stolen credentials used to access financial or IP systems

4. Threat Likelihood & Impact (Risk Rating)

Threat Type	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level
Phishing & Social Engineering	High	High	**Critical**
Ransomware	High	High	**Critical**
Insider Threats	Medium	Medium	**Moderate**
Data Breaches / Credential Attacks	High	High	**Critical**

5. Mitigation Strategies

Threat Type	Mitigation Controls
Phishing & Social Engineering	Security awareness training, phishing simulations, strong email filters, MFA
Ransomware	Regular backups (offline & immutable), patching, endpoint detection, incident response playbooks
Insider Threats	Least-privilege access, monitoring user behavior, data loss prevention (DLP), HR + legal policies
Data Breaches / Credential Attacks	MFA everywhere, passwordless/SSO solutions, credential monitoring (dark web), encryption of sensitive data

6. Threat Modeling Diagram (Simplified View)

Actors → Entry Points → Threats → Assets → Mitigations

- **External Actor (Phisher, Ransomware Gang, Nation-State)** → Entry Points: Email, Malicious Links, Unpatched Systems → Threats: Phishing, Ransomware, Credential Attacks → Assets: Data, Accounts, Systems → Mitigations: MFA, Patching, Backups

- **Internal Actor (Malicious Insider, Negligent Employee)** → Entry Points: Authorized Access, Privileged Accounts → Threats: Insider Threats, Data Breaches → Assets: Databases, Confidential Records → Mitigations: Least Privilege, Monitoring, DLP

7. Output

This model helps:

- **Prioritize threats** → Phishing, Ransomware, and Data Breaches rank highest.
- **Define controls** → Focus on MFA, backup resilience, training, access management.
- **Enable cross-industry defense alignment** → Since these 4 threats are common, joint defense strategies are feasible.