🧾 Risk Assessment for Commercial Bank - Risk Register Summary by Jordan Butler

📝 Risk Factors (2–3 Sentence Summary)

The cybersecurity team at a commercial bank is assessing various risk factors that could disrupt business operations, compromise customer data, or impact system integrity. These risks range from insider threats to phishing attacks and third-party vendor vulnerabilities. The goal is to assign risk scores based on **likelihood** and **severity** to prioritize mitigation strategies and resource allocation.

✅ Risk Register Table

Risk Description	Likelihood (1–5)	Severity (1–5)	Risk Score (L x S)
1. Phishing attacks targeting employees	5	4	20
2. Insider threat through privileged access misuse	3	5	15
3. Third-party vendor compromise	4	4	16
4. Ransomware infection via infected email attachment	4	5	20
5. Outdated software on customer-facing banking systems	2	4	8

📌 Breakdown

1. **Phishing Attacks**
   - *Likelihood:* Very high due to regular email communication and human error.
   - *Severity:* Could result in credential theft or unauthorized access to banking systems.
   - **Risk Score:** 20
2. **Insider Threat**
   - *Likelihood:* Moderate, as employees may become malicious or careless.
   - *Severity:* High due to access to sensitive internal systems.
   - **Risk Score:** 15
3. **Third-Party Vendor Compromise**
   - *Likelihood:* High, especially if vendors lack proper security controls.
   - *Severity:* High since vendors often have indirect access to bank systems or data.
   - **Risk Score:** 16
4. **Ransomware Infection**

   - *Likelihood:* High, as ransomware is common and frequently delivered via email.
   - *Severity:* Very high due to potential data encryption and business disruption.
   - **Risk Score:** 20
5. **Outdated Software on Customer Systems**
   - *Likelihood:* Low, as updates are typically scheduled but may be delayed.
   - *Severity:* Moderate, with potential for exploit if unpatched vulnerabilities exist.
   - **Risk Score:** 8

🧠 Summary Insight

The highest priority risks based on this assessment are **phishing attacks** and **ransomware infections**, both scoring 20. These threats are both frequent and highly damaging and should be addressed immediately through employee training, email filtering, and endpoint protection. **Third-party risk** and **insider threats** follow closely and require strategic controls like vendor risk assessments and privileged access monitoring. The **outdated software** risk is the least urgent but should still be included in a scheduled update policy.