5 Star Data Systems, LLC

Small and Medium-size Business

Sample Risk Register

Small and medium-sized manufacturers face a rapidly growing array of cyber threats—ranging from ransomware and phishing to insider risks and more—alongside persistent operational, regulatory, and supply chain challenges. The most effective way to manage these risks is with a focused, quantitative risk register that also allows leaders to measure the value of their security investments.

We provide a sample risk register that focuses on 15 risks we would most likely target for small or medium-sized manufacturers. For this register, we normalized the loss expectancy values for a company with $5 million annual revenue. There is also a brief explanation of the ROSI ("Return on Security Investment") metric, which we use to prioritize controls with the most significant business impact. ROSI is useful, with the caveat that, while some controls provide a seemingly negative return on investment, they account only for the cost of the countermeasure and its investment return and do not consider the overall health of the organization it provides, or the compliance requirements it satisfies.

Risk Register

Every risk entry below includes the likelihood (ARO), loss severity (SLE), anticipated annual loss (ALE), key mitigation/control actions (with estimated cost), residual risk after implementing controls, and the ROSI score.

Sample Risk Register

Risk Type	ARO	SLE ($)	ALE ($)	Mitigation / Cost $	ALE After ($)	ROSI
Ransomware Attack	0.40	250,000	100,000	EDR, backup, awareness (35,000)	50,000	0.43
Phishing/BEC	0.40	50,000	20,000	MFA, phishing training (12,000)	12,000	-0.33
Insider Threat	0.10	80,000	8,000	Monitoring, policy (10,000)	3,000	-0.50
Supply Chain Attack	0.16	150,000	24,000	TPRM, segmentation (10,000)	9,000	0.50
Legacy OT System	0.18	75,000	13,500	Segmentation, patching (15,000)	7,500	-0.60
Cloud Misconfiguration	0.15	90,000	13,500	Cloud posture mgmt. (8,000)	9,000	-0.44
Unpatched Vulnerability	0.20	120,000	24,000	Patch mgmt. (8,000)	12,000	0.50
Inadequate Backup/DR	0.10	160,000	16,000	Offsite backup/DR test (12,000)	4,000	0.00
Regulatory Non-compliance	0.16	40,000	6,400	Consulting, GRC (10,000)	8,000	-1.16
Physical Security Breach	0.12	40,000	4,800	Access controls, cameras (6,000)	6,000	-1.20
IoT/ICS Device Attack	0.10	70,000	7,000	Segmentation/device mgmt. (6,000)	7,000	-1.00

Risk Type	ARO	SLE ($)	ALE ($)	Mitigation / Cost $	ALE After ($)	ROSI
Business Continuity Failure	0.07	175,000	12,250	BCP test, alt. suppliers (8,000)	3,500	0.09
Unauthorized Remote Access	0.12	40,000	4,800	VPN, MFA, monitoring (4,000)	5,000	-1.05
Lost/Stolen Device/Media	0.07	30,000	2,100	Encryption, MDM (2,000)	3,000	-1.45
Social Engineering/Pretext	0.10	20,000	2,000	Security training (3,000)	2,000	-1.00

Key Columns Explained:

- ARO: Annual Rate of Occurrence (probability/year)
- SLE: Single Loss Expectancy (direct cost per event)
- ALE: Annualized Loss Expectancy = ARO × SLE
- Mitigation/Cost: Main control actions and annual cost
- ALE After: Residual ALE after control deployed
- ROSI: See explanation below

What Is ROSI, and Why Does It Matter?

ROSI (Return on Security Investment) is a metric that helps you quantify the financial effectiveness of your security spending. It answers: "Does this investment save more in risk reduction than it costs?"

ROSI Formula

$$ROSI = \frac{(ALE_{before} - ALE_{after}) - \text{Control Cost}}{\text{Control Cost}}$$

- ALE_before: Expected annual loss from this risk before any control.
- ALE_after: Expected annual loss after the control has been fully implemented.

- **Control Cost**: Total annual cost (including tech, labor, training, etc.) of the mitigation.

How to Read ROSI

- **Positive ROSI (>0)**: Investment is projected to generate net savings (good financial return).
- **Zero ROSI (0)**: The control "breaks even"—savings exactly match cost.
- **Negative ROSI (<0)**: Control costs outweigh the loss reduction, but the control may still be required for compliance, contracts, or insurance.

Example Calculation

Suppose:

- ALE before for ransomware = $100,000
- After controls, ALE after = $50,000
- Control cost = $35,000

$$ROSI = \frac{(100{,}000 - 50{,}000) - 35{,}000}{35{,}000} = 0.43$$

This means each $1 spent yields $1.43 in reduced risk—a strong result for most manufacturers.

Why 15 Key Risks?

Experience shows **10–20 well-chosen risks** provide the best combination of comprehensiveness and focus. Fewer risks may miss significant exposures; too many can overwhelm lean SMB teams and dilute resources from the highest impact improvements.

In summary

A clear, prioritized risk register—backed by easy-to-understand ROSI analysis—empowers manufacturing leaders to act with confidence, combining compliance, safety, and the highest return on resource investment.

For more guidance and risk management resources, contact us at info@5sds.com.