Threat Model Worksheet

ACPA
IDRI

Actors
Who are you defending against?

Capabilities
What can they do?

Prevention
How do you stop attacks?

Assets
What are you defending?

Incentives
What can someone gain by compromising you?

Detection
How will you detect a compromise?

Response
What will you do once compromised?

Impact
What happens when you are compromised?

Threat Model Worksheet

My example website

ACPA IDRI

Actors
Who are you defending against?

Script Kiddies

~~The NSA~~

Organized Crime

Capabilities
What can they do?

SQL injection

~~Implant hardware~~

Email phishing links

Prevention
How do you stop attacks?

Don't know?

Can't prevent

Email scanning

Assets
What are you defending?

Login credentials

Credit card numbers

Incentives
What can someone gain by compromising you?

Lulz

Credit Fraud

Accounts to sell

~~Collect Intelligence~~

Detection
How will you detect a compromise?

Employee browser logging & alerts

System logs

Response
What will you do once compromised?

Employee password reset

Who monitors these logs?

Impact
What happens when you are compromised?

Bulk password reset

Bad publicity

Breach notifications & Increased fees