The OWASP Risk Rating Methodology

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Discovering vulnerabilities is important, but being able to estimate the associated risk to the business is just as important. Early in the life cycle, one may identify security concerns in the architecture or design by using threat modeling. Later, one may find security issues using code review or penetration testing. Or problems may not be discovered until the application is in production and is actually compromised.

By following the approach here, it is possible to estimate the severity of all of these risks to the business and make an informed decision about what to do about those risks. Having a system in place for rating risks will save time and eliminate arguing about priorities. This system will help to ensure that the business doesn't get distracted by minor risks while ignoring more serious risks that are less well understood.
Ideally there would be a universal risk rating system that would accurately estimate all risks for all organizations. But a vulnerability that is critical to one organization may not be very important to another. So a basic framework is presented here that should be *customized* for the particular organization.

The authors have tried hard to make this model simple to use, while keeping enough detail for accurate risk estimates to be made. Please reference the section below on customization for more information about tailoring the model for use in a specific organization.

Drive/Car DB

				Likelihood				
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
6 - Network and programming skills	9 - High reward	4 - Special access or resources required	9 - Anonymous Internet users		7 - Easy	7 -	9 - Public knowledge	3 - Logged and reviewed
			Overall likelihood:	6.750	HIGH			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9 - All data disclosed	9 - All data totally corrupt	3 -	7 - Possibly traceable		8 -	8 -	9 -	9 - Millions of people
	Overall technical impact:	7.000	HIGH			Overall business impact:	8.500	HIGH
			Overall impact:	7.750	HIGH			

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

user DB

				Likelihood				
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
6 - Network and programming skills	9 - High reward	4 - Special access or resources required	9 - Anonymous Internet users		7 - Easy	7 -	9 - Public knowledge	3 - Logged and reviewed
			Overall likelihood:	6.750	HIGH			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
5 - Extensive critical data disclosed	5 - Extensive slightly corrupt data	3 -	7 - Possibly traceable		5 -	4 - Loss of major accounts	4 -	4 -
	Overall technical impact:	5.000	MEDIUM			Overall business impact:	4.250	MEDIUM
			Overall impact:	4.625	MEDIUM			

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

laptop client ↔ server

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5 - Advanced computer user	7 -	4 - Special access or resources required	9 - Anonymous Internet users		9 - Automated tools available	9 - Automated tools available	9 - Public knowledge	3 - Logged and reviewed
			Overall likelihood:	**6.875**	**HIGH**			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9 - All data disclosed	9 - All data totally corrupt	9 - All services completely lost	7 - Possibly traceable		9 - Bankruptcy	9 - Brand damage	9 -	9 - Millions of people
Overall technical impact:		**8.500**	**HIGH**		**Overall business impact:**		**9.000**	**HIGH**
			Overall impact:	**8.750**	**HIGH**			

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	**Low**	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Rating

	Skill level	Motive	Opportunity	Size	Ease of discover	Ease of exploit	Awareness	Intrusion detecti	Loss of confiden	Loss of integrity	Loss of availabili	Loss of accounta	Financial damag	Reputation dam	Non-compliance	Privacy violation
0			Full access or expensive resources required													
1	No technical skills	Low or no reward			Practically impossible	Theoretical	Unknown	Active detection in application		Minimal slightly corrupt data	Minimal secondary services interrupted	Fully traceable	Less than the cost to fix the vulnerability	Minimal damage		
2				Developers, system administrators					Minimal non-sensitive data disclosed						Minor violation	
3	Some technical skills				Difficult	Difficult		Logged and reviewed		Minimal seriously corrupt data			Minor effect on annual profit			One individual
4		Possible reward	Special access or resources required	Intranet users			Hidden		Minimal critical data disclosed, extensive non-sensitive data disclosed					Loss of major accounts		
5	Advanced computer user			Partners		Easy			Extensive critical data disclosed	Extensive slightly corrupt data	Minimal primary services interrupted, extensive secondary services interrupted			Loss of goodwill	Clear violation	Hundreds of people
6	Network and programming skills			Authenticated users			Obvious									
7			Some access or resources required		Easy					Extensive seriously corrupt data	Extensive primary services interrupted	Possibly traceable	Significant effect on annual profit		High profile violation	Thousands of people
8								Logged without review								
9	Security penetration skills	High reward	No access or resources required	Anonymous Internet users	Automated tools available	Automated tools available	Public knowledge	Not logged	All data disclosed	All data totally corrupt	All services completely lost	Completely anonymous	Bankruptcy	Brand damage		Millions of people