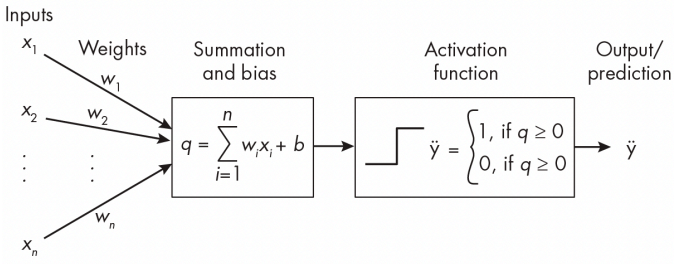
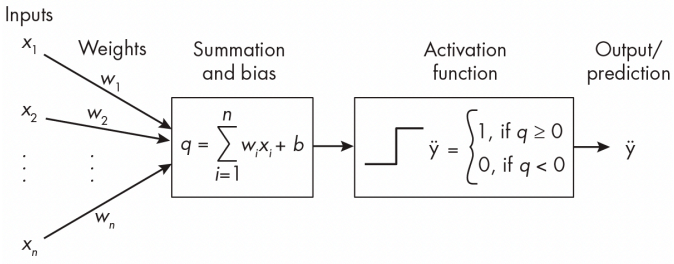
Practical AI Security

A Hands-on Guide to Attacking, Defending, and Securing Modern AI Systems

by Harriet Farlow

Errata updated to print 1

Page	Error	Correction	Print corrected
5	 *Figure 1-2: The Perceptron*	 *Figure 1-2: The Perceptron*	Pending