6 Areas to Improve ROI for Security Penetration Testing

Richard Hollis
Risk Crew Ltd, United Kingdom

Abstract:
Why do we conduct security penetration testing? What’s the objective? What’s the right approach? Do we have the right supplier? Does the methodology matter? Is it worth it? What should we get for our investment? How can we prove it? More importantly, how can we improve it? Very few businesses have answers to these straightforward, practical questions, yet continue to spend vast sums conducting security penetration testing year after year with little tangible return. This session begins by presenting a quick, simple formula template for calculating the annual loss expectancy (ALE) and return on investment (ROI) required for establishing a business case for a security penetration testing program. The presenter then discusses how to ensure the right testing approach, objective, scope, methodology, qualifications, reporting formats are used for your next test providing over 30 specific actions for improving the ROI for security penetration testing. The session delivers simple, pragmatic, cost-effective actions attendees can take back to their businesses for implementation. Upon completion, attendees will receive a “take-away” list of these recommended actions for their reference. The content of this presentation is based on over 20 years of penetration testing case studies and is devoid of commercial content.

Biography:

Publication of speakers: