

## **I. LA GESTIONE DEL PROGRAMMA DI SECURITY AWARENESS**

1.1	Introduzione.....	13
1.2	I problemi più comuni .....	14
1.3	Il modello .....	15
1.3.1	I componenti del modello.....	15
1.3.2	Come usare il modello .....	17
1.3.3	Un programma continuo .....	17
1.4	I benefici di business .....	18

## **2. COME GIUSTIFICARE UN PROGRAMMA DI SECURITY AWARENESS**

2.1	Introduzione.....	21
2.2	Il modello del Ritorno sugli investimenti in sicurezza .....	22
2.3	Quantificare l'esposizione al rischio .....	25
2.4	Quantificare la mitigazione del rischio .....	29
2.5	Quantificare il costo di un'attività di Awareness.....	30
2.6	Pianificare a lungo termine .....	31

## **3. PIANIFICARE UN PROGRAMMA DI AWARENESS**

3.1	Gli obiettivi della Security Awareness .....	35
3.2	I problemi.....	35
3.2.1	La scotomizzazione, ovvero, l'ottimismo è il profumo della vita .....	35
3.2.2	Le minacce evolvono con l'evolvere del mercato e delle aziende .....	36
3.2.3	La sicurezza non ha niente a che fare con la mission aziendale .....	37
3.3	Il processo di pianificazione .....	37
3.3.1	Definire il team di progetto.....	37
3.3.2	Definire gli obiettivi.....	37
3.3.3	Definire l'audience.....	38
3.3.4	I gruppi target.....	39
3.3.5	Individuare le necessità del pubblico .....	39
3.3.6	Definire gli obiettivi di performance.....	41
3.3.7	Le risorse.....	43
3.3.8	La sponsorship del top management.....	43
3.3.9	Budget e costi .....	45
3.4	Preparare un business case.....	46
3.5	Un esempio di business case.....	47
3.5.1	Sommario esecutivo .....	47
3.5.2	Introduzione.....	48
3.5.3	Scopo di questo documento.....	48
3.5.4	Introduzione al programma di Awareness.....	48
3.5.5	L'audience del programma .....	49
3.5.6	Gestione, delivery e monitoraggio del programma di Awareness .....	49
3.5.7	Contenuti del programma di Awareness .....	50
3.5.8	Tecniche di Awareness .....	51
3.5.9	Fonti di materiale.....	51

3.5.10	I metodi della Security Awareness.....	52
3.5.11	Il sito web della sicurezza.....	54
3.5.12	Il branding.....	55
3.5.13	La formazione per i nuovi dipendenti.....	55
3.5.14	La gestione del programma.....	56
3.5.15	Piano di programma e attività principali.....	56
3.5.16	Monitoraggio del programma.....	56
3.5.17	Analisi dei costi e benefici.....	58
3.5.18	Conclusioni.....	59
3.6	La strategia di comunicazione.....	60
3.7	La valutazione delle soluzioni.....	60
3.7.1	Un esempio di Richiesta di Offerta.....	61
3.8	La scelta dei media.....	65
3.8.1	Presentazioni di gruppo.....	66
3.8.2	Presentazioni individuali.....	66
3.8.3	Produzioni video.....	67
3.8.4	CD interattivo.....	67
3.8.5	Formazione via web.....	67
3.8.6	Newsletter, guide.....	67
3.8.7	Nuovi modelli di apprendimento: il blended learning.....	68
3.9	Il programma di Security Awareness.....	70
3.9.1	Bisogni e obiettivi.....	71
3.9.2	I contenuti del programma.....	73
3.9.3	L'uso di prodotti di Security Awareness.....	74
3.9.4	Costruire il programma.....	74
3.9.5	Pianificare gli eventi.....	75
3.10	Esempio di Piano esecutivo.....	77
3.10.1	Executive Summary.....	77
3.10.2	Comitato direttivo.....	78
3.10.3	I destinatari della Security Awareness.....	79
3.10.4	I contenuti della Security Awareness.....	79
3.10.5	Le modalità di erogazione dei contenuti.....	80
3.10.6	Feedback e miglioramento.....	83
3.10.7	Metriche e valutazione.....	84
3.10.8	Piano di progetto.....	84
3.11	Documento di progetto ( <i>Project charter</i> ).....	86
3.12	Obiettivi di apprendimento.....	87
3.12.1	Modulo 1 – La sottrazione di informazioni confidenziali.....	87
3.12.2	Modulo 2 – La privacy e la sicurezza dipendono da te.....	88
3.12.3	Modulo 6 – Proteggi i tuoi dati: la sicurezza in mobilità.....	89
3.12.4	Modulo 9 – Sicurezza anche a casa.....	90
3.12.5	Modulo 8 – Riconoscere i segnali di pericolo.....	91
3.13	Lista di controllo del progetto.....	91
<b>4. LA VALUTAZIONE DI UN PROGRAMMA DI SICUREZZA</b>		
4.1	Introduzione.....	97
4.2	Livelli di valutazione.....	97
4.2.1	Esempi di strumenti di valutazione.....	98

4.3	Il sondaggio sul rischio del fattore umano .....	101
4.3.1	Come usare il sondaggio.....	101
4.3.2	Tabella dei risultati .....	101
4.3.3	Come diffondere il sondaggio.....	102
4.3.4	Un esempio di sondaggio.....	102
4.4	Il Security Awareness Maturity Model.....	106
4.5	Metriche di valutazione e strumenti di misura .....	109
4.6	L'elenco delle metriche.....	110

## **5. IL MARKETING DELLA SICUREZZA**

5.1	Vendere la sicurezza.....	115
5.2	La sicurezza è un servizio.....	115
5.3	Tecniche e strategie di marketing .....	116
5.3.1	Stabilire la credibilità del venditore.....	116
5.3.2	Posizionamento e immagine del prodotto.....	118
5.3.3	La soddisfazione del cliente (customer satisfaction) .....	121
5.3.4	Costruire la soddisfazione del cliente.....	122
5.4	Strumenti di vendita.....	124
5.4.1	Ausili visivi .....	125
5.4.2	Utilizzare gli ausili visivi .....	127
5.4.3	Concorsi a premi.....	130

## **6. PRINCIPI DI BASE DELLA FORMAZIONE SUI TEMI DELLA SICUREZZA DELLE INFORMAZIONI**

6.1	Introduzione.....	135
6.1.1	Frequenza della formazione .....	135
6.1.2	Formazione come processo continuo .....	135
6.1.3	Formazione come parte della responsabilità dei dipendenti .....	136
6.2	Istruzione come responsabilità .....	136
6.3	Alcuni esempi .....	139
6.3.1	Barclays si dà al cinema .....	139
6.3.2	Security Awareness contest .....	140
6.3.3	Le «Pillole di sicurezza» .....	141
6.4	Raccontare storie.....	142
6.4.1	Il metodo .....	142
6.4.2	L'apprendimento attraverso storie interattive .....	143
6.4.3	Un esempio .....	144
6.4.4	Conclusione.....	145

## **7. PERFORMANCE ED ESPERIENZA DI APPRENDIMENTO**

7.1	La performance nel luogo di lavoro .....	149
7.1.1	Problemi di performance e soluzioni .....	150
7.1.2	I problemi ambientali.....	151

7.1.3	Le carenze di conoscenze o competenze .....	154
7.1.4	I problemi motivazionali .....	156
7.1.5	Le soluzioni .....	156
7.2	Principi dell'apprendimento negli adulti .....	157
7.2.1	Gli adulti sono motivati internamente e si dirigono da soli .....	159
7.2.2	Gli adulti portano esperienze di vita e conoscenza all'esperienza di apprendimento .....	160
7.2.3	Gli adulti sono orientati all'obiettivo .....	160
7.2.4	Gli adulti sono orientati a temi rilevanti .....	161
7.2.5	Gli adulti sono pragmatici .....	161
7.2.6	Gli adulti vogliono essere rispettati .....	161
7.3	I deficit del training .....	162
7.4	Effetti positivi .....	164
7.5	Rendere efficace l'esperienza di apprendimento .....	165
7.5.1	Parlare di minacce .....	167
7.6	Approcciare i discenti .....	168
7.7	Comunicare in modo efficace .....	169
7.7.1	Rompere il guscio della presunzione .....	170
7.8	La responsabilità dei dipendenti .....	171
7.8.1	Ambiti a maggiore confidenzialità .....	171
7.8.2	La formazione iniziale .....	172
7.8.3	La classificazione delle informazioni .....	172
7.8.4	La protezione delle informazioni .....	173
7.8.5	La declassificazione delle informazioni .....	173
7.8.6	Altri ambiti .....	174
7.9	Motivare i collaboratori .....	174
7.9.1	Sollecitare la motivazione .....	174
7.9.2	I problemi della motivazione .....	175
7.9.3	Applicare la motivazione .....	177
7.9.4	L'atteggiamento verso la sicurezza .....	178
7.9.5	Un modello per la motivazione .....	180
7.9.6	Motivazione positiva e negativa .....	181
7.9.7	Un modello di motivazione .....	182
7.9.8	La teoria dei bisogni di Maslow .....	185

## 8. SECURITY AWARENESS E STANDARD DI SICUREZZA

8.1	Introduzione .....	191
8.2	ISO 27001/27002 .....	191
8.3	PCI DSS .....	191
8.4	COBIT .....	192
8.5	Legislazione italiana – Codice in materia di protezione dei dati personali .....	192
8.6	Legislazione svizzera – Circolare FINMA 2008/21 – Allegato 3 .....	192
8.7	Le <i>policy</i> aziendali .....	193
8.7.1	Policy generale di Security Awareness .....	193
8.7.2	Procedura di gestione di attacchi di social engineering per gli operatori di Front Desk .....	194