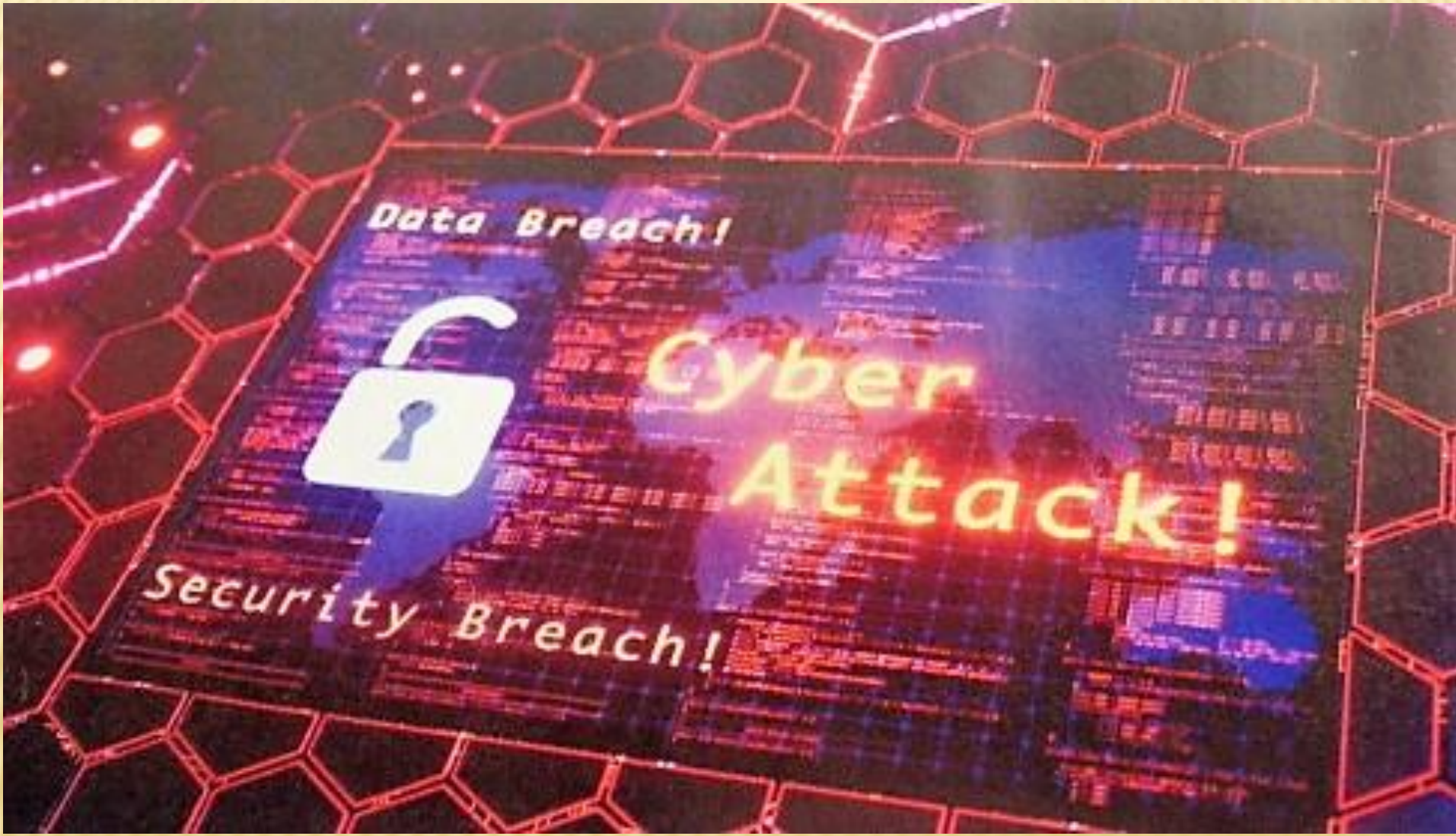


FATTORI CAUSALI NEL COINVOLGIMENTO DEI DIPENDENTI NELLE VIOLAZIONI INFORMATICHE

MODALITÀ DI ATTACCO INFORMATICO

- Debolezze intrinseche nei sistemi informativi
- Mancato aggiornamento delle misure di sicurezza
- **Ignoranza** nei comportamenti dei soggetti fisici coinvolti
- N**egligenza** nei comportamenti dei soggetti fisici coinvolti
- **Ingenuità** nei comportamenti dei soggetti fisici coinvolti
- **Dolosità** nei comportamenti dei soggetti fisici coinvolti

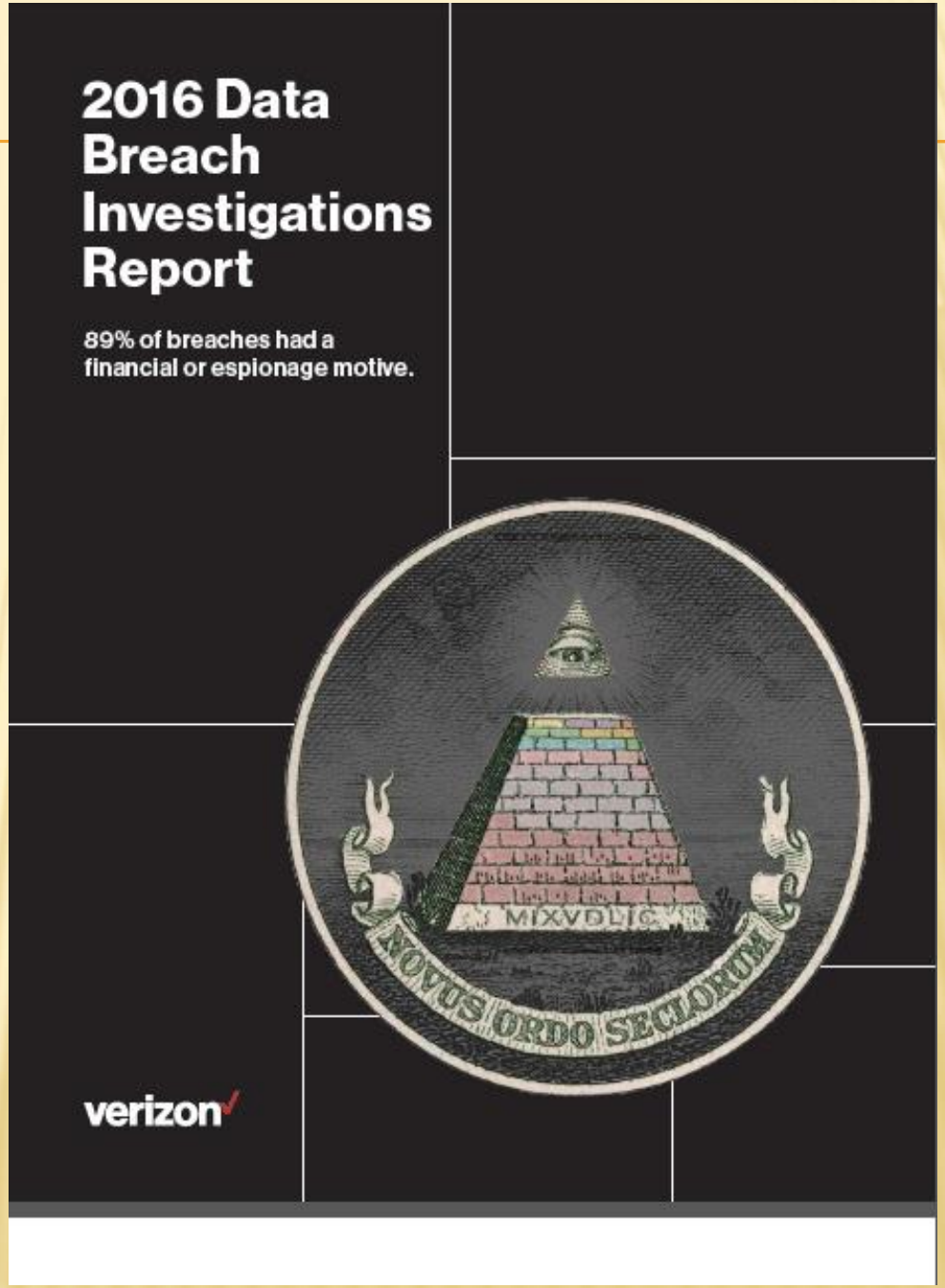
- Ignoranza – non ti detto come comportarti
- Negligenza – ti ho detto come comportarti e non lo hai fatto!
- Ingenuità – le istruzioni di comportamento erano incomplete
- Dolosità – senza commenti

QUALCHE DATO STATISTICO SUGLI ENTI COINVOLTI

- Istituzioni finanziarie 3,7 %
- Industria e commercio 33,9%
- Settore Educazione e scuole 9%
- Settore governativo e militare 10,2%
- Settore sanitario 43%

- *Identity theft response center 2013*

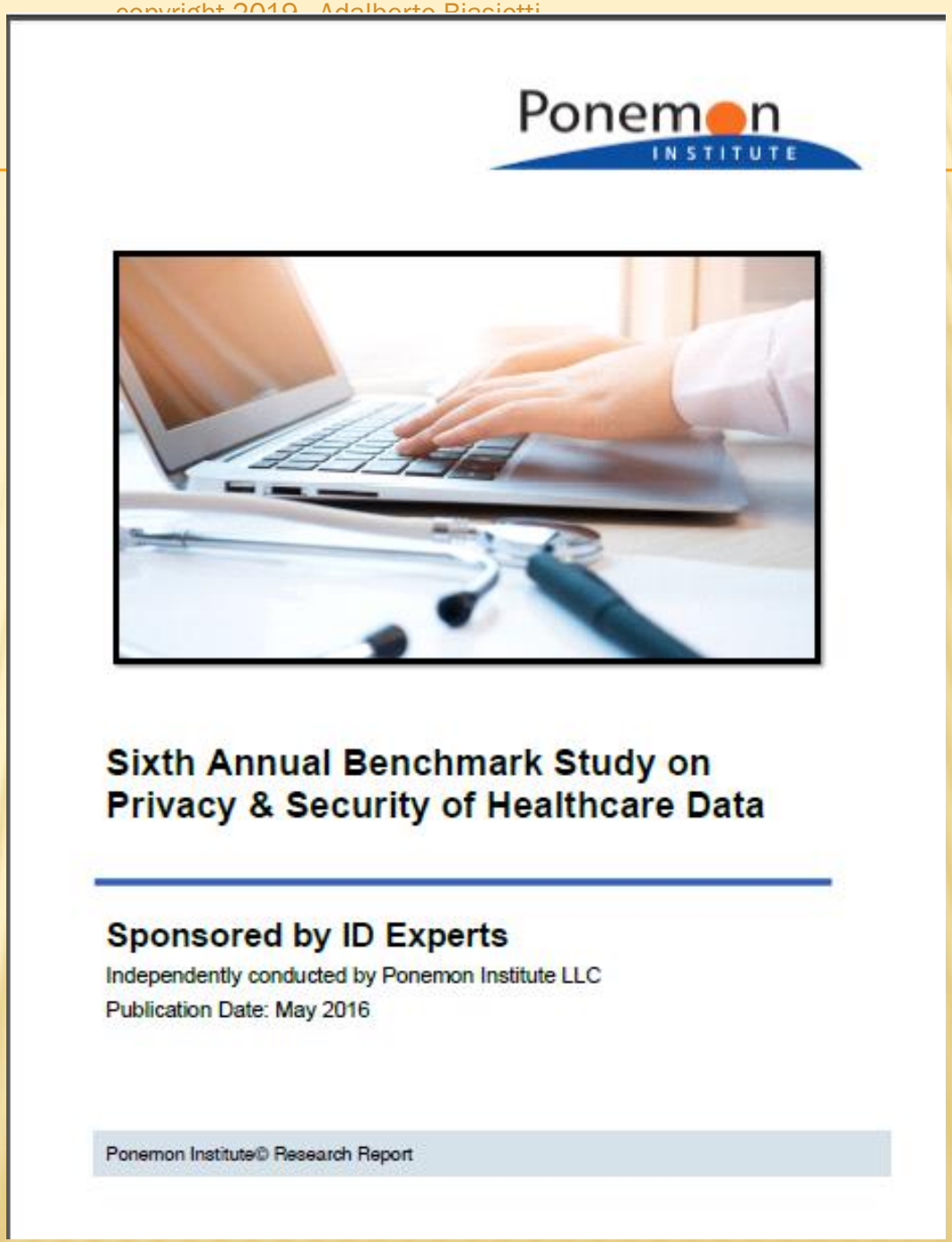
UN DOCUMENTO PREZIOSO



LO STUDIO PONEMON DEL 2016

- Quasi il 90 % delle strutture sanitarie ha registrato una perdita di dati negli ultimi due anni ad un costo medio di $ 2,2 milioni per perdita
- Addirittura il 79 % delle strutture sanitarie ha registrato almeno due perdite di dati e il 45 % cinque perdite di dati
- Questo l'esito di una serie di interviste presso 200 strutture sanitarie, aziende farmaceutiche, produttori di dispositivi sanitari e simili
- Il dato più spesso violato è la cartella clinica, seguita da dati assicurativi ed afferenti pagamenti
- La teoria che la salute sia più importante della privacy non può reggere ancora a lungo!

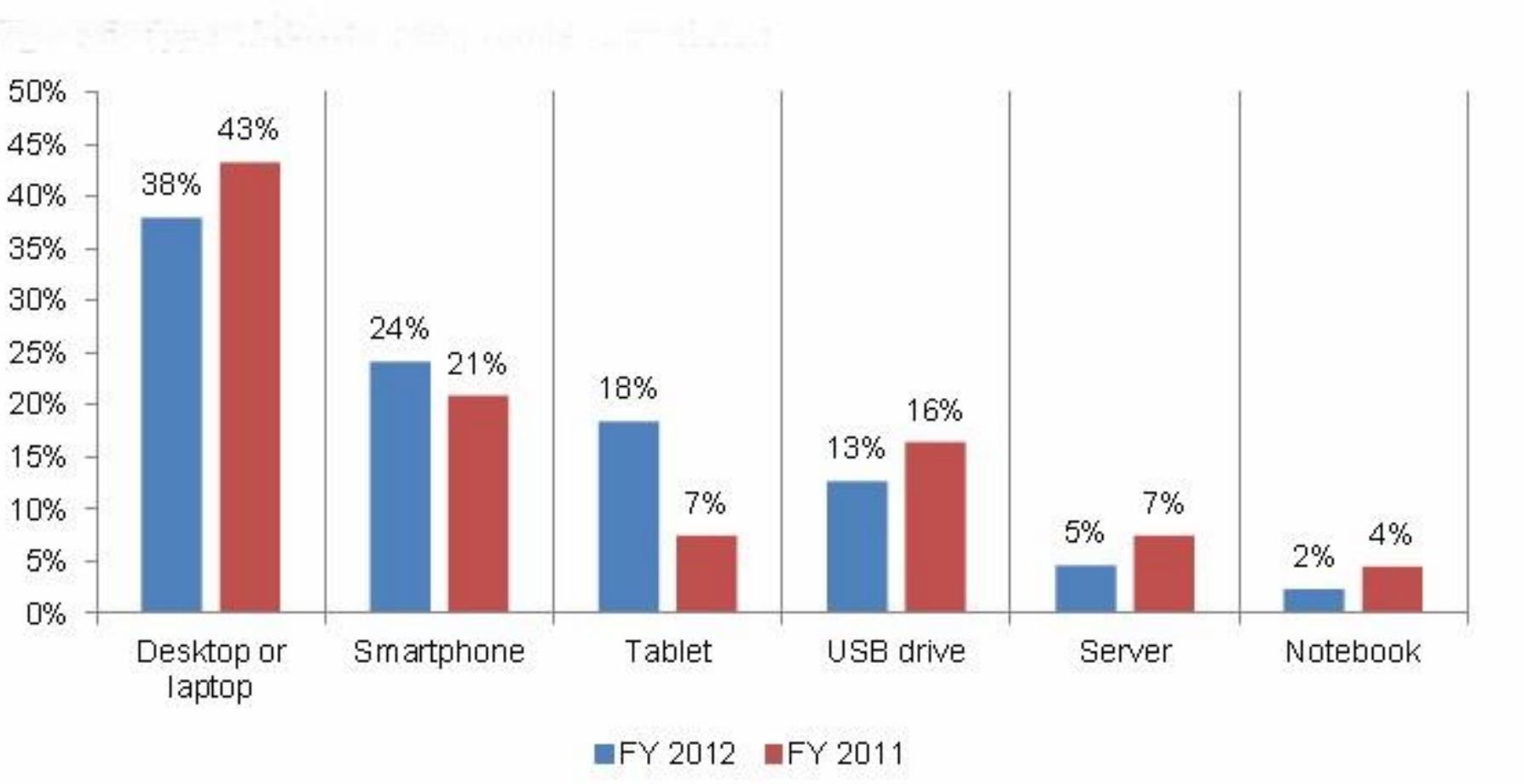
IL MONDO DELLA SANITÀ FA RABBRIVIDIRE



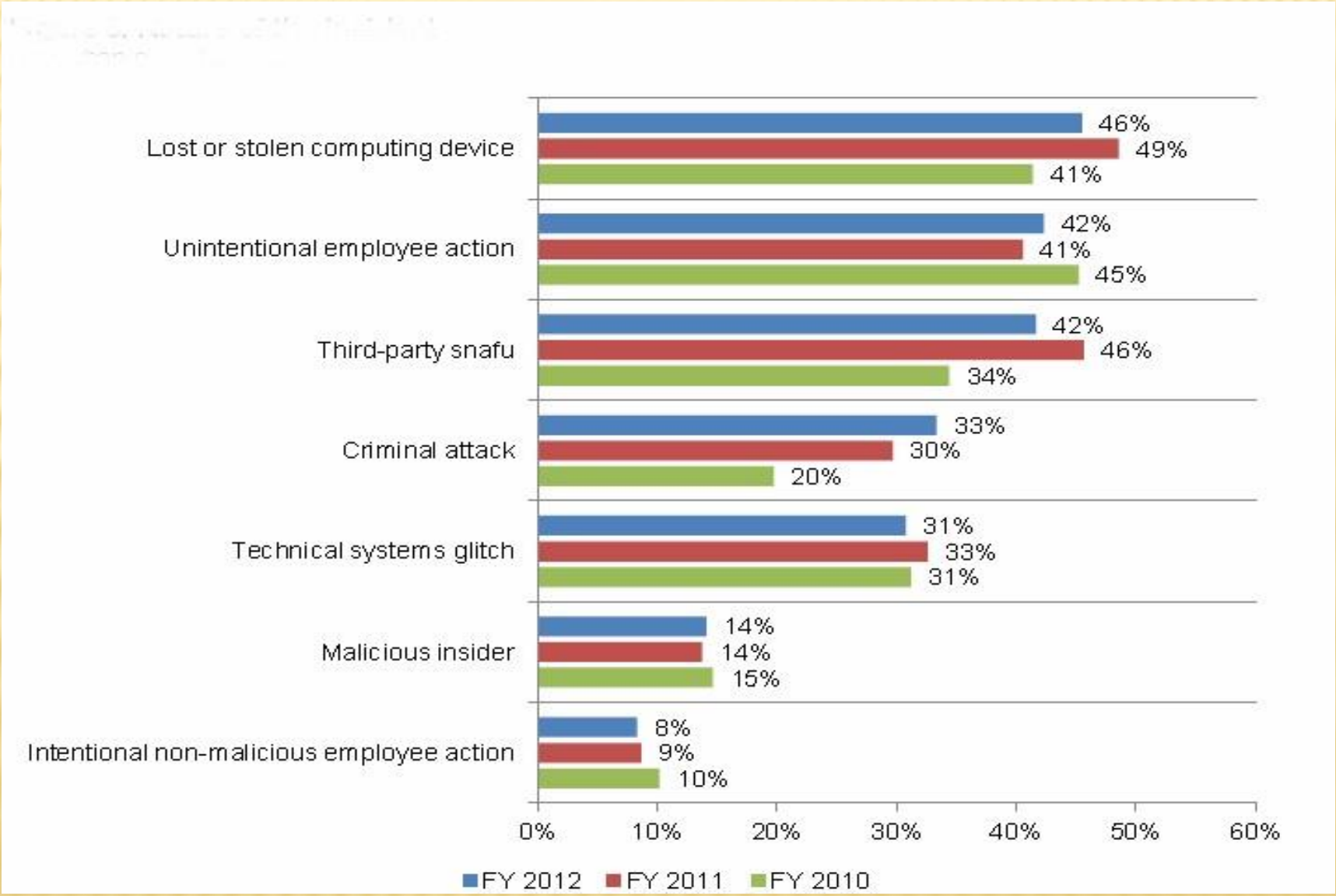
UNO STUDIO SU STRUMENTI E COMPORTAMENTI, CHE HANNO PORTATO A VIOLAZIONE INFORMATICA O PERDITA DI DATI

- Tabella 1 – gli apparati informatici coinvolti
- Tabella 2 – i comportamenti dei soggetti coinvolti

TIPOLOGIE DI STRUMENTI COINVOLTI - 1



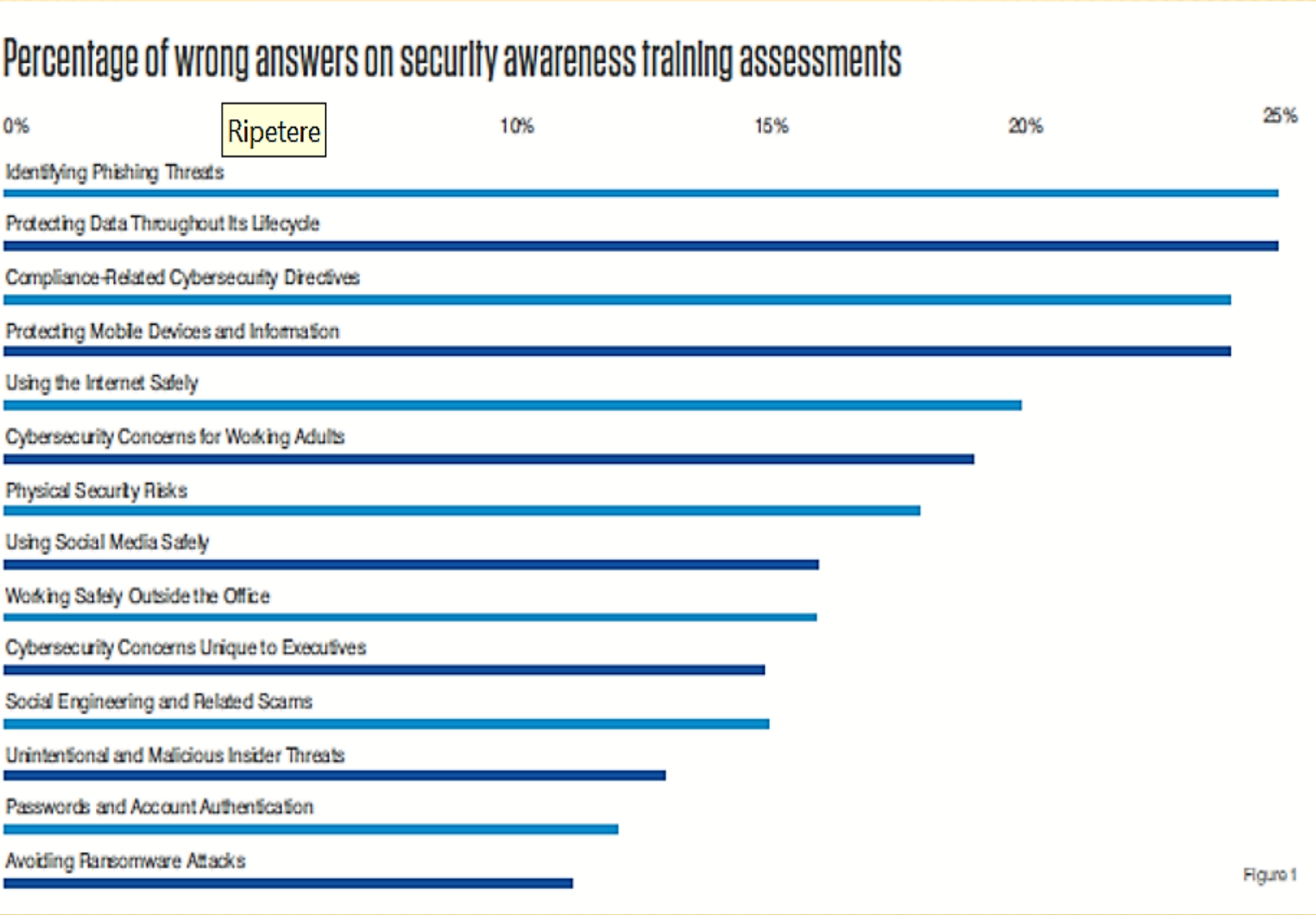
I COMPORTAMENTI COINVOLTI - 2



- Il 50% delle violazioni o perdite informatiche è dovuto a comportamenti dei dipendenti non diligenti e negligenti, ma non dolosi

- La educazione ed il monitoraggio dei dipendenti rappresentano quindi un aspetto essenziale in una politica di protezione da attacchi informatici

UNO STUDIO DEL 2019 OFFRE UN PANORAMA ASSAI PREOCCUPANTE


Percentage of wrong answers on security awareness training assessments
0%
Ripetere
10%
15%
20%
25%
Identifying Phishing Threats
Protecting Data Throughout Its Lifecycle
Compliance-Related Cybersecurity Directives
Protecting Mobile Devices and Information
Using the Internet Safely
Cybersecurity Concerns for Working Adults
Physical Security Risks
Using Social Media Safely
Working Safely Outside the Office
Cybersecurity Concerns Unique to Executives
Social Engineering and Related Scams
Unintentional and Malicious Insider Threats
Passwords and Account Authentication
Avoiding Ransomware Attacks
Figure 1

- Identificare le minacce di pishing
- proteggere i dati nell'arco dell'intero ciclo di vita
- rispettare le procedure di sicurezza informatica
- proteggere i dati su supporti mobili
- usare con attenzione Internet
- prestare attenzione ai rischi fisici
- usare con prudenza i social media
- operare in modo sicuro anche fuori dell'ambiente lavorativo
- ritenere che la sicurezza informatica sia solo un problema dei dirigenti
- prestare attenzione a rischi di origine interna, sia accidentale, sia dolosa
- usare correttamente i profili di accesso e di autentica
- evitare gli attacchi ransomware

SO CHE È DIFFICILE DA CREDERE, MA IL 90% DELLE SCHEDE DI MEMORIA DI SMARTPHONE, RESTITUITE O SOSTITUITE DALL'UTENTE, SONO ANCORA PIENE DI DATI PERSONALI!

VI RACCONTO UN CASO VISSUTO

- A tutti i dipendenti è stata distribuita una circolare, con la proibizione di utilizzare chiavette USB di origine non sicura
- Sono state sparpagliate parecchie chiavette USB, prive di qualsiasi contrassegno, sui tavoli e sui pavimenti dell'insediamento sotto test
- Più di tre quarti delle chiavette sono state prese dai dipendenti ed utilizzate senza alcuna precauzione, sia in ufficio, sia a casa
- Su ogni chiavetta era stato caricato un applicativo, che segnalava a distanza il fatto che la chiavetta era stata utilizzata e su quale terminale
- **PER FAVORE, VORREI ASCOLTARE I VOSTRI COMMENTI!**

COME USARE UNA CHIAVETTA USB REGALATA

- Spesso durate mostre e fiere gli espositori regalano chiavette USB con testi ed informazioni varie
- Non apritele mai sul vostro PC, ma su quello di un amico (!) o su una postazione pubblica
- Estraete quanto vi interessa, indi formattate la memoria
- Se la chiavetta USB è priva di dati, formattatela lo stesso!

UNA AREA DI RISCHIO IN CRESCITA ESPONENZIALE: SMARTPHONE E SIMILI

- **I responsabili della sicurezza informatica hanno davanti due strategie:**
- *consegnare al dipendente coinvolto uno smartphone di proprietà aziendale, sul quale il responsabile della sicurezza informatica ha pieno controllo*
- *consentire al dipendente di utilizzare il proprio smartphone, anche per usi aziendali.*
- *Quest'ultima strada viene chiamata BYOD - Bring your own device*

LA PRIMA STRATEGIA

- Alla luce del costo sempre più contenuto degli smartphones, non vi sono ostacoli di natura economica
- I vantaggi afferenti alla sicurezza sono significativi; ad esempio, è possibile cancellare a distanza tutti i dati presenti, in caso di necessità
- Vi sono invece ostacoli di natura personale, perchè il dipendente non gradisce di dover gestire due diversi apparati, il proprio e quello aziendale, che magari usano due diversi sistemi operativi

LA SECONDA STRATEGIA - BYOD

- Il dipendente per solito non pone ostacoli ad un uso promiscuo, a certe condizioni
- È possibile inserire sullo smartphone del dipendente degli applicativi di controllo da remoto, assai poco graditi al dipendente
- L'azienda risparmia quattro soldi e si espone e rischi elevati

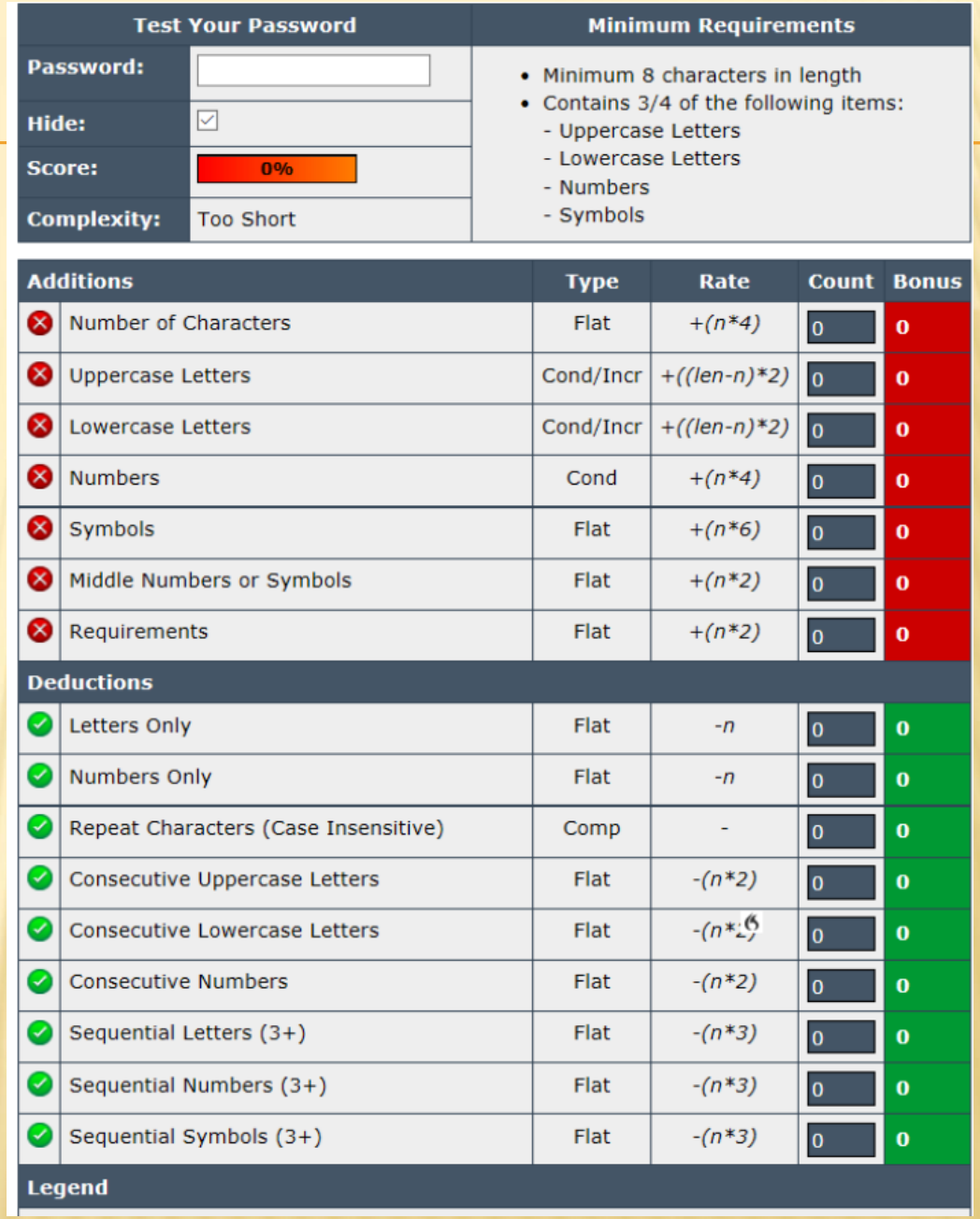
GLI INTERVENTI DI MESSA SOTTO CONTROLLO DEL RISCHIO BYOD

- Imporre al personale di attivare sempre la protezione di accesso al dispositivo, sia con impronta digitale, sia con parola chiave
- Raccomandare al personale di ridurre al minimo i dati aziendali che vengono caricati sullo smartphone. In caso, questi dati devono essere inseriti in una specifica directory, ad accesso protetto e debitamente criptografati
- Di concerto con il responsabile della sicurezza informatica, può essere opportuno attivare un applicativo di cancellazione automatica di questa directory, con comando remoto
- L'azienda deve stipulare un contratto con un servizio di manutenzione degli smartphone, in modo da essere certa che, in caso di malfunzionamento dell'apparato, esso venga affidato ad azienda di fiducia e non ad un qualsiasi punto di assistenza, la cui affidabilità può essere ignota.

INFINE: COME SCEGLIRE UNA PAROLA CHIAVE AFFIDABILE

- L'esperienza insegna che la violazione della parola chiave, sia su apparati portatili, sui su apparati fissi, rappresenta la più diffusa situazione, che porta ad una violazione dei dati personali aziendali, cui l'autorizzato ha accesso
- I responsabili della sicurezza sono soliti offrire consigli "sadici", come ad esempio imporre caratteri maiuscoli, minuscoli, §, £, ¥, e simili.
- L'esperienza insegna che la scelta di una parola chiave, basata su questi criteri, impone un onere sproporzionato all'autorizzato, che finisce assai spesso nel trascrivere la parola chiave, violando così una precisa disposizione di sicurezza.
- Esistono sistemi più responsabilizzanti, di cui offro un esempio

WWW.PASSWORDMETER.COM



Test Your Password		Minimum Requirements
Password:		• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	0%	
Complexity:	Too Short	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	0	0
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	0	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0
Legend				

ED ORA UNA SINTESI DEGLI INTERVENTI RACCOMANDATI

- Sensibilizzazione e formazione dei dipendenti
- Attenzione al social engineering
- Attenzione al phising
- Attenzione ai messaggi attraenti, provenienti da fonti non conosciute
- Attenzione alla sicurezza fisica
- Attenzione a creare parole chiave robuste
- Cifrare tutto ciò che è possibile cifrare
- Fare frequenti backup e custodire bene i supporti
- Tenere sempre aggiornati i programmi di sicurezza
- Attenti all'uso di reti wifi
- Non lasciate il computer attivo e non presidiato
- Usare sempre il salva schermo automatico

CONOSCETE QUESTE MASSIME?

- Non ho paura del nemico che mi attacca, ma del falso amico che mi abbraccia
- Ci sono amici bravi e amici falsi… ma soprattutto amici bravi a fare i falsi
- Dagli amici mi guardi Iddio, che dai nemici mi guardo io

GRAZIE PER LA ATTENZIONE