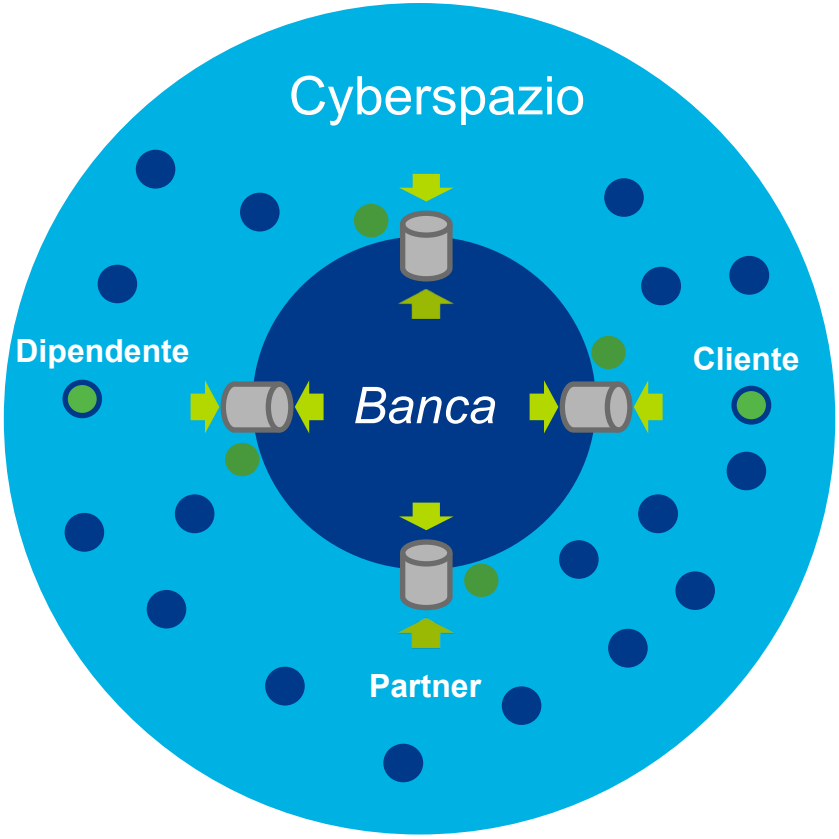
Indice

Background

Cyber Security
Un paradigma di protezione dei dati che cambia

Nel Cyberspazio cambiano completamente i paradigmi di protezione classici: non si governa ciò che è noto e che sta all'interno del perimetro della Banca, ma ci si deve preparare a governare l'ignoto, ciò che non si conosce e che sfugge al controllo dell'organizzazione, proprio perché i rischi si concretizzano nel Cyberspazio.

Obiettivi	Implicazioni sulla sicurezza
Consumerisation ('bring your own')	De-perimeterisation and loss of control of data and devices
Collaboration	Cross-channel, cross-platform sharing of large volumes of sensitive data
Technology innovation	Lack of understanding of risks introduced by new tools and processes
Commoditisation of IT (e.g. cloud computing)	Business functions can procure IT services outside of internal controls
Market trust	Reputational damage of a cyber attack destroys trust which is very hard to recover
Globalisation	New threats arising from expansion into new markets and new ways of working



Cyber risks and threats

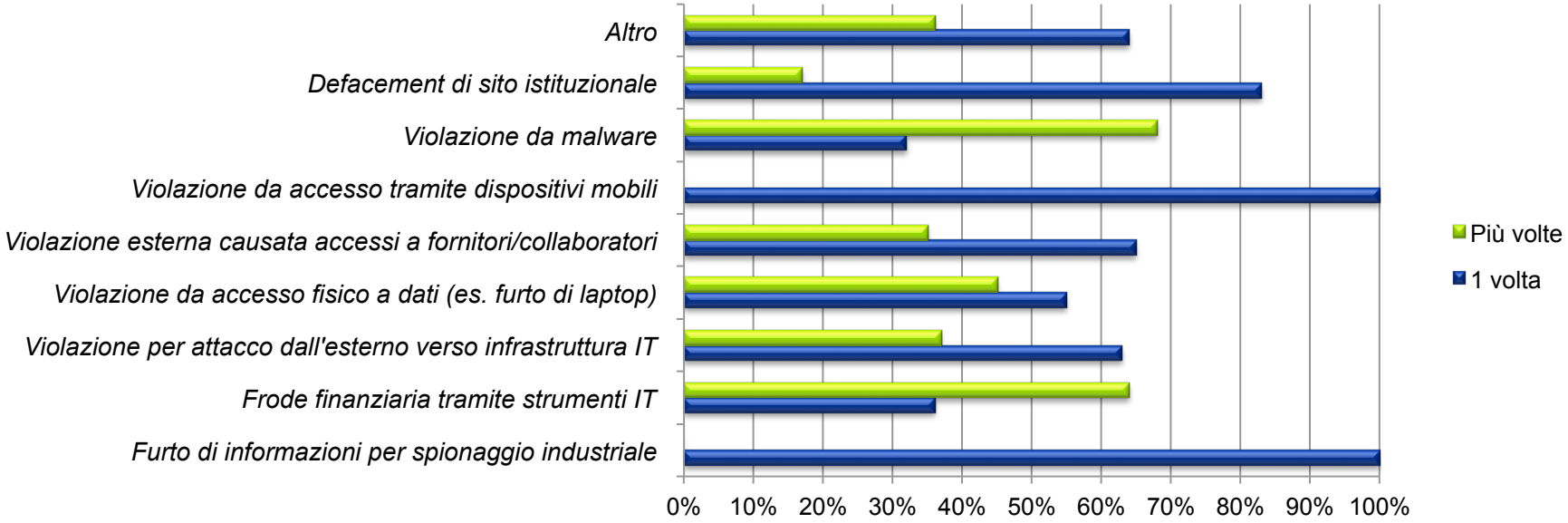
Cyber Risk and threats
Quello che succede nel mondo reale

- Nell'ultimo anno le più grandi realtà FSI sono state più volte oggetto di attacchi hacker di elevata complessità:

Cyber Risk and threats
Quello che succede nel mondo reale

- Key findings della Survey Deloitte del 2012 sul mondo FSI:
  - il 25% delle aziende dichiara di aver subito attacchi dall'esterno durante il 2012
  - il 31% delle aziende dichiara di aver subito attacchi dall'interno durante il 2012
  - Le tipologie di attacco sono innumerevoli

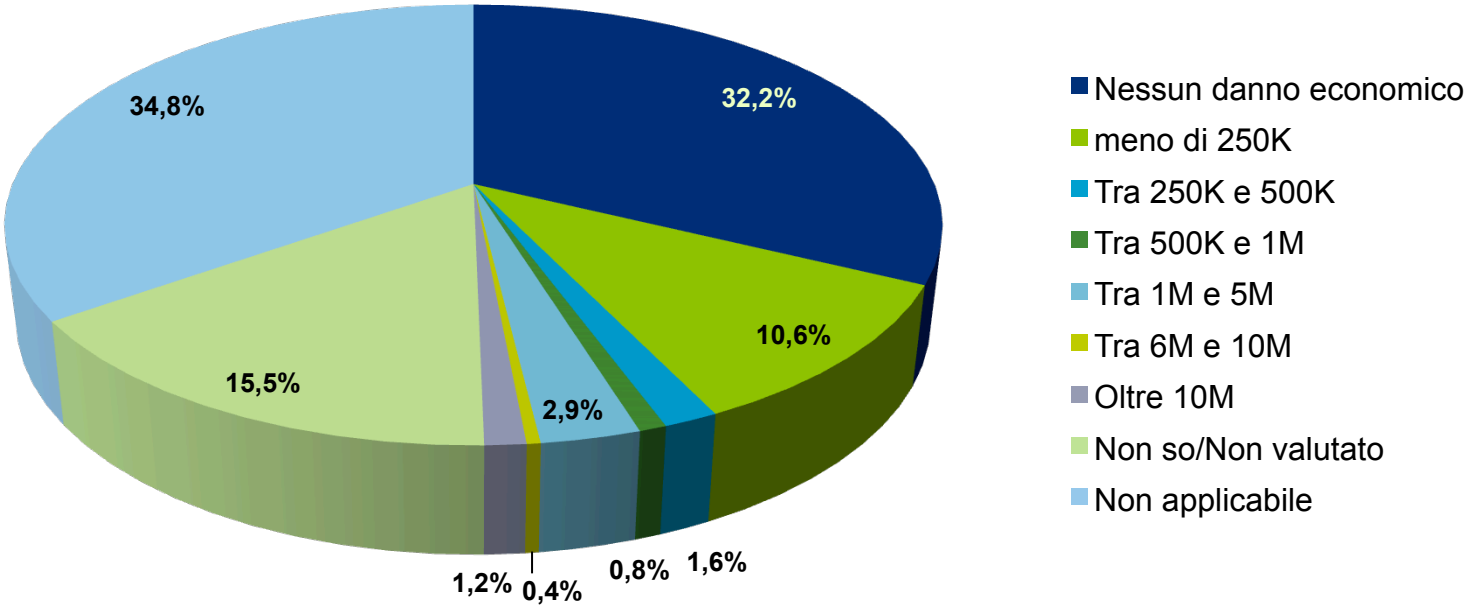
Tipologie di attacco dall'esterno alle quali le aziende sono state soggette nel 2012:



*Survey Deloitte del 2012 su oltre 250 organizzazioni del settore FSI nel mondo

Cyber Risk and threats
Quello che succede nel mondo reale

- I danni economici, diretti ed indiretti, provocati da queste violazioni possono essere elevati anche se non sempre facili da quantificare
- Oltre il 15% delle aziende **non conosce o non è in grado di valutare** l'entità del danno economico subito



* Valori in $

Cyber Risk and threats
I fattori da considerare

1	Gli eventi recenti portano ad accrescere l'attenzione verso i cyber risks	Implicazioni finanziarie, rischio reputazionale, operativo e di compliance con le normative
2	Gli attori coinvolti sono spesso diversi, e spinti da diverse motivazioni	Hactivists, criminali informatici, dipendenti, fornitori, stati
3	Le violazioni possono avvenire in qualsiasi momento, verso ogni punto	Internet, mobile, social networks, cloud, serve un approccio di sicurezza data-centrico
4	Gli attacchi sfruttano debolezze nei metodi di controllo tradizionali	Phishing, malware sofisticati, vulnerabilità software, ecc
5	Gli attacchi sfruttano l'anello più debole	Infrastrutture IT, fornitori, dipendenti, collaboratori, clienti, etc

Cyber Risk and threats
I fattori da considerare

6	Gli attaccanti non hanno confini geografici nazionali	Le normative nazionali non possono tutelare da attività eseguite da alcuni stati esteri
7	La velocità di esecuzione degli attacchi aumenta, il tempo per la reazione diminuisce	I dati possono essere trasferiti prima che le contromisure riescano ad impedirlo
8	I dati hanno un valore, che i criminali sanno monetizzare	Dati personali dei clienti, dati societari, commerciali, proprietà intellettuali
9	I controlli tradizionali sono necessari, ma non adeguati ai nuovi rischi	Serve un nuovo approccio di prevenzione e reazione, anche verso le nuove tecnologie
10	Le violazioni possono portare a rischi normativi	L'attenzione delle istituzioni è solo verso alcuni aspetti della sicurezza

Cyber Risk and threats
Il punto di vista del Chief Security Officer

- I controlli tradizionali (es. Antivirus) non sono sufficienti
- I rischi possono provenire da qualsiasi classe di soggetti
- User-id e password sono spesso insufficienti
- La cifratura è un arma a doppio taglio (anche i criminali la usano mentre rubano i dati)
- Il furto di credenziali porta spesso al danno maggiore
- Le vulnerabilità sono il vettore principale di attacco
- La mancanza di standard tecnologici comporta aumento della complessità e dei rischi
- Serve personale preparato per affrontare sfide sempre più complesse
- Essere conforme alle normative non vuol dire gestire in maniera esaustiva il rischio

Gestione dei rischi con una crescente attenzione ai costi

Serve un nuovo approccio strategico per la gestione dei rischi

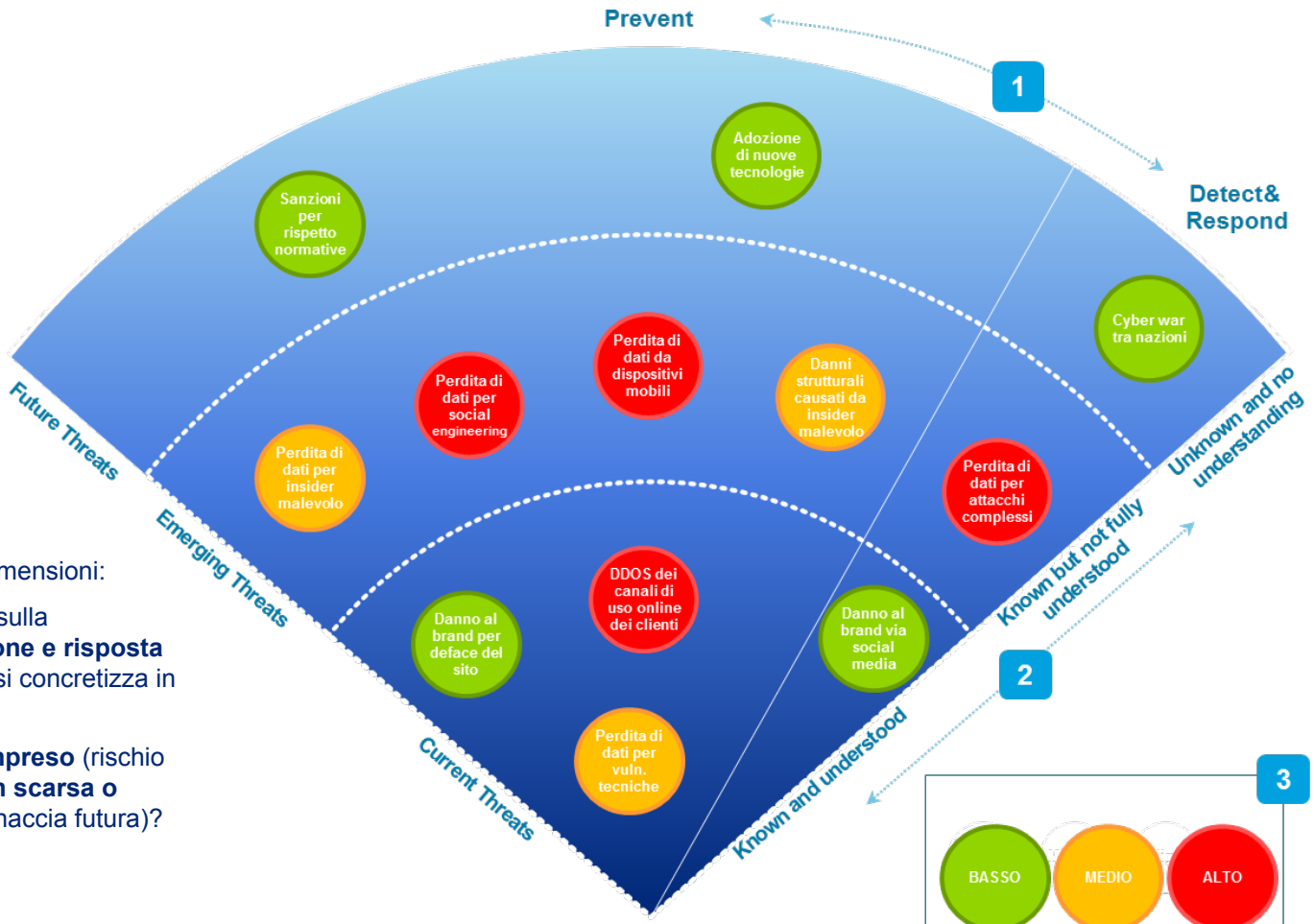
Essere pronti

Essere pronti
I principi chiave

- Quali sono i principi chiave su cui basare la definizione di una strategia di per la cyber security?

Essere pronti
Comprendere le minacce

- Analizzare le potenziali minacce è fondamentale per potersi preparare nei giusti modi. Attacchi diversi richiedono risposte diverse.



I rischi sono mappati secondo tre dimensioni:

1. L'organizzazione si focalizza sulla **prevenzione** o sulla **rilevazione e risposta** al rischio una volta che esso si concretizza in un incidente?
2. Il rischio è **conosciuto e compreso** (rischio corrente), o **sconosciuto con scarsa o nessuna comprensione** (minaccia futura)?
3. Quale **impatto** ha il rischio?

Essere pronti
Gli step fondamentali

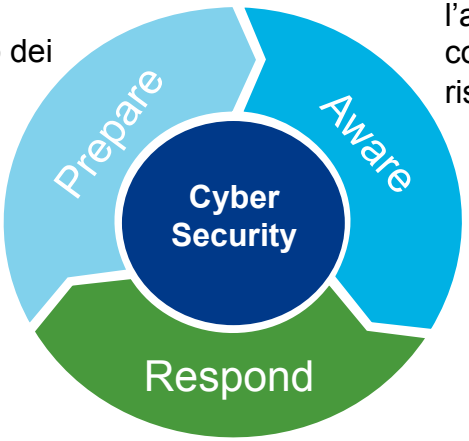
- Serve un processo continuo e costante, che consenta di **prepararsi** agli eventi, **conoscerne** le entità ed i significati e avere strutture e procedure per **rispondere** al meglio.

Cyber Readiness Assessment

Misura del livello di maturità della gestione dei Cyber Risks, identificazione dei gap e sviluppo dei piani correttivi

Cyber Threat Intelligence

Analisi preventiva dell'ambiente in cui l'azienda opera, tramite monitoraggio costante e gestione dinamica dei rischi



Cyber Resilience

Miglioramento delle capacità di reazione ad attacchi e violazioni, recuperando produttività

Vulnerability Management

Identificazione e test di vulnerabilità note o meno. È il primo passo di un approccio preventivo completo

Cyber Forensics

Analisi di un incidente informatico. Chi ha fatto cosa, quando e come? Come prevenire l'incidente prima che accada di nuovo?

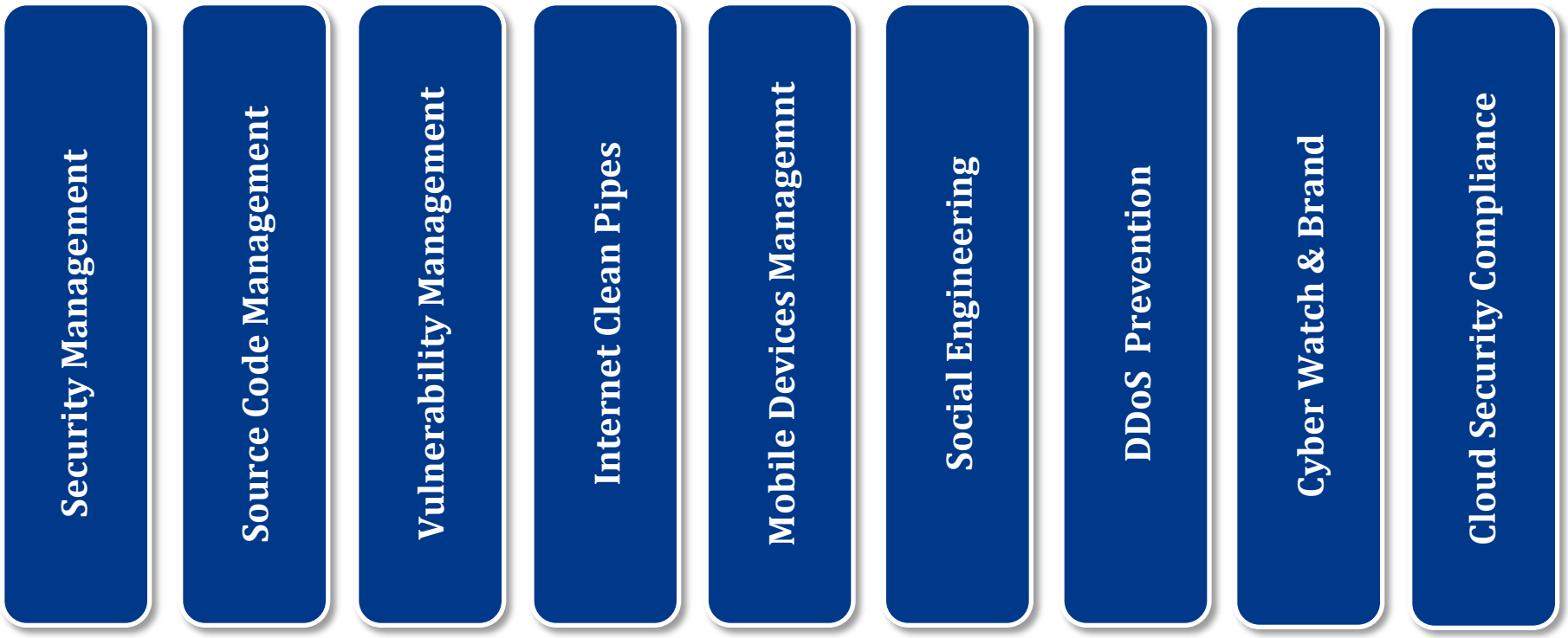
Cyber Incident Management

Identificazione degli incidenti, con risposta immediata ed azioni efficaci per contenerne i danni e ridurre al minimo l'impatto.

Essere pronti

Le diverse dimensioni di un programma di Cyber Security

- Un buon programma di Cyber Security per una banca richiede di gestire diverse dimensioni, come mostrato di seguito



Questions and Answers?


Deloitte.