
# *Economia della sicurezza informatica e cyber-risk management. Il caso della Bank of Valletta*

**Lorenzo Bonucci**


UNIVERSITÀ
DEGLI STUDI
FIRENZE

**Research Analysis**

*Aprile 2019*

**Center for Cyber Security and International Relations Studies (CCSIRS)**

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

**https://www.cssii.unifi.it/ls-6-cyber-security.html**

Center for Cyber Security and International Relations Studies

# *Economia della sicurezza informatica e cyber risk management. Il caso della Bank of Valletta*

**Lorenzo Bonucci**

UNIVERSITÀ DEGLI STUDI FIRENZE

**Research Analysis**

*Aprile 2019*

# Riguardo all’autore

**Lorenzo Bonucci** Si è laureato con lode in Relazioni Internazionali e Studi Europei presso la "Cesare Alfieri" di Firenze, con una tesi sulla guerra economica nella prospettiva francese e si occupa, principalmente, di studi sulla sicurezza. Ha preso parte, in qualità di assistente di ricerca, al progetto OSCE in collaborazione con l'Università degli Studi di Firenze: "Enhancing the Implementation of OSCE Confidence Building Measures in order to Reduce the Risks of Conflict Stemming from the Use of ICTs". Ha lavorato per l'Italian Chamber of Commerce and Industry for the UK, a Londra, occupandosi di innovazione e FDI ed ha fatto uno stage presso l'Ambasciata d'Italia a Doha, Qatar, dove è stato impiegato in ambito di diplomazia economica. Attualmente vive a Bruxelles, e lavora come Policy and Project Assistant presso EOS - European Organisation for Security collaborando, prevalentemente, alla ricerca per progetti in ambito di counter-terrorism e cybersecurity e risk management. È stato redattore web del CSSII-CCSIRS fino a maggio 2018

# Economia della sicurezza informatica e cyber risk management. Il caso della Bank of Valletta[1]

È ormai ampiamente risaputo che gli attacchi informatici possono danneggiare beni immateriali quali la reputazione, la proprietà intellettuale e il *know-how*. Tuttavia, esiste ancora una grande disparità tra l'efficienza degli attacchi e la solidità delle difese, sempre troppo inadeguate. Risulta di grande interesse, quindi, sia per le imprese private che per gli enti pubblici, avere la corretta percezione del *cyber-risk*, ossia saper quantificare il rischio che si corre mantenendo bassi gli investimenti in cyber security.

Tramite il progetto Hermeneut[2] – finanziato dal programma "Horizon2020" – un consorzio composto da enti di ricerca, organizzazioni di *advocacy* e aziende del ramo security sta sviluppando un modello micro e macroeconomico per stimare quantitativamente le conseguenze degli attacchi cibernetici verso i beni intangibili. Attraverso un'analisi dinamica del *risk assessment* e una valutazione integrata delle vulnerabilità dei sistemi informatici, il consorzio mira a promuovere la cultura della gestione del rischio e a fornire un'innovativa metodologia di valutazione dell'impatto che possono avere gli attacchi cibernetici non solo sui beni tangibili di un'azienda, ma anche su quelli intangibili.

In questa cornice s'inserisce il caso della Bank of Valletta[3]. Il 13 febbraio scorso, la banca della capitale maltese ha deliberatamente

[1] La seguente analisi è apparsa su Formiche.net il giorno 14 aprile 2019 ed è reperibile al seguente link: https://formiche.net/2019/04/economia-sicurezza-cyber-risk-management-bank-valletta/.
[2] https://www.hermeneut.eu/.
[3] Times of Malta, "BOV goes dark after hackers go after €13", 13 febbraio 2019, reperibile al seguente link: https://timesofmalta.com/articles/view/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896.

bloccato tutte le su funzioni per mitigare gli effetti di un potente attacco informatico. Sostanzialmente, la banca, ha interrotto tutti i servizi: filiali, Atm, mobile banking app – oltre ad aver oscurato il sito web – dopo che alcuni hackers erano riusciti a penetrare il suo sistema informatico e trasferire una somma di circa 13 milioni di euro su una serie di conti esteri. La mitigazione implementata ha limitato gli effetti dell'intrusione. La banca ha rassicurato che i correntisti non sono stati compromessi, ma ha anche sottolineato che l'azione avrebbe potuto seriamente intaccare il capitale intangibile della società.
Ed è proprio questo l'elemento che dobbiamo seriamente tenere in considerazione. Prendiamo uno degli *asset* intangibili più importanti: la reputazione. Saranno tranquilli i clienti di una banca che per mitigare un attacco cibernetico altro non può fare che bloccare qualsiasi tipo di operazione? Quanto è stata importante la perdita di reputazione per l'istituto maltese? Tale "colpo" genera una conseguente perdita di clienti? E non finisce qui. Considerando le condizioni dell'istituto di credito in sé: come possiamo quantificare l'impatto sul valore del brand? I servizi online e B2B correlati si basano sulla continuità operativa 24/7, pertanto un'interruzione giornaliera potrebbe avere un effetto significativo sulla salute della banca stessa.

Questo caso ci fa capire che il vero problema di tali attacchi è la serie di effetti collaterali che portano. Purtroppo, come si sente spesso affermare dagli addetti ai lavori, molte aziende continuano ancora a non dotarsi di strumenti di difesa adeguati, alimentando così un vero e proprio circolo vizioso.

Infatti, seguendo l'analisi del sopracitato progetto, si riscontra che sovente gli approcci all'IT security tendono a sottostimare alcuni aspetti chiave degli attacchi cibernetici, quali il fattore umano, il peso delle risorse immateriali e le strategie dei cyber attaccanti. Nel caso

appena riportato, si può osservare come vi sia stata una sottovalutazione del secondo e del terzo elemento. Difatti, più della metà del valore delle società di tutto il mondo consiste in beni immateriali (come la proprietà intellettuale) e molti di essi sono altamente vulnerabili agli attacchi informatici.

L'altro problema non sufficientemente affrontato è quello relativo alle nuove strategie degli hacker. Si è osservato che al giorno d'oggi queste seguono la stessa logica commerciale utilizzata dalle grandi aziende nella definizione dei loro piani. In sostanza, la stessa combinazione multidisciplinare di ingegneria, valutazione del rischio e conoscenze economiche, comportamentali e legali che mirano a scoprire i punti più deboli ed attaccarli, in modo tale da paralizzare tutta la struttura di sicurezza della "preda" prescelta.

Insomma, la capacità di saper quantificare il rischio 'cyber' dovrebbe essere un elemento imprescindibile per formare il 'paniere' della domanda di security aziendale. Una maggiore consapevolezza dell'impatto che un attacco cibernetico ha sul capitale intangibile potrebbe essere, oltretutto, la leva per dare una spinta alla messa in sicurezza di molteplici attori privati e del sistema-Paese in generale.

**Center for Cyber Security and International Relations Studies (CCSIRS)**

Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CCSSII)

Università degli Studi di Firenze

Via delle Pandette 2, 50127, Firenze

**https://www.cssii.unifi.it/ls-6-cyber-security.html**