La sicurezza Informatica

Agenda

1. I nuovi rischi
2. L’approccio alla sicurezza in Banca
3. La declinazione nel tempo
4. La normativa
5. I ruoli organizzativi
6. Il personale interno ed esterno
7. La tecnologia
8. I processi
9. Cyber Resilience

1 I nuovi rischi

I rischi sono in continua evoluzione:

- Cyber risk
- Information *warfare*
- Perdita di informazioni
- Risposta disarticolata ai rischi
- Interdipendenza tra sistemi informatici
- Rischio tecnologico
- Scomparsa del “perimetro” fisico

2 L’approccio alla sicurezza in Banca

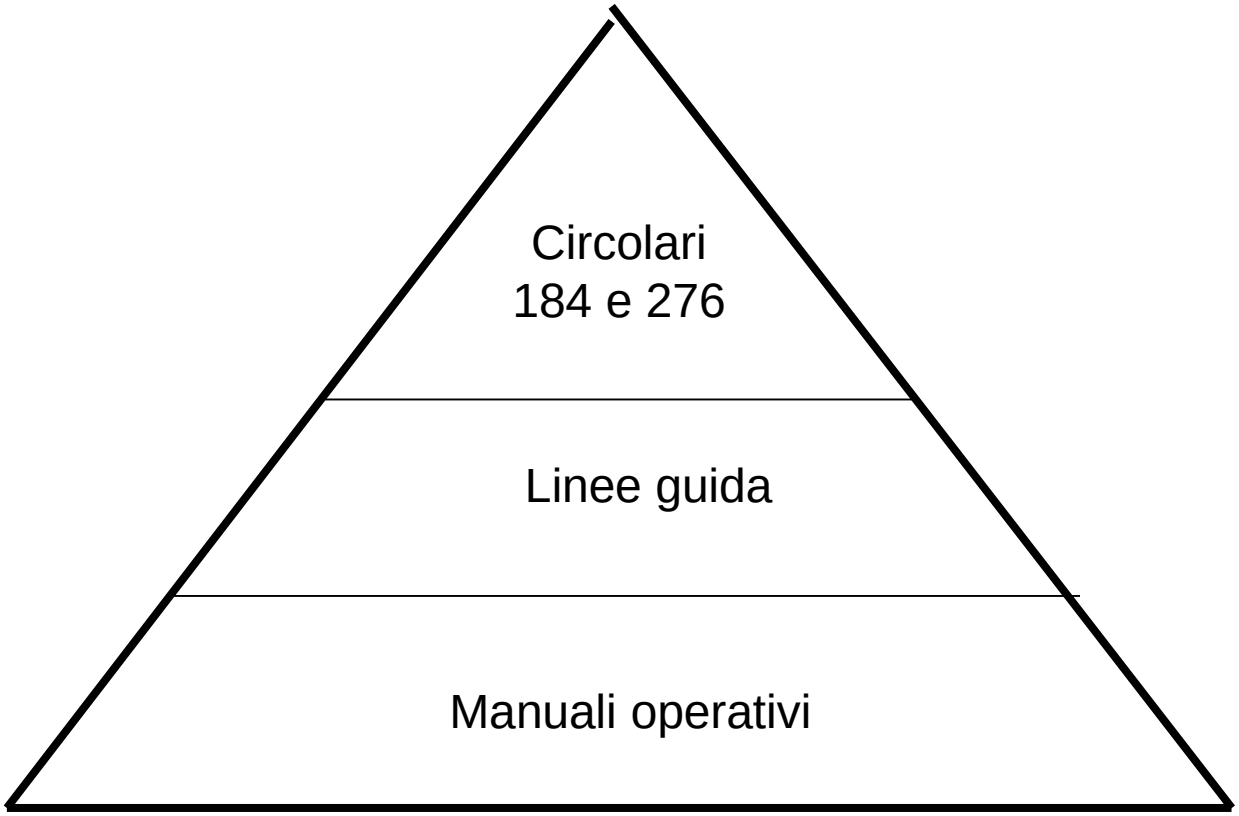
L’approccio alla sicurezza dell’informazione è basata su:

- Organizzazione
- Tecnologia
- Personale interno ed esterno
- Processi

3 La declinazione nel tempo

- 1989: nascita della Funzione di sicurezza informatica all'interno della DSS del SESI; sicurezza tecnologica dell'ambiente mainframe
- 1993: emanazione della Normativa Quadro di Sicurezza Informatica; sicurezza applicativa; organizzazione strutturata; approccio *risk avoidance*
- 1994: nascita della Divisione Sicurezza Informatica del SESI; sicurezza dei sistemi dipartimentali e delle reti; si rafforza il processo di sicurezza sui mainframe e sulle applicazioni; monitoraggio della sicurezza mainframe
- 2003: l'amministrazione della sicurezza viene spostata dalla DSI alla DPLS; individuazione e strutturazione dei processi di sicurezza; approccio al rischio; primi programmi di sensibilizzazione
- 2009: riorganizzazione della funzione informatica: organizzazione per processi separati (progettazione esercizio); emanazione della nuova Normativa Quadro di Sicurezza Informatica; approccio *risk acceptance.*
- *2017 CERT e SOC* Cyber *resilience*

4 la normativa



5 I ruoli organizzativi

- CTI
- Servizio Organizzazione
- *system owner*
- SVI
- GES
- PIA
- Servizio Revisione Interna
- Personale interno ed esterno

5 I ruoli organizzativi
5.1 CTI

- A livello strategico, le funzioni di supervisione, indirizzo, coordinamento e controllo della sicurezza delle risorse informatiche dell'Istituto sono prerogativa del Direttorio
- Il Direttorio si avvale del Comitato Tecnico per l'EAD (CTI)

Fonte: circolare 184

5 I ruoli organizzativi
5.2 Servizio Organizzazione

- elabora la normativa quadro e provvede inoltre alla sua emanazione;
- redige le linee guida;
- è *system owner* delle applicazioni aziendali rivolte alla generalità degli utenti e delle piattaforme utilizzate in contesti diversificati per le quali non sia individuabile una specifica competenza funzionale (posta elettronica, Intranet, ambiente di c*ollaboration)*.

Fonte: circolare 184

5 I ruoli organizzativi
5.3 System owner

Durante la fase di sviluppo:

- Effettua la classificazione delle risorse informatiche sotto i profili della riservatezza, dell'integrità e della disponibilità, al fine di individuarne i requisiti di sicurezza;
- Collabora all'individuazione dei presidi tecnici e organizzativi
- Propone al CTI l'accettazione del rischio residuo e gli eventuali scostamenti dalle norme di sicurezza
- Documenta i controlli di tipo amministrativo individuati per il trattamento delle informazioni e la gestione dei sistemi informatici
- ..

Durante il periodo di esercizio:

- Autorizza l'accesso alle risorse e, ove autonomo, cura direttamente il processo abilitativo
- Pone in essere le misure di tipo organizzativo
- Esercita i controlli previsti dalla normativa
- attiva il processo di analisi dei rischi in caso di cambiamenti significativi
- ..

Con riferimento agli incidenti di sicurezza:

- Collabora con la struttura tecnica competente per contenere gli effetti dell'incidente.
- E' destinatario delle informazioni necessarie all'assunzione di decisioni circa eventuali misure di difesa che abbiano impatto sui livelli di servizio
- Segnala i fatti anomali in materia di sicurezza informatica

Fonte: circolare 184

5 I ruoli organizzativi
5.4 SVI

- tutela l'integrità, la riservatezza e la disponibilità del patrimonio di risorse informatiche dell'Istituto;
- elabora e aggiorna linee guida e manuali in collaborazione con il Servizio Organizzazione e l'Ispettorato Banca;
- esegue le attività di analisi del rischio informatico, anche in relazione ai nuovi scenari, individuando i profili di rischio di infrastrutture e applicazioni e fornendo supporto per l'individuazione delle misure di mitigazione;
- effettua la valutazione di sicurezza prima del rilascio in produzione;
- è *system owner*, nella fase di progettazione, delle infrastrutture tecnologiche di supporto alle funzioni aziendali;
- progetta e realizza le infrastrutture di sicurezza.

Fonte: circolare 7 e 184

5 I ruoli organizzativi
5.5 GES

- elabora e aggiorna i manuali operativi per la gestione corrente dei sistemi in esercizio;
- è *system owner*, nella fase di esercizio, delle infrastrutture tecnologiche di supporto alle funzioni aziendali;
- assegna e gestisce le abilitazioni degli utenti, salvo il caso di gestione decentrata;
- cura gli adempimenti operativi connessi con il rilascio e la gestione delle identità digitali e delle credenziali di accesso;
- cura la gestione, la manutenzione e l'aggiornamento dei presidi di sicurezza;
- esegue compiti connessi alle verifiche di sicurezza delle infrastrutture e delle applicazioni;
- effettua attività di monitoraggio della sicurezza.

Fonte: circolare 7 e 184

5 I ruoli organizzativi
5.7 PIA

- formula, d'intesa con le funzioni competenti, proposte in materia di sicurezza informatica da sottoporre agli organi decisionali dell'Istituto e assicura l'evoluzione della metodologia di analisi del rischio informatico

Fonte: circolare 7

5 I ruoli organizzativi
5.6 Servizio Revisione interna

- nell'ambito degli interventi di audit, accerta la rispondenza degli assetti tecnico organizzativi di sicurezza informatica rispetto alla normativa, effettuando una valutazione generale dell'adeguatezza delle misure di sicurezza poste in essere con riguardo agli obiettivi e ai requisiti di sicurezza individuati;
- collabora alla conduzione dell'analisi del rischio dei sistemi informatici qualora, sulla base della classificazione effettuata, il relativo grado di criticità risulti alto in almeno uno dei tre profili di sicurezza presi in considerazione (riservatezza, integrità e disponibilità);
- è incaricato, ove del caso, della ricostruzione dei fatti e delle responsabilità relative ad eventuali incidenti di sicurezza e fatti anomali riguardanti risorse informatiche.

Fonte: circolare 184

6 Personale interno/esterno

- sono tenuti all'osservanza delle norme interne e dell'ordinamento giuridico in materia di sicurezza informatica (ad esempio per la tutela dei sistemi informatici, la protezione dei dati personali, il diritto di proprietà intellettuale)

- sono responsabili delle risorse informatiche loro assegnate; in particolare, sono tenuti ad accedere a sistemi e servizi soltanto per scopi connessi con la propria attività lavorativa, limitatamente alle modalità autorizzate e in accordo con le istruzioni ricevute;

- se titolari di utenze privilegiate, devono utilizzarle in modo strettamente conforme alle esigenze di servizio

Fonte: circolare 184

6 Personale interno/esterno: approfondimento

Gestione del rischio dell'utente sotto il proprio diretto controllo e responsabilità

- Posta elettronica
- Accesso ad in internet
- Strumenti per operare in mobilità (Blackberry, Laptop,)
- Gestione delle "share di rete" (creazione, autorizzazione)
- Apparati speciali (fax, fotocopiatrici, ..)
- Gestione di utenze privilegiate
- Utilizzo di strumenti di collaboration
- Informatica utente
- Utilizzo di piattaforme PaaS (Platform as a service)

8 I processi della sicurezza

processi	descrizione	accountability
Governo della sicurezza	strategia della sicurezza in Banca	CTI
Threat management	individuazione dei nuovi scenari di rischio IT	SVI
IT risk management	analisi dei rischi IT e individuazione delle contromisure	SVI
Pre production security assessment	effettuazione dei test di sicurezza prima della produzione	SVI
Security awareness	campagne di sensibilizzazione	SVI
Post production security assessment	effettuazione dei test di sicurezza in fase di produzione	GES
Security incident management	gestione degli incidenti di sicurezza	GES
Technical vulnerability management	individuazione delle vulnerabilità di sistemi e applicazioni	GES
Security monitoring	monitoraggio dello stato della sicurezza	GES
Asset management	classificazione degli asset informatici dal punto di vista R, I, D	GES
Business continuity management	gestione della continuità operativa	ORG

Fonte: ISO 27001

Cyber risks in the financial sector had been underestimated

CYBER SECURITY THREATS

FEBRUARY 2016 – BANGLADESH

Bangladesh Bank robbery

From Wikipedia, the free encyclopedia

The **Bangladesh Bank robbery**, also known colloquially as the **Bangladesh Bank cyber heist**,[1] was a theft that took place in February 2016. Thirty-five fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer close to US$1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank, the central bank of Bangladesh. Five of the thirty-five fraudulent instructions were successful in transferring US$101 million, with US$20 million traced to Sri Lanka and US$81 million to the Philippines. The Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to US$850 million, due to suspicions raised by a misspelled instruction.[2] All the money transferred to Sri Lanka has since been recovered. However, as of 2018 only around US$18 million of the US$81 million transferred to the Philippines has been recovered.[3] Most of the money transferred to the Philippines went to four personal accounts, held by single individuals, and not to companies or corporations.

The Federal Reserve Bank of New York Building

https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

lay 2018 – Banco de Chile victim of a wiper attack …

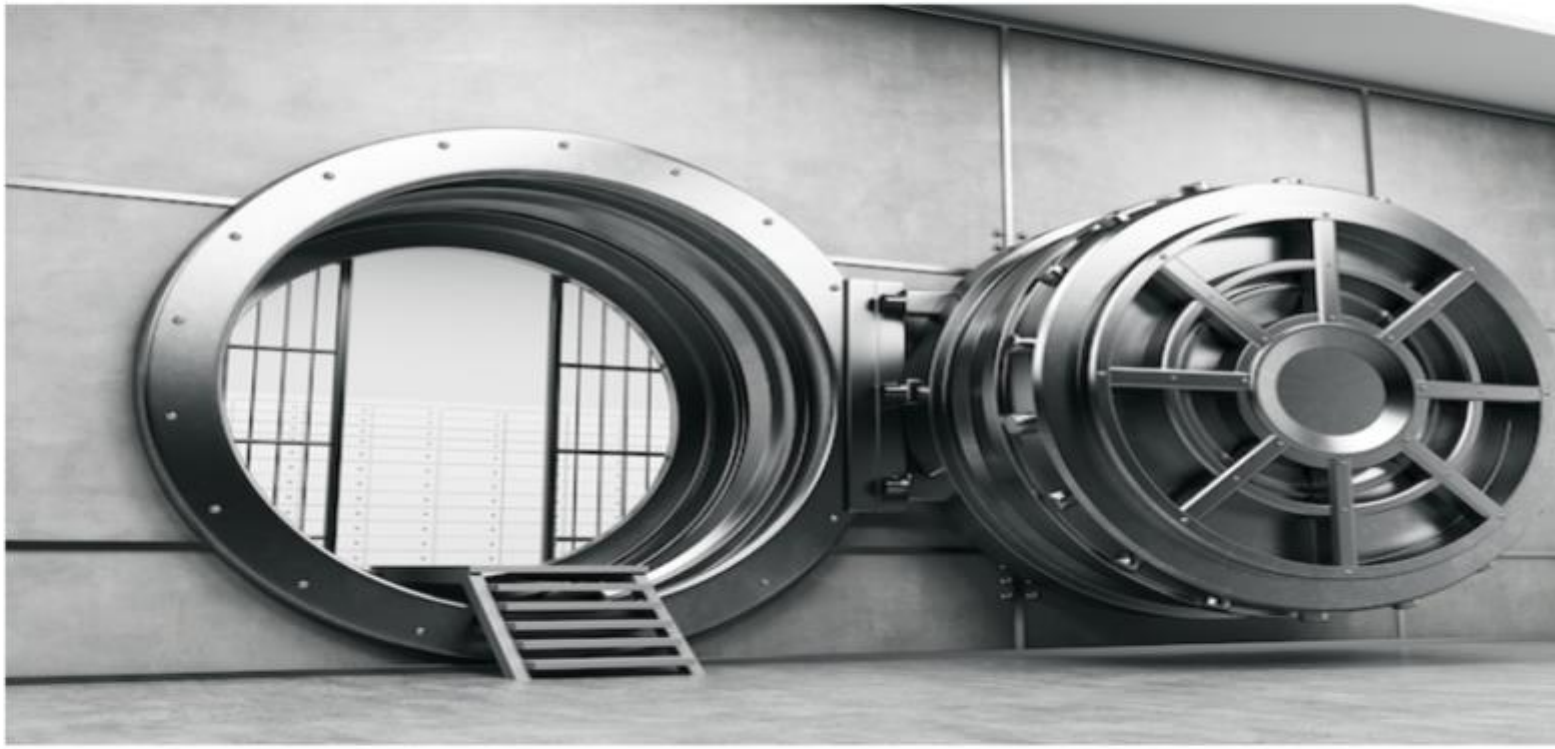
Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist

uthor:
ara Seals
ne 13, 2018 / 12:19 pm

30 minute read

Write a comment

are this article:



The wiper malware affecting 9,000 workstations and 500 servers inside Chile's largest financial institution turns out to have been a distraction.

https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/

March 2021 – Cyber-attack on the European Banking Authority

Cyber-attack on the European Banking Authority

07 March 2021

The European Banking Authority (EBA) has been the subject of a cyber-attack against its Microsoft Exchange Servers, which is affecting many organisations worldwide. The Agency has swiftly launched a full investigation, in close cooperation with its ICT provider, a team of forensic experts and other relevant entities.

As the vulnerability is related to the EBA's email servers, access to personal data through emails held on that servers may have been obtained by the attacker. The EBA is working to identify what, if any, data was accessed. Where appropriate, the EBA will provide information on measures that data subjects might take to mitigate possible adverse effects.

As a precautionary measure, the EBA has decided to take its email systems offline. Further information will be made available in due course.

When email communication channels are restored, our Data Protection Officer, Jonathan Overett Somnier, can be contacted at dpo@eba.europa.eu.

https://www.eba.europa.eu/cyber-attack-european-banking-authority

ebruary 2019 – Cyber attack on Bank of Valletta

Hackers tried to steal €13 million from Malta's Bank of Valletta

Hackers tried to send funds to banks in the UK, the US, the Czech Republic, and Honk Kong. Transactions are being reverted.

ttps://www.zdnet.com/article/hackers-tried-to-steal-eur13-million-from-maltas-bank-of-vallett

December 2018

- Phishing attack (email with an embedded link to a document/malware)

Mid February 2019

- Discrepancies discovered during a reconciliation process
- Applied incident response and recovery procedures

End February 2019

- SWIFT issued a Security Notification (SWIFT ISAC bulletin)

uropean institutions are fully aware of the situation

ndustry estimates for 2018 already put e global cost of cyber attacks at etween USD 45 billion and USD 654 llion.

.

s forthcoming analysis from the uropean Systemic Risk Board shows, ere are plausible channels through hich a cyber attack could morph into a erious financial crisis. …»

https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200205_1~cc8a8787f6.en.html

ıne 2016 - Guidance on cyber resilience for financial market frastructures

uidance on cyber resilience for financial arket infrastructures" was published by PMI-IOSCO

Guidance for FMIs to enhance their cyber resilience

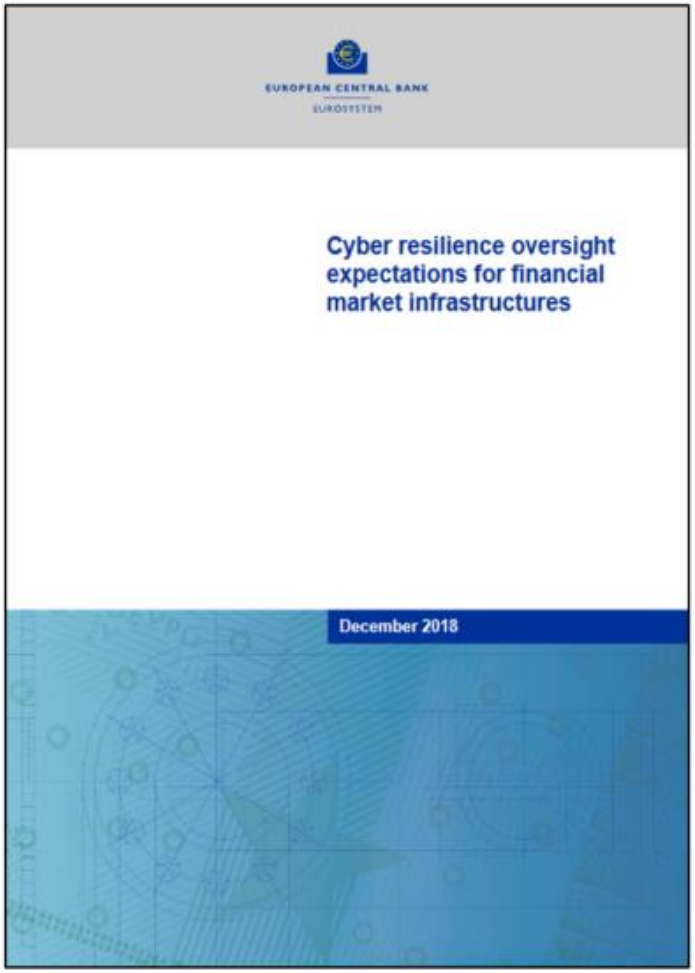
Supplemental guidance to the Principles for Financial Market Infrastructures (PFMI)

Outlines five primary risk management categories and three overarching components that should be addressed

https://www.bis.org/cpmi/publ/d146.htm

December 2018 - Cyber resilience oversight expectations for financial market infrastructures (CROE)

- Cyber resilience oversight expectations (CROE) for FMIs was published. The document
  - describes oversight approach to assess their FMIs against the Guidance
  - serves the following three key purposes:
    i. provides FMIs with detailed steps on how to operationalise the CPMI IOSCO Guidance on Cyber Resilience, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time;
    ii. provides overseers with clear expectations to assess the FMIs for which they are responsible
    iii. provides the basis for a meaningful discussion between the FMIs and their respective overseers.



hat's new? Cyber resilience, not only information security!

formation security

Preservation of confidentiality, ntegrity and availability of information *(from ISO27000:2018-Overview and vocabulary*)

Mostly about keeping the attackers out

Cyber resilience

- Ability to anticipate, withstand, conta and rapidly recover from a cyber attack
- **Mostly about responding when th attackers get in (because they probably will)**


Specific
Cyber resilience
implementations

ecurity Services improvements

Security Operations Centre (SOC) capabilities

- Real Time monitoring
- Incident response including forensic

CERT capabilities

- Cyber Threat Intelligence
- Info-Sharing
- Security awareness

ecurity Testing improvements

Vulnerability Assessments & Penetration Tests

- Every year
- Covering all the infrastructure

Red Team tests (internal)

- Every year

TIBER-EU

Recovery improvements

- **Software integrity**
  - **Run only integrity checked and signed software**
- **Data copy**
  - **Nearly-instant storage based snapshots**