Promosso da

ABI Associazione Bancaria Italiana

PROGRAMMA PROVVISORIO

Organizzato da ABISERVIZI ABI EVENTI

Media Partner BANCAFORTE innovation key

In collaborazione con ABI Lab CERTFin FEduF OSSIF

#wesec

MARTEDÌ 22 SETTEMBRE
TUESDAY 22 SEPTEMBER

10.00
13.00

SESSIONE PLENARIA DI APERTURA - *OPENING PLENARY SESSION*

Navigare l'incertezza: la fiducia come fondamento della stabilità
Navigating uncertainty: trust as the foundation of stability

Chair: Mariavittoria Zaglio, *Journalist & Editor - Innovation & Technology* ***Class CNBC***

In diretta sul canale 507 di SKY */ Live on SKY 507 channel*

10:00
10:30

WeSec: Apertura dei lavori / *WeSec: Opening of proceedings*

10:30
11:35

TAVOLA ROTONDA I/ROUND TABLE I
Navigare l'incertezza: la fiducia come fondamento della stabilità
Navigating uncertainty: trust as the foundation of stability

11:35
11:55

Fireside Chat
Cyber conflict e resilienza europea nell'era dell'AI
Cyber conflict and European resilience in the AI era

11:55
13:00

TAVOLA ROTONDA II/ROUND TABLE II
Governare il digitale tra etica, sicurezza, innovazione e investimenti
Governing the digital realm: ethics, security, innovation, and investment

	SESSIONI / WORKSHOP DI APPROFONDIMENTO *SESSIONS / IN-DEPTH WORKSHOPS*
14.30 **16.00** ***SESSIONE*** **Cybersecurity, frodi e data privacy** ***Cybersecurity, Fraud, and Data Privacy***	**LE FRODI NON DORMONO MAI E NEMMENO CHI LE COMBATTE** *FRAUDSTERS NEVER SLEEP. BUT NEITHER DO THEIR OPPONENTS* Chair**: Mario Trinchera**, Technical Coordinator **CERTFin** Il panorama delle frodi nel settore finanziario e assicurativo è in profonda trasformazione: tecniche sempre più sofisticate, utilizzo dell'intelligenza artificiale per scalare gli attacchi e una superficie di rischio che si allarga con la digitalizzazione dei processi. Nel corso della sessione sarà presentato l'ultimo Report Sicurezza e Frodi in Banca che evidenzia come i volumi di frode crescono, ma cambiano anche forma: da quelle tradizionali a quelle sintetiche, dall'identità clonata al deepfake vocale. In questo panel discuteremo dei trend più rilevanti osservati negli ultimi 12-18 mesi, delle tecnologie e dei modelli organizzativi che le aziende stanno adottando per contrastarle e di come stia cambiando il rapporto tra detection, prevenzione e risposta. Un confronto tra chi vive questo problema ogni giorno: dal fronte operativo a quello strategico. The fraud landscape within the financial and insurance sectors is undergoing a profound transformation: increasingly sophisticated techniques, the use of artificial intelligence to scale attacks and a risk surface that is expanding with the digitalisation of processes. The latest Banking Security and Fraud Report will be presented during this session and the audience will see how fraud is not only on the rise, but also shapeshifting: from traditional to synthetic and from cloned identities to deepfake voices. On this panel, we'll be discussing the most meaningful trends noted over the last 12-18 months, the technologies and organisational models adopted by companies to thwart the fraudsters and how the relationship between detection, prevention and response is changing. A place where those grappling with the problem on a day-to-day basis can exchange views: from the working frontline to the strategic theatre of operations.
14.30 **16.00** ***SESSIONE*** **Artificial Intelligence e nuove tecnologie** ***Artificial Intelligence and new technologies***	**AI CONTRO AI: LA NUOVA GUERRA SILENZIOSA DELLA CYBERSECURITY BANCARIA** *AI PITTED AGAINST AI: THE NEW SILENT WAR OF BANK CYBERSECURITY* Chair**: Marco Rotoloni**, Co-Responsabile Ricerca **ABI Lab** L'AI generativa ha già riscritto le regole del cybercrime bancario: phishing perfetti, deepfake vocali per frodi al CEO, account takeover automatizzati. Con l'arrivo dell'Agentic AI il salto è ulteriore - agenti autonomi capaci di pianificare, adattare ed eseguire attacchi multi-step senza supervisione umana. La banca si trova così in una corsa agli armamenti dove le stesse tecnologie che possono blindare clienti e infrastrutture sono quelle che gli attaccanti usano per aggirarle. Il panel mette a confronto banche, vendor di sicurezza e regolatori per capire chi, oggi, sta vincendo questa partita - e a quali condizioni la difesa può tornare a giocare d'anticipo. *Generative AI has already rewritten the rules of banking cybercrime: perfect phishing, deepfake voice cloning for CEO fraud and automated account takeovers. And the advent of Agentic AI has taken the whole thing on step further - there are autonomous AI agents able*

	to plan, adapt and execute multi-tier attacks without any need for human supervision. Thus, banks are now scrambling in an arms race whereby the very same technologies designed to protect customers and infrastructure are also the ones used by attackers to circumvent them. This panel draws up a comparison of banks, security vendors and regulators in an attempt to understand who is leading the pack today —and what conditions should be put in place to turn the tables and put our defence players back in the lead again and able to troubleshoot.
14.30 **16.00** ***SESSIONE*** **Sicurezza fisica e resilienza infrastrutturale** ***Physical security and infrastructure resilience***	**SICUREZZA PARTECIPATA: UNA COLLABORAZIONE VINCENTE PER IL PRESIDIO DEL TERRITORIO** *PARTICIPATORY SECURITY: A WINNING WAY TO STAY SAFE* Chair**: Marco Iaconis**, Coordinatore **OSSIF** Per fronteggiare in maniera sempre più efficace i reati ai danni del settore bancario, l'ABI ha definito e reso operativa, nel dicembre 2025, una nuova versione del Protocollo d'intesa con le Prefetture per la prevenzione della criminalità ai danni delle banche e dei clienti. Nella sessione si evidenzierà l'importanza della collaborazione con le Autorità di Sicurezza. *With a view to effectively tackling crimes against the banking sector, ABI set out and implemented a new version of the Memorandum of Understanding in December 2025 together with the Prefectures for the prevention of crime against banks and their customers. The session will emphasise how important it is to work hand in hand with national security agencies.*
14.30 **16.00** ***SESSIONE*** **Cultura della Sicurezza: Awareness e responsabilità condivisa** ***Security culture: awareness and shared responsibility***	**CONSAPEVOLEZZA DIGITALE E FATTORE UMANO: RAFFORZARE LA PRIMA LINEA DI DIFESA** *DIGITAL AWARENESS AND THE HUMAN FACTOR: REINFORCING THE FIRST LINE OF DEFENCE* Chair**: Romano Stasi**, Direttore Operativo **CERTFin** In un panorama caratterizzato da minacce cyber sempre più sofisticate, personalizzate e difficili da individuare, la consapevolezza degli utenti rappresenta un elemento cruciale nella prevenzione degli attacchi. Il panel approfondisce il ruolo del fattore umano come primo presidio di sicurezza, analizzando le principali tecniche di social engineering e le vulnerabilità comportamentali che possono essere sfruttate dagli attaccanti. Verranno analizzate le strategie più efficaci per costruire programmi di cybersecurity awareness continui e misurabili, rivolti a clienti e dipendenti, con particolare attenzione alla capacità di riconoscere e reagire tempestivamente alle minacce. All'interno della sessione verrà illustrata la nuova campagna di awareness del CERTFin, evidenziandone gli elementi di evoluzione, innovazione e continuità rispetto alle iniziative precedenti. *In a landscape characterised by increasingly sophisticated, personalised and elusive cyber threats, user awareness is a crucial element in preventing attacks. The panel will be exploring the human factor as a fundamental security safeguard, taking a closer look at the main social-engineering techniques and behavioural vulnerabilities that attackers tend to exploit.*

We will examine the most effective strategies for building continuous and measurable cybersecurity awareness programmes for customers and employees, with a special focus on the ability to recognise and respond to threats in a timely manner.
The session will discuss CERTFin's new awareness campaign, highlighting its evolution, innovation, and continuity with past initiatives.

14.30
16.00
SESSIONE

INFRASTRUTTURE DIGITALI DI MERCATO: SICUREZZA, CONTROLLO E SOVRANITÀ NELL'ERA DELLA BLOCKCHAIN

DIGITAL MARKET INFRASTRUCTURES: SECURITY, CONTROL, AND SOVEREIGNTY IN THE BLOCKCHAIN ERA

Chair: ***in corso di definizione***

Sovranità infrastruttura finanziaria

Financial infrastructure sovereignty

Nell'era della finanza digitale, le infrastrutture e gli standard blockchain stanno assumendo un ruolo sempre più critico nel supportare pagamenti, asset tokenizzati, stablecoin e nuovi servizi finanziari. La loro sicurezza non riguarda più soltanto gli aspetti tecnologici, ma investe la stabilità dei mercati e la protezione degli interessi strategici europei, oltre alla capacità di innovare le modalità di scambio di valore. La sessione analizzerà il legame tra blockchain e sovranità digitale, evidenziando il ruolo che istituzioni, operatori finanziari e imprese tecnologiche europee possono svolgere nella costruzione di un ecosistema capace di coniugare innovazione, sicurezza e autonomia strategica. Quali sono le opportunità che l'UE non può perdere in questa trasformazione? Di cosa c'è bisogno per consentire agli operatori di entrare stabilmente nel mondo tokenizzato? Quali sono le sfide legate alla gestione delle infrastrutture critiche su cui si fonderanno gli scambi di valore del futuro?

In the age of digital finance, blockchain infrastructure and standards are taking on an increasingly vital role in supporting payments, tokenised assets, stablecoins and new financial services. Security is no longer a question of technology, it now extends to market stability and the protection of strategic European assets as well as requiring us to find innovative ways in which to exchange value. This session will delve into the connection between blockchain technology and digital sovereignty, highlighting the role that European institutions, financial operators and technology companies can play in building an ecosystem capable of delivering a combination of innovation, security and strategic autonomy. What opportunities can the EU not afford to miss in this shifting scenario? What do operators require in order to enter the tokenised world on a permanent basis? What challenges might arise when managing the critical infrastructures that will underpin future value exchanges?

16.30 **17.30** ***SESSIONE***	**OCCHIO ALLE TRUFFE** *WATCH OUT FOR SCAMS*
Cultura della Sicurezza: Awareness e responsabilità condivisa ***Security culture: awareness and shared responsibility***	Chair: **Igor Lazzaroni,** Responsabile Ufficio Stampa **Feduf** L'attore e regista Massimo Giordano interpreta Charles Ponzi, il truffatore italiano che nel 1920 raccolse 15 milioni di dollari da circa 40.000 investitori utilizzando uno schema ancora oggi noto con il suo nome e replicato anche attraverso la posta elettronica e il web. Alla rappresentazione segue un dialogo con il pubblico teso a illustrare i meccanismi psicologici di cui bisogna essere consapevoli e le precauzioni da prendere per evitare di rimanere vittime di una truffa. *Actor and director Massimo Giordano portrays Charles Ponzi, the Italian con artist who, in 1920, raised $15 million from approximately 40,000 investors using a scheme that still bears his name today—and which is replicated via email and the web. The performance is followed by a discussion with the audience aimed at highlighting the psychological mechanisms one must be aware of, as well as the precautions to take to avoid falling victim to a scam.*
16.30 **17.30** ***SESSIONE***	**SOVRANITÀ TECNOLOGICA: L'EUROPA TRA AMBIZIONE E DIPENDENZA** *TECHNOLOGICAL SOVEREIGNTY: EUROPE BETWEEN AMBITION AND DEPENDENCE*
Sovranità infrastruttura finanziaria ***Financial infrastructure sovereignty***	Chair**: Marco Rotoloni**, Co-Responsabile Ricerca **ABI Lab** Cloud, intelligenza artificiale, quantum: le tre infrastrutture su cui si decide il futuro economico e politico dei prossimi vent'anni sono oggi in larga parte fuori dal controllo europeo. L'80% del mercato cloud UE è in mano agli hyperscaler americani, sull'AI dipendiamo da modelli e GPU progettati altrove, sul quantum abbiamo eccellenza scientifica ma non scala industriale. Bruxelles risponde con il Tech Sovereignty Package e il Cloud and AI Development Act, ma basterà? Il panel mette a confronto istituzioni, industria e analisti per capire se la sovranità tecnologica europea sia una strategia praticabile o uno slogan destinato a restare sulla carta. *The cloud, artificial intelligence and quantum computing: to a large extent, the three infrastructures set to shape the economic and political future of the next two decades fall out of the control of Europe today. 80% of the EU cloud market lies in the hands of American hyperscalers, for AI we rely on models and GPUs designed elsewhere and, while we can boast scientific excellence for quantum technology, it cannot be produced on an industrial scale. Brussels has responded with the Tech Sovereignty Package and the Cloud and AI Development Act, but will that be enough?* *The panel brings together institutions, industry, and analysts who will try to establish whether European technological sovereignty is a viable strategy or just a slogan that is unlikely to get off the ground.*

16.30
17.30
SESSIONE

CRIMINALITÀ PREDATORIA IN BANCA E NEGLI ALTRI SETTORI ESPOSTI: TREND E INIZIATIVE DI CONTRASTO

CROSS-SECTOR CRIME: PREDATORY CRIME IN BANKS AND IN OTHER SUSCEPTIBLE SECTORS: TRENDS AND COUNTERMEASURES

Sicurezza fisica e resilienza infrastrutturale

Physical security and infrastructure resilience

Chair**: Isabella Corradini,** Presidente **Centro Ricerche Themis**

L'utilizzo del contante in Italia è ancora elevato e la circolazione del denaro comporta un rischio predatorio non solo ai danni del settore bancario ma anche in tutti i settori esposti. La sessione, partendo dalla presentazione del Report Intersettoriale OSSIF 2026 affronterà i temi della sicurezza e prevenzione anche negli altri settori approfondendo le iniziative in atto per la sicurezza dei territori e del Paese.

The use of cash in Italy is still common. This poses a predatory risk not only to the banking sector but to all other susceptible sectors. The session will start with the presentation of the OSSIF 2026 Intersectoral Report, after which it will address the issues of security and prevention in other sectors as well, examining current security initiatives aimed at protecting local areas and the country itself.

16.30
17.30
SESSIONE

QUANTUM IS COMING

QUANTUM IS COMING

Artificial Intelligence e nuove tecnologie

Artificial Intelligence and new technologies

Chair**: Mario Trinchera**, Technical Coordinator **CERTFin**

Il quantum è la prossima grande discontinuità tecnologica. Sul piano industriale apre scenari concreti - dall'ottimizzazione dei portafogli finanziari alla scoperta di nuovi farmaci, dai materiali avanzati alla logistica - con applicazioni che alcuni grandi player stanno già sperimentando in produzione. Sul piano della sicurezza cambia le regole del gioco: la crittografia che oggi protegge dati bancari, comunicazioni e infrastrutture critiche è destinata a diventare vulnerabile, e la migrazione verso algoritmi post-quantistici è già una priorità di governi e regolatori. Il panel fa il punto su dove siamo davvero, quali opportunità si possono cogliere subito e come prepararsi a una transizione che non è più una questione di "se", ma di "quando".

Quantum is the next great technological breakthrough. Industrially speaking, it will open the door to very real scenarios (from the optimisation of financial portfolios to the discovery of new drugs and from advanced materials to logistics) with applications that a number of major players are already testing on the production floor. As far as security goes, the rules of the game are shifting: encryption standards currently protecting banking data, communications and critical infrastructure are destined to become vulnerable, and governments and regulators have already prioritised the migration to post-quantum algorithms. The panel will establish where we stand now, what avenues are immediately open to us and how to get ready for an inevitable transition. Because it is no longer a question of "if" but of "when."

16.30
18.00
SESSIONE

IDENTITÀ DIGITALE E ARCHITETTURE ABILITANTI: SPID, CIE, EUDIW NELLA NUOVA CORNICE DI EIDAS 2

DIGITAL IDENTITY AND ENABLING ARCHITECTURES: SPID, CIE & EUDIW WITHIN THE NEW FRAMEWORK OF EIDAS 2

Chair**: Daniele Di Stazio**, Innovazione **ABI**

Artificial Intelligence e nuove tecnologie

Artificial Intelligence and new technologies

La sessione affronta l'evoluzione dell'identità digitale e delle architetture abilitanti per il settore finanziario. Verranno approfonditi i sistemi di autenticazione (SPID, CIE, EUDIW) e l'interoperabilità tra sistemi e piattaforme. La discussione includerà come le banche possono integrare questi strumenti per offrire servizi più sicuri, efficienti e user-friendly, mantenendo al contempo il controllo dei dati e la conformità normativa. Un focus sarà dedicato all'approfondimento delle principali vulnerabilità nelle fasi di identificazione e autenticazione del cliente nonché alle soluzioni tecnologiche e organizzative adottate per mitigarle.

This session will be addressing the evolution of digital identity and enabling architectures for the financial sector. Authentication systems (SPID, CIE and EUDIW) and interoperability between systems and platforms will be explored in depth. The conversation will also focus on how banks can integrate these tools to deliver more secure, efficient and user-friendly services while continuing to ensure data control and regulatory compliance. There will be a special focus on the main vulnerabilities affecting customer identification and authentication as well as on the technological and organisational solutions adopted to deal with this.

MERCOLEDÌ 23 SETTEMBRE
WEDNESDAY 23 SEPTEMBER

9.30
11.00
SESSIONE

Cybersecurity, frodi e data privacy

Cybersecurity, Fraud, and Data Privacy

RESILIENZA: SEI FORTE QUANTO IL TUO ANELLO PIÙ DEBOLE. E OGGI QUELL'ANELLO POTREBBE NON ESSERE TUO

RESILIENCE: YOU ARE AS STRONG AS YOUR WEAKEST LINK. AND TODAY THAT LINK MIGHT NOT BE YOURS.

Chair**: Roberto Tordi**, Osservatorio Continuity e Resilience **ABI Lab**

La resilienza operativa non è più una questione interna. La dipendenza da fornitori, outsourcer, cloud provider e partner tecnologici ha ridisegnato i perimetri del rischio: un incidente che colpisce un terzo può fermare un'intera catena operativa, con effetti a cascata su clienti, mercati e reputazione.
DORA ha reso questo tema urgente e vincolante per molti operatori, ma la vera sfida va oltre la compliance: come testare la capacità del sistema finanziario di resistere agli attacchi più sofisticati (test TLPT agli esercizi di sistema e cooperativi)? Come si costruisce una governance reale del rischio terze parti? Come si valuta la resilienza di chi non controlli direttamente? Questo panel esplora approcci concreti, esperienze sul campo e le lezioni imparate - nel tentativo di trasformare un obbligo normativo in un vantaggio competitivo.

Operational resilience is no longer an internal issue. Reliance on suppliers, outsourcers, cloud providers and technology partners has shifted the risk boundaries. An incident affecting a third party could disrupt an entire operational chain, leading to a domino effect on customers and markets as well as incurring reputational damage.
DORA has not only made this an urgent issue, but also one which is binding on many operators. The true challenge, however, is to transcend compliance. The question is how do we test the ability of our financial system to withstand the most sophisticated attacks (TLPT testing on system and cooperation exercises)? How does one set up effective third-party-risk governance? How does one assess the resilience of operators who do not fall under one's direct control? This panel will be taking a close look at concrete approaches, experiences in the field and lessons learned - in an attempt to turn a regulatory requirement into a competitive edge.

9.30
11.00
SESSIONE

EVOLUZIONE DELLA MONETA PUBBLICA E DELLA MONETA PRIVATA E IMPATTO SULLA SOVRANITÀ MONETARIA

THE EVOLUTION OF PUBLIC MONEY AND PRIVATE MONEY AND THE IMPACT ON MONETARY SOVEREIGNTY

Sovranità infrastruttura finanziaria

Financial infrastructure sovereignty

Chair**: Silvia Attanasio,** Responsabile innovazione **ABI**

Moneta pubblica e moneta privata: un ampio ventaglio di strumenti e novità: Euro Digitale, progetto Pontes, programma Appia, soluzioni private europee per i pagamenti digitali, e-money token, depositi tokenizzati e cripto-attività. In questo scenario di digitalizzazione della moneta nelle sue diverse forme, si impone una domanda chiave: che scenario stiamo disegnando? Cosa ci attendiamo in termini di governo delle leve della sovranità monetaria? Come evolve il ruolo delle banche nell'ecosistema della moneta digitale, nella trasmissione della politica monetaria e nella gestione dei pagamenti? Quali rischi si aprono in termini di dipendenza tecnologica e finanziaria da attori extra europei? La sessione metterà a confronto istituzioni, banche e operatori del mercato per discutere dell'evoluzione della moneta pubblica e privata, di sovranità monetaria e di rischi e opportunità per il sistema bancario e per la stabilità finanziaria.

Public money and private money: a broad array of tools and innovation initiatives: the Digital Euro, Pontes project, Appia programme, private European solutions for digital payments, e-money tokens, tokenised deposits and crypto-assets. Against a backdrop of digitalisation of money in a variety of guises, one pressing question is begged: what kind of scenario exactly are we designing? What expectations do we have in terms of monetary sovereignty lever management? How is the role of banks evolving within the digital currency ecosystem and as far as the transference of monetary policy and payment management are concerned? What risks are linked to our technological and financial reliance on non-European players? The session will bring together institutions, banks and market participants to discuss the evolution of public and private money, monetary sovereignty and the risks and opportunities for the banking system and financial stability.

9.30
11.00
SESSIONE

SICUREZZA ATM: TREND DEGLI ATTACCHI E MISURE DI CONTRASTO

ATM SECURITY: ATTACK TRENDS AND COUNTERMEASURES

Sicurezza fisica e resilienza infrastrutturale

Physical security and infrastructure resilience

Chair**: Marco Iaconis**, Coordinatore **OSSIF** e **Giovanni Gioia**, Research Analyst **OSSIF**

Le recenti analisi OSSIF evidenziano una recrudescenza degli attacchi agli ATM sul territorio italiano. Nella sessione verranno illustrati gli ultimi dati disponibili e le nuove soluzioni di sicurezza ad alta innovazione tecnologica proposte dalle aziende.

The latest findings by OSSIF reveal that there has been a resurgence of ATM attacks in Italy. In the course of this session, an illustration will be given of the latest data and new highly innovative technological security solutions available on the market.

9.30
11.00
SESSIONE

LA CYBERSECURITY NON È PIÙ SOLO UN PROBLEMA IT. È UNA QUESTIONE DI SICUREZZA NAZIONALE ... E AZIENDALE

CYBERSECURITY IS NO LONGER JUST AN IT PROBLEM. IT IS A QUESTION OF NATIONAL AND... CORPORATE SECURITY

Chair: ***in corso di definizione***

Cybersecurity, frodi e data privacy

Cybersecurity, Fraud, and Data Privacy

Il contesto geopolitico degli ultimi anni ha accelerato una convergenza che molti già temevano: le tensioni tra stati si combattono sempre più attraverso il dominio digitale. Attacchi ibridi che combinano disinformazione, sabotaggio infrastrutturale e intrusioni nei sistemi critici non sono più scenari teorici - sono realtà documentate. E le aziende si trovano in prima linea, spesso senza esserne consapevoli.
In questo panel affrontiamo le nuove minacce che stanno emergendo - dall'AI offensiva agli attacchi alle supply chain digitali - e il ruolo crescente del rischio geopolitico nelle valutazioni di sicurezza. Come stanno evolvendo le strategie di difesa? Come si parla di questi temi ai board? E dove si trova oggi il confine tra sicurezza aziendale e sicurezza collettiva?

In recent years, the geopolitical landscape has resulted in the acceleration of a convergence dreaded by many: tensions between one nation and another are increasingly being fought out in the digital domain. Hybrid attacks combining disinformation, infrastructure sabotage and critical-system intrusions have left the realms of mere theory and have now become documented reality. And enterprise finds itself in the line of fire, often without even realising what is happening.
On this panel, we will be addressing emerging threats—from offensive AI to attacks on digital supply chains—and we will also be examining the increasingly important role played by geopolitical risk in security assessments. How are defence strategies coming along? How does one tackle these issues at a board meeting? And where do we draw the boundary today between corporate security and collective security?

9.30
11.30
WORKSHOP

WORKSHOP

In corso di definizione

11.30
12.30
SESSIONE

OGNI NUOVA NORMA È UN VINCOLO MA ANCHE UNA MAPPA VERSO UN SISTEMA PIÙ SOLIDO

EACH NEW REGULATION IS A HINDRANCE, BUT IT ALSO HELPS TO PLOT A MAP TOWARDS A MORE ROBUST SYSTEM

Chair**: ABI**

Cybersecurity, frodi e data privacy

Il Nuovo Regolamento dei Sistemi di Pagamento (PSR) si aggiunge al quadro normativo europeo che negli ultimi anni si è fatto più denso e più esigente: DORA, NIS2, AI Act, aggiornamenti in materia di antiriciclaggio, nuove linee guida EBA e EIOPA. Per molte organizzazioni, il rischio è di vivere la compliance come un esercizio difensivo - un costo da sostenere, non un'occasione da cogliere.

Cybersecurity, Fraud, and Data Privacy	Eppure, le normative più ambiziose nascono per rispondere a rischi reali: chi le affronta con intelligenza, costruisce processi più robusti, governance più chiare e una reputazione più solida sul mercato. In questo panel discutiamo di come le organizzazioni stiano navigando questa stagione regolamentare, di cosa funziona e cosa no nell'approccio alla compliance, e di dove si nascondono le vere opportunità per chi guarda oltre la scadenza. *The New Payment Systems Regulation (PSR) goes to supplement a European regulatory framework that has become denser and more demanding over recent years: DORA, NIS2, the AI Act, anti-money laundering updates, the new EBA and EIOPA guidelines. There is a risk that many organisations will see compliance as an onslaught they must defend themselves against. A burden to be borne rather than an opportunity to be seized.* *Yet, the most ambitious regulations stem from a response to real risks. If we address them intelligently, they will spur us to build more robust processes, clearer governance models and a better market reputation. On this panel, we'll be discussing how organisations are navigating the regulatory season, what's working (and what's not) in their approach to compliance and where the real opportunities lie for those who are able to look beyond the deadline.*
11.30 **13.00** ***SESSIONE***	**COOPERAZIONE INTERNAZIONALE E SICUREZZA FINANZIARIA: MODELLI DI COLLABORAZIONE IN UNO SCENARIO GLOBALE FRAMMENTATO** *INTERNATIONAL COOPERATION AND FINANCIAL SECURITY COOPERATION MODELS IN A FRAGMENTARY GLOBAL SCENARIO*
Sovranità infrastruttura finanziaria ***Financial infrastructure sovereignty***	Chair**: Andrea Rigoni,** Founder and Managing Partner **Altirium** La crescente interconnessione dei sistemi finanziari e digitali rende la cooperazione internazionale un fattore determinante per il contrasto alle minacce cyber e ibride. Il panel esplora le principali iniziative di collaborazione tra autorità, istituzioni finanziarie e organismi sovranazionali, evidenziando best practice, criticità e aree di miglioramento. Saranno analizzati i meccanismi di condivisione delle informazioni, le sfide normative e le opportunità offerte da approcci coordinati nella gestione degli incidenti e nella prevenzione dei rischi sistemici. La discussione metterà in luce il valore della cooperazione come leva strategica per garantire stabilità, fiducia e sicurezza nei mercati globali. *The progressive interconnectedness between financial and digital systems means that international cooperation assumes a crucial role in the fight again cyber and hybrid threats. The panel will be exploring the main forms of cooperation between authorities, financial institutions and supranational organisations, underscoring best practices, critical issues and areas for improvement. Information-sharing mechanisms, regulatory challenges and the opportunities afforded by a coordinated approach to incident management and systemic risk prevention will be examined. The discussion will shine a spotlight on the importance of cooperation as a strategic lever for ensuring stability, trust and security across global markets.*
11.30 **13.00** ***SESSIONE***	**INFRASTRUTTURE CRITICHE, CYBER WARFARE E HYBRID THREATS: LA NUOVA FRONTIERA DELLA GUERRA IBRIDA** *CRITICAL INFRASTRUCTURE, CYBER WARFARE AND HYBRID THREATS: THE NEW FRONTIER OF THE HYBRID WAR*

Sicurezza fisica e resilienza infrastrutturale

Physical security and infrastructure resilience

Chair**: Mario Trinchera**, Technical Coordinator **CERTFin**

Il 99% del traffico internet intercontinentale viaggia sotto i nostri mari, e sotto i nostri mari è in corso una guerra silenziosa: nel solo Mar Baltico oltre dieci cavi danneggiati negli ultimi due anni, con sospetti che puntano alla flotta ombra russa e a navi cinesi. Ma i cavi sottomarini sono solo la punta dell'iceberg. La stessa logica di guerra ibrida colpisce reti elettriche, gasdotti, sistemi idrici, hub logistici, data center, infrastrutture sanitarie e finanziarie: bersagli ad alto impatto, attribuzione difficile, costi politici bassi per chi attacca. Lo scenario combina sabotaggio fisico, intrusioni cyber e minacce alla supply chain, in un contesto in cui la NIS2 e le nuove direttive europee alzano l'asticella ma la capacità di risposta resta frammentata tra Stati membri, operatori privati e Alleanza atlantica.
La sessione esamina come le minacce ibride e il cyber warfare si inseriscono nel contesto geopolitico internazionale. Verranno analizzati i rischi per la stabilità economica nazionale e il ruolo strategico della tecnologia e della cybersecurity nella difesa nazionale. La discussione affronterà come il settore finanziario, in coordinamento con le istituzioni, può contribuire a rafforzare la resilienza economica del Paese di fronte a scenari geopolitici instabili.

Ninety-nine percent of intercontinental internet traffic travels along the ocean floor and a silent war is being waged beneath the waves. In the Baltic Sea alone, more than ten cables have been damaged in the last two years, the finger of suspicion pointing at the Russian shadow fleet and Chinese ships. But deep-sea cables are just the tip of the iceberg. The same hybrid warfare approach zeros in on electricity grids, gas pipelines, water systems, logistics hubs, data centres, healthcare and financial infrastructure: these high-impact targets cause maximum disruption, while making it difficult to identify the perpetrator and ensuring low political costs for the attacker. The scenario involves a mixture of physical sabotage, cyber intrusions and supply chain threats in a context where NIS2 and the new European directives raise the bar, but responsiveness continues to be fragmented between member states, private operators and the Atlantic Alliance.
The session will look at how hybrid threats and cyber warfare fit into the international geopolitical backdrop. The risks to national economic stability and the strategic role of technology and cybersecurity in national defence will be examined. The discussion will centre on how the financial sector in tandem with the various institutions can contribute to boosting the country's economic resilience in the midst of an unstable geopolitical landscape.

11.30
13.00
SESSIONE

VULNERABILITY ASSESSMENT 2.0: COME L'AI AGENTICA RIDISEGNA PRIORITÀ E TEMPI DI RISPOSTA

VULNERABILITY ASSESSMENT 2.0: HOW AGENTIC AI IS REDEFINING PRIORITIES AND RESPONSE TIME

Artificial Intelligence e nuove tecnologie

Artificial Intelligence and

Chair**: Simone Coltellese**, Cyber Security and Fraud Analyst **ABI Lab**

L'evoluzione degli strumenti di AI, inclusi gli agenti autonomi, sta trasformando profondamente i processi di patch management e vulnerability assessment nel settore finanziario. Da un lato, queste tecnologie accelerano la capacità degli attaccanti di individuare e sfruttare vulnerabilità, comprimendo drasticamente i tempi di esposizione. Dall'altro, offrono alle istituzioni finanziarie strumenti per automatizzare la scoperta, la prioritizzazione e la remediation delle vulnerabilità, rendendo la difesa più rapida e proattiva.

new technologies	Questo panel metterà a confronto esperti del settore su come ripensare questi processi critici alla luce delle nuove capacità offensive e defensive abilitate dall'AI. *The advance of AI tools (including autonomous agents) is radically changing patch-management processes and vulnerability assessment in the finance sector. On the one hand, these technologies boost attackers' ability to pinpoint and exploit vulnerabilities, drastically narrowing the exposure window. On the other hand, they provide financial institutions with a means to automate the discovery, prioritisation and remediation of vulnerabilities, making for a faster and more proactive defence mechanism. This panel will bring together industry experts to discuss how we can rethink these critical processes in light of new AI-enabled offensive and defensive capabilities.*
11.30 **13.00** ***SESSIONE***	**AWARENESS VERSO LE PMI** *SME AWARENESS*
Cultura della Sicurezza: Awareness e responsabilità condivisa ***Security culture: awareness and shared responsibility***	Chair: ***in corso di definizione*** Con l'AI generativa il phishing è ormai indistinguibile dalle comunicazioni reali, i deepfake vocali rendono credibili le frodi al CEO, e il rischio Ransomware è sempre dietro l'angolo. Tutte insidie che interessano le piccole e medie imprese - la spina dorsale dell'economia italiana, ma quasi sempre senza risorse di sicurezza dedicate. Le azioni di awareness davvero efficaci non sono più la formazione "una tantum", ma percorsi continui, personalizzati sui ruoli, affiancati da simulazioni realistiche e da una governance che misuri l'impatto comportamentale, non solo le ore erogate. In questo scenario le banche giocano un ruolo doppio e ancora poco esplorato: target primari di attacchi, ma anche punto di osservazione privilegiato sulle imprese clienti e potenziale hub di formazione, alert, fraud detection e servizi di sicurezza dedicati. Il panel mette a fuoco quali azioni di sensibilizzazione funzionano davvero, come superare il limite della "compliance formativa" e in che modo il sistema bancario possa accompagnare le aziende - soprattutto le PMI - verso una postura di sicurezza più matura. *With generative AI, phishing is now indistinguishable from real communications, voice deepfakes make CEO fraud believable and the risk of ransomware is always looming. All these pitfalls negatively affect small and medium-sized businesses which form the backbone of the Italian economy, but which can hardly ever count on dedicated security resources. Truly effective awareness campaigns can no longer be relegated to one-off training courses. There must be ongoing, role-specific training programmes backed up by realistic simulations and governance that gauges behavioural impact and does not simply count the number of training hours. In this scenario, banks play a dual and, as yet, superficially explored role. They are a primary target for attacks, but they also have a privileged vantage point over corporate clients as well as being a potential hub for training schemes, alerts, fraud detection and dedicated security services. The panel will focus on which awareness-raising initiatives truly work, how to overcome the limits of "compliance training" and how the banking system can steer companies—especially SMEs—towards a more mature security posture.*

14.30
15.30
SESSIONE

Cybersecurity, frodi e data privacy

Cybersecurity, Fraud, and Data Privacy

CYBER THREAT LANDSCAPE PER IL SETTORE FINANZIARIO

THE CYBER-THREAT LANDSCAPE FOR THE FINANCIAL SECTOR

Chair**: Simone Coltellese**, Cyber Security and Fraud Analyst **ABI Lab**

Il settore finanziario italiano è bersaglio di minacce sempre più sofisticate e geopoliticamente orientate. Questo panel mette a confronto il Threat Landscape Report del CERTFin con ulteriori prospettive di Cyber Threat Intelligence di settore, per offrire ai partecipanti una lettura condivisa e operazionabile del rischio cyber: dalle campagne di phishing e malware ai gruppi APT, fino alle vulnerabilità sistemiche che attraversano l'infrastruttura finanziaria europea.

The Italian financial sector is increasingly targeted by sophisticated and geopolitically oriented threats. This panel sets CERTFin's Threat Landscape Report and additional industry CyberThreat Intelligence perspectives side by side in a quest to provide participants with a shared and actionable grasp of cyber risk: from phishing and malware campaigns to APT groups and systemic vulnerabilities affecting Europe's financial infrastructure.

14.30
15.30
SESSIONE

Artificial Intelligence e nuove tecnologie

Artificial Intelligence and new technologies

IL VALORE DELLE INFORMAZIONI: AI E STRUMENTI DI ANALISI PER UNA SICUREZZA DATA-DRIVEN

THE VALUE OF INFORMATION: AI & ANALYSIS TOOLS FOR DATA-DRIVEN SECURITY

Chair**: Pierluigi Martusciello**, People & Property Security Country Manager **BNL BNP Paribas**

I dati abbondano ma non tutti i dati hanno lo stesso valore. E' fondamentale passare dai dati alle informazioni e poi alla conoscenza per arrivare infine alle analisi predittive. Nel corso della sessione si parlerà di sicurezza data-driven con un focus sui progetti in essere e sviluppi futuri: APP sugli eventi criminosi; GeoCrime: uno strumento di analisi dei rischi per la sicurezza del territorio; AI e Machine learning: i modelli di analisi del rischio per la prevenzione del crimine; Centralizzazione e gestione remota allarmi; Informazioni per gestire frodi, attacchi cyber, intrusioni.

There is an abundance of data, but not all this data is equal. It is vital to move first from data to information, then to knowledge before ultimately reaching predictive analysis. This session will centre on data-driven security with a focus on current projects and future developments: Apps on criminal events; GeoCrime: a risk-analysis tool for homeland security; AI and machine learning: risk-analysis models for crime prevention; centralisation and remote alarm management; information on how to handle fraud, cyber attacks and intrusions.

14.30
15.30
SESSIONE

Sicurezza fisica e resilienza infrastrutturale

Physical security and infrastructure resilience

SICUREZZA INTEGRATA PER UNA NUOVA VISIONE STRATEGICA
INTEGRATED SECURITY FOR A NEW STRATEGIC VISION

Chair**: Claudio Ferioli,** Senior Director **Intesa Sanpaolo**

Sicurezza fisica e sicurezza digitale non possono più agire separatamente. La sicurezza integrata è necessaria per migliorare l'efficacia e l'efficienza del Governo della Sicurezza aziendale. La sessione approfondirà questi aspetti con focus su: attacchi multivettoriali fisico-informatici (keylogger, KVM, skimmer): funzionamento e contromisure; digitalizzazione dei sistemi di sicurezza fisica e nuovi rischi cyber; protezione delle sedi come ecosistemi cyber-fisici: integrazione tra sistemi di sicurezza fisica e digitale per la gestione degli incidenti ibridi; attacchi black-box, esempi reali e convergenza tra rischio fisico e digitale; sicurezza fisica e digitale dei dispositivi per la protezione delle sedi; sistemi innovativi e basati sull'AI a supporto della sicurezza integrata.

Physical security and digital security can no longer run on two separate tracks. Integrated security is a necessary step if we are to boost the effectiveness and efficiency of corporate security governance. During this session, we will explore these aspects in depth, focusing on: multi-vector physical-cyber attacks (keyloggers, KVMs and skimmers): how they work and how they can be thwarted; digitalisation of physical security systems and new cyber risks; securing premises as cyber-physical ecosystems: integrating physical and digital security systems for managing hybrid incidents; black-box attacks, real-world examples and the convergence of physical and digital risks; physical and digital security of premises protection devices; innovative and AI-based systems supporting integrated security.

14.30
15.30
WORKSHOP

WORKSHOP

In corso di definizione

15.45
17.15

SESSIONE PLENARIA DI CHIUSURA
CLOSING PLENARY SESSION

15.45
16.45

TAVOLA ROTONDA - SOVRANITÀ DIGITALE: L'EUROPA TRA AUTONOMIA TECNOLOGICA E SCELTE DEMOCRATICHE
ROUND TABLE - DIGITAL SOVEREIGNTY: EUROPE BETWEEN TECHNOLOGICAL AUTONOMY AND DEMOCRATIC CHOICES

Chair**:** ***in corso di definizione***

L'Europa ha normative forti (GDPR, AI Act) ma dipende da tecnologie non-europee. Cybersecurity e AI non sono solo questioni tecniche: sono questioni di sovranità politica e geopolitica. Come possiamo essere democratici e autonomi simultaneamente? Quali sono i rischi di dipendenza tecnologica? Come competere globalmente mantenendo sovranità?

	Europe has robust regulations (GDPR, AI Act) but relies on non-European technologies. Cybersecurity and AI are not merely technical issues; they are matters of political and geopolitical sovereignty. How can we be both democratic and autonomous? What are the risks of technological dependence? How can we compete globally while maintaining sovereignty?
16.45 **17.15**	**CLOSING** **Fireside chat** Il futuro nell'era quantistica: opportunità, sfide e nuove responsabilità per disegnare un modello di sicurezza, innovazione e competitività all'altezza delle trasformazioni che ci attendono. *The future in the quantum era: opportunities, challenges, and new responsibilities for shaping a model of security, innovation, and competitiveness capable of meeting the transformations that lie ahead.*