Post event report

Strategic Sponsors

BITSIGHT
The Standard in SECURITY RATINGS

onelogin

SEGASEC

zscaler

Education Seminar Sponsors

INTSIGHTS
Defend Forward

ManageEngine

OneTrust
Privacy
PRIVACY MANAGEMENT SOFTWARE

Networking Sponsor

VERACODE

Branding Sponsor

ZEROFOX

"Necesitaría, si es posible, un certificado de asistencia al evento del pasado jueves para poderlo aportar como créditos CPE en las certificaciones de CISP y CISM."

Accesos remotos en Internet, Mapfre

"Me pareció el evento interesante. Pude contactar con las empresas que hicieron sus presentaciones e intercambiar tarjetas y opiniones."

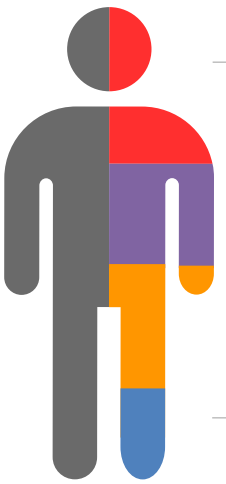
Compliance Expert Consultant CEC, Mag Abogados

Inside this report:

Key themes

- Moving to secure solutions in the cloud
- Complying with new regulations
- Finding solutions that fit your needs
- Achieving the visibility you need
- Securing yourself against digital fraud
- Outsourcing what you cannot do in-house

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Maite Avelino, CISO, Ministry of Finance

Manuel Barrios Paredes, CISO, Solvia

Andrea Bellinzaghi, Technical Director Southern Europe, IntSights

Jesús García Bautista, CISO and IT Chief, Correos Express

Paulo Glorias, Regional Sales Director, BitSight

Alvaro Grande, Security Engineer, Telefónica

Héctor Guzmán Rodríguez, Director of Data Protection and Privacy, BGBG Abogados

Eduardo Helering, EMEA Head of Solutions Engineering, OneLogin

Dr. Susana Infantes, Principal Researcher, Group Institut de Reserca Biomèdica de Lleida

Teresa Minguez Diaz, Director Compliance, Porsche

Gabriel Moline, CISO, Leroy Merlin

Alvaro Ortega, Head of Law Enforcement Outreach and Investigations Southern Europe, UK, Ireland & Nordic, Western Union

Axel Pérez, Sales Engineer Iberia, Zscaler

Laura del Pino Jiminez, Discipline Leader of Data and People Information Security, BBVA

Teba Ríos, CIPP/E, CIPM, Solutions Engineer, OneTrust

Ignacio Rodriguez, Lead Security Manager, BT

Irene Rodriguez Ortega, Specialist, EMEA Cybersecurity Center, Deloitte

María Rojo, Information Security Manager, Airbus Defence & Space

Borja Rosales, UK, Spain & EMEA Director, SegasecJavier Sánchez Salas, CISO, Haya Real Estate

Pablo Rubio, IT Risk Management Engineer and Specialist, Nationale Nederlanden

Siddharth Sharath Kumar, Product Evangelist, ManageEngine

Raúl Vázquez Pastor, IT Risk Control – CyberRisk Manager, Banco Sabadell

Fernando Vegas, former CIO and CRO, OHL

Agenda	
08:30	Registration and breakfast networking
09:30	Chairman's welcome
09:40	**DevSecOps pilot without bumping into the iceberg** **Javier Sánchez Salas,** CISO, Haya Real Estate • Addressing security in the developments of a company in continuous evolution • Security as part of the Software Quality process • Securisation of the Development and Production Commissioning cycle
10:00	**2019 cyber risk – the year of the supply chain** **Paulo Glorias,** Regional Sales Director, BitSight • Why supply chain management programmes need to be updated as the risks (hidden and not) presented by suppliers have drastically changed • Why current assurance mechanisms are failing and how companies can gain a deeper understanding of the risks hidden deep within their supplier ecosystems • Managing the types of risks presented by suppliers such as, human rights, diversity, cybersecurity, intellectual property and the handling of personal information • Use cases: how organisations are leveraging BitSight to manage risk in the supply chain framework, meet the demands of the business and manage cyber-risk
10:20	**Blockchain, new paradigms and its practical application in public administration** **Ignacio Rodriguez,** Lead Security Manager, BT • Blockchain, new paradigm • Blockchain and cybersecurity • AAPP and new legislative and practical DNA • Challenges to assume
10:40	Refreshments and networking
11:10	**EXECUTIVE PANEL DISCUSSION** — **Women leadership executive panel discussion. Discussions on diversity in the cybersecurity, fraud and compliance industries** **Irene Rodriguez Ortega,** Specialist, EMEA Cybersecurity Center, Deloitte (Chair) **Dr. Susana Infantes,** Principal Researcher, Group Institut de Reserca Biomèdica de Lleida **María Rojo,** Information Security Manager, Airbus Defence & Space **Teresa Minguez Diaz,** Director Compliance, Porsche **Laura del Pino Jiminez,** Discipline Leader of Data and People Information Security, BBVA
11:30	**Leveraging the cloud for a successful digital transformation** **Axel Pérez,** Sales Engineer Iberia, Zscaler • Cloud and mobility: the end of legacy security perimeter? • Taking advantage of corporate network transformation • App Access: the Zero Trust Network Access (ZTNA) concept
11:50	**The future of Multifactor Authentication (MFA)** **Eduardo Helering,** EMEA Head of Solutions Engineering, OneLogin • What is multifactor authentication (MFA)? • How does it work? • How can it help us prevent a security breach? • The future of multifactor authentication, where are we going?
12:10	**Education Seminars | Session 1** IntSights **The IntSights advantage** **Andrea Bellinzaghi,** Technical Director Southern Europe, IntSights OneTrust **Overcoming today's most pressing third-party risk management challenges** **Teba Ríos,** CIPP/E, CIPM, Solutions Engineer, OneTrust
12:50	Lunch and networking

Agenda

13:50 **EXECUTIVE PANEL DISCUSSION** — **The new cybersecurity rulebook: how to survive in today's changing regulatory landscape**

Fernando Vegas, former CIO and CRO, OHL (Chair)
Alvaro Grande, Security Engineer, Telefónica
Héctor Guzmán Rodríguez, Director of Data Protection and Privacy, BGBG Abogados
Gabriel Moline, CISO, Leroy Merlin

The £183 million fine imposed on British Airways and the £99 million fine on Marriott for its Starwood breach are evidence that data privacy breaches can cause material financial losses. So is this the beginning of a new era in data privacy and protection? Do these fines finally give information security professionals the numbers they need to demonstrate the true financial value of what they do? In this panel we will look at:

- GDPR enforcement: the full picture
- Lessons from the fines: what does it mean for you?
- Managing data governance across multiple regulatory regimes

14:10 **Anti-phishing 3.0: Strategies to REDUCE the phishing that undermines the reputation of your brand**

Borja Rosales, UK, Spain & EMEA Director, Segasec

- Demo: a real IDN and Content Replication Attack-Simulation on a Spanish FS company
- Why protecting your customers/consumers starts by bulletproofing your brand
- Consumer targeting phishing: deal with the symptoms or tackle the roots
- Defensive countermeasures that effectively reduce the number of attacks that use your brand to scam your customers

14:30 **Information security for the C-Level: measuring effectiveness**

Pablo Rubio, IT Risk Management Engineer and Specialist, Nationale Nederlanden

- Both external and internal (corporate) contexts are changing their perception about information security. There is a gap between security level offering and market/regulatory demands
- Security topics need to accommodate in the Board of Directors agenda, in the same way other topics are discussed (accounting, sales, marketing, ...). Include information security in the business strategy as standalone security strategies are not considered relevant
- Current technologies provide capabilities to measure security advantages business wise and more accurate, showing the outcome to the C-level in terms of business strategy: security RoI, security effectiveness and security culture achievements

14:50 **Education Seminars | Session 2**

ManageEngine	OneTrust
Advanced security monitoring techniques: augmenting SIEM with UEBA	**Bolster your incident response plan across privacy & security teams**
Siddharth Sharath Kumar, Product Evangelist, ManageEngine	**Teba Ríos,** CIPP/E, CIPM, Solutions Engineer, OneTrust

15:30 Refreshments and networking

15:50 **EXECUTIVE PANEL DISCUSSION** — **The unsustainable paradigm of the CISO: managing the business demands on today's information security professional**

Manuel Barrios Paredes, CISO, Solvia (Chair)
Raúl Vázquez Pastor, IT Risk Control – CyberRisk Manager, Banco Sabadell
Pablo Rubio, IT Risk Management Engineer and Specialist, Nationale Nederlanden
Maite Avelino, CISO, Ministry of Finance

16:10 **Staying intelligent about fraud: new lessons in the fight against organised crime**

Alvaro Ortega, Head of Law Enforcement Outreach and Investigations Southern Europe, UK, Ireland & Nordic, Western Union

- The Intelligence Unit in the fight against organised crime
- The importance of public-private collaboration in crime-fighting
- The evolution of fraud in connection with other criminal activity

16:30 **The unsustainable paradigm of the CISO**

Jesús García Bautista, CISO and IT Chief, Correos Express

- The unsustainable paradigm of the CISO. The responsibility of the CISO has increased substantially in recent years, taking a more defined form and seeing how its recommendations are being considered, but progress is still needed. How does today's information security leader balance the various business demands?
- Technology does not stop: infrastructure in the cloud, containers, the loss of roles of systems and development personnel, leads us to think and design new ways to protect ourselves. How do we develop the right strategies and choose the right partners to keep up?
- Securing a hyper-connected world. The growth of online commerce and shopping on web services such as Amazon, PC Components, Zara is changing the way we do business. El Corte Inglés, is revolutionising the world of express transport. Case study and actionable takeaways on how to secure the digitalised business

16:50 Chairman's close

Education Seminars	
IntSights **The IntSights advantage** **Andrea Bellinzaghi,** Technical Director Southern Europe, IntSights	With the ever-growing threat universe, cybersecurity teams trying to protect their organisations from every attack are in a losing battle. They are overwhelmed, exhausted, and ultimately ineffective. A smarter approach would be for teams to focus on the attacks that matter most – those specifically targeting their organiszations. The problem is how to do this efficiently. Until now, finding the most relevant threats required research that was so time-consuming, it defeated the purpose. IntSights has changed this dynamic. Only IntSights provides cybersecurity teams with an effective, automated way to identify threat data, attack indicators specific to their organisations and automatically mitigate them. • External threat protection • The IntSights Intelligence Process • Orchestration, automation and remediation
ManageEngine **Advanced security monitoring techniques: augmenting SIEM with UEBA** **Siddharth Sharath Kumar,** Product Evangelist, ManageEngine	In the age of advanced threats and sophisticated malicious insiders, security teams face an uphill task. In order to detect and mitigate security incidents, organisations must revisit their security monitoring strategy and ensure that they are equipped with the right set of tools. This session talks about the latest trends in the realm of security information and event management (SIEM) and why it is important to incorporate machine learning techniques by leveraging user and entity behaviour analytics (UEBA). • Challenges in security monitoring • Integrating event and non-event information into your SIEM solution • Anomaly-based detection with UEBA • Key concepts and use cases
OneTrust **Overcoming today's most pressing third-party risk management challenges** **Teba Ríos,** CIPP/E, CIPM, Solutions Engineer, OneTrust	Managing third-party vendor risk before, during and after onboarding is a continuous effort under global privacy laws and security regulations. While outsourcing operations to vendors can alleviate business challenges, managing the associated risk with manual tools like spreadsheets is complex and time consuming. To streamline this process, organisations must put procedures in place to secure sufficient vendor guarantees and effectively work together during an audit, incident – or much more. In this session, we'll breakdown a six-step approach for automating third-party vendor risk management and explore helpful tips and real-world practical advice to automate third-party privacy and security risk programmes. • Review the drivers and challenges organisations face when managing third-party vendor risk • Identify priorities before, during and after vendor procurement • Takeaway a six-step approach for automating the third-party vendor risk lifecycle • Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk
OneTrust **Bolster your incident response plan across privacy & security teams** **Teba Ríos,** CIPP/E, CIPM, Solutions Engineer, OneTrust	In the event of a breach, privacy and security professionals often approach incident response from two different outlooks. Whereas security teams are focused on threat vectors, privacy teams are concerned with personal data leaks and adhering to various global privacy laws. While the two come from different perspectives, it is possible to build an incident and breach response plan that addresses the needs of both teams. In this session, we'll discuss how to build a harmonised response plan that addresses both the security team's technical needs and privacy team's regulatory requirements across the patchwork of US privacy laws, the GDPR and other global privacy regulations. We'll also provide tips to help you map out a 72-hour personal data breach action plan and share practical advice to improve your privacy programme. • Learn how to build an incident and breach response plan that fits the needs of security teams and privacy teams • Breakdown what stakeholders, teams, tools and processes should come together in the event of an incident or breach • Understand how to maintain a consistent approach to incident response while complying with privacy regulations across the globe