# Post event report


## Strategic Sponsors

BeyondTrust

BITSIGHT
The Standard in SECURITY RATINGS

CROWDSTRIKE

DUO

LastPass by LogMeIn

proofpoint

ThreatMetrix
A LexisNexis® Risk Solutions Company

## Education Seminar Sponsors

ANOMALI

INTSIGHTS
Threat Intelligence Realized.

OneTrust
Privacy Management Software

## Networking Sponsors

SECLORE

## Branding Sponsors

PATECCO
dynamic identity systems.

RiskBased SECURITY

“ Die Agena ist perfekt vorbreitet. Eine vorbildliche und sehr effiziente Organisation. ”

**Senior Security Strategy Specialist, Commerzbank**

“ Eine wirklich gelungene Veranstaltung mit sehr, sehr vielen interessanten Beiträgen. ”

**Information Security Officer, KfW**

“ Es hat mir sehr gut gefallen! ”

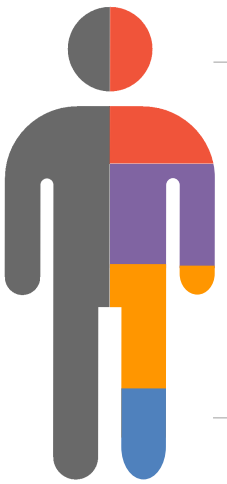
**Business Information Security Officer, Citigroup**

Inside this report:


## Key themes

- Getting the basics right
- The nature of nation state actors
- Cyber-risk identification, measurement and management
- Cost-effective compliance
- Securing specialised systems
- AI: separating the hype from the reality

## 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

Richard Archdeacon,
Advisory CISO
**Duo Security**

Henrik Becker,
Director of Compliance & Risk Management
**Unitymedia**

Charlie Grey,
Privacy Consultant
**OneTrust**

Mohamed Ibbich,
Senior Technology Consultant
**BeyondTrust**

Markus Kügel,
Information Security Officer (Eurex Clearing & Clearstream Banking)
**Deutsche Börse**

Frank Lange,
Principal Security Architect
**Anomali**

Ryan Manyika,
Privacy Consultant
**OneTrust**

Chris Meidinger,
Sales Engineer DACH
**CrowdStrike**

Isabel Münch,
Head of Preventive Cyber Security and Critical Infrastructures Division
**Federal Office for Information Security (BSI)**

Klaus Nötzel,
Corporate ICT Information Security Officer
**EUMETSAT**

Giovanni Pascale,
Sales Engineer
**Proofpoint**

Mischa Peters,
Director of Systems Engineering, EMEA
**IntSights**

Dr Christoph Ritzer,
Partner
**Norton Rose Fulbright**

Yao Schultz-Zheng,
former Information Protection, IT Risk, IT Security, IT Compliance and Privacy Officer
**BMW**

Michael Seele,
Company Owner
**Protea Networks GmbH**

Stephen Topliss, VP of Products,
**ThreatMetrix**

Peter Vahrenhorst,
Detective Chief Superintendent
**Landeskriminalamt North Rhine-Westphalia**

Peter van Zeist,
Sr. Solutions Consultant,
**LogMeIn**

## Agenda

**08:00** Registration

**08:50** Conference welcome

**09:00** **Privacy and cybersecurity – legal framework and case study**

**Dr Christoph Ritzer,** Partner, Norton Rose Fulbright

- Legal implications in case of a cyber-incident – how to deal with the incident and comply with the law
- Overview on legal and regulatory risk landscape
- GDPR aspects and NIS Directive
- Cyber-incident response – case study: legal and regulatory best practices

**09:20** **Digital identities, social engineering and mule networks**

**Stephen Topliss,** VP of Products, ThreatMetrix

- How digital identities are used today to enhance new customer acquisition on the digital channel and protect digital banking sessions for existing customers
- Specific approaches to identify the risk of social engineering based account takeover
- How a targeted approach to real-time mule account detection can enhance existing fraud prevention strategies

**09:40** **Enabling faster incident response via intelligence automation: making the data work for you**

**Chris Meidinger,** Sales Engineer DACH, CrowdStrike

- How to achieve automated investigation TODAY
- How to apply intelligence and cutting-edge technology to incident response
- How to turn attacks into an opportunity to improve defence – automatically

**10:00** **Do we understand the ISO 27001 correctly?**

**Klaus Nötzel,** Corporate ICT Information Security Officer, EUMETSAT

- The ISO 27001 demands an analysis of the culture of an organisation and the context it is operating. But what is a culture and context analysis and what are the advantages to improve information security compliance?
- How the ISO 270001 relies on other business functions e.g. risk assessment
- How will AI and digital innovation change and impact the compliance and regulatory landscape?

**10:20** **Education Seminars | Session 1**

| Anomali | OneTrust |
|---|---|
| **Threat or not? How threat intelligence supports informed decision making in the modern SOC** | **Developing a GDPR-ready incident & breach 72-hour action plan** |
| **Frank Lange,** Principal Security Architect, Anomali | **Charlie Grey,** Privacy Consultant, OneTrust |

**11:00** Networking & refreshments break

**11:30** **EXECUTIVE PANEL DISCUSSION** **Know your business: evaluating and addressing your organisation's key risks**

**Henrik Becker,** Director of Compliance & Risk Management, Unitymedia

**Isabel Münch,** Head of Preventive Cyber Security and Critical Infrastructures Division, Federal Office for Information Security (BSI)

**Klaus Nötzel,** Corporate ICT Information Security Officer, EUMETSAT

**Chairman: Peter Vahrenhorst,** Detective Chief Superintendent, Landeskriminalamt North Rhine-Westphalia

**11:50** **Enterprise password management and reporting – best practice**

**Peter van Zeist,** Sr. Solutions Consultant, LogMeIn

Besides multi-factor authentication, single sign-on and biometric data, passwords are still the most common form of authentication. In our session we will talk about how:

- organisations are better able to reconcile the needs of IT departments and users
- companies can counteract bad password habits
- LastPass makes companies more secure in an unconventional way
- you can enable your employees to do the same without much effort
- you'll be safer in five steps.

**12:10** **Trust is good, awareness is better: using security awareness training to successfully reduce the risks of cyber-attacks**

**Giovanni Pascale,** Sales Engineer, Proofpoint

- Email fraud and phishing continue to be the fastest growing and most vicious corporate security threats, with even the most sophisticated technical security measures bypassed by carefully planned, social email attacks
- Learn how to protect your employees and businesses from these targeted attacks with Proofpoint's Phishing Simulation and Security Awareness solution
- Learn about the maturity levels of security awareness and the Proofpoint training methodology

## Agenda

**12:30** **How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the Bitsight Portal)**

**Michael Seele,** Company Owner, Protea Networks GmbH

Participants will see a live view into the BitSight Portal. We will demonstrate how continuous cyber-risk monitoring works for your company and the affiliates, your suppliers and peers.

*What will attendees learn:*

- How the cyber-risk rating can be improved in the easiest way. All risk vectors and the results will be demonstrated
- How cyber-risk for your own company and the affiliates, the suppliers and peers can be managed based on qualified events and ratings

**12:50** **Education Seminars | Session 2**

| IntSights | OneTrust |
|---|---|
| **The digital risk dilemma: how to protect what you don't control** | **Don't acquire your next breach: managing the vendor risk lifecycle** |
| **Mischa Peters,** Director of Systems Engineering, EMEA, IntSights | **Ryan Manyika,** Privacy Consultant, OneTrust |

**13:30** Lunch

**14:30** **Data protection regulation as a fuel for sustainable digital transformation**

**Yao Schultz Zheng,** Former Head of Compliance, BMW

*Why*

- Centralised IT organisations have historically been considered a cost centre, not a business enabler. Therefore many monolithic systems have been built to save on license, maintenance and operating costs
- Data protection (GDPR and intellectual property), however, is a cultural, national or regional issue, since collecting and consuming valuable data in the digital age has a very high impact on the security, profitability and competitiveness of a country or region
- There is therefore a high tension between legacy centralised data processing and the strict requirement to store the data locally and close to the owner

*How (illuminated by a case study)*

- Breaking down rigid, centralised and waterfall-based silo process and organisational structure and establishing a risk-based, policy- & identity-driven, distributed and networked BizDevOps process and organisation model
- Disassemble historically grown monolithic systems according to data protection as well as the need-to-know principle, and additionally to provide more agility
- Build decentralised hybrid cloud infrastructures

**14:50** **Privileged Access Management (PAM): the critical missing piece in your security strategy**

**Mohamed Ibbich,** Senior Technology Consultant, BeyondTrust

- What does 'privilege' mean to your business?
- How implementing a Privileged Access Management (PAM) solution drives significant improvements across your organisation

**15:10** **Beyond security: zero trust – making the perimeter less lonely**

**Richard Archdeacon,** Advisory CISO, Duo Security

- Concept of zero trust or the BeyondCorp model
- Why a zero trust model will reduce risk
- Key elements in implementing a zero trust approach

**15:30** Networking & refreshments break

**15:50** **EXECUTIVE PANEL DISCUSSION** **2019: the toughest year in cybersecurity yet**

**Markus Kügel,** Information Security Officer (Eurex Clearing & Clearstream Banking), Deutsche Börse

**Yao Schultz-Zheng,** former Information Protection, IT Risk, IT Security, IT Compliance and Privacy Officer, BMW

**Chairman: Peter Vahrenhorst,** Detective Chief Superintendent, Landeskriminalamt North Rhine-Westphalia

**16:30** Closing remarks

**16:40** Conference close

| Education Seminars | |
|---|---|
| **Anomali**<br><br>**Threat or not? How threat intelligence supports informed decision making in the modern SOC**<br><br>**Frank Lange,** Principal Security Architect, Anomali | The current widely adopted methodologies for cybersecurity operations are failing. The approach for addressing current threat actors is ridged, non-adaptive and relies on a small infinite amount of investigation approaches. Due to change management processes, configuration changes slowly, typically at the scale of days or weeks. Many only allow for time-based threat discovery from the current point in time into the future. This passive approach to detection and defence frequently misses the advanced attack threat actor for months. The new approach needs to be supported by creating a more dynamic system that drives active investigation for breaches by continuously updating security detection controls with new intelligence and active searches over historical data for intruder activity.<br><br>What you will learn in this session:<br><br>• How to achieve proactive threat detection with threat intelligence<br>• How to handle the security information overload<br>• How to enable risk-based prioritisation of threats<br>• How to increase SOC efficiency in the age of limited cyber resources |
| **IntSights**<br><br>**The digital risk dilemma: how to protect what you don't control**<br><br>**Mischa Peters,** Director of Systems Engineering, EMEA, IntSights | More of your attack surface resides on web infrastructure you don't own or control. To protect your digital assets and prevent malicious lookalikes on everything from social networks to criminal marketplaces, you must shift security priorities from prevention to detection and remediation.<br><br>This session will outline tools, tactics and best practices to safeguard your entire digital footprint.<br><br>• Monitor the clear, deep and dark web for your organisation's digital assets<br>• Gain visibility and take action when malicious brand lookalikes pop-up<br>• Discover and mitigate phishing attacks targeting your executives and customers |
| **OneTrust**<br><br>**Developing a GDPR-ready incident & breach 72-hour action plan**<br><br>**Charlie Grey,** Privacy Consultant, OneTrust | The GDPR put stricter guidelines on when data controllers need to notify supervisory authorities when a personal data breach occurs. The notification needs to be done without undue delay, no later than 72 hours after the controller has become aware of the breach (with some exceptions). It is crucial for organisations to understand their obligations and the details of this tight timeline as well as the risk-based triggers, and what they entail. In this session, we'll review the personal data breach rules under the GDPR and provide tips to help you map out a 72-hour personal data breach action plan.<br><br>Attendees will learn:<br><br>• Map out a GDPR-ready 72-hour personal data breach action plan<br>• Outline the details of this tight timeline as well as the risk-based triggers and what they entail<br>• Implement efficient and effective data handling practices in the face of new GDPR requirements |
| **OneTrust**<br><br>**Don't acquire your next breach: managing the vendor risk lifecycle**<br><br>**Ryan Manyika,** Privacy Consultant, OneTrust | Managing your vendor risk before, during and after onboarding is a continuous effort for privacy and security regulations. While outsourcing operations to third- and fourth-party vendors can alleviate business problems and needs, it often comes with risk of acquiring your next breach. To streamline this risk, organisations must prioritise privacy and security 'by design' to improve their programmes, as well as secure sufficient vendor guarantees to effectively work together during an audit, incident – or much more. In this session, you'll learn how to implement a successful vendor risk management process and explore helpful tips and real-world practical advice to improve your privacy and security programmes.<br><br>Attendees will learn:<br><br>• Review GDPR regulation, scope, and the new legal obligations it presents for 3rd and 4th party vendor risk management<br>• Identify priorities before, during, and after vendor procurement<br>• Secure sufficient guarantees from vendors to efficiently work with them during audits or incidents |