

THE FUTURE OF CYBER
SECURITY EUROPE
BRINGS YOU UP TO DATE
WITH THE LATEST ISSUES



GDPR

The little things that matter...

MARCH 16 | LONDON

Myths, robots and superpowers

Neira Jones FBCS, MSc

Independent Advisor, Payments, Risk, Cybercrime, & Digital Innovation

Non-Executive Director, Cognosec

 @neirajones

 cognosec



CONSUMER BEHAVIOUR DRIVES CHANGE

Technology & hyper-connectivity generate even more data...

OUR DIGITAL LIVES

2016: 7.2 Bn People



2016: 6.4 Bn Connected Things ***

2018: 45% of the fastest-growing companies will have fewer staff than instances of smart machines

2020: 24Bn Connected Things****

7.7Bn People

85% of customer interactions will be handled without a human

1.3 Bn People (30%) will routinely work remotely *



*Source: Symantec, August 2014

** Source: International Labour Organisation, World Bank

*** <http://www.gartner.com/newsroom/id/6165217>

****: Gartner, Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing.

*****: <http://uk.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5>

THE DRIVERS FOR CONSUMER BEHAVIOUR

Hyper-connected consumers are spoilt for choice and consequently demand more...

SOCIAL MEDIA

IoT: WEARABLES, CONNECTED HOME, CONNECTED CAR, ETC...

INSTANT FULFILMENT

UBIQUITY

ARE WE IN CHARGE OR OUR DATA?...

Hyper-connected consumers are spoilt for choice and consequently demand more...

**DATA IS THE NEW
COAL
OIL
MONEY**

MORE AND MORE DATA, EVERYWHERE

MORE CONNECTIVITY

MORE AND MORE TECHNOLOGIES

MORE COMPUTING POWER

MORE COMPLEX ANALYTICS, MORE INSIGHTS

EXTENDED SUPPLY CHAIN

MORE WAYS TO COMMERCIALISE & MONETISE

IT ALSO INTRODUCES MORE RISK...

MANAGING RISK IS CRUCIAL

FIGHTING FRAUD AND CYBERCRIME
BEING SERIOUS ABOUT INFORMATION SECURITY
MANAGING THE EXTENDED SUPPLY CHAIN
UNDERSTANDING HOW NEW TECHNOLOGIES
CAN STREAMLINE OPERATIONS
UNDERSTANDING REGULATIONS



MANAGING RISK IS CRUCIAL

Cybersecurity: It's Now the Board's Problem



Greg Bell, KPMG

Cybercrime is no longer just a "tech" issue for companies. It's not even just for top management. Today, the problem sits firmly on the laps of the company's board.

Among other things, investors and regulators want board members to provide more transparency about major data breaches and their impact on the company's business.

So boards and audit committees are now putting the issue near the top of their agenda. The problem is that few have much experience with cyber theft or related cyber issues or disruption. Even more alarming, most say they aren't getting adequate information about it from their company.



The stakes are enormous. Whether there's accidental data leakage or deliberate attacks, boards now have to deal with the consequences. They include:

- Intellectual property losses including patented information and trademarked material, client lists and commercially sensitive data.
- Legal expenses including damages for data privacy breaches/compensation for delays, regulatory fines and the cost associated with defense.
- Property losses of stock or information leading to delays or failure to deliver.
- Reputational loss, which may lead to a decline in market value, and loss of goodwill and confidence by customers and suppliers.
- Time lost and distraction to the business due to investigating how the breach occurred and what information (if any) was lost, keeping shareholders advised and explaining what occurred to regulatory authorities.
- Administrative cost to correct the impact such as restoring client confidence, communications to authorities, replacing property and restoring the organization's business to its previous levels.

SecurityScorecard Insights & News



Third Party Vendor Breaches Still A Major Cybersecurity Issue in 2016

Posted on July 20, 2016 by Josue Ledesma | Fraud, Newswire, Risk Mitigation, Third Party Risk, Vendor Management

Share with your network



Last summer we reviewed the third party vendor breaches that made some of the biggest impacts on companies and consumers. This year, data breaches linked to a third party vendor have not let up and the issue is getting worse. Soha Systems Survey on Third Party Risk Management notes that 63% of all data breaches can be attributed to a third party vendor.

JAN 17, 2016 @ 11:01 AM 21,807 VIEWS

Cyber Crime Costs Projected To Reach \$2 Trillion by 2019



Steve Morgan, CONTRIBUTOR
I write about the business of cybersecurity. FULL BIO
Opinions expressed by Forbes Contributors are their own.

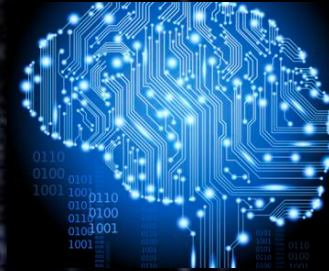
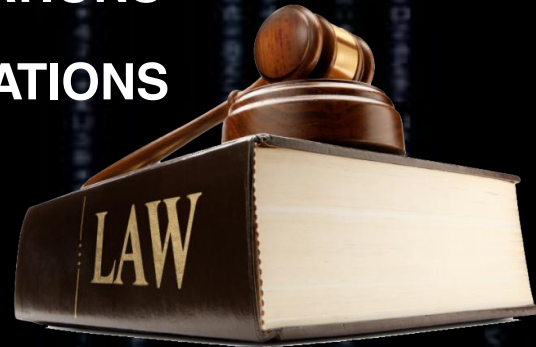


Photographer: Ken Cedeno/Bloomberg News.

'Crime wave' is an understatement when you consider the costs that businesses are suffering as a result of cyber crime. 'Epidemic' is more like it. IBM Corp.'s Chairman, CEO and President, Ginni Rometty, recently said that cyber crime may be the greatest threat to every company in the world.

MANAGING RISK IS CRUCIAL

FIGHTING FRAUD AND CYBERCRIME
BEING SERIOUS ABOUT INFORMATION SECURITY
MANAGING THE EXTENDED SUPPLY CHAIN
UNDERSTANDING HOW NEW TECHNOLOGIES
CAN STREAMLINE OPERATIONS
UNDERSTANDING REGULATIONS



MACHINE LEARNING



THREAT INTELLIGENCE



IDENTITY & AUTHENTICATION



WHAT REGULATIONS SHOULD I LOOK AT?...

A complex landscape...

THERE ARE MANY...



EU-US Privacy Shield



e-Privacy Directive



Payment Services Directive (PSD2)



AND THERE ARE MANY...



NIS Directive



Trade Secrets Directive



General Data Protection Regulation (GDPR)



Anti-Money Laundering Directive (4AMLD, 5AMLD)

MANY REGULATIONS INTER-MINGLE, OVERLAP, & SOMETIMES CONFLICT...

MANY SILOS

SECURITY & PRIVACY REGULATIONS

GDPR. Comes into force May 2018.

NIS Directive. Came into force August 2016.

e-Privacy Directive. Will come into force May 2018.

Trade Secrets Directive

EU-US Privacy Shield. Came into force July 2016.

PCI DSS. This standard has been in force since 2004.

INDUSTRY EXAMPLE: FINANCIAL REGULATIONS

Payment Services Directive (PSD2). Will come into force in January 2018.

EBA Strong Customer Authentication (with PSD2).

4th Anti-Money Laundering Directive (4AMLD). will come into force in June 2017.

DATA PROTECTION – DATA PRIVACY

GENERAL DATA PROTECTION REGULATION (GDPR)

Comes into force **May 2018**. Applies to data “**Controllers**” and “**Processors**”.

Applies to processing carried out by organisations operating **within the EU & outside the EU** when offering goods or services to individuals in the EU.

Extends the definition of “**Personal Data**” and defines “**Sensitive Personal Data**” and makes specific provisions for **Children**.

Stringent requirements on “**Consent**” & “**Explicit Consent**”

New rights for individuals (e.g. Data Portability, Profiling, Erasure, Access free of charge)

Privacy Notices

Data Protection Officer

Accountability, transparency & governance

DATA PRIVACY

e-PRIVACY DIRECTIVE

Will come into force in May 2018 for EU member states, **aligns with the GDPR.**

Includes **social messaging** (e.g. Skype, Whatsapp, Facebook Messenger)

One single set of rules for people & businesses in the EU.

Direct Marketing implications for **consent** (B2B or B2C)

Simpler rules on cookies.

Protection against spam.

More effective enforcement.

The screenshot shows a news article on the Recode website. The article title is "Google's Allo app can reveal what you've searched to your friends". The byline is "BY PERS TOWNSEND | MAR 15, 2017, 9:00PM EDT". The article text states: "The mobile messaging app lets you include Google Assistant in conversations." Below the text is a large image of a smartphone displaying the Allo app interface. To the right of the main image is a "TRENDING" section with a smaller image of the same smartphone and a caption: "Google's Allo app can reveal what you've searched to your friends". Below that is another trending item featuring a photo of Jeff Bezos and the caption: "Jeff Bezos has a new top adviser at Amazon". At the bottom of the article, there is a small caption: "The Verge" and a paragraph: "Google's mobile messaging app Allo can reveal your Google search history to people you message, which could have big privacy implications. The behavior appears to be a glitch."

INTELLECTUAL PROPERTY

TRADE SECRETS DIRECTIVE

Directive on the Protection of Undisclosed Know-How and Business Information. Will be implemented throughout the European Union during 2018, **aligns with the GDPR.**

Harmonises the definition of a trade secret which must meet **all** of the following requirements:

- **is secret** in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- **has commercial value because it is secret;**
- has been subject to **reasonable steps** under the circumstances, by the person lawfully in control of the information, **to keep it secret.**

Focus on cybercrime and the requirement for businesses to take greater steps to protect what they regard as their trade secrets.



DATA TRANSFERS

EU-US PRIVACY SHIELD

Came into force in June 2016.

Protects the fundamental rights of anyone in the EU whose **personal data is transferred to the United States** as well as bringing legal clarity for businesses relying on transatlantic data transfers.

Strong obligations on companies handling data.

Clear safeguards and transparency obligations on US government access.

Effective protection of individual rights.

Annual joint review mechanism.



CARDHOLDER INFORMATION SECURITY

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

This standard has been in force since 2004.

Whilst it is not law in the EU, Card Schemes mandate it as part of their operating regulations.

Its fundamental aim is to **protect cardholder information**.

The PCI Security Standards Council defines the PCI Standards and the Card Schemes enforce it through mandates.

Card Schemes levy penalties for breach of mandates.

PCI DSS compliant service providers can be found at:

<https://www.visaeurope.com/receiving-payments/security/downloads-and-resources>

<https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html>

NETWORK & INFORMATION SECURITY

DIRECTIVE ON SECURITY OF NETWORK & INFORMATION SYSTEMS (NIS)

Came into force in July 2016 for EU member states (deadline May 2018).

Promotes a culture of security across sectors which are vital for our economy and society and rely heavily on IT, such as **energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure**.

Businesses in these sectors that are identified by the Member States as operators of essential services must take **appropriate security measures** and **must notify serious incidents** to the relevant national authority (sometimes double-whammy).

Key **digital service providers** (search engines, cloud computing services and online marketplaces) must comply with the security and notification requirements under the new Directive.

FINANCIAL SERVICES SECURITY

PAYMENT SERVICES DIRECTIVE

The EU's 2nd Payment Services Directive will come into force in January 2018.

Focus on Security & Incident Reporting. Also refers to the NIS Directive.

Strong Customer Authentication requirements have been published by the European Banking Authority (EBA).

Extended coverage to Third Party Providers (TPPs), putting focus on the supply chain.

Promotes Open Access & Competition



FINANCIAL CRIME

4th ANTI-MONEY LAUNDERING

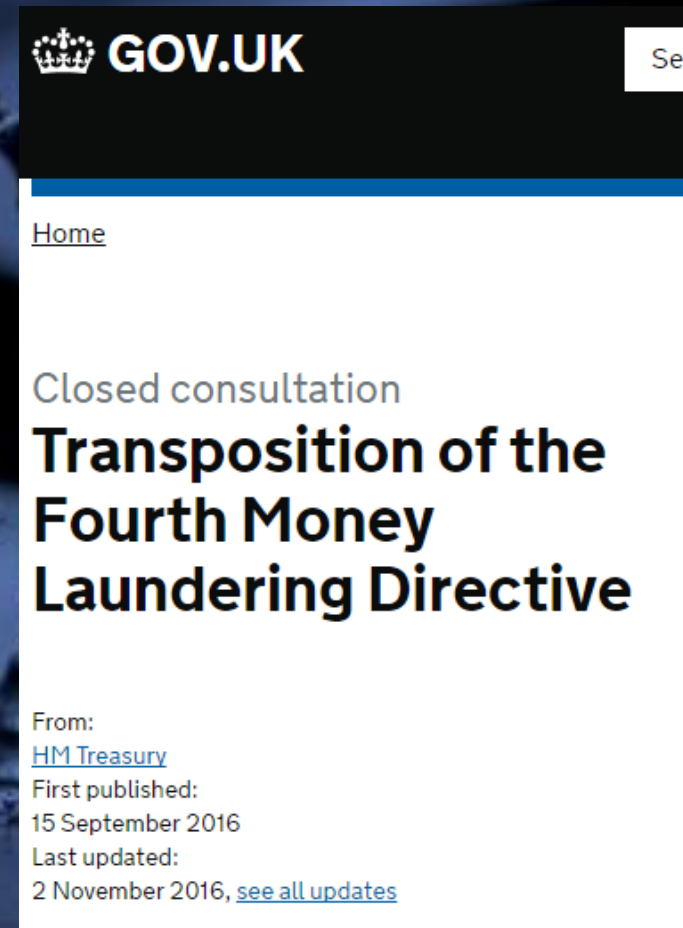
Comes into force in June 2017.

New requirements for financial institutions to **include data protection policies** within their AML policies and **procedures for customer information sharing**.

KYC: Customer Due Diligence, Beneficial Ownership, etc.
Collecting more data (5 years retention unless relating to an “identified or identifiable natural person” where it must be deleted, unless provided for by national law).

Business & Personal Accountability: fines of at least €5M or 10% of the total annual turnover (and at least €5M for a natural person).

Risk Assessment & Governance



The screenshot shows a GOV.UK page for a closed consultation. The header includes the GOV.UK logo and a search bar. The main content area features the title "Closed consultation Transposition of the Fourth Money Laundering Directive". Below the title, it lists the source as "HM Treasury", the first published date as "15 September 2016", and the last updated date as "2 November 2016, see all updates".





NAVIGATING THE MAZE

REGULATIONS & STANDARDS ARE
NUMEROUS IN ALL INDUSTRIES.

THIS CAN BE OVERWHELMING AND A
HOLISTIC APPROACH IS RECOMMENDED.

AUTOMATION HAS BECOME NECESSARY AND
THIS HAS CREATED A NEW INDUSTRY:
REGTECH

Pe RAVN launches GDPR Robot
Added on the 10th Mar 2017 at 3:23 pm

W    

01 F Compliance with The General Data Protection Regulation (GDPR) is top of most 2017 legal
Sour agendas and RAVN Systems last night (9 March) unveiled an astutely timed GDPR Robot
powered by its Applied Cognitive Engine (RAVN ACE).

Pe The GDPR Robot allows users to quickly search, retrieve, flag, classify and report on data
sol considered to be sensitive and personal under GDPR. Users have the ability to identify
Pel personal data from documents, view feeds on the latest personal data that requires attention
and provide reports on the data suggested to be deleted or secured.

Har RAVN's GDPR Robot is also able to expedite requests for information (Data Subject Access
Pre Requests – "DSAR"), removing the need for a manual, labour intensive approach.

and Organisations are currently having to ensure that they have internal data protection policies
stat and procedures in place, in preparation for GDPR's onerous obligations on data controllers
and processors, greater fines, and enhanced rights for individuals.

Wit As the GDPR Robot was formally unveiled at RAVN's annual office party last night, European
fra operations director Sebastiaan Bos, [who joined in 2016 from HighQ](#), also gave a
com demonstration of RAVN Extract – a self-service, simpler version of RAVN ACE that enables
net law firms to identify, analyse and extract text themselves.

par It is envisaged that RAVN Extract will enable firms to further analyse contracts and
and agreements to ensure privacy policy clauses and other relevant obligations meet the new
regulatory standards under GDPR.

NAVIGATING THE MAZE

REG
NUM
THIS
HOL
AUT
THIS
REG

RAVN launches GDPR Robot

Added on the 10th Mar 2017 at 3:23 pm



Compliance with The General Data Protection Regulation (GDPR) is top of most 2017 legal agendas and RAVN Systems last night (9 March) unveiled an astutely timed GDPR Robot powered by its Applied Cognitive Engine (RAVN ACE).

The GDPR Robot allows users to quickly search, retrieve, flag, classify and report on data considered to be sensitive and personal under GDPR. Users have the ability to identify personal data from documents, view feeds on the latest personal data that requires attention and provide reports on the data suggested to be deleted or secured.

RAVN's GDPR Robot is also able to expedite requests for information (Data Subject Access Requests – "DSAR"), removing the need for a manual, labour intensive approach.

Organisations are currently having to ensure that they have internal data protection policies and procedures in place, in preparation for GDPR's onerous obligations on data controllers and processors, greater fines, and enhanced rights for individuals.

As the GDPR Robot was formally unveiled at RAVN's annual office party last night, European operations director Sebastiaan Bos, [who joined in 2016 from HighQ](#), also gave a demonstration of RAVN Extract – a self-service, simpler version of RAVN ACE that enables law firms to identify, analyse and extract text themselves.

It is envisaged that RAVN Extract will enable firms to further analyse contracts and agreements to ensure privacy policy clauses and other relevant obligations meet the new regulatory standards under GDPR.

ED.
RY AND

Pelican applies AI to fight Swift and wire transfer fraud

01 February 2017 | 5324 views | 0

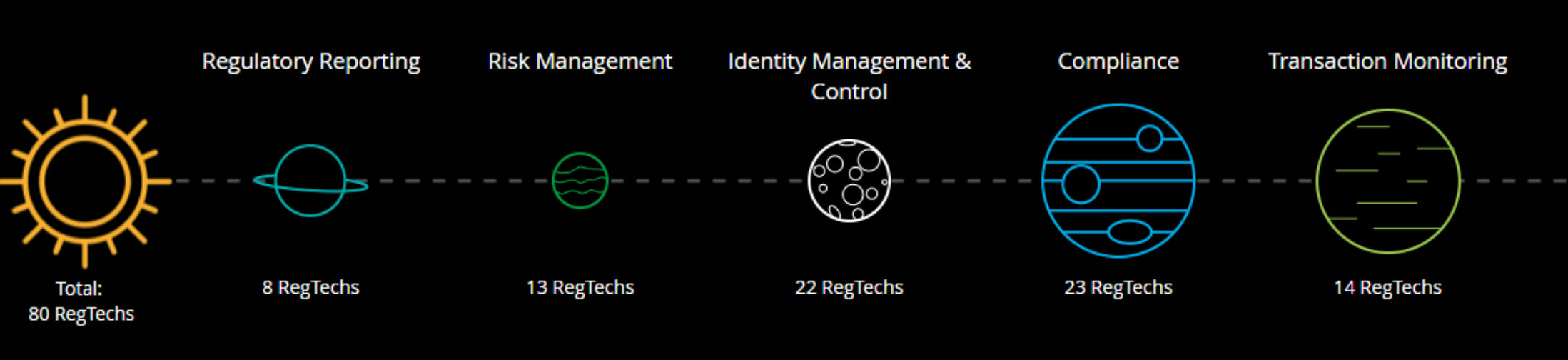
Source: Pelican

Pelican, a global provider of payments and compliance solutions for banks and corporates, today unveiled its PelicanSecure Fraud Prevention solution.

Harnessing artificial intelligence technology the PelicanSecure Fraud Prevention solution actively and intelligently monitors, analyses, detects and prevents attempted fraud breaches - going far beyond existing static 'check-box' compliance systems.

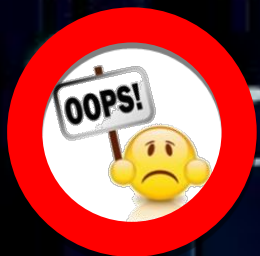
With seemingly daily revelations of cyber hacks and security breaches, fraud prevention and detection should be a top priority in correspondent banking networks. Recent breaches across the SWIFT network further highlight the ever-increasing fraud threats and the particular vulnerabilities facing SWIFT, Real-Time Gross Settlement and wire payments.

REGULATORY AUTOMATION: REGTECH CAN HELP



Source: Deloitte RegTech Universe, January 2017
<https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-universe.html>

REMEMBER! PUTTING THINGS IN CONTEXT...



Common denominator in 75% of incidents: PEOPLE *



63% of all data breaches are linked directly or indirectly to THIRD PARTIES in the supply chain **

* Source: Verizon DBIR 2016

** Source: Soha Systems, April 2016

PRO TIP: PRIORITISE MANAGING INSIDER THREATS

Establish a **Staff Data Protection Programme** to address insider threats:

Phishing

Malicious behaviour

Miscellaneous Errors

Lost & Stolen devices



The screenshot shows a news article on the CYWARE website. The article title is "Insider Misuse of Computers: No Big Deal? It Could be a Data Breach, ask Boeing", dated March 12, 2017, under the category "Laws, Policy, Regulations". The article text discusses a Boeing employee's misuse of internal documents, leading to a data breach. It explains that sensitive data left Boeing's control when it was shared with a non-employee. The article also mentions that determining a breach depends on local laws, specifically citing the Texas Breach of Security of Computerized Data law, which defines SPI (Sensitive Personal Information) as: 1) Information made lawfully available is not personal information; 2) Personal information includes all personal details; 3) Information about the person's health and healthcare. An image of a Boeing airplane is shown on the right side of the article.

PRO TIP: PRIORITISE SUPPLY CHAIN GOVERNANCE

Establish a **supply chain review programme**:

Procurement processes

Contracts

Data location and transfers

PRO TIP: PRIORITISE SUPPLY CHAIN GOVERNANCE

ICO making enquiries into Landauer breach of NHS staff data

Laura Stevens

13 March 2017



The Information Commissioner Office "is making enquiries" into the hack of a US company that has compromised the privacy of thousands of NHS staff at all nine health boards and trusts in Wales.

Over 3,000 NHS Wales staff are the latest victims of the data breach at US company Landauer, with their names, dates of birth, radiation doses and NI numbers stolen from one of the company's UK computer servers.



SC US
SC UK

NEWS CYBER-CRIME NETWORK SECURITY PRODUCTS JOBS VIDEO EVENTS WHITEPAPERS

THE CYBER-SECURITY SOURCE

Orchestrate workflows to scale threat detection and response. 

Get Newsletter

SC Magazine UK > News > Data Breaches > Thousands of NHS Wales staff lose personal data in breach

by Danielle Correa, Production Editor

March 13, 2017

Thousands of NHS Wales staff lose personal data in breach



The details of thousands of NHS staffers in Wales have been stolen from the servers of a private contractor, Landauer.

A hacker **reportedly** stole personal details including names, birthdates, national insurance numbers and radiation doses from Welsh NHS medical staff.



NHS Wales said that not every staff member was impacted in the same way since a different combination of data was being held on each staffer. Over 500 people working at Velindre NHS Trust and 654 at Betsi Cadwaladr University Health Board were victimised.

Thousands of NHS Wales staff lose personal data in breach

PRO TIP: THIS IS NOT NEW...

Policies/ Procedures/ Procurement/ Governance
Process Control/ DevOps/ Workflow Management
Disposal/ Decommissioning
Data Classification
Education / Enablement
User Behaviour Monitoring
Incident Response
Continuous Improvement

DPO, CDO, CISO,
CRO, HR, LEGAL,
PR, COMMS

PEOPLE

PROCESS

Endpoint security
Behavioural analytics
Server/ Network/ Application Security & Monitoring
Email security
Encryption/Tokenisation
Access management
Multi-factor Authentication/ Privilege Account management
Patch All The Things!!!
Threat Intelligence/ Data Leakage Prevention

CISO, CIO

TECHNOLOGY



INTERNET OF THINGS

A new challenge: toys and more toys...

CHILDREN AT RISK

The GDPR makes new provisions in Article 8: children's consent for:

- “Information Society Services” offered directly to children (other than preventive or counselling services) and you want to rely on **consent** rather than another lawful basis for processing, parental consent must be obtained for children under 16 – although the UK may choose to lower this, to a minimum age of 13.
- If you choose to rely on children's consent, you will need to implement **age-verification measures**, and make “reasonable efforts” to verify parental responsibility for those under the relevant age.
- For other types of processing, the general rule in the UK is that you should consider whether the individual child has the **competence to understand and consent** for themselves (the “Gillick competence test”)

Mashable

The latest internet-of-things privacy breach was brought to you by teddy bears

1.6k SHARES

Share on Facebook Share on Twitter



CloudPets

\$39.99

They're really quite sinister.

IMAGE: COURTESY I3

CHILDREN AT RISK

The GDPR makes new provisions in Article 8:
children's consent for:

Mashable

The latest internet-of-things privacy breach was brought to you by teddy bears

1.6k SHARES

Share on Facebook Share on Twitter +

CloudPets \$39.99

They're really quite sinister.

IMAGE: CLOSURE/FB

engadget UK

Germany bans creepy doll over privacy concerns

No, it's not Chucky.

Stefanie Fogel, @stefaniefogel
02.17.17 in Gadgets

CNBC HOME INTL NEWS MARKETS INVESTING TECH MAKE IT VIDEO

VTech hack: Data of 6.4M kids exposed

Wednesday, 2 Dec 2015 | 12:08 AM ET

REUTERS

"LARGEST KNOWN HACK TARGETING CHILDREN"

A cyber attack on digital toymaker VTech Holdings exposed the data of 6.4 million children, the company said on Tuesday, in what experts called the largest known hack targeting youngsters.

that you should consider whether the individual child has the **competence to understand and consent** for themselves (the "Gillick competence test")

TOYS FOR ADULTS...

Manufacturers of IoT devices are in focus of data privacy regulators.

Privacy Notices are becoming increasingly important

Even more **sensitive personal data** may be at risk...

Big Data, AI & Profiling...

GIZMODO

SENSITIVE PERSONAL DATA

Data consisting of **racial** or **ethnic** origin, **political** opinions, **religious** or **philosophical** beliefs, or **trade union** membership, **genetic** data, **biometric** data, data concerning **health** or data concerning a natural person's **sex life** or sexual orientation.

TOYS FOR ADULTS...

Manufacturers of IoT devices are in focus of data privacy regulators.

Privacy Notices are becoming increasingly important

Even more **sensitive personal data** may be at risk...

Big Data, AI & Profiling...

SENSITIVE PERSONAL DATA

Data consisting of **racial** or **ethnic** origin, **political** opinions, **religious** or **philosophical** beliefs, or **trade union** membership, **genetic** data, **biometric** data, data concerning **health** or data concerning a natural person's **sex life** or sexual orientation.

TOYS FOR ADULTS...

SENSITIVE PERSONAL DATA
Data consisting of **racial** or **ethnic** origin, **political** opinions, **religious** or **philosophical** beliefs, or **trade union** membership, **genetic** data, **biometric** data, data concerning **health** or data concerning a natural person's **sex life** or sexual orientation.

GIZMODO

Smart Sex Toy Maker Agrees to Pay Customers \$10k Each For Violating Privacy



Rhett Jones

Yesterday 8:02pm · Filed to: TELEDILDONICS



At Standard Innovation we take customer privacy and data security seriously. We have enhanced our privacy notice, increased app security, provided customers more choice in the data they share, and we continue to work with leading privacy and security experts to enhance the app. With this settlement, Standard Innovation can continue to focus on making new, innovative products for our customers.



f Share

🐦 Tweet

TOYS FOR ADULTS...


Ma
foc
Priv
incr
Eve
may
Big

GIZMODO

Smart Sex Toy Maker Agrees to Pay Customers \$10k Each For Violating Privacy

Rhett Jones
Yesterday 8:02pm · Filed to: TELEDILDONICS

22.0K 20 2



Share Tweet

At Standard Innovation we take customer privacy and data security seriously. We have enhanced our privacy notice, increased app security, provided customers more choice in the data they share, and we continue to work with leading privacy and security experts to enhance the app. With this settlement, Standard Innovation can continue to focus on making new, innovative products for our customers.

TOYS FOR ADULTS...

Manufacturers of IoT
focus of data privacy

Privacy Notices are becoming
increasingly important

Even more sensitive personal
may be at risk...

Big Data, AI & Profiling

MailOnline

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money

Latest Headlines | News | World News | Arts | Headlines | France | Pictures | Most read | Wires | Discounts

How cyber hackers could use our Fitbits and other gadgets to hold us to ransom: Criminals could steal pictures, videos and sensitive information to blackmail users

- Fitness trackers, smartphones and voice-activated gadgets are a gift to hackers
- Cyber crooks could steal sensitive information and hold people to ransom
- Findings were highlighted in a report by the NCSC and the National Crime Agency

By CHRIS GREENWOOD, CHIEF CRIME CORRESPONDENT FOR THE DAILY MAIL
PUBLISHED: 01:21, 14 March 2017 | UPDATED: 01:25, 14 March 2017

Share 30 shares View comments 60

The soaring popularity of gadgets which chronicle every moment of our lives leaves us wide open to blackmail and fraud, security chiefs warned last night.

Fitness trackers, smartphones and voice-activated gadgets are recording swathes of intimate information which is a gift for hackers.

Experts suggested it is almost inevitable that sophisticated criminal gangs operating online will move from targeting big businesses to individuals.

The Telegraph HOME | NEWS | SP

Technology

News | Reviews | Opinion | Internet security | Social media | Apple | Google

Technology

Why your smart TV is the perfect way to spy on you

1 Comment

Guide Timeline View

Samsung's F8000 range of smart TVs were named as a device the CIA could have hacked. CREDIT: SAMSUNG.

By Cara McGougan
8 MARCH 2017 - 11:16AM

In a world of internet connected devices that could be targeted by hackers in a number of ways it has become common parlance to hear of smartphones and computers being hacked and turned into spying tools. But recently another common device has been added to the roster of possible monitors: smart TVs.

BIG DATA & ARTIFICIAL INTELLIGENCE

Big Data, analytics & AI are increasingly used for **Profiling**

More opportunities to personalise the customer experience

Privacy Notices, Fair Processing, Minimisation, Portability, Purpose Limitation, Consent, etc.



VIACOM

May 2016

Viacom & Amex help advertisers "forecast commercial intent before it has formed" and target the right moment in time to reach people.

BIG DATA & ARTIFICIAL INTELLIGENCE

Big Data
increasing

More
the cost

Private
Minimize

Limited

information management

Trove of consumer data pledged in new credit bureau product

By Andy Peters
Published March 10 2017, 6:30am EST

More in [Customer experience](#), [Customer data](#), [Customer-centricity](#)

Print | Email | Reprints | Share

Equifax has introduced a software product that gives lenders instant access to all of its consumer data in a single platform.

The new product, Equifax Ignite, pulls together 3 terabytes of data, including its own proprietary data culled from clients plus data from alternative sources such as social media and utility payment records, said Prasanna Dhore, chief data and analytics officer. Ignite also includes analytical tools for risk management,

rise

rise

Grow Your Business > Sales & Marketing

Retailers Turn to AI to Integrate Marketing Channels

By Karina Fabian, B2B Writer | March 12, 2017 08:37 am EST

Want to see better marketing results? You might want to jump on the artificial intelligence bandwagon.



Credit: Miles Studio/Shutterstock

A February 2017 study of 200 businesses showed that retailers plan on expanding their marketing, particularly social media and mobile marketing, and incorporating artificial intelligence to better personalize the customer's journey as well as analyze results.

The study was conducted by [Sailthru](#), a cross-channel management platform company. When discussing what marketing channels best met marketing goals, 56 percent of businesses surveyed said their websites generate the most online revenue, with email marketing and mobile coming in next at 18 percent and 7 percent. Social media trailed at 4 percent.

BIG DATA & ARTIFICIAL INTELLIGENCE

Big Data, analytics & AI are increasingly used for **Profiling**

More opportunities to personalise the customer experience

Privacy Notices, Fair Processing, Minimisation, Portability, Purpose Limitation, Consent, etc.

Viacom taps AmEx transaction data to help advertisers target TV viewers

17 May 2016 | 3501 views | 0



US media behemoth Viacom is to start using American Express transaction data to help firms better target their television adverts.

The two firms are launching a tool, called Vantage Intent, that promises to help advertisers "forecast commercial intent before it has formed and target the right moment in time to reach people," says Kern Schireson, EVP, data strategy and consumer intelligence, Viacom.

BIG DATA & ARTIFICIAL INTELLIGENCE

Big Data, analytics & AI are increasingly used for **Profiling**

More opportunities to personalise the customer experience

Privacy Notices, Fair Processing, Minimisation, Portability, Purpose Limitation, Consent, etc.

Data Protection Act and General Data Protection Regulation

Big data, artificial intelligence, machine learning and data protection

ico.
Information Commissioner's Office

DATA QUALITY

91.4% of organisations are plagued with **data quality issues** (Source: Royal Mail Data Services)

Data management is often shared across multiple functions without consistent collection processes. 65% of organisations cleanse their customer data only once a year, have no **cleansing processes** in place at all, or simply don't know how often their data is cleansed.

Unless organisations act now to improve the quality of their customer data, they will face a **shortfall** in usable, permissioned customer information in May 2018.

Consent, erasure, rectification

The screenshot shows a webpage from 'information age' with a blue header and navigation menu. The article title is 'Will poor data quality jeopardise GDPR compliance?' dated 16 FEBRUARY 2017. The sub-headline reads: 'The costs of poor-quality customer data continue to mount as marketers prepare to comply with the General Data Protection Regulation'. Below the text is a green-tinted image of a compass with 'QUALITY' written on it and a line graph overlaid. To the right of the image is a 'Subscribe' form with fields for 'First Name', 'Last Name', and 'Your Email', and two checkboxes for email preferences.

DATA QUALITY

91.4% of organisations are plagued with **data quality issues** (Source: Royal Mail Data Services)

Data management is often shared across multiple functions without consistent collection processes.

65% of organisations cleanse their customer data only once a year, have no **cleansing processes** in place at all, or simply don't know how often their data is cleansed.

Unless organisations act now to improve the quality of their customer data, they will face a **shortfall** in usable, permissioned customer information in May 2018.

Consent, erasure, rectification



Information Commissioner's Office

Consultation: GDPR consent guidance

Start date: 2 March 2017
End date: 31 March 2017

ico.
Information Commissioner's Office

CONSENT



Do you always need it?...

CONSENT

Consent gives individuals **choice** about how you use their data and ensures that you are **accountable** and **transparent** when it comes to data processing.

Consent is not appropriate if

- You would do it anyway
- You made it a pre-condition of accessing services (and therefore not freely given)
- You are in a position of power

GDPR Lawful Processing
(Article 6, section 1)

(a) Consent

(b) Contractual Obligation

(c) Legal Obligation

(d) Protect a person

(e) In the public interest

(f) Legitimate interests of the controller

GDPR RECITALS

Interpretation is crucial...

RECITALS

Recitals are essential to your understanding of how the Regulation will be interpreted by the Data Protection Authorities.

Both the Court of Justice of the European Union (CJEU) and the European Data Protection Board (EDPB) will use them to **ensure the Regulation is consistently applied across Europe.**

As an EDPB decision on interpretation is binding as far as the UK is concerned, the EDPB will use the Recitals to come to its conclusions (and as the Recital refer to identification “by any other person”, **the ICO interpretation will be overturned**).

Suppose the UK’s Information Commissioner (ICO) interprets the definition of “personal data” in a similar way as in the current Data Protection Act (e.g. **identifiability of the data subject has to be by the data controller**) whereas the rest of Europe includes the impact of **Recital 23** in the Regulation (i.e. identifiability of the data subject has to take account of all the means reasonably likely to be used ...either by the controller **or by any other person** to identify the individual directly or indirectly”).



TRANSPARENCY & ACCOUNTABILITY

Privacy Notices, Impact Assessments, the DPO...

EU GDPR: THE DATA PROTECTION OFFICER



- Must be **appointed for at least 4 years** (employee) or 2 years (contractor).
- Must have the **appropriate experience & expertise**.
- **Controller must maintain the DPO skills.**

A DPO MUST AT A MINIMUM:

- **advise colleagues** and **monitor** their organisation's GDPR/privacy law/policy compliance
- **conduct training** and awareness raising
- **run audits**
- advise regarding **Privacy Impact Assessments & Privacy Notices**
- cooperate with supervisory authorities.

DPOs **must have adequate resources** to be able to meet their GDPR obligations.

DPOs should **report directly to the highest level of management.**

DPOs **must be able to operate independently** of instruction and must not be dismissed or penalised for performing their task.

DPOs **must publish their contact details** for supervisory authorities and data subjects.

EU GDPR: THE DATA PROTECTION OFFICER



IN SUMMARY, THE DPO

- is responsible for application of **policies**,
- **assignment of responsibilities**,
- staff **training & audit**,
- **liaising** with Competent Authorities and data subjects,
- must have a **good understanding of information/cyber security, data protection and data privacy**,
- must have a **good understanding of the applicable laws** (e.g. GDPR obviously, but also DPA, e-Privacy, NIS, EU-US Privacy Shield, Trade Secrets, and for Financial Services, PSD2/AML would be good etc.),
- must have a **good understanding of the supply chain in their sector** and
- should also **understand contract law**, and
- be an **extremely good communicator/negotiator**.

EU GDPR: THE DATA PROTECTION OFFICER



Study: At least 28,000 DPOs needed to meet GDPR requirements



Rita Heimes, CIPP/US



Sam Pfeifle

The Privacy Advisor | Apr 19, 2016



PRO TIP: START HERE

FAMILIAR YOURSELF WITH ALL REGULATIONS IN YOUR SECTOR

A holistic approach and cooperation is required to avoid overlap and inconsistencies
Avoid regulatory silos

APPOINT A DPO

Full or part-time
DPO to establish a Staff Data Protection Programme to address insider threats
DPO to establish a Supply Chain Review Programme
DPO to establish cross-disciplinary working group to address all regulations

CLASSIFY YOUR DATA

Decide which processing basis will apply to each category (e.g. consent or otherwise)
Examine impact of Big Data, IoT, AI, etc, for fair processing
Start working on Impact Assessments and Privacy Notices

IF YOU ALREADY COMPLY WITH THE DPA & HAVE GOOD INFORMATION SECURITY PRACTICES, YOU SHOULD BE A LONG WAY THERE...

THE FUTURE OF CYBER
SECURITY EUROPE
BRINGS YOU UP TO DATE
WITH THE LATEST ISSUES



MARCH 16 | LONDON

THANK YOU!

Neira Jones FBCS, MSc
Independent Advisor, Payments, Risk, Cybercrime, & Digital Innovation
Non-Executive Director, Cognosec

 <http://about.me/neirajones>

 <http://uk.linkedin.com/in/neirajones>

 @neirajones

 neirajones.blogspot.co.uk

 <http://paper.li/neirajones/1369506964>