White Paper

Data Breaches: 2018 Outlook

Overview

The level of data breaches during 2017 was unprecedented. Each time news of one breach died down, the headlines broke again announcing a different organisation had been breached, impacting not only its employees but also customers. No business was too big or too small to remain untouchable. Germany's government continues to investigate the security breach in December of its defence and interior ministry's private servers, with local media reporting that the Russian hacking group Fancy Bear is behind the attack.[1]

Cybercriminals hit Equifax and stole personal data of 145 million people.[2] Revealing the hack two months after it occurred resulted in Chief Executive Officer (CEO), Richard Smith, having to step down. Yahoo's parent company, Verizon, announced that three billion accounts were hacked in 2013, not one billion as originally claimed in 2016.[3] In Poland, hackers stole large amounts of unidentified encrypted data via compromised servers at the Polish financial regulator Komisja Nadzoru Finansowego (KNF)[4] causing significant problems for the country's banks. And some businesses even paid ransoms in an attempt to smooth over the cracks. It is anticipated that the Uber breach and cover up will rumble on for some time with several executives facing jail time for their part in the scandal.

It is estimated that ransomware alone cost businesses $2 billion last year[5], double that of 2016. The WannaCry ransomware attack spanned more than 150 countries, and in September, FedEx attributed a $300 million loss to the NotPetya attack[6], with its subsidiary, TNT Express, having to suspend business for a period of time. Furthermore, Trend Micro predicts global losses from compromised business email scams will exceed $9 billion[7] this year.

Last year, it is estimated that ransomware alone cost businesses

$2 billion

(double that of 2016)

Breach cost – as estimated by the Ponemon Institute

Average breach cost (on a global basis) of

$3.5 million

(in 2017)[8]

IN SOME GEOGRAPHIES THIS BREAKS INTO

$3.62 million in Turkey

$3.6 million in Spain

$1.32 million in the UK

[1] Fancy Bear attack https://www.bbc.co.uk/news/world-middle-east-43232520
[2] http://money.cnn.com/2018/03/01/technology/equifax-impact-more-customers/index.html
[3] https://finance.yahoo.com/news/3-billion-yahoo-users-were-221629268.html
[4] http://www.pbwcz.cz/Articles%20of%20english/crime2.html
[5] Anti-virus software firm Bitfender - https://www.cyberscoop.com/ransomware-2-billion-bitdefender-gpu-encryption/
[6] https://www.infosecurity-magazine.com/news/fedex-notpetya-cost-us-300-million/
[7] http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html
[8] https://www.ibm.com/security/data-breach

The research also cited that there was a 27% probability that a U.S. company will experience a breach in the next 24 months, costing them between $1.1M and $3.8M. And, as IDG journalist Dave Rickard[9] highlighted, when reviewing the findings:

> "The Mean Time to Identify and Mean Time to Contain for 2017 remain respectively at 208 and 52 days, dramatically increasing breach costs. It's not just that proper controls, architecture, and policy are lacking: suboptimal incident detection and response raise the cost of a breach even higher."
>
> – **Dave Rickard**, contributor to CSO from IDG

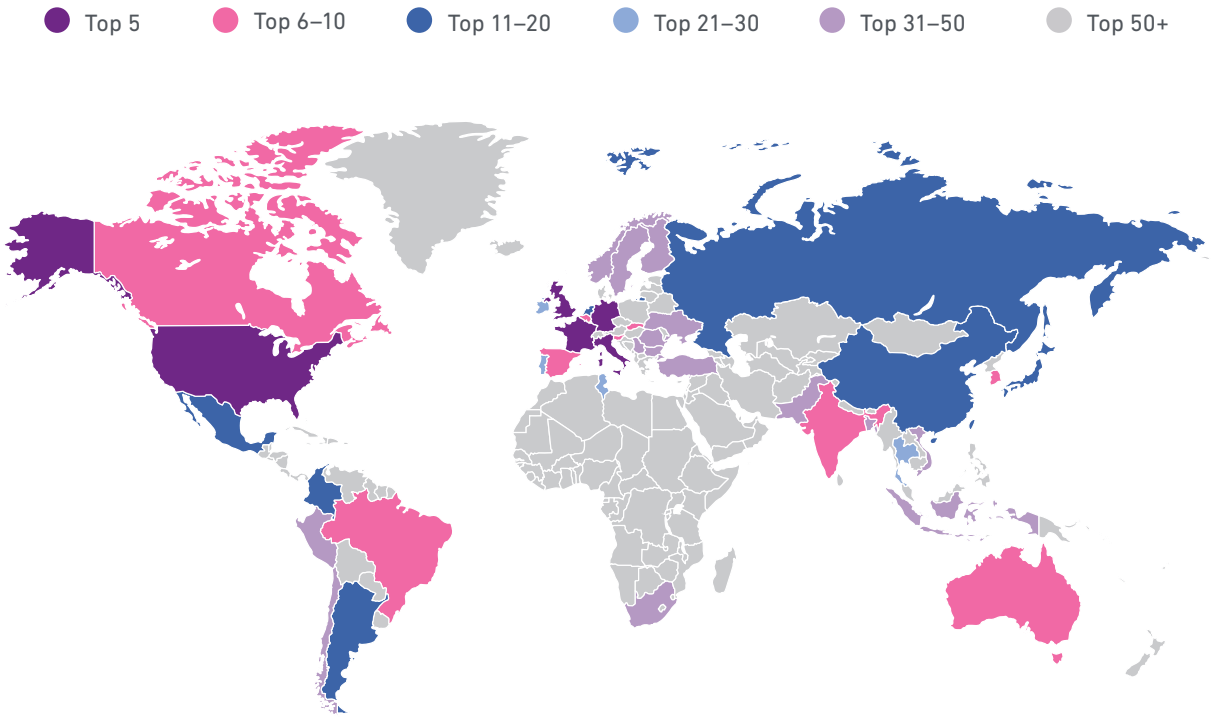
Mean Time to
identify a breach
208
days

Mean Time to
contain a breach
52
days

[9] https://www.csoonline.com/article/3249088/data-breach/the-cost-of-2017-data-breaches.html

Identity Theft Attacks Globally[10]

Based on total number of attacks detected by geography of origin



2018 has followed hot on the heels, with a flurry of record fines ranging from the U.S. Federal Trade Commission (FTC) charging Vtech a £480,000 ($647,506.56) fine[11] relating to a data breach in 2015 to Carphone Warehouse being fined £400,000 ($539,110)[12] by the Information Commissioner's Office (ICO). It's a stark reminder that businesses can no longer deny a breach has occurred or pay cybercriminals in order to survive the aftermath. Proof that the ripple effect of a data breach lasts not just days and months but years.

Organisations are waking up to the fact that it's not a case of if they will be hit by a data breach but when, and the events of the last few years have shown that heads will roll and fines will be dispensed. Indeed, it has been predicted that UK businesses alone could face up to £122 billion in penalties this year[13] now that the European Union's (EU) General Data Protection Act (GDPR) has come into force (25th May 2018).

> "The new EU legislation will be an absolute game-changer for both large organisations and SMEs as the regulator will be able to impose a stratospheric rise in penalties for security breaches, and it remains to be seen whether businesses facing these fines will be able to shoulder the costs...Companies, both large and small, need to act now and start putting in place robust standards and procedures to counter the cyber security threat, or face the prospect of paying astronomical costs in regulatory fines and reputational harm to their brand."
>
> – **Jeremy King**, international director at PCI SSC

[10] Threatmetrix 2017
[11] https://www.scmagazine.com/ftc-punishes-childrens-app-company-for-not-playing-by-the-rules/article/757556/
[12] https://www.bbc.co.uk/news/business-44465331
[13] https://www.computerweekly.com/news/450401190/UK-firms-could-face-122bn-in-data-breach-fines-in-2018

GLOBAL IDENTITY THEFT IN NUMBERS[14]

$2 Trillion

- the estimated global cost of cybercime by 2019

€750 Billion

- the number of euros lost by cybercrime victims globally

$80 Billion

- the estimated global spending to combat cybercrime in 2018

Further research by the Ponemon Institute reveals that cyber risk and data breaches remain a key concern of Chief Information Security Officers (CISOs) in 2018.

67%

of respondents believe their companies are more likely to fall victim to a cyber-attack or data breach in 2018[15]

[14] Threatmatrix, Hackmaggedon.com, SecurityIntelligence.com 2017
[15] https://www.opus.com/resource/2018-ciso-survey-ponemon-institute/

The landscape

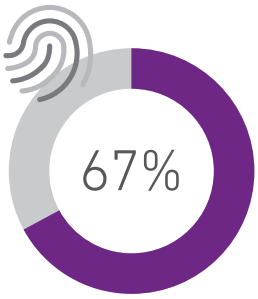
The tremendous growth of data breaches and the sheer impact on a global scale demonstrates that the data breach is no longer the misfortune of rich businesses in a western world. Data breaches impact everyday people across the globe. The rapid demonetisation in India in 2016 threw vast numbers of the population into smartphone ownership, if only so that they could pay for everyday items. But who's educated the nation on internet and mobile safety?

Similarly, Africa's adoption of technology has meant that they've leap frogged the home PC trend and jumped straight to mobiles. With these sudden adoption rates and little education from governments, banks or other service providers on how to protect themselves online it's hardly surprising to find that, in a worldwide population of 7 billion people, 2.2 billion records were stolen in 2017 alone.

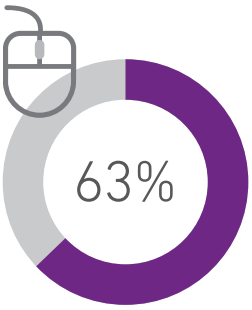
The impact of a breach on a business and on individuals

The ripple effect of a data breach is far reaching, impacting not only the organisations and staff within but also people on an individual level. Falling victim to identity fraud not only threatens to tarnish their name, ruin their credit but can also compromise their financial and medical history as well as drain their assets. Once the damage has been done the path back to restoring what was theirs is both time-consuming and expensive.

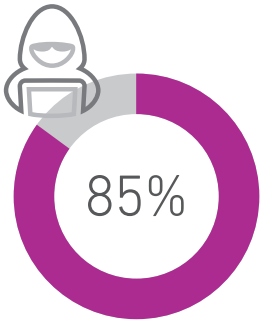
Special Eurobarometer 423 Cyber Security Report[16]



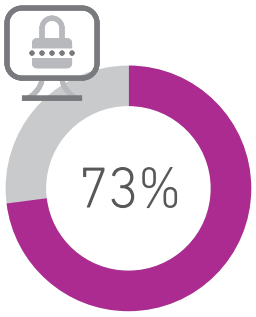
Two out of three internet users in the EU are concerned about experiencing identity theft



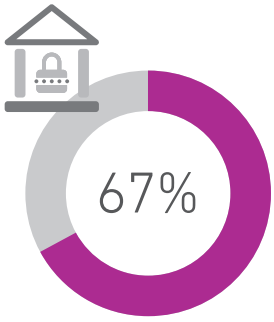
63% are concerned about being the victim of bank card or online banking fraud



85% agree that the risk of becoming a victim of cybercrime is increasing



73% agree that they are concerned that their online personal information is not kept secure by websites



67% agree that they are concerned that their online personal information is not kept secureby public authorities

New regulations will help to ensure organisations take responsibility for data breaches, but their responses will need to cover more than just the payment of a hefty fine. The Ponemon Institute highlights that CISOs are all too well aware of the negative consequences a data breach can have beyond the financial and data loss with 54% concerned about the loss of relationships with third parties and business partners as well as 40% concerned about the loss of customers.

[16] https://data.europa.eu/euodp/data/dataset/S2019_82_2_423_ENG

Significant numbers over the last decade

As the statistics below show, 10 years ago a data breach was rare however, the numbers have risen exponentially over the last two years. Here are just some of the examples:

[17] https://www.opus.com/resource/2018-ciso-survey-ponemon-institute/
[18] https://www.telegraph.co.uk/technology/2016/05/31/myspace-hack-millions-of-passwords-and-email-addresses-up-for-sa/
[19] https://www.express.co.uk/news/uk/674464/linkedin-hack-password-email-stolen-dark-net-gangs-164-million
[20] https://www.bullguard.com/blog/2013/11/adobe-hack-153-million-accounts-breached-not-38-million-as-previously-stated.html
[21] https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html
[22] https://www.bbc.co.uk/news/business-34743185
[23] https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m
[24] https://www.independent.co.uk/news/business/news/sports-direct-cyber-attack-compromise-30000-employees-data-workers-fail-telling-a7569766.html
[25] https://www.cybersecurity-insiders.com/cyber-attack-on-wonga-database-affects-250000-customer-bank-details/
[26] https://www.theregister.co.uk/2017/02/06/polish_banks_hit_by_malware_sent_through_hacked_financial_regulator/
[27] https://uk.reuters.com/article/us-spain-cyber/telefonica-other-spanish-firms-hit-in-ransomware-attack-idUKKBN1881TJ
[28] https://gdprcamp.co.uk/equifax-data-breach-14-million-uk-names-and-dates-of-birth-stolen
[29] https://www.thesun.co.uk/tech/6289670/facebook-data-leak-personal-information-users/

What's around the corner?

THE CYBERCRIMINAL

One thing regulators, law enforcement, businesses and security specialists all accept: The cybercriminal is smart and determined. According to online payments firm, Jumio, cybercriminals are:

Rarely operating alone, cybercriminals have grouped together in syndicates to share resources and skills. Security firm, Kaspersky[30], uncovered a gang that had stolen an estimated $1billion from over 100 banks during 2016 and found that the criminals were from Russia, the Ukraine, China and Europe. All were equipped with sophisticated spying software that was used to observe and mimic the behaviour of bank staff, enabling them to deposit cash into accounts they had set up.

These individuals and groups will continue to find a way of carrying out a data breach and, with new events or developments in technology and commerce, so too come new ways to wreak havoc on businesses across the globe.

> "The biggest danger facing enterprises in 2018 is organised threat actors. 2017 showed us that businesses are facing criminal organisations, hackers backed by competitors and even nation states... We've long suspected this would be the case, but it's becoming increasingly clear that the level of sophistication and tenacity shown by these attackers is far beyond the opportunistic hacking many enterprises are currently prepared to defend against.
>
> Because attribution is so hard and proving who the attackers are is nearly impossible for most organisations, the hacks will be more brazen as the year goes by."
>
> – **Jay Coley**, senior director of security services for Akamai

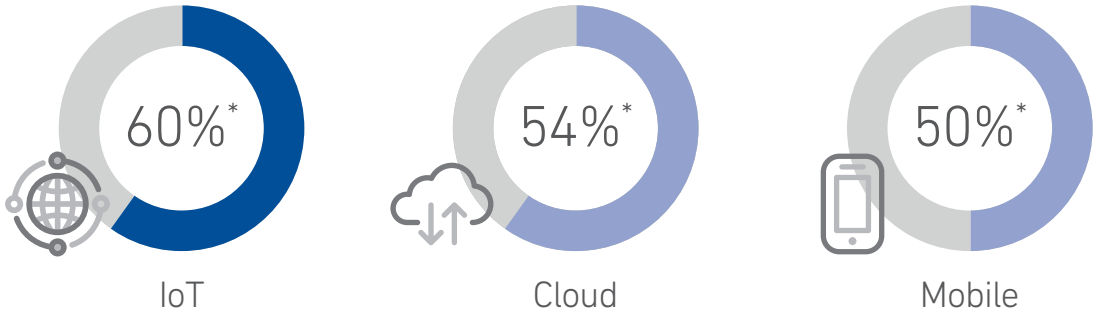
[30] https://www.telegraph.co.uk/business/sme-home/cyber-criminal/

Internet of Things

Mark Nunnikhoven, from Trend Micro, has predicted that attacks on the Internet of Things will continue to hit industries including airlines, manufacturing and cars because they rely so much on smart technology.[31]

Disruptive technologies considered the most challenging to secure

* of CISO respondents – The Ponemon Institute



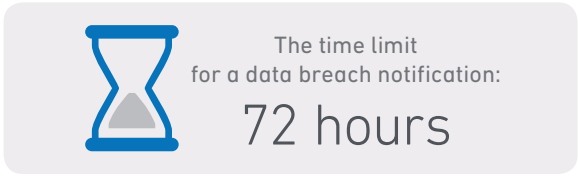
> "They face the same cybersecurity challenges that our laptops and our phones do, but they're attached to real things in the real world.
>
> If someone hacks my laptop, my data is at risk. But if someone hacks a robotic manufacturing arm, that entire manufacturing line is at risk."
>
> **– Mark Nunnikhoven**, Vice President, Cloud Research, Trend Micro

[31] http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

GDPR

The European Union's General Data Protection Act (GDPR) from May 25th onwards carries a non-compliance penalty that is 4% of a company's global revenues, or €20 million, whichever is the greater. While many businesses are scrambling to comply, it was reported in March this year that 94% of companies weren't ready for GDPR.[32]

The time limit for a data breach notification is now 72 hours. Most companies know very little at this stage, but the penalties are so significant that the dialogue (with the ICO) is forced much earlier than has previously occurred.



Despite being an EU directive, GDPR applies not only to businesses that reside within the EU but also to any organisation providing a product or service to residents of the EU.

Artificial Intelligence

Artificial Intelligence (AI) has also hit the headlines over the last year or so. While that discussion has so far focused on whether machines will replace humans in certain industries several security experts have also voiced their concerns on whether AI tools will be used by cybercriminals too.

If legitimate organisations are using AI to test their infrastructure, carry out penetration tests and other tasks within the business then it's a sure thing that cybercriminals will also be embracing it too. AI will enable them to identify the most vulnerable places to attack as quickly as possible.

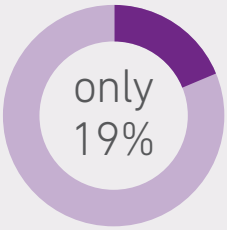
> "... We are very worried about the stage when there is widespread access and adoption of AI-enabled malware and toolkits for attackers to use. That is because by and large, applications of AI unlock decision-making, and that is what human-driven attacks do.
>
> You have an attacker in a network, on a keyboard, and they can case the joint. They can see what the weak points are. They can adapt the attack path they follow to the particular environment they find themselves in, that's why they're hard to detect."
>
> – **Andrew Tsonchev**, director of cyber analysis at Darktrace

[32] https://www.smartinsights.com/email-marketing/email-communications-strategy/is-your-company-gdpr-ready/

Cashless Society (Bitcoin)

While the uptake of electronic money is expected to increase and become mainstream, G4S recently reported that physical money now accounts for 9.6% of global gross domestic product (up from 8.1% in 2011). Some countries are making more progress towards a cashless economy than others. As cited in a recent Financial Times article, only 19% of payments are made using cash in Sweden compared to a European average of nearly 80%.[33]

> "If you extrapolate current trends the last note will have been handed back to the Riksbank by 2030."
>
> – **Cecilia Skingsley**, deputy governor, The Riksbank, Sweden's central bank



of payments are made using cash in Sweden

And Sweden isn't the only country reducing its reliance on cash. India announced its demonetisation in late November 2016 (of the 500 and 1,000 Rupee notes), South Korea's central bank will phase out coins by 2020, and the UK Government is looking into whether 1p and 2p coins as well as £50 notes are efficient or cost effective any more.

The march of the cashless society brings with it other challenges though. A few years ago, Mastercard worked with the Nigerian government to launch an identity card with a payment facility, but the Civil Rights Congress protested (citing "stamped ownership of a Nigerian by an American company"), and only 1.5 million cards have been issued with reports that a further 28.5 million applications are stuck in the system.

Progress of the cashless economy will vary from country to country but whether it be e-wallets or the innovative bitcoin and other cryptocurrencies, businesses and individuals alike are going to be at risk of cybercrime. Former head of Interpol and now head of campaign group Kontantupproret (Cash Rebellion) Bjorn Eriksson, highlighted the dangers of ditching cash in a recent Financial Times interview:

> "If we move to a wholly cashless society... and something disturbs this digitalised system, what happens?[34]"
>
> – **Bjorn Eriksson**, former head of Interpol and Kontantupproret

Disruption can be caused by a number of events, power cuts, malfunctioning cash machines or mistakes on the banks' IT systems, such as the recent UK TSB bank outage.[35] The financial sector will continue to be cautious and while there is more data thanks to the electronic payment trail, a bit like AI, if the legitimate organisations are doing it, so too will the cybercriminals.

[33] https://www.ft.com/content/9fc55dda-5316-11e8-b24e-cad6aa67e23e
[34] https://www.ft.com/content/9fc55dda-5316-11e8-b24e-cad6aa67e23e
[35] https://www.independent.co.uk/news/business/news/tsb-it-failure-latest-fraud-attempts-thousands-online-banking-paul-pester-a8386271.html

Phishing

Phishing attacks continue to hit organisations, and as cybercriminals become more sophisticated the harder it is to spot the scam email. The long-held tradition of spelling mistakes and grammatical errors are (almost) a thing of the past. In 2016, a Snapchat employee shared information on 700 colleagues believing the request for payroll data to be a legitimate request from the company's CEO.[36] Similarly, a Canadian university was tricked into sending almost $12 million to a cybercriminal posing as a trusted construction partner.[37]

CISOs also believe it's highly likely they'll experience credential theft due to a careless employee falling for a phishing scam – a 65% chance – even more likely than a malware attack, a data breach or a cyber-attack.

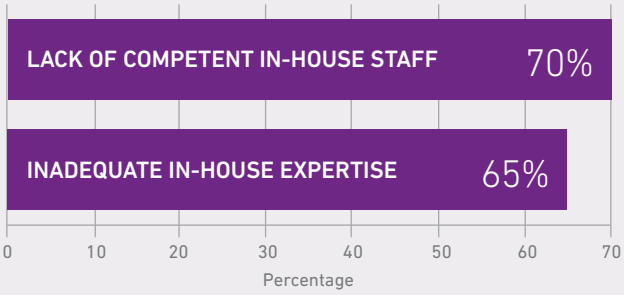
– The Ponemon Institute

[36] https://www.theverge.com/2016/2/29/11132988/snapchat-employee-data-breach-payroll-phishing
[37] https://globalnews.ca/news/3713350/clark-builders-identified-as-company-involved-in-11-8m-macewan-university-phishing-scam/

Conclusion

Legislation will change how organisations combat data breaches on a global scale yet, as businesses and governments continue to get smarter on how to protect their interests, so too do the cybercriminals. And while advances in technology and currencies will continue, one risk will always remain the same - the ever-present human factor.

Top security threat*

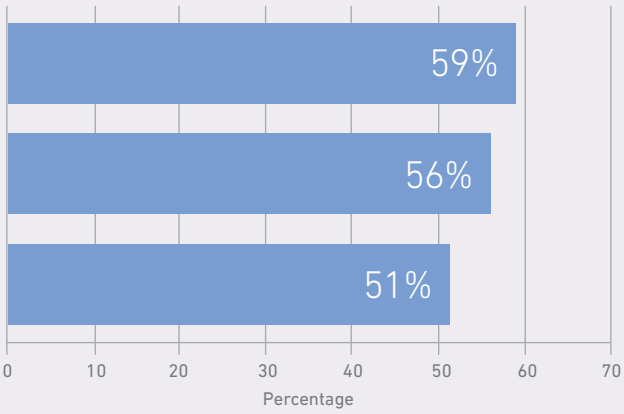


70% of CISOs calling "lack of competent in-house staff" their number one concern

65% of CISOs stating "inadequate in-house expertise" as the top reason they are likely to have a data breach

The human factor
is the top security threat

Other key factors seen as likely reasons for a data breach*



THE INABILITY TO PROTECT SENSITIVE AND CONFIDENTIAL DATA FROM UNAUTHORIZED ACCESS

THE INABILITY TO KEEP UP WITH THE STEALTH OF THE ATTACKERS

FAILURE TO CONTROL THIRD PARTIES' USE OF SENSITIVE DATA

* The Ponemon Institute

Innocent mistakes from leaving data on a laptop on the train to reacting to a CEO or Chief Financial Officer's (CFO) request for company-critical data when in fact it's a phishing email will always occur. The faults range from the naive to the malicious – a disgruntled employee, in the case of Morrison's supermarket where 100,000 employees' payroll data[38] including names, addresses, dates of birth, national insurance numbers and bank details were posted online.

Data breaches are not only a security crisis but a financial disaster for most businesses. They need to respond at speed and bring a broad mix of experts ranging from legal and communications as well as security experts to help fix the problem.

[38] https://www.personneltoday.com/hr/morrisons-data-breach-sounds-warning-on-vicarious-liability/

> "The number of high-profile international breaches has been a wake-up call this year (2017) to businesses that security is a top-level item. It affects the bottom line."
>
> **– Mark Nunnikhoven,** Vice President, Cloud Research, Trend Micro

After the shockwaves of 2017 the introduction of not only the EU's GDPR but also Australia's Privacy Amendment (Notifiable Data Breaches) Act 2016[39], this year governments and businesses, so far, seem to be finally taking the threat of cybercrime seriously. Advances in technology such as smart ID, tokens and biometrics will certainly help, but the fight with cybercrime will never cease.

Regulations enforced will help to encourage companies to be proactive in protecting not only their business interests and employees but that of their customers too.

HOW EXPERIAN CAN HELP YOUR ORGANISATION

CyberAgent

Experian's end-to-end identity theft protection solution, CyberAgent®, minimises the risk of identity theft, through preemptive early warning alerts and identity restoration services

CyberAgent is a proprietary technology that proactively detects stolen personal data and compromised confidential data online. The CyberAgent database currently holds 3.2 billion records of stolen personal data with up to 100 million new records added every month due to the sheer scale of data breaches taking place.

CyberAgent is the leading identity monitoring solution designed for proactive cyber detection on an international level - breaking language barriers and detecting identity theft across the globe. And at any point in time, our CyberAgent technology is monitoring thousands of websites and millions of data points, alerting consumers if we find their personal information in a compromised position online. This information is being gathered in real-time, giving consumers both the opportunity to react quickly and to take the necessary steps to protect themselves.

[39] http://www.mondaq.com/australia/x/709952/data+protection/Data+Breaches+Exposing+Businesses+to+New+Litigation+Risks

Denmark
Lyngbyvej 2
2100 Copenhagen
www.experian.dk

France
Tour PB5
1 avenue du Général de Gaulle
La Défense 8
92074 Paris La Défense Cedex
www.experian.fr

Germany
Speditionstraße, 1
40221 Düsseldorf
www.experian.de

Italy
Piazza dell'Indipendenza, 11/b
00185 Roma
www.experian.it

Netherlands
Grote Marktstraat 49
2511 BH, Den Haag
Postbus 13128, 2501 EC, Den Haag
www.experian.nl

Norway
Karenlyst Allè 8B, 0278 Oslo
Postboks 5275, Majorstuen
0303 Oslo
www.experian.no

Russia
5, bldg. 19, Nizhny Susalny lane
105064 Moscow
www.experian.ru.com

South Africa
Ballyoaks Office park
35 Ballyclare Drive
2191 Bryanston, Sandton
www.experian.co.za

Spain
Calle Príncipe de Vergara, 132
28002 Madrid
www.experian.es

Turkey
River Plaza
Buyukdere Cad. Bahar Sok.
No: 13 Kat: 8 Levent
34394 Istanbul
www.experian.com.tr

United Arab Emirates
Dubai Islamic Bank Building 01
Office 102, First Floor
Dubai Internet City
www.experian.ae