



Today's talk...

1. Refresher on the General Data Protection Regulation, aka GDPR
2. GDPR, so what 'I'm an American'?
3. Ticketmaster UK breach and more 'so what'?
4. Here comes the GOV!
5. Impact of the GDPR to states' legislation
6. Q&A



Why is a marketing guy doing an InfoSec presentation?

- I'm an InfoSec techie, researcher, copywriter
- We are business journalists who tell software stories.
 - We are software justifiers
 - 90% of client base is rooted in InfoSec
 - Serving s/w vendors on Win/UNIX, Mainframe systems
 - Started out in 2011 after 18 years helping ISVs battle enterprise s/w giants
- We provide Marketing as a Service
 - Long form/short form content
 - Social media
 - Graphic design online/offline
 - Sales & marketing strategies for long sales cycles into the Fortune 1000 in Banking, Finance, HC, Gov
- Also Marketing Automation solution vendor [[SharpSpring](#)]



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perrimarketing

The GDPR is here!

To refresh:

- GDPR = General Data Protection Regulation
- Originated in European Union
- Protects PII of European citizens NO MATTER WHERE THEY RESIDE
- The GDPR's coverage is ubiquitous – a picture on Facebook can be considered PII
 - Can you monitor all the PII in your network?
 - You must remove it if requested...all of it! And quickly. And then prove you did it.
- Fines can reach 4% of annual global revenue for habitual offenders
- 72-hour time to report breach mandate
 - Ave. Time to Discover in 2017 was 197 days
- There is a clause for 3rd Party data that might kill data brokering altogether
 - You must have greater transparency than ever before



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perrimarketing

THE GDPR is here – the 72-hour precedent!

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with [Article 55](#), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

GDPR FINES ARE 2-4% GROSS REVENUE, OR €20 MILLION, WHICHEVER IS HIGHEST!

And, the GDPR is also here!

1. Alabama
2. Arizona
3. Colorado
4. Iowa
5. Louisiana
6. Nebraska
7. Oregon
8. South Carolina
9. South Dakota
10. Vermont
11. Virginia



Yeah, but we have plenty of security in place.

- 90% of the participants state that the protection of information and data is the most important driver for information security¹
- 90% indicate an increase of their security expenses in the next fiscal year¹
- 70% of the respondents state customer data as the most critical asset¹



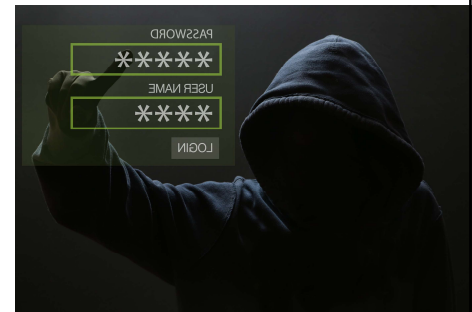
¹Information Security Benchmarking 2017 Survey Report, Cap Gemini

CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perrimarketing

Yeah, but we have plenty of security in place.

- #1 worry for CISOs in 2018 will be employee negligence²
 - 70% said they had "lack of competent in-house staff"
- 65% stating "inadequate in-house expertise" as the top reason they are likely to have a data breach²
- Most challenging threat vectors are²
 - IoT
 - Mobile
 - Cloud



² Ponemon "What CISOs Worry About in 2018" eBook

CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perrimarketing

And....today's CISO is under enormous pressure.

- 69% anticipate their roles will be even more stressful in 2018
- 63% expect information security budgets to decline or remain flat
- 45% even fear job loss in the event of a data breach.

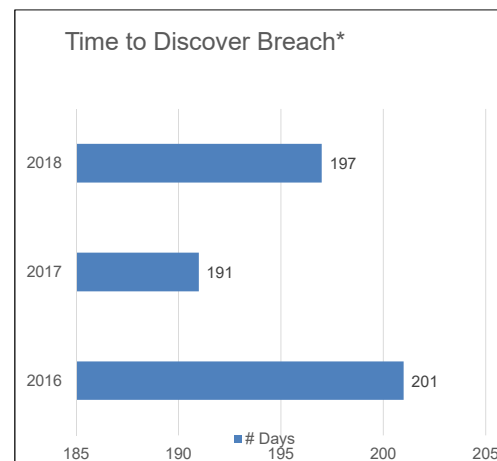
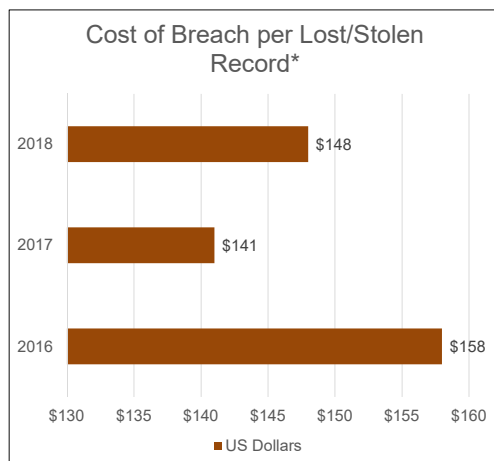


2 Ponemon "What CISOs Worry About in 2018" eBook

CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perri marketing

And, our security sucks.



*IBM/Ponemon Breach reports | Verizon Data Breach Investigation Reports

CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perri marketing

Time to discover is a friend of the devil in the U.S.



CYBER SECURITY //ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perri marketing

WHAT TICKETMASTER UK BREACH MEANS FOR THE U.S.

CYBER SECURITY //ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

pmi
Peri Marketing Incorporated

Ticketmaster UK: Pre- and post-GDPR breach problem

- Ticketmaster UK reports 40k records compromised on June 23, 2018
- Ticketmaster UK did not discover breach.
 - Monzo bank reported it to TM on April 6 (according to Monzo)
- The GDPR went live on May 25, 2018
 - We have a pre- and post-GDPR breach
 - Fine could be £500,000 or £17,000,000!



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

Source: DarkReading.com

perri marketing

Pre- and post-GDPR breach problem

- Ticketmaster has admitted breach and affected customers could receive as much as £5,000 per each in compensation
 - If 40k records = £200 million!
- Ticketmaster took 78 days to discover breach, which is actually good considering the average...



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

Source: DarkReading.com

perri marketing

Other Ticketmaster UK takeaways

- Hack originated from a TM supplier
 - Ibenta Technologies' support product
- An alert was issued on Ticketmaster UK's website
 - North America not affected according to TM
- Magecart hacker group allegedly responsible
 - Also alleged to be responsible for British Airways attack Aug/Sept 2018
 - 380 BA customers affected, according to BA website
- After Monzo bank notified TM on 4/12, TM internal investigative team said there was no sign of breach no other banks reported an issue
 - TM unable to identify breach until 6/23
 - TM currently offering customers 12 months of free ID monitoring services



Yeah but so what? I'm an American.



Federal & State Govs' patience running out



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perrimarketing

11 State Govs have created PII laws in 2018

- States' with current breach laws: AL, AZ, CO, IA, LA, NE, OR, SC, SD, VT, VA
 - <https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/>
- Let's look at CA and NC...

Data Protection Report
Data protection legal insight at the speed of technology

Home » Compliance and risk management » US states pass data protection laws on the heels of the GDPR

US states pass data protection laws on the heels of the GDPR

By: [Andrew Kim Serrano \(US\)](#), [Chris Goodwin \(US\)](#), [Anne Redmon \(US\)](#), [Trenton Coughlin \(US\)](#) and [Katie Forrester \(US\)](#) on July 9, 2018
Posted in [Compliance and risk management](#), [Regulatory response](#)

Several U.S. states have recently introduced and passed legislation to expand data breach notification rules and to mirror some of the protections provided by Europe's newly enacted General Data Protection Regulation ("GDPR"). See our previous blog posts on GDPR [here](#) and [here](#). Like their European counterparts, these state laws are intended to provide consumers with greater transparency and control over their personal data. The California and Vermont laws, in particular, go beyond breach notification and require companies to make significant changes in their data processing operations. See our earlier post on the California Consumer Privacy Act ("CCPA") [here](#).

On the security front, as of March 2018, all 50 U.S. states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted breach notification laws that require businesses to notify consumers if their personal information is compromised. These new and amended state data breach laws expand the definition of personal information and specifically mandate that certain information security requirements are implemented. Below are the key takeaways from U.S. data protection laws that were passed in the last year.

About
More than a news source, the Data Protection Report provides thought leadership on emerging privacy, data protection and cybersecurity issues, and helps its readers proactively address risks and anticipate next steps in this crucial emerging field.
[Read more](#)

Stay connected
in [Twitter](#) [LinkedIn](#) [YouTube](#)
[Subscribe by email](#)

bn blog network

Topics
[Compliance and risk management](#)
[cybercrime](#)
[Data breach](#)
[Dispute resolution and litigation](#)
[General](#)

CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perrimarketing

California Consumer Privacy Act of 2018

- Goes into effect January 1, 2020
- Designed to give power back to the consumer (sound familiar?). Right to:
 - Know how you are categorized
 - Know has your data been sold
 - Request to stop
- Requires businesses to secure data with best practices
- Targets orgs that “sells PII of 100k or more consumers or devices”or
 - \$50 million annual revenueor
 - Gets 50% of revenue from selling PII



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perri marketing

California Consumer Privacy Act of 2018

- The Act can be enforced by the California Attorney General.
 - Businesses can be subject to civil damages up to \$7,500 per violation
 - Consumer can receive between \$100-\$750 per incident
 - Potential for penalties from other orgs (PCI DSS, etc.)
- Businesses do have some protection
 - Consumers will need to jump through a few hoops to file a claim
 - 30-day “cure period” to become compliant
 - If still non-compliant after, up to \$7,500 per violation



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perri marketing

'Act to strengthen ID theft protections' (N. Carolina)

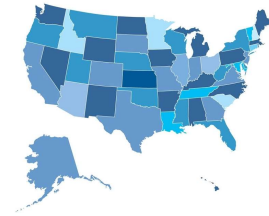
- Updates NC's Identity Theft Protection Act. (2005) which provides:
 - Provides "greater consumer control"
 - Allows for consumers to sue for civil damages
- AKA ASITP – Not currently a law but said to be one of the toughest PII laws yet, when passed. ASITP loosely defined at this time:
 - Sponsored by state representative Jason Saine
 - 15-day breach notification
 - Failure to protect consumers' PII could violate NC's Unfair & Deceptive Trade Practices Act.
 - Each person affected constitutes a separate violation
 - "Trebled Damages" – x3 of civil awards
- You've heard it before – "not if, but when"
 - Better yet, have visibility now to all data access!



GIVE YOURSELF A CYBER FIGHTING CHANCE

Prepare NOW for states' legislation.

- You will need to know how to navigate the statutes
 - What constitutes a violation
 - Financial damages
 - Supervisory board or authority
 - Right to be forgotten
 - Consent and consumers' rights – they are going to have the power!
 - Privacy by design - the inclusion of data protection from the onset of the designing of systems, rather than an addition
 - You will be required to be proactive
 - Better communication: a liaison between business and IT side of your enterprise
 - Review and understand your cyber insurance coverage
 - GET YOUR LEGAL TEAM INVOLVED NOW.



Biz vs. IT – Understand the tipping scale towards Biz

- The CEO and CMO are becoming the keepers of BIG DATA
 - The Business vs. IT communications gap
- The CMO is also taking budget away from IT to manage Big Data
- The CMO is also quickly becoming the main purchaser in large orgs of software solutions that run the business
 - CRM
 - Marketing Automation
 - Data subscription services
 - Intent insight software for sales & marketing
- Are your CEO, CIO, CISO and CMO communicating about data security compliance?



Data laws and standards all have 1 common denominator.

- PII laws and data standards are here to protect consumers' PII
- Generally data laws and standards (GDPR, PCI DSS, HIPAA, FISMA, GLBA, other) are essentially the same:
 - Know what datasets you have that apply to the law/standard
 - A picture can constitute PII as far as the GDPR is concerned
 - Have visibility to all accesses, most importantly privileged users
 - Secure the data, or there will be consequences
 - There is a timeframe that should alarm you
 - Consumers have the power in the EU (and now here)
 - They can request what data you have on them
 - They can request you remove them
 - They can lodge a complaint and get the penalty process rolling
 - Visibility and real-time alerting is key



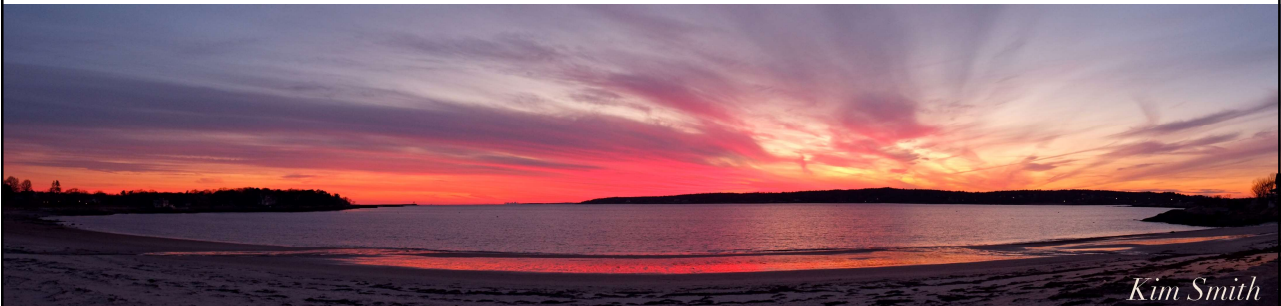
CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perrimarketing

And a silver lining...

- From a Gartner Forecast this past August
 - Worldwide spending on information security products and services will increase 12.4 percent in 2018
 - Reaching more than \$114 billion
 - In 2019, the market is forecast to grow 8.7 percent to \$124 billion.

Gartner®



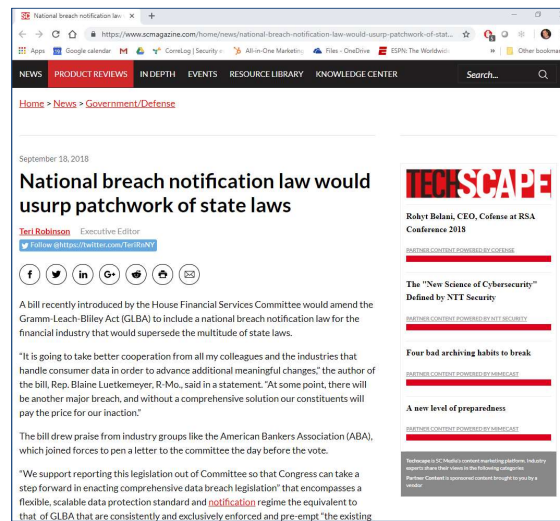
Kim Smith

CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

<https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

perrimarketing

And, just to muck up the waters even further...



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perri marketing

Our latest whitepaper recapping this presentation



CYBER SECURITY // ATLANTA
17-18 OCTOBER 2018, GEORGIA WORLD CONGRESS CENTER

perri marketing




THANK YOU!

Please visit our website for more information on how we are helping clients sell software and bringing greater awareness for InfoSec.

 **Address**
Gig City, Tennessee

 **Contact Info**
Email: moreinfo@perrimarketing.com
<https://perrimarketing.com>

 **Telephone**
Phone: +1 (423) 212-3127, ext. 1
Mobile: Just ask

