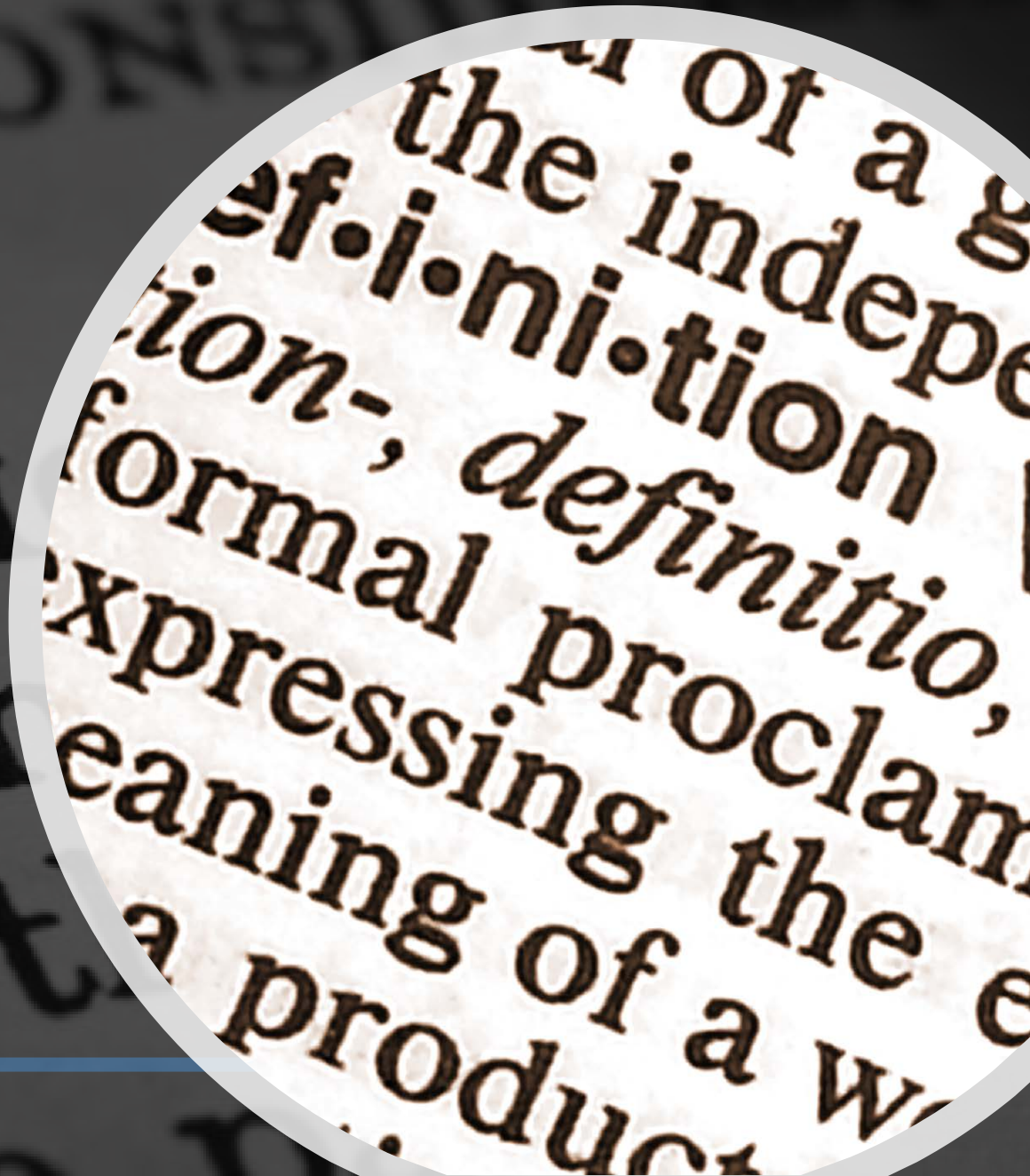
Security, Compliance and Data Privacy

GDPR and More!

Craig S. Mullins
Mullins Consulting, Inc.
http://www.craigsmullins.com

Defining Terms

- Security
  - Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption.
- Compliance
  - The term compliance describes the ability to act according to an order, set of rules or request. In this case, compliance with industry and governmental regulations.
- Data Privacy
  - Data privacy (*or data protection*) is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.



You can have security without data privacy

You cannot have data privacy without security

Security Measures

At a high-level, there are three (3) types of Security controls:

- **Preventative** - prevent an incident from occurring such as by locking out unauthorized intruders
- **Detective** - identify an incident in progress such as by sounding an alarm and sending an alert
- **Corrective** - limit the extent of damage caused by an incident such as by quickly and effectively recovering the organization to normal working status

Security Trends

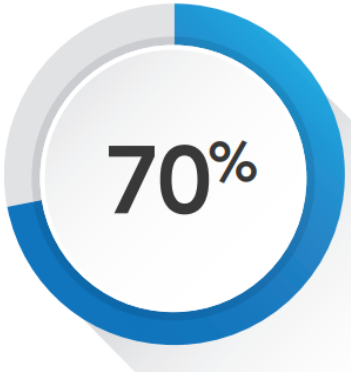
Security is Top IT Initiative for 2018

Source: 2018 State of Resilience Report, Syncsort & Vision Solutions

Confidence is Increasing for Data Protection

Source: 2018 Cyberthreat Defense Report, Cyber Edge Group

Fast can be the enemy of secure



of app developers admitted that business pressures to release app updates quickly often override security concerns

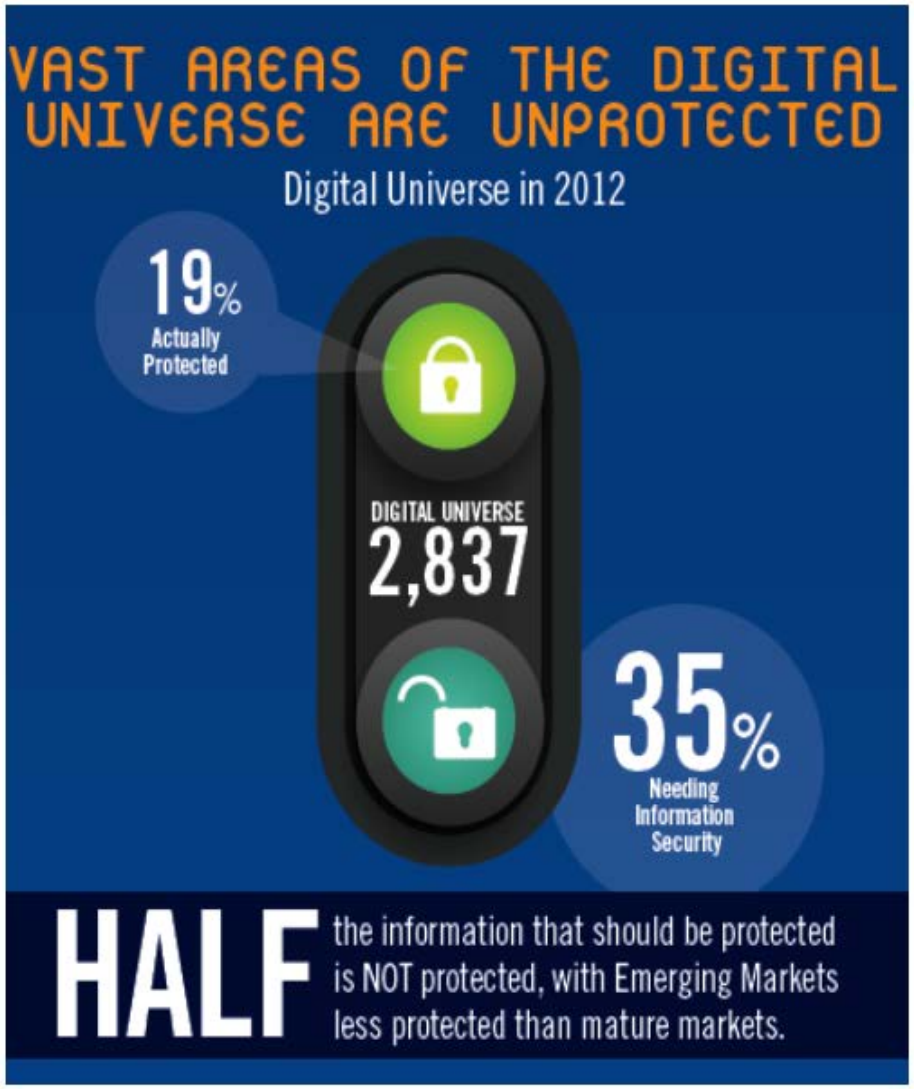
Source: The Impact of Security on Development: 2015 Survey Report

ONLY 24% of organizations have cutting edge or have mature application security in place

Source: 2017 Cybersecurity Trends Spotlight Report

Another Reality Check

- IDC projects that the digital universe will reach 40 ZB by 2020
  - And IDC further states that the digital universe will increase 50-fold between 2010 to 2020
- The amount of data that requires protection is growing faster than the digital universe itself
- Only half of the information that should be protected is actually protected…



Source: IDC Digital Universe Study, sponsored by EMC

Data Breaches

Data Breaches: Still a Significant Threat to Data

- Privacy Rights Clearinghouse

http://www.privacyrights.org/data-breaches

- Since Feb 2005:
  - There have been 8,209 data breaches impacting **over 10.5 billion total records** containing sensitive personal information were exposed due to data security breaches*
  - That averages out to about 12 data breaches per week
    - Starting with ChoicePoint: (Feb 15, 2005) – data on 165,000 customers breached

* As of June 25, 2018, reported by Privacy Rights Clearinghouse

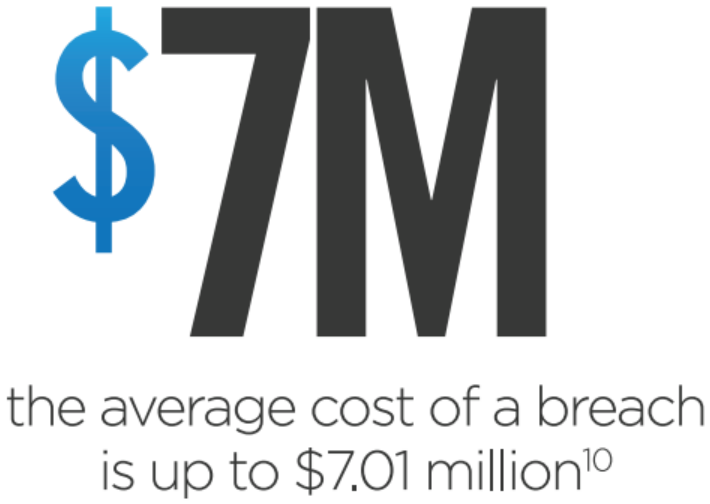
Data Breaches:
A Recent Example

- 2 terabytes of data Including personal information on hundreds of millions of American adults, and millions of businesses.
  - Phone numbers
  - Home addresses
  - Email addresses
  - Information on children
  - Etc.

ANDY GREENBERG SECURITY 06.27.18 01:34 PM

MARKETING FIRM EXACTIS LEAKED A PERSONAL INFO DATABASE WITH 340 MILLION RECORDS

The Average Cost of a Data Breach



Factors that increase the cost of a breach

- Increase in lost business due to abnormal churn of existing customers
- Increase in the cost to acquire new customers
- Increase in the cost in the average size of a breach

Regulatory Fines and Legal Judgments . . . Legal Defense Costs . . . Customer Notifications . . . Credit Monitoring . . . Forensic Analysis . . . Reputational Losses

Source: Ponemon Institute 2016 Cost of a Data Breach Study: United States

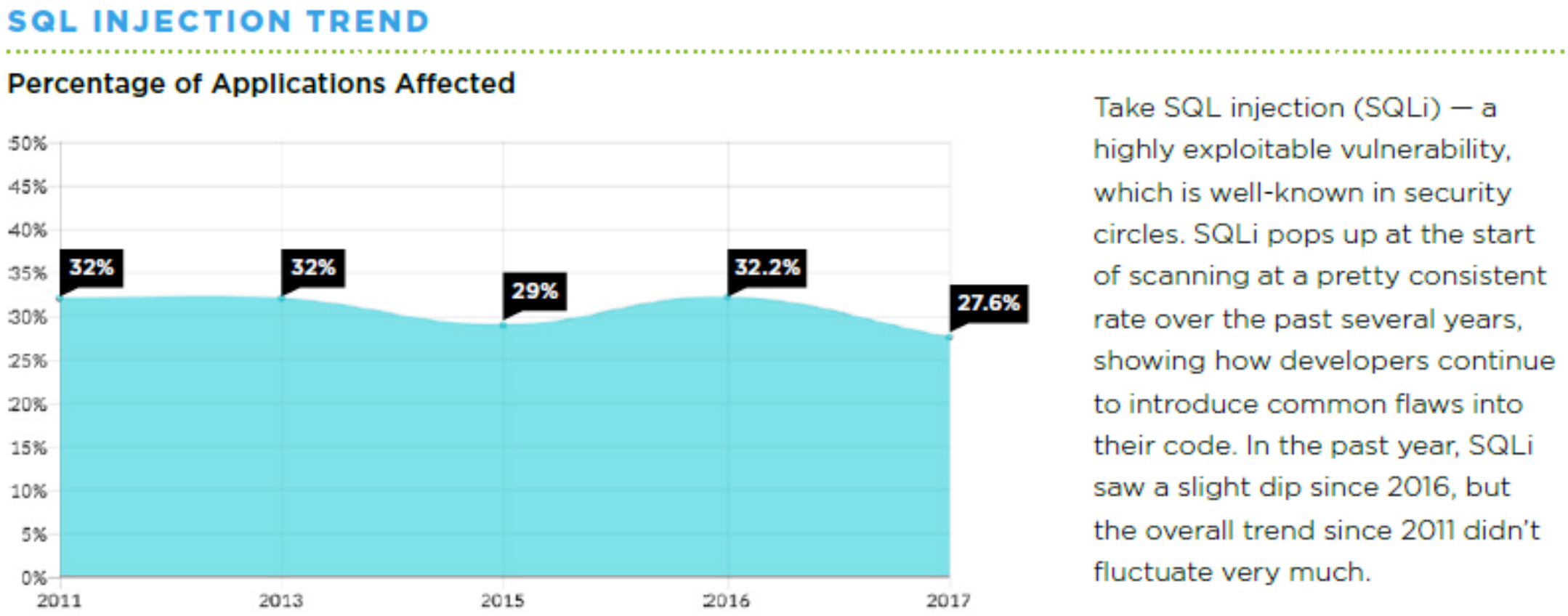
$141/record

Source: Ponemon Institute 2017 Cost of a Data Breach Study

Use the Data Breach Loss Calculator *on IBM Bluemix*

https://databreachcalculator.mybluemix.net/

SQL Injection Still a Big Problem

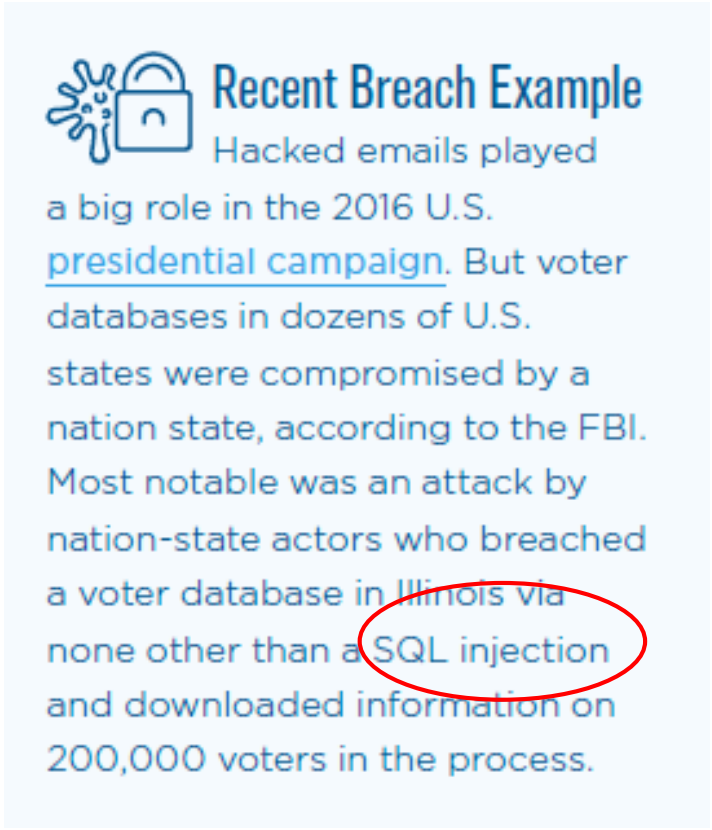


Source: State of Software Security 2017 Report

https://tinyurl.com/DBACORNER-sqlinj

SQL Injection Example

- SQL injection attacks are one of the most severe types of attacks on data
- These type of attacks exploit vulnerabilities allowing the hacker to gain unauthorized access to your databases using maliciously crafted input.
- 2016 US presidential campaign
  - impacted 200K voter records



Source: State of Software Security 2017 Report

Regulatory Compliance

What is Regulatory Compliance?

Regulatory compliance has to do with a set of guidelines that an organization is required to follow in accordance with the law. A compliance definition in hiring practices, advertising, accounting, benefits, workplace environment and safety, discipline, and termination comes largely from departments in the U.S. executive branch. Those who wish to ensure regulatory compliance for a business should investigate all relevant rules for the industry and follow each law to the letter.

- Industry
- Governmental
- *Internal*

What is Driving Increased Regulation?

- Data breaches continue to occur… and make headlines
- More data than ever being gathered for Big Data analytics projects
- Other regulations that mandate data retention
- Ever-increasing technological capabilities and slow-moving remediation of known issues

Legislation & Compliance (Examples)

- The Sarbanes-Oxley Act (SOX) established standards for all U.S. public company boards, management, and public accounting firms. The Public Company Accounting Oversight Board (PCAOB) was created by SOX to oversee auditors of public companies. The primary goals of SOX were to strengthen and restore public confidence in corporate accountability and to improve executive responsibility.

Section 404

- HIPAA (Health Insurance Portability and Accountability Act) creates national standards to protect individuals' medical records & personal health information. The Privacy Rule provides that, in general, a covered entity may not use or disclose an individual's healthcare information without permission except for treatment, payment, or healthcare operations.

- PCI DSS (Payment Card Industry Data Security Standard) includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Legislation & Compliance (Examples)

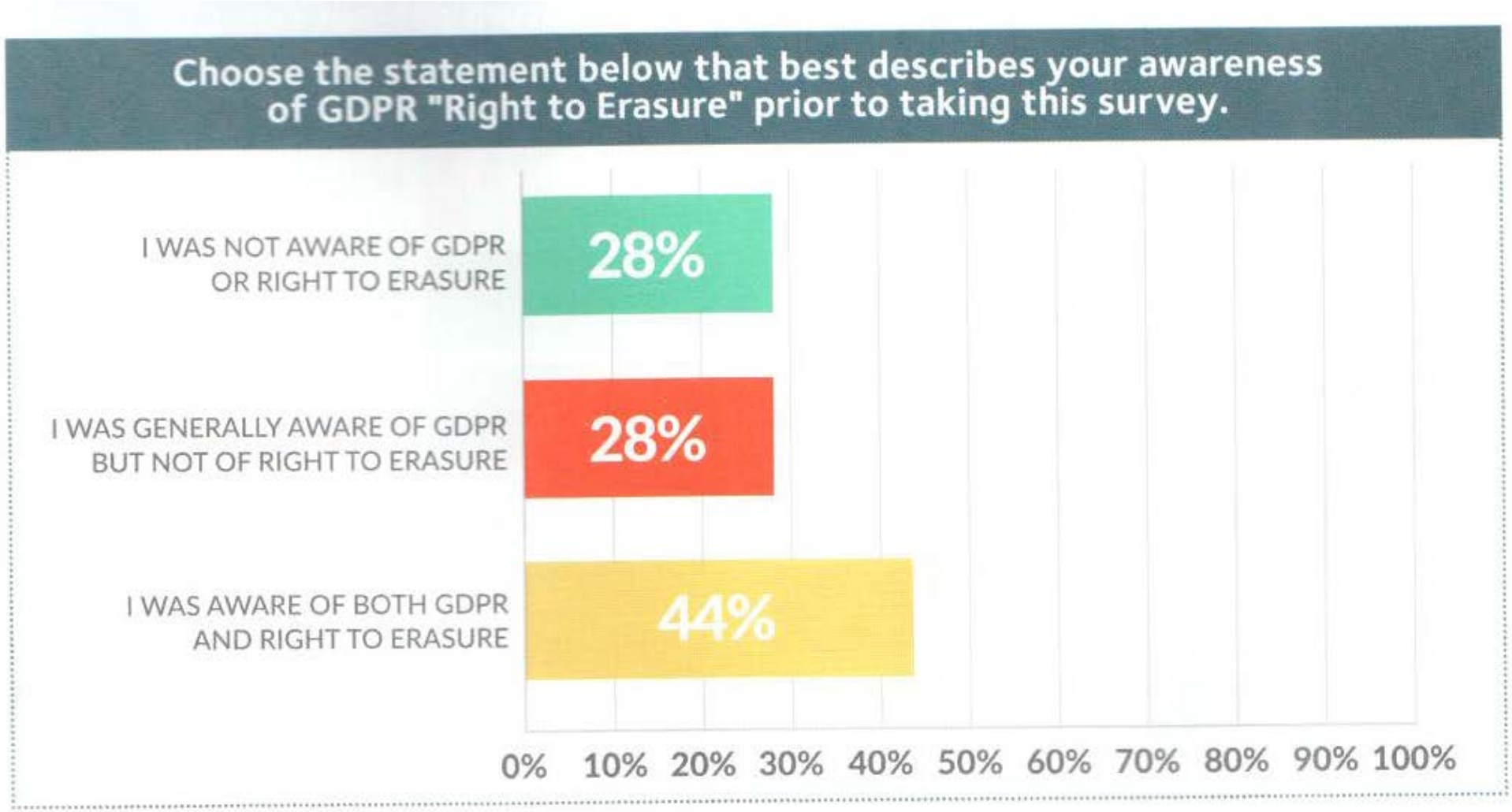
- The Gramm-Leach-Bliley Act (GLB), is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. The Act regulates the collection and disclosure of private financial information; stipulates safeguards requiring security programs; and prohibits the practice of pretexting.
- Basel II is an international banking regulation the goal of which is to produce uniformity in the way banks and banking regulators approach risk management across national borders.
- The Fair and Accurate Credit Transactions Act (FACTA), requires all federally regulated financial institutions and creditors to develop and deploy an Identity Theft Prevention Program for combating ID theft on new and existing accounts. This is also known as the "Red Flag" rules.
- The California Security Breach Notification Law (CA SB 1386) requires companies to notify California customers if PII maintained in computerized data files have been compromised by unauthorized access.

Regulatory Compliance is International

Country	Examples of Regulations
Australia	Commonwealth Government's Information Exchange Steering Committee, Evidence Act 1995, more than 80 acts governing retention requirements
Brazil	Electronic Government Programme, EU GMP Directive 1/356/EEC-9
Canada	Bill 198, Competition Act,
France	Model Requirements for the Management of Electronic Records, EU Directive 95/46/EC
Germany	Federal Data Protection Act, Model Requirements for the Management of Electronic Records, EU Directive 95/46/EC
Japan	Personal Data Protection Bill, J-SOX
Switzerland	Swiss Code of Obligations articles 957 and 962
United Kingdom	Data Protection Act, Civil Evidence Act 1995, Police and Criminal Evidence Act 1984, Employment Practices Data Protection Code, Combined Code on Corporate Governance 2003

Which Brings us to…

But Isn’t it Too Late?



Source: Melissa Data Magazine, Summer 2018

GDPR is a Different Kind of Regulation

Most industry and governmental security regulations and standards such as HIPAA (Healthcare data), PCI DSS (credit card data), FISMA (U.S. Government data), and GLBA (banking/finance data) focus on the data broadly

The focus of GDPR is on the data for a group of citizens in a **defined geography** – the European Union.

GDPR refers to EU citizens as “data subjects”

- Protected not just while in EU (e.g. on vacation or holiday)

GDPR applies to any EU resident 16 years of age or older

- There is a provision for member states, if they choose, to lower the age to 13

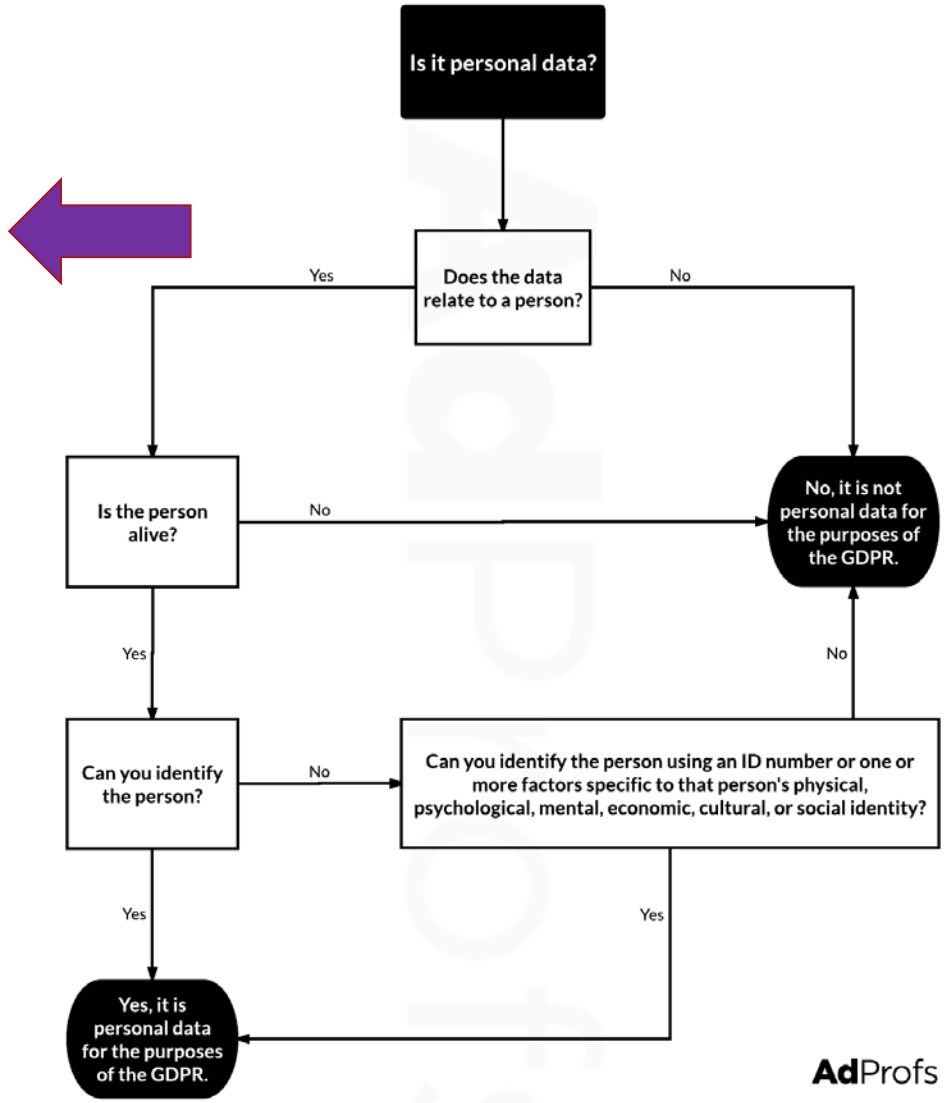
Any personal data of protected “data subjects” that you keep must have the *active* consent of the data owner

Your Organization Likely Must Comply

- Although it sounds like it applies to only the EU, this is not the case
- Answering these three questions can help determine whether your company is impacted by the GDPR:
  - Does my company offer goods or services to EU residents?
  - Does my company monitor the behavior of EU residents?
  - Does my company have employees in the EU?
- If you do business with any EU citizen, GDPR applies to you!

Q: What Does GDPR Regulate?
A: Use of PII

- GDPR regulates the collection and usage of personal data of a data subject.[1]
- Personal data (or PII) includes:
  - Name
  - Photo
  - Email address
  - Bank details
  - Social media posts
  - Medical information
  - Computer data (including location data, IP address, cookie data, and RFID tags)
- It also comprises subsegments of information, such as sensitive personal data
  - That is, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, etc.



Source: AdProfs, http://adprofs.co/beginners-guide-to-gdpr/

[1] GDPR does not apply to deceased persons or to non-natural persons (e.g., corporations).

GDPR and PII

Under GDPR, companies may not legally process the personally identifiable information of any EU citizen (data subject) without meeting at least one of six conditions.

1. Express consent of the data subject.
2. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
3. Processing is necessary for compliance with a legal obligation.
4. Processing is necessary to protect the vital interests of a data subject or another person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

The right to be forgotten

- Article 17 of the GDPR provides for the right to erasure, commonly known as the "right to be forgotten."
- This means that people can require that companies erase their personal data in a number of situations, including when the information is no longer necessary in relation to the purpose for which it was originally collected.

You will need to establish mechanisms to allow for data subjects to request the erasure of their data.

And you will need to establish operational controls to ensure that these requests are reviewed and acted upon in a timely manner.

The Right to be Forgotten:

Do You Know Where all of your Data Is?

Excel spreadsheets

Unload Files

Backups

Flat Files

Database Tables

Reports

Indexes

ETL Feeds

USB

GDPR Action Items: Data Privacy Officers

- If your organization engages in regular, systematic collection or storage of sensitive customer data you need to hire a Data Protection Officer (DPO).
- GDPR requires a DPO to be “designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices”
- Tasks of the DPO:
  - Regulatory compliance
  - Training staff on proper data handling
  - Coordinating with the supervisory authority
  - Ability to understand and balance data processing risks
- IAAP estimates that there will be a need for at least 28,000 Data Protection Officers globally.

Source: https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/

GDPR Action Items: Data Breach Notification

- Perhaps the biggest action item is the GDPR data breach notification requirement making it mandatory to inform customers and authorities within 72 hours of a data breach
  - All too often, in the past, data breaches were not immediately divulged by impacted organizations
    - Perhaps not until the data breach was uncovered by someone else, sometimes much more than 72 hours after it had occurred
- Tactic: Avoid the notification requirement by preventing data breaches in the first place
  - Most breaches are caused by known vulnerabilities (where a patch is available at the time of the breach)
  - Of course, you can never assure 100% prevention so you will need to prepare strong alerting and notification procedures, too.

GDPR Action Items: Data Breach Notification (continued)

- Compliance with the data breach notification requirement will be more difficult than companies expect.
- It requires that organizations first understand, and then share complicated details with regulators and customers about any exfiltration of personal data, including how many records were lost or stolen, and over what period.
- Incident response teams must be customer-savvy in order to develop clear and complete messages pertinent to both regulatory bureaucrats and customers.
  - The USA has no national data breach notification requirement, and the 48 state laws that do exist require notification anywhere between 30 to 45 days.
  - For GDPR it is 3 days.

GDPR Action Items: Data Privacy by Design

- GDPR states that organizations must implement privacy by design. This means that you have to consider privacy at the start of any new project and ensure that proper security controls are in place throughout all development phases.
- Sustained collaboration between teams will be critical, so firms will have to establish new processes to encourage, enforce, and oversee it.
- Implementing privacy by design is a significant challenge.

GDPR Action Items: Global Mandate

- The reach of GDPR makes it a global mandate.
  - Non-EU organizations that provide goods or services to EU residents or monitor their behavior — or collect and re-sell this information to other business partners — must comply with GDPR requirements.
  - Your DPO, compliance team, and legal counsel must determine how and when GDPR applies.
  - Security team must evaluate ability to comply for both your organization and your partner chain

GDPR Action Items: Evidence of Risk Mitigation

- GDPR requires organizations to be able to demonstrate that they have implemented appropriate measures to mitigate privacy risks.
- This is compulsory even if you have not had a data privacy breach or customer complaint. Regulators may require evidence of compliance and risk management strategies.
- You must be able to provide evidence of risk mitigation documentation, possibly including a privacy impact assessment (PIA).
- To build this documentation your organization must demonstrate that it has deployed access controls and rights management.

GDPR Action Items: Data Recovery

GDPR also mandates timely data recovery. It states that to be in compliance your organizations must be able to “restore the availability and access to personal data in a timely manner in the event of a physical or technical incident”

Of course, timely recovery should be a part of all of your data contingency and disaster plans… But “timely” is not defined in the regulations

It is a good idea to re-evaluate all backup and recovery plans for any databases with PII in them

Most organizations perform regular (annual?) disaster recovery tests but…

- …do you test your local backups for recovery?

GDPR Action Items: Metadata Management

Article 30 of the GDPR requires organizations to maintain a record of processing activities.

This record has to include:

- Description of the categories of personal data
- Categories of recipients of personal data, including those in third countries or international organizations
- Transfers of personal data to a third country or an international organization

The recordkeeping requirements also extend to those who process data on behalf of an organization.

This is challenging, and to comply you must strengthen your organization’s metadata management and data lineage capabilities.

Metadata Management is a Discipline

- Metadata management is the administration of data that describes your data. It involves establishing policies and processes that ensure information can be integrated, accessed, shared, linked, analyzed and maintained to best effect across the organization.
  - Managing metadata should not fall to DBAs
  - It is less technical, more business-focused
  - It is a discipline unto itself
  - Metadata is necessary to be in compliance!

Cost of Non-Compliance can be Significant

- GDPR requires that you obtain the consent to collect and use a person's personal data. Consent must be clearly and specifically requested.
- The penalty for non-compliance with GDPR is steep:
  - Fines up to 20,000,000 EUR or 4% of total worldwide annual revenue for the preceding year, (whichever is higher).
- Aside from financial penalties, many businesses will require their vendors to be fully compliant with the GDPR as a condition to doing business.
  - These requirements are usually part of the RFP process and / or privacy & security audits.
  - Non-compliance could lead to significant loss of business to competitors who are able to demonstrate their GDPR compliance.

- Forrester predicts that 80 percent of firms affected by GDPR will not comply with the regulation by May 2018.[1]
- Gartner estimates that less than half of companies that GDPR applies to will be in compliance by the end of 2018. [2]

[1] https://go.forrester.com/wp-content/uploads/Forrester-2018-Predictions.pdf

[2] https://www.gartner.com/newsroom/id/3701117

GDPR Enforcement

GDPR sets out the obligation for Member States to set up a supervisory authority - Data Protection Authorities (DPA).

These national authorities will monitor the application of the GDPR regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.

The obligation of the DPA from an enforcement perspective can then be divided into two parts:

- Monitoring whether individuals can exercise their rights; and
- Evaluating whether the processing of personal data complies with the rules on processing set out by the GDPR.

Enforcement

- Enforcing the regulation is always the most difficult aspect of regulatory compliance
  - Although GDPR applies universally for all members of the European Union, it is unlikely to be applied equally
  - All 28 different countries will handle enforcement.
  - Will Germany be tougher on GDPR enforcement, than say, Denmark or Malta?
  - And what about the U.K.?
    - It has pushed back against data-privacy rules that could impede global trade
    - And then there is the looming Brexit
  - Finally, how will it play out when trying to enforce penalties against a non-EU actor for infringing on data privacy of EU citizens…

Lawsuits Filed Almost Immediately

GOOGLE | FEATURED VIDEOS | TECH

Facebook and Google hit with $8.8 billion in lawsuits on day one of GDPR

189

By Russell Brandom | @russellbrandom | May 25, 2018, 10:21am EDT

SHARE

On the first day of GDPR enforcement, Facebook and Google have been hit with a raft of lawsuits accusing the companies of coercing users into sharing personal data. The lawsuits

MOST READ

GDPR is Not a Project…

- Compliance should be thought of as an on-going, vital component of your business… and GDPR compliance is part of that.
- Really, if you stop to think about it, all GDPR is doing is requiring responsibility and management for your data

If we had been treating data appropriately for all these years these (compliance) **action items would not seem quite as onerous**

Good idea to treat <u>all data</u> as if it is covered by GDPR, not just European citizens' data.

More and New Regulations are Coming

Passed June 29, 2018

…takes effect in 2020

POLICY BLOG

COMMENTARY

California Passes Broad Online Privacy Bill

by **Wendy Davis** , Staff Writer **@wendyndavis**, Yesterday

Lawmakers in California on Thursday passed a sweeping privacy bill that gives consumers the right to prevent the sale of their personal information, including their web-browsing history.

The bill, which was **signed** Thursday afternoon by Governor Jerry Brown, contains numerous other provisions -- including one that allows consumers to require the deletion of their personal information. Another term prohibits companies from charging higher fees to consumers to refuse to share their personal data -- though that provision has some wiggle room.

To Do…

Encryption

- GDPR explicitly mentions encryption as one of the security and personal data protection measures
- However, under GDPR, encryption is **not** mandatory
- Nevertheless, it is important to consider encryption as a means to comply
  - With other data protection laws the presence of encryption has been used as an argument to show that an organization took technical and organizational measures to protect personal data
  - **Guidelines for implementing and enforcing GDPR are not crystal clear the further you dig into them.**
    - Supervisory authorities may differ by country
    - Additional regulations are being planned (ePrivacy Regulation)

Data Access Auditing and SIEM

To keep tabs on your data and who's accessing (or even looking at) your data, you need a 360-degree view of all user activity surrounding your data.

- SIEM can offer such a view through log mgmt. in conjunction with event correlation.
- Requires collecting & correlating event logs:
  - Endpoint devices, firewalls, routers, switches, desktops, servers, and applications (log management)

From a database perspective, database auditing can track all access to database data

- "Who did what to which data when?"

Real-Time Alerting

- Article 33 of the GDPR states:
  - “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 55,8 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.”
- In other words, you need real-time alerting across all threat vectors because in the world of cyber-crime, 72 hours is not that long, considering the average time to discover a breach is still 191 days!

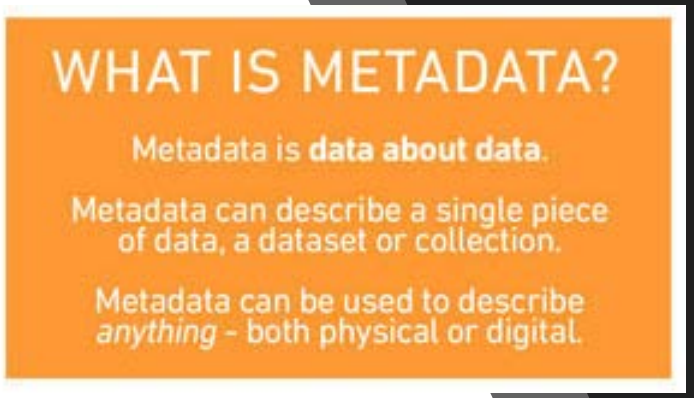
(according to the latest IBM/Ponemon Institute “2017 Cost of Data Breach Study”)

But isn't Auditing Built-in to Db2?

- Db2 (and most DBMSes) can produce the audit trail

- The problem comes when you need real-time alerting and the ability to produce compliance reports on the audit details

Compliance Requires Metadata



- As data volume expands and more regulations hit the books, metadata will increase in importance
  - Metadata: data about the data
  - **Metadata** characterizes data. It is used to provide documentation such that data can be understood and more readily consumed by your organization. Metadata answers the **who**, ***what***, ***when***, ***where***, ***why***, and ***how*** questions for users of the data.
- Data without metadata is meaningless
  - Consider: 27, 010110, JAN

Data Categorization

- Data categorization is critical
  - Metadata is required to place the data into proper categories for determining which regulations apply
    - PII → GDPR, PCI
    - Financial data → SOX
    - Health care data → HIPAA
  - Some data will apply to multiple regulations
  - Who does this now at your company?
    - Anyone?

What about Db2?

Db2 Security Modernization

- More granular control of System authority
  - Db2 10: SECADM, System DBADM, SQLADM
  - ACCESSCTRL | DATAACCESS
  - EXPLAIN privilege
- Improved audit functionality
  - No expensive data collectors
  - Audit Policies are managed in the catalog
    - Audit policy does not require AUDIT clause to be specified
- Row Permissions
  - Improved access by row contents
- Column Masks
  - Improved compliance
- TRUSTED CONTEXT and Roles
  - Authorized remote connections for applications

Data Encryption

- By encrypting data you can show that your organization is taking steps to mitigate the risk of data being surreptitiously accessed, stolen or breached…
- But…

Pervasive Encryption

- It can be difficult to analyze and understand all of the data, and all of the regulatory implications
- Especially if you have not been rigorously managing metadata definitions and data lineage for your data
  - And let's face it, that is most of us!
- The IBM z14 delivers pervasive encryption to encrypt it all
  efficiently and effectively
  - A good step to show evidence of risk mitigation

Db2 12, Pervasive Encryption and FL 502

- Db2 11 + 12 for z/OS support z/OS DFSMS data set encryption

  Part of the Pervasive Encryption for IBM Z solution

- Encrypt all relevant Db2 data
  - Tables, indexes, logs, catalog/directory and backups
- Safely load and unload data from encrypted tables
- APARs PI90288 and PI97037

Encrypting your Db2 for z/OS data sets
http://ibm.biz/BdZ9ud

Function Level 502

- New Db2 policy controls for DFSMS data set encryption
  - Requires a key label to encrypt and decrypt the data
- FL502 enhances Db2 to make setting & viewing key label information easier and more integrated with the data sets
  - Catalog/Directory objects, User objects, and Active/Archive logs.

`APPLCOMPAT(V12R1M502)`

Db2 12 for z/OS - FL 502

Db2 Function Level 502 delivers several new features, one of which bolsters DFSMS data set encryption (part of the Pervasive Encryption for IBM Z solution introduced with the z14).

With FL502 we get KEYLABEL management capability for z/OS DFSMS data set encryption. You can manage the key labels for z/OS DFSMS data set encryption to transparently encrypt Db2 data sets.

DFSMS can be used to encrypt various types of Db2 data sets including Db2-managed table space and index space data sets, data sets that are used by Db2 utilities, and sequential input and output data sets.

After moving to FL502 an administrator (DBA, security admin, system admin or storage admin depending on your shop) can enable z/OS DFSMS data set encryption for your Db2 data sets.

Additionally, IBM offers a free tool, IBM z Systems Batch Network Analyzer (zBNA), which can be used to help estimate the costs of DFSMS data set encryption for your Db2 data sets.

Additionally, the Db2 Statistics Trace has been enhanced to report CPU time, which you can look at to help determine which data sets to encrypt.

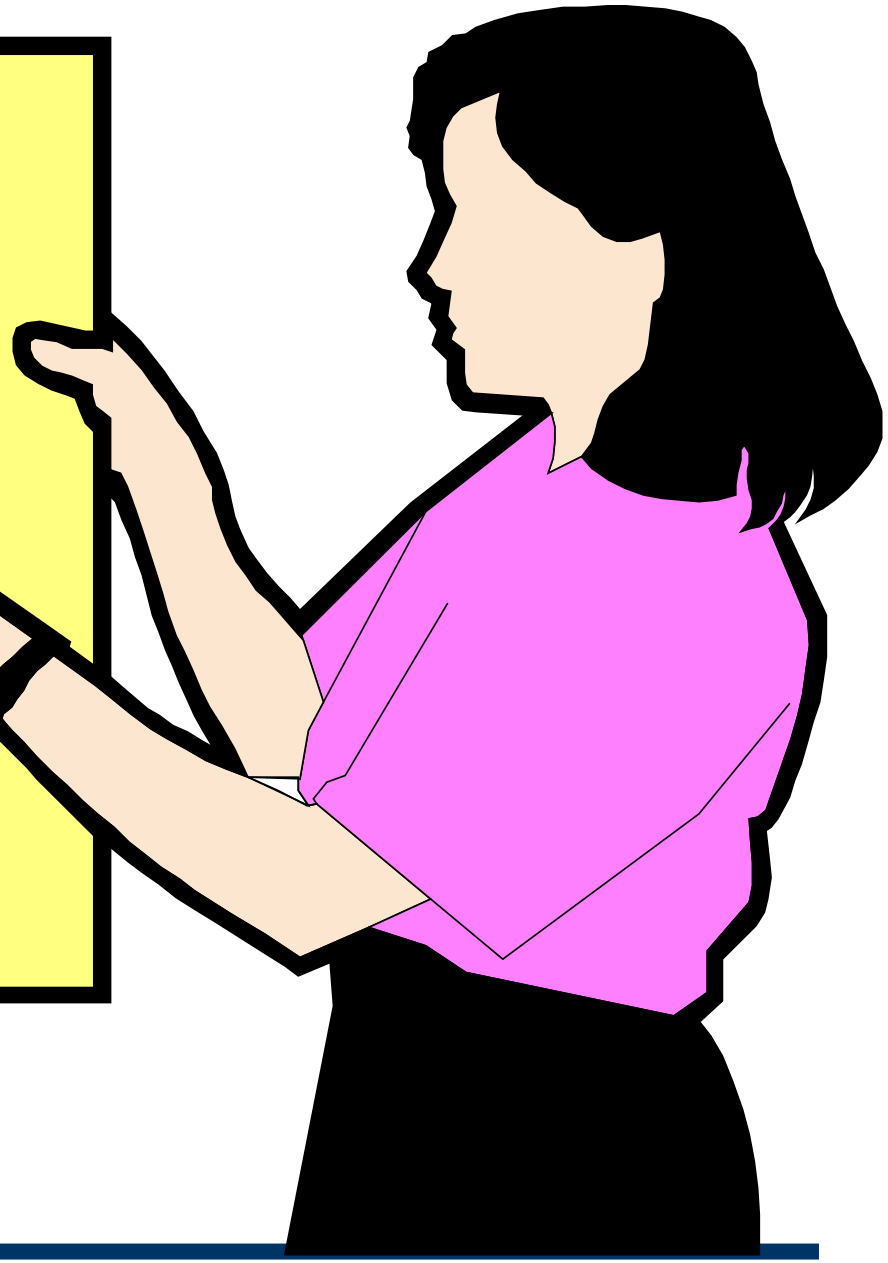
Summary

Security and Data Privacy
can no longer be an afterthought

Regulations demand our action

Db2 and Z offer
built-in capabilities
to help

Keep up on new technologies
and new Db2 capabilities!



Contact Information

Craig S. Mullins

Mullins Consulting, Inc.
15 Coventry Ct
Sugar Land, TX 77479

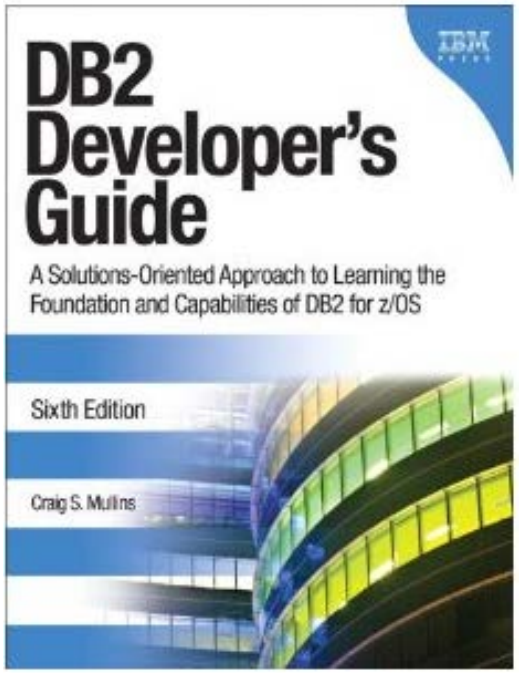
E-mail: craig@craigsmullins.com

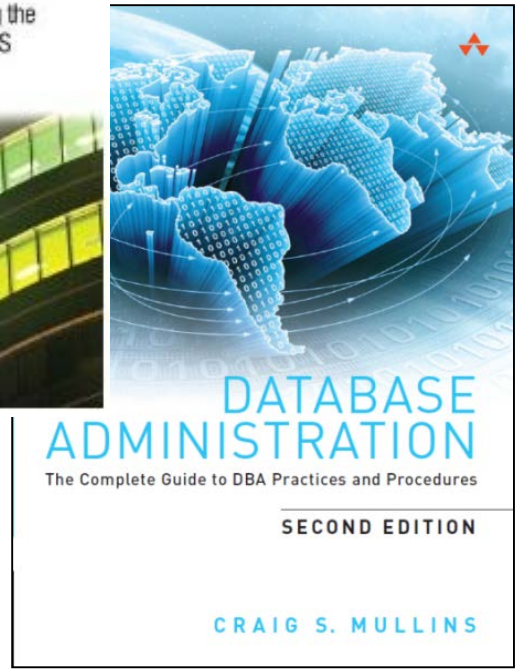
Web: www.mullinsconsulting.com

IBM CHAMPION

IBM Gold CONSULTANT

http://mullinsconsulting.com/cm-book.htm





http://mullinsconsulting.com/dba_book.htm

Web References

- gdpr-ionfo.eu
- www.isaca.org
- www.coso.org
- www.aicpa.org
- www.auditnet.org
- www.sox-online.com
- www.bis.org/publ/bcbs107.htm - (Basel II)
- www.snia-dmf.org/100year
- www.pcisecuritystandards.org/