Data Security:
The Cost of Doing Business as Usual

David Siles
Chief Technology Officer, DataGravity
dsiles@datagravity.com

DataGravity®

Quick Poll

Q1. Do you know where all the sensitive data in your environment is stored?

DataGravity

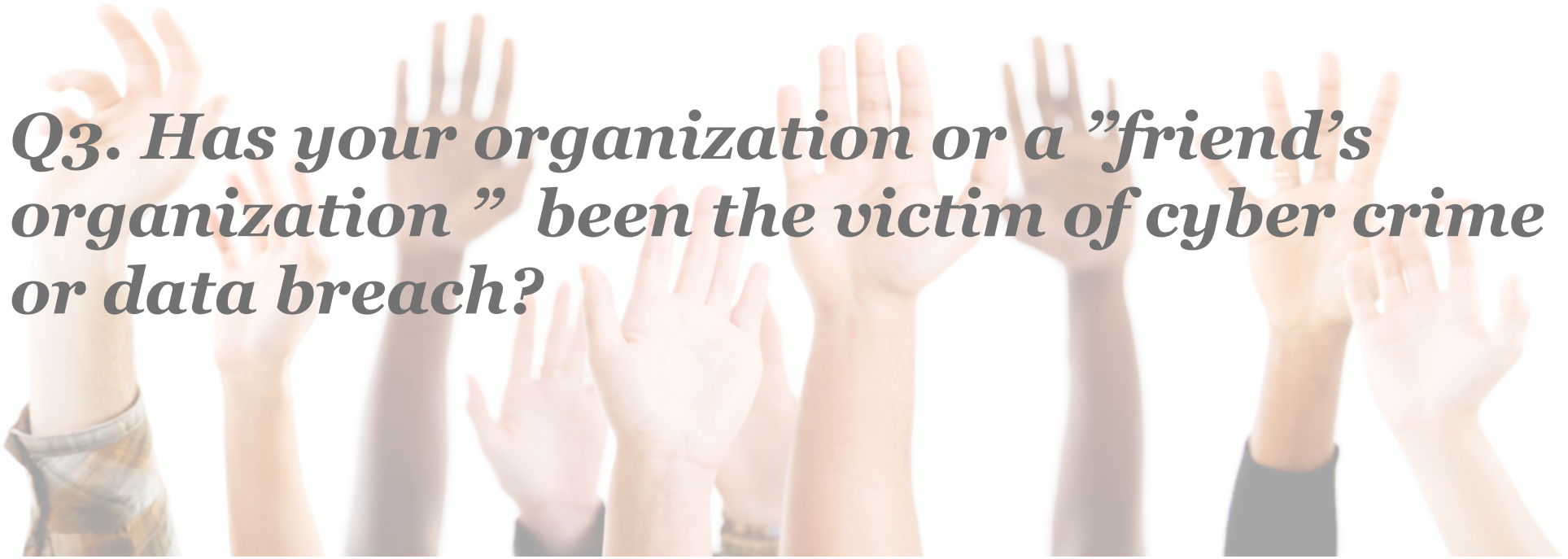
Quick Poll

Q2. Are you in a regulated industry or responsible to a compliance standard?

(PCI-DSS, HIPAA, FERPA, FISMA, GDPR, etc.)

DataGravity

Quick Poll



Q3. Has your organization or a "friend's organization " been the victim of cyber crime or data breach?

DataGravity

Quick Poll

Q4. How many here have a dedicated security team watching all your data 24/7/365 with an unlimited security budget?

DataGravity

DataGravity®

Introduction 1

Business As Usual 2

Financial Penalties 3

Unanticipated Costs 4

Becoming Data Aware 5

Summary 6

Have You Heard These Common Objections?

"We've never been breached before…"

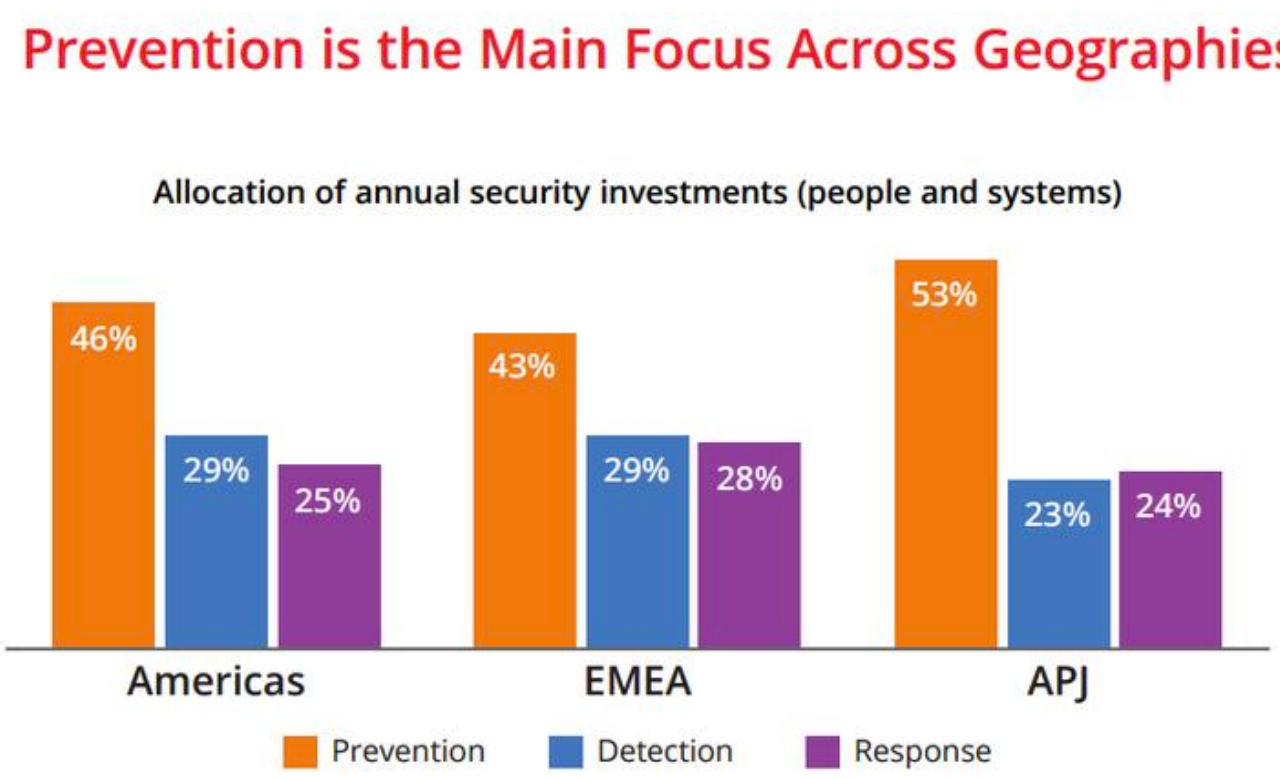
"Nobody cares about attacking our organization…"

"We have nothing that an attacker would want…"

"We can't afford to invest in…"

DataGravity

2016 RSA Threat Detection Effectiveness Survey



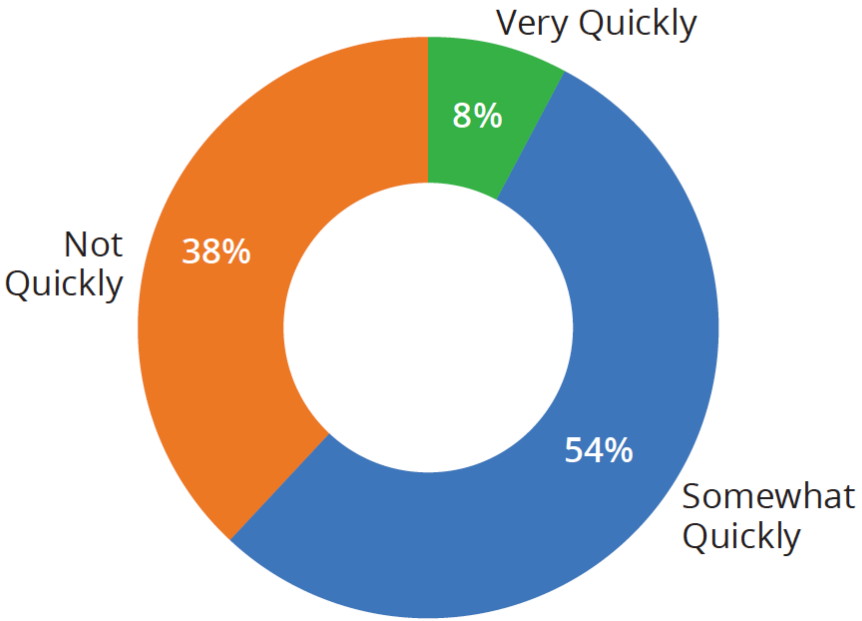
- 47 percent of annual security investments went into preventative measures
- Detection and response made up just 25 percent and 29 percent respectively

Source: https://www.rsa.com/content/dam/rsa/PDF/H14916-threat-detection-effectiveness-pdf-eb.pdf

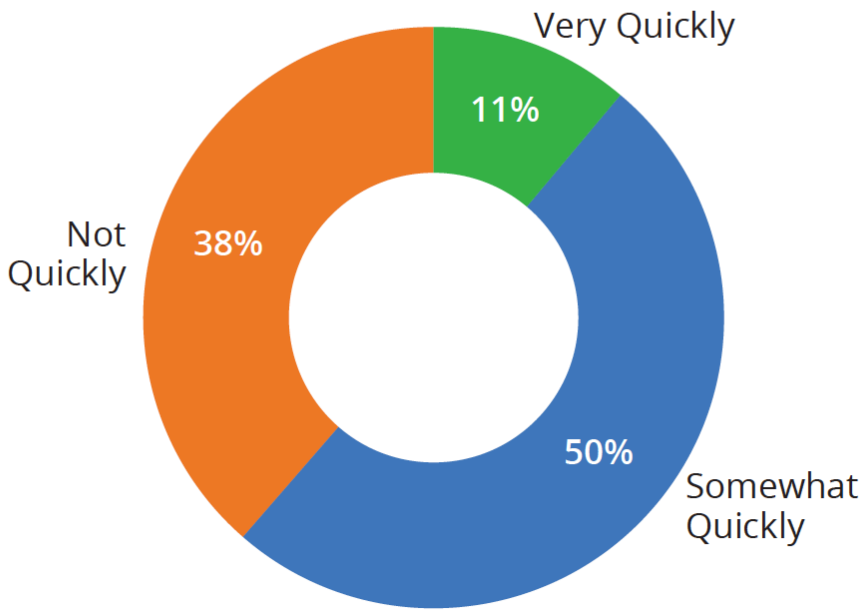
DataGravity

What Happens If A Breach DOES Occur?

How quickly are you able to detect attacks using your current data and tools?



How quickly are you able to investigate attacks using your current data and tools?

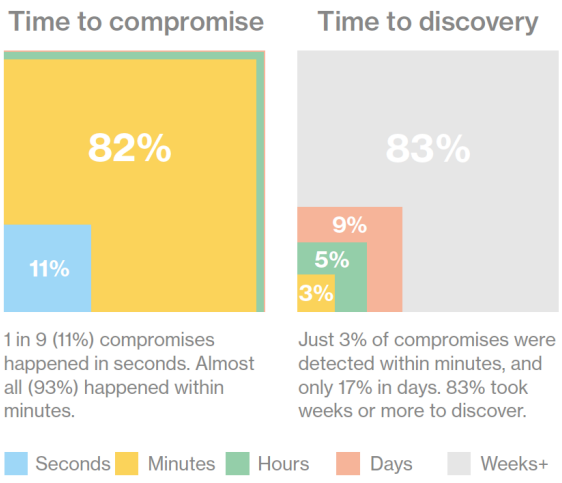


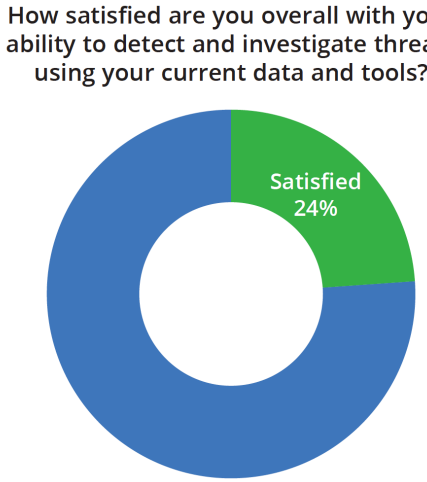
Source: https://www.rsa.com/content/dam/rsa/PDF/H14916-threat-detection-effectiveness-pdf-eb.pdf

DataGravity

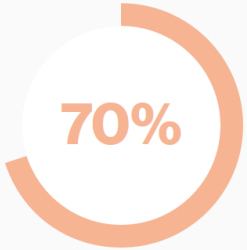
There Is A Disconnect Here…

- There is a disconnect between the executive team and those that are in the trenches
- The organization may not have experienced a damaging breach in the past, data shows that their organization may be incapable of effectively mitigating such an event





70% of breaches involving insider misuse took months or years to discover.

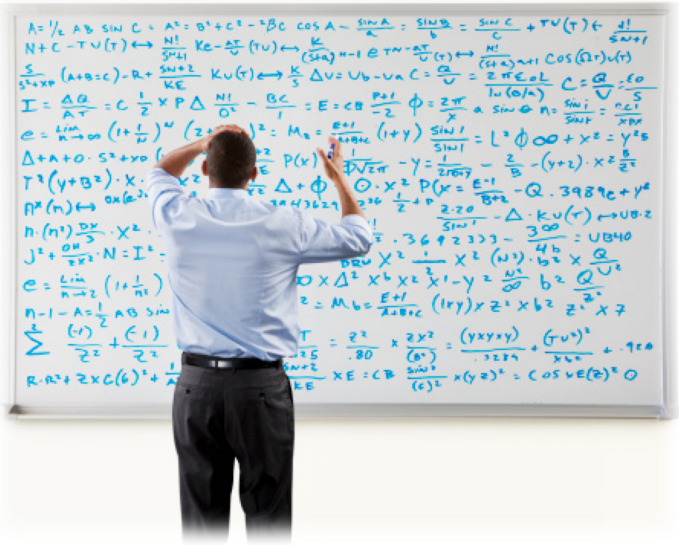


Source: https://www.rsa.com/content/dam/rsa/PDF/H14916-threat-detection-effectiveness-pdf-eb.pdf
Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

DataGravity

Why Is This Such A Problem?

- Why do practitioners have such a hard time convincing their management team about the value of investing in things?
- Business leaders have their own language
  - To better communicate with shareholders, board members, partners, and peers



- Unfortunately, this language is often as foreign to most security practitioners as yours is to them
- It is likely that you haven't found the best way to communicate the threat or need to the business in a language that they understand…

DataGravity

You Need To Pitch Properly

- Walk a mile in your managers shoes…
  - Objectives
    - Managers **exist to help employees and the business succeed**
  - Ideas
    - Are weighed, measured, and **executed** following industry best practices and **within budgetary constraints**
  - A Job Well Done
    - The **business keeps running**, nobody gets hurt, and all **objectives can be measured and communicated to business stakeholders**
- So speak their language…**the language of business success and threats to profitability**

DataGravity

DataGravity®

Introduction 1

Business As Usual 2

Financial Penalties 3

Unanticipated Costs 4

Becoming Data Aware 5

Summary 6

Financial Penalties Are Easy to Quantify

Just look in the news…

FOR IMMEDIATE RELEASE
November 30, 2015

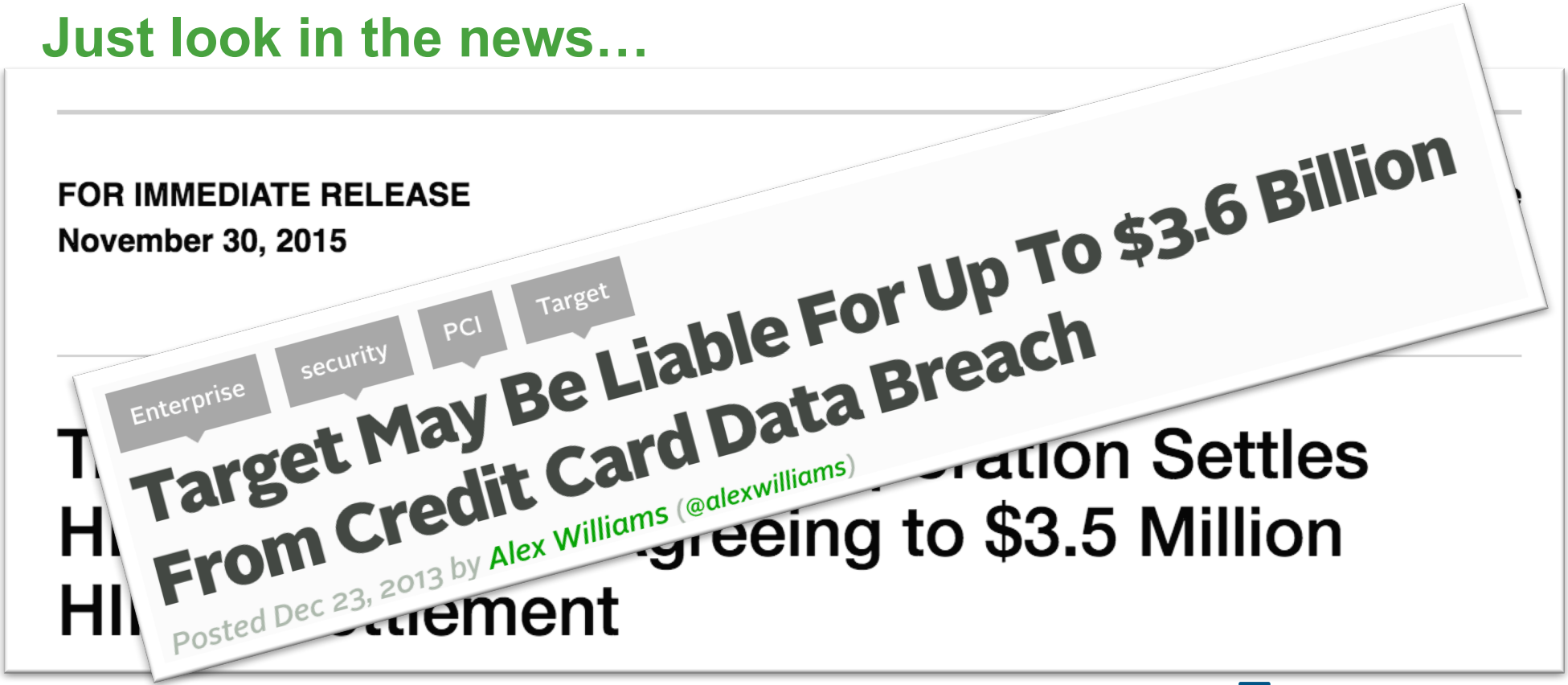
Contact: HHS Press Office
202-690-6343
media@hhs.gov

Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement

DataGravity

Financial Penalties Are Easy to Quantify

Just look in the news…



DataGravity

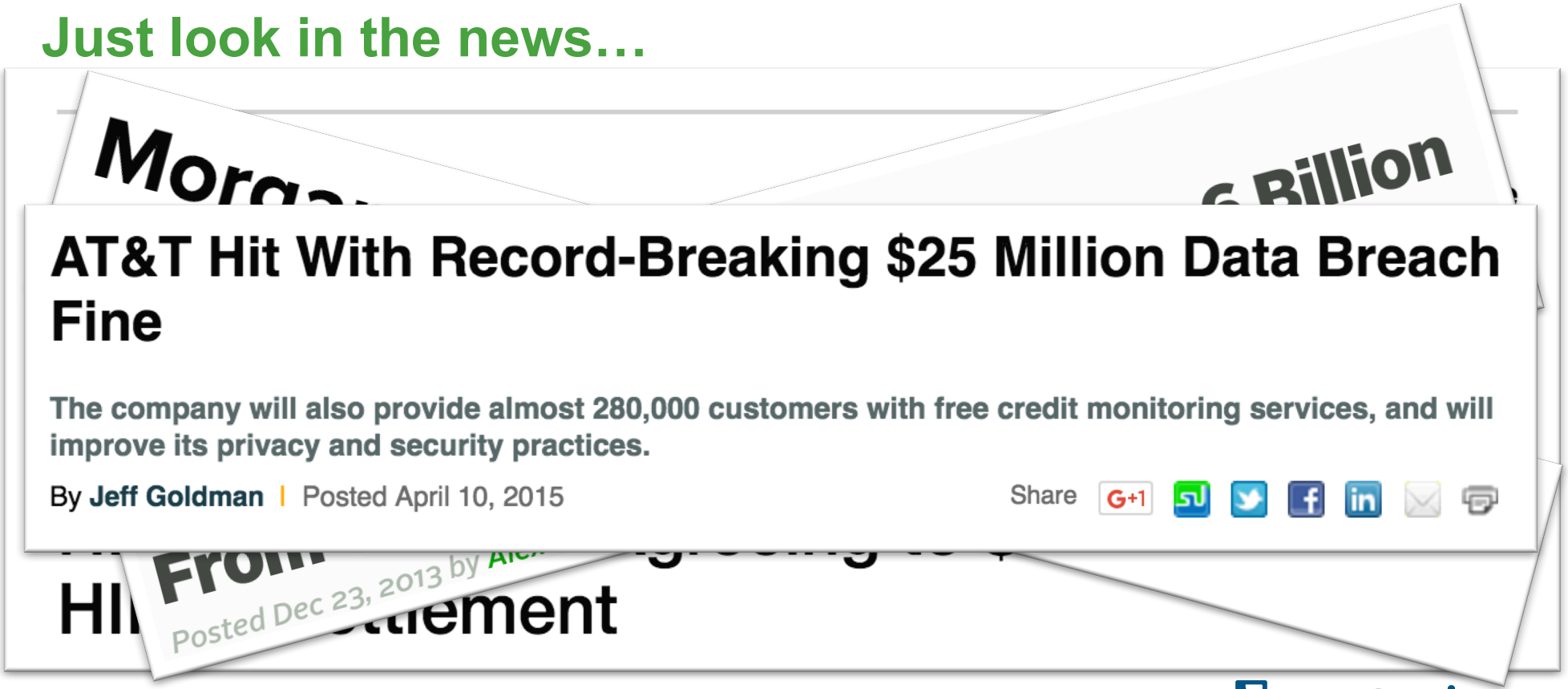
Financial Penalties Are Easy to Quantify

Just look in the news…

DataGravity

Financial Penalties Are Easy to Quantify

Just look in the news…



DataGravity

The Cost of Regulatory Fines

Depending on the industry, applicable regulatory compliance mandates, and geographic location (of both the company and its customers) the fines imposed for non-compliance can be devastating to a business.

DataGravity

Fines: PCI DSS

- If a merchant experiences a security breach and is found to be non-compliant with PCI rules, they may be subject to steep fines.
- Depending on the circumstances, merchants might have to pay anywhere from $5,000 to $100,000 every month until they address all identified compliance issues
- If they don't resolve the problem satisfactorily, they may even have their ability to accept cards revoked

DataGravity

Fines: HIPAA

- Failure to comply with the Health Insurance Portability and Accountability Act (HIPAA) can result in both civil and criminal penalties (42 USC § 1320d-5)
- Civil penalties can range from $100 to $50,000 per violation with maximum of $1.5 million per calendar year

- Criminal penalties carry both fines and prison time for covered entities and specified individuals
  - These criminal penalties range from $50,000 in fines and imprisonment up to one year, to $250,000 in fines and imprisonment for up to 10 years.

DataGravity

Fines: GDPR

- The following sanctions can be imposed:
  - A warning in writing in cases of first and non-intentional non-compliance
  - Regular periodic data protection audits
  - A fine up to 10m EUR (**~12.4m USD**)
    - or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater
  - A fine up to 20m EUR (**~22.5m USD**),
    - or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher

DataGravity

Introduction 1
Business As Usual 2
Financial Penalties 3
Unanticipated Costs 4
Becoming Data Aware 5
Summary 6

Some Unanticipated Costs To Consider

Productivity
How long can you tolerate the disruption to the operational state of your business?

DataGravity

Some Unanticipated Costs To Consider

Technology
Will a breach cause a knee-jerk purchasing reaction within your organization to prevent the same thing from happening again?

Productivity
How long can you tolerate the disruption to the operational state of your business?

DataGravity

Some Unanticipated Costs To Consider

Brand Damage
Can your brand navigate through a highly publicized and damning breach? Will your partners return? Will your customers?

Technology
Will a breach cause a knee-jerk purchasing reaction within your organization to prevent the same thing from happening again?

Productivity
How long can you tolerate the disruption to the operational state of your business?

DataGravity

Some Unanticipated Costs To Consider

Brand Damage
Can your brand navigate through a highly publicized and damning breach? Will your partners return? Will your customers?

IP Loss
Lost future earnings by having your intellectual property sold/used on the open market by competitors

Technology
Will a breach cause a knee-jerk purchasing reaction within your organization to prevent the same thing from happening again?

Productivity
How long can you tolerate the disruption to the operational state of your business?

DataGravity

Some Unanticipated Costs To Consider

Brand Damage
Can your brand navigate through a highly publicized and damning breach? Will your partners return? Will your customers?

IP Loss
Lost future earnings by having your intellectual property sold/used on the open market by competitors

Technology
Will a breach cause a knee-jerk purchasing reaction within your organization to prevent the same thing from happening again?

Innovation
Will innovation suffer because you're organization is spending all of its time trying to recover from a breach?

Productivity
How long can you tolerate the disruption to the operational state of your business?

DataGravity

Some Unanticipated Costs To Consider

Brand Damage
Can your brand navigate through a highly publicized and damning breach? Will your partners return? Will your customers?

IP Loss
Lost future earnings by having your intellectual property sold/used on the open market by competitors

Technology
Will a breach cause a knee-jerk purchasing reaction within your organization to prevent the same thing from happening again?

Innovation
Will innovation suffer because you're organization is spending all of its time trying to recover from a breach?

Productivity
How long can you tolerate the disruption to the operational state of your business?

Perception
Will your organization have a permanent 'black mark' in the eyes of potential employees, investors, and partners?

DataGravity

Introduction 1
Business As Usual 2
Financial Penalties 3
Unanticipated Costs 4
Becoming Data Aware 5
Summary 6

Revisiting The Common Objections…

"We've never been breached before…"

"Nobody cares about attacking our organization…"

"We have nothing that an attacker would want…"

"We can't afford to invest in…"

DataGravity

Objection Handling

"We've never been breached before..."

- Do you currently have the visibility or capability to discern this?
  - Or has the organization simply been oblivious?
- Has your industry been targeted as of late?
- Have your partners or supply chain ever suffered a breach?

DataGravity

Objection Handling

"Nobody cares about attacking our organization…"

- Upon what assumptions are these statements based?
  - Perhaps the previous slide?
- If compute resources are connected to the Internet you must always assume that at least ONE person wants to exploit or gain access to them
  - *Ever put an unpatched Windows 95 workstation on the Internet to see what happens?*

DataGravity

Objection Handling

"We have nothing that an attacker would want…"

- The answer to this is almost always "Yes, we do"
- Money isn't the only asset an attacker would want
- Other assets include:
  - Compute resources (a.k.a. Bots)
  - Intellectual property
  - Financial information
- Intangibles are tangible in an online world

DataGravity

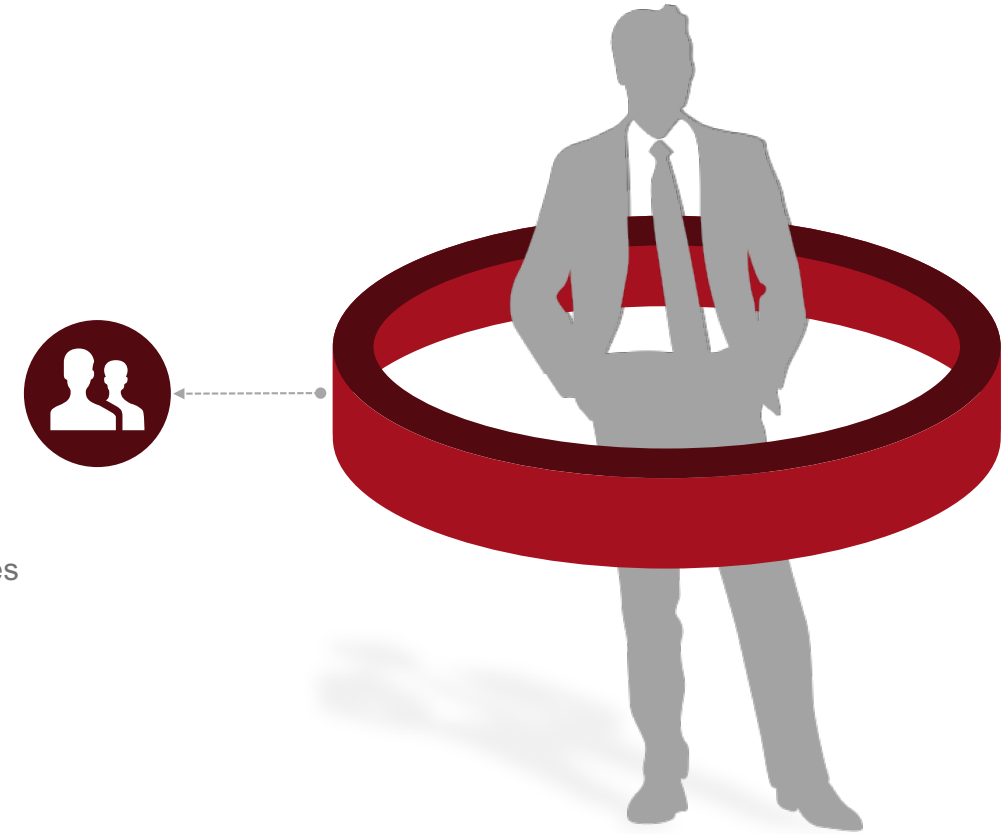
Objection Handling

"We can't afford to invest in…"

- What is the business tolerance for pain vs. expense?
  - Remember the cost-benefit analysis?
- How much do the following cost the business:
  - Bad press
  - Downtime
  - Public breach disclosure?
  - Opportunistic attack recovery (e.g. Ransomware)

DataGravity

What Does Being ‘Data Aware’ Mean?



Identifying

- Who has access
- What sensitive content exists within
- When data is being accessed
- Where your data lives
- Why it exists

DataGravity

What Does Being ‘Data Aware’ Mean?

Identifying

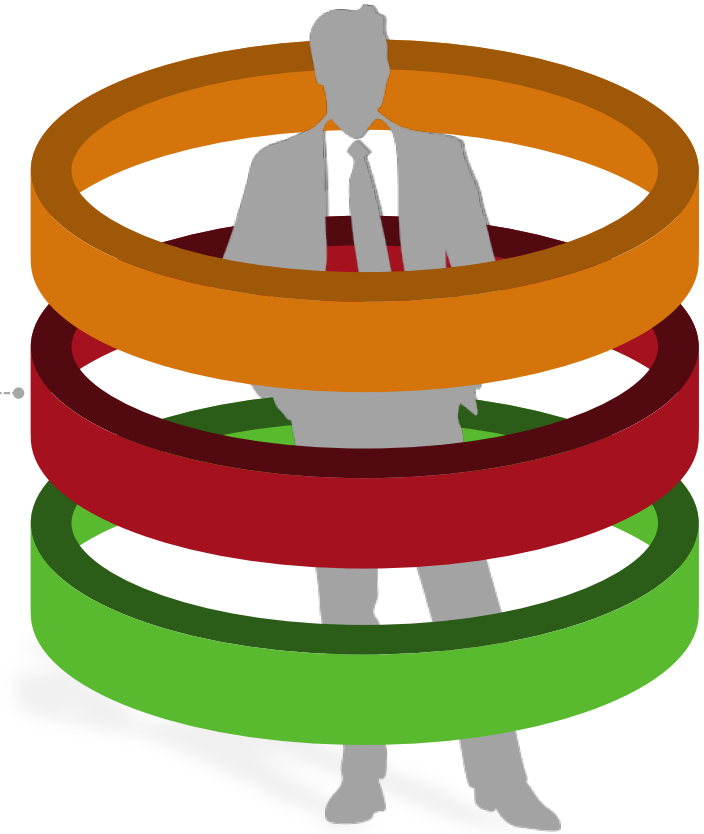
- Who has access
- What sensitive content exists within
- When data is being accessed
- Where your data lives
- Why it exists

Monitoring

- How the data is being used
- If its use follows defined standards and guidelines
- Suspicious and anomalous changes

DataGravity

What Does Being ‘Data Aware’ Mean?



Identifying

- Who has access
- What sensitive content exists within
- When data is being accessed
- Where your data lives
- Why it exists

Protecting

- From theft
- From misuse
- From abuse
- From proliferation
- From deletion

Monitoring

- How the data is being used
- If its use follows defined standards and guidelines
- Suspicious and anomalous changes

DataGravity

Free DataGravity® DataMRI® Assessment Today

LOOK INSIDE THE BLACK BOX

Get your free assessment today at datagravity.com

Free Assessment

DataGravity®

DataGravity®

Introduction 1

Business As Usual 2

Financial Penalties 3

Unanticipated Costs 4

Becoming Data Aware 5

Summary 6

Summary

- Focus threat discussions around adverse material impact to the business and its continued ability to generate revenue
- Lead with data supporting the need for increased vigilance by citing published data, peer conversations, and recent events in the media
- Become data-aware so that you can easily quantify the extent of a breach and recover as quickly and as effortlessly as possible

DataGravity

Questions?

David Siles
Chief Technology Officer, DataGravity
dsiles@datagravity.com

DataGravity®

’Common Objection’ Handling

- Always be prepared to challenge the preconceived notions or beliefs of your leaders
- The best way to do this is **with data**
- Sources of data that can be used to make your case:
  - FBI field office (for trends, patterns, etc.)
  - Closed peer trust or working groups (what are your peers seeing?)
  - Published industry data and studies (e.g. DBIR, Ponemon, etc.)

DataGravity