



ISOAG Meeting December 2, 2015

Welcome to CESC!





ISOAG December 2 , 2015 Agenda

I. Welcome & Opening Remarks

Mike Watson, VITA

II. The Fog of More

Robert Shields, Informatica,

III. Upcoming Events

Bob Baskette/Mike Watson, VITA

IV. Partnership Update

NG



Welcome and Opening Remarks

Michael Watson

December 2, 2015



The Fog of More

Robert Shields, CISSP

PMM Data Security and Privacy, Informatica

Robert Shields

- ***Robert Shields, CISSP***
Principal PMM, Data Security and Privacy
- Robert Shields leads product marketing for Informatica's Secure@Source and data masking solutions. Robert is responsible for market development and strategy, sales enablement, analyst relations and thought leadership.

Robert has extensive information security experience and helped introduce and pioneer key security technologies including encryption, two-factor authentication, computer forensics, eDiscovery and data masking and data security analytics.

data breach

*Turns out, the hackers have gotten smarter,
the breaches have gotten bigger,
and the threats are coming in from all directions.
Meanwhile, the organizations responsible for
all this data have been scrambling to keep up.*

Informatica, "Data Centric Security e-Book"

More Data, More Protections, More Risks = Less Security

“The Fog of More”

Security Audit and Assurance Services

User and Entitlement Security

- Access Control
- Single Sign-on
- Strong Authentication
- Federation
- Identity Lifecycle Management
- Provisioning
- Role and Entitlement Management
- Attestation and Recertification

Application Security

- Secure SDLC
- Process Assessment
- Web Application Scanning
- Vulnerability Testing
- Static Code Analysis

Data Security

- Data Masking
- Data Encryption
- Tokenization
- File Security
- Disk Encryption

Infrastructure Security

- Network/Perimeter Security
- End Point Security
- LAN Security
- Email and Web Security
- Data Loss Prevention
- Security Event and Log Management
- Privileged Identity Mgmt.
- Governance, Risk & Compliance

Mobile Security

- Unmanaged Device Identification
- Mobile Security Blueprinting
- Mobile Device Mgmt.
- Mobile Security Testing
- Mobile Data Security

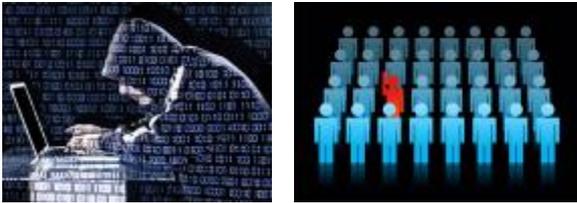
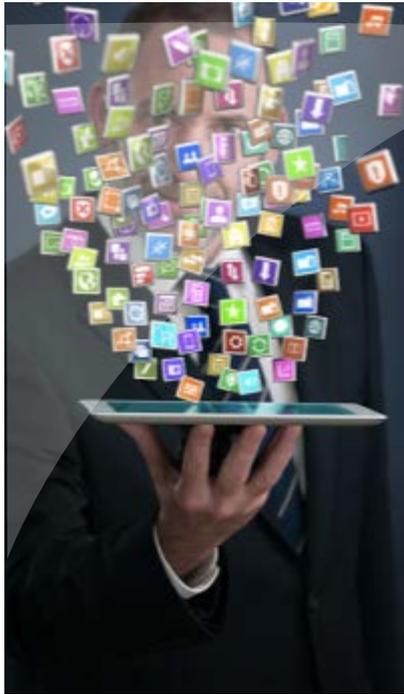
Security Operations Center (SOC)

“The Fog of More”

- Thousands of databases, millions and billions of files
- *Poor understanding of the sensitive data; inventory, location, proliferation and protection mechanisms.....*
- *This landscape is dynamic and changes weekly if not daily...*
- *PII and other sensitive information is going and proliferating.*



Fog of More: The Key Drivers



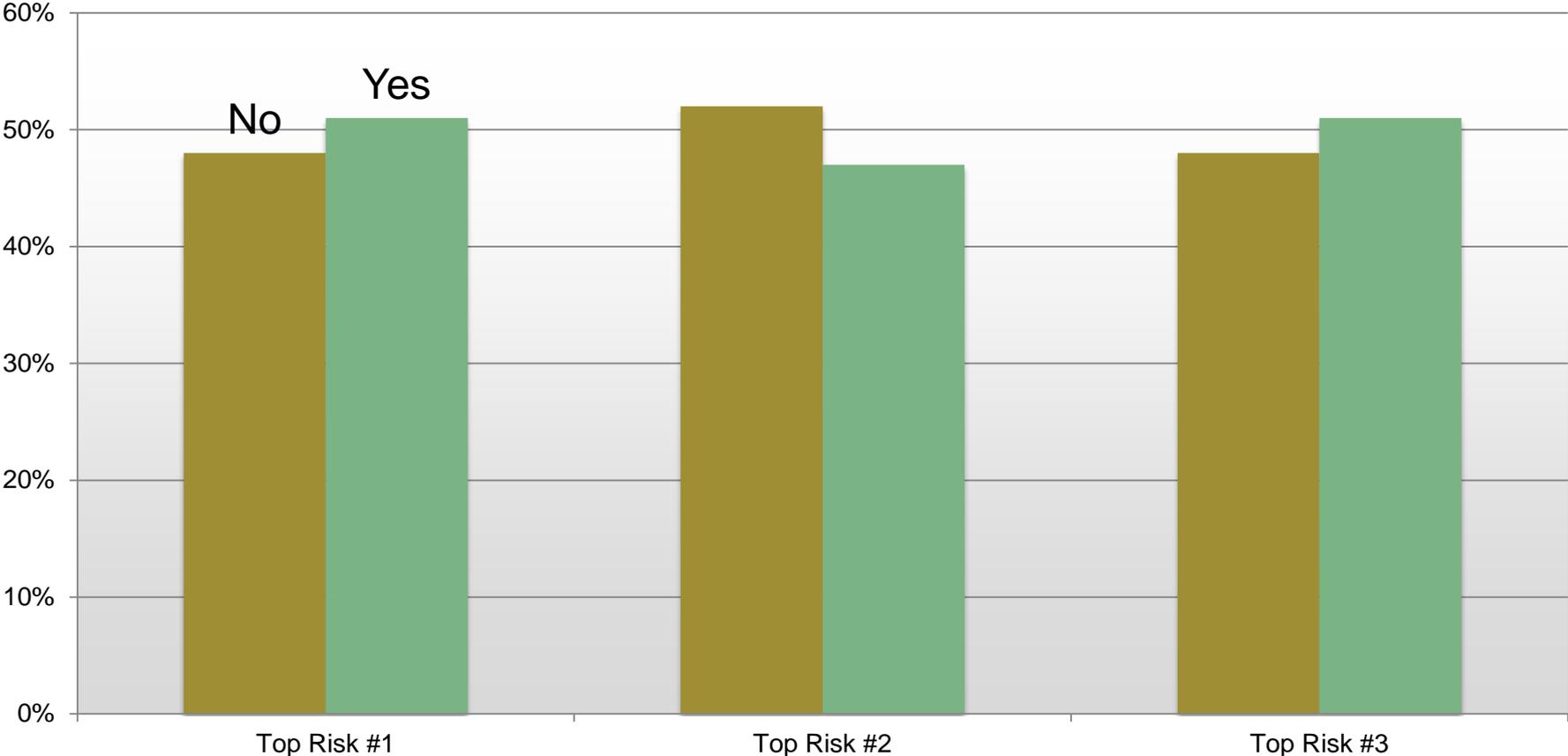
Three key insights from our CISO peer research

- Cloud, Mobility and Compliance put pressure on their data security programs
 - Legacy controls becoming irrelevant
- They lack confidence in their current controls
 - Despite increasing perceived industry and peer risk
- They struggle to measure their impact on the business
 - Security tool metrics fail to correlate effort and impact

Lack of Metrics, Unable to Map to Business Impact

Q: Do you have metrics to track your top risks?

A: Half do NOT have metrics (!)



What keeps IT practitioners up at night?

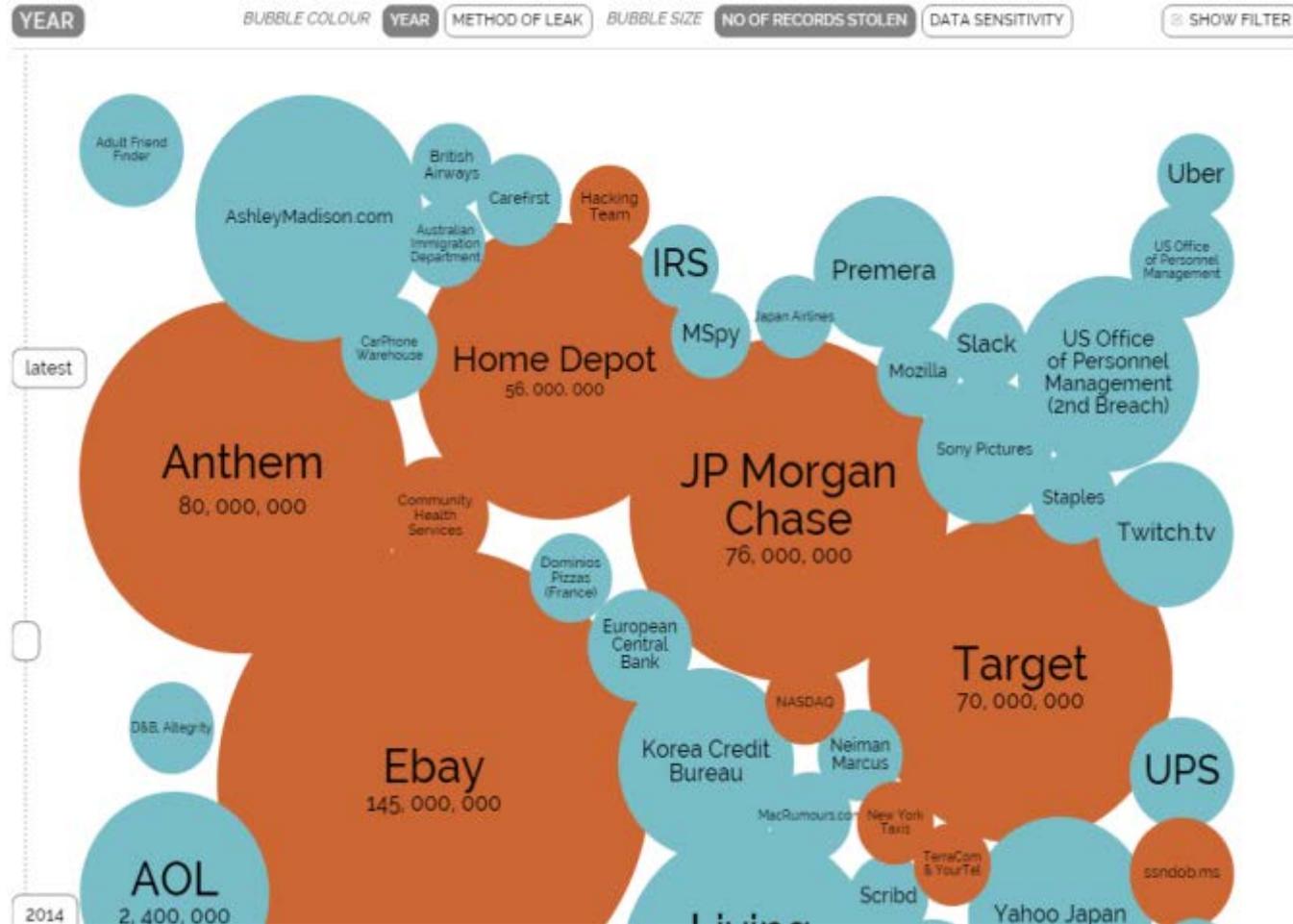
Figure 1. More sleepless nights for IT practitioners



* This response was not available for 2014

Is it safe?

- Consumers
 - Millions comprised
- Governments
 - US-OPM, IRS
 - State-CA, WA, FL
- Corporations
 - "...cannot ensure that we will be able to identify, prevent or contain the effects of additional cyber attacks...."



66%

CAGR of security incidents since 2004
CSO, Global State of Information Security, 2014

Each organization is unique, but not immune

Government:

- *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought* Sept 23, Washington Post

Commercial: 2014 Annual Report Excerpts

- **Major Retailer:**

- 10K-2012: To date, all incidents we have experienced have been **insignificant**.
- 10K-2013: ...data breach in ...2013 has resulted in government inquiries and private litigation...
- 10-K 2014: We have **recorded significant expenses** related to the Data Breach...

- **Major Healthcare Organization:**

- 10K-2012: ...our facilities and systems....**may be** vulnerable to cyber attacks.....
- 10K-2013: ...our facilities and systems....**are** vulnerable to cyber-attacks...
- 10K-2014: ...cannot ensure that we will be able to identify, prevent or contain the effects of additional cyber attacks....

A Data Focus

CUTTING THROUGH “THE FOG OF MORE”

- An overabundance of options for information security technologies and controls can make it painfully difficult for the security team in any given organization to sort through all the alternatives – and to make the necessary choices for the mix of controls that represents the best fit for their specific business context
- It can be tempting to [seek a shortcut](#), and simply use a technology that worked in one area as the solution for another
- Having **visibility, intelligence, and analytics** about your specific environment is the foundation for making smarter, more effective, risk-based decisions about technical controls

Sensitive Data Security is Key



Network Security



Host Security



Endpoint Security

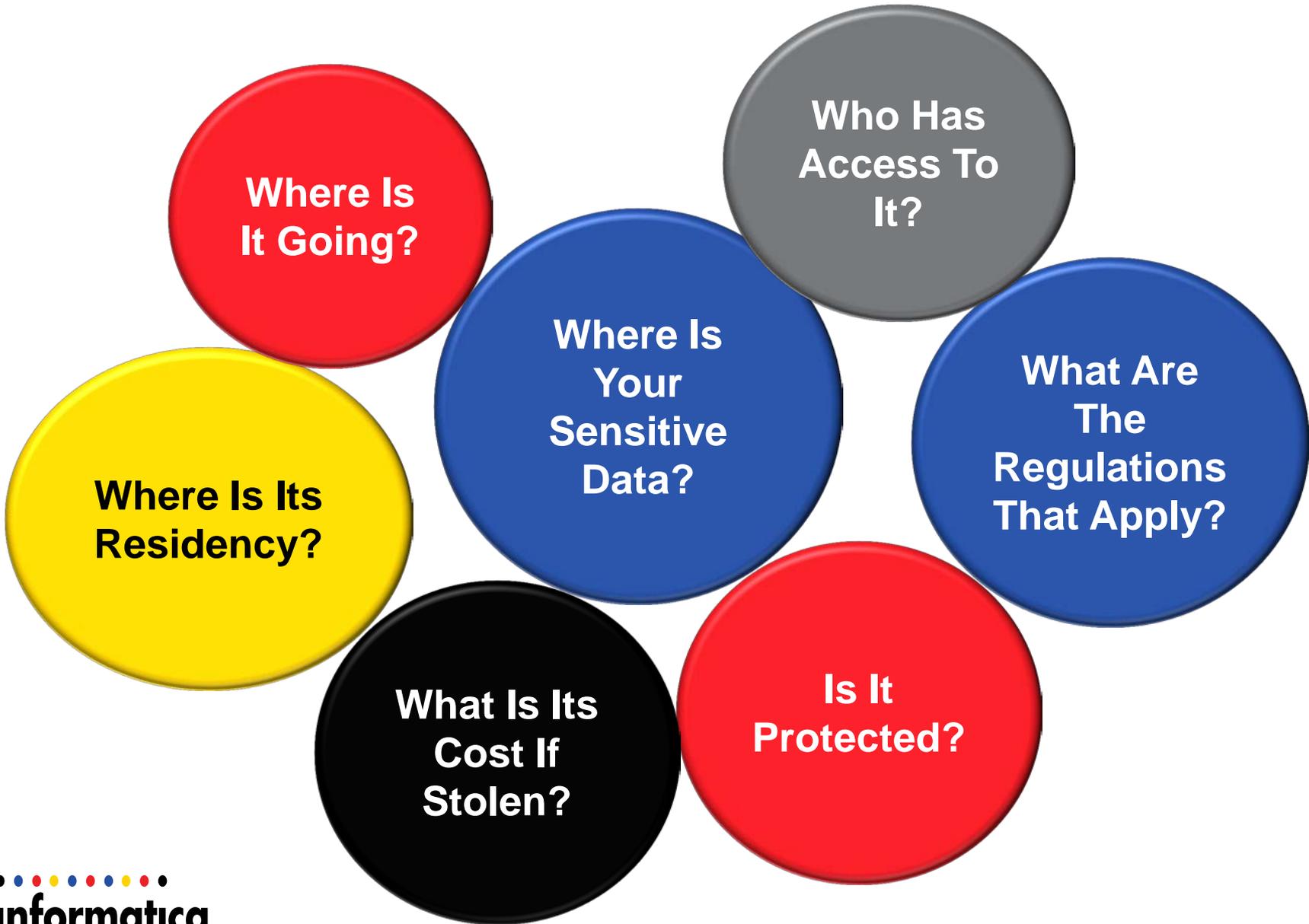
| STORE | | | PRODUCT | | |
|-----------|---------------|---------|-------------|-----------------------|-----------------|
| Store_key | City | Region | Product_key | Description | Brand |
| 1 | New York | East | 1 | Beautiful Girls | MKV Studios |
| 2 | Chicago | Central | 2 | Toy Story | Walt |
| 3 | Atlanta | East | 3 | Sense and Sensibility | Parabuster Inc. |
| 4 | Los Angeles | West | 4 | Holiday of the Year | Walt |
| 5 | San Francisco | West | 5 | Pulp Fiction | MKV Studios |
| 6 | Philadelphia | East | 6 | The Juror | MKV Studios |
| .. | .. | .. | 7 | From Dusk Till Dawn | Parabuster Inc. |
| .. | .. | .. | 8 | Heisenberg: Bloodline | Big Studios |
| .. | .. | .. | 9 | .. | .. |
| .. | .. | .. | .. | .. | .. |

| SALES_FACT | | | | |
|------------|-------------|-------|------|--------|
| Store_key | Product_key | Sales | Cost | Profit |
| 1 | 6 | 2.39 | 1.15 | 1.24 |
| 1 | 2 | 16.7 | 6.91 | 9.79 |
| 2 | 7 | 7.16 | 2.76 | 4.40 |
| 3 | 2 | 4.77 | 1.84 | 2.93 |
| 5 | 3 | 11.93 | 4.59 | 7.34 |
| 5 | 1 | 14.31 | 5.51 | 8.80 |
| .. | .. | .. | .. | .. |
| .. | .. | .. | .. | .. |



Data Centric Security

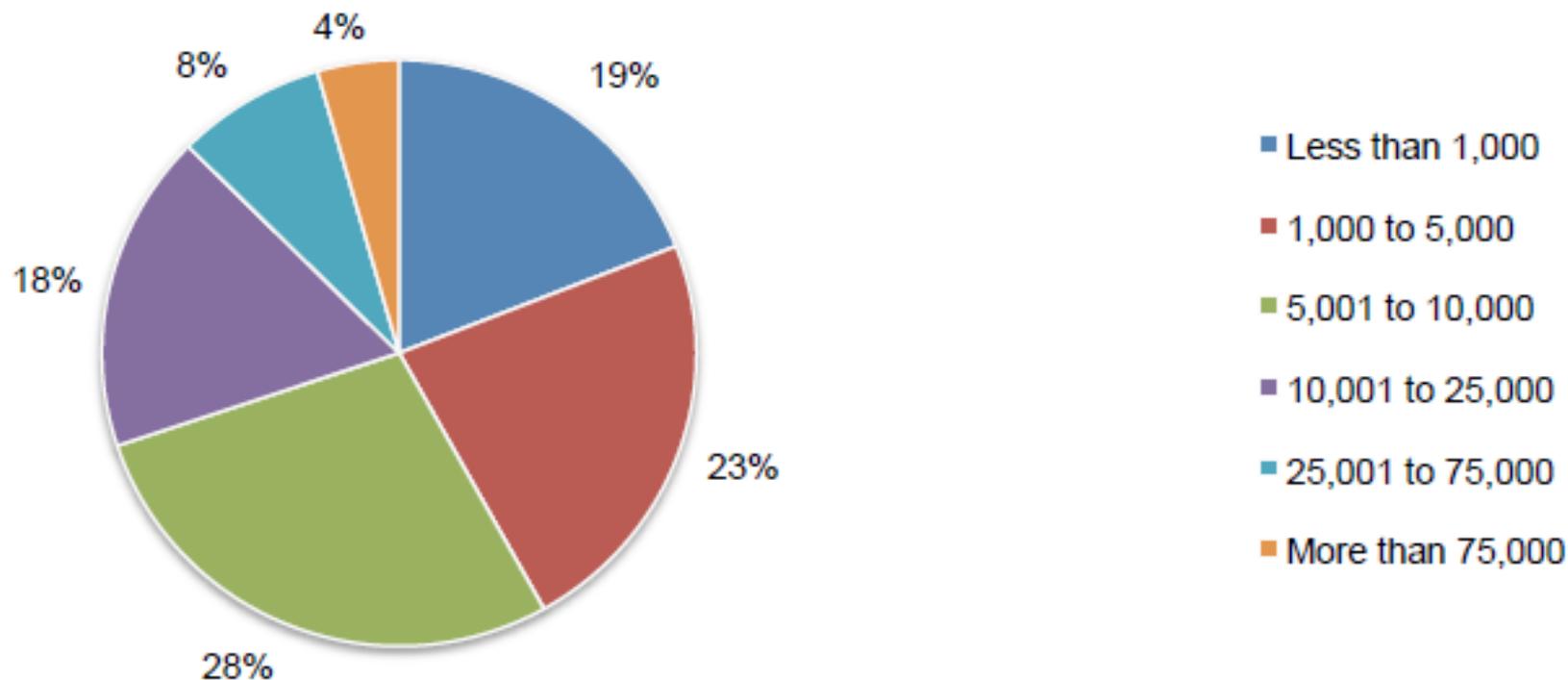
We need Insights to Manage Sensitive Data Risks



Structured DB Footprint

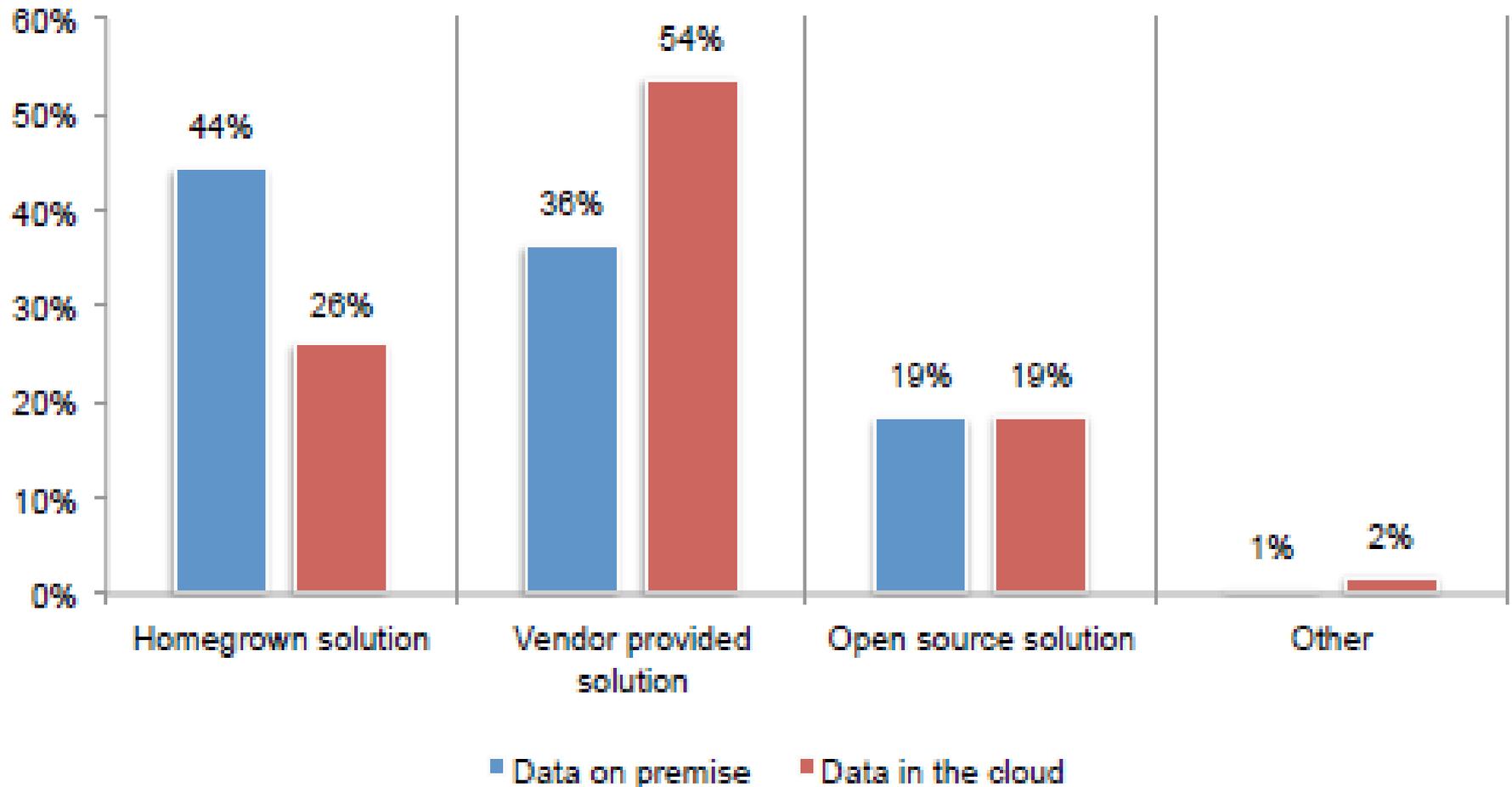
Pie Chart 5 reveals the number of databases that are in use within the organization. More than half of respondents (58 percent) report having more than 5,000 databases in use.

Pie Chart 5. Databases in use within the organization



Sensitive Data Risk: Manual Efforts

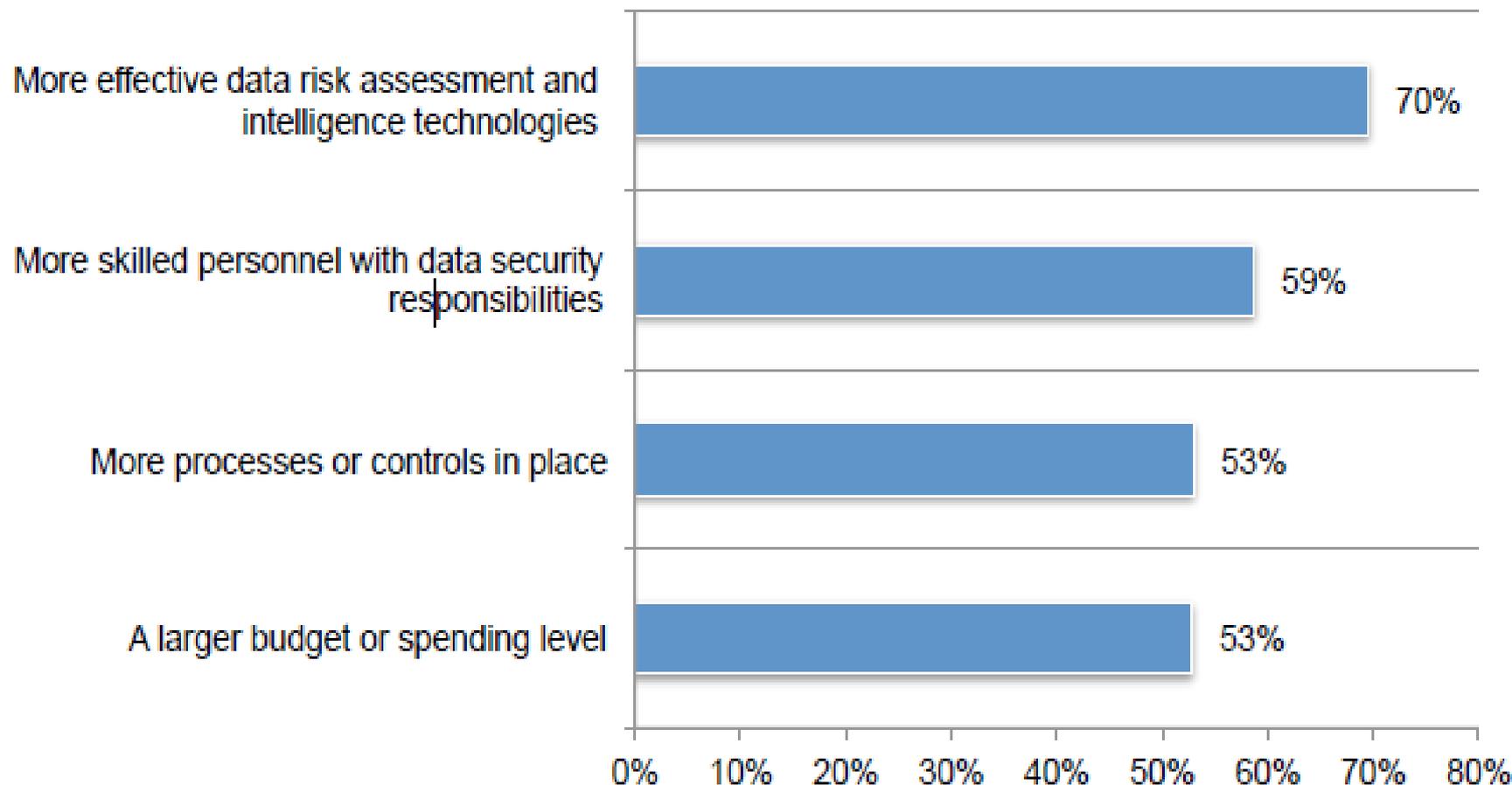
Figure 4. Solutions used for assessing the risks to sensitive or confidential data



What would work?

Figure 7. How could organizations have avoided the data breach incidents they experienced in the last 12 months?

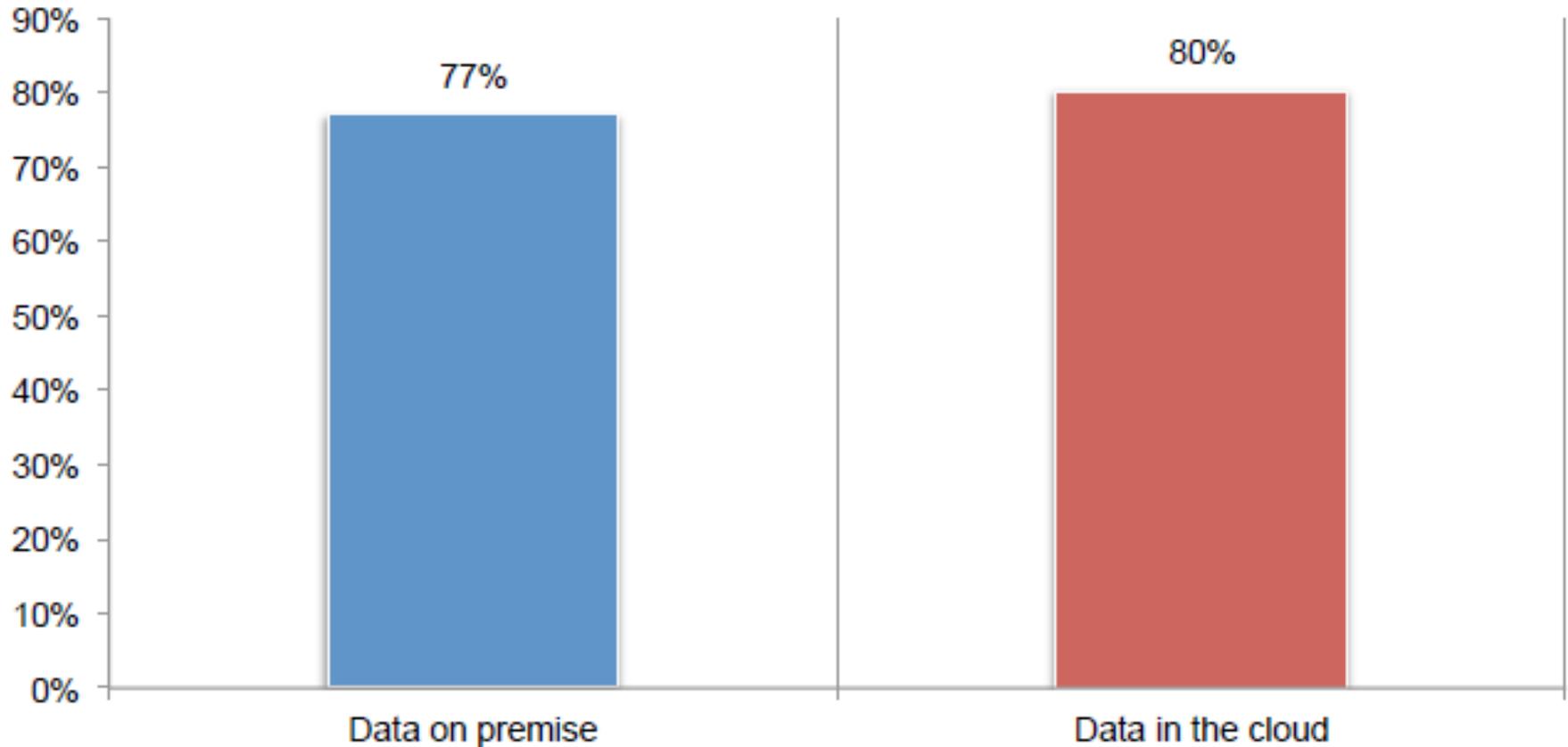
Very likely and likely responses combined



Would automation help?

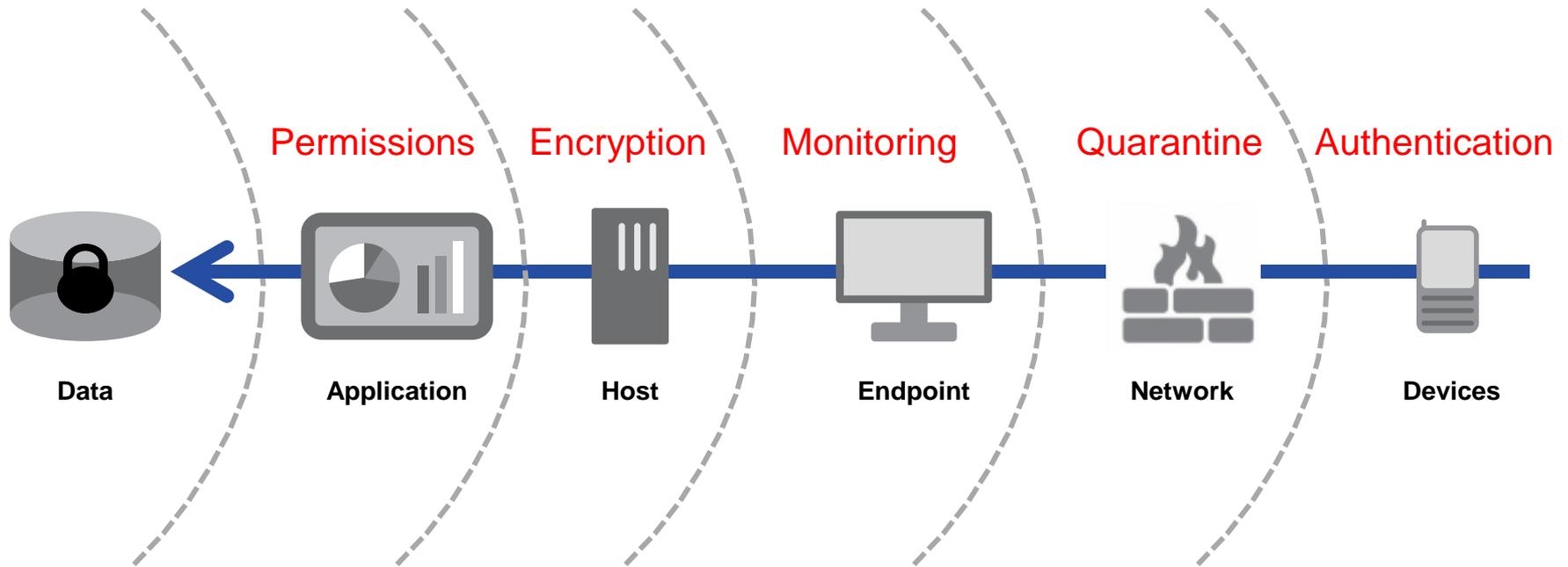
Figure 10. Would automated solutions increase the effectiveness of your data security activities?

Yes response



Data Centric Security

Security at Every Layer...



...and yet your data is still at risk

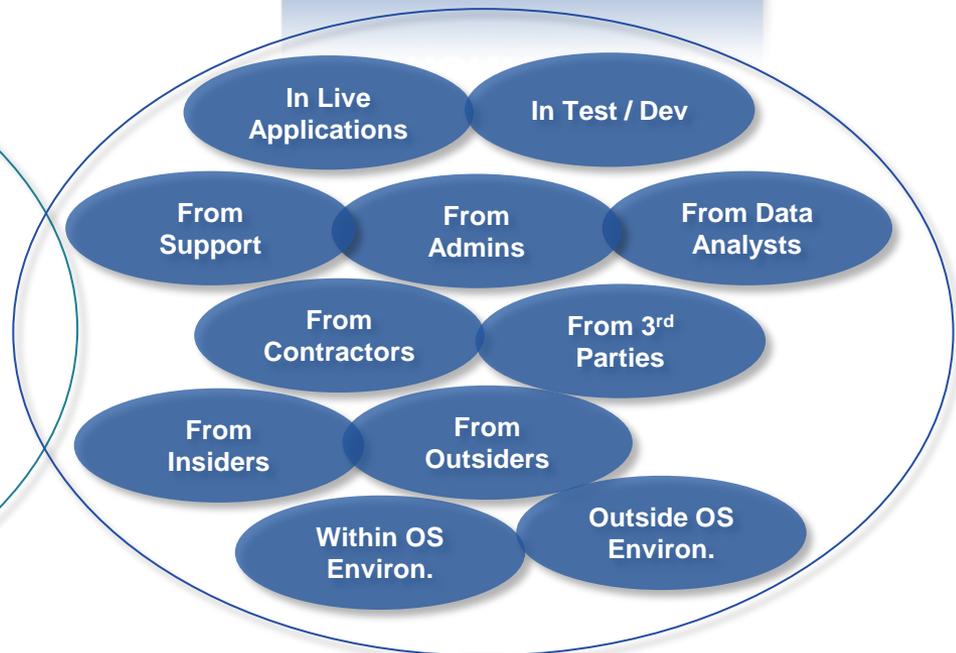
Sensitive Data Challenges



Understanding of Sensitive Data



Protection of Sensitive Data

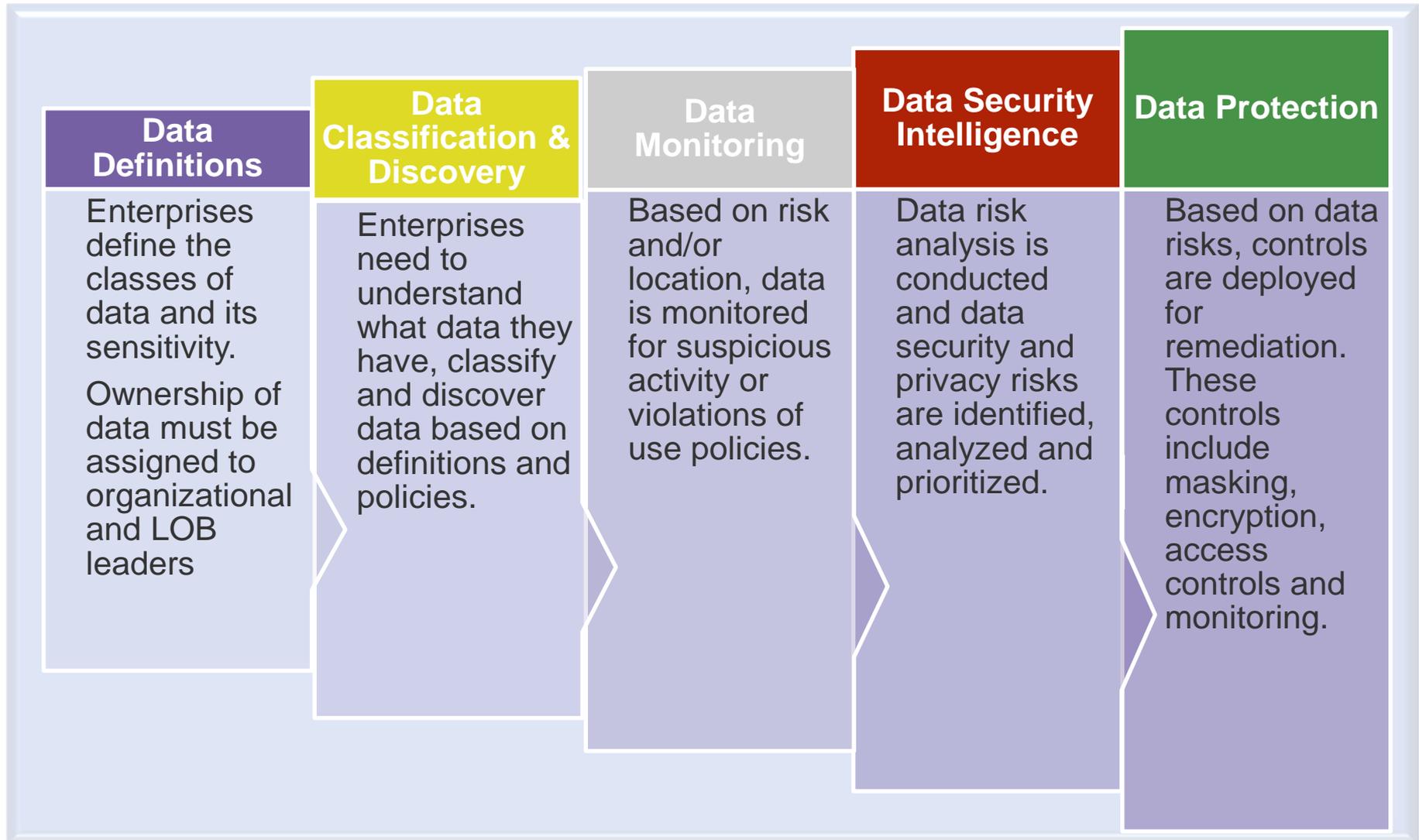


Data-Centric Security

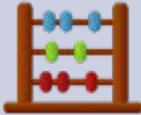
- **Insights, context, and risk scoring of sensitive data**
- **Data protection for sensitive data in use, at rest and in motion**

Focus security investments on high risk data assets

Data Centric Security



Sensitive Data Risk Must Include Multiple Factors

| | |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|  | What is your definition of Sensitive Data? |
|  | Where is it in your environment? |
|  | How much of it do you have? |
|  | How does it move throughout your organization? |
|  | Is there any protection for it already in place? |
|  | Who or what is accessing it? |
|  | Do you have any existing policy governing it? |
|  | Are there combinations of your sensitive data that are more valuable than individual pieces? |

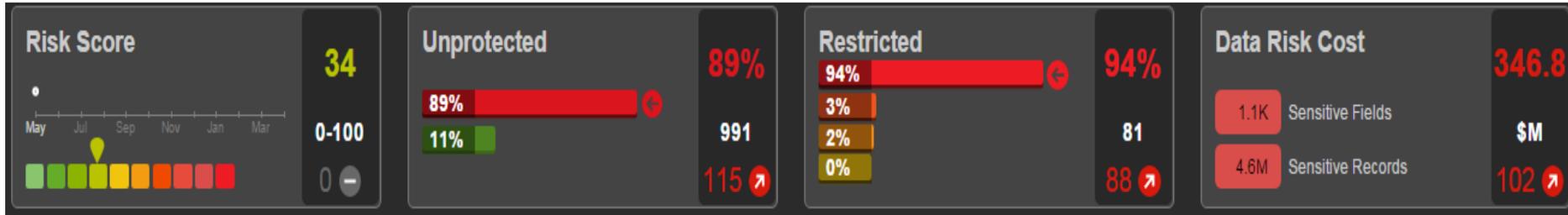
Sensitive Data Risk

- Enterprise-wide **sensitive data risk analytics**
- Sensitive data classification & discovery
- Proliferation analysis
- Policy-based alerting
- Integrates data security information from 3rd parties:
 - Data stores
 - Data owners
 - Classification
 - Protection status



Sensitive Data Risk

- Track risk of sensitive data with key risk indicators

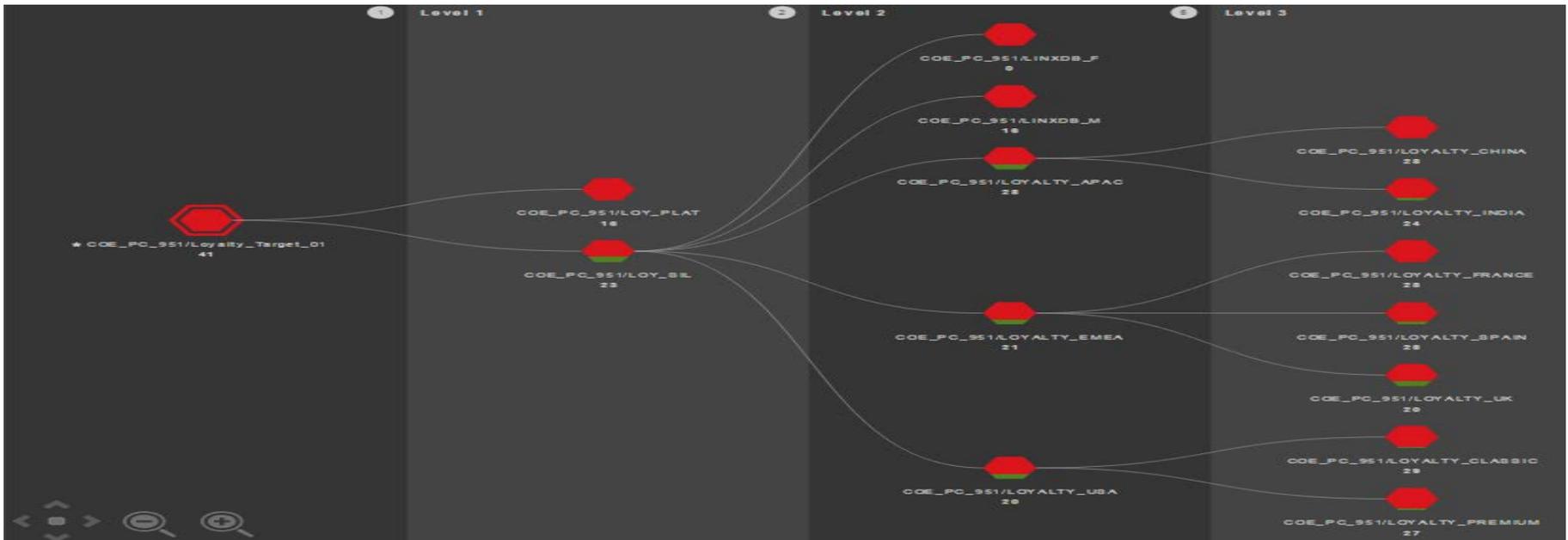


- Top level risk summations by department and locations



Sensitive Data Risk

- Data Proliferation Summary



Sensitive Data Protection

Data at Rest

(Inactive data stored physically in DBs, DWs, Spreadsheets, etc.)



Encryption

Persistent Data Masking

Tokenization

Data in Motion

(Data that is traversing a network or temporarily residing in memory to be read or updated)



Encryption (TLS/SSL)

Data In Use

(De-Identify, De-Sensitize, Anonymize.....Protect Data Used by Applications, Test, Outsourcing, BI and Reporting)



Dynamic Data Masking

Persistent Data Masking

Masking 101

Permanently or dynamically alter sensitive data

Variety of Techniques:

- Shuffle Employee ID's
- Substitute Names
- Constant for City
- Special Credit Card Technique

| ID | Name | City | Credit Card |
|------|---------------|-----------|---------------------|
| 0964 | Mike Vee | Singapore | 4417 9741 1949 9471 |
| 9388 | Mary Chew | Mumbai | 4981 1341 0854 0508 |
| 2586 | Rod Saunders | Bangkok | 4298 9341 9544 9114 |
| 7310 | Jeff Phillips | Mumbai | 4198 9481 9147 0521 |

Conclusions

- A new perimeter is needed: “Data Perimeter”
- Key to the data perimeter is Data Security Analytics/Intelligence
- The security and privacy landscape will continue to grow in challenges and complexity
- Data Centric Security Provides:
 - Risk assessment for data
 - Targeting of sensitive data protection....and other controls
 - Monitoring and audit of sensitive data

Award Winning Products



- 2015 Gold Award for Best New Security Product - **Informatica Secure@Source**
- 2014 Gold Award for Database Security - **Informatica Dynamic Data Masking**
- **Gartner 2014 Data Masking MQ: Leader**
- 2015, **Secure@Source** named “**Must Have**” Security Technology by CSO Online:





Virginia Information Technologies Agency

Upcoming Events





IS Orientation

When: Thursday, December 10, 2015

Time: 10:00 am to 12:00 pm

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?>

MeetingID=10



Future ISOAG

January 6, 1:00 - 4:00 pm @ CESC

**Speaker: Sarah Day, ATM
Investigations, ATM Fraud Task Force**

&

**James Lamatina, Special Agent,
US Secret Service**

ATM SKIMMING

ISOAG meets the 1st Wednesday of each month in 2015



Coming Events:

- Virginia Cyber Security Partnership
- Meeting topic: MALWARE
- Location: State Corporation Commission
 - Tyler Building
 - 1300 E. Main St.
 - Richmond, Virginia 23219
- December 10
- Registration: 7:30 am to 8:30 am
- Meeting: 8:30 am to noon



IS Security Conference 2016

“Securing the Commonwealth”

Save the Date: April 7 & 8, 2016

**Keynotes: Theresa Carlton, VP
Amazon Web Services**

**Eric O’Neil, Security Expert
Subject of the feature film
“The Breach”**

Registration website:

<http://www.vita.virginia.gov/itac/default.aspx?id=6442472001>

ADJOURN

THANK YOU FOR ATTENDING

