

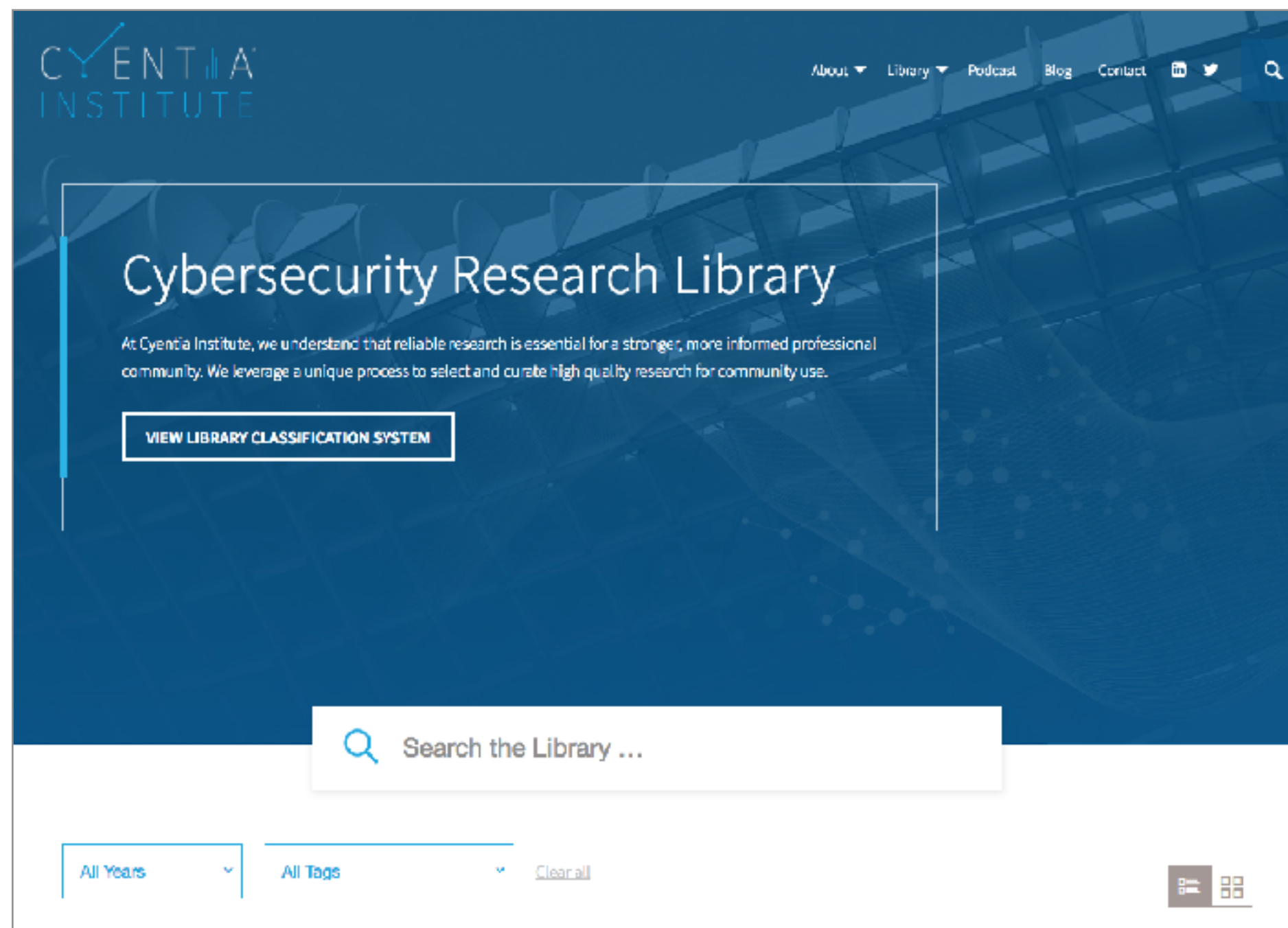
Data is Everywhere

Jay Jacobs
jay@cyentia.com

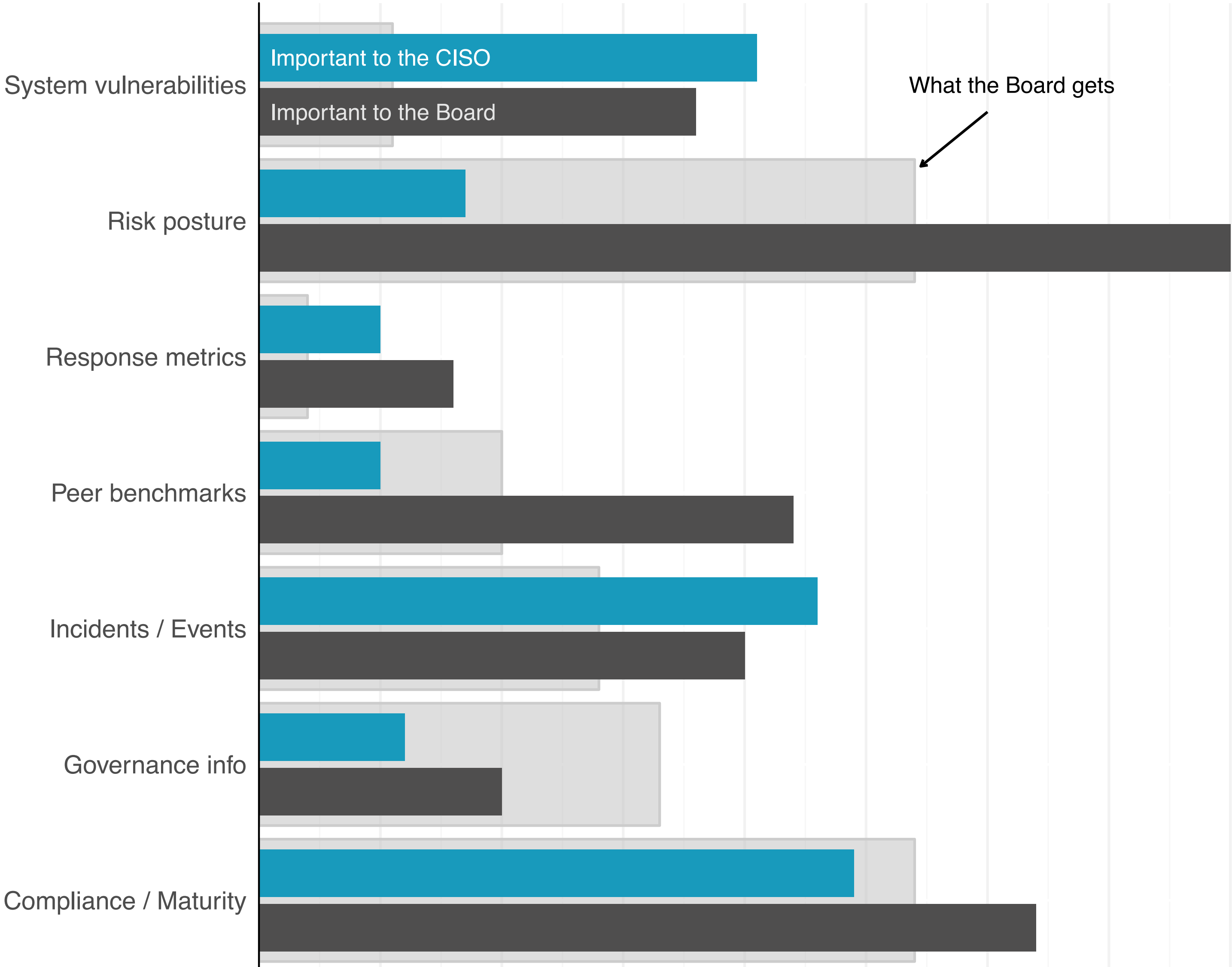
CY^{ENTIA}
INSTITUTE

Whatcha Been Doing?

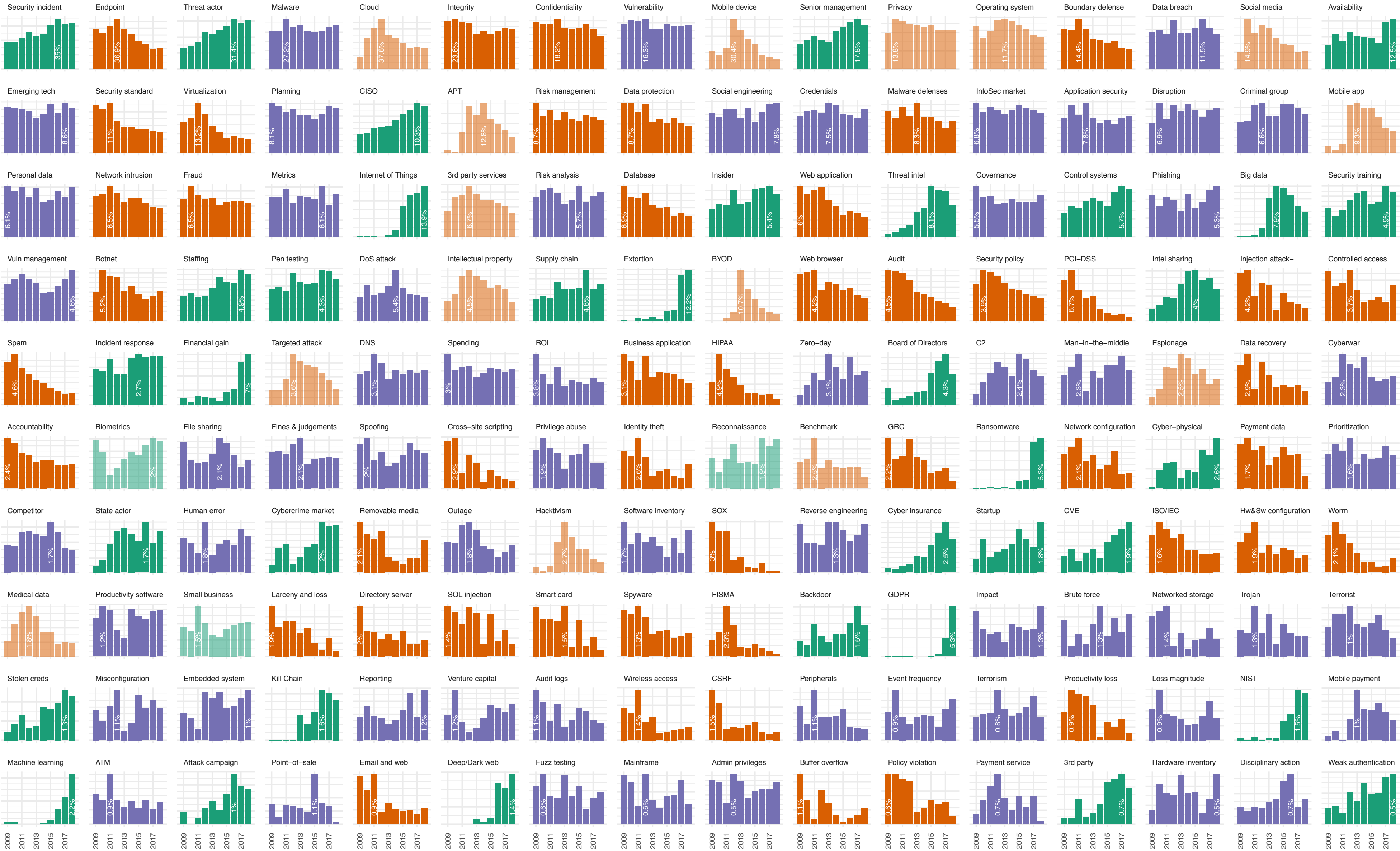
- (Mostly) Full-time with Cyentia Institute
- Conducting sponsored research
- Building Cyentia Library



Cyber Balance Sheet 2017



RSAC: Topics and Trends



STRIKING SECURITY GOLD

Uncovering hidden insights in a decade's worth of RSA Conference abstracts.

As the premier security conference in the world, RSA Conference offers an excellent lens through which to study the topics and trends within our industry. The Conference's slogan of "Where the World Talks Security" shows that's not just an accident. It's the goal.

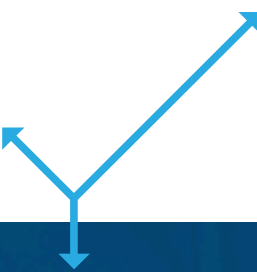
But what exactly do we talk about, when we talk "security"? That's the question we seek to answer in this report, which has its roots in a similar question asked by an eight-year-old daughter two and a half years ago: "What's the RSA Conference about, Daddy?" That root sprouted into a four-part blog series and a panel discussion a year later where we analyzed 25 years of session titles in honor of the 25th anniversary of RSA Conference.

To really study the question, however, titles provide limited value. They're often created to grab attention rather than impart information. Call for Paper (CFP) submissions, by comparison, are a veritable goldmine of details and insight about the sessions just waiting to be mined. Once again, RSA Conference was smart enough to supply the ore for our digital pickaxe. Did we strike gold and unearth valuable nuggets of insight about our industry? You'll have to read on to find out.

This report was produced by the Cyentia Institute, a research and analytics firm that specializes in security intelligence and provides thought leadership analysis. This content is provided for the community partner with vendors to create compelling research, and this information does not represent the views of the Cyentia Institute.

RSA Conference | Where the world talks security

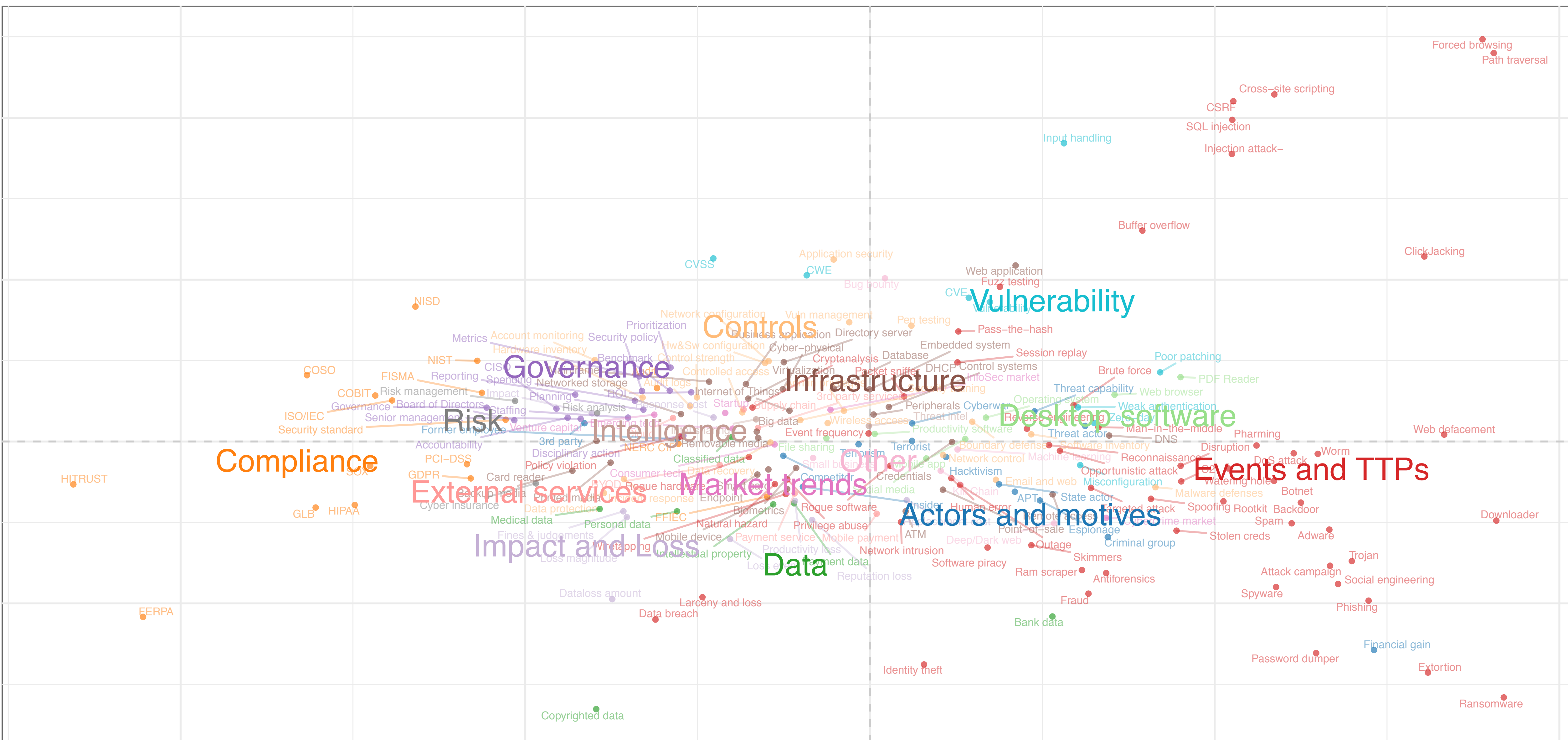
Source: Cyentia Institute with data from RSA Conference



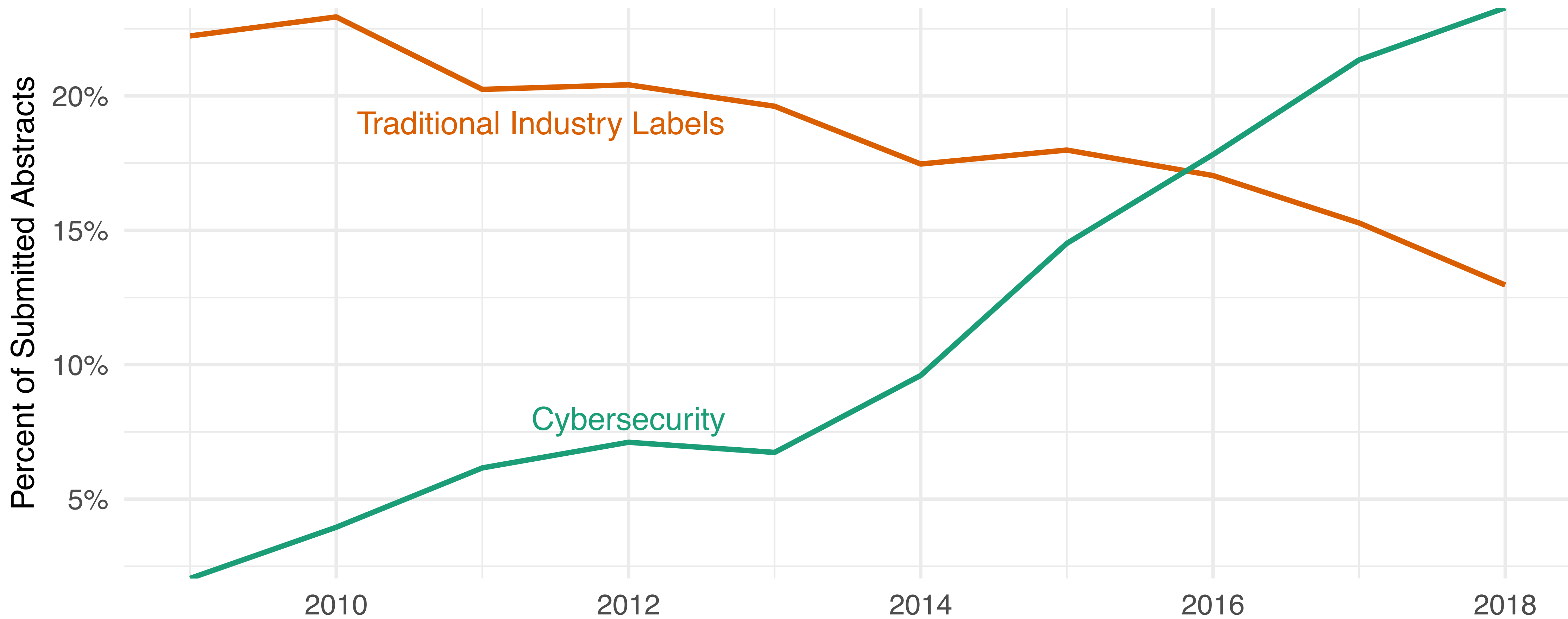
RSAC: Topics and Trends



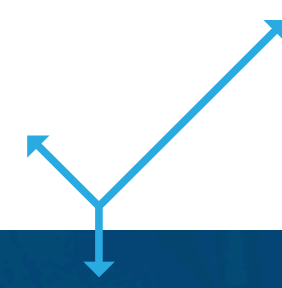
CYENTIA[®]
INSTITUTE



To Cyber or Not to Cyber?



Source: Cyentia Institute with data from RSA Conference

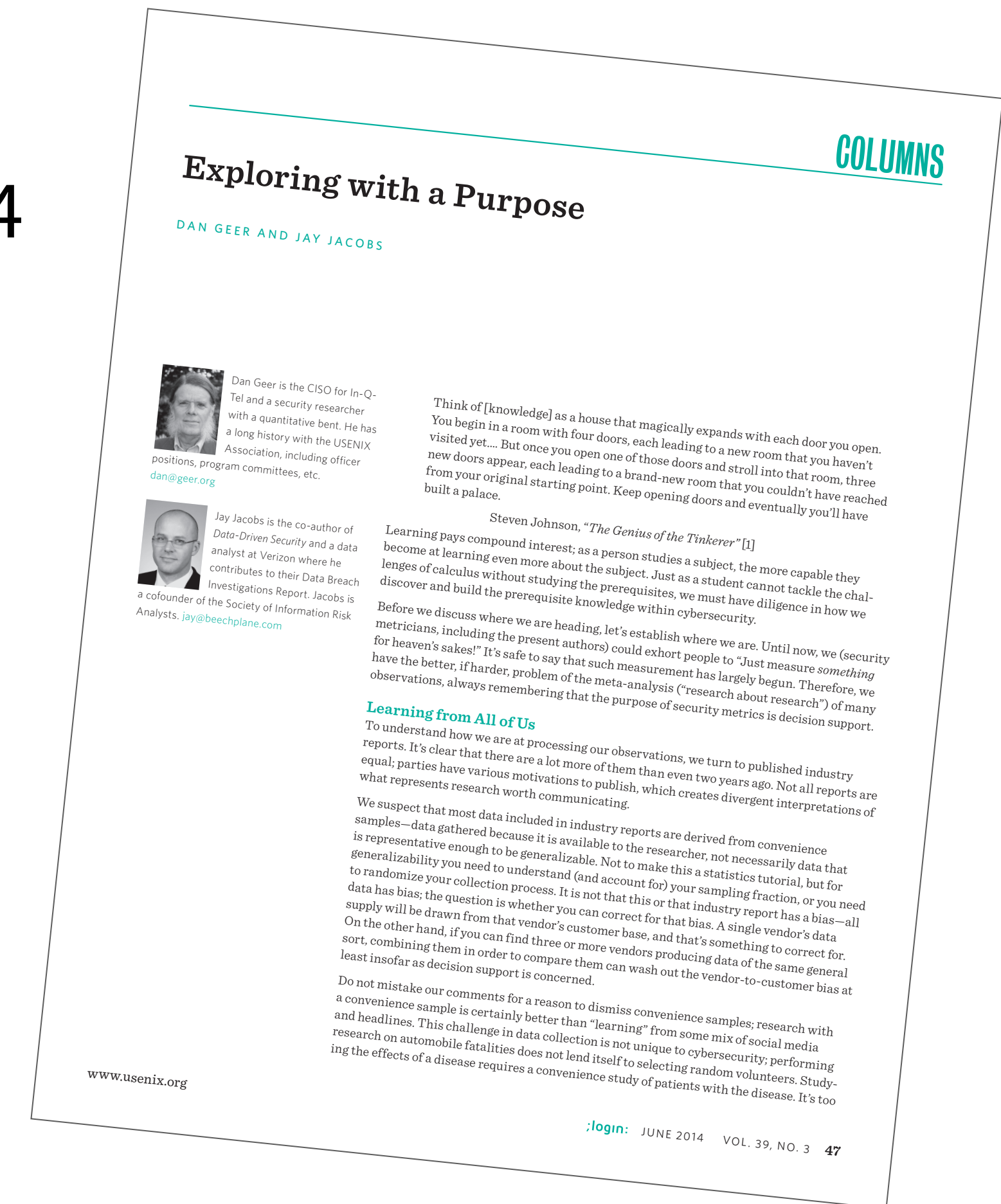


Where we are headed

“What we (the security metrics people) must now do is learn how to do meta-analysis in our domain...”

- Geer, Jacobs, 2014

1. Meta-Analysis and standing on the shoulders of giants: Cochrane Library
2. Case study: Ransomware
3. The Cyentia Library: present and future





Cochrane
Library

**Trusted evidence.
Informed decisions.
Better health.**

What is a systematic review?

A systematic review attempts to identify, appraise and synthesize all the empirical evidence that meets pre-specified eligibility criteria to answer a given research question. Researchers conducting systematic reviews use explicit methods aimed at minimizing bias, in order to produce more reliable findings that can be used to inform decision making. (See Section 1.2 in the ***Cochrane Handbook for Systematic Reviews of Interventions***.)

<http://www.cochranelibrary.com/>





Cochrane
Library

**Trusted evidence.
Informed decisions.
Better health.**

What is a systematic review?

A systematic review attempts to identify, appraise and synthesize all the empirical evidence that meets pre-specified eligibility criteria to answer a given research question.

findings that can be used to inform decision making. (See Section 1.2 in the *Cochrane Handbook for Systematic Reviews of Interventions*.)

<http://www.cochranelibrary.com/>



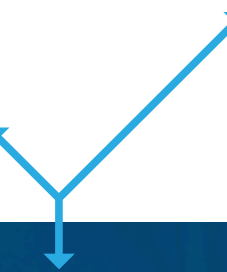
Systemic Reviews

A systematic review attempts to identify, appraise and synthesize all the empirical evidence that meets pre-specified eligibility criteria to answer a given research question.

Given a Research Question:

- Identify sources of evidence and information
- Appraise the quality of the evidence
- Synthesize and aggregate the evidence together (meta-analysis)

Research Question → Identify Sources → Appraise Quality → Synthesize Evidence



Developing Research Questions

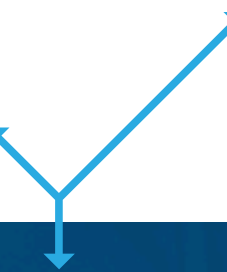
A great research question:

- ...is interesting
- ...can be supported by observation/evidence
- ...frames the object of measurement

Poor Research Questions	Better Research Questions
“How Secure is this web app?”	“What is the probability this web app will have a vulnerability exploited in the next 12 months?”
“What risks do we face?”	“What is the probability of these events occurring this year?”

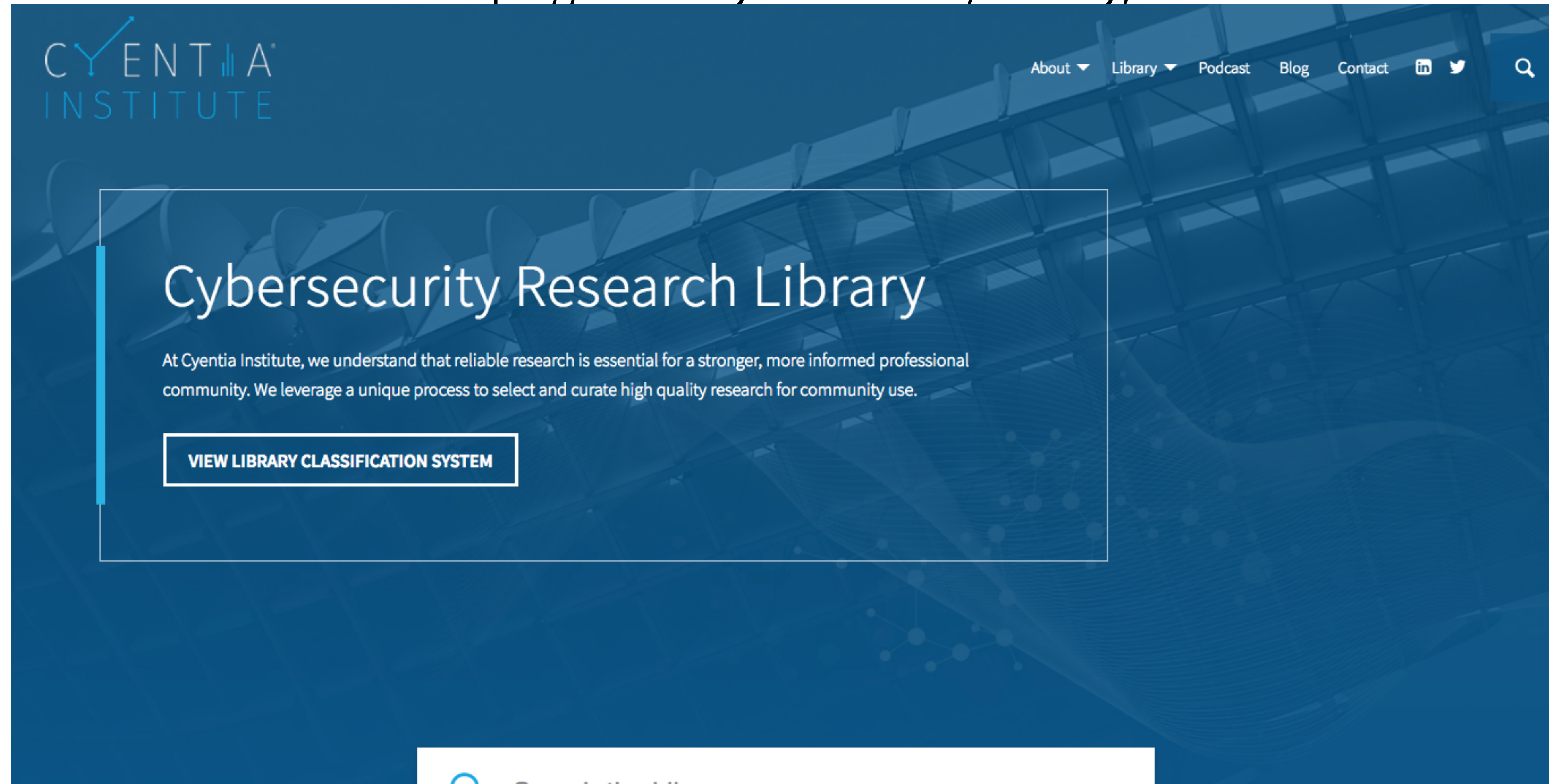
Breakdown broad topics into a series of research questions

Research Question → Identify Sources → Appraise Quality → Synthesize Evidence



Identify sources

<https://www.cyentia.com/library/>



Research Question → Identify Sources → Appraise Quality → Synthesize Evidence



Identify sources

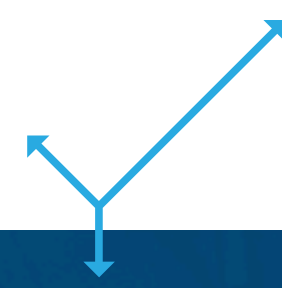
DDoS

All Years

All Tags

Clear all

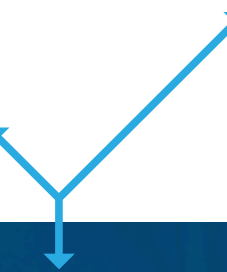
Cover	Name	Year	Type	Topic	Subtopic
	Verisign DDoS Trends Report Q1 2017	2017	Industry report	Information Assets, Security attributes, Threats	Actors and motives, Availability, Events and TTPs
	Neustar DDOS Attacks & Protection Report:North America	2015	Industry report	Controls, GRC Management, Impact and Loss, Market trends, Security attributes, Threats	Actors and motives, Availability, CIS "Top20" Controls
	State Of The Internet/Security Q4 2015 report	2015	Industry report	Controls, Information Assets, Security attributes, Threats	Actors and motives, Availability, Data
				Controls, Information	Actors and motives,



“Quality” is study-specific (survey vs collected data), but always contains:

1. Source of data, collection process (selection bias)
2. Sample size, sub-sample slices (sampling error)
3. Data Interpretation (e.g. statistics)

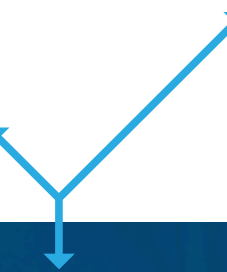
Appraising quality is subtle, complex and often subjective



A meta-analysis uses a statistical approach to combine the results from multiple studies in an effort to **increase power** (over individual studies), **improve estimates** of the size of the effect and/or to **resolve uncertainty** when reports disagree.

<https://en.wikipedia.org/wiki/Meta-analysis>

- Offset convenience samples
- Research in security is relatively simple: counts, proportions, means, etc.



Meta-Analysis: Combining Proportions

Think about picking marbles from an urn:

- First person picked 19 out of 50 red
- Second person picked 32 out of 75 red
- total: 51 out of 125 were red

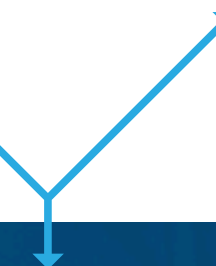
...Assuming the studies are drawing from the same “urn” or are representative of the same urn

Can visualize and talk about confidence in proportions with the **beta distribution**

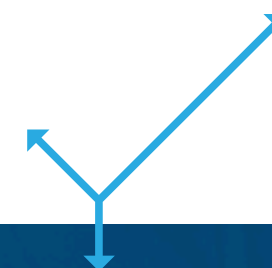
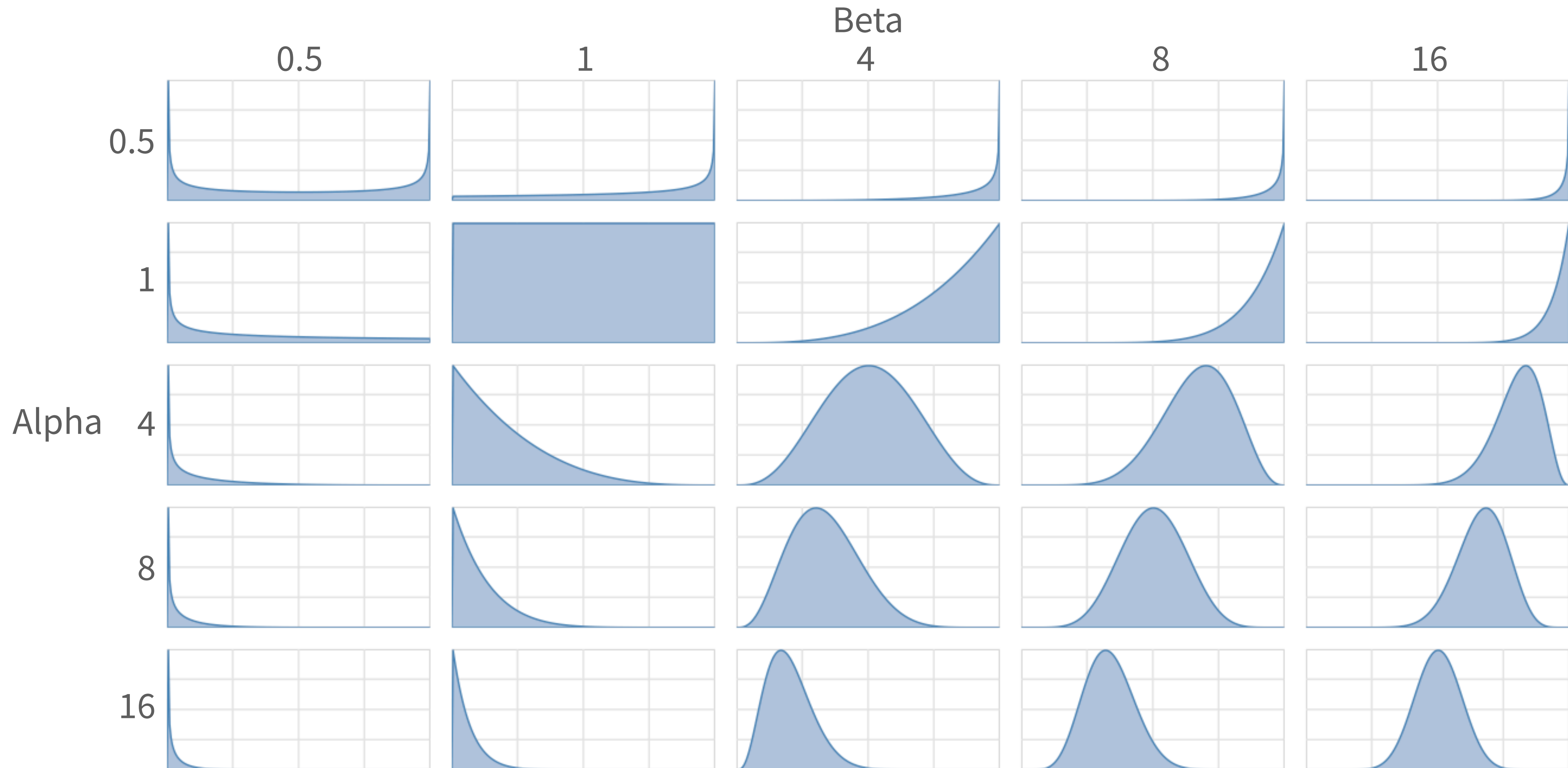


- “[The beta distribution] represents all the possible values of a probability when we don't know what that probability is.” - David Robinson, stats.stackexchange.com
- Basis for betaPERT, conjugate prior for bayesian inference
- Has two parameters: alpha (α) and beta (β)
 - α are counts of class 1 (success/heads/red/breached/infected)
 - β are counts of class 2
- 50 out of 250 machines infected with malware:

$$\text{beta}(\alpha=50, \beta=200)$$



Visualizing the Beta

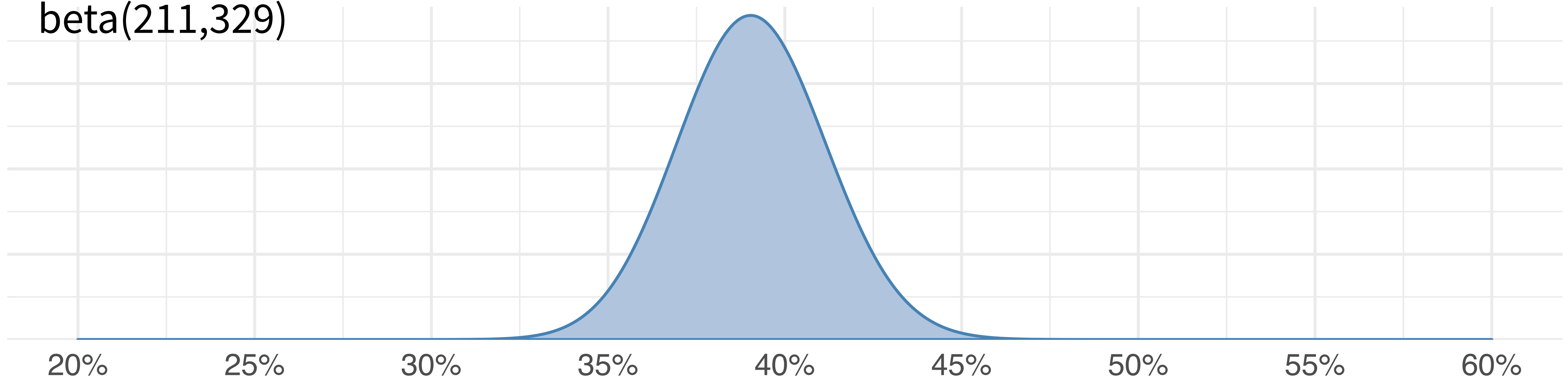


Applying the beta

- Osterman does a ransomware study and surveys 540 people
- Claims the “average ransomware penetration rate” is 39 percent
- How confident should we be about that 39%?

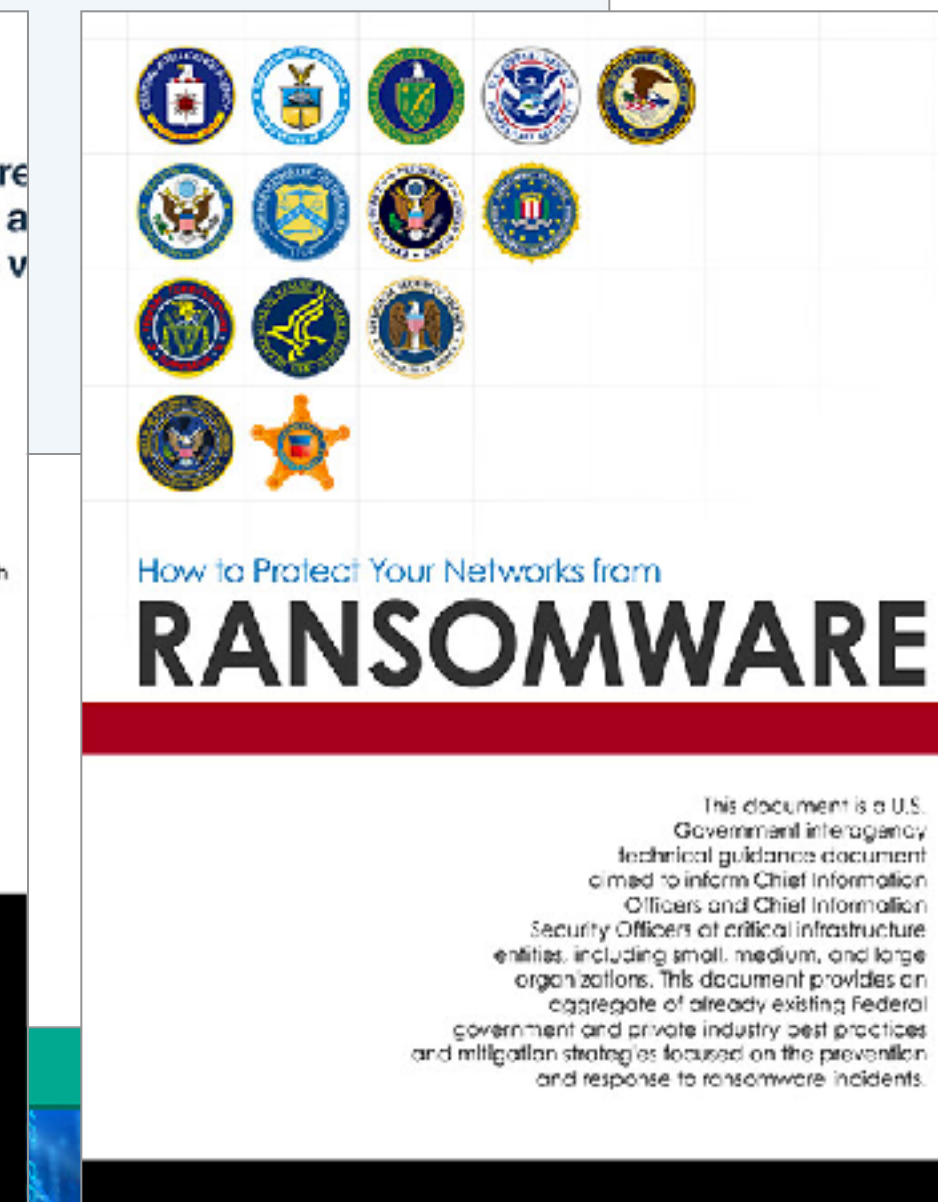
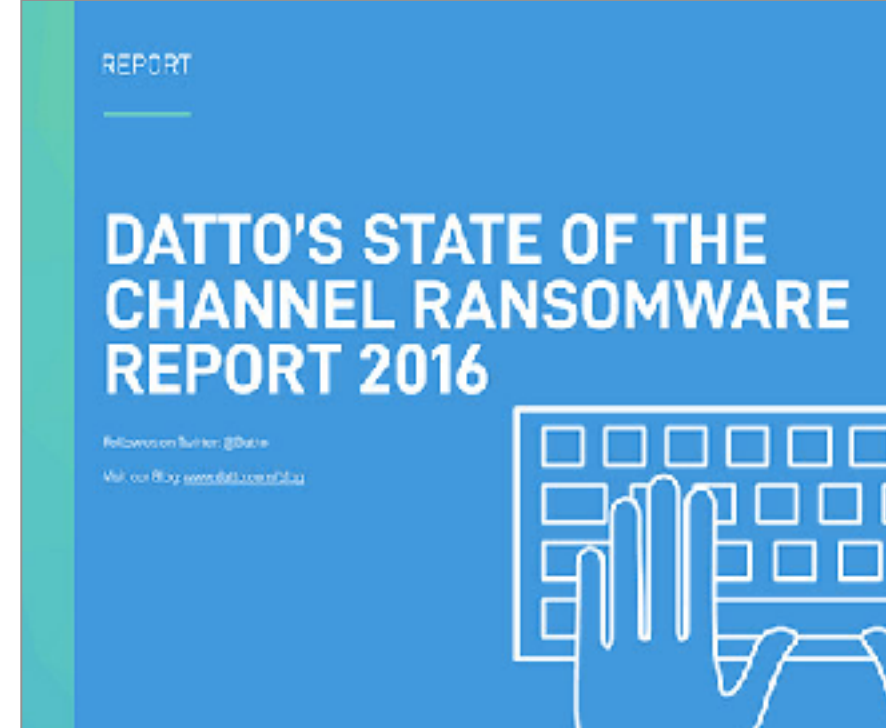
$540 * 0.39 = 211$ (but could be 208 to 213)

$\text{beta}(211, 329)$



Measuring Ransomware

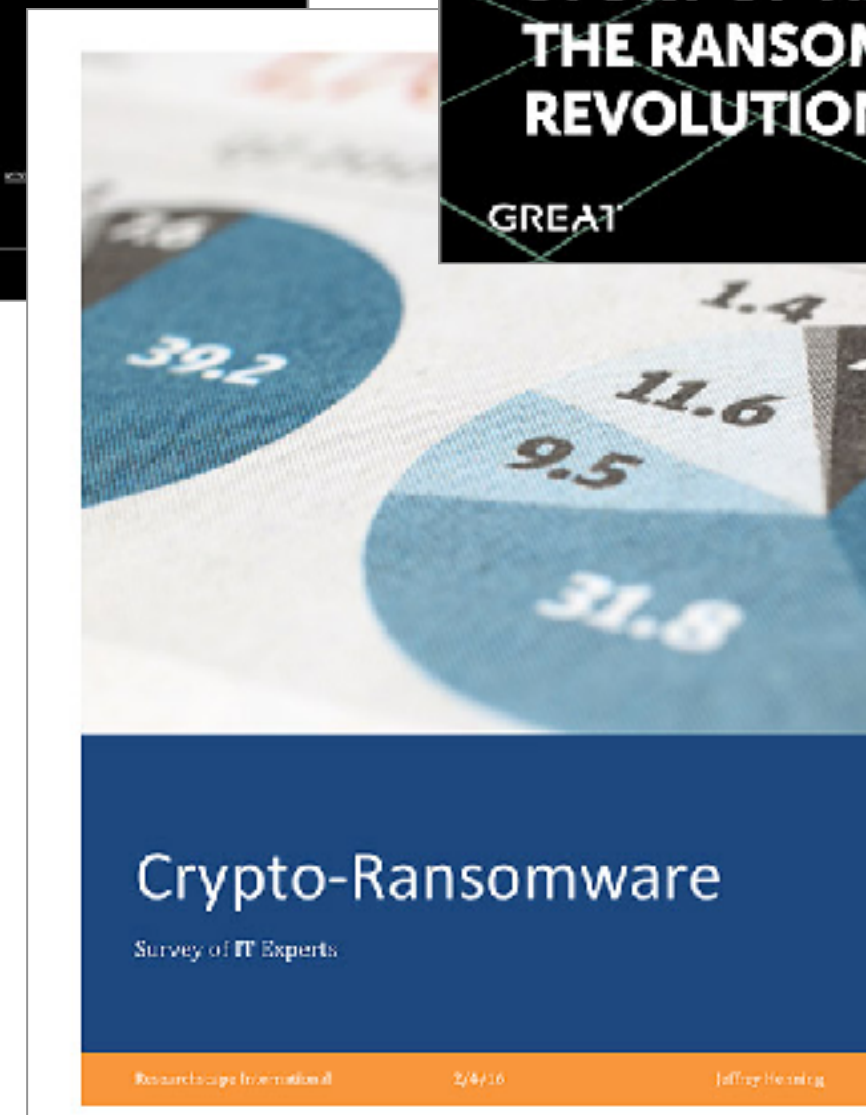
CYENTIA[®]
INSTITUTE



The Rise of Ransomware

Sponsored by Carbonite
Independently conducted by Pantheon Institute LLC
Publication Date: January 2017

Pantheon Institute Research Report



KSN Report: Ransomware in 2016-2017

www.kaspersky.com

Measuring Ransomware: The Setup

Three broad research questions

- How many orgs are affected by ransomware (prevalence)?
- How many orgs are paying the ransom amount (payment rate)?
- How much does ransomware cost (ransom amount)?

BSI, Ergebnisse der Umfrage zur Betroffenheit durch Ransomware (2016)

Fortinet, Q4 2016 Threat Landscape Report (2017)

IBM, Ransomware: How Consumers and Businesses Value Their Data (2016)

Kaspersky, Cost of Cryptomalware : SMBs at the Gunpoint (2016)

Osterman Research / Malwarebytes, Understanding the Depth of the Global Ransomware Problem (2016)

Ponemon Institute / Carbonite, The Rise of Ransomware (2017)

Symantec report (2012)

Dell Secureworks blog post (2013)

University of Kent study (2015)

BitDefender report (2016)

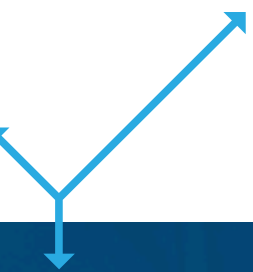
Datto report (2016)

Kaspersky - Consumer Security Risks (2016)

TrustLook blog post (2017)

Cisco Annual Security Report (2016)

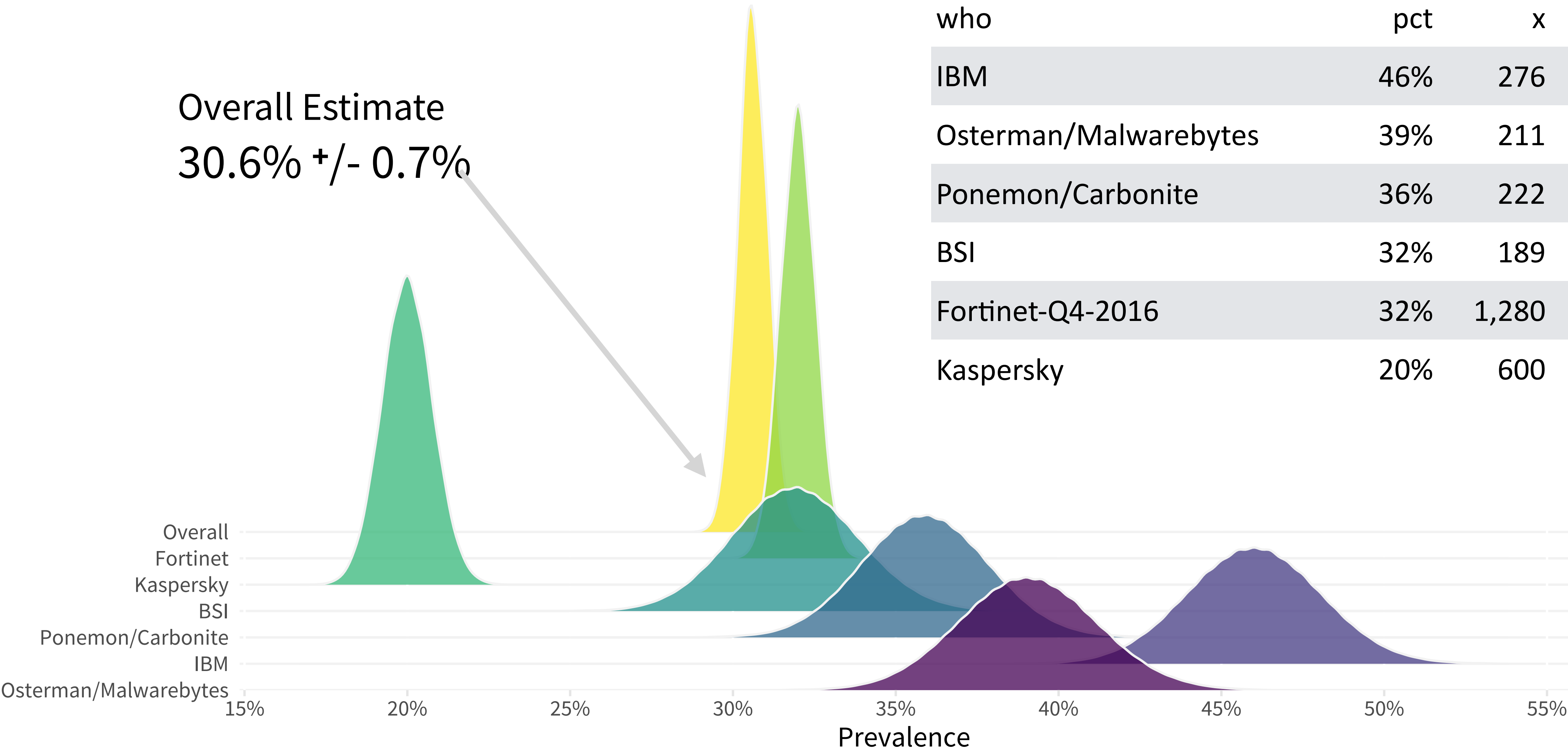
Cyber Extortion Risk Report, NYA International (2015)



Ransomware Prevalence

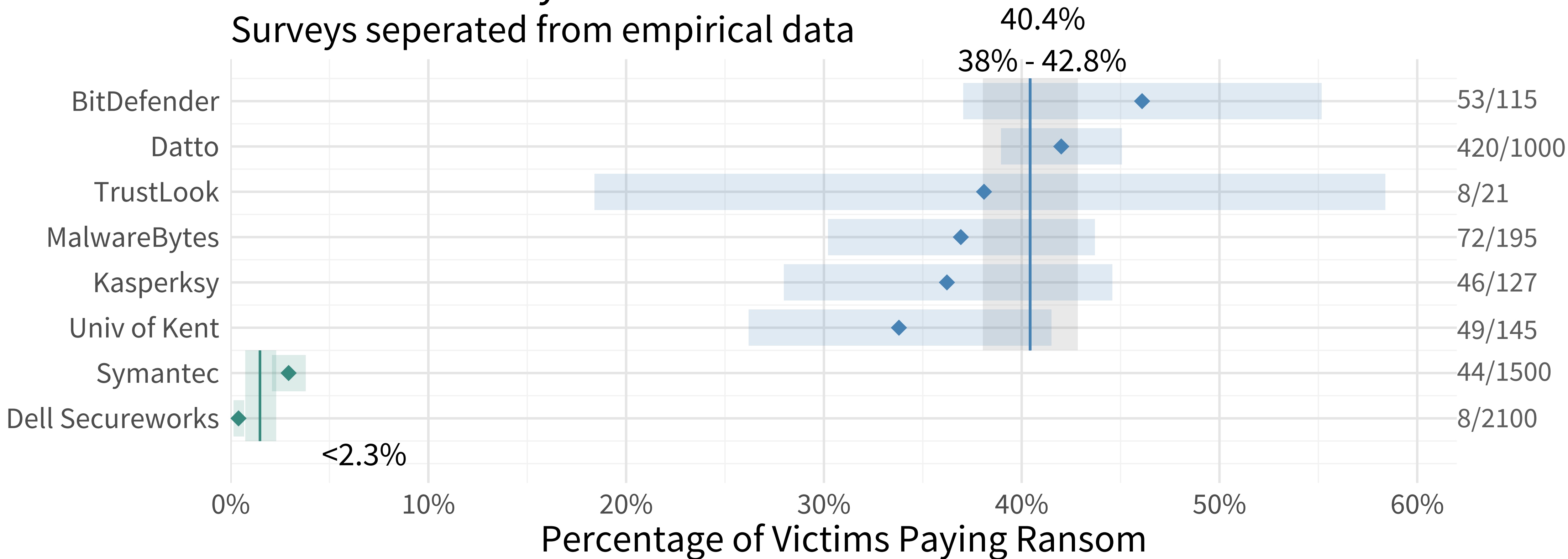
Overall Estimate
30.6% +/- 0.7%

who	pct	x	n
IBM	46%	276	600
Osterman/Malwarebytes	39%	211	540
Ponemon/Carbonite	36%	222	618
BSI	32%	189	592
Fortinet-Q4-2016	32%	1,280	4,000
Kaspersky	20%	600	3,000



How many orgs are paying?

Ransomware Payment Rate
Surveys seperated from empirical data



Source: Cyentia Institute

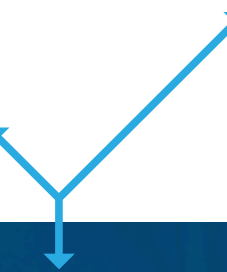




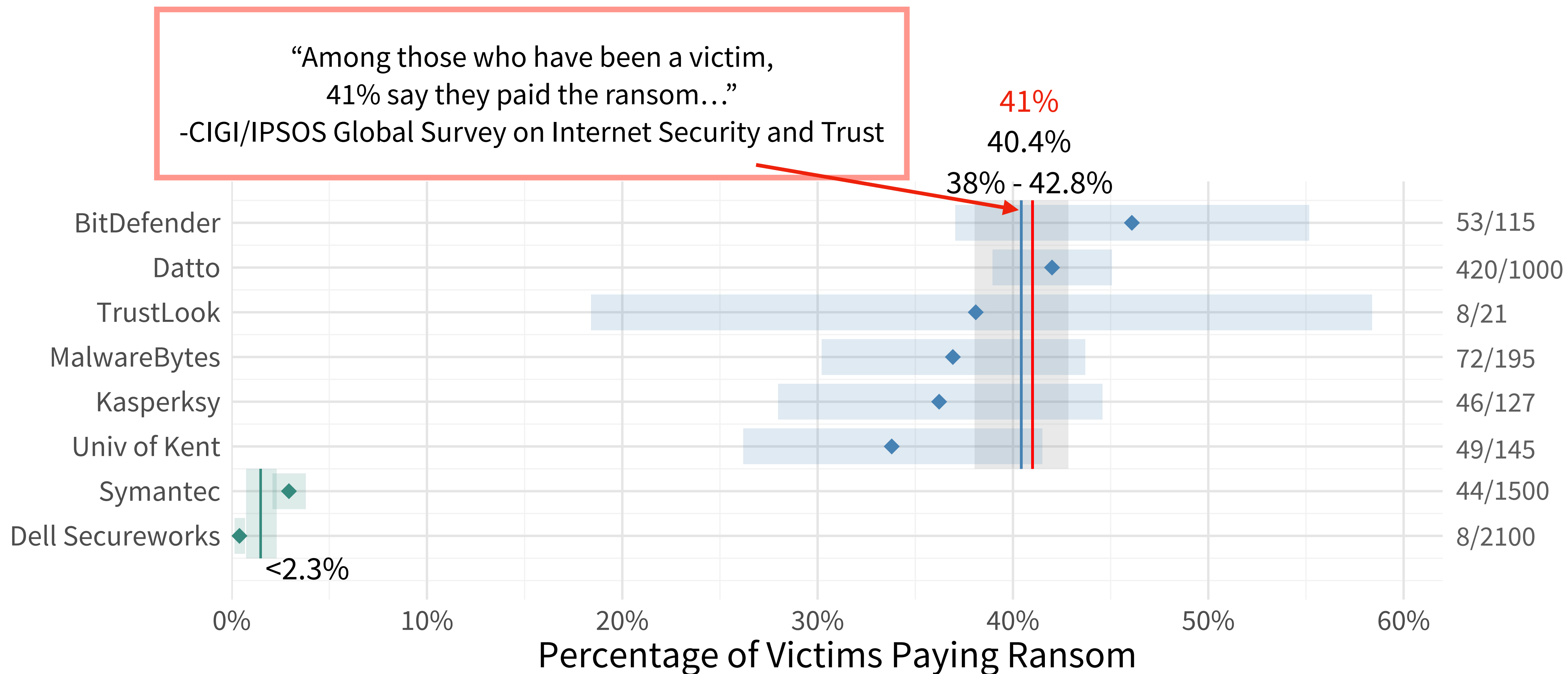
Methodology

- This survey was conducted by Ipsos on behalf of the Centre for International Governance Innovation ("CIGI") between December 23, 2016, and March 21, 2017.
- The survey was conducted in 24 economies—Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey and the United States—and involved 24,225 Internet users.
- Twenty of the countries utilized the Ipsos Internet panel system while Tunisia was conducted via CATI, and Kenya, Nigeria and Pakistan utilized face-to-face interviewing, given online constraints in these countries and the length
- In the US and Canada respondents were aged 18-64, and 16-64 in all other countries.
- Approximately 1000+ individuals were surveyed in each country and are weighted to match the population in each country surveyed. The precision of Ipsos online polls is calculated using a credibility interval. In this case, a poll of 1,000 is accurate to +/- 3.5 percentage points. For those surveys conducted by CATI and face-to-face, the margin of error is +/-3.1, 19 times out of 20.

- Early 2017 study
- 24,225 Internet users
- Across 24 countries (individual surveys conducted)
- Weighted to match population of country

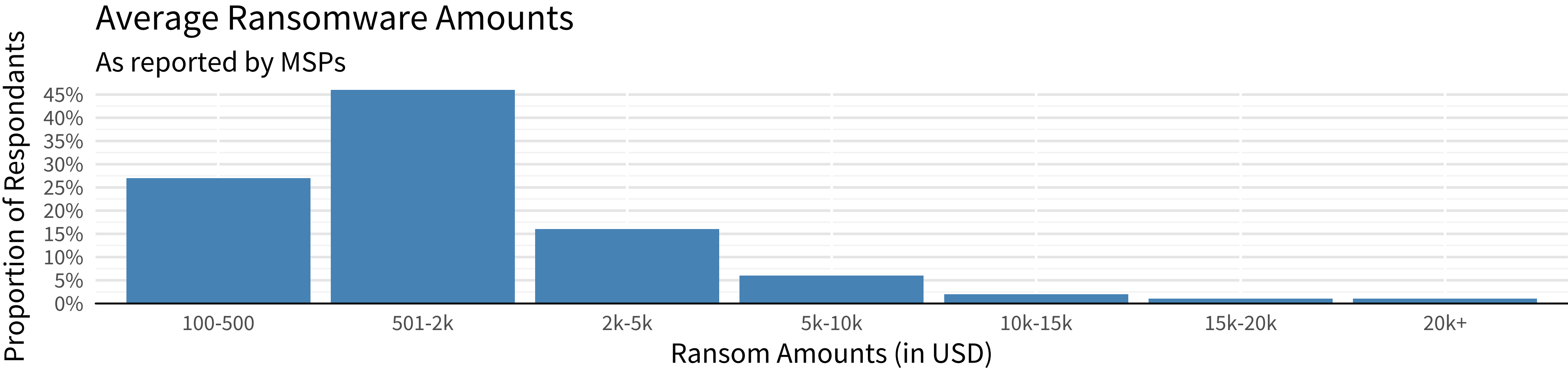


How many orgs are paying?

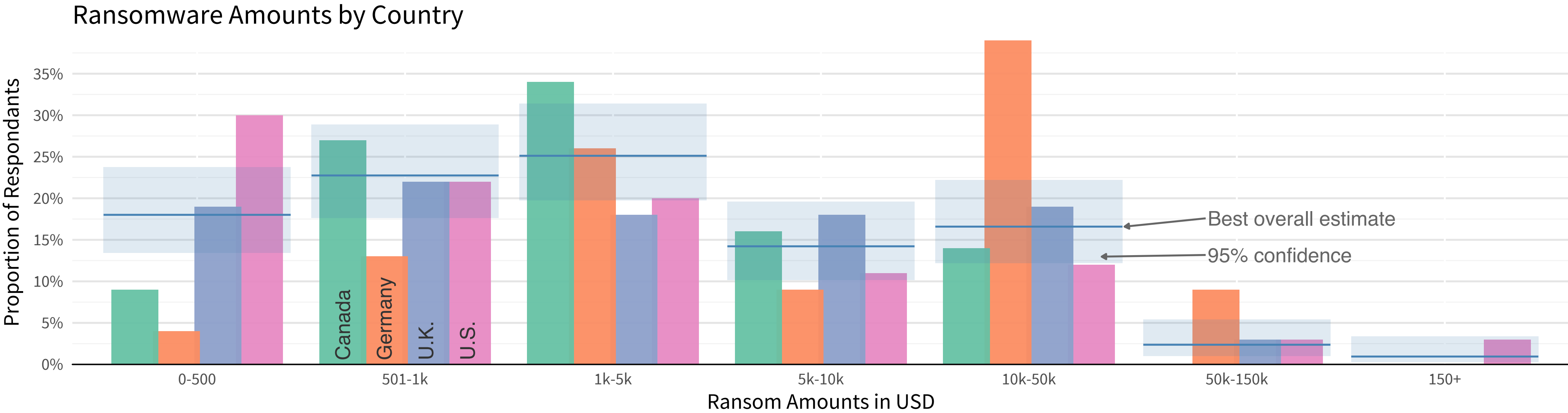


Source: Cyentia Institute

Ransom Amounts

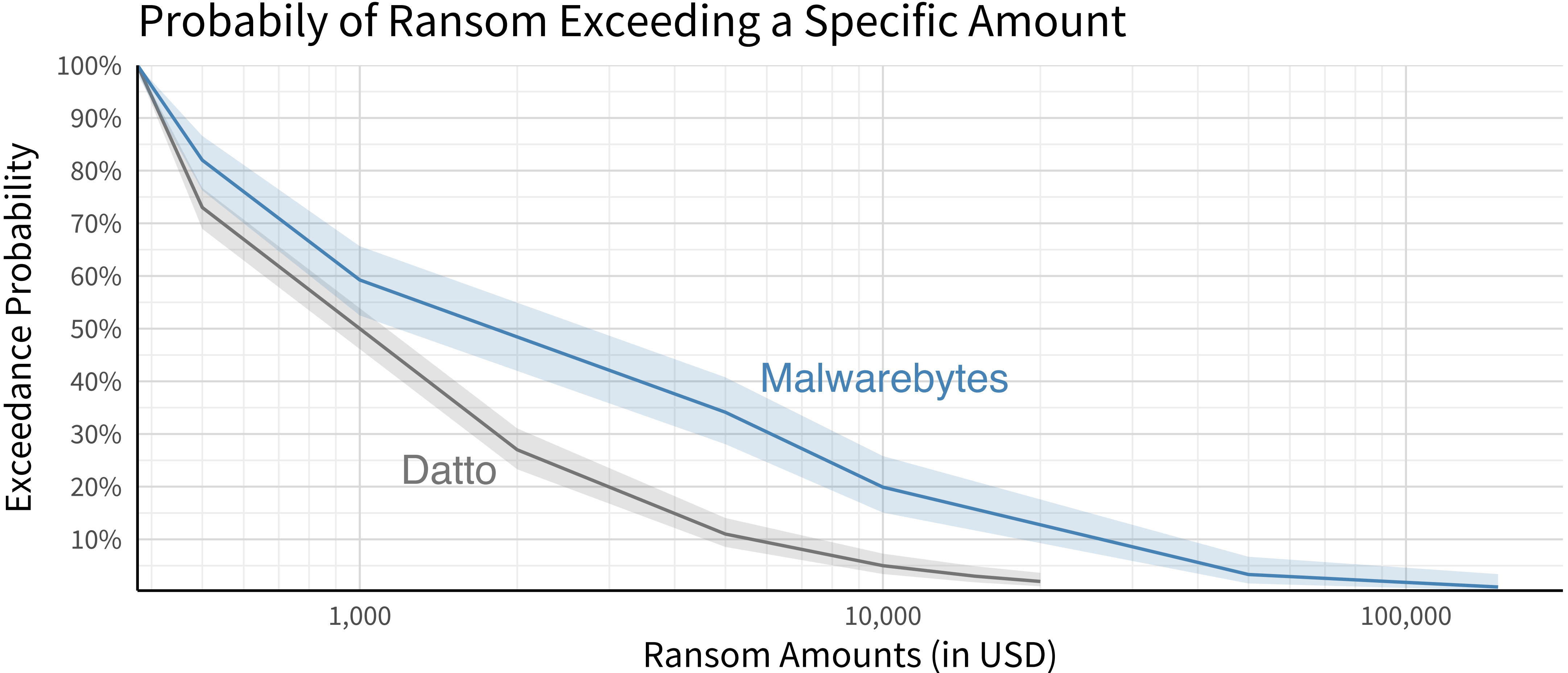


Source: Cyentia Institutue, data from:
Datto's State of the Channel Ransomware Report, 2016

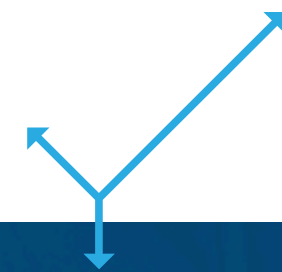


Source: Cyentia Institute, data from:
MalwareBytes/Osterman Research, "Understanding the Depth of the Global Ransomware Proble"

Exceeding Ransom Amount



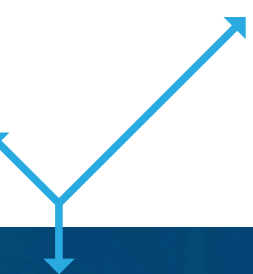
Source: Cyentia Instutue, data from:
MalwareBytes/Osterman Research, "Understanding the Depth of the Global Ransomware Problem",
Datto's "State of the Channel Ransomware Report 2016"



Challenges: Lessons Learned

- Experiment successful!
- While Library helped, identifying and narrowing down sources was a challenge **
- Quality of vendor reports was terrible, rejected 2 out 3 on average
 - “Not all reports are equal; parties have various motivations to publish, which creates divergent interpretations of what represents research worth communicating.” - Geer, Jacobs 2014*
- Very poor, circular or missing citations
- Terminology is loose and/or confusing
- Object of measurement and framing is muddled or misaligned
- ...is Ponemon: 51% (perception), 36% (included), 1.2% (excluded on wording)
- Getting a simple sample size shouldn't be this hard
- Synthesizing the evidence was relatively straight-forward.

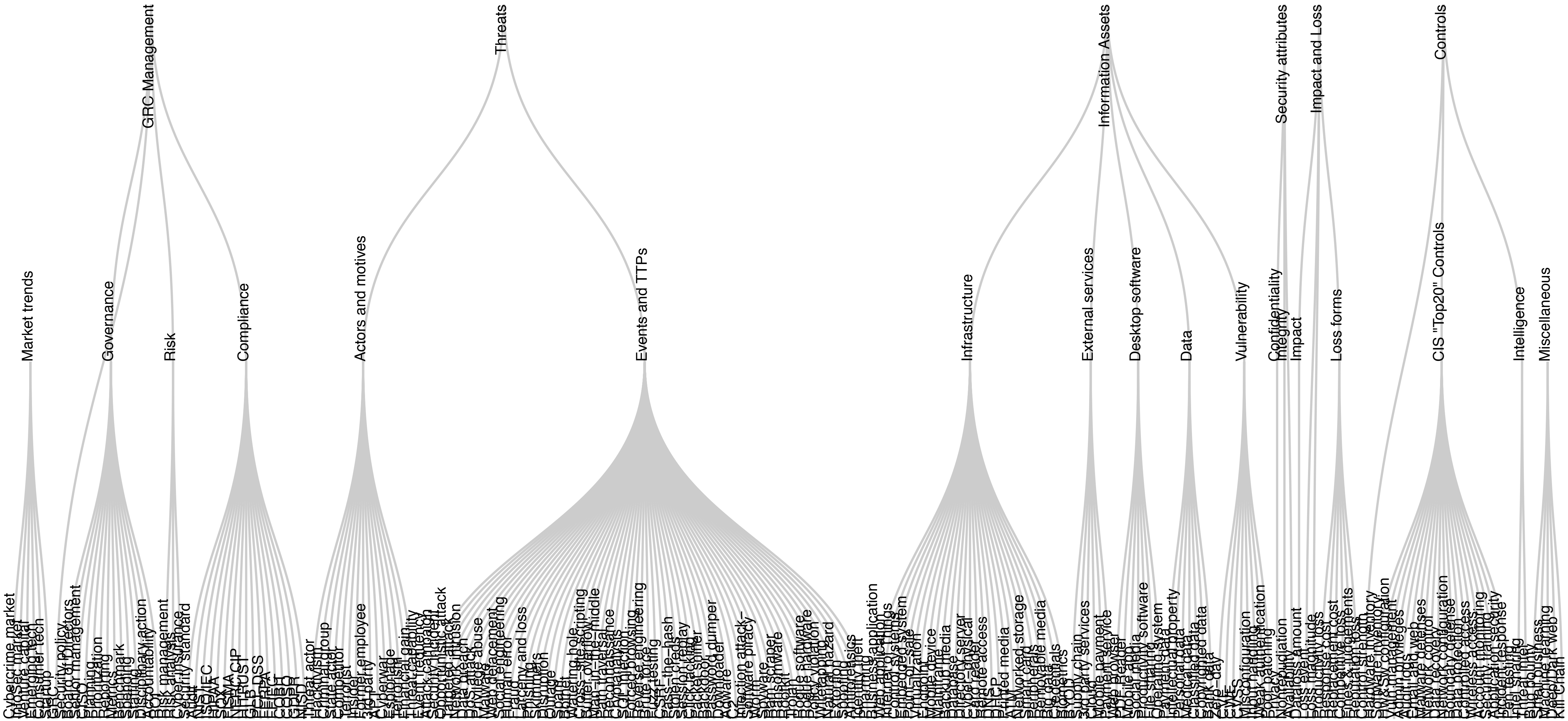
** ...that we can improve



Cyentia Library: Present and Future

CYENTIA[®]
INSTITUTE

Cyentia Library Tagging



CYENTIA[®]
INSTITUTE

The diagram illustrates the flow of information and influence between various market trends and governance factors. The diagram is divided into three main sections: Market trends, Governance, and GRC Management.

Market trends (Left):

- Cybercrime market
- Virtual Sec market
- Venture capital
- Emerging tech
- Startup
- AI

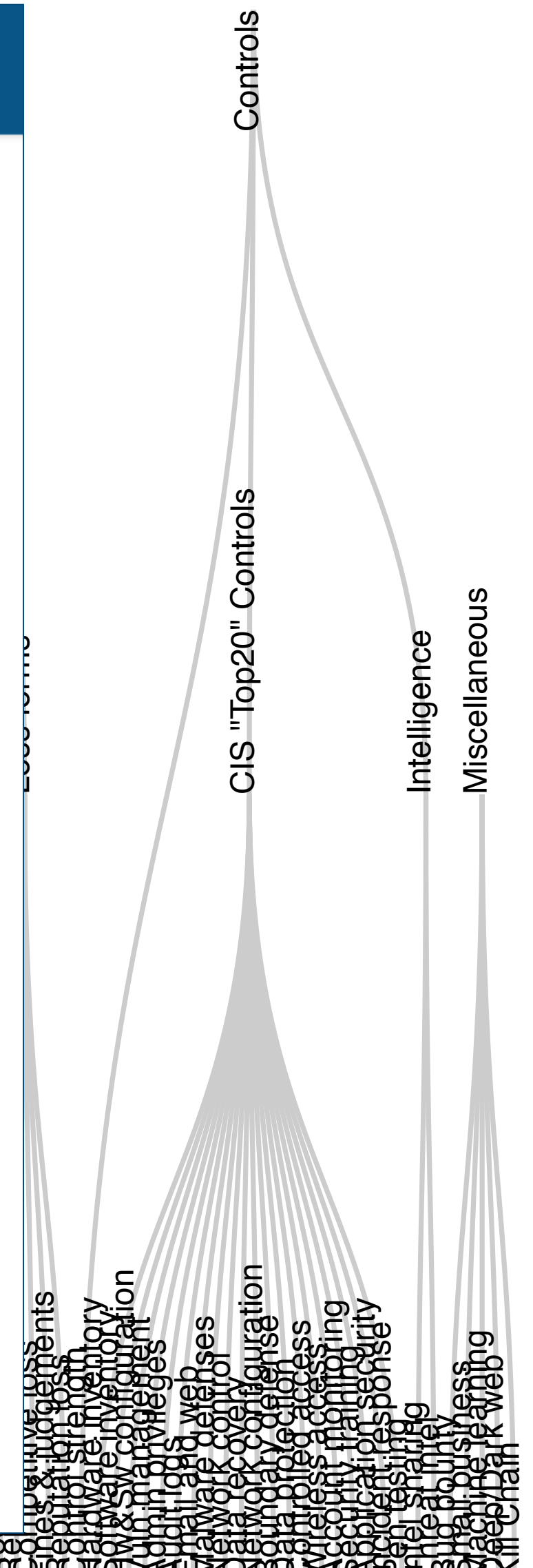
Governance (Middle):

- Security policy
- Security of directors
- Board management
- Boarding
- Reporting
- Metrics
- Benchmarking
- Standards
- Regulatory action
- Accountability
- Risk management

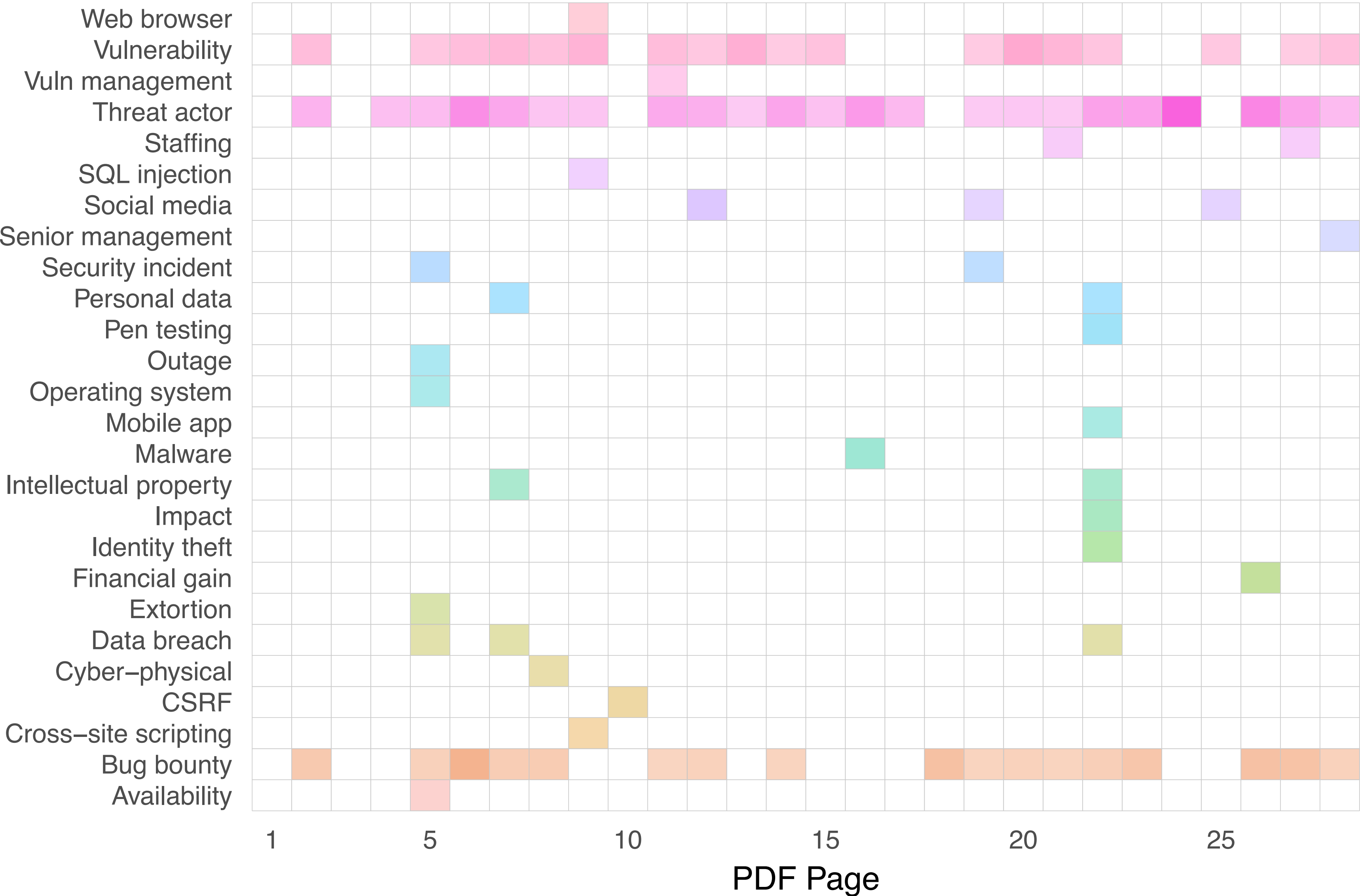
GRC Management (Right):

- Boarding
- Reporting
- Metrics
- Benchmarking
- Standards
- Regulatory action
- Accountability
- Risk management

The flows show how market trends influence governance and GRC management, with a significant flow from 'Cybercrime market' to 'Security policy' and 'Security of directors'.



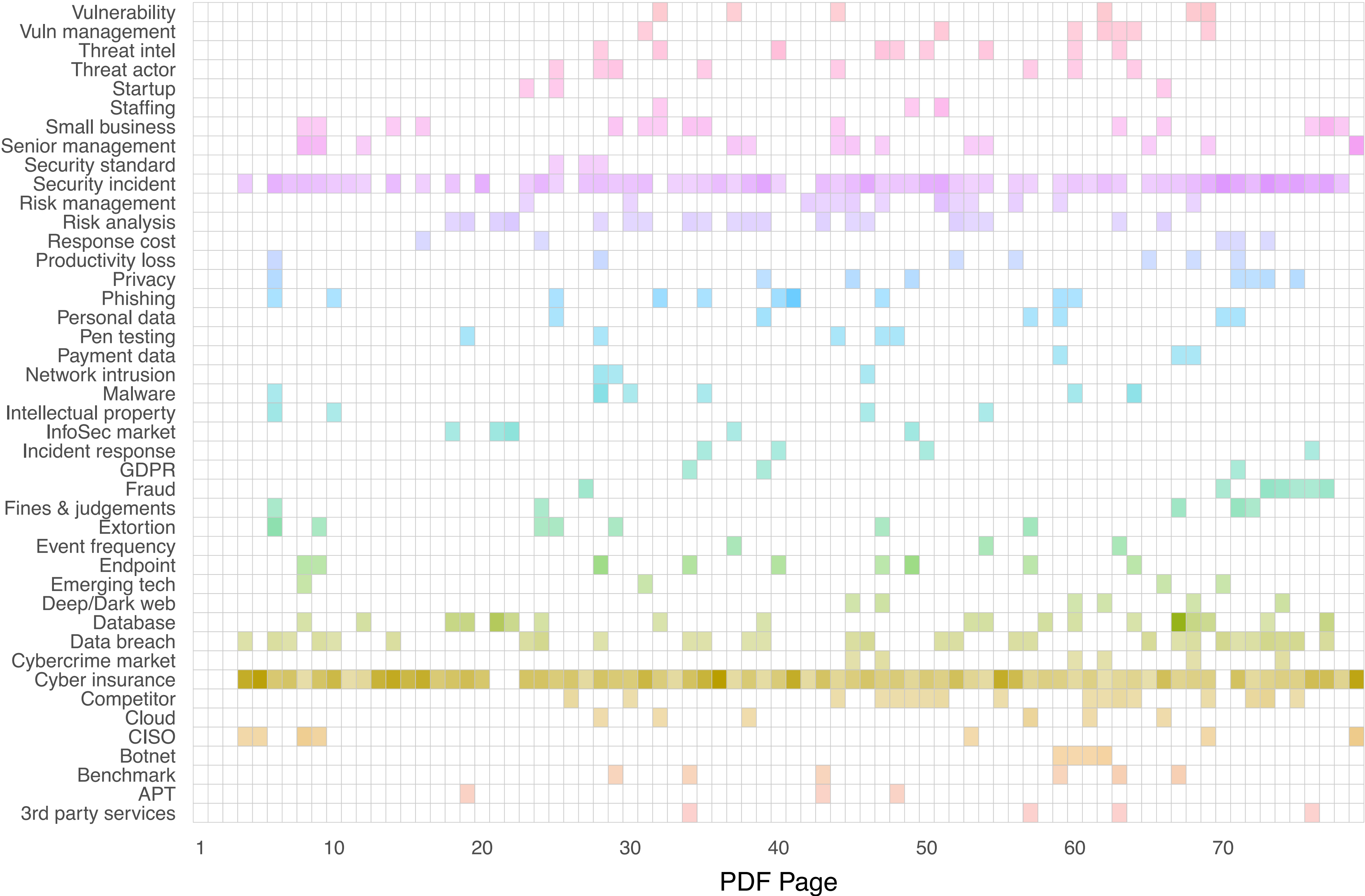
Report: Hacker One




Report: Cisco Mid-year Report 2017



Aite: Cyber Insurance





PARTNER. ADVISOR. CATALYST.

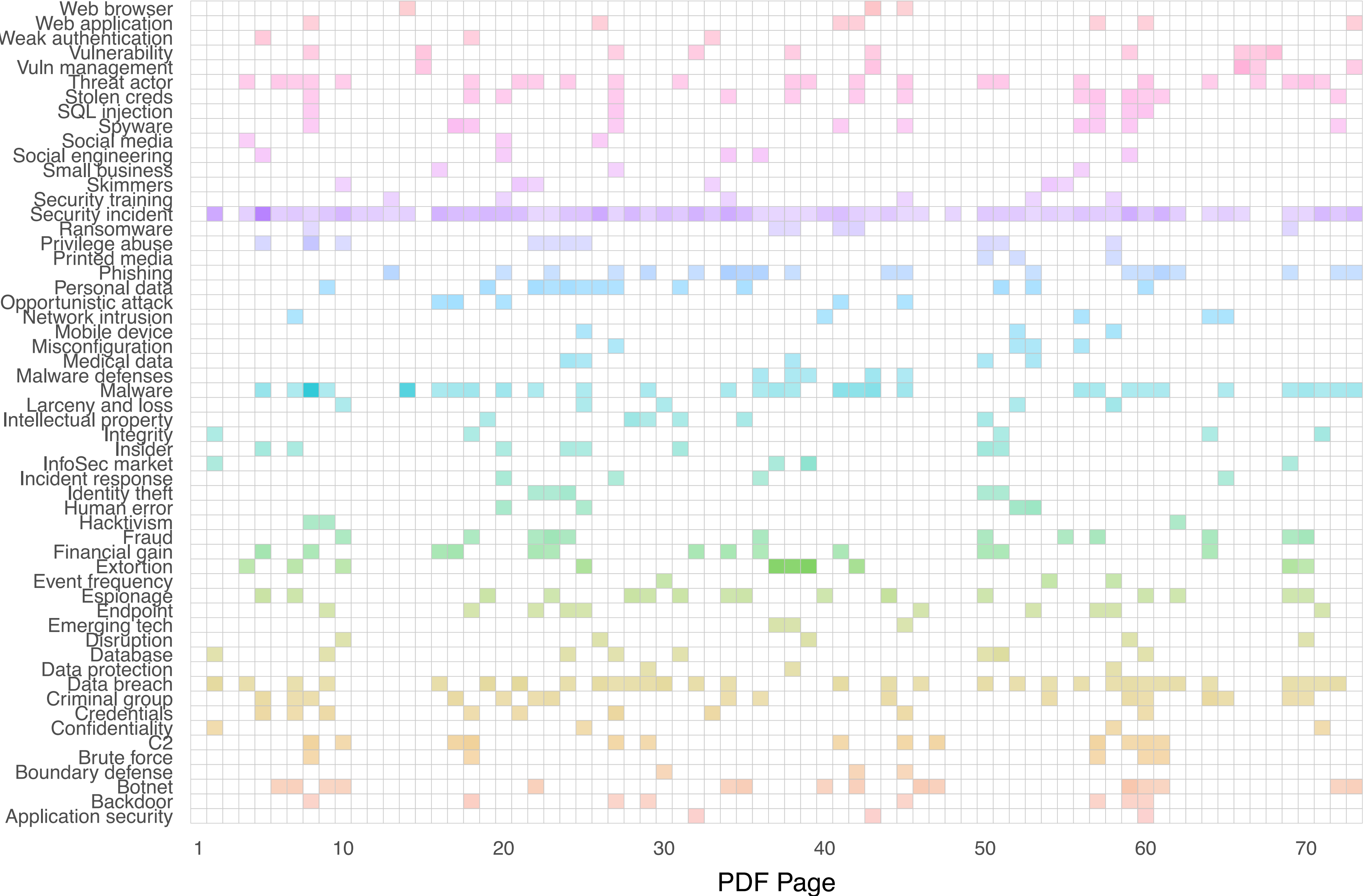
Cyber Insurance and Cybersecurity: The Convergence

June 2016

Gwenn Bézard

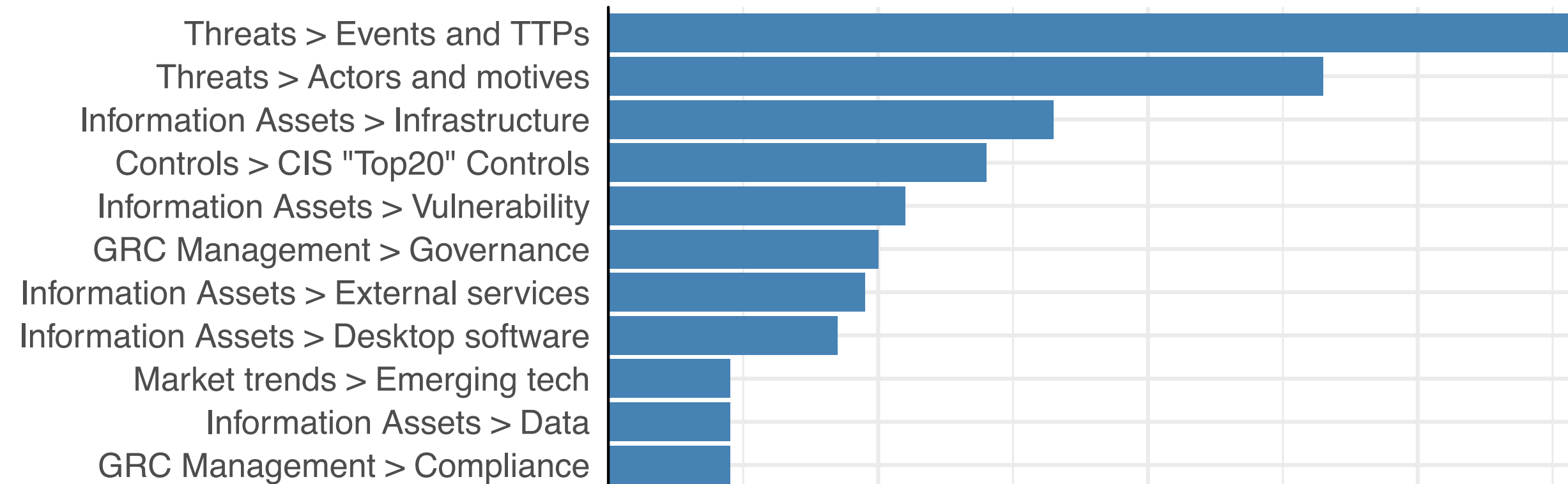
© 2016 Aite Group LLC. All rights reserved. Reproduction of this report by any means is strictly prohibited. Photocopying or electronic distribution of this document or any of its contents without prior written consent of the publisher violates U.S. copyright law, and is punishable by statutory damages of up to US\$150,000 per infringement, plus attorneys' fees (17 USC 504 et seq.). Without advance permission, illegal copying includes regular photocopying, faxing, excerpting, forwarding electronically, and sharing of online access.

Verzion DBIR 2017

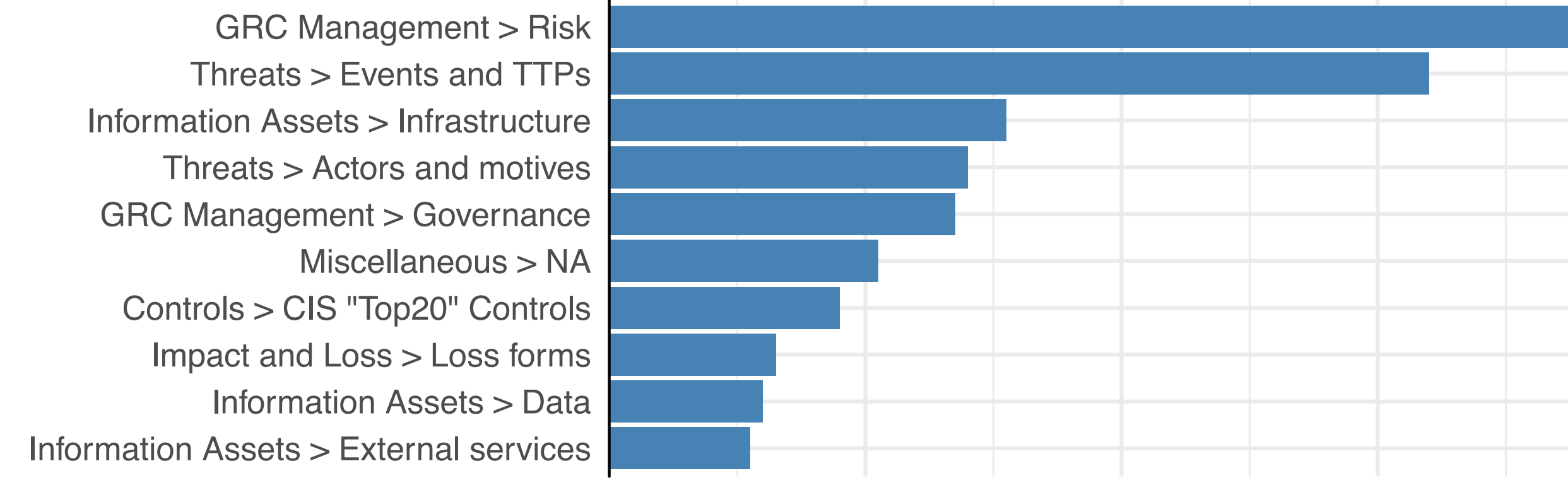


Topic/Tagging

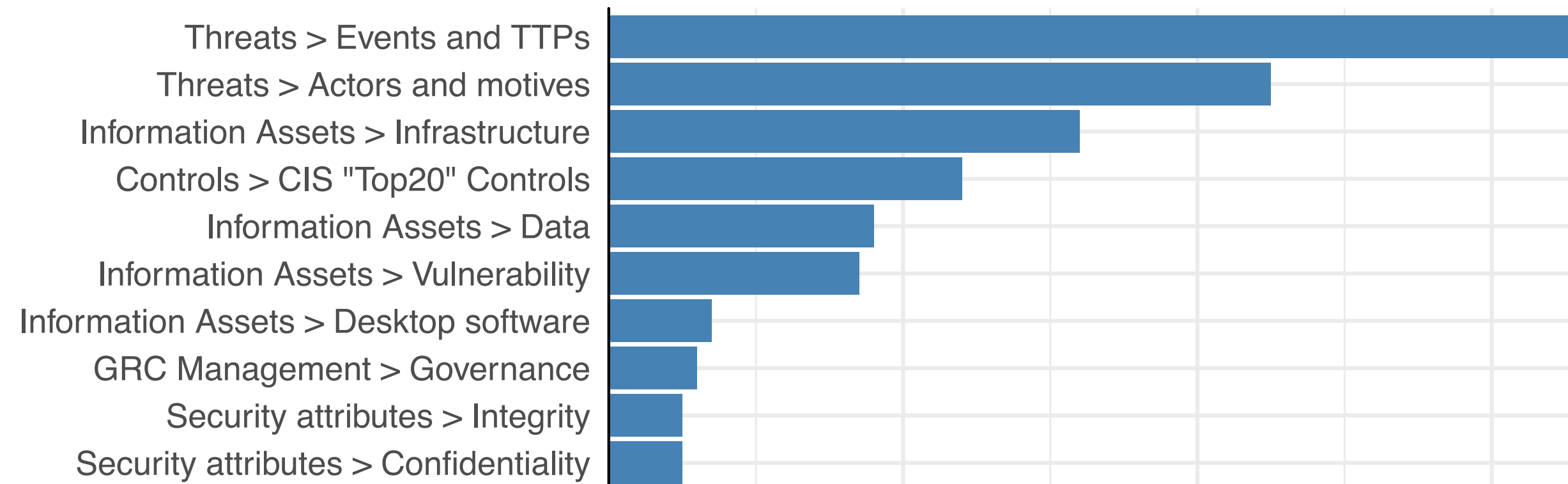
Cisco Midyear 2017



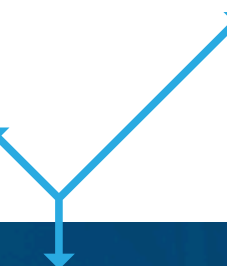
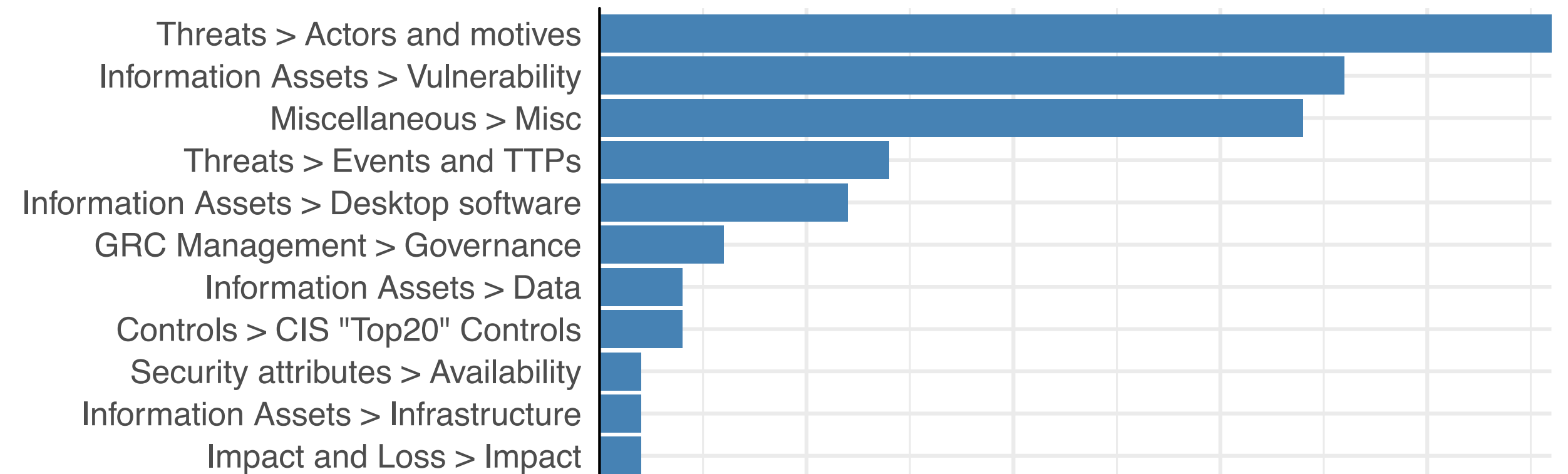
Aite: Cyber Insurance



Verizon DBIR 2017



HackerOne: Bug Bounty



Parsing PDFs: Text Extraction

TOP 3 LOCATIONS WHERE DATA IS AT RISK IN VOLUME:

- Databases (49%)
- File Servers (39%)
- Cloud (36%)

Corporate servers and databases pose the highest risk, yet spending remains stubbornly focused on endpoint and mobile

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare, and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data

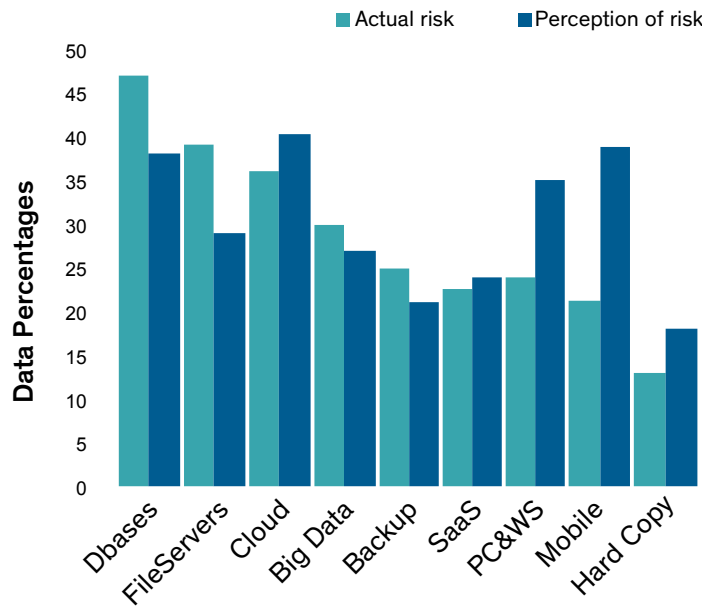


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk

locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved, and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of IT Decision Makers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. Irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

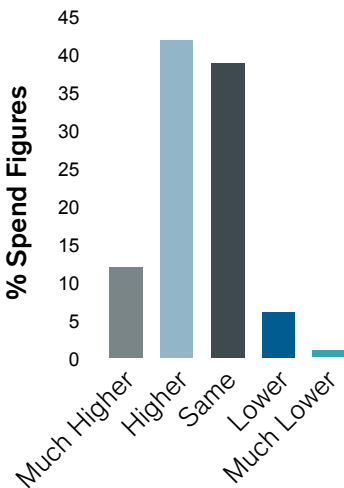


Figure 4: Global spending on security solutions during the next 12 months

TOP 3 LOCATIONS WHERE DATA IS AT RISK IN VOLUME:

- Databases (49%)
- File Servers (39%)
- Cloud (36%)

Corporate servers and databases pose the highest risk, yet spending remains stubbornly focused on endpoint and mobile

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare, and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data

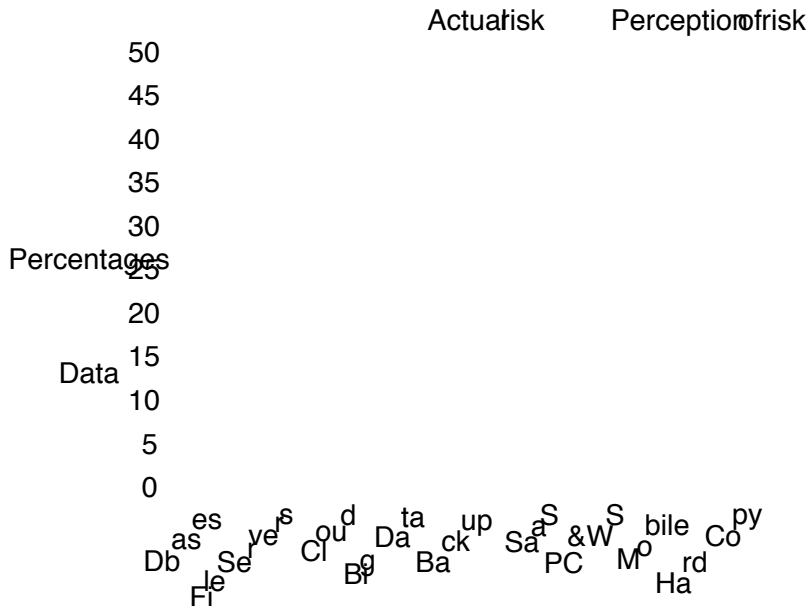


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk

locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved, and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of IT Decision Makers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. Irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

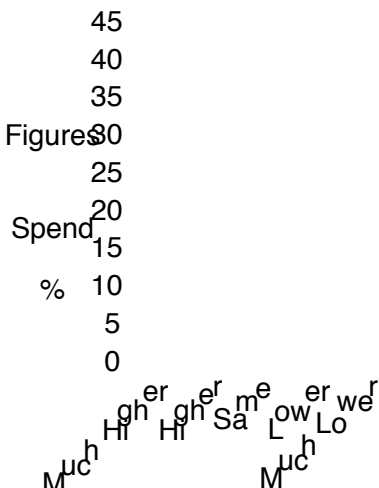


Figure 4: Global spending on security solutions during the next 12 months

Parsing PDFs: early attempt

TOP 3 LOCATIONS WHERE DATA IS AT RISK IN VOLUME:

- Databases (49%)
- File Servers (39%)
- Cloud (36%)

Corporate servers and databases pose the highest risk, yet spending remains stubbornly focused on endpoint and mobile

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare, and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data

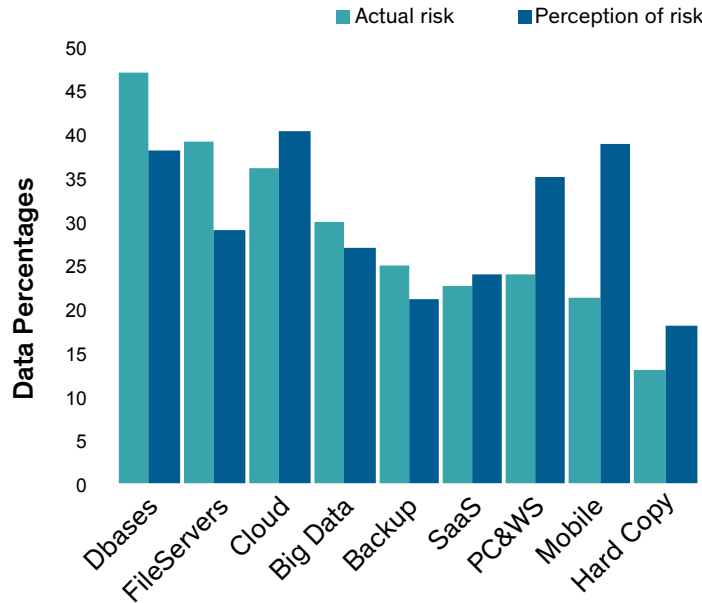


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk

locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved, and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of IT Decision Makers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. Irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

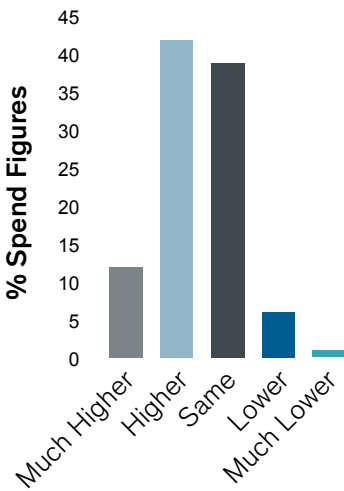


Figure 4: Global spending on security solutions during the next 12 months

TOP 3 LOCATIONS WHERE DATA IS AT RISK IN VOLUME:

- Databases (49%)
- File Servers (39%)
- Cloud (36%)

Corporate servers and databases pose the highest risk, yet spending remains stubbornly focused on endpoint and mobile

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare, and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data

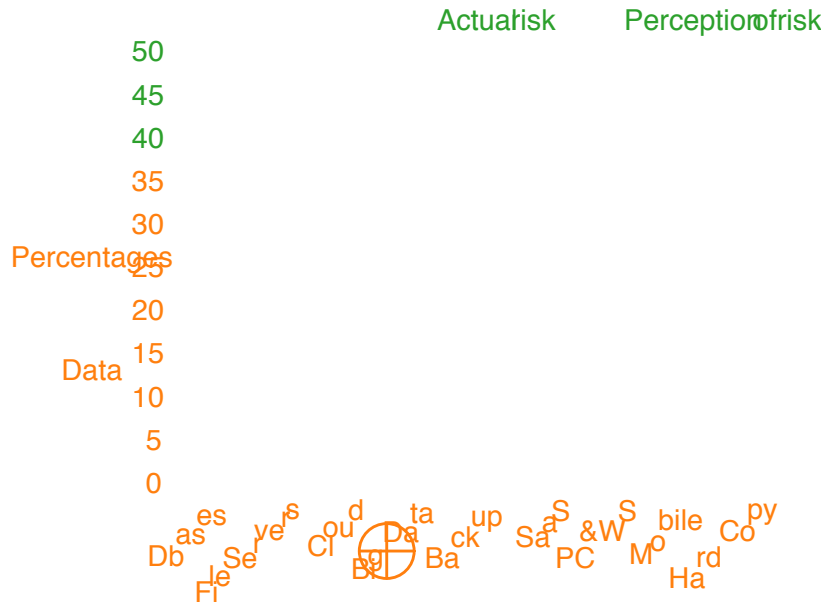


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk

locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved, and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of IT Decision Makers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. Irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

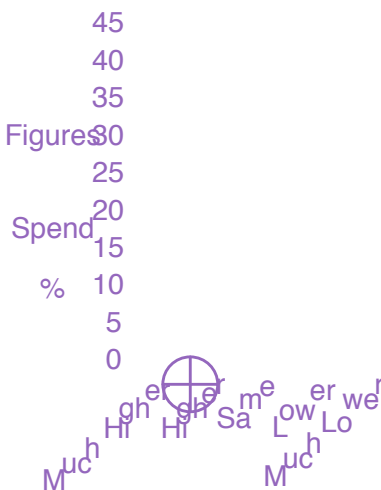


Figure 4: Global spending on security solutions during the next 12 months

Parsing PDFs Spatially

**TOP 3 LOCATIONS WHERE
DATA IS AT RISK IN VOLUME:**

- *Databases (49%)*
- *File Servers (39%)*
- *Cloud (36%)*

**Corporate servers and databases pose the
highest risk, yet spending remains stubbornly
focused on endpoint and mobile**

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare, and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data

locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved, and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of IT Decision Makers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. Irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

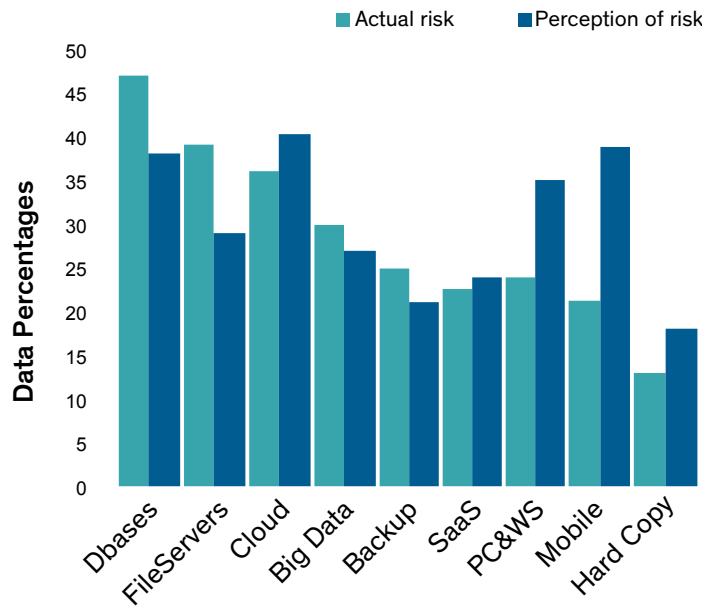


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk

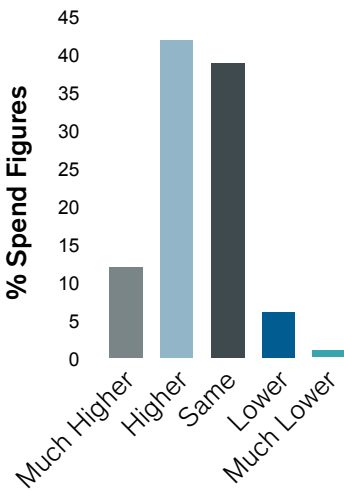
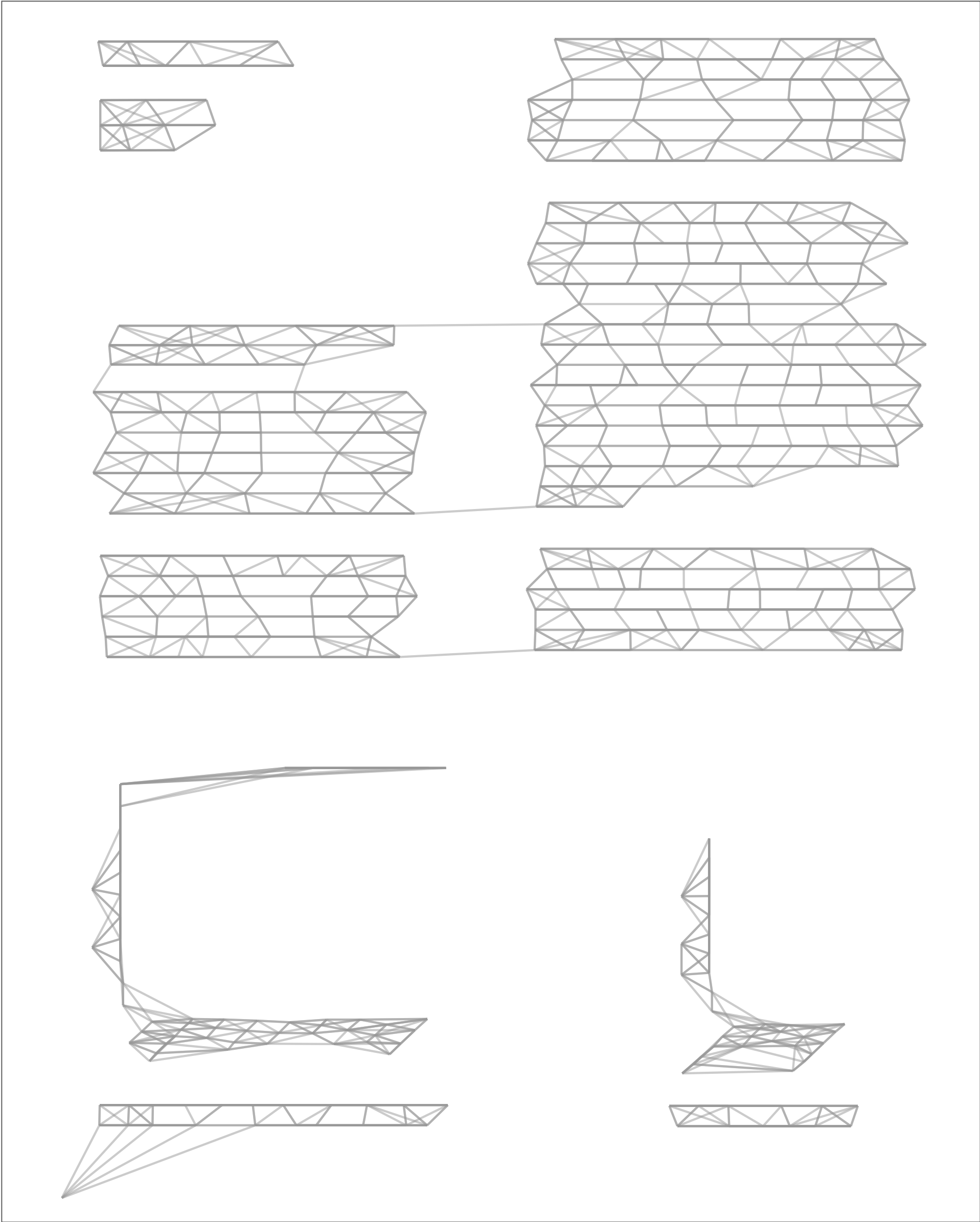


Figure 4: Global spending on security solutions during the next 12 months



TOP 3 LOCATIONS WHERE
DATA IS AT RISK IN VOLUME:

- Databases (49%)
- File Servers (39%)
- Cloud (36%)

Corporate servers and databases pose the
highest risk, yet spending remains stubbornly
focused on endpoint and mobile

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare, and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data

locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved, and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of IT Decision Makers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. Irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

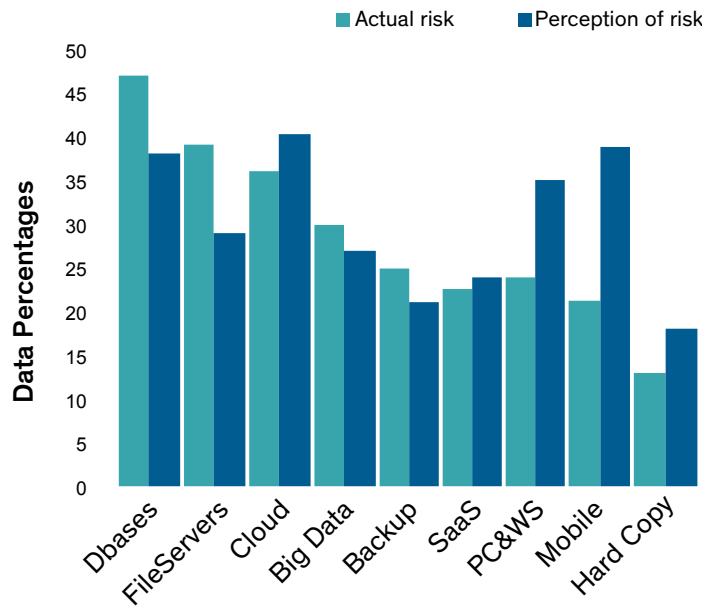


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk

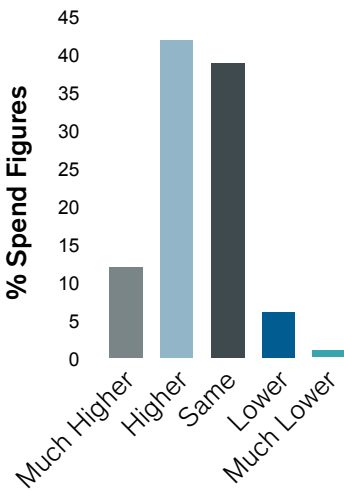


Figure 4: Global spending on security solutions during the next 12 months

TOP 3 LOCATIONS WHERE
DATA IS AT RISK IN VOLUME:

- Databases (49%)
- File Servers (39%)
- Cloud (36%)

Corporate servers and databases pose the
highest risk, yet spending remains stubbornly
focused on endpoint and mobile

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data

locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of IT Decision Makers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer irrespective of where the data is being held. It is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse that could otherwise put company-sensitive data at risk.

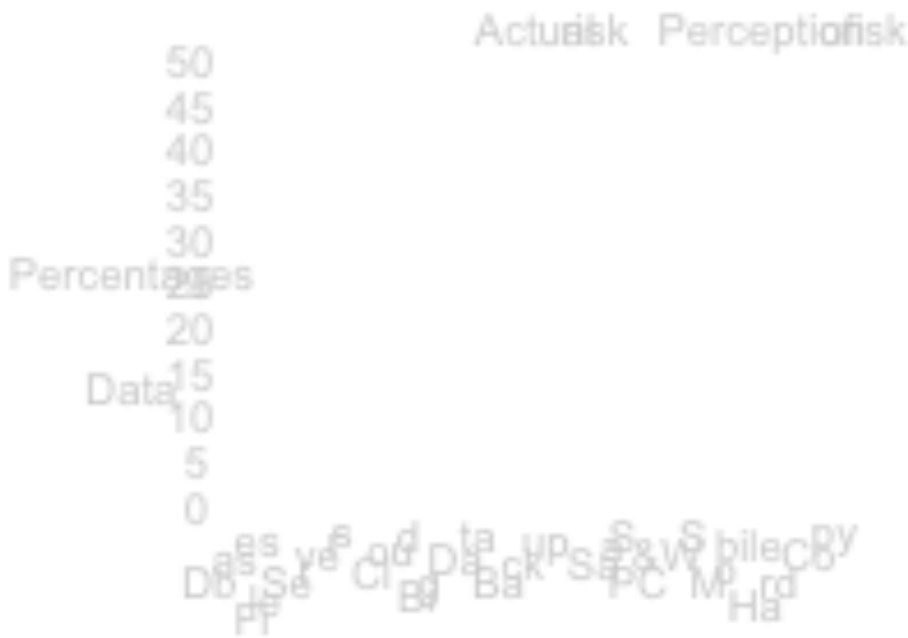


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk



Figure 4: Global spending on security solutions during the next 12 months

The most effective data protection technologies and the ones most frequently deployed by enterprise organizations were database and file encryption products, data access monitoring solutions, and data loss prevention technologies. As shown below, these topped a long list of protection solutions and were considered by enterprise respondents to offer the most effective protection against insider threats. Surprisingly tokenization, which has compliance-related uses, came bottom of the list. This may be due to restricted knowledge about the specific benefits the technology has. For example, if organizations need to protect data for specific purposes such as fulfilling payment card industry data security standard (PCI DSS) compliance, tokenization has scoping advantages over other forms of encryption that ensure the scope of audit requirements is reduced, as well as enabling the data to be used by other systems without compromising security.

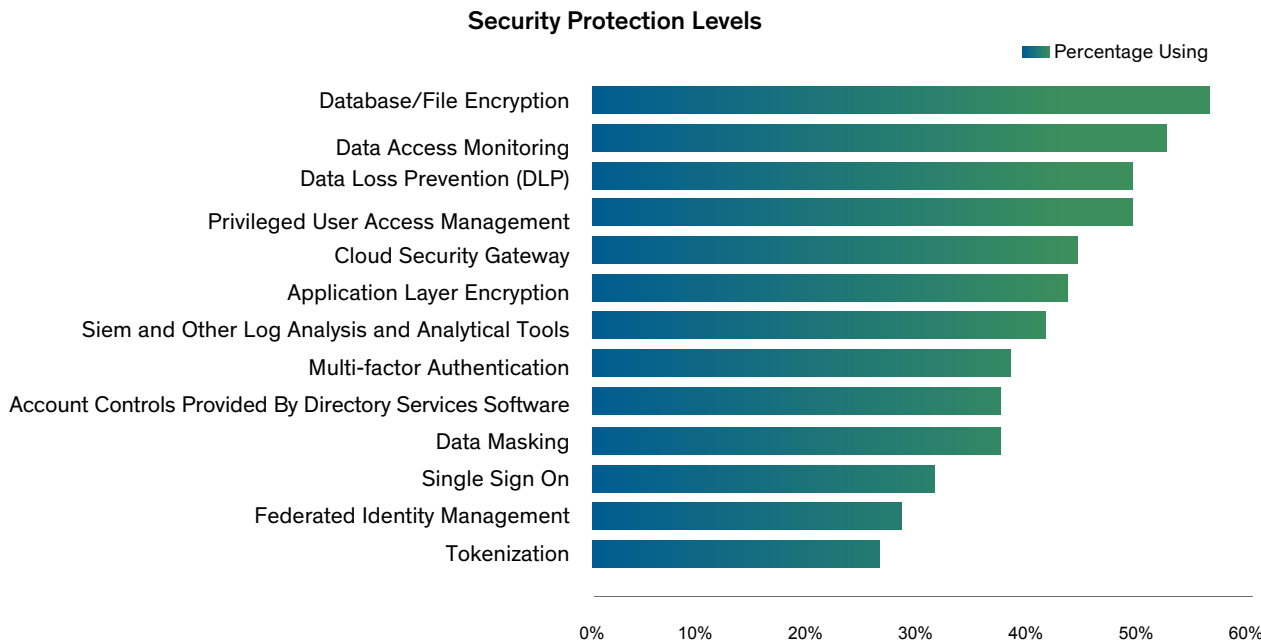


Figure 7: Protection solutions used by enterprise organizations against insider threats

- THE MOST EFFECTIVE DATA PROTECTION TECHNOLOGIES:
- Database and file encryption
 - Data Access Monitoring

The most effective data protection technologies and the ones most frequently deployed by enterprise organizations were database and file encryption products, data access monitoring solutions, and data loss prevention technologies. As shown below, these topped a long list of protection solutions and were considered by enterprise respondents to offer the most effective protection against insider threats. Surprisingly tokenization, which has compliance-related uses, came bottom of the list. This may be due to restricted knowledge about the specific benefits the technology has. For example, if organizations need to protect data for specific purposes such as fulfilling payment card industry data security standard (PCI DSS) compliance, tokenization has scoping advantages over other forms of encryption that ensure the scope of audit requirements is reduced, as well as enabling the data to be used by other systems without compromising security.



Figure 7: Protection solutions used by enterprise organizations against insider threats

- THE MOST EFFECTIVE DATA PROTECTION TECHNOLOGIES:
- Database and file encryption
 - Data Access Monitoring

ANALYST PROFILE—ANDREW KELLETT, PRINCIPAL
ANALYST SOFTWARE—IT SOLUTIONS, OVUM

Andrew enjoys the challenge of working with state-of-the-art technology. As lead analyst in the Ovum IT security team, he has the opportunity to evaluate, provide opinion, and drive the Ovum security agenda, including its focus on the latest security trends. He is responsible for research on the key technologies used to protect public and private sector organizations, their operational systems, and their users. The role provides a balanced opportunity to promote the need for good business protection and, at the same time, to research the latest threat approaches.



Andrew Kellett
Principal Analyst Software
IT Solutions, Ovum

HARRIS POLL—SOURCE/METHODOLOGY

Vormetric's 2015 Insider Threat Report was conducted online by Harris Poll on behalf of Vormetric from September 22-October 16, 2014, among 818 adults ages 18 and older, who work full-time as an IT professional in a company and have at least a major influence in decision making for IT. In the U.S., 408 ITDMs were surveyed among companies with at least \$200 million in revenue with 102 from the health care industries, 102 from financial industries, 102 from retail industries and 102 from other industries. Roughly 100 ITDMs were interviewed in the UK (103), Germany (102), Japan (102), and ASEAN (103) from companies that have at least \$100 million in revenue. ASEAN countries were defined as Singapore, Malaysia, Indonesia, Thailand, and the Philippines. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that protect data-at-rest across physical, big data and cloud environments. Vormetric helps over 1500 customers, including 17 of the Fortune 30, to meet compliance requirements and protect what matters—their sensitive data—from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database and any application's data—anywhere it resides—with a high performance, market-leading solution set.

ANALYST PROFILE—ANDREW KELLETT, PRINCIPAL
ANALYST SOFTWARE—IT SOLUTIONS, OVUM

Andrew enjoys the challenge of working with state-of-the-art technology. As lead analyst in the Ovum IT security team, he has the opportunity to evaluate, provide opinion, and drive the Ovum security agenda, including its focus on the latest security trends. He is responsible for research on the key technologies used to protect public and private sector organizations, their operational systems, and their users. The role provides a balanced opportunity to promote the need for good business protection and, at the same time, to research the latest threat approaches.

HARRIS POLL—SOURCE/METHODOLOGY

Vormetric's 2015 Insider Threat Report was conducted online by Harris Poll on behalf of Vormetric from September 22-October 16, 2014, among 818 adults ages 18 and older, who work full-time as an IT professional in a company and have at least a major influence in decision making for IT. In the U.S., 408 ITDMs were surveyed among companies with at least \$200 million in revenue with 102 from the health care industries, 102 from financial industries, 102 from retail industries and 102 from other industries. Roughly 100 ITDMs were interviewed in the UK (103), Germany (102), Japan (102), and ASEAN (103) from companies that have at least \$100 million in revenue. ASEAN countries were defined as Singapore, Malaysia, Indonesia, Thailand, and the Philippines. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.

Andrew Kellett
Principal Analyst Software
IT Solutions, Ovum

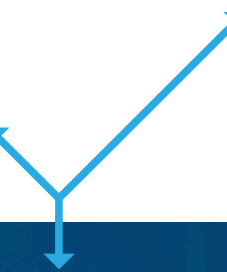
ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that protect data—at-rest across physical, big data and cloud environments. Vormetric helps over 1500 customers, including 17 of the Fortune 30, to meet compliance requirements and protect what matters—their sensitive data—from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database and any application's data—anywhere it resides—with a high performance, market-leading solution set.



Data is Everywhere

- Security Industry has hundreds if not thousands of research reports released each year.
- **Meta-Analysis** is a promising approach (ransomware)
 - Research question > Identify Sources > Assess Quality > Synthesize Results
- Lots of opportunities to improve quality of research
- Discovery of publications is a challenge
 - Lower effort with better text extraction and NLP



Data is Everywhere

Jay Jacobs
jay@cyentia.com

CY^{ENTIA}
INSTITUTE