Securosis 2010 Data Security Survey

Author's Note

The content in this report was developed independently of any sponsors. The full anonymized data set is being released in conjunction with this report under a Creative Commons license so readers can perform their own analysis.

Special thanks to Chris Pepper for editing and content support.

Licensed by Imperva, Inc.

More organizations trust Imperva for the activity monitoring, real-time protection and risk management of their critical business data and applications than any other vendor. Imperva's award-winning application firewall and database security solutions provide full visibility and granular control over the usage of enterprise business data to more than 4,500 organizations worldwide. For more information, visit www.imperva.com.

Contributors

The following individuals contributed significantly to this report through comments on the Securosis blog and follow-on review and conversations:

DMcElligott
Wade Baker
Amichai Shulman
Adrian Lane
Pablo Osinaga
LLou
Anton Chuvakin

Copyright

Table of Contents

Introduction

How do we know what really works in data security?

One of the biggest problems in security is that we rarely have a good sense of which controls actually improve security outcomes. This is especially true for newer areas like data security, filled with tools and controls that haven't been as well tested or widely deployed as things like firewalls. In an ideal world we would have a library of standard metrics shared across organizations; measured with objective instrumentation and reported to public benchmarks. But today we lack the metrics, raw collection capabilities, and public sharing that are essential to allow us to make informed risk decisions. We choose our security controls, especially our data security controls, based on anecdote, personal experiences, and perhaps some private conversations with our peers. Every organization is forced to learn their own lessons, from scratch, with very little public data to build on.

The Securosis 2010 Data Security Survey is designed as an early step towards providing security managers and practitioners with practical information on the perceived effectiveness of major data security tools and techniques. The results are based on the responses of over one thousand security and IT professionals within organizations of all sizes.

Key Findings

- We received over 1100 responses with a completion rate of over 70% representing all major vertical markets and company sizes.
- On average, most data security controls are in at least some stage of deployment in 50% of responding organizations. When deployed, controls tend to have been in use for 2 years or more.
- Most responding organizations still rely heavily on “traditional” security controls like system hardening, email filtering, access management, and network segregation to protect data.
- When deployed, 40-50% of participants rate most data security controls as completely eliminating or significantly reducing security incident occurrence.
- The same controls rated slightly lower for reducing incident severity (when incidents occur), and still lower for reducing compliance costs.
- 88% of survey participants must meet at least 1 regulatory or contractual compliance requirement, with many having to comply with multiple regulations.
- Despite this, “to improve security” is the most cited primary driver for deploying data security controls, followed by direct compliance requirements and audit deficiencies.
- 46% of participants reported about the same number of security incidents in the most recent 12 months compared to the previous 12, with 27% reporting fewer incidents, and only 12% reporting a relative increase.
- Organizations are most likely to deploy USB/portable media encryption and device control or data loss prevention in the next 12 months.
- Email filtering is the single most commonly used control, and the one cited as the overall least effective.

- Our overall conclusion is that even accounting for potential response bias, ***data security has transitioned past early adopters and significantly penetrated the early mainstream of the security industry***.

Top Rated Controls (Perceived Effectiveness):

- The top 5 rated controls for reducing the number of incidents are network data loss prevention, full drive encryption, web application firewalls, server/endpoint hardening, and endpoint data loss prevention.
- The top 5 rated controls for reducing incident severity are network data loss prevention, full drive encryption, endpoint data loss prevention, email filtering, and USB/portable media encryption and device control. (Web application firewalls nearly tied to make the top 5).
- The top 5 rated controls for reducing compliance costs are network data loss prevention, endpoint data loss prevention, storage data loss prevention, full drive encryption, and USB and portable media encryption and device control. (Very closely followed by network segregation and access management).

Methodology

The 2010 Data Security Survey was developed and managed in accordance with the Securosis Totally Transparent Research process (available for review at http://securosis.com/about/totally-transparent-research). The survey was initially proposed by the report sponsor, Imperva, but all questions and analysis were developed independently.

Development and Structure

The generation of the survey and initial parameters were announced on the Securosis blog in May, 2010 and public comments solicited. This feedback was used to develop the initial draft question set, which was also posted for public comment. We additionally solicited direct feedback from the Security Metrics community at http://securitymetrics.org.

Based on this extensive feedback, which was captured as comments on the Securosis blog, we created the final question set. Conceptually, the survey changed dramatically as a result of the feedback. The initial idea was to have respondents share their data security practices during different phases of data security, but the survey quickly transformed to focus more on evaluating the effectiveness of various security controls, rather than the maturity of organization's implementations of said controls.

Thus the survey breaks out into four major sections:

- Background Information and Demographics- Basic information on the respondent and their organization, including size, vertical market, compliance requirements, and staffing.
- Incidents- Rough estimates of the number and types of breaches experienced by the organizations, and if breaches increased or decreased over the last year.
- Controls Effectiveness- Perceived effectiveness of various major data security controls in reducing the number of breaches, severity of breaches, and costs of compliance.
- Controls Usage- The scope of deployed controls, how long they have been deployed, and the primary reason for deployment.

The survey as designed to take 10-20 minutes to complete, and was open for public review and comments during every stage of development. The question set is available for review at http://www.surveymonkey.com/s/DataSecurity2010-Draft, where it will remain for a minimum of one year.

Collection and Analysis

The survey was hosted on SurveyMonkey and launched on June 16, 2010 and remained open until July 23. It was publicized on the Securosis blog, Security Metrics mailing list, Twitter, the WhiteHatWorld.com mailing list, and the sponsor's mailing list (Imperva). Additional blogs and associates also promoted the survey throughout various social media networks.

The survey was public and open, and received 1,176 responses, with 72.4% of respondents completing all questions. Respondents could respond completely anonymously or provide an email address to register for an iPad giveaway.

Analysis was then performed independently, with the exception of using a tool provided by the sponsor to determine the country of origin of responses based on IP address. This analysis was performed internally, and no identifiable information was shared outside of Securosis.

The full anonymized data set used for analysis will be released publicly 45 days after this report. Other than IP addresses and emails the data set is exactly the same as used to generate this document.

Flaws and Limitations

Due to the features supported by SurveyMonkey we were unable to effectively design the survey with conditionals to allow respondents to select a list of the technologies that they use, then answer questions on their effectiveness. While SurveyMonkey supports conditions, the feature doesn't allow you to populate multiple-selection lists based on a multi-selection conditional, which means we would have had to ask a series of repetitive questions for every control the respondent identified in use.

Instead we asked all respondents to reply to a complete list of controls, increasing the chance for survey fatigue and error.

In the *Incidents* section the options did not include "no incidents", but did include "N/A". Based on the comments of respondents some used this answer option if they didn't suffer any known incidents, while others used it if they didn't have access to breach data.

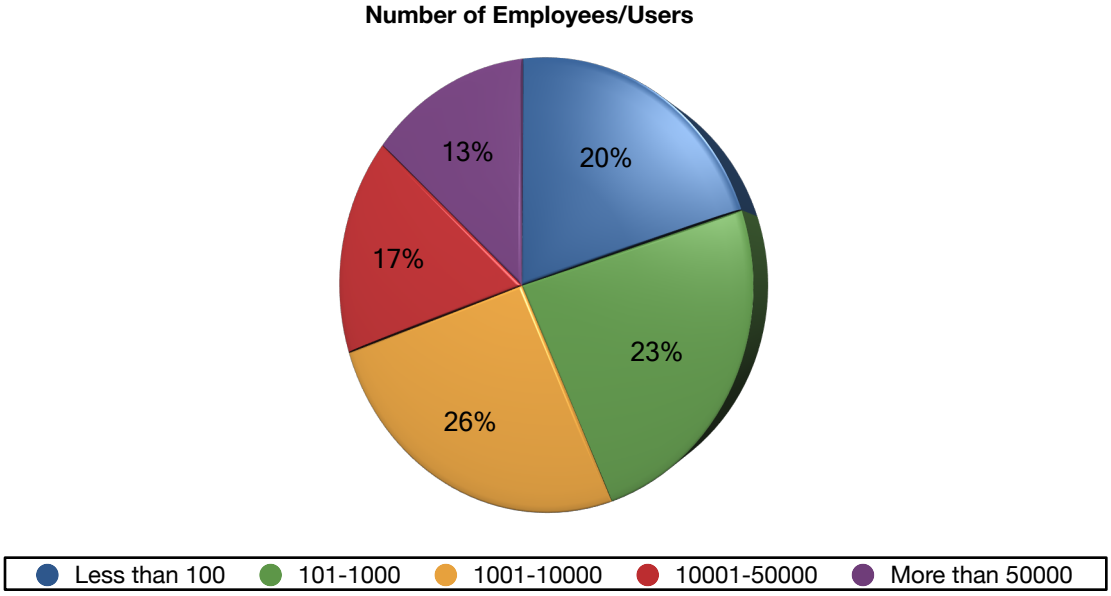
Finally, it's important to emphasize that this survey evaluated *perceived effectiveness*, not *actual effectiveness*. Since organizations lack a consistent, objective, metrics-based way to evaluate their security controls it is impossible to compare actual effectiveness across organizations. Also, as you will see in the detailed analysis, there is naturally a considerable bias towards the controls an organization is most familiar with, and many of the tools and techniques we asked about in this survey are not in nearly as wide deployment as standard network and endpoint security tools.

Background Information and Demographics

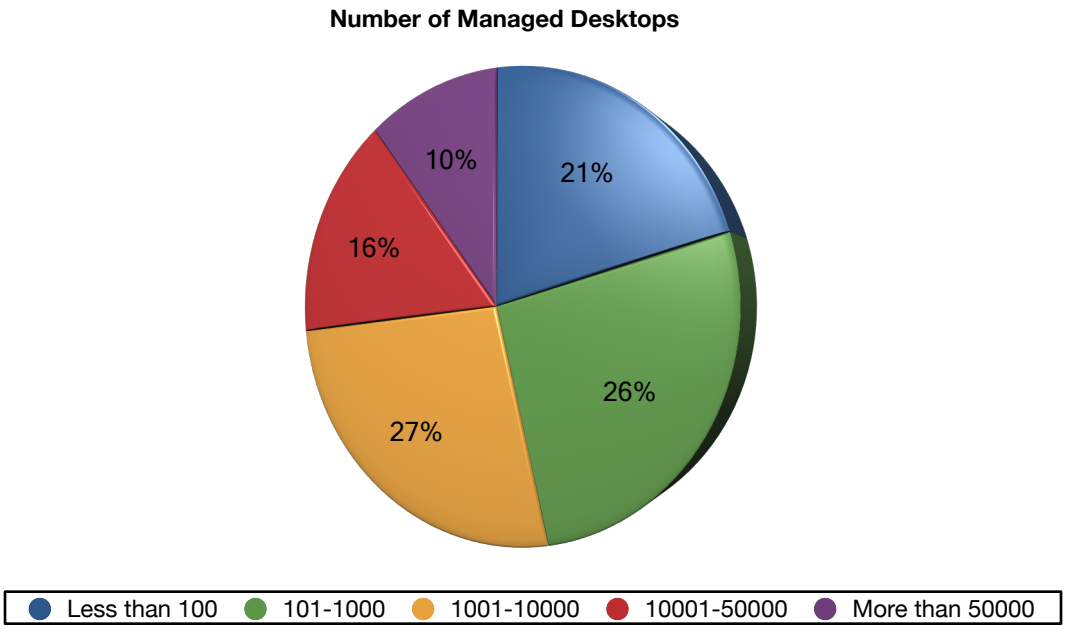
Organization Size

1,176 individuals responded to the survey, with 851 (72.4%) completing all of the questions. We received responses from an extremely wide range of organizations; from those with less than 10 employees, all the way up to very large enterprises with more than 50,000 employees. Overall the distribution was surprisingly even, skewing, as you might expect, towards medium to the lower edge of large organizations.

	Less than 100	101-1000	1001-10000	10001-50000	More than 50000
a. Number of employees/users	235	269	308	199	156
b. Number of managed desktops	233	292	305	185	119



The number of managed desktops aligned fairly closely with the number of employees.

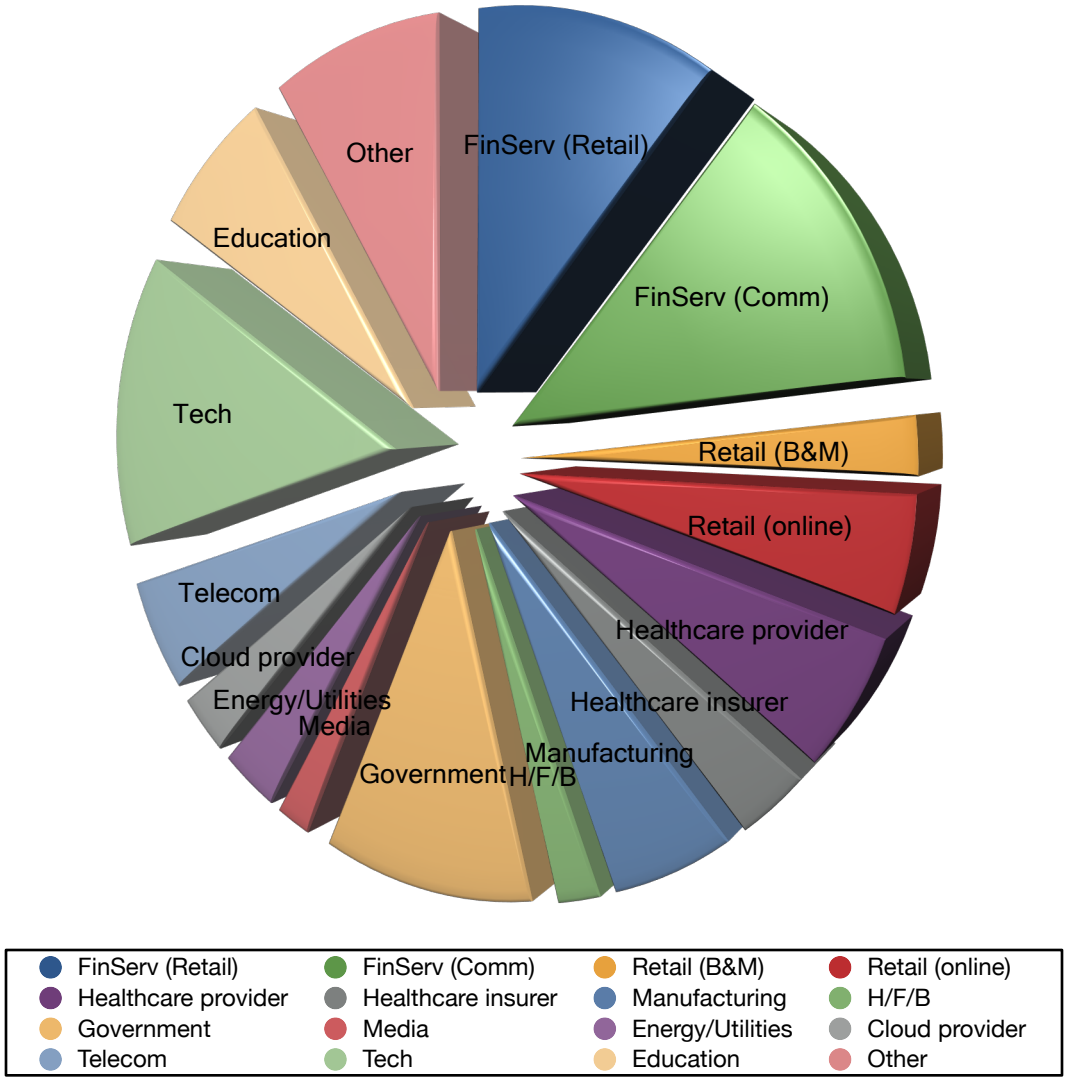


Vertical Markets

Our vertical market distribution was not nearly as even as organization size, and heavily skewed towards financial services, government, and technology companies, followed by education. This seems fairly common in security surveys, likely due to response bias since those industries tend to both skew larger, and spend more on security (based on third-party reports and anecdotal experience).

Vertical	Count
FinServ (Retail)	186
FinServ (Comm)	206
Retail (B&M)	38
Retail (online)	77
Healthcare provider	95
Healthcare insurer	54
Manufacturing	94
H/F/B	34
Government	178
Media	31
Energy/Utilities	53
Cloud provider	49
Telecom	93
Tech	245
Education	119
Other	148

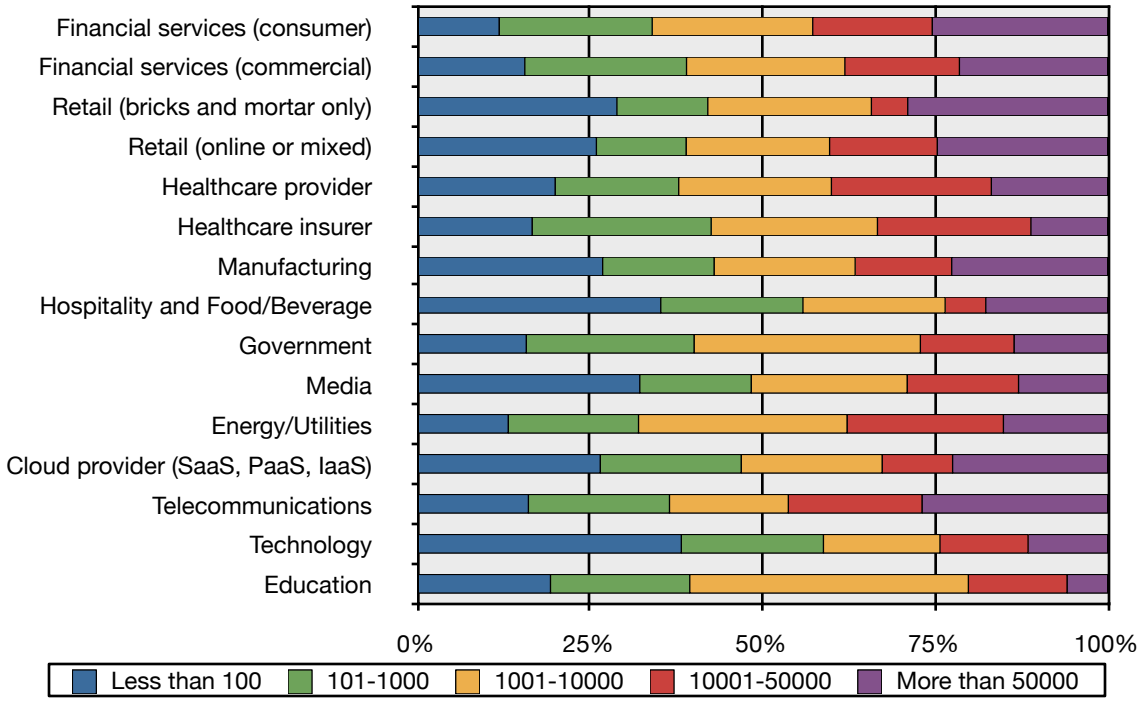
Vertical Market Distribution



We can see the probable response bias when we evaluate the organization size by vertical market as opposed to raw response rate, which smooths out the size distribution for most of the verticals. We see that financial services, retail, telecommunications, and healthcare skew most towards larger organizations (but still with a healthy representation of the mid-market), and technology skews most towards smaller companies, likely due to startups and smaller providers.

Number of Employees:	Less than 100	101-1000	1001-10000	10001-50000	More than 50000
Financial services (consumer)	22	41	43	32	47
Financial services (commercial)	32	48	47	34	44
Retail (bricks and mortar only)	11	5	9	2	11
Retail (online or mixed)	20	10	16	12	19
Healthcare provider	19	17	21	22	16
Healthcare insurer	9	14	13	12	6
Manufacturing	25	15	19	13	21
Hospitality and Food/Beverage	12	7	7	2	6
Government	28	43	58	24	24
Media	10	5	7	5	4
Energy/Utilities	7	10	16	12	8
Cloud provider (SaaS, PaaS, IaaS)	13	10	10	5	11
Telecommunications	15	19	16	18	25
Technology	93	50	41	31	28
Education	23	24	48	17	7

Size by Vertical Market (Percentage)



Staffing and Data Centers

We asked respondents to provide some basic information to gauge the size of their IT program- focusing on the number of data centers, IT staff, and security staff.

	Partial/ Less than 1	1-5	6-10	11-50	51-100	101-500	More than 500
a. Number of data centers	153	745	104	88	34	25	16
b. How many IT staff	61	238	93	161	118	235	246
c. How many IT security staff	187	457	135	184	76	68	39
d. How many staff dedicated to data security	349	415	127	136	47	41	31

In analyzing these by organization size, as expected we find the number of staff and data centers scale fairly consistently:

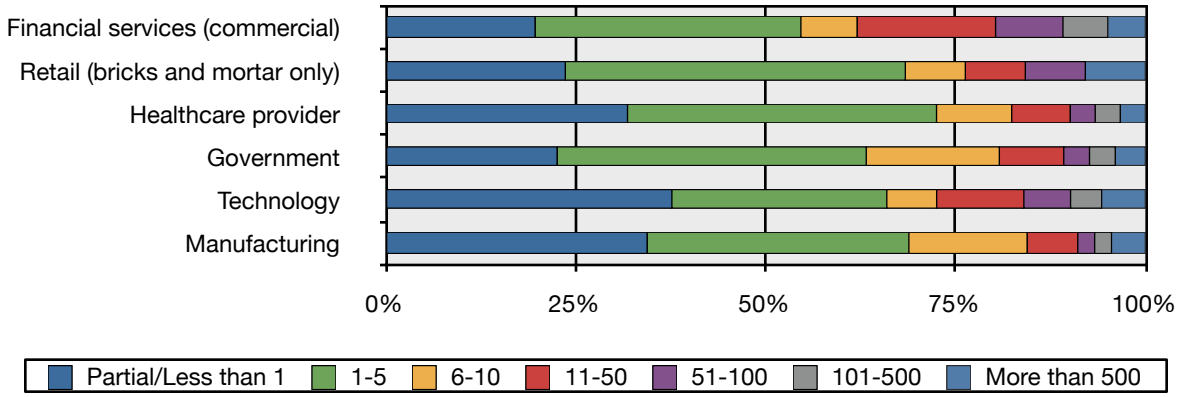
	Organization sizing: -- a. Number of employees/users				
	Less than 100	101-1000	1001-10000	10001-50000	More than 50000
a. Number of data centers					
Partial/Less than 1	114	30	6	2	0
1-5	118	222	241	115	47
6-10	1	10	30	42	20
11-50	2	6	18	26	36
51-100	0	1	6	9	18
101-500	0	0	2	5	18
More than 500	0	0	0	0	16
b. How many IT staff					
Partial/Less than 1	60	0	0	1	0
1-5	142	89	5	0	0
6-10	16	59	16	2	0
11-50	11	82	57	7	3
51-100	1	23	65	21	8
101-500	1	9	128	70	27
More than 500	0	3	32	94	116
c. How many IT security staff					
Partial/Less than 1	102	68	14	2	1
1-5	118	153	141	33	9
6-10	9	28	64	26	8
11-50	2	9	62	74	36
51-100	1	2	14	37	22
101-500	0	1	3	21	43
More than 500	0	1	1	3	34
d. How many staff dedicated to data security					
Partial/Less than 1	139	126	61	17	6
1-5	80	111	154	52	16
6-10	8	21	37	38	22
11-50	2	3	40	60	30
51-100	1	1	6	14	25
101-500	0	1	4	12	24
More than 500	0	1	0	1	29

But when we analyze the responses based on a subset of vertical markets we start to see more differentiation:

	Vertical industry/market:					
	Financial services (commercial)	Retail (bricks and mortar only)	Healthcare provider	Government	Technology	Manufacturing
a. Number of data centers						
Partial/Less than 1	14	7	9	19	59	16
1-5	127	26	65	118	110	50
6-10	26	1	5	18	31	8
11-50	20	1	8	10	19	9
51-100	9	0	3	4	8	6
101-500	6	0	2	2	11	2
More than 500	2	3	3	7	7	3
b. How many IT staff						
Partial/Less than 1	2	0	4	3	22	6
1-5	35	12	18	36	81	24
6-10	18	6	10	14	17	4
11-50	22	4	10	32	29	14
51-100	19	5	8	23	16	5
101-500	37	2	28	38	27	16
More than 500	71	9	14	32	51	22
c. How many IT security staff						
Partial/Less than 1	16	5	14	16	52	21
1-5	76	17	43	78	89	32
6-10	17	5	13	26	24	10
11-50	35	6	10	29	31	19
51-100	25	2	5	11	12	1
101-500	20	0	4	9	18	3
More than 500	14	3	3	8	15	4
d. How many staff dedicated to data security						
Partial/Less than 1	40	9	29	40	92	31
1-5	71	17	37	72	69	31
6-10	15	3	9	31	16	14
11-50	37	3	7	15	28	6
51-100	18	3	3	6	15	2
101-500	12	0	3	6	10	2
More than 500	10	3	3	7	14	4

To visualize this better, here's a chart showing the percentage scale of staff dedicated to data security, by these verticals:

Number of staff dedicated to data security by vertical



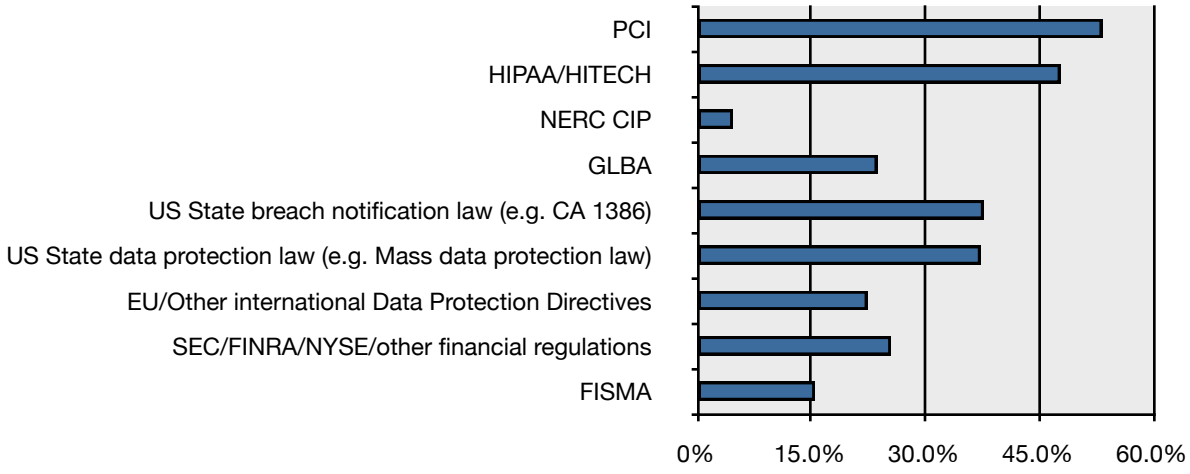
Financial services and government show relatively higher investment in data security personnel compared to the other verticals.

Regulatory Compliance

Fully 88% of respondents reported having to meet regulatory or compliance requirements, with PCI and HIPAA/HITECH the most frequently cited:

Regulation	Responses
PCI	521
HIPAA/HITECH	467
NERC CIP	46
GLBA	232
US State breach notification law (e.g. CA 1386)	368
US State data protection law (e.g. Mass data protection law)	364
EU/Other international Data Protection Directives	219
SEC/FINRA/NYSE/other financial regulations	249
FISMA	151
Other (please specify)	188

Regulatory compliance (percentage of responses)

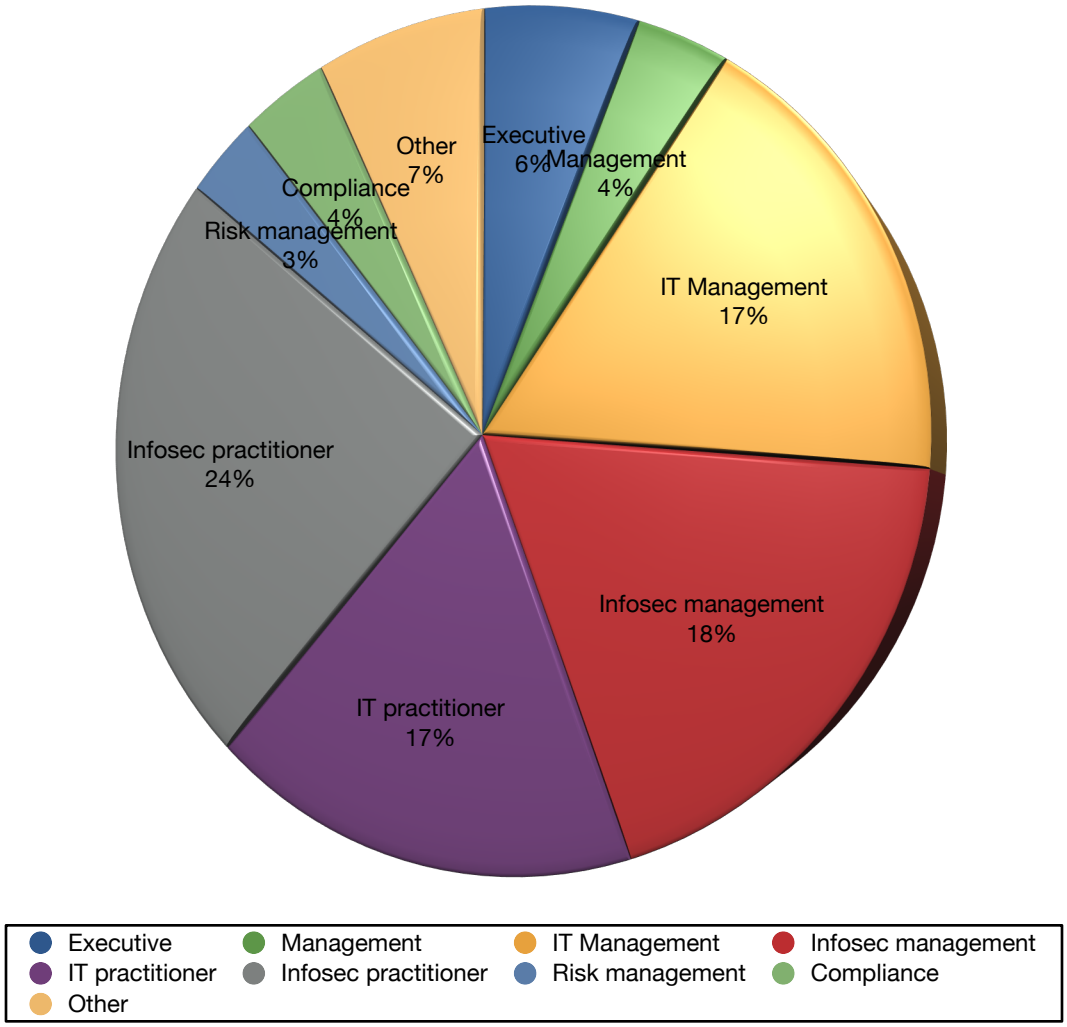


Of the regulations we didn't ask about, FERPA and SOX were the most commonly cited. As we'll see later, although respondents feel compliance plays a large role in security, it seems to be less influential than our anecdotal experience indicates. We will delve into this in more detail in the *Controls Effectiveness* section.

Job Roles

Most respondents work within IT or security, with slightly more practitioners than managers participating. Based on the free form responses it seems at least a few Chief Information Security Officers don't consider themselves part of information security management.

Role	Responses
Executive management	88
General management	52
IT Management	240
IT security management	257
IT professional/practitioner	248
IT security professional/practitioner	349
Other risk management	47
Other compliance	54
Other	101



Conclusions

Overall the survey seems reasonably representative of the general market. We received responses from organizations with more employees than many municipalities, and those with few enough employees you can count them on one hand, with fingers leftover. Participants are also very representative of multiple vertical markets and job roles (practitioner vs. management, general IT vs. security-specific). With just over 1100 responses, and a completion rate of over 70%, we feel confident that the data is both statistically significant and broadly representative. We do have higher representation from security-heavy industries like financial services, technology, and government, which is common in the security industry.

Although this section is focused on general demographics, two interesting results emerge:

- 88% of organizations must comply with a major regulatory or contractual requirement (PCI is contractual, not regulatory).
- Organizations do not invest equally in data security- financial services and government invest most in data security personnel, with healthcare, retail, and manufacturing investing relatively less (note that we only performed this analysis for some of the verticals surveyed).

Incidents

Knowing is (more than) half the battle

We asked participants to give us a sense of the kinds of security incidents they've suffered over the past few years. Rather than asking for an exact count, which we believe few organizations accurately track, we used general categories across different types of incidents (major, minor, and accidental) and information (regulated data, unregulated personal information, and intellectual property).

Due to a flaw in survey design we didn't provide a "no incidents" response option, and many of those answers combined with the NA/Don't have this data. This still allows us to characterize the kinds of incidents that people did experience, but we are unable to draw any conclusions on actual incident rates. This is especially true since in all categories, most participants reported that they either didn't have the data or didn't suffer any incidents.

But as we will show later in this section, more respondents report their breach rates as either staying the same or decreasing this year vs. last year.

Definitions

We asked participants to tell us about their incidents in three different categories, using the following definitions:

- A *major incident* is one that could result in a breach notification, material financial harm, or high reputation damage. In other words something that would trigger an incident response process, and involve executive management.
- A *minor incident* would not result in a disclosure, fines, or other serious harm. Something managed within IT, security, and the business unit without executive involvement.
- A *breach* is a malicious internal or external attack.
- An *accidental disclosure* is the accidental release of information, but not as the result of an attack (e.g. including lost media).

Within each category, we asked about the following kinds of information:

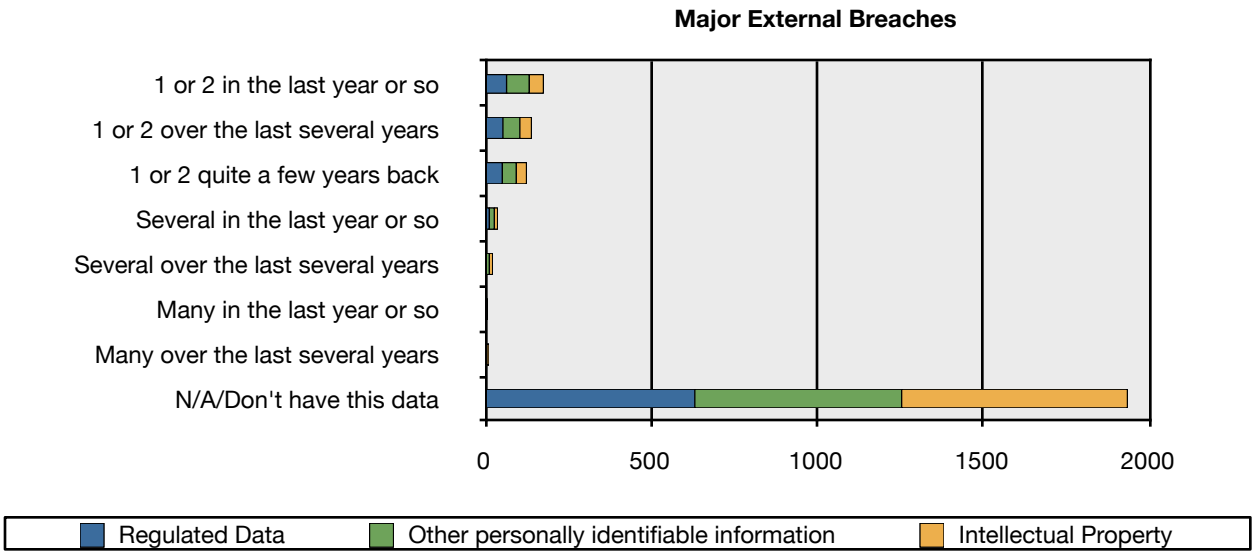
- Regulated Data (credit card numbers, HIPAA information, Social Security Numbers, bank account numbers).
- Other personally identifiable information (non-regulated names/address).
- Intellectual Property.

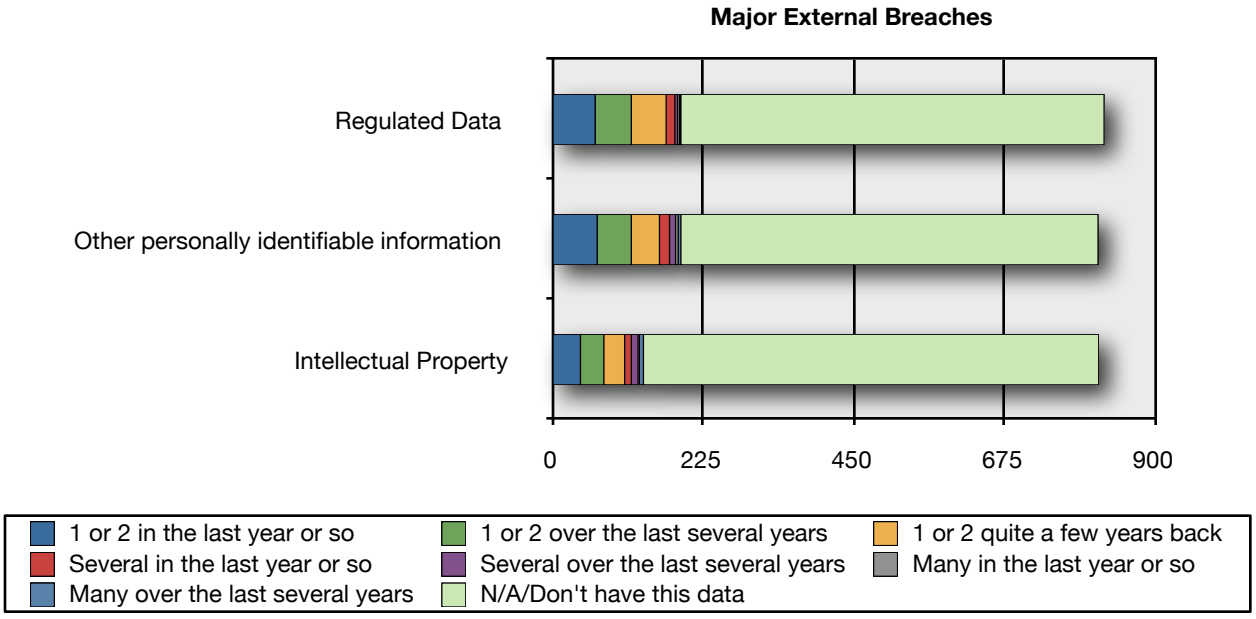
Major Incidents

We asked, “Please estimate the following **major** successful attacks you have experienced for these different data types:”

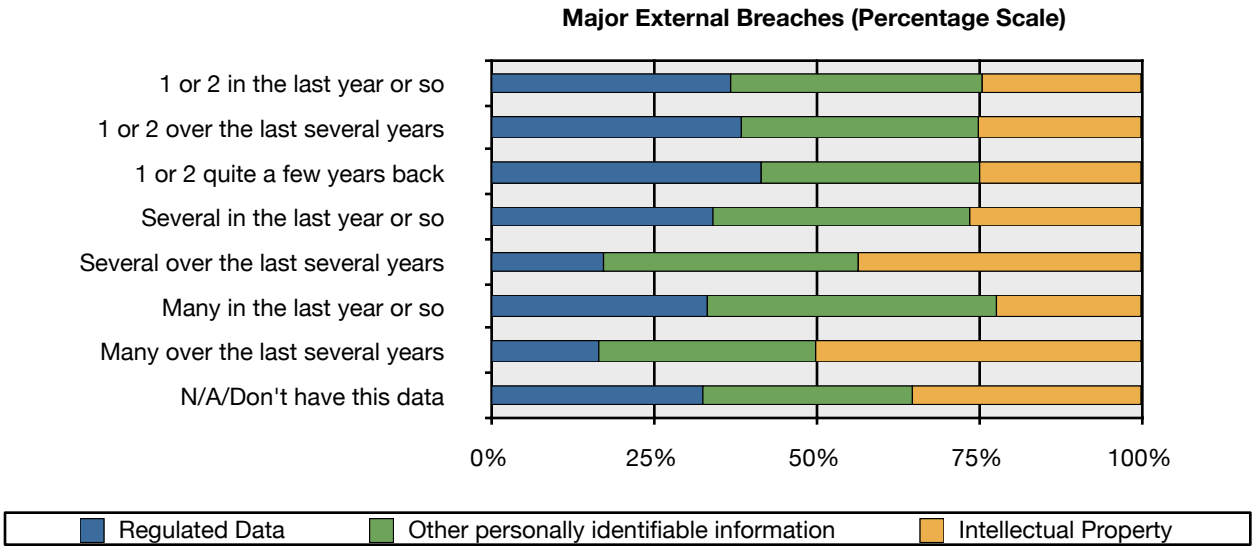
External Breaches:

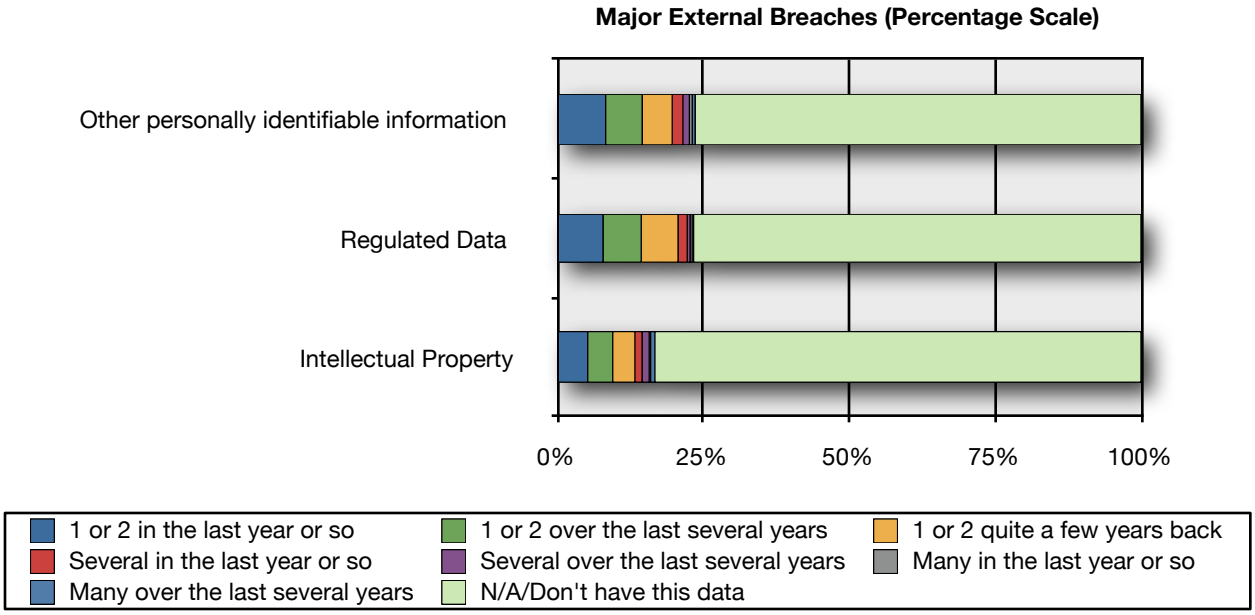
	1 or 2 in the last year or so	1 or 2 over the last several years	1 or 2 quite a few years back	Several in the last year or so	Several over the last several years	Many in the last year or so	Many over the last several years	N/A/Don't have this data
Regulated Data	65	54	52	13	4	3	2	632
Other personally identifiable information	68	51	42	15	9	4	4	623
Intellectual Property	43	35	31	10	10	2	6	680





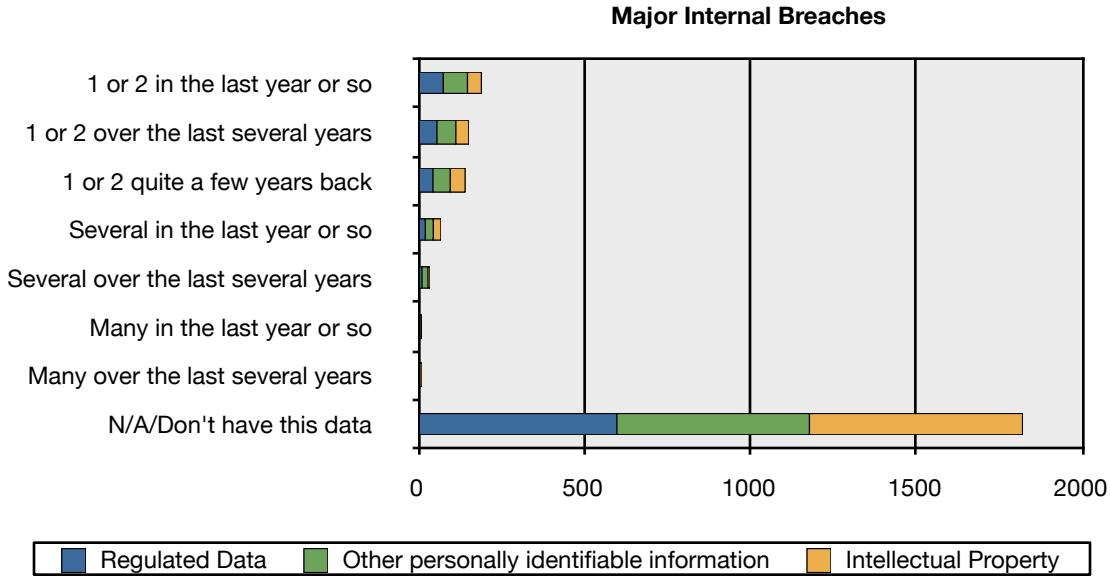
We've translated this into a percentage scale to better visualize the results:

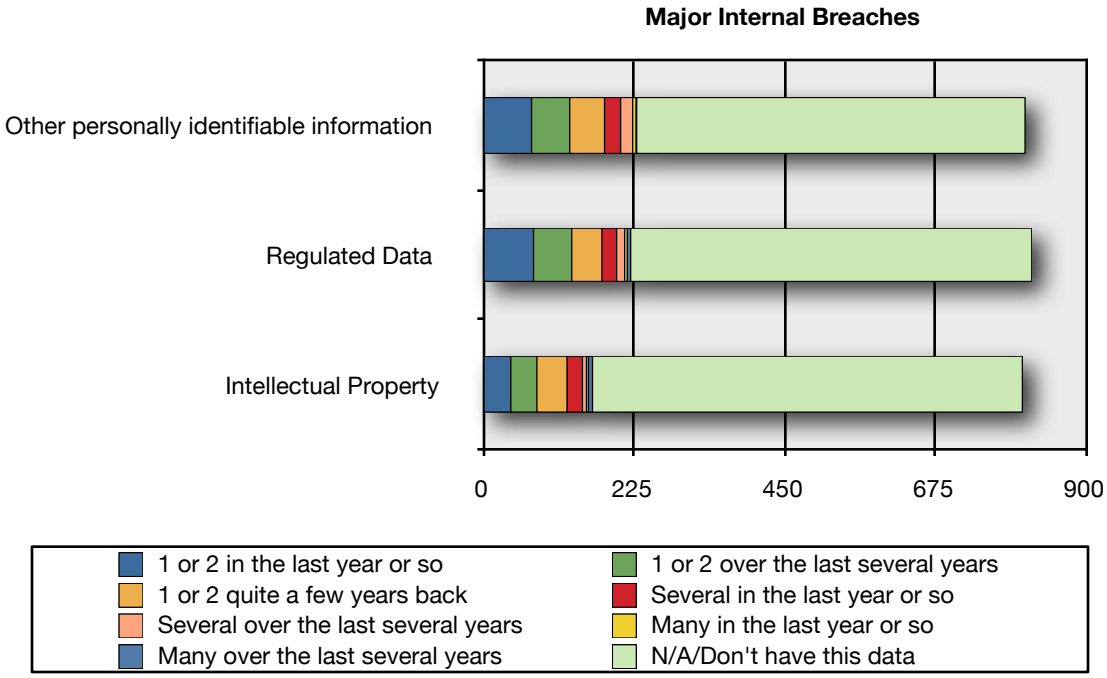

Major External Breaches (Percentage Scale)
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data
0%
25%
50%
75%
100%
Regulated Data
Other personally identifiable information
Intellectual Property

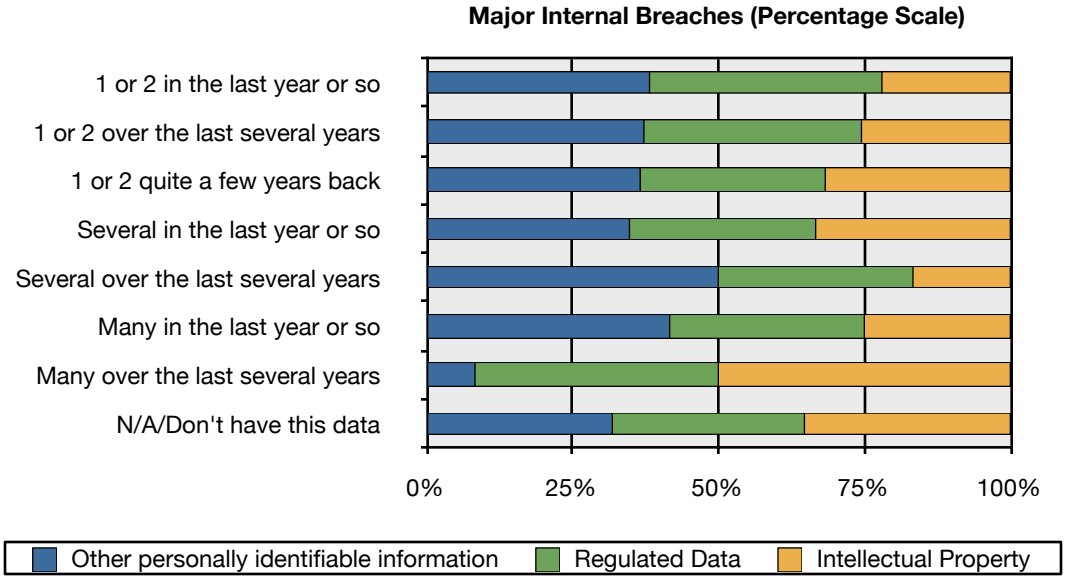

Major External Breaches (Percentage Scale)
Other personally identifiable information
Regulated Data
Intellectual Property
0%
25%
50%
75%
100%
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data

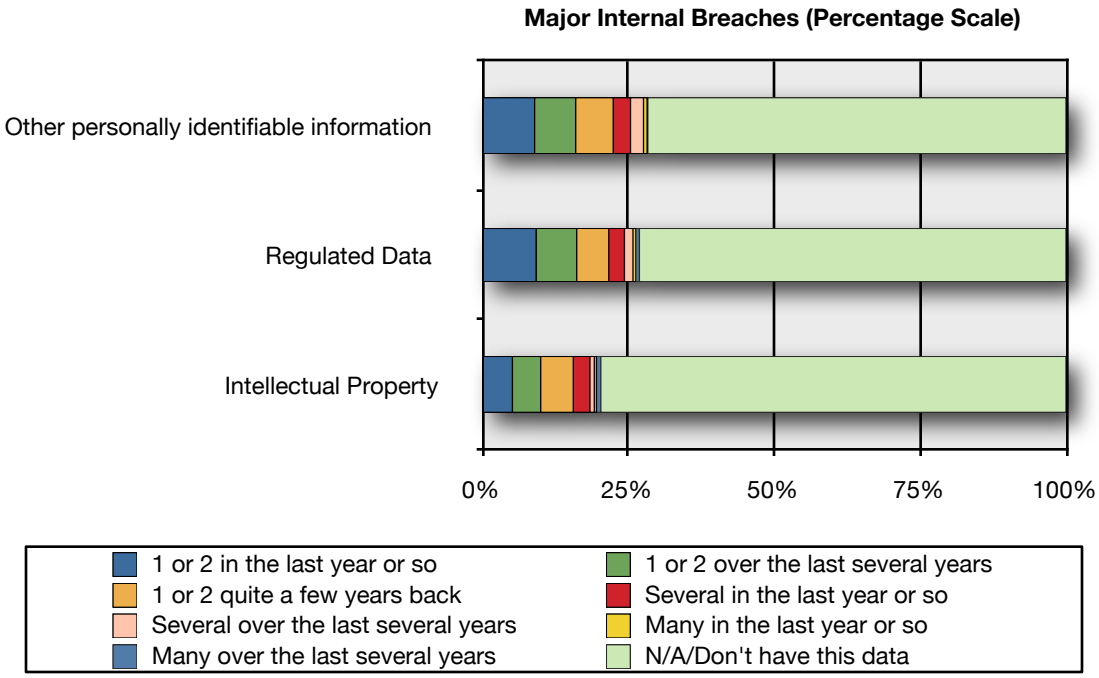
Internal Breaches:

	1 or 2 in the last year or so	1 or 2 over the last several years	1 or 2 quite a few years back	Several in the last year or so	Several over the last several years	Many in the last year or so	Many over the last several years	N/A/Don't have this data
Regulated Data	76	57	45	22	12	4	5	599
Other personally identifiable information	73	57	52	24	18	5	1	580
Intellectual Property	42	39	45	23	6	3	6	642



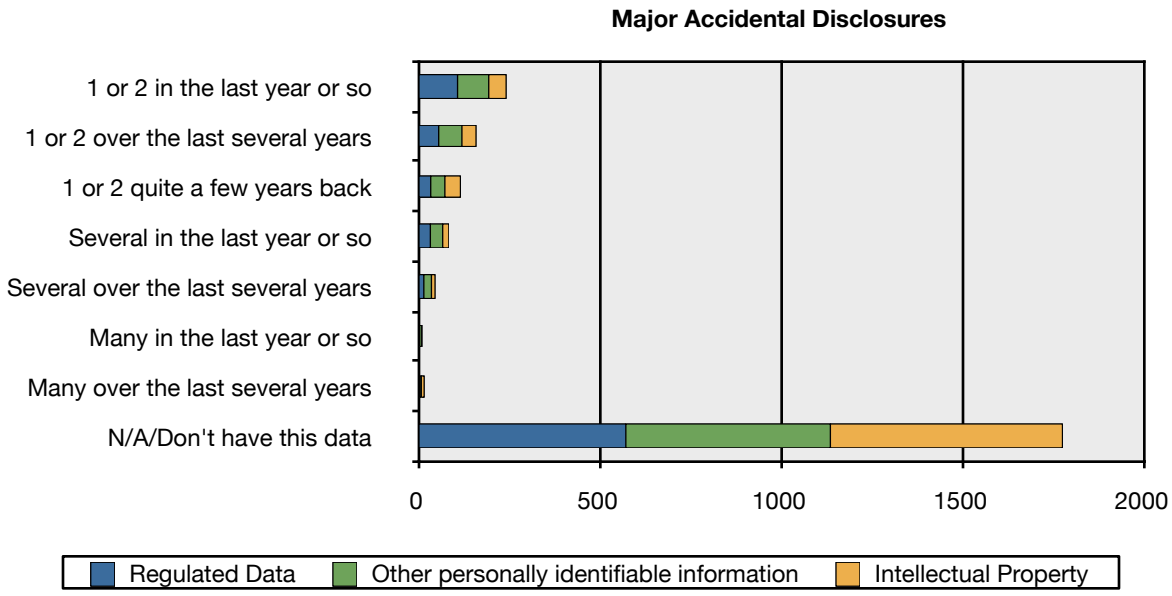

Major Internal Breaches
Other personally identifiable information
Regulated Data
Intellectual Property
0
225
450
675
900
1 or 2 in the last year or so
1 or 2 quite a few years back
Several over the last several years
Many over the last several years
1 or 2 over the last several years
Several in the last year or so
Many in the last year or so
N/A/Don't have this data

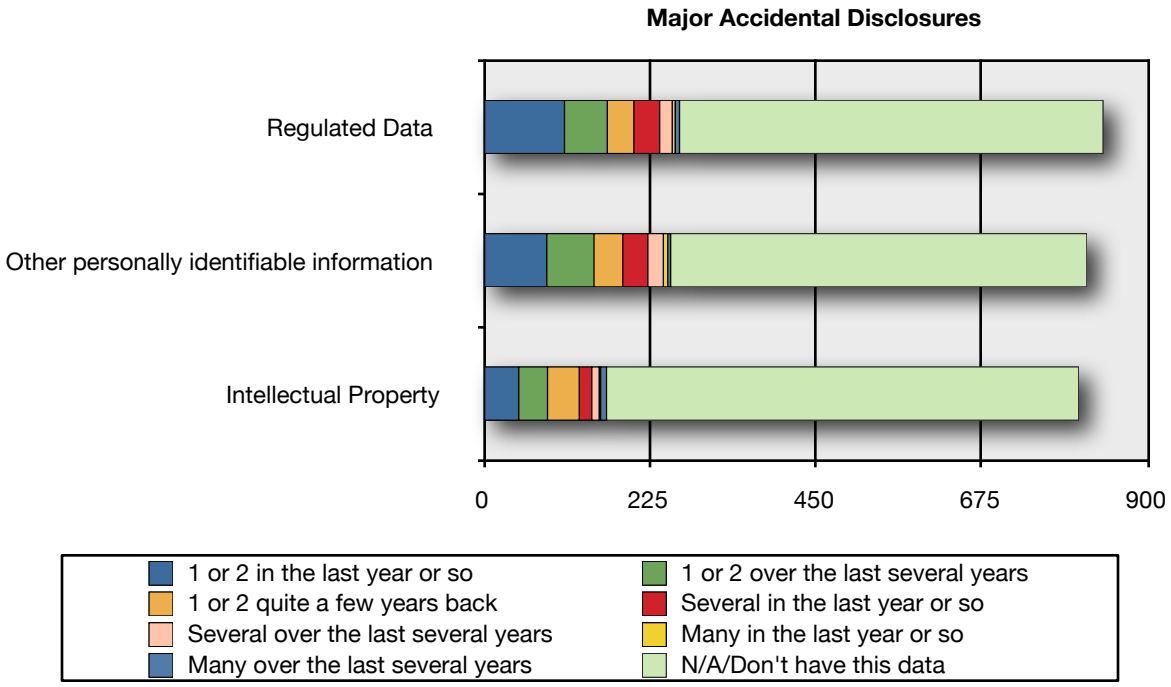

Major Internal Breaches (Percentage Scale)
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data
0%
25%
50%
75%
100%
Other personally identifiable information
Regulated Data
Intellectual Property

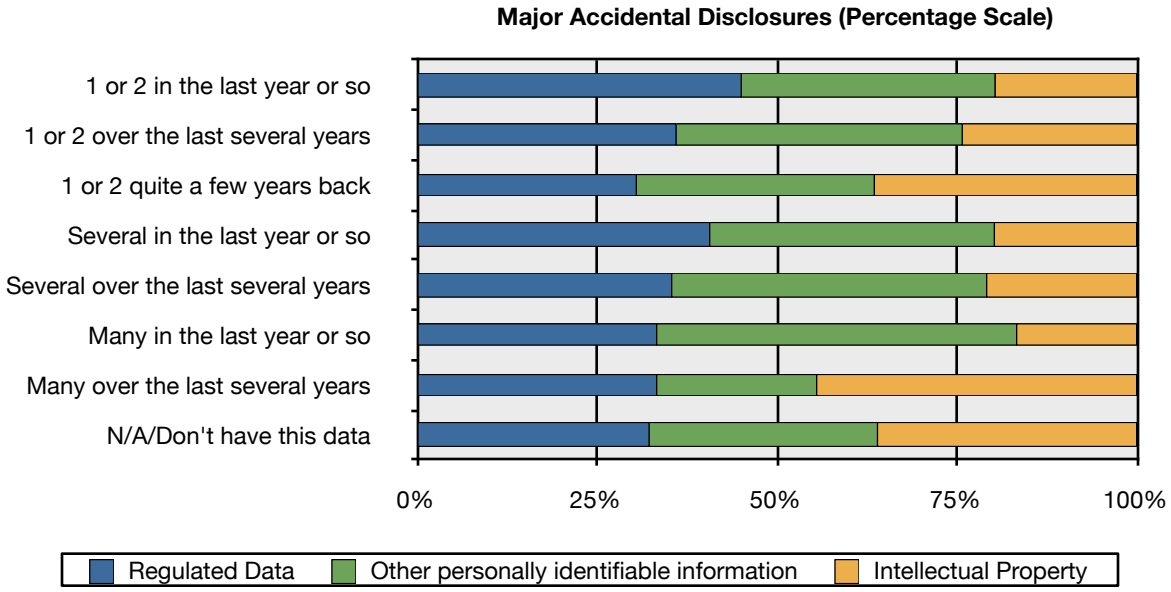

Major Internal Breaches (Percentage Scale)
Other personally identifiable information
Regulated Data
Intellectual Property
0%
25%
50%
75%
100%
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data

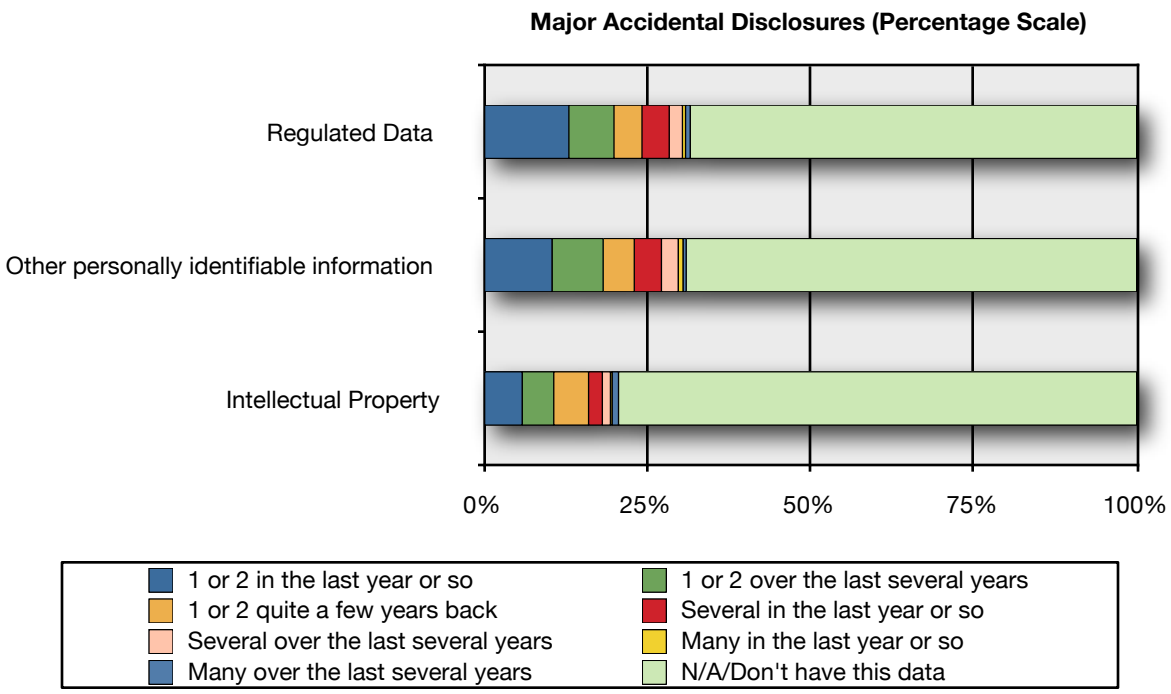
Accidental Disclosures:

	1 or 2 in the last year or so	1 or 2 over the last several years	1 or 2 quite a few years back	Several in the last year or so	Several over the last several years	Many in the last year or so	Many over the last several years	N/A/Don't have this data
Regulated Data	110	58	36	35	17	4	6	574
Other personally identifiable information	86	64	39	34	21	6	4	564
Intellectual Property	48	39	43	17	10	2	8	640




Major Accidental Disclosures
Regulated Data
Other personally identifiable information
Intellectual Property
0
225
450
675
900
1 or 2 in the last year or so
1 or 2 quite a few years back
Several over the last several years
Many over the last several years
1 or 2 over the last several years
Several in the last year or so
Many in the last year or so
N/A/Don't have this data


Major Accidental Disclosures (Percentage Scale)
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data
0%
25%
50%
75%
100%
Regulated Data
Other personally identifiable information
Intellectual Property

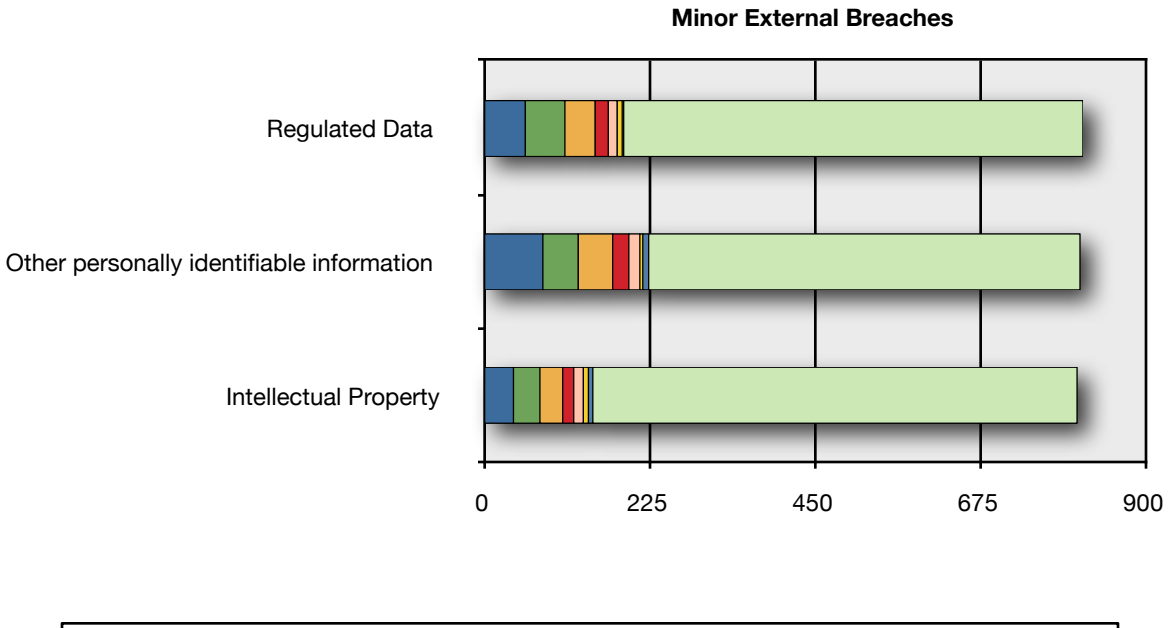

Major Accidental Disclosures (Percentage Scale)
Regulated Data
Other personally identifiable information
Intellectual Property
0%
25%
50%
75%
100%
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data

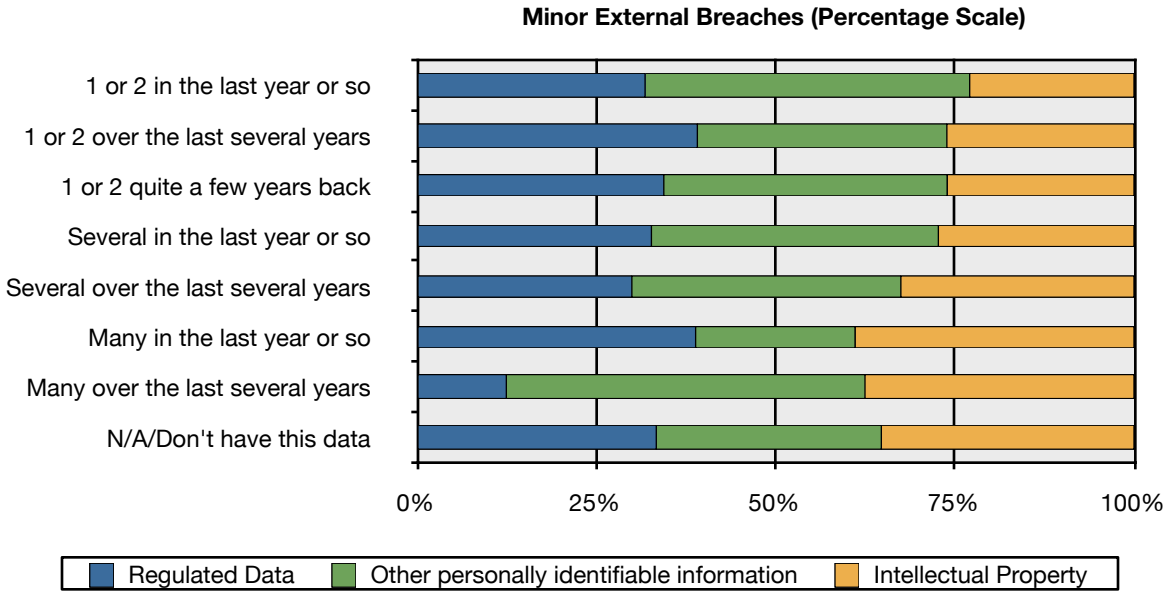
Minor Incidents

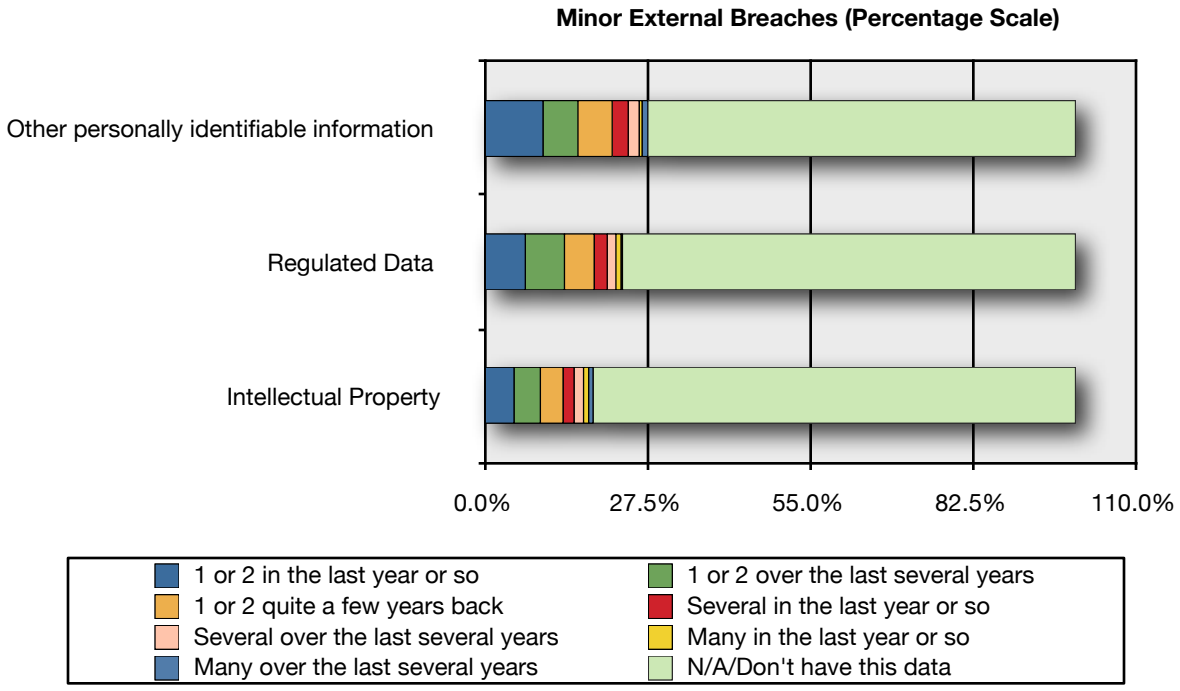
We asked, “Please estimate the following **minor** successful attacks you have experienced for these different data types:”

External Breaches

	1 or 2 in the last year or so	1 or 2 over the last several years	1 or 2 quite a few years back	Several in the last year or so	Several over the last sev-eral years	Many in the last year or so	Many over the last several years	N/A/Don't have this data
Regulated Data	57	54	41	18	12	7	2	625
Other per-sonally identifiable informa-tion	81	48	47	22	15	4	8	587
Intellectual Property	41	36	31	15	13	7	6	659

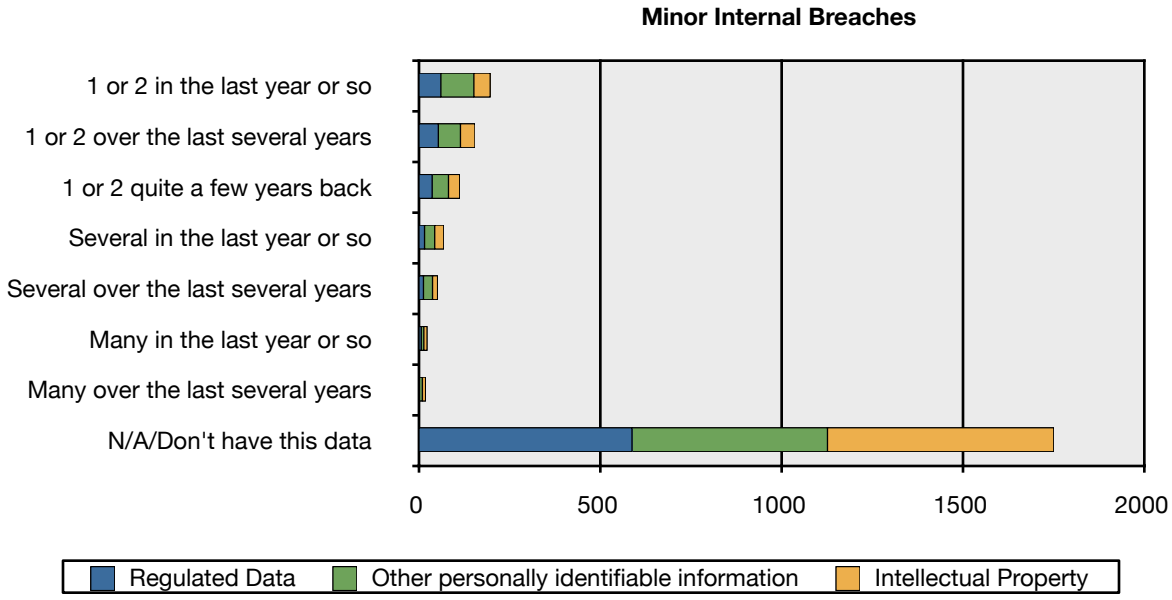

Minor External Breaches
Regulated Data
Other personally identifiable information
Intellectual Property
0
225
450
675
900
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data

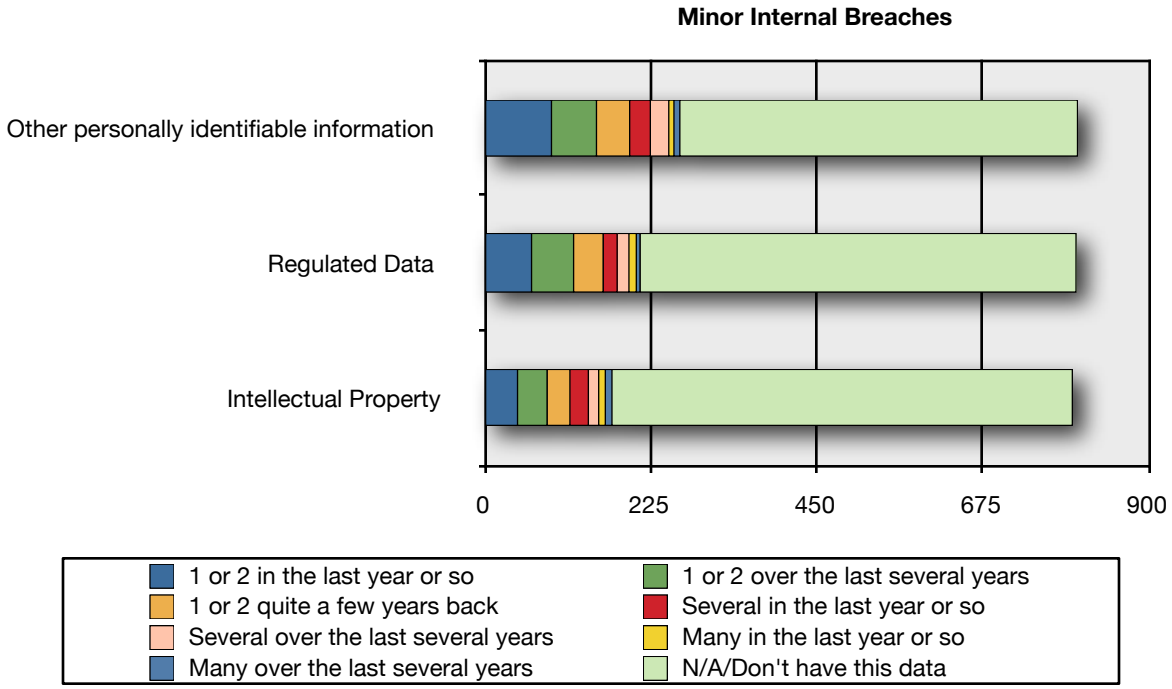

Minor External Breaches (Percentage Scale)
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data
0%
25%
50%
75%
100%
Regulated Data
Other personally identifiable information
Intellectual Property

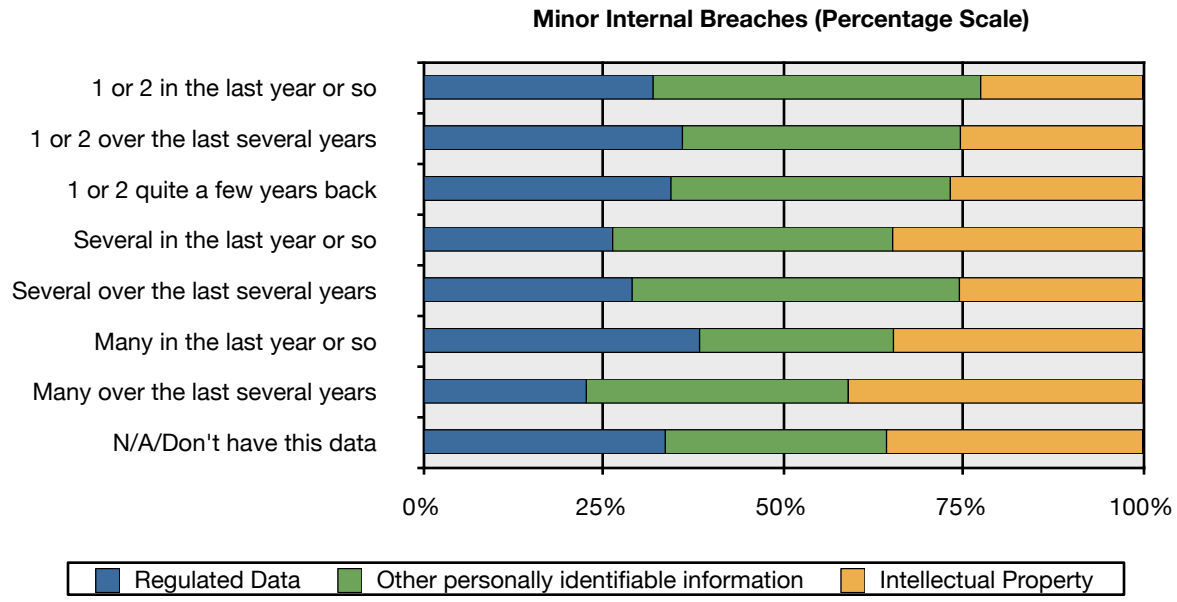


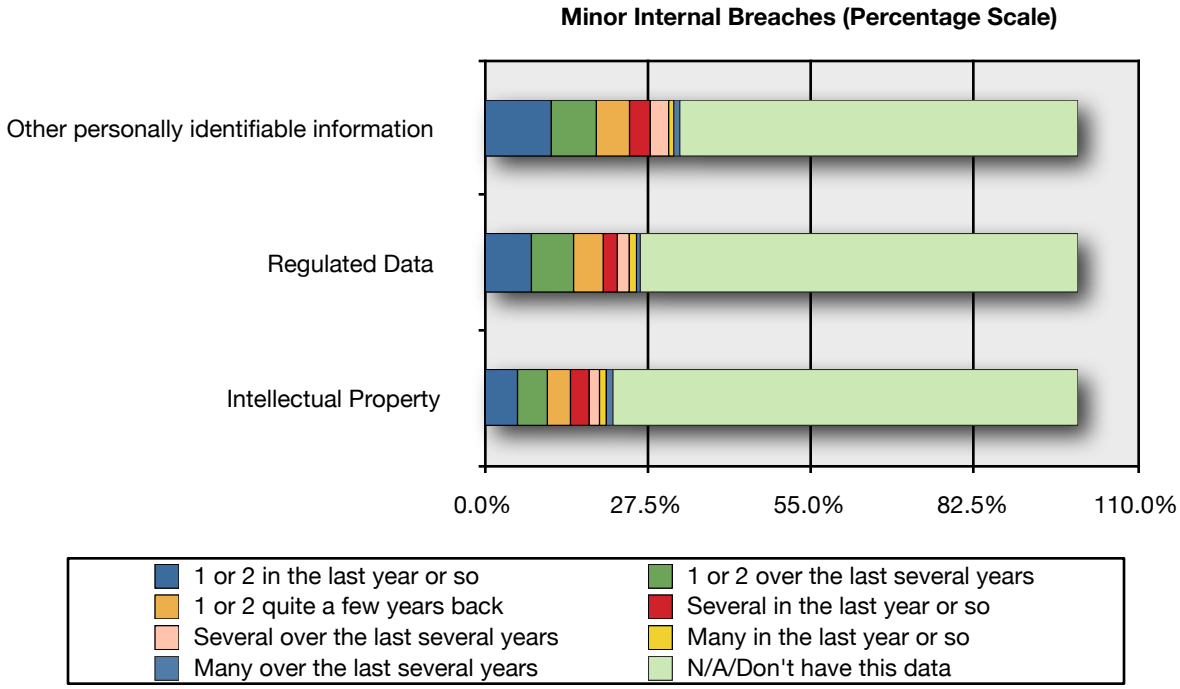
Internal Breaches

	1 or 2 in the last year or so	1 or 2 over the last several years	1 or 2 quite a few years back	Several in the last year or so	Several over the last several years	Many in the last year or so	Many over the last several years	N/A/Don't have this data
Regulated Data	64	57	40	19	16	10	5	591
Other personally identifiable information	91	61	45	28	25	7	8	539
Intellectual Property	45	40	31	25	14	9	9	624


Minor Internal Breaches
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data
0
500
1000
1500
2000
Regulated Data
Other personally identifiable information
Intellectual Property

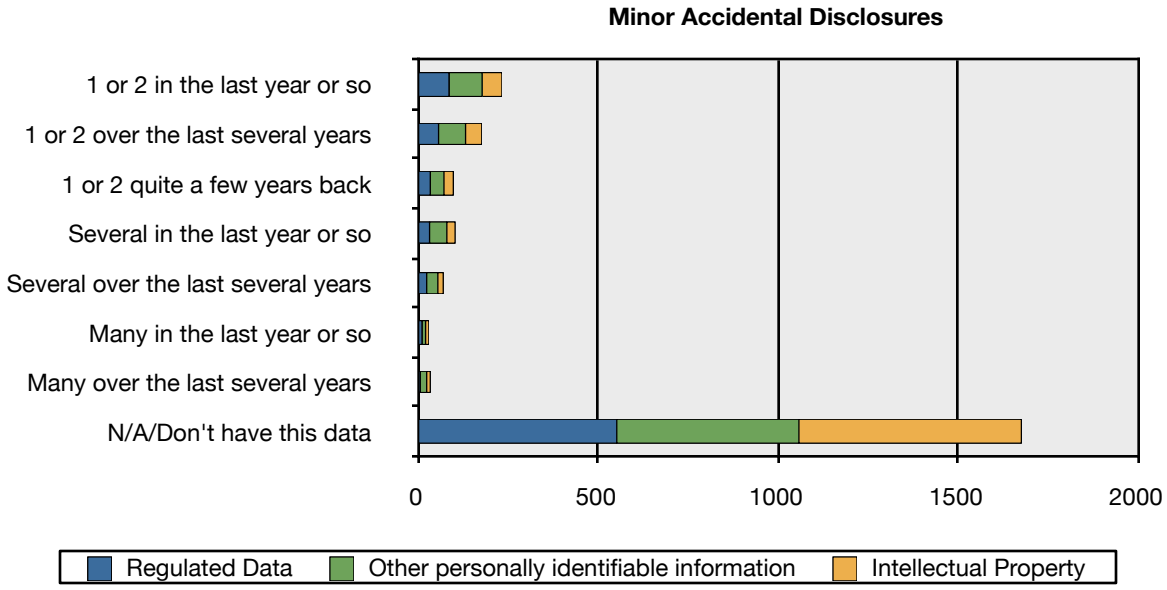

Minor Internal Breaches
Other personally identifiable information
Regulated Data
Intellectual Property
0
225
450
675
900
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data

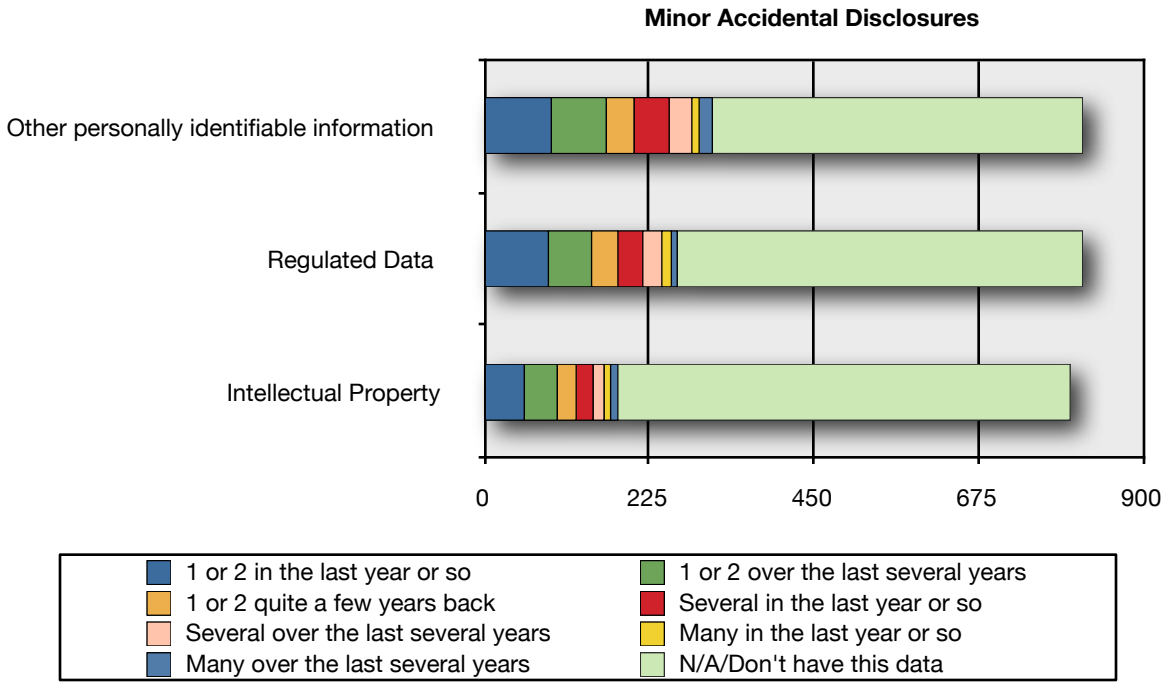

Minor Internal Breaches (Percentage Scale)
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data
0%
25%
50%
75%
100%
Regulated Data
Other personally identifiable information
Intellectual Property

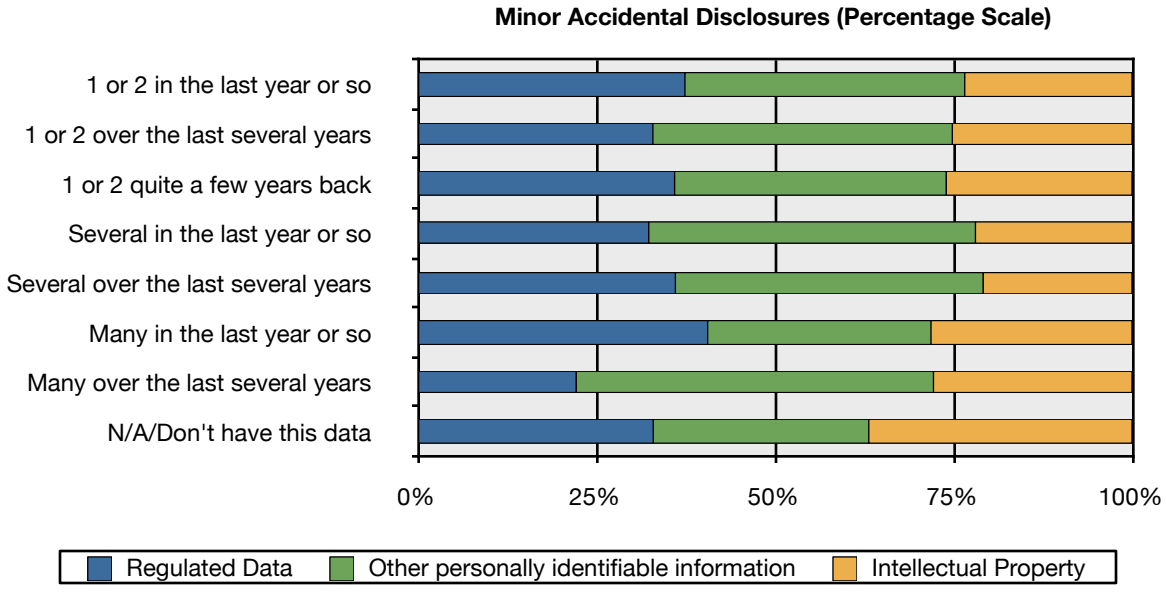

Minor Internal Breaches (Percentage Scale)
Other personally identifiable information
Regulated Data
Intellectual Property
0.0%
27.5%
55.0%
82.5%
110.0%
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data

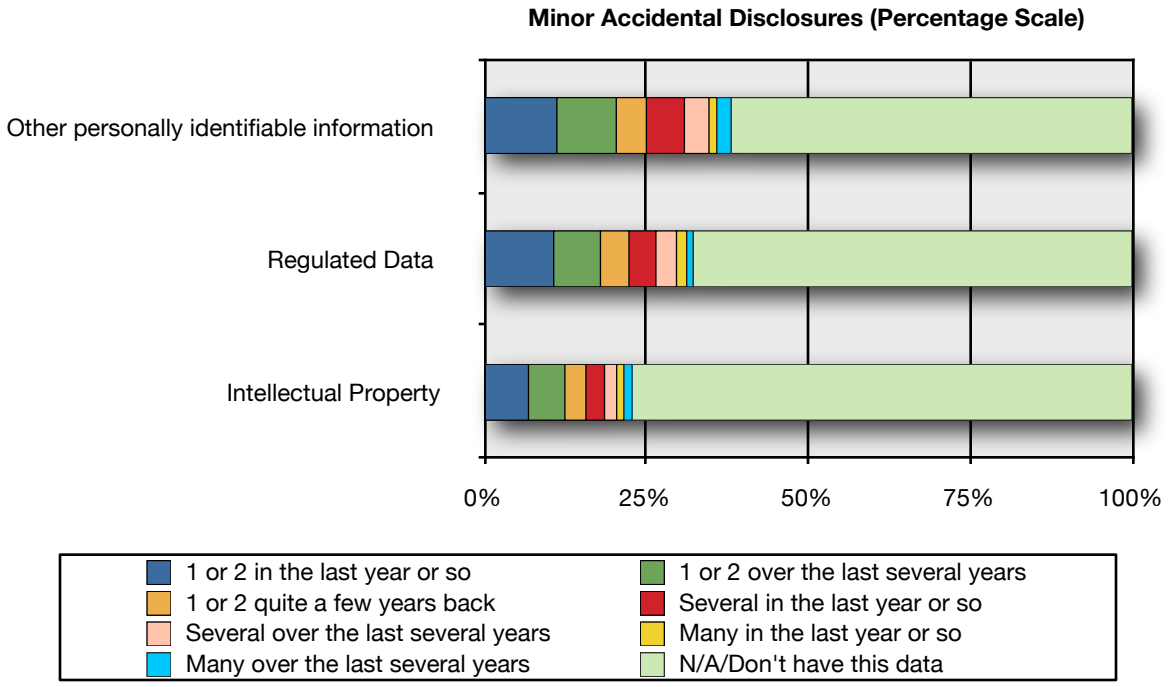
Accidental Disclosures

	1 or 2 in the last year or so	1 or 2 over the last several years	1 or 2 quite a few years back	Several in the last year or so	Several over the last several years	Many in the last year or so	Many over the last several years	N/A/Don't have this data
Regulated Data	88	59	36	34	26	13	8	554
Other personally identifiable information	92	75	38	48	31	10	18	506
Intellectual Property	55	45	26	23	15	9	10	618




Minor Accidental Disclosures
Other personally identifiable information
Regulated Data
Intellectual Property
0
225
450
675
900
1 or 2 in the last year or so
1 or 2 quite a few years back
Several over the last several years
Many over the last several years
1 or 2 over the last several years
Several in the last year or so
Many in the last year or so
N/A/Don't have this data

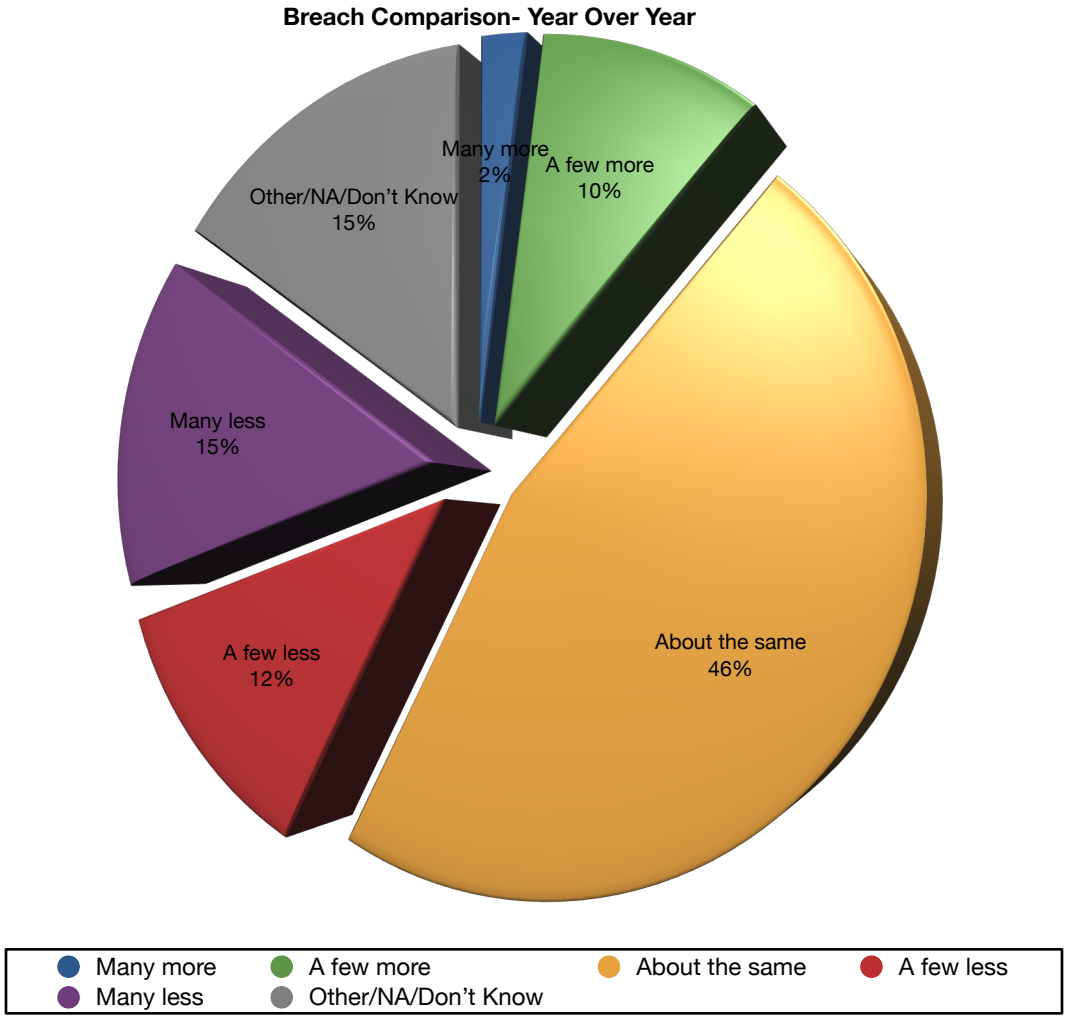

Minor Accidental Disclosures (Percentage Scale)
1 or 2 in the last year or so
1 or 2 over the last several years
1 or 2 quite a few years back
Several in the last year or so
Several over the last several years
Many in the last year or so
Many over the last several years
N/A/Don't have this data
0%
25%
50%
75%
100%
Regulated Data
Other personally identifiable information
Intellectual Property



Year Over Year Comparisons

We also asked respondents to estimate how their incident numbers changed over the past 2 years; "How would you characterize the overall number of breaches you have experienced this year (12 months) compared to the previous year?"

	Responses
Many more	21
A few more	98
About the same	465
A few less	123
Many less	153
Other/NA/Don't Know	153



Conclusions

When we review the reported incidents across the different categories, an interesting pattern emerges The following table summarizes all responses in each category. Keep in mind this *does not represent total breaches* since we are consolidating any response where a breach was reported (no matter how many incidents over any time period). **These are *counts of responses*, not sums of incidents.**

Major Incidents

	External	Internal	Accidental	*Total*
Regulated Data	193	221	266	680
Other PII	193	230	254	677
IP	137	164	167	468
Total	**523**	**615**	**687**	**1825**

Minor Incidents

	External	Internal	Accidental	*Total*
Regulated Data	191	211	264	666
Other PII	225	265	312	802
IP	149	173	183	505
Total	**565**	**649**	**759**	**1973**

For both major and minor incidents we see that most incidents are accidental, followed by internal and lastly by external causes. We see more of a difference emerge as we compare across data types, with more exposure of unregulated personal information in minor incidents compared to major, more regulated data (relatively) exposed in major incidents, and intellectual property with the least volume of incidents across both major and minor categories.

Since we can't assume all participants have the equal ability to detect and measure breaches, *we can't assume that these responses accurately represent the real incidents the organizations suffer*. For example, as we will see later far more organizations deploy email filtering than most other data security controls, and as a result are more likely to detect incidents originating over email from internal sources than external attacks using covert channels.

The most interesting trend is the relative decline in incidents reported year over year. 46% of participants reported about the same number of incidents, with 27% reporting fewer incidents, and only 12% reporting a relative increase.

Controls Effectiveness

What do we (think) really works?

For the core of the survey we asked participants a series of questions on the perceived effectiveness of various data security controls. Note that we call this *perceived* effectiveness, not actual effectiveness, since we don't have consistent methodologies and metrics used equally by different organizations to measure the effectiveness or efficiency of their controls. This is a huge gap in the security industry, forcing us to rely more on anecdote and perceptions than hard measurements. Our hope is that the volume of our responses, in aggregate, translate these perceptions to some sort of operational reality.

Since we couldn't ask about every possible security control we decided to focus on those that met the following criteria:

- Controls that, in our experience, are commonly used for data security.
- Data security controls required by specific regulations (e.g. full drive encryption, database encryption).
- Data security controls frequently hyped in the press and social media.
- Controls that our end user customers most frequently ask us about.

The final list includes the following 18 controls, plus we asked people to include additional controls in the comments associated with each question:

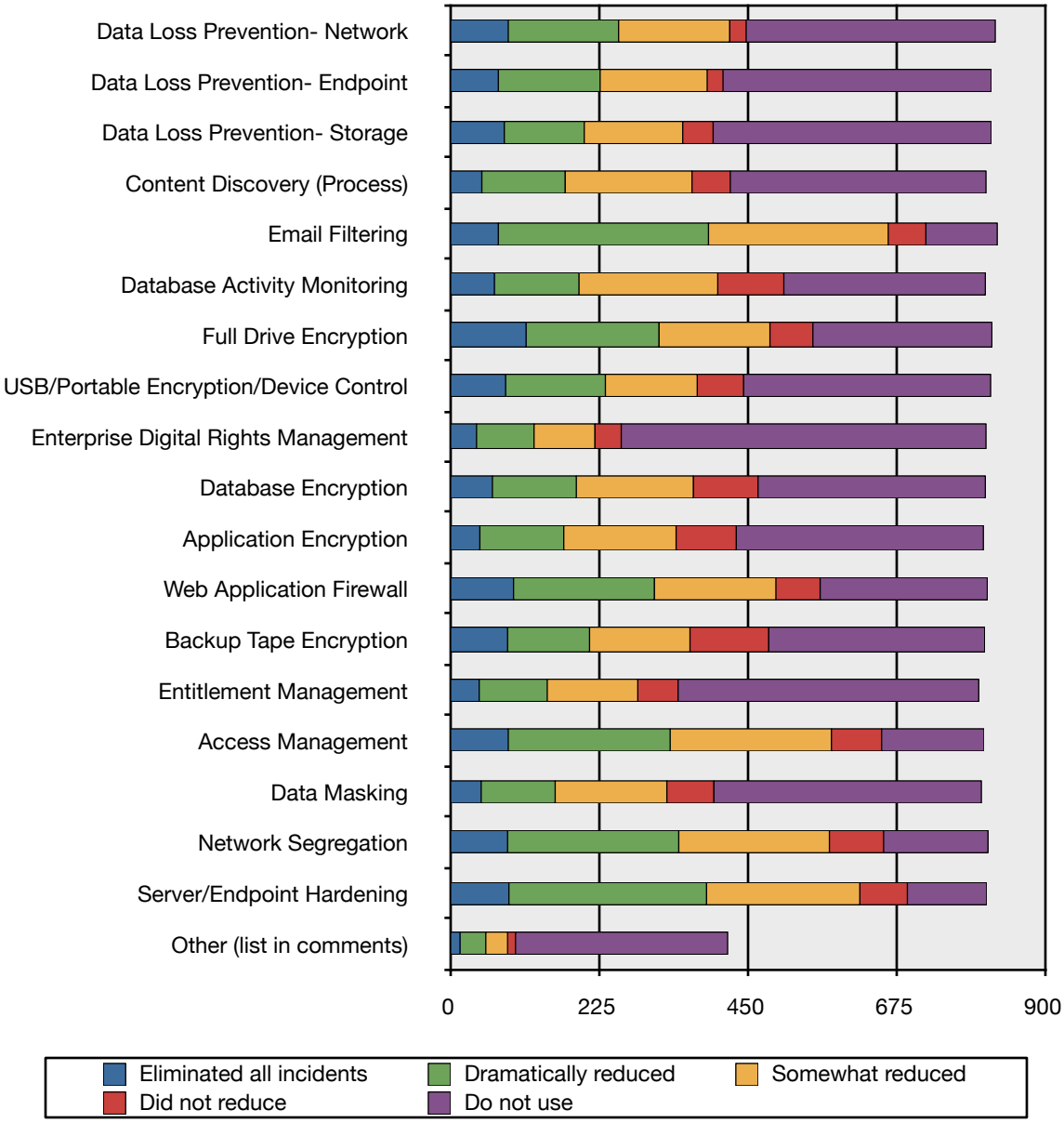
- Data Loss Prevention- Tools capable of scanning for content with advanced techniques (more than regular expressions).
- Content Discovery- The process of finding where sensitive information is stored in your organization, which may be a manual process or leverage a tool like DLP.
- Email Filtering- Basic keyword/regular expression filtering of email.
- Database Activity Monitoring- Tools to actively monitor all or some database activity (more than basic audit logs).
- Full Drive Encryption- Encryption of laptop/desktop drives.
- Portable Device Control (USB blocking)- Basic blocking or management of USB drives.
- Database Encryption- Encryption of all or some of database content.
- Application Encryption- Encryption of sensitive content in an application as it is collected.
- Entitlement Management- Actively scanning and managing user permissions for file/content access.
- Access Management- Tools to restrict access to files/content beyond standard access controls.
- Data Masking- Generation of test/development data based on production data, but scrambling/masking sensitive values.
- Network Segregation- Isolating sensitive data/applications on subnets.
- Server/Endpoint Hardening- Locking down systems, including whitelisting, HIPS, and other lockdown/patch management.

We also broke effectiveness out into three categories- reducing the number of incidents, reducing the severity of incidents, and reducing compliance costs. We closed by asking participants to rate their top 3 most effective controls, and their least effective control.

How well do controls reduce incidents?

We asked participants, "For the following security controls, rate their effectiveness at reducing the number of incidents/ breaches in your organization:"

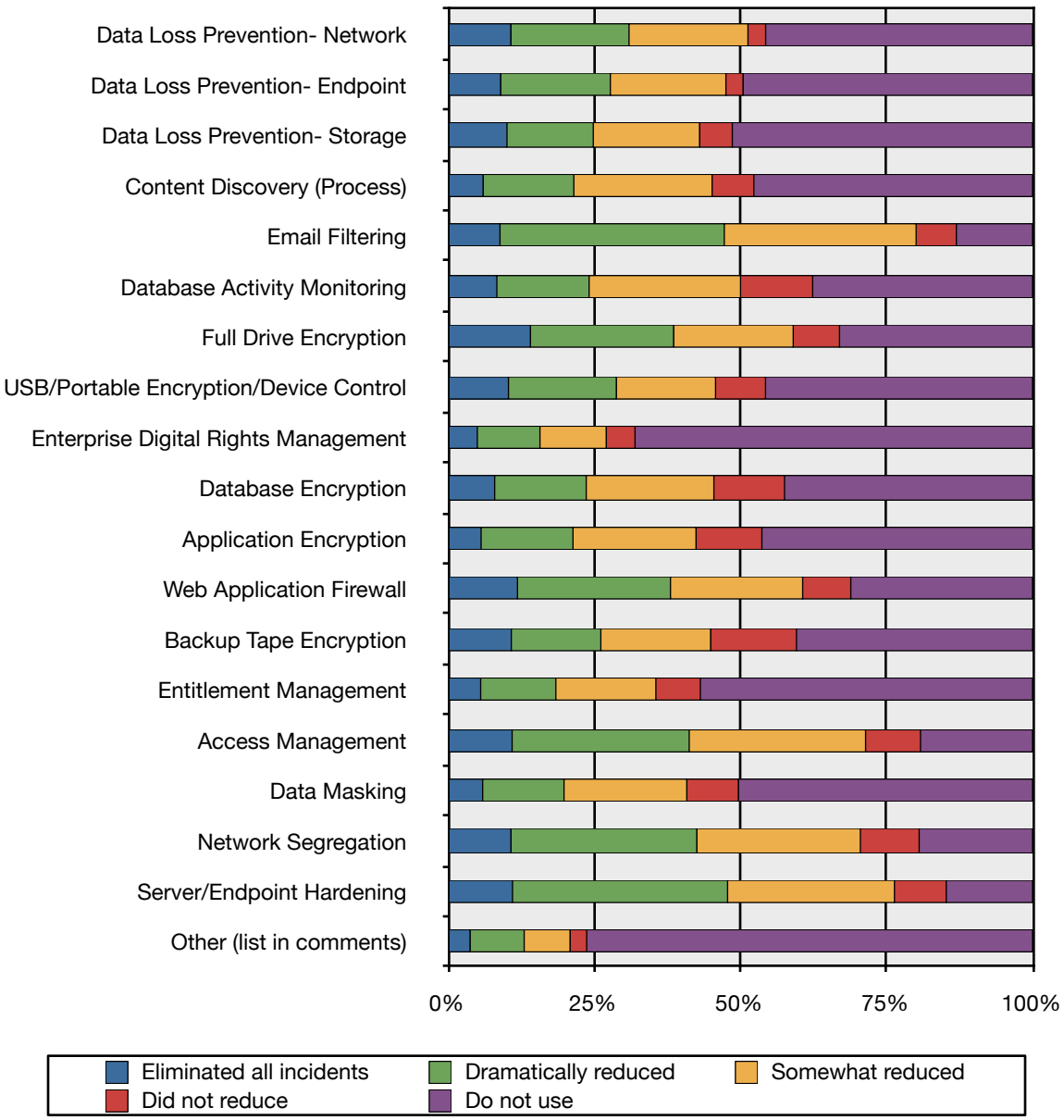
Control	Eliminated all incidents	Dramatically reduced	Somewhat reduced	Did not reduce	Do not use
Data Loss Prevention-Network	89	167	168	25	377
Data Loss Prevention-Endpoint	74	154	162	24	406
Data Loss Prevention-Storage	83	121	149	46	421
Content Discovery (Process)	49	126	192	58	387
Email Filtering	74	318	272	57	108
Database Activity Monitoring	68	128	210	100	305
Full Drive Encryption	116	201	168	65	271
USB/Portable Media Encryption or Device Control	85	151	139	70	374
Enterprise Digital Rights Management	41	87	92	40	552
Database Encryption	65	127	177	98	344
Application Encryption	46	127	170	91	374
Web Application Firewall	97	213	184	67	253
Backup Tape Encryption	88	124	152	119	327
Entitlement Management	45	103	137	61	455
Access Management	89	245	244	76	155
Data Masking	48	112	169	71	405
Network Segregation	88	259	228	82	158
Server/Endpoint Hardening	90	299	232	72	120
Other (list in comments)	16	39	33	12	321



As you can see, most of the data security specific controls (like DLP) are not nearly as widely deployed as more traditional controls like server/endpoint hardening. Aside from one write-in suggesting “well armed ninjas”, of other tools listed in the comments the most common was user education.

To further visualize these results, let’s look at them on a percentage scale:

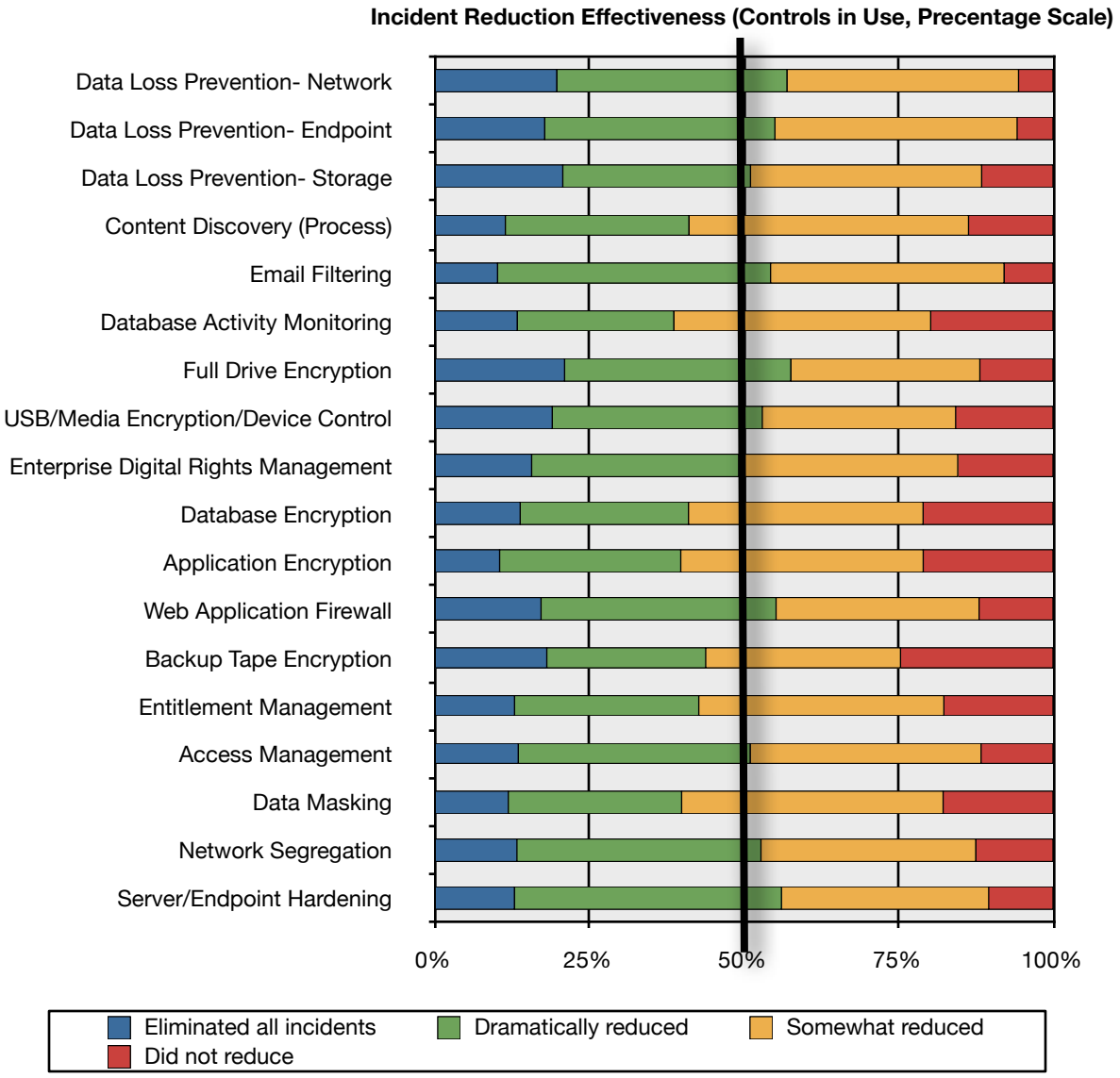
Incident Count Effectiveness (Percentage Scale)



While some of the numbers seem to be low, these results show far deeper penetration of data-security-specific tools than is commonly believed. Our assessment is that much of this is due to survey bias, since those completing this survey are more likely to be educated and interested on data security than the general security population. For example, our experience does not validate that one in four organizations is using Enterprise Digital Rights Management.

Our recommendation is to focus on the perceived effectiveness, not the volume of deployments. *No survey with a self-selected audience will reflect deployment numbers as accurately as random sampling*.

To refine the view of effectiveness here is the same data charted on a percentage scale, excluding the 'do not use" response:



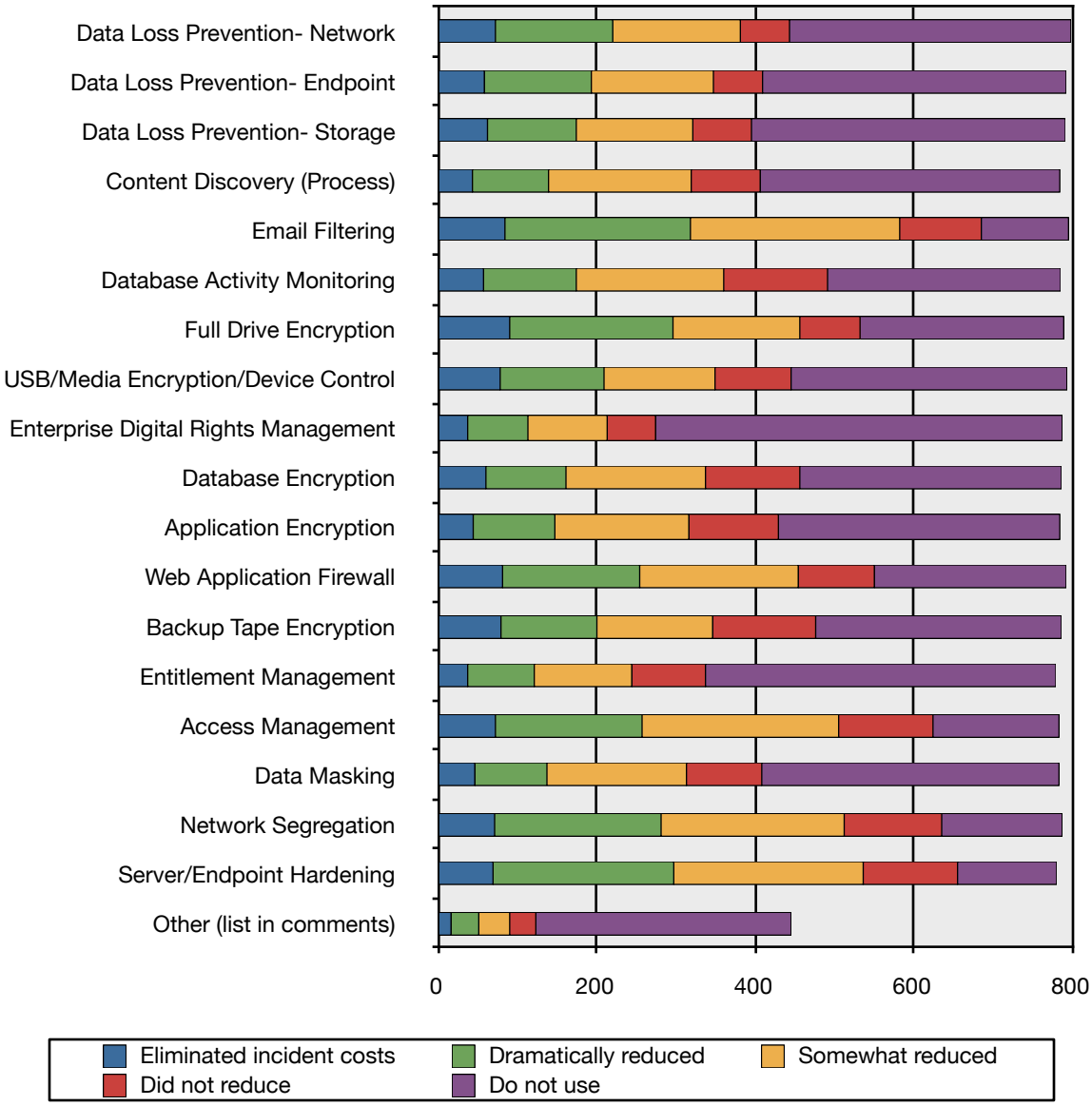
We also added a marker at 50% to better delineate those tools reported as showing greater effectiveness. It's now easier to see that the top 5 rated controls for reducing the number of breaches are network DLP, full drive encryption, web application firewalls, server/endpoint hardening, and endpoint DLP.

How well do controls reduce incident severity?

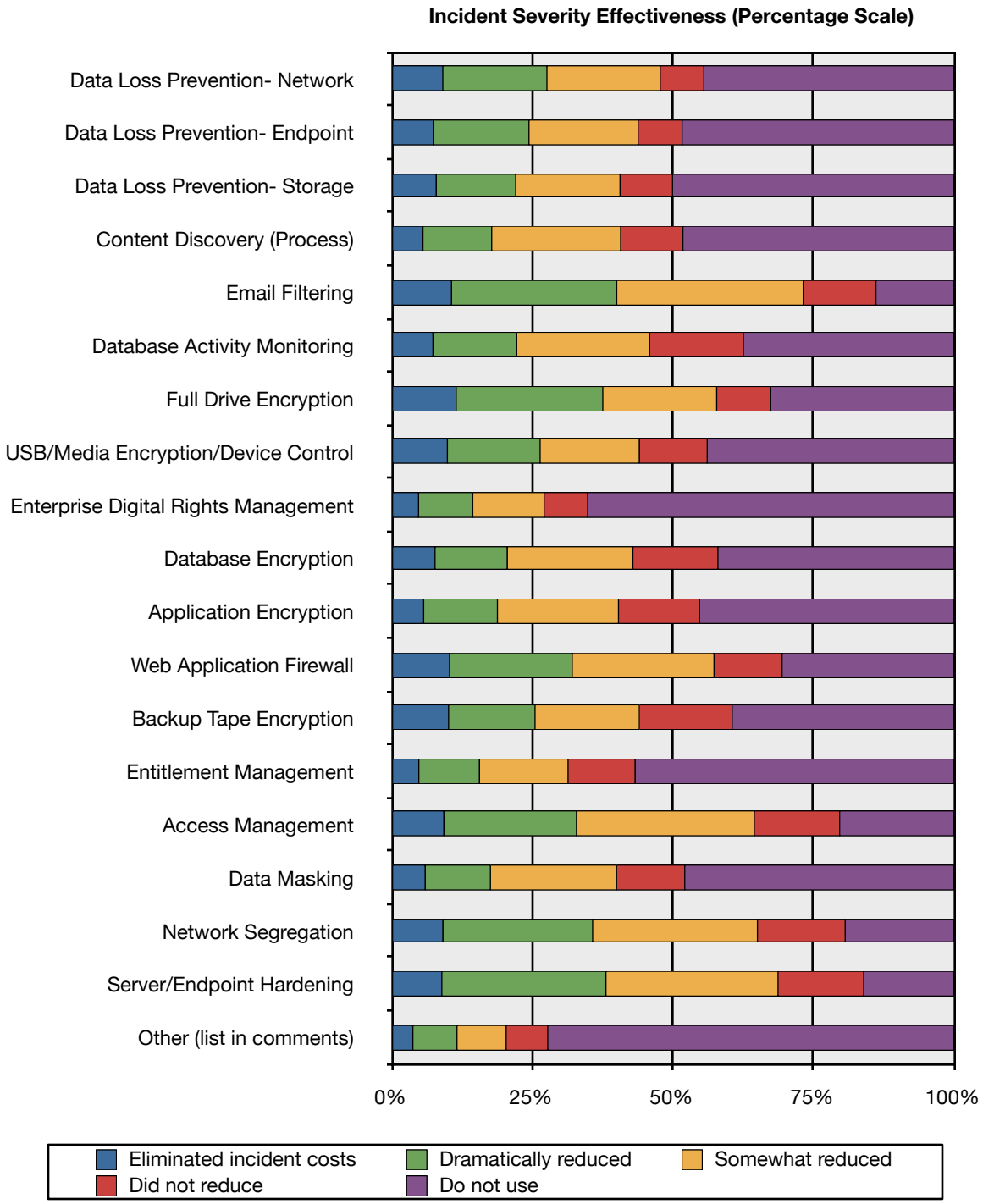
For this question we asked participants, "For the following data security controls, please rate their effectiveness at reducing the impact/costs of incidents:"

Control	Eliminated incident costs	Dramatically reduced	Somewhat reduced	Did not reduce	Do not use
Data Loss Prevention- Network	73	148	161	62	355
Data Loss Prevention- Endpoint	59	135	154	62	383
Data Loss Prevention- Storage	63	112	147	74	396
Content Discovery (Process)	44	96	180	87	378
Email Filtering	85	234	264	103	110
Database Activity Monitoring	58	117	186	131	294
Full Drive Encryption	91	206	160	76	257
USB/Portable Media Encryption or Device Control	79	131	140	96	348
Enterprise Digital Rights Management	38	76	100	61	513
Database Encryption	61	101	176	119	330
Application Encryption	45	103	169	113	355
Web Application Firewall	82	173	200	96	242
Backup Tape Encryption	80	121	146	130	310
Entitlement Management	38	84	123	93	442
Access Management	73	185	248	119	159
Data Masking	47	91	176	95	375
Network Segregation	72	210	231	123	152
Server/Endpoint Hardening	70	228	239	119	125
Other (list in comments)	17	35	39	33	322

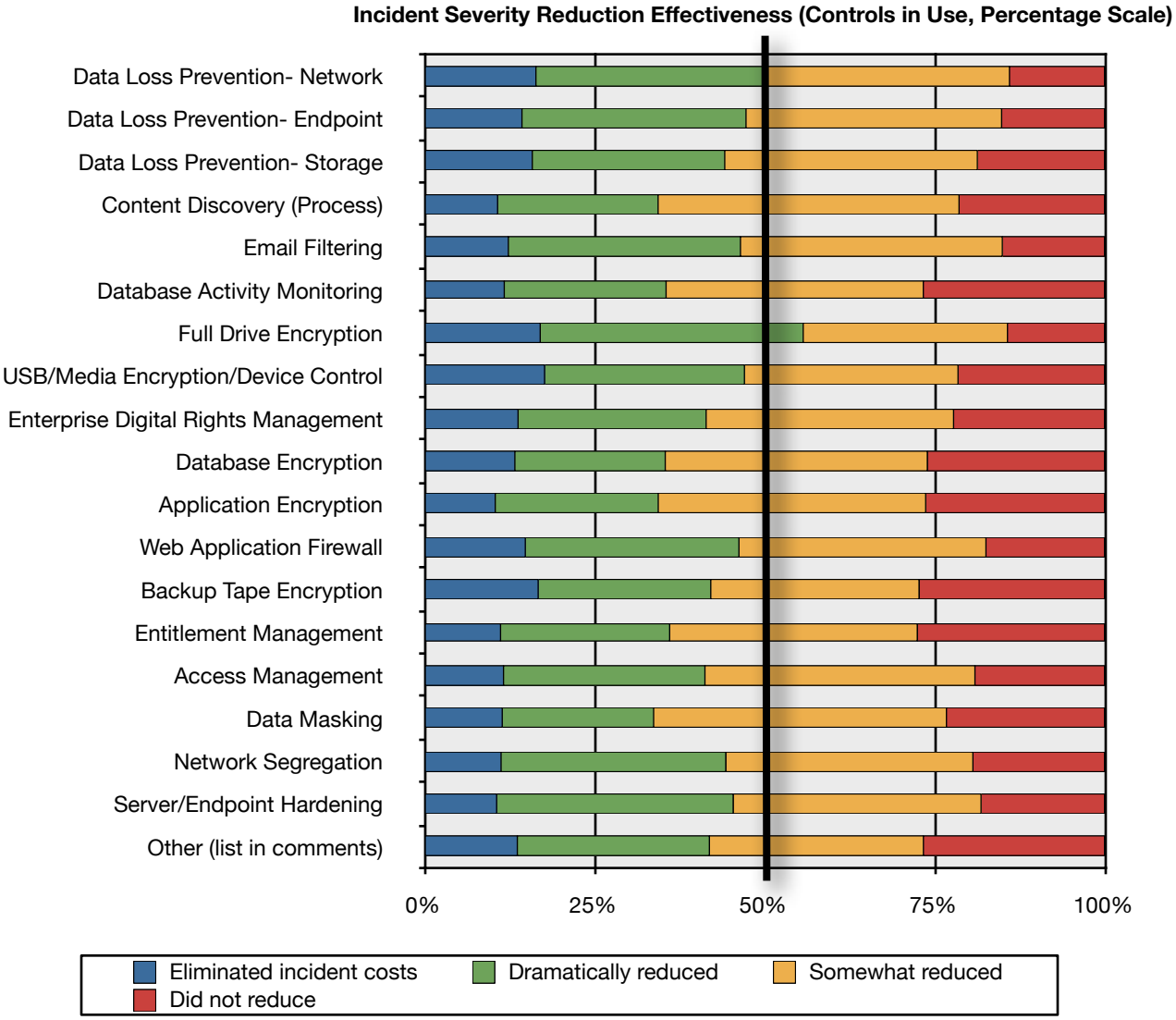
As with the previous question, user education was the most common write-in control (although it seems well armed ninjas only reduce incident occurrence, not severity, since they weren't listed in these responses).



As before, here is the same data on a percentage scale:



And finally, the same data focused only on those that reported using the controls:



With this visualization the differentiation is more apparent. Only two controls hit the 50% mark for eliminating or dramatically reducing incident severity- network DLP and full drive encryption. endpoint DLP, email filtering, USB/portable media encryption and device control, and web application firewalls round out the top 5. In general all the ratings are lower than those for reducing the number of incidents.

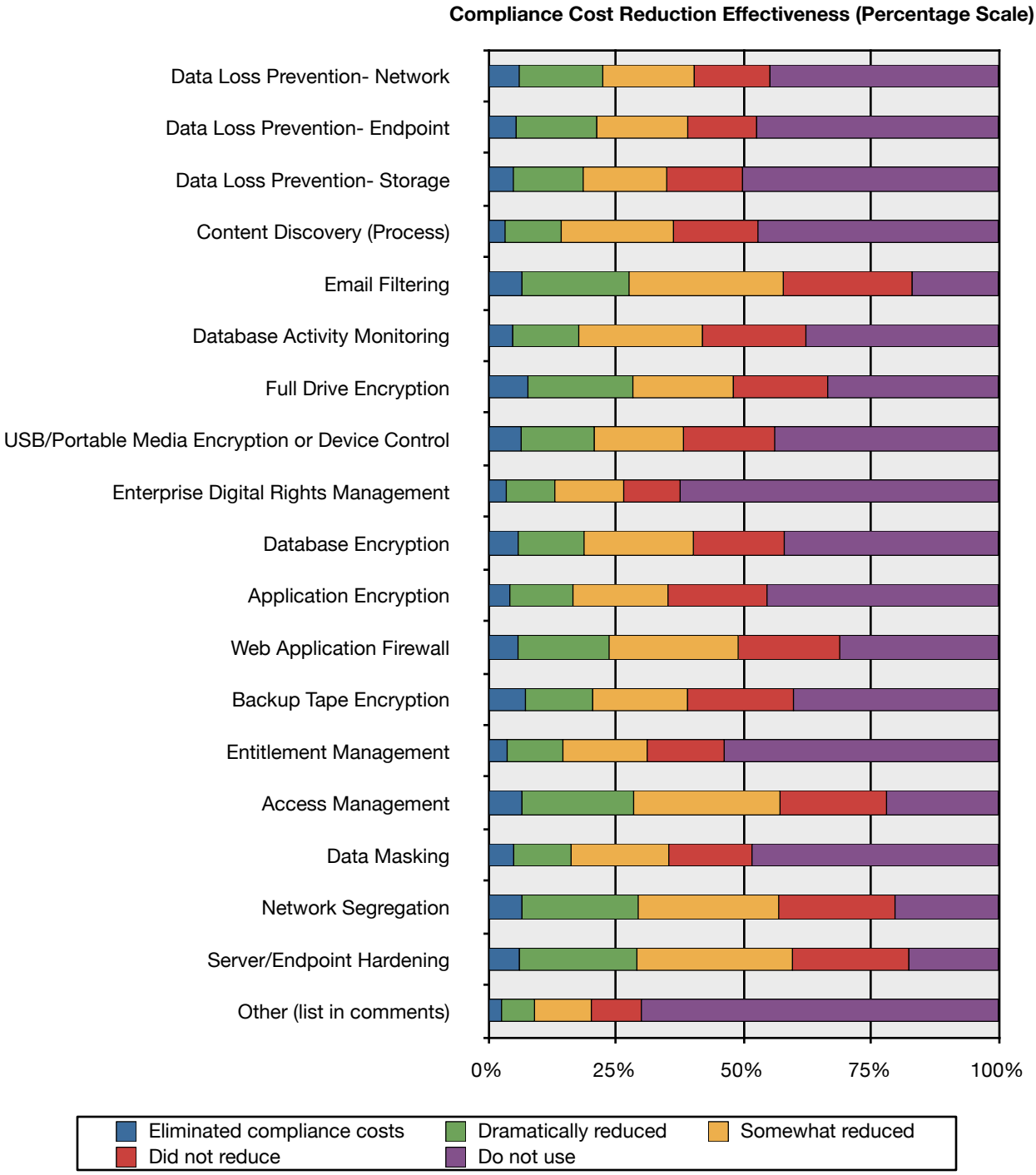
Do controls help reduce compliance costs?

For our final question on the effectiveness of specific controls we decided to focus on their capability to reduce compliance costs. We asked, "For the following data security controls, please rate their effectiveness at reducing compliance costs:"

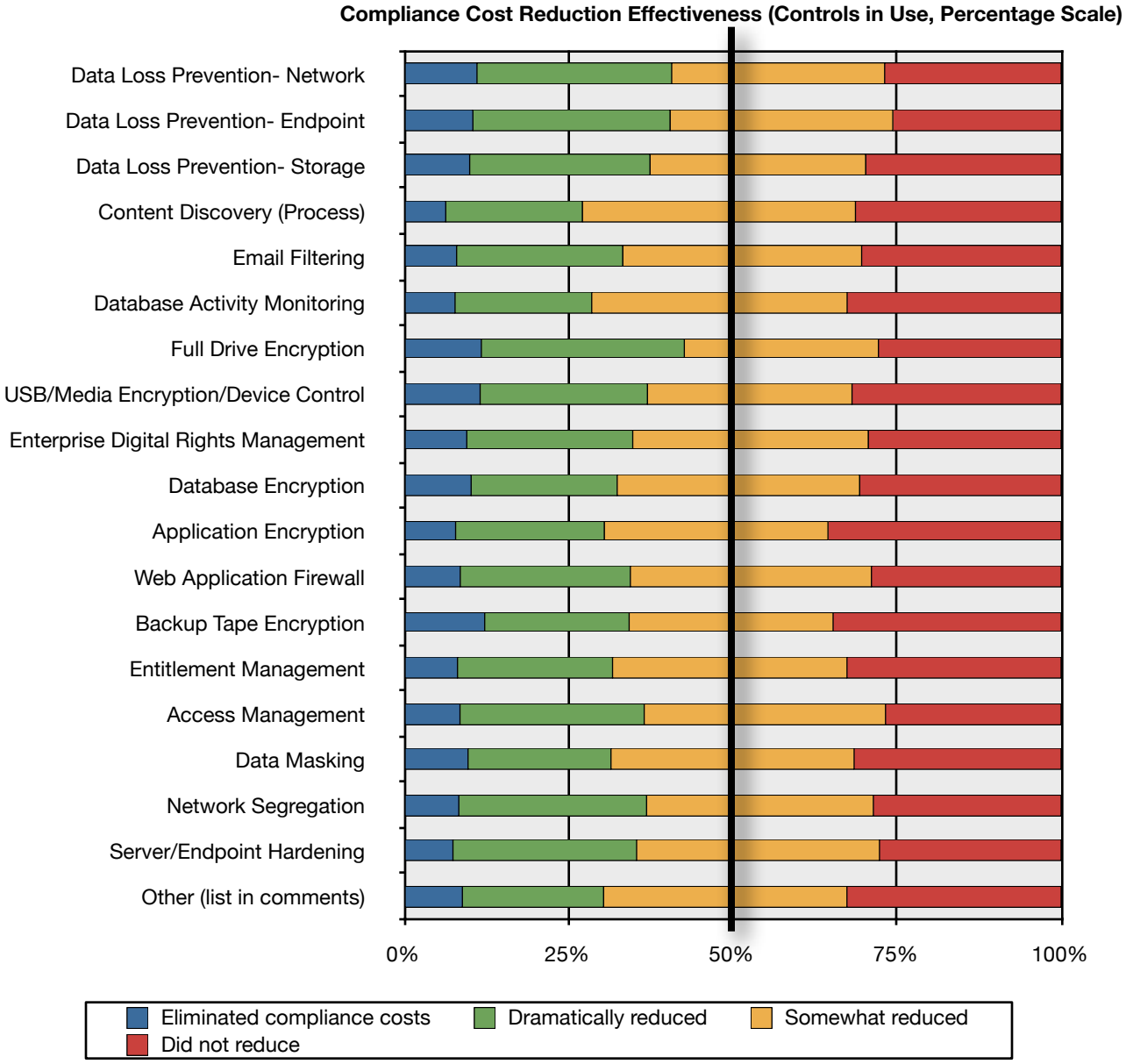
Controls	Eliminated compliance costs	Dramatically reduced	Somewhat reduced	Did not reduce	Do not use
Data Loss Prevention- Network	48	128	140	116	350
Data Loss Prevention- Endpoint	43	123	139	105	369
Data Loss Prevention- Storage	39	107	128	116	392
Content Discovery (Process)	26	85	170	128	364
Email Filtering	52	164	236	197	132
Database Activity Monitoring	37	99	185	155	288
Full Drive Encryption	61	160	153	144	260
USB/Portable Media Encryption or Device Control	51	112	137	140	343
Enterprise Digital Rights Management	28	74	105	86	485
Database Encryption	46	100	166	138	325
Application Encryption	33	95	143	149	348
Web Application Firewall	46	139	197	155	242
Backup Tape Encryption	57	102	144	161	311
Entitlement Management	29	84	127	116	413
Access Management	52	171	224	163	171
Data Masking	39	87	148	126	373
Network Segregation	52	178	215	178	158
Server/Endpoint Hardening	48	180	238	178	137
Other (list in comments)	12	29	50	44	314

This time we received more write in responses for log management than user education.


Data Loss Prevention- Network
Data Loss Prevention- Endpoint
Data Loss Prevention- Storage
Content Discovery (Process)
Email Filtering
Database Activity Monitoring
Full Drive Encryption
USB/Portable Media Encryption or Device Control
Enterprise Digital Rights Management
Database Encryption
Application Encryption
Web Application Firewall
Backup Tape Encryption
Entitlement Management
Access Management
Data Masking
Network Segregation
Server/Endpoint Hardening
Other (list in comments)
0
200
400
600
800
Eliminated compliance costs
Dramatically reduced
Somewhat reduced
Did not reduce
Do not use



And finally, to better visualize the results:



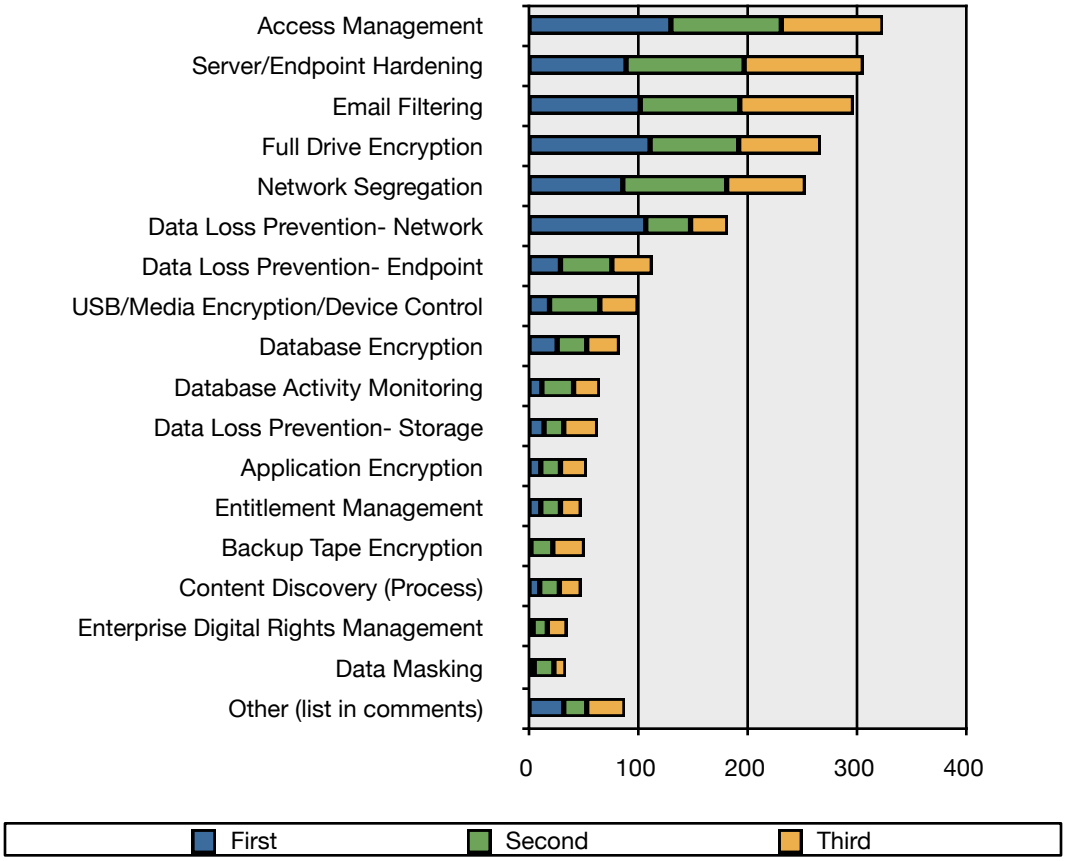
As you can see, all controls tend to rate lower in their capability to reduce compliance costs, but even the lowest ranked control was perceived to at least “somewhat reduce” compliance costs around 60% of the time. The top 5 rated controls for reducing compliance costs are network data loss prevention, endpoint data loss prevention, storage data loss prevention, full drive encryption, and USB and portable media encryption and device control. (Very closely followed by network segregation and access management).

Top three most effective controls.

We next asked participants to provide their top three most effective controls in ranked order:

Control	First	Second	Third
Data Loss Prevention- Network	108	41	34
Data Loss Prevention- Endpoint	30	47	37
Data Loss Prevention- Storage	15	18	31
Content Discovery (Process)	11	18	20
Email Filtering	103	91	104
Database Activity Monitoring	13	29	24
Full Drive Encryption	112	81	75
USB/Portable Media Encryption or Device Control	20	46	35
Enterprise Digital Rights Management	5	13	18
Database Encryption	27	27	30
Application Encryption	12	18	24
Backup Tape Encryption	3	20	29
Entitlement Management	12	18	19
Access Management	131	101	93
Data Masking	6	18	11
Network Segregation	87	95	72
Server/Endpoint Hardening	90	108	109
Other (list in comments)	33	21	35

The chart below allows us to assess the results based on the total number of votes for a particular control, and the top 3 stack ranking within the responses:



These results are interesting because the reflect more response bias than the previous questions since we didn't offer a "do not use" option for each technology. The results do appear to correlate well with the previous questions, showing that most respondents use "traditional" security controls that are in broader use, such as email filtering and server/endpoint hardening.

One major flaw in the survey is that, despite our quality assurance and editing before releasing the questions, web application firewalls were omitted from the potential response list, and rated well in the previous questions. *WAF was also the most cited write in control*, followed (again) by user education.

This was essentially a control question, and we see the results correlate well with earlier results. Access management, server/endpoint hardening, email filtering, full drive encryption, and network segregation are the top 5 rated controls. Of that collection, only full drive encryption is necessarily data specific. Among the data security specific controls, data loss prevention rates the highest and, if rated, was most likely to be the respondent's top rated control.

Least effective control

We also asked participants to select their single most least effective control. This time we've sorted responses in rank order:

Control	Percentage	Responses
Email Filtering	11.8%	94
USB/Portable Media Encryption or Device Control	11.3%	90
Database Activity Monitoring	7.0%	56
Backup Tape Encryption	7.0%	56
Content Discovery (Process)	6.8%	54
Network Segregation	6.5%	52
Other (list in comments)	6.2%	49
Enterprise Digital Rights Management	6.0%	48
Data Masking	5.5%	44
Full Drive Encryption	4.4%	35
Access Management	4.4%	35
Application Encryption	4.3%	34
Entitlement Management	4.2%	33
Server/Endpoint Hardening	3.6%	29
Data Loss Prevention- Network	3.5%	28
Database Encryption	2.8%	22
Data Loss Prevention- Storage	2.4%	19
Data Loss Prevention- Endpoint	2.1%	17

Again, we need to account for bias based on greater usage of certain controls, which may account for the positioning of email filtering.

Conclusions

Overall, most organizations appear to be relying more on "traditional" security controls such as network segregation and system hardening than controls that tend to be more specific to data security, such as data loss prevention. This shouldn't be a surprise, since traditional controls are more widely deployed, generally more mature, and are essential components of any security program. If you don't harden your servers or control who has access to information, it's nearly impossible to effectively deploy any data security specific controls.

One of the more interesting controls for showing the dichotomy between traditional and data security specific controls, and for monitoring response bias, is email filtering. It is one of the most widely deployed controls that rates well for effectiveness in the questions where we didn't force a stack ranking for controls, but drops to the middle of the pack when we asked for the top 3 controls, and also wins as the least effective control. While it's never safe to make any assumptions, it's possible this split personality is due to the nature of incidents email filtering is deployed to manage. Email filtering reduces the number of exposures due to accidental (or purposeful) emailing of information, but providing little to no protection against malicious external attacks.

We also noted clear differences in effectiveness ratings based on what problems controls were deployed to manage. In general, they rated higher for preventing incidents, followed by reducing incident severity and then by reducing

compliance costs. Despite compliance being a major driver for security, these controls are still seen mostly as cost centers that improve security, rather than as a means of reducing compliance costs.

Probably the most significant finding is that overall effectiveness, especially for incident reduction, rates well for most of the controls we asked about. Around half of respondents reported that nearly half of the controls completely or dramatically reduced incidents. Looking at it from the other direction, only one control was reported as not reducing incidents in just under 25% of organizations (backup tape encryption). It's somewhat surprising that tape encryption rated even more poorly in reducing incident severity since the loss of an encrypted tape typically doesn't require disclosure or result in the potential exposure of sensitive information. This could indicate a misunderstanding in how tape encryption works, tapes being involved in few (or no) incidents, or that organizations have limited deployments and lose unencrypted tapes.

Technology and Process Usage

How and why people implement data security controls

For the final section of our survey we asked participants to characterize the nature of their deployments- which tools are they using (some of which we asked in earlier questions), the scope of deployment, the primary driver behind the deployment, and how long the tools have been in use. We closed by asking them to tell us which tools they are considering deploying in the coming year.

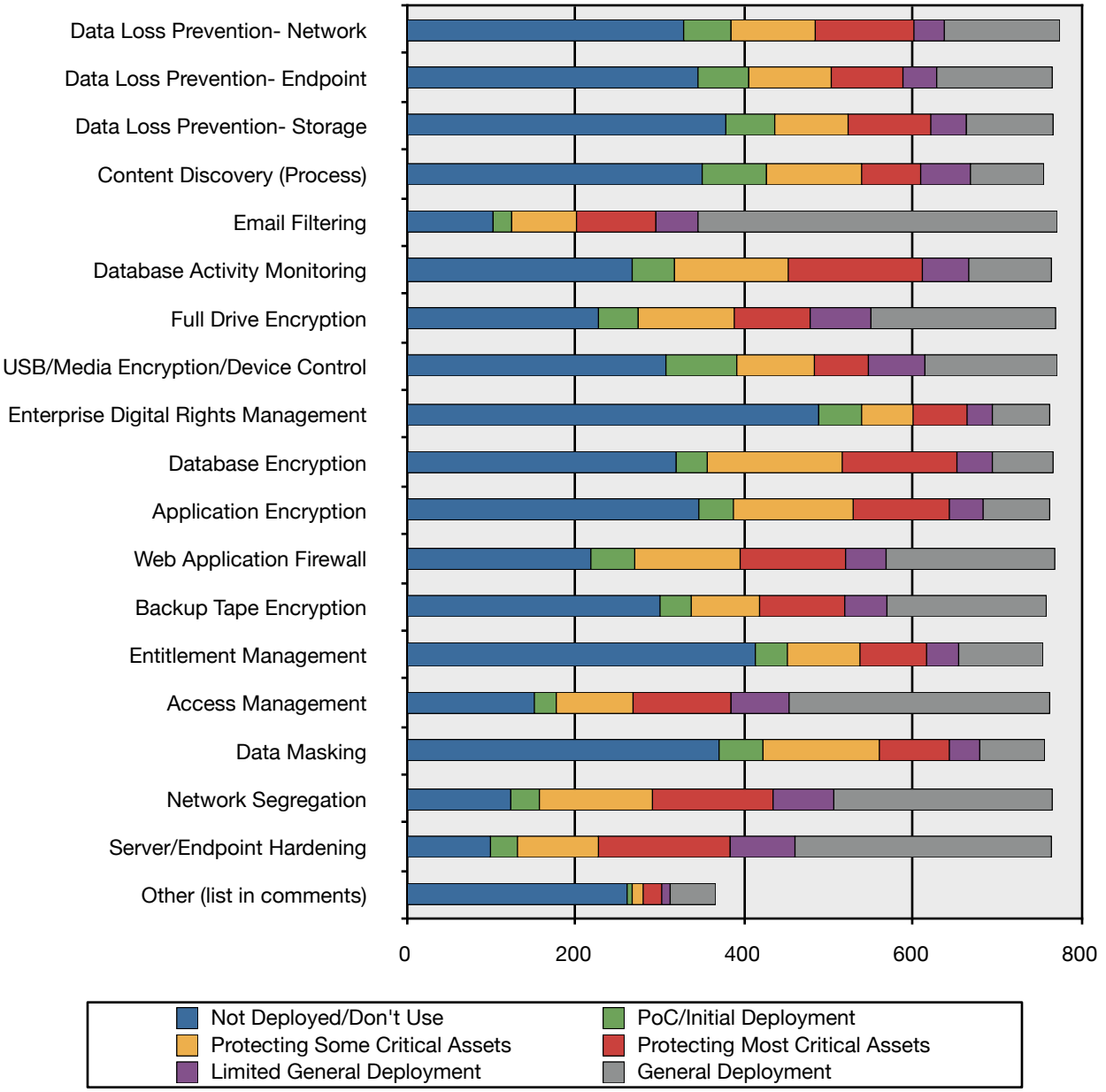
As we'll discuss through the analysis, the results are fairly interesting. Even accounting for response bias, many data security tools seem to be in wider deployment than typically believed. Compliance seems to play a smaller role in driving data security controls implementation, and one of the least rated controls is one of the most likely to be deployed in the next 12 months.

Scope of deployment

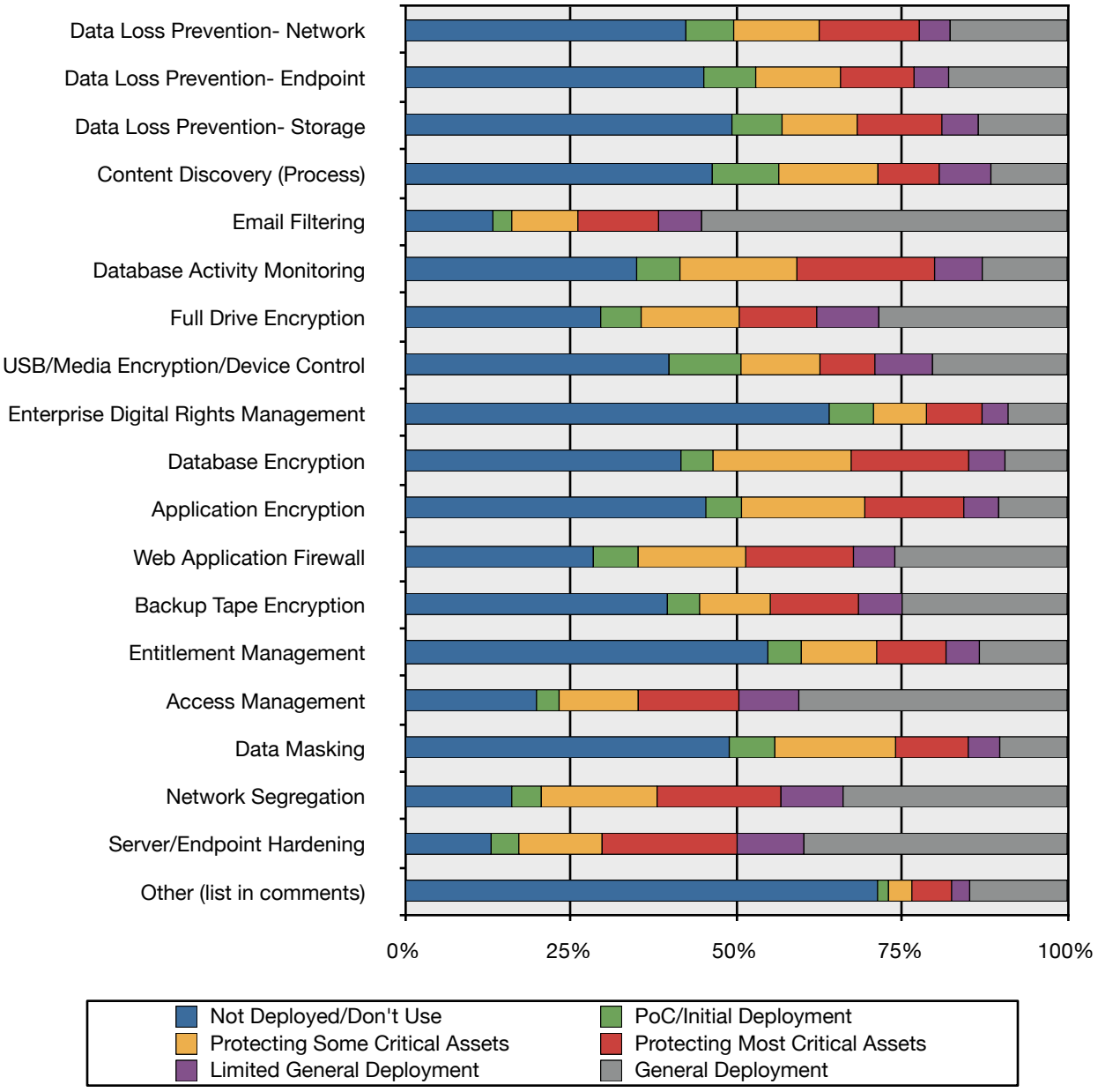
Rather than simply asking if organizations used particular controls, we thought it would be interesting to see how deeply they deployed them. We build a scale ranging from proof of concepts through general/wide deployment:

Controls	Not Deployed/ Don't Use	PoC/Initial Deploy-ment	Protecting Some Critical Assets	Protecting Most Criti-cal Assets	Limited General Deploy-ment	General Deploy-ment
Data Loss Prevention- Network	329	56	100	117	36	137
Data Loss Prevention- Endpoint	346	60	98	85	40	137
Data Loss Prevention- Storage	379	58	87	98	42	103
Content Discovery (Process)	351	76	113	70	59	87
Email Filtering	103	22	77	94	50	426
Database Activity Monitoring	268	50	135	159	55	98
Full Drive Encryption	228	47	114	90	72	219
USB/Portable Media Encryption or Device Control	308	84	92	64	67	157
Enterprise Digital Rights Manage-ment	489	51	61	64	30	68
Database Encryption	320	37	160	136	42	72
Application Encryption	347	41	142	114	40	79
Web Application Firewall	219	52	125	125	48	200
Backup Tape Encryption	301	37	81	101	50	189
Entitlement Management	414	38	86	79	38	100
Access Management	152	26	91	116	69	309
Data Masking	371	52	138	83	36	77

Controls	Not Deployed/ Don't Use	PoC/Initial Deploy-ment	Protecting Some Critical Assets	Protecting Most Criti-cal Assets	Limited General Deploy-ment	General Deploy-ment
Network Segregation	124	34	134	143	72	259
Server/Endpoint Hardening	100	32	96	156	77	304
Other (list in comments)	262	6	13	22	10	54

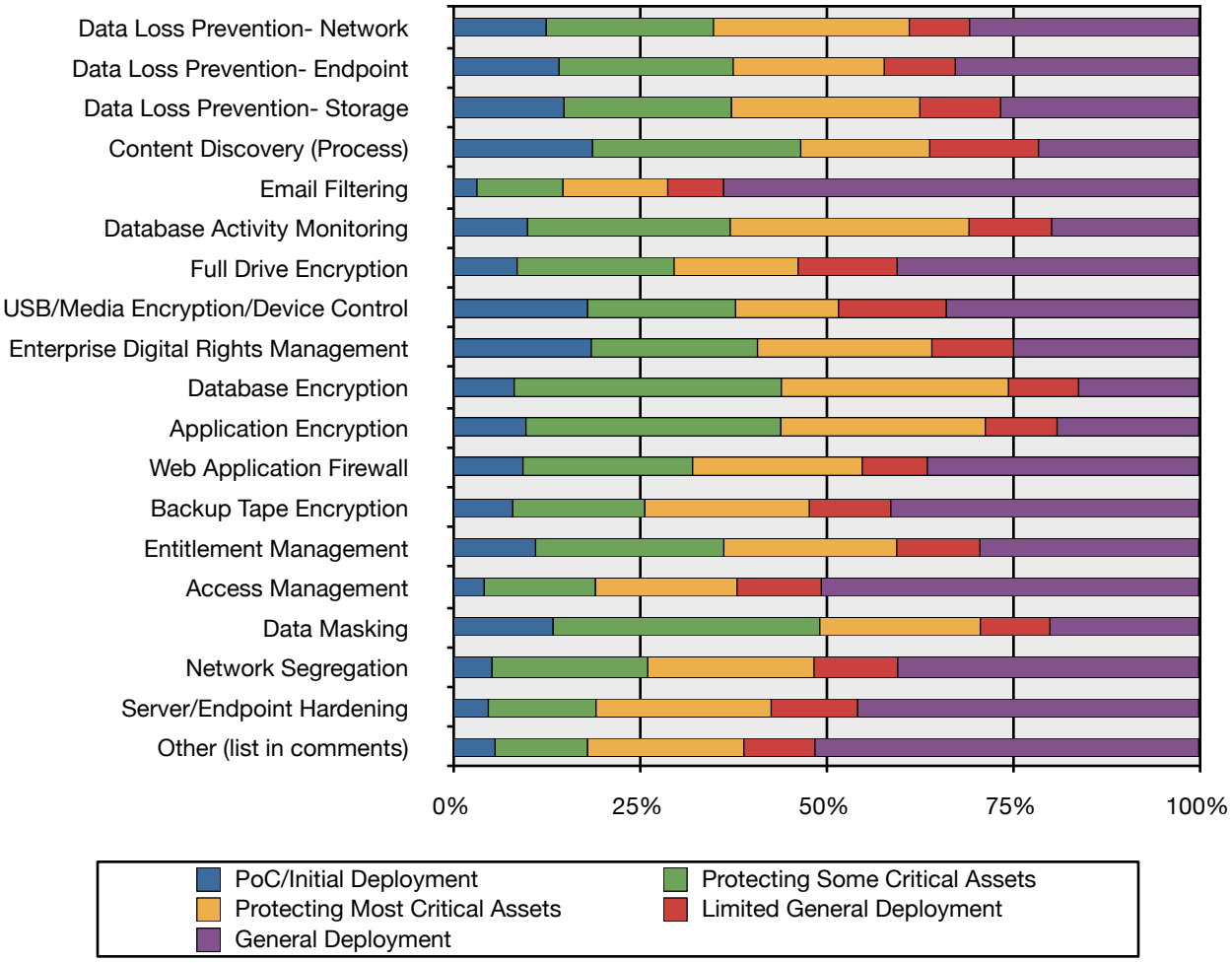


We again convert to a percentage scale.



Keep in mind that this question is organized progressively, so the most used widely controls are on the right side of the chart vs. the left, as they are organized in previous questions where “do not use” was the last option.

Here is the same data with the “do not use” option eliminated:



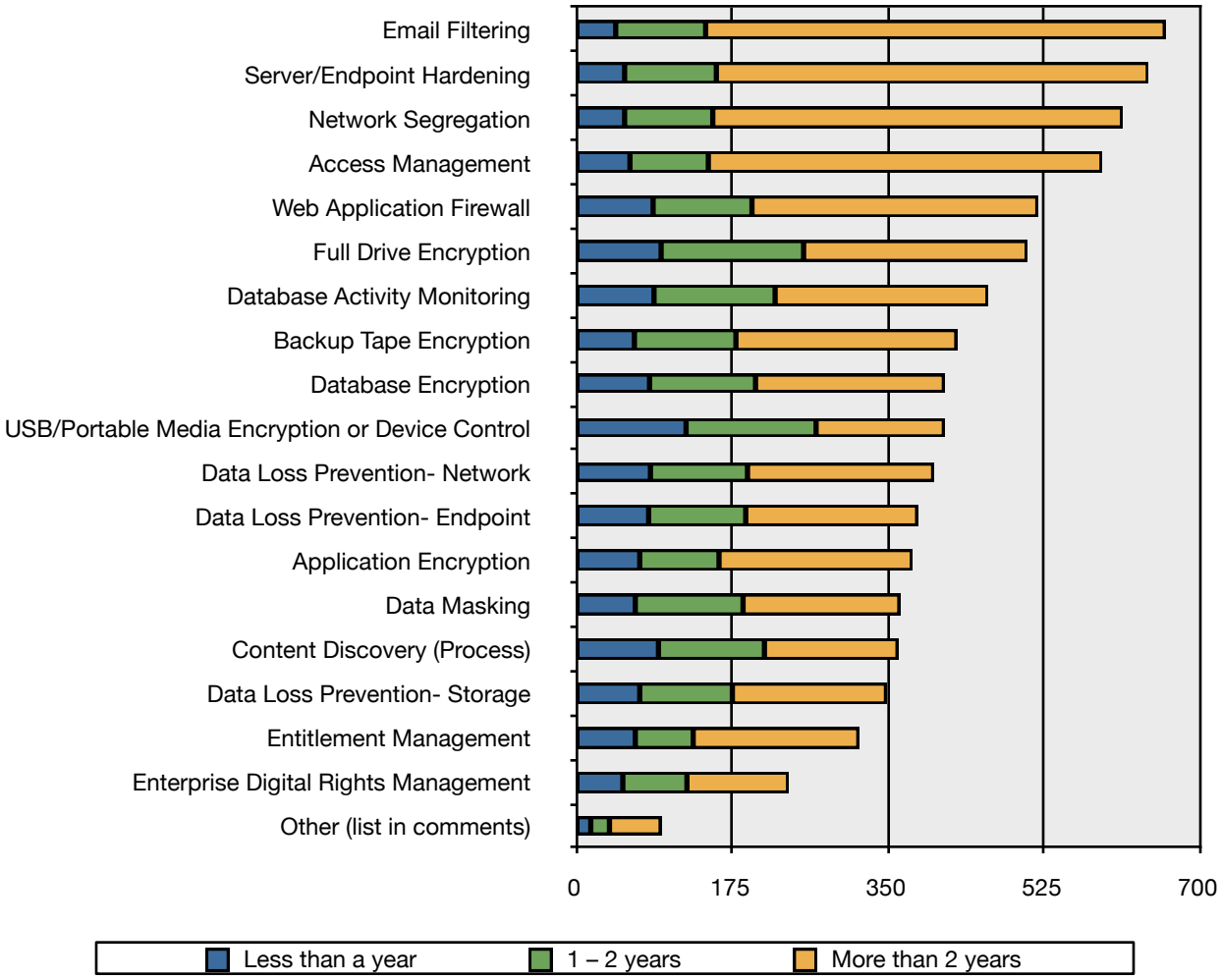
When used, every control we surveyed is, on average, protecting at least most critical assets. This is a higher maturity level than we expected when beginning the survey.

Time deployed

We next asked participants to let us know how long they've been using these controls.

Control	Less than a year	1 – 2 years	More than 2 years
Data Loss Prevention- Network	84	109	209
Data Loss Prevention- Endpoint	82	109	193
Data Loss Prevention- Storage	72	104	173
Content Discovery (Process)	93	119	150
Email Filtering	45	101	516
Database Activity Monitoring	88	136	239
Full Drive Encryption	96	160	251
USB/Portable Media Encryption or Device Control	124	146	144
Enterprise Digital Rights Management	53	72	114
Database Encryption	83	119	212
Application Encryption	72	89	217
Web Application Firewall	87	111	321
Backup Tape Encryption	66	114	248
Entitlement Management	67	65	186
Access Management	61	88	442
Data Masking	67	121	176
Network Segregation	55	99	460
Server/Endpoint Hardening	55	103	485
Other (list in comments)	17	21	58

Aside from USB/portable media encryption and device control, most organizations have been using these tools and processes for more than two years. For our chart we've ordered it based on length of deployment:



Overall, as with the scope of deployment, this shows greater usage than we expected.

Primary driver

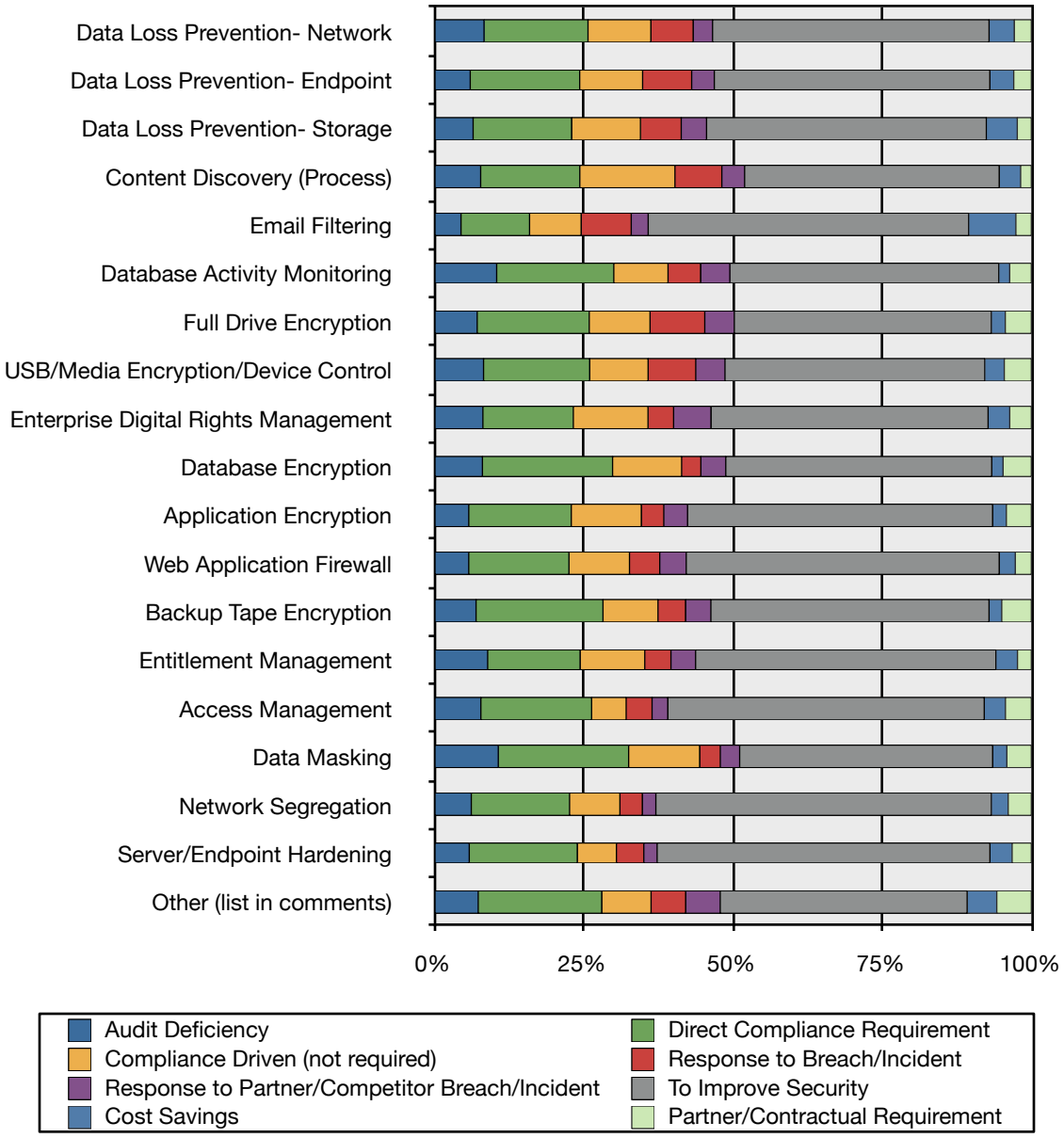
We frequently site compliance or fear of data breaches as the main reason to deploy data security controls, but when we asked participants the results were somewhat surprising:

We asked if the primary driver for deployments was:

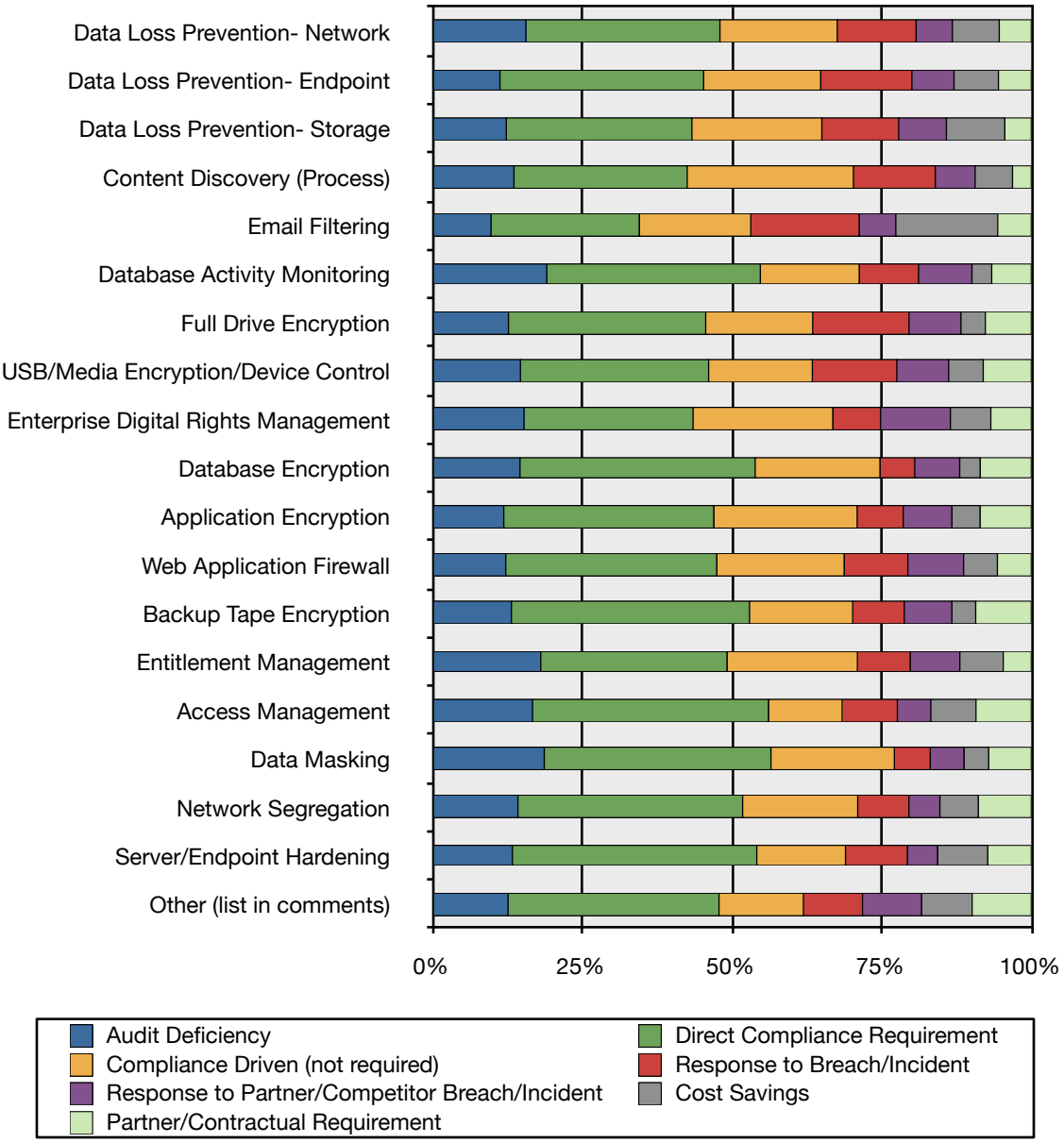
- Audit Deficiency
- Direct Compliance Requirement
- Compliance Driven (not required)
- Response to Breach/Incident
- Response to Partner/Competitor Breach/Incident
- To Improve Security
- Cost Savings
- Partner/Contractual Requirement
- N/A

We've removed N/A responses since that option is well covered by other questions:

Control	Audit Deficiency	Direct Compliance Requirement	Compliance Driven (not required)	Response to Breach/Incident	Response to Partner/Competitor Breach/Incident	To Improve Security	Cost Savings	Partner/Contractual Requirement
Data Loss Prevention- Network	44	91	55	37	17	242	22	15
Data Loss Prevention- Endpoint	29	87	50	39	18	219	19	14
Data Loss Prevention- Storage	28	70	49	29	18	199	22	10
Content Discovery (Process)	35	74	71	35	17	190	16	8
Email Filtering	37	93	70	68	23	435	64	21
Database Activity Monitoring	58	108	50	30	27	248	10	20
Full Drive Encryption	50	129	70	63	34	296	16	30
USB/Portable Media Encryption or Device Control	46	98	54	44	27	240	18	25
Enterprise Digital Rights Management	25	46	38	13	19	141	11	11
Database Encryption	43	115	61	17	22	235	10	25
Application Encryption	28	82	56	18	19	244	11	20
Web Application Firewall	37	106	64	32	28	331	17	17
Backup Tape Encryption	40	120	52	26	24	263	12	28
Entitlement Management	35	60	42	17	16	195	14	9
Access Management	60	141	44	33	20	403	27	33
Data Masking	50	101	55	16	15	196	11	19
Network Segregation	47	123	63	28	17	420	21	29
Server/Endpoint Hardening	48	146	53	37	18	450	30	26
Other (list in comments)	9	25	10	7	7	50	6	7



"To improve security" was the top rated driver, but since this was a multi-select question it was often chosen in conjunction with other answers. If we remove that option, we find compliance requirements dominate the results:

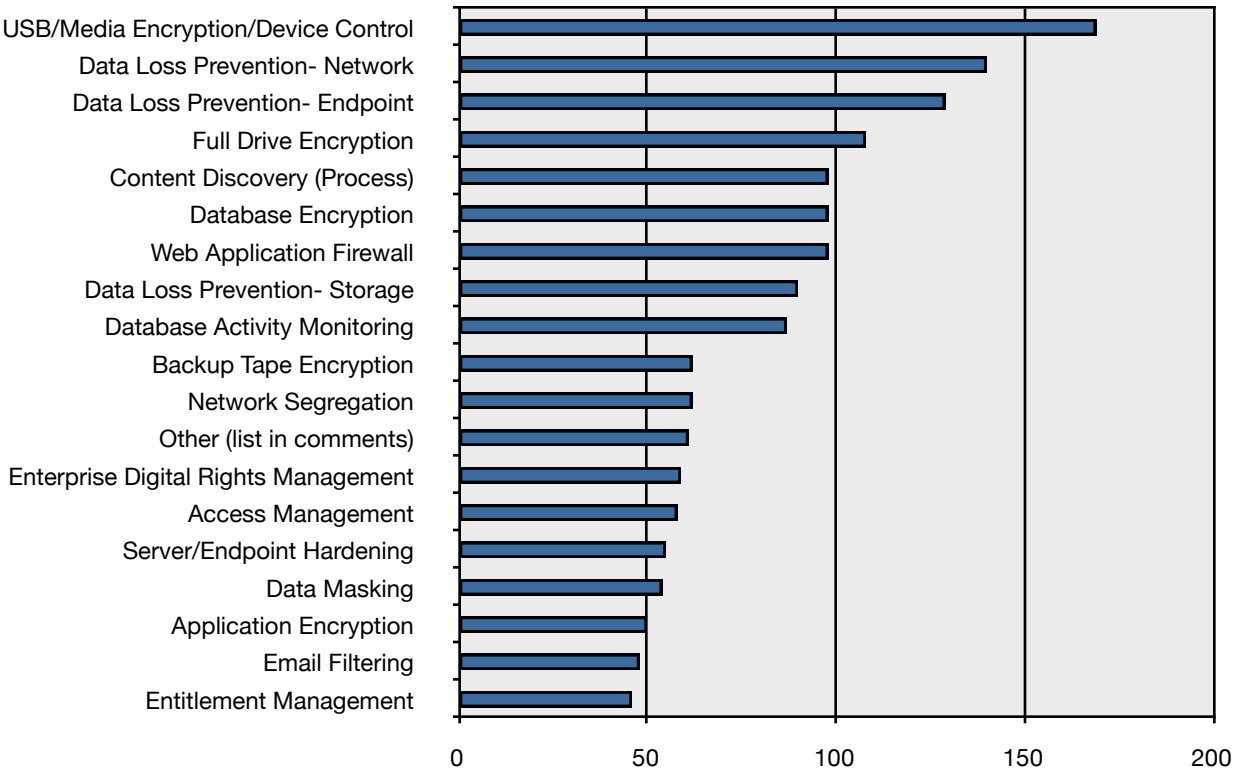


Thus while general security drives most data security projects, specific compliance deficiencies or requirements still play an extremely large role. These responses also correlate well with our understanding of various compliance regulations. For example, database activity monitoring is often used for SOX compliance, database encryption is mandated by PCI, and data masking is required for certain financial regulations (on top of PCI).

What will you deploy next?

For our final question we asked participants to tell us which security controls they were considering deploying over the next 12 months:

	Responses
USB/Portable Media Encryption or Device Control	169
Data Loss Prevention- Network	140
Data Loss Prevention- Endpoint	129
Full Drive Encryption	108
Content Discovery (Process)	98
Database Encryption	98
Web Application Firewall	98
Data Loss Prevention- Storage	90
Database Activity Monitoring	87
Backup Tape Encryption	62
Network Segregation	62
Other (list in comments)	61
Enterprise Digital Rights Management	59
Access Management	58
Server/Endpoint Hardening	55
Data Masking	54
Application Encryption	50
Email Filtering	48
Entitlement Management	46



Data loss prevention clearly rates highly, but it's interesting that one of the least-well-rated controls in terms of effectiveness, portable media encryption and device control, is the most likely to be deployed in the coming 12 months.

Conclusions

Overall it appears that data security tools and techniques are increasing in maturity and are no longer limited to the early adopter phase. It's our assessment, based on these results, that data security controls are fully in the early mainstream of the market.

With a few exceptions, most notable enterprise digital rights management, most controls are being used to at least some degree by 40-50% of the survey participants. Even if we drop this number in half to account for response bias, it still means fully a quarter of organizations are deploying multiple data security controls.

Who We Are

About the Author

Rich Mogull, Analyst and CEO

Rich has twenty years experience in information security, physical security, and risk management. He specializes in data security, application security, emerging security technologies, and security management. Prior to founding Securosis, Rich was a Research Vice President at Gartner on the security team where he also served as research co-chair for the Gartner Security Summit. Prior to his seven years at Gartner, Rich worked as an independent consultant, web application developer, software development manager at the University of Colorado, and systems and network administrator. Rich is the Security Editor of TidBITS, a monthly columnist for Dark Reading, and a frequent contributor to publications ranging from Information Security Magazine to Macworld. He is a frequent industry speaker at events including the RSA Security Conference and DefCon, and has spoken on every continent except Antarctica (where he's happy to speak for free -- assuming travel is covered).

About Securosis

Securosis, L.L.C. is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services.

We provide services in four main areas:

- Publishing and speaking: Including independent objective white papers, webcasts, and in-person presentations.
- Strategic consulting for end users: Including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessments.
- Strategic consulting for vendors: Including market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessments.
- Investor consulting: Technical due diligence including product and market evaluations, available in conjunction with deep product assessments with our research partners.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Securosis has partnered with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis.