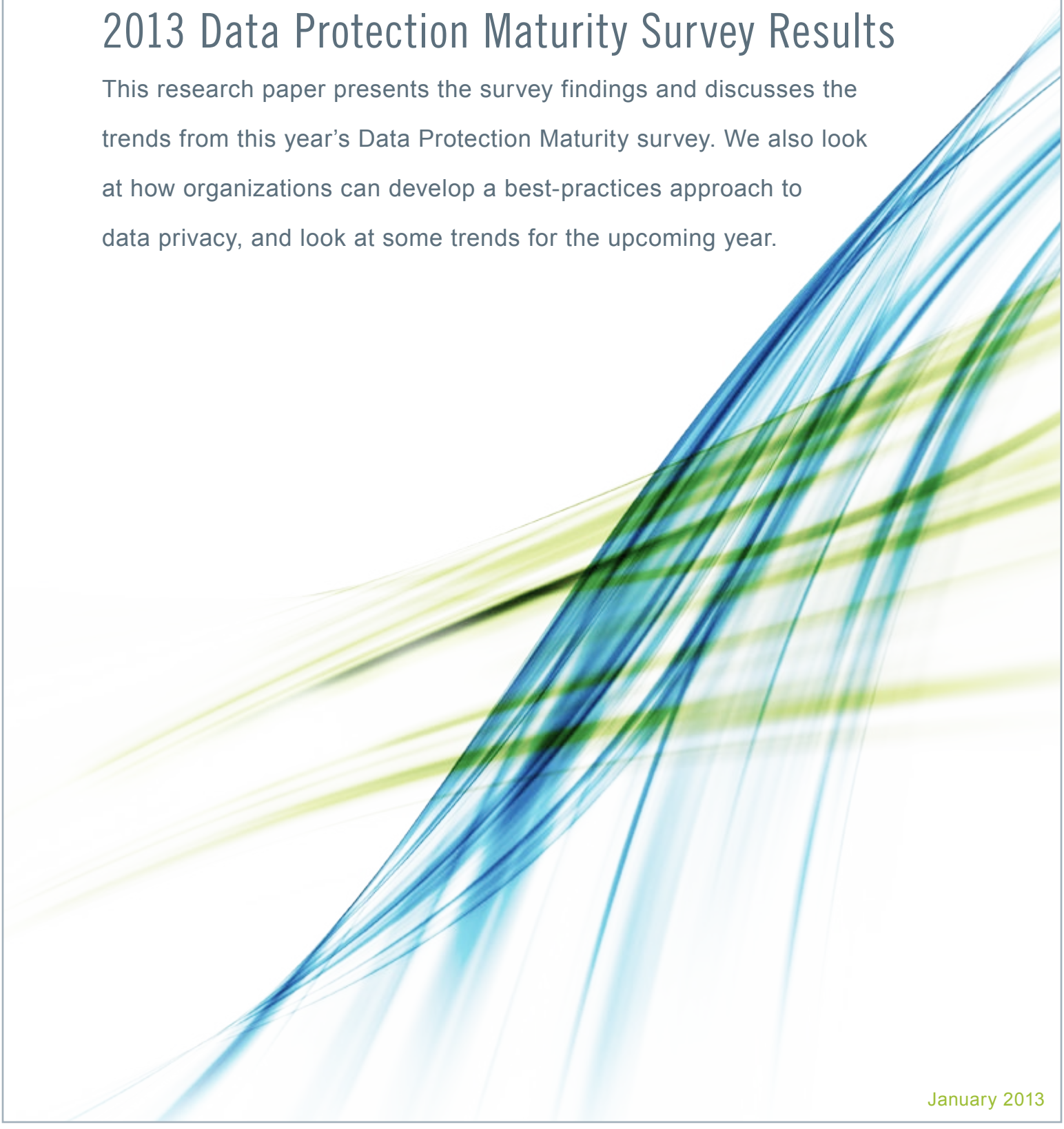
2013 Data Protection Maturity Survey Results

This research paper presents the survey findings and discusses the trends from this year's Data Protection Maturity survey. We also look at how organizations can develop a best-practices approach to data privacy, and look at some trends for the upcoming year.



January 2013

WP-EN-01-21-13

Overview

The job of protecting sensitive information has become more difficult in the last couple years. One factor is the booming use of mobile devices, which is putting considerable pressure on traditional network perimeter defenses. This growth also means that priceless corporate data is now as likely to be outside of the corporate firewall as within its protective reach. In addition, the adversaries intent in gaining illicit access to confidential data are growing in number and sophistication. In order to counter these trends, organizations need to develop and maintain appropriate data protection best practices that keep them compliant and secure.

> In the 2013 results, we saw 6% of respondent organizations categorized as having Optimal data protection maturity, with 26% classified as Operational, 41% labeled Standardizing, and 27% in the Ad Hoc group.

In late-2012, Lumension conducted the 2nd annual worldwide survey of organizational attitudes, policies and programs designed to protect sensitive information – be it so-called "toxic" customer data (PII) or valuable organizational intellectual property (IP). Approximately 300 respondents from around the globe representing organizations from very small to 5000+ employees completed the survey, which examined the challenges faced by organizations trying to protect data under their care today. We not only asked about the threats they are facing and how they are going about defending against them, but also about compliance with statutory and industry regulations related to data privacy.

This research paper presents the survey findings, and discusses the trends from this year's Data Protection Maturity Survey. We will conclude by looking at how organizations can develop a best-practices approach to data protection, and looking at some trends for the upcoming year.

Changing IT Network Landscape

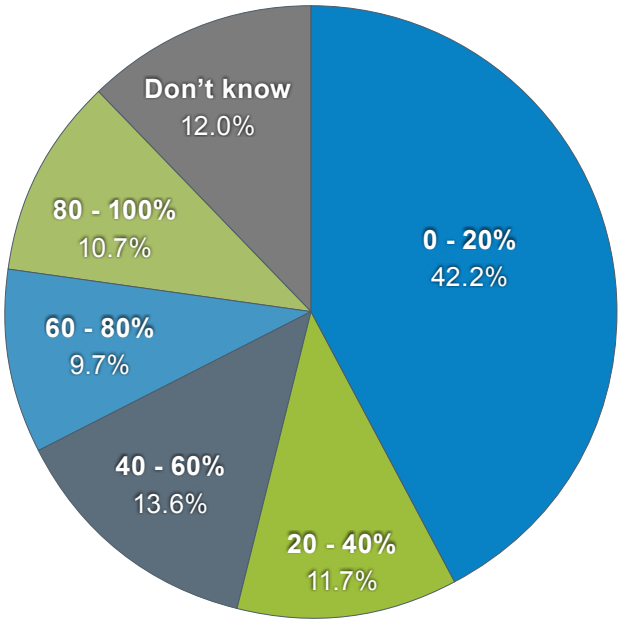
One cannot be in the IT security arena without having heard – or been impacted by – the "Bring Your Own Device" (BYOD) or consumerization trends. In fact, as Gartner states, [u]ser's increasing attraction to unsupported electronic tools will push IT organizations to offer new types of support.[1] But the extent to which it has been embraced – and secured – varies greatly per our respondents.

Last year we saw an even split between those who estimated the use of personally-owned devices in the organization at 0 – 20% (46%) and those who put it at 20 – 100% (45%). This year, we see the gap reversing and widening somewhat, with more organizations in the 20 – 100% (46%) than in the 0 – 20% range (42%). In both years we saw roughly 1 in 10 respondents admitting that they did not know how many personally-owned devices were accessing organizational assets via the network, which might be indicative of the risks associated with the lack of comprehensive device visibility.

1. Gartner, Media Tablets and Beyond: The Impact of Mobile Devices on Enterprise Management (Jan-2012)

About 30% of organizations are reported to have minimal or no security policies which address data protection concerns.

What portion of your organization's regularly used USB and mobile devices are personally owned? Please consider flash drives, smartphones, tablets, etc.



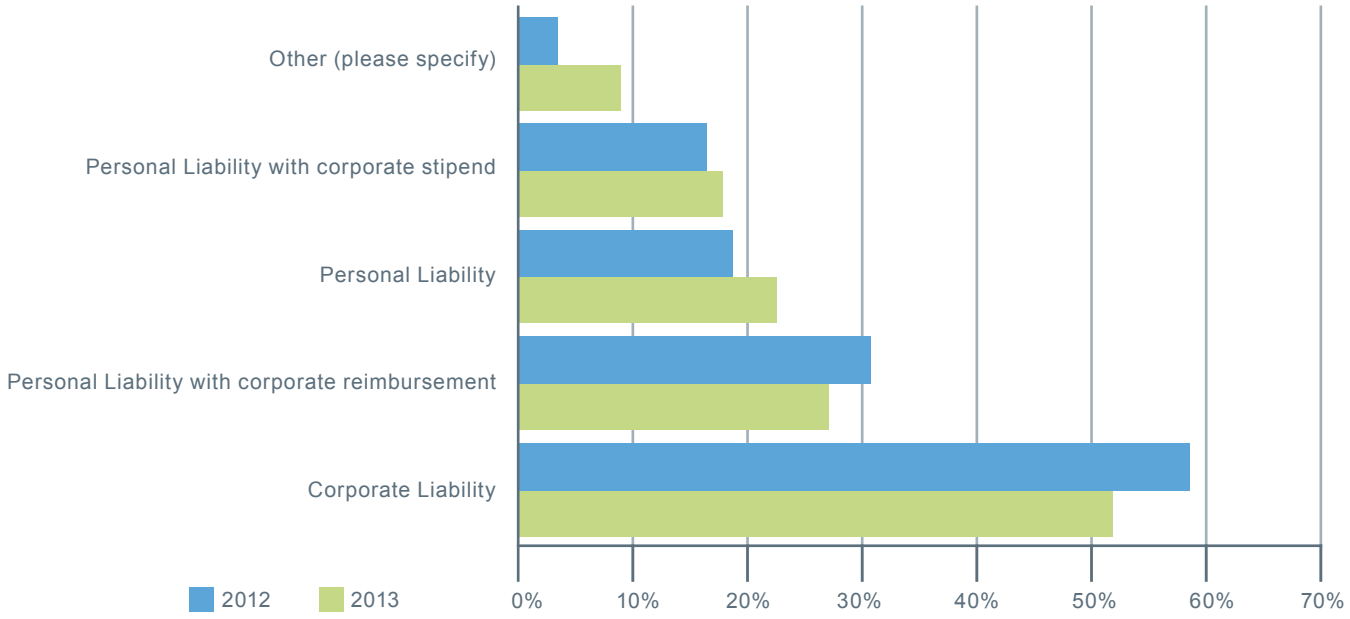
We continued by looking into how employee-owned mobile devices were administratively, legally or technically controlled within the organization. Once again we see a majority of organizations (51%) either currently blocking device access (31%) or using some sort of isolation controls (20%). It is interesting to note that only "access with education" increased – by a little over 6% – from last year's survey. While none of the other categories dropped significantly, in the aggregate we see a slight loosening of access policies. In fact, this combined with the increased use of personally-owned devices to access organizational data and other resources, suggest that organizations need to pay close attention to the changing IT network environment.

Which of the following best describes your firm's policy for network access for personal devices such as smart phones and tablets?

Open access is provided.	8.1%
We accept that personal devices will access corporate data and resources but we try to educate users on the importance of security.	19.5%
A limited number of higher level employees are allowed to use their personal devices to access our corporate network.	19.2%
Access for all devices is provided through a DMZ or other isolated access controls (e.g. email or web only).	20.1%
We do not currently allow them to access the network but may in the future.	14.9%
We do not currently allow them to access the network and there are no plans to provide future access.	15.9%
Don't know.	2.3%

And our respondents confirmed this when asked: "How are personal mobile devices, such as phones and tablets, financially and administratively managed within your organization?" In 2012, 59% of respondents indicated these devices were classified as "Corporate Liability" – that is, they are an extension of the corporate network, with a personal-use policy which is strictly defined. However, in 2013 this dropped to 52%, with the biggest

How are personal mobile devices, such as phones and tablets, financially and administratively managed whithin your organization?



increase seen in the "Personal Liability" – without reimbursement or stipend. This gives a good indication of just how far organizations have come in embracing the BYOD movement. However, again highlighting the need for organizations to pay closer attention to the changing IT environment, there is a dark side to this "Personal Liability" device statistic – it suggests that there is minimal or no access policy, which puts data privacy initiatives at risk.

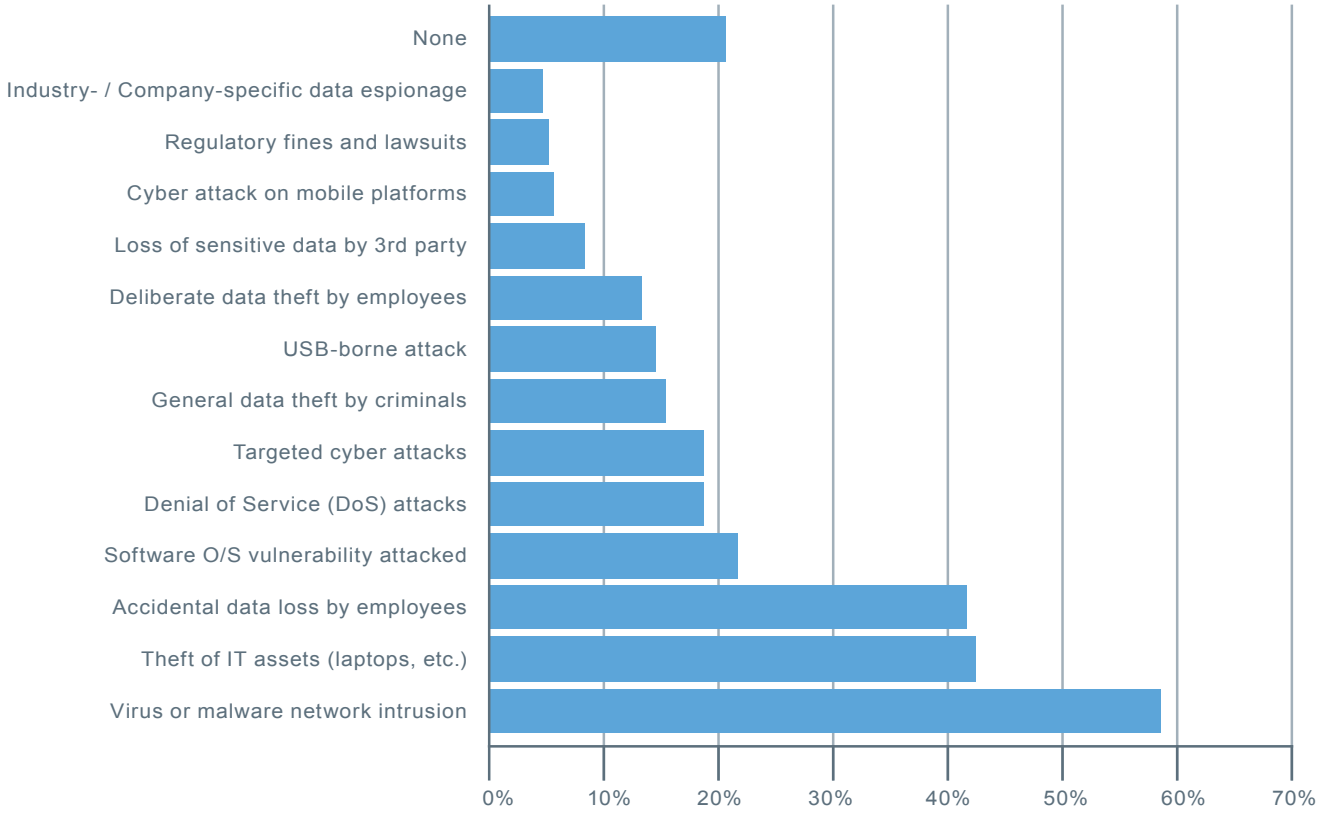
In order to better understand the data protection guidelines within organizations today, we asked about the restrictions included in employee agreements. An overwhelming majority of the respondents indicated that corporate confidentiality (81%) clauses were included, followed by customer confidentiality rules (63%) and mobile device policies (59%). Interestingly, the customer confidentiality rules response dropped almost 9% from 2012, while none of the other responses changed appreciatively. In fact, much like last year, just under 50% of organizations have set out an explicit statement of what rights the company retains to data on personal devices. Taken as a whole, this suggests that employment agreements may not have kept pace with the changes in the IT environment – potentially putting confidential or sensitive data at risk.

> The average reported security spend ratio (relative to overall IT budget) dropped from 6.1% in 2011 to 5.6% in 2012.

Increasing Threats Landscape

Respondents were asked whether they had experienced any data security issues during the previous year – by far the greatest issues were network intrusion by a virus or malware (58%), theft of IT assets such as laptops (43%) and the accidental loss of data by employees (42%). These were the top-3 in 2012 as well.

Have you experienced any of the following incidents in the past year?



It is interesting to note that the "none" category dropped by almost 5% from 2012. However, the largest changes from 2012 were seen in following categories:

- Virus or malware network intrusion...10% increase
- Targeted cyber attacks...7.5% increase
- Theft of IT assets (laptops, etc.)...6% increase

But in fact almost every category increased in some amount, with only "cyber attack on mobile platforms" decreasing a bit. As such, these results mirror data presented in countless other reports which demonstrate the multitude of threat vectors and the increasing magnitude and sophistication of attacks. This has led to an increasing feeling of endpoint insecurity among IT professionals year on year, which has risen from 59 percent to 67 percent since 2009.[2]

> The overwhelming perception that no data protection regulations pertain suggests a fundamental disconnect between the regulatory landscape and our respondents understanding of it.

2. Ponemon Institute, 2013 State of the Endpoint (Dec-2012)

Evolving Organizational Landscape

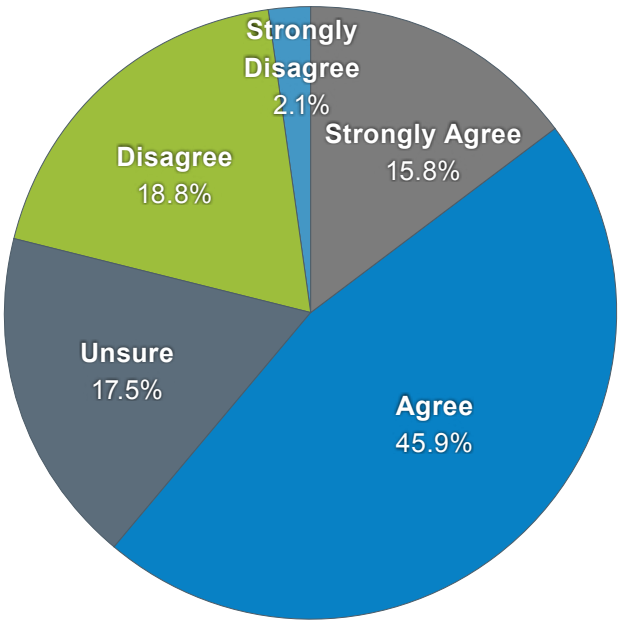
At the heart of it, most cyberattacks against an organization are designed to obtain valuable information, regardless of the type of attack – be it "standard" malware, phishing expeditions or even so-called Advanced Persistent Threat (APT) attacks – or the motivations of the attacker, be they cybercriminals bent on monetary gains, competitors seeking an edge, hacktivists sending a message, or even nation-states or their proxies. And we're seeing plenty of attacks, plenty of data breaches, and plenty of costs associated with these breaches:

- According to the Ponemon Institute, 58% of organizations have more than 25 malware incidents each month, and another 20% are unsure how many incidents they're dealing with.[3]
- The data breaches reported in 2012 increased almost 35% over 2011, according to datalossdb.org.[4]
- The average cost of a data breach was about $194 per record in 2011; of this, about 70% were indirect costs such as lost business, customer churn, etc.[5]
- About 70 – 80% of an organization's market value is based on intangible assets such as IP.[6]

Protecting against data breaches requires a commitment from management and of resources. Almost 62% of our respondents indicate that they have sufficient resources to achieve compliance with data security policies and best practices, while only about 21% indicated they did not. This is roughly unchanged from the results we saw in 2012. On the other side, about 77% of our respondents proclaim that data security is a strategic initiative across the enterprise, while only about 12% suggest it is not. This too is basically unchanged from the results we saw in 2012. Interestingly, we see weak correlation between the responses to these two questions, which might indicate that just because data security is a strategic initiative does not mean that our respondents see it being adequately funded. Equally interesting was the drop in average reported security spend ratio (relative to overall IT budget) from 6.1% to 5.6% – not a large decrease, but it does shed a certain light on what our respondents considered sufficient resources.

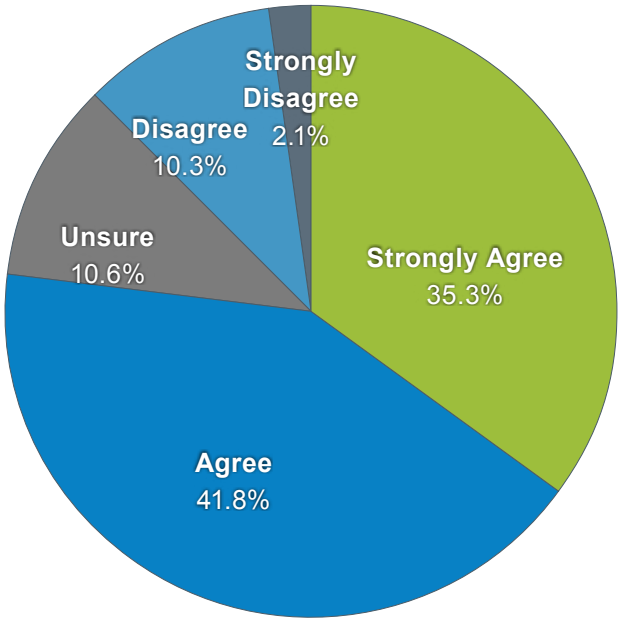
How much do you agree with this statement?

"My organization has sufficient resources to achieve compliance with data security policies and best practices."



3. Ponemon Institute, 2013 State of the Endpoint (Dec-2012)
4. Based on data retrieved 11-Jan-2013.
5. Ponemon Institute, 2011 Cost of Data Breach Study (Mar-2012)
6. Ocean Tomo, http://www.oceantomo.com/about/intellectualcapitalequity

"Data security is a strategic initiative across the enterprise."



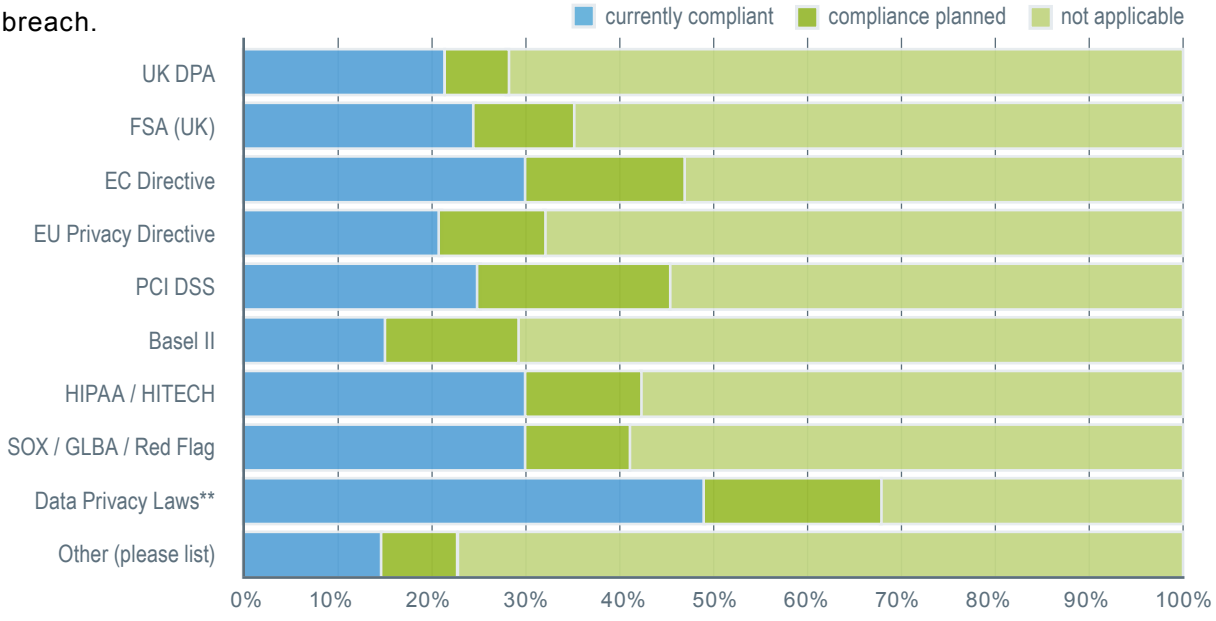
But overall, these results bode well for the maturity of organizational data privacy efforts. In general it seems that those setting and funding organizational strategy with respect to these efforts understand the need for commitment in order to avoid the top- and bottom-line impacts that arise from a data breach.

Uncertain Regulatory Landscape

The survey looked into compliance with relevant legal and industry regulations concerning data protection. Data privacy and data breach notification rules have been on the books for some time now, and the regulatory environment is ever-changing as government and industry grapple with these issues.

Indeed, it seems our respondents are uncertain or unaware about what statutory and industry regulations apply to their organizations. On average, just over 25% of respondents claimed to be compliant to any of the regulations, with planned compliance at just about half that. This means that on average roughly 60% of respondents did not think any of these regulations were applicable.

Is your organization compliant with the following regulations, or do you plan to be compliant within the next 24 months?



**Includes State / National data privacy, data protection and/or data breach notification laws.

Digging deeper, we find that just over 25% of respondents state their organization are not compliant with any data protection regulations, while about half of those folks suggest none of them are actually applicable. However, as we noted in last year's study, almost all jurisdictions have some sort of data privacy law that applies, not only to confidential customer data but employee data as well – so these results are hard to understand.

True, the regulatory landscape is changing rapidly. In 2012 we saw numerous new statutory regulations coming on line (e.g., the "final rule" for HITECH or the PDPA in Malaysia) or being pushed through the legislative process (e.g., the work in the EU on the GDPR), as well as changes to many industry regulations (such as the recently updated PCI DSS). That said, most jurisdictions around the world have some sort of data protection law which applies not only to customer data but also employee personal information. In addition, we're starting to see governments becoming concerned about cyberespionage, at least when it comes to so-called critical infrastructure; for instance, the recently signed US National Defense Authorization Act gives the DOD 90 days to establish procedures for defense contractors to disclose cyber breaches.

> The biggest threat issues seen in 2012 were: network intrusion by a virus or malware (58%), theft of IT assets such as laptops (43%) and the accidental loss of data by employees (42%).

That notwithstanding, the overwhelming perception that none of the data privacy regulations pertain (both individually and in aggregate) suggests a fundamental disconnect between the regulatory landscape and our respondents understanding of it. Organizations hoping to meet their data protection obligations need to understand all the regulations which apply.

Rising to the Challenge

So, we see how respondents perceive the rising threat environment, the evolving organizational environment and the uncertain regulatory environment. But how are they coming to terms with the data privacy challenges in light of all this? To find out, we asked the survey respondents how they were *creating* organization-wide data protection policies, *educating* employees about these policies, and *enforcing* them via technical means.

Creating Data Protection Policies

We asked about the policies currently being used in their organizations. Only 23% of respondents indicated that their organizations adhere to a best-practice approach of formally developing extensive security policies in which procedures, guidelines and technology standards are actively utilized. Almost twice as many (46%) indicated that they have multiple security policies covering a majority of data privacy concerns. Perhaps more worrying are the 22% and 8% of organizations which have minimal or no security policies which address data protection concerns.

What type of IT data protection policies exist?

None.	7.8%
A minimal high-level security policy which address less than 25% of data protection concerns.	21.8%
A minimal high-level security policy which address less than 25% of data protection concerns.	45.8%
Exhaustive, extensive, formally developed security policies, procedures, guidelines and technology standards are actively utilized.	23.4%
Other.	1.3%

While these numbers are essentially unchanged from 2012, we did see a slight increase in both the middling and none responses, while the sharpest (yet still minor) drop was seen in the minimal response. None of this is terribly encouraging, especially in light of the increasing complexity in organizational IT environments and increasingly sophisticated threat environment – both, to some extent, driven by the BYOD trend.

> Roughly 1 in 10 respondents admit that they did not know how many personally-owned devices were accessing organizational assets.

Educating Employees

Next we wanted to know the level of data protection training employees get, which directly impacts their understanding of the importance of those policies. Here we see nearly half (49%) of respondents said that their organizations have formal, ongoing training covering IT security best practices. Although this is good news, it means that the other half have either informal or *ad hoc* training (24%), one-time training (16%) or no training at all (8%).

What type of data protection training is offered at your organization?

Formal, ongoing training covering IT security best practices.	48.8%
Informal or ad hoc: reactive, typically event-driven notices sent to employees.	24.4%
One-time training, typically when the employee first joins the company.	16.2%
None.	8.2%
Other (please specify)	2.4%

Here again we see that these numbers are in essence unchanged from 2012, with the exception of the formal category which jumped 7.5% — good news indeed. The biggest decreases (albeit only about 4%) were seen in the informal and none categories. All this is encouraging because, as noted last year, having a detailed data privacy policy is worth little if employees are unaware of it – or the implications of violating that policy.

Continued »

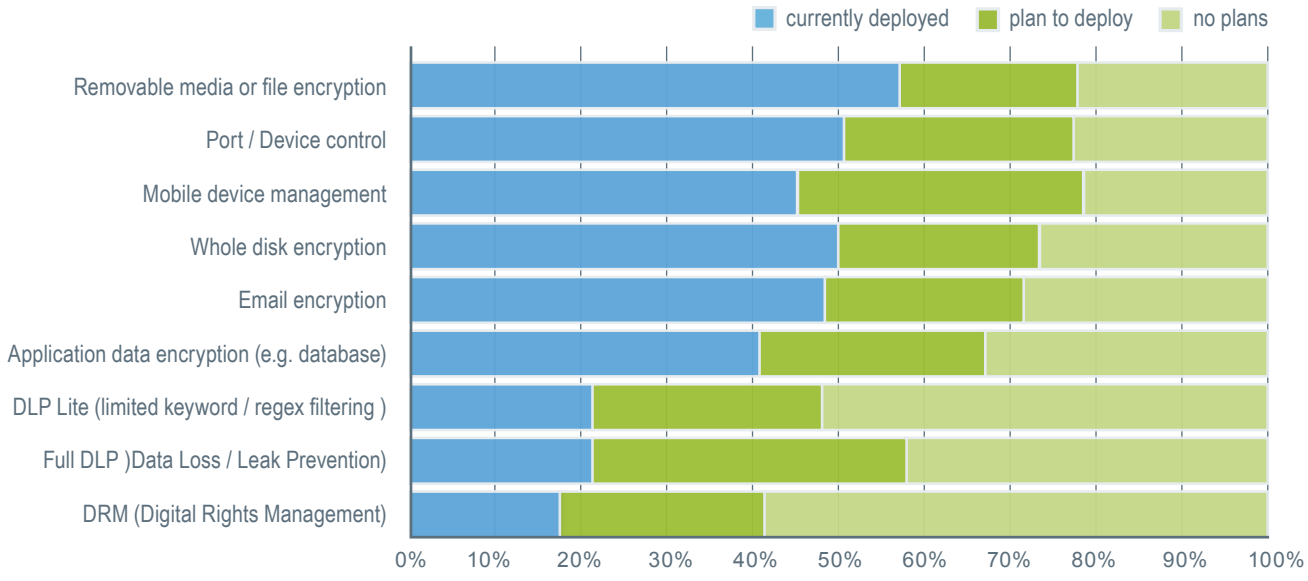
Enforcing Data Protection Policies

As IT security professionals know, having a strong data protection policy and an educated workforce are two important legs of a good data security strategy. The third is having the technical means to enforce those policies – after all, policies are worthless if they are more theory than practice and if security best practice transgressions are not halted before they cause any damage.

Therefore we asked what data security technologies are being used in organizations today. Much like last year, the three most commonly – and relatively well understood – deployed technologies were removable media or file encryption (56%), port / device control (51%) and whole disk encryption (50%). On the other side, the three least commonly deployed technologies were Data Rights Management (DRM, at 17%), Data Loss Prevention (DLP) "lite" (22%), and full DLP (22%). In both cases these results are basically unchanged from last year; the only area we saw a significant increase was in the email encryption category, which climbed about 5%.

Looking forward, we learned that full DLP (36%), Mobile Device Management (MDM, at 33%) and DLP "lite" and port / device control (26% each) are the top technology plans for the next two years. This matches with what we learned last year, with the exception of full DLP – implementation plans for full DLP jumped about 16%, which was by far the biggest change we saw year-over-year. On the other side of that coin, both full DLP (43%) and DLP "lite" (52%) were also noted as technologies for which there are no plans, along with DRM (59%) – exactly as seen in 2012, although the percentage of respondents mentioning full DLP dropped by 14%.

Which of the following technologies does your organization currently use, or plan to deploy within the next 24 months?



A piecemeal approach to data protection can be worse than none at all as it offers a false sense of security that data is safe. Poorly configured endpoints represent a major source of vulnerabilities and IT teams will want to ensure that all removable devices that are plugged in are visible and controlled, that all data is automatically encrypted and that data privacy policies are enforced at a user level.

A View of US Corporate Data Protection Maturity

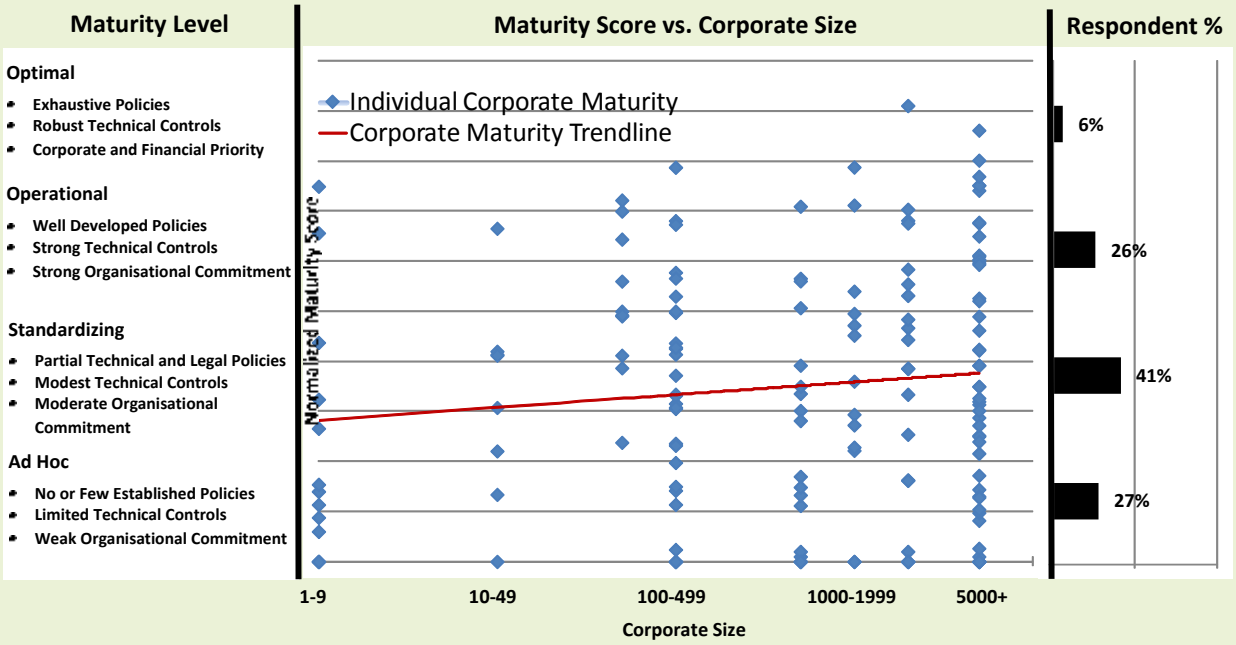
Formal maturity models, such as *Common Capability Maturity® Model Integration* (CMMI) from Carnegie-Mellon University and the UK's Office of Government and Commerce (OGC) *Portfolio, Programme and Project Management Maturity Model* (P3M3®) have been developed over time to assess organizational and process maturity.

Lumension developed a simplified Data Protection Maturity Model to analyze the survey data. Within the model, the survey questions were classified into one of three broad categories: Technical Controls, Administrative Controls or Organizational Motivation. Effective in-place Technical Controls were the highest weighted category as these controls best represent pragmatic data protection action beyond what might simply be unrealized corporate intention. The Model also incorporates some regional dependence accounting for the compliance regulations which vary across the globe. Based on complete survey responses, each individual response was given a weighted score to create a composite Maturity Score. The Maturity Scores are represented by the individual diamond-shaped points in the graphic below. This Maturity Score classifies the respondent organization's maturity level.

Continued »

In 2012, we highlighted results for the UK Data Protection Model. This year, the results for North American respondents are shown. Respondent organizations were categorized into one of four maturity bins: Optimal (6%), Operational (26%), Standardizing (41%) or Ad Hoc (27%).

Data Protection Maturity - North American Respondents



Direct comparison are of course difficult, but there is a striking homogeneity in data protection maturity across organizations of all sizes within the US in this year's survey when compared to the much steeper rise from Ad Hoc for the smallest UK organizations to Operational for the largest UK organizations based on the 2012 survey.

To view the full survey results or learn about technologies to improve your organization's data protection program, please visit www.lumension.com/data-protection-maturity.

Continued »

Conclusion

As the old bromide goes, the only thing that is constant is change. IT departments are in the midst of some significant changes, driven by both organizational and end user needs. Increasing use of personal devices to access organizational data and increasingly sophisticated attacks from motivated adversaries are just two of these that impact the protection of sensitive organizational and customer data. In the last year, 58% of our respondents indicated that their organization had been infiltrated by a virus or malware, while another 42% had employees accidentally lose data.

The growth in the BYOD model and the gradual erosion of the traditional organizational network boundary serves to remind us that a best-in-class approach to data protection should not only focus on comprehensive administrative policies and pragmatic technical controls, but must also find its origin in the core of the organization. Indeed, organizations must engage on multiple fronts to provide superior data privacy:

Visibility: understand, through surveys and technical measures, how consumer devices are being utilized within the organization. This is needed as a baseline to understand basic risk and behavior and to recruit executive buy-in for future measures.

Cultural indoctrination: make data protection core to the mission of the organization with executive backing. Data protection awareness and understanding should be as "everyday" as locking the front door.

Policy: develop official policies with legal and liable guidelines for both organization and employees. A comprehensive data protection policy should be put in place to cover all devices no matter whether they are owned by the company or staff. IT policies should be regularly reviewed and updated to fortify against ever evolving exploit techniques.

Training: educate end users and staff regularly to ensure awareness of these policies and the importance of data protection. The approach of simply ensuring that staff, upon commencement of employment, sign-up to a policy which might have remained unchanged for several years is no longer adequate.

Technical control: do not forget low hanging fruit. Enforcement starts at a simple level – ensure that anti-malware software is up-to-date and promptly deploy security patches. Investigate encryption technologies fundamental to providing protection for your data. Small and mid-market companies may find it easier to implement solutions such as device control to eliminate additional risk without requiring the effort and overhead of a full DLP solution. As financial constraints allow, implement increasingly sophisticated technical controls which concentrate on reinforcing the business' mission and have strategic commitment from above.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, Antivirus and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Texas, Florida, Washington D.C., Ireland, Luxembourg, Singapore, the United Kingdom, and Australia. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension®
IT Secured. Success Optimized.™

Global Headquarters
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.480.970.1025
fax: +1.480.970.6323