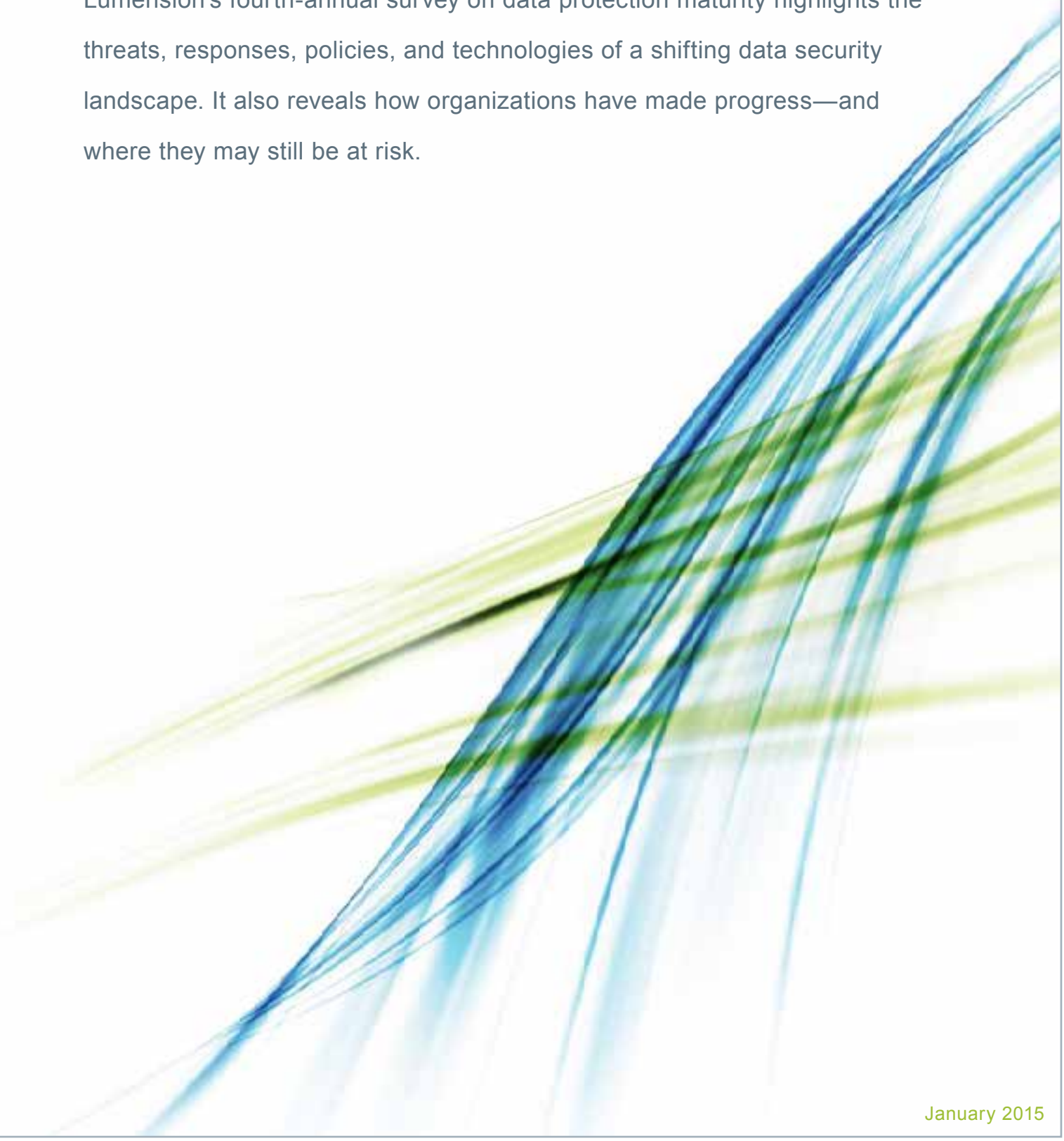
2015 Data Protection Maturity Report

Lumension's fourth-annual survey on data protection maturity highlights the threats, responses, policies, and technologies of a shifting data security landscape. It also reveals how organizations have made progress—and where they may still be at risk.



January 2015

WP-EN-01-28-15

It has become a truism that you can't go more than a couple of weeks without seeing a news headline about a major data security breach. It's the goal of every security manager—and indeed, of every CIO, CMO, and CEO—to stay out of those headlines.

But the attacks described in news reports are evolving. So is the way organizations approach security, as revealed in Lumension's comprehensive yearly survey on data protection maturity.

Cyber-attacks are increasingly motivated by financial gain as well as by geopolitical advantage. They target not only financial transactions handled by large banks and retailers, but every kind of data owned by every type of enterprise. A case in point is the recent Sony Pictures data breach, which disabled computers, leaked unreleased films and scripts, and exposed employee data. It also divulged a trove of email exchanges that opened the company to legal and financial risk, not to mention the operational and reputational impacts.

That last item should have every security manager quaking. Conventional wisdom is that you focus on protecting the data crown jewels: company intellectual property and customer personal data. But if every email is a target, if every piece of data on your network is at risk, then the bar for data protection maturity just got that much higher.

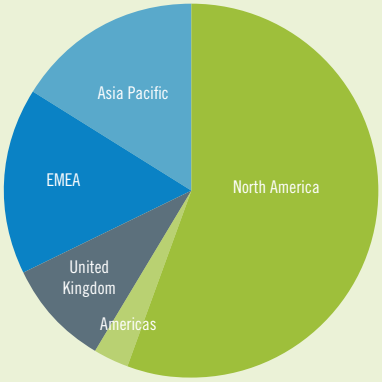
The *Lumension 2015 Data Protection Maturity Report* reflects these trends. It shows how organizations are responding to growing threats with better technology, policies, financial commitment, and corporate focus. It also uncovers some gaps—in IT's response to cloud and mobile, as well as in security fundamentals.

Finally, our report leads to the security best practices that can better protect your information and your business—and help you achieve the level of data protection maturity that's right for your organization.

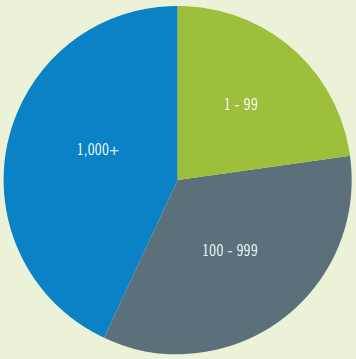
2015 Survey Respondents

In late 2014, Lumension surveyed more than 700 professionals from countries around the world, primarily North America (56 percent), Europe/Middle East/Africa (16 percent) and Asia Pacific (16 percent). About one-quarter worked at small businesses with 99 or fewer workers, one-third at midsize organizations with 100 to 999 employees, and slightly less than half at large enterprises with a workforce of 1,000 or more. All were directly involved in managing key aspects of IT security.

Respondents by region



Respondents by number of employees



Continued »

Incidents in the Night

Organizations continue to confront a wide range of cyber-attacks, from malware intrusion (57 percent), to exploitation of software vulnerabilities (23 percent), to denial-of-service attacks (19 percent). (See Figure 1.) They also grapple with a variety of related risks, including theft of IT assets (34 percent), accidental data loss by employees (40 percent), and deliberate data theft by employees (9 percent).

The average number of incidents per respondent, at 2.34, fell for the third year in a row, down 6 percent since 2014 and 12 percent since 2013.

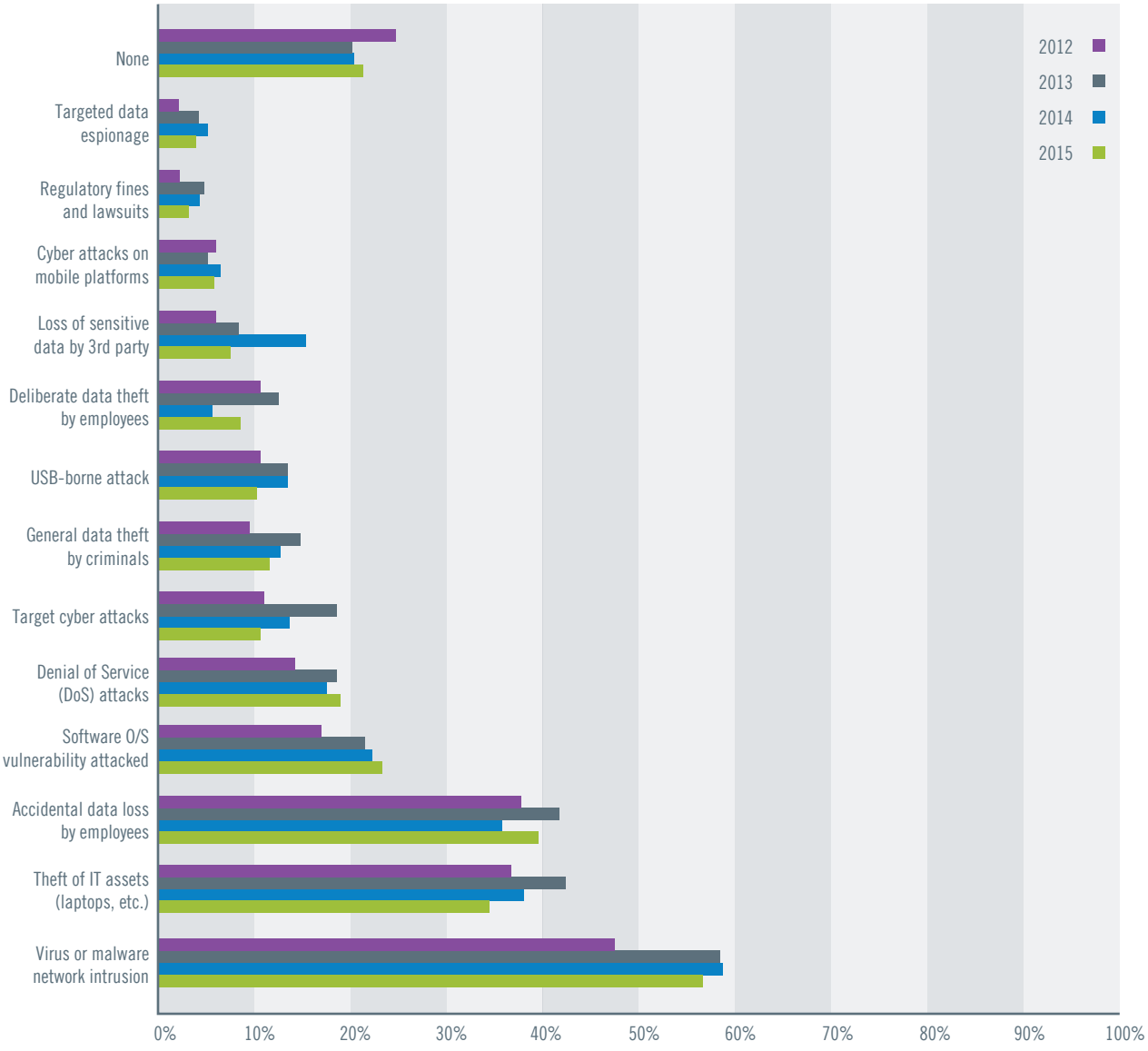


Figure 1

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

Continued »

The most common form of attack, virus or malware network intrusions, was down 4 percent since last year, though up 19 percent since 2012. Other notable changes included attacks on operating system or software vulnerabilities, up 5 percent since 2014 and 36 percent since 2012; and denial of service attacks, up 9 percent in the last year and 34 percent over the past four years.

The largest increase in the past year was in accidental data loss by employees, up 10 percent. Very likely that reflects the growing reliance on mobile devices and the overall increased use of corporate data by a broad cross-section of employees.

The biggest decrease was loss of sensitive data by a third party, down 52 percent. That may be a result of closer attention on data security by all organizations. More likely it reflects better governance of how partners, subcontractors, and service providers manage their data.

Threat Response

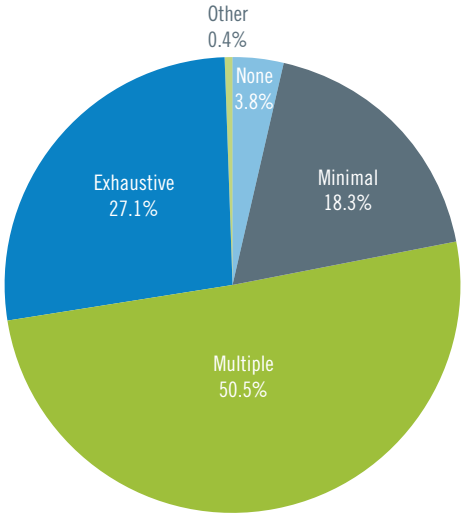
Organizations respond to data security threats—and the business risk they represent—through a range of policies, processes and technologies:

Data protection policies — One-half of organizations now maintain multiple data protection policies. (See Figure 2.) Nearly one-third say their policies are exhaustive. For the most part these numbers have increased progressively over the past four years, which is what we'd expect to see as organizations recognize the strategic importance of security.

Likewise, organizations that maintain minimal security policies fell 12 percent since 2014 and 30 percent since 2012, while those that have no security policies dropped 46 percent in the last year. Still, it's a concern that well over one-fifth of companies have minimal or no security policies.

Figure 2

What type of IT data protection policies exist?



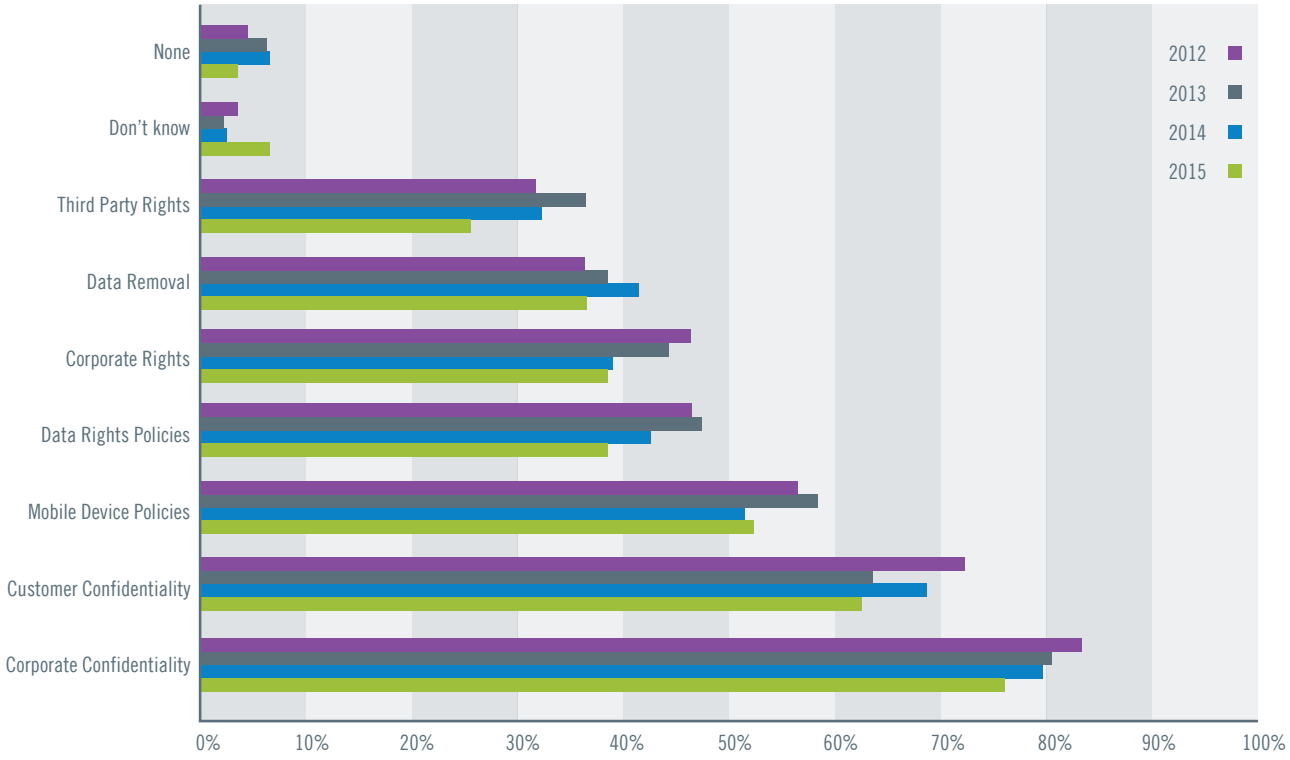
Employee guidelines — Organizations maintain a range of data protection guidelines as part of employee agreements, covering issues such as corporate confidentiality (76 percent), customer confidentiality (63 percent), and mobile device policies (52 percent). (See Figure 3.)

Surprisingly, though, several of these categories saw marked declines, some for the second or third year in a row. Third-party rights guidelines plunged by 21 percent since last year. Data removal guidelines dropped by 13 percent over the same period. Most astonishing, given the strategic importance and high level of risk associated with customer data, customer confidentiality guidelines slid by 9 percent; in fact, well under two-thirds of companies now maintain employee guidelines that address customer confidentiality. The only category that showed growth was organizations that don't know what data protection guidelines are included in employee agreements, a worrisome development.

Continued »

Figure 3

In some organizations employees are required to adhere to data protection guidelines as part of their employee agreement. Which of the following organizational guidelines are included in your employee agreements?



Security training — Nearly half of organizations that offer data security training do so on a formal, ongoing basis, a number that has held relatively steady over the past few years. (See Figure 4.) Twenty-eight percent of companies provide informal or ad hoc education, while 15 percent offer only one-time training. A troubling observation is that 9 percent of organizations offer no security training at all.

Security technologies — We asked respondents which security technologies their organization currently uses or plans to deploy in the next 24 months. Enterprises rely on a wide selection of solutions, from port/device control, to mobile device management, to whole disk, removable media, email, and file encryption. (See Figure 5.)

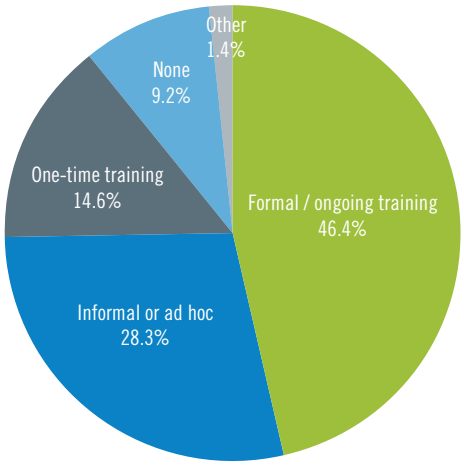


Figure 4

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

Continued »

The relative rankings of one technology against another has remained remarkably consistent over the past four years. But that doesn't mean we haven't seen interesting movement among the solutions currently used or planned for deployment.

First, while use of mobile device management (MDM) increased by 7 percent over 2014 and by 15 percent over 2013, planned use remains steady, at 28 percent of organizations. That might suggest we're approaching a saturation point in mobile device use, as 79 percent of organizations either have mobile device management or know they need it.

The biggest year-over-year advances came in four other areas: full data loss/leak prevention (DLP), email encryption, whole disk encryption, and port/device control. Among currently used technologies, full DLP leapt 44 percent. And while full DLP remains below the middle of the pack in terms of prevalence, with 29 percent of companies using the technology, the number of firms planning its deployment jumped 38 percent.

Meanwhile, email encryption gained 16 percent, disk encryption grew 13 percent, and device control rose 12 percent. Surely these increases are in response to recent high-profile breaches, as organizations strive to prevent data loss or at least ensure that leaked information can't be read.

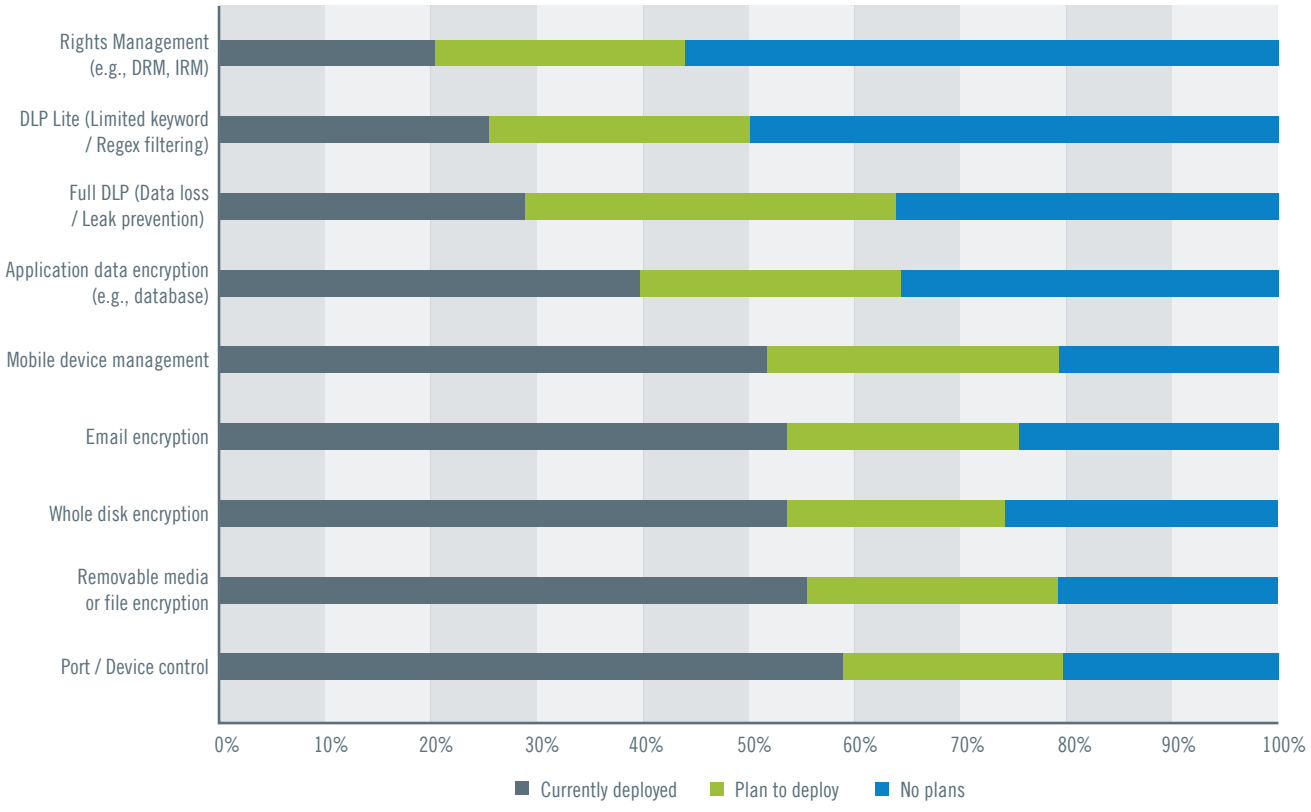


Figure 5

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

Continued »

Compliance Confusion?

While organizations are clearly responding to security risks, they may be less assured when it comes to regulatory compliance. (See Figure 6.) Between 2013 and 2014, compliance with industry-specific regulations—such as the PCI Data Security Standard (DSS) for retail and Health Insurance Portability and Accountability Act (HIPAA) rules for healthcare—rose significantly. But in 2015 those numbers fell, in some cases back to 2013 levels.

If we factor in those that said particular regulations don't apply to them, the average number of organizations in compliance dropped only slightly, from 40 percent in 2014 to 39 percent this year. But what does it mean that less than 40 percent of companies report they're compliant with the regulations they should be following? If nothing else, it suggests confusion over how relevant regulations apply to data security.

We see that confusion reflected in data privacy compliance—at a time when state and federal agencies in countries around the world are sharpening their focus on safeguarding personal information. The number of organizations that say they're compliant with data privacy laws leapt 90 percent, from 32 percent last year to 61 percent in 2015. Still, 39 percent say they're not currently compliant, while 18 percent say the laws don't apply to them. But given that data privacy laws generally cover both customer and employee data, there's almost certainly at least one data privacy law that applies to every organization.

Data Security Leaders

Every bell curve has its leaders and laggards. Security laggards are those lacking in data protection culture, policies, and resources. But what about security leaders? What factors place enterprises ahead of the curve? Overall, data security leaders:

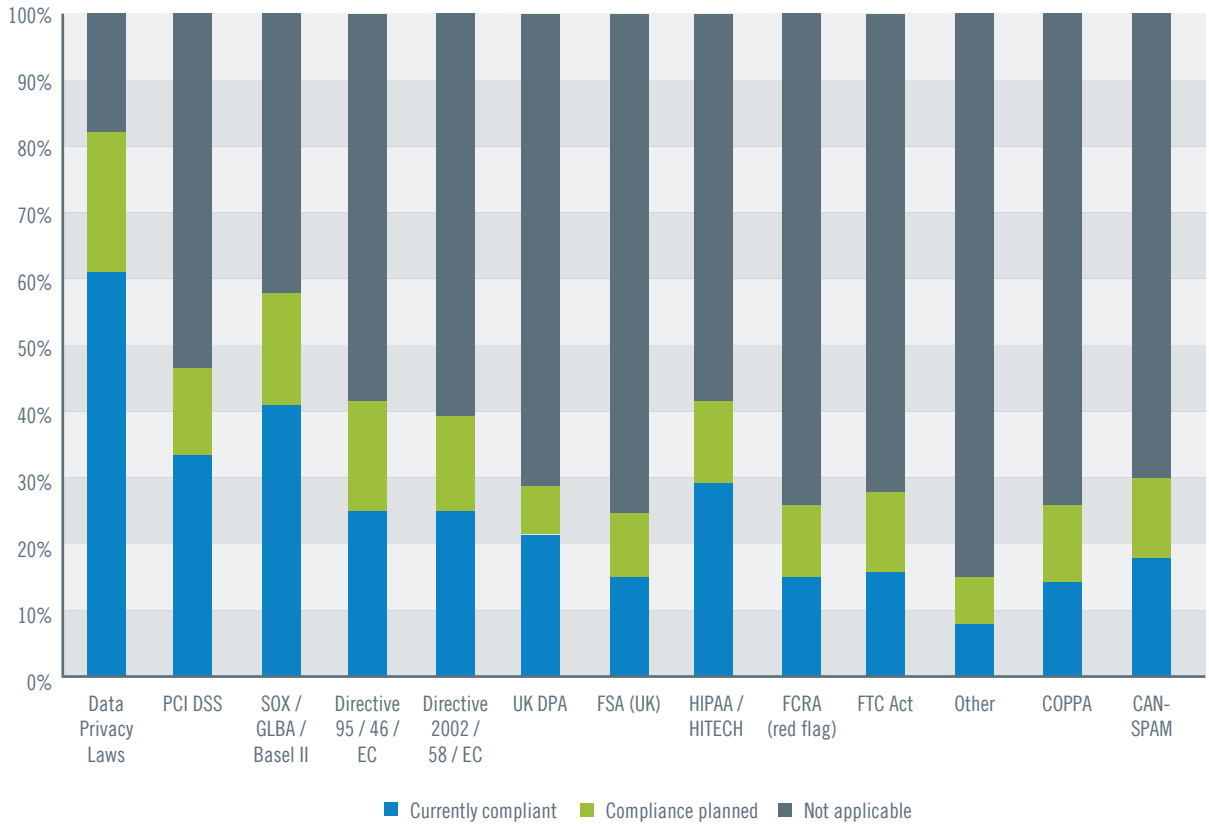
1. Maintain comprehensive data protection policies
2. Include security guidelines in their employee agreements
3. Offer ongoing, formalized security training
4. Dedicate an appropriate proportion of their IT budget to security
5. Assign appropriate people and financial resources to security
6. Invest in both basic and sophisticated security technologies
7. Maintain clear policies for use of personal devices
8. Understand the legal and financial implications of relevant regulations
9. Emphasize security as a strategic initiative
10. Build data protection into their corporate culture

The largest increase in incidents last year was due to accidental data loss by employees.

Continued »

Figure 6

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



Organizational Priorities

Another piece of good news is that security spending as a proportion of overall IT budget seems to be moving in the right direction. (See Figure 7.) For example, the number of organizations that assign less than 2 percent of their IT budget to security slid 26 percent between 2014 and 2015, while the number that dedicate as much as 10 percent ticked up 34 percent. At a time when researchers from Gartner to the Corporate Executive Board are predicting annual IT spending growth in the range of 3.3 percent to 3.9 percent, that should mean more real dollars for data protection.

The average IT security budget in 2015 is expected to be 6.65% of the overall IT budget.

Continued »

Figure 7

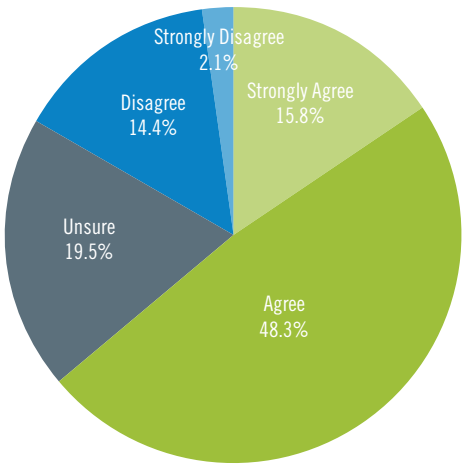
How much of your IT budget is spent on IT security?

Not surprisingly, then, more respondents say their organizations are applying the right resources to data protection. (See Figure 8.) Fully two-thirds agree or strongly agree they have sufficient resources to comply with data security policies and best practices. Seventeen percent disagree or strongly disagree. These numbers are all improvements, reversing a three-year downward trend. Still, 20 percent are unsure, a number that has remained roughly consistent over the past four years.

Well over one-fifth of companies have minimal or no security policies.

Figure 8

How much do you agree with this statement? "My organization has sufficient resources to achieve compliance with data security policies and best practices."

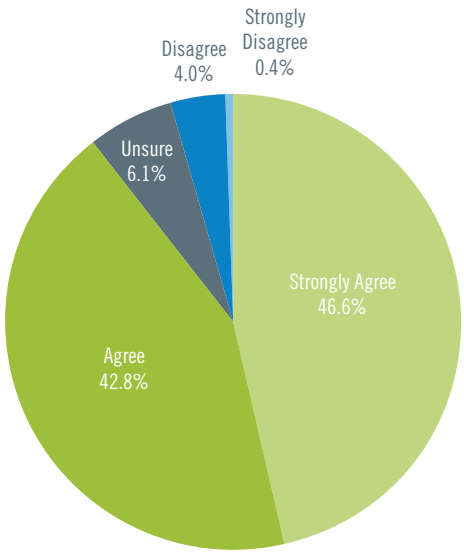


Continued »

Likewise, businesses increasingly recognize that data protection is fundamental to their operations. (See Figure 9.) Nearly 90 percent of organizations agree or strongly agree that data security is a strategic initiative across the enterprise. Only 4 percent disagree or strongly disagree, while only 6 percent are unsure. After remaining fairly consistent over three years, these numbers all improved significantly in 2015.

Figure 9

How much do you agree with this statement? "Data security is a strategic initiative across the enterprise."



Data Security on the Go

Among the top trends in IT over the past few years have been mobile and cloud computing. While these developments are no longer new, they remain pervasive and influential, and those realities are reflected in our survey results.

We queried respondents on how their organizations manage personal mobile devices from a financial and administrative perspective. (See Figure 10.) Forty-seven percent assign responsibility for mobile devices to the corporation, while more than two-thirds allow some form of "bring your own device," or BYOD. In fact, 29 percent cede full responsibility for mobile devices to employees. These numbers all reflect a gradual trend away from company-supplied devices toward BYOD. Organizations retaining liability for devices dropped 9 percent since last year, while those turning complete responsibility over to workers rose by one-quarter.

To get an even clearer picture, we asked respondents which portion of their organization's mobile and USB devices are personally owned. (See Figure 11.) Fourteen percent report that all or nearly all those devices are employee-owned, a one-quarter expansion year over year. Thirty-five percent said less than one-fifth of mobile devices are owned by workers, a 10 percent decline.

These shifts further suggest that enterprises increasingly accept a BYOD strategy. Whether that's good for data security is an open question. Still, the number of respondents that don't know what proportion of devices are owned by employees has steadily declined, by 15 percent in 2014 and another 16 percent this year.

For more perspective on mobile strategies, we asked respondents to describe their organization's approach to network access by employee-owned smartphones and tablets. (See Figure 12.) Only eight percent maintain an "open access" policy. One-fifth allow access with employee education, while 16 percent limit access to higher-level staff. One-quarter permit "controlled access," while more than one-quarter restrict access. These numbers have remained remarkably consistent year over year, and they suggest that while more enterprises are allowing BYOD, they're being circumspect about connecting those devices to corporate networks.

Continued »

Figure 10

How are personal mobile devices, such as phones (and tablets), financially and administratively managed within your enterprise?

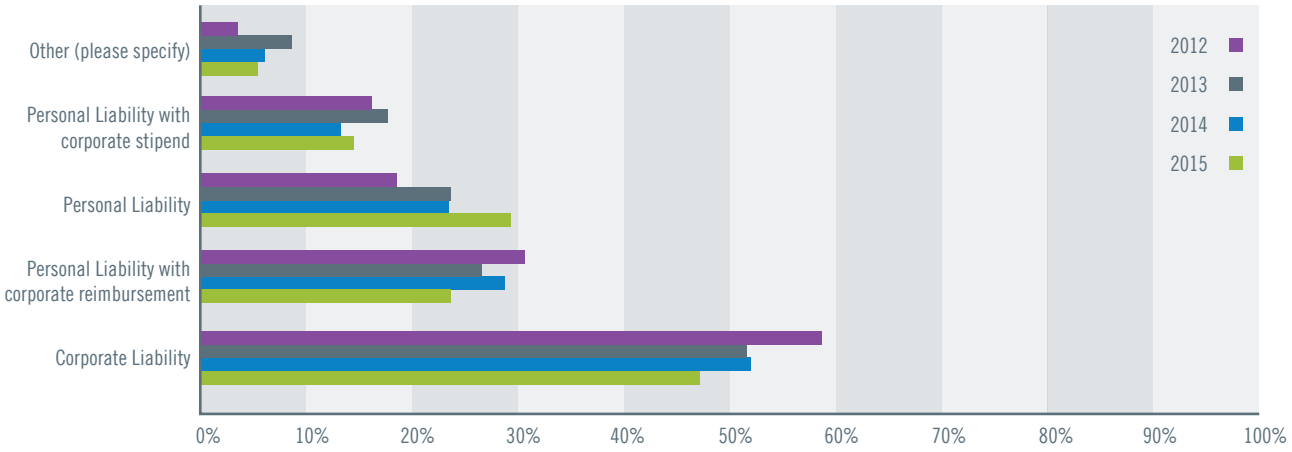
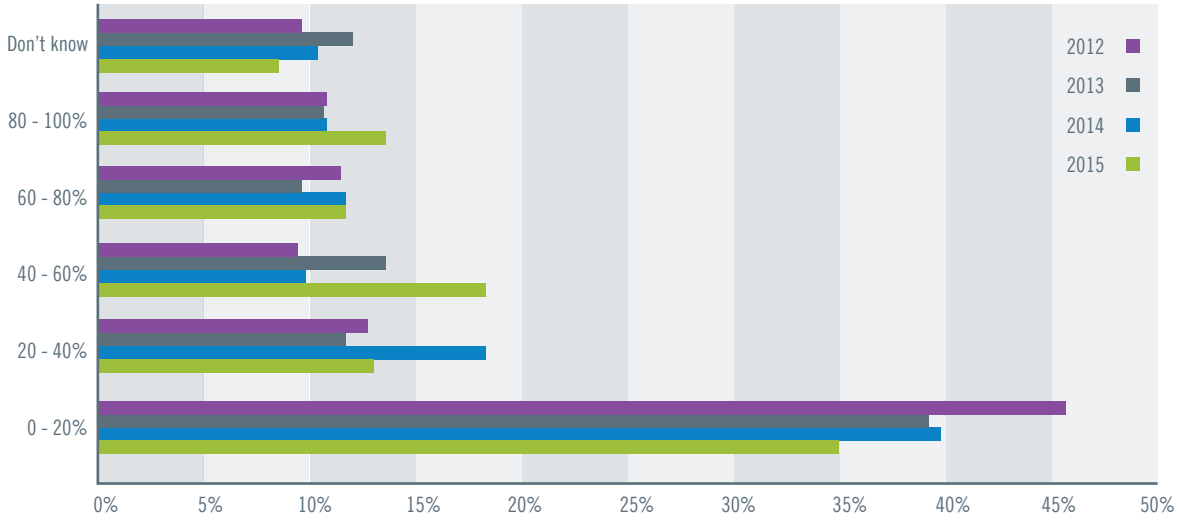


Figure 11

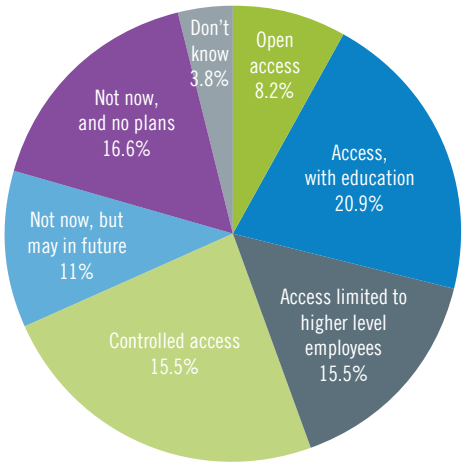
What portion of your administrative's regularly used USB and mobile devices are personally owned? Please consider flash drives, smartphones, and tablets.



Continued »

Figure 12

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

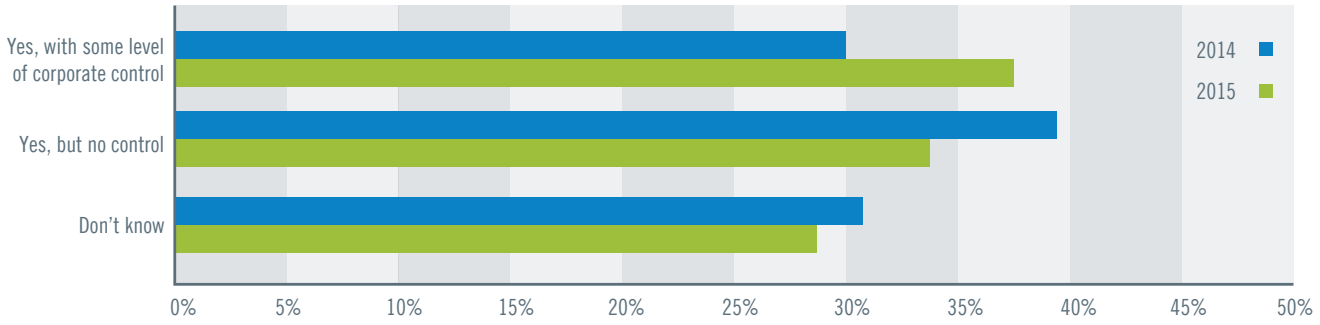


Finally, for the first time last year we asked whether employees use personal cloud storage such as Dropbox and Microsoft OneDrive. The results this year show significant shifts in cloud usage and policy. (See Figure 13.)

The number of organizations that have no visibility or control over employee use of cloud storage dropped 14 percent, while those that have visibility, policies, and control rose 62 percent. Those are positive developments, and they suggest that companies are catching up to the real-world behaviors of their workers. Still, 29 percent of enterprises don't know whether employees are using personal cloud storage, potentially exposing them to risk.

Figure 13

Do your employees use personal cloud-storage (e.g., Dropbox, iCloud, SkyDrive, etc)?



The results this year show significant shifts in cloud usage and policy.

Continued »

Best Practices Make Perfect

The *Lumension 2015 Data Protection Maturity Report* demonstrates the continuing need for security best practices. While organizations appear to be making progress on several security fronts, the threats persist, and fundamental approaches in both policy and practice are sometimes lacking.

Enterprises that achieve the highest levels of data protection maturity focus on best practices in five essential areas:

» **Security policy** — Create comprehensive, documented security policies, with support from your legal department and clear statements about what happens if employees fail to comply. You should have policies and procedures for the organization overall, as well as for workers at all levels. Bearing in mind ongoing developments in mobile platforms, cloud computing, and social media, you probably need rules that address these issues specifically. Be sure to review your policies regularly and update them to reflect changes in security threats and business needs.

» **Employee training** — Train all users on an ongoing basis to ensure they understand your security policies, as well as their roles and responsibilities in protecting corporate data. Security education should be regular, formalized, and required. It should start at the beginning of employment, and it should adapt to changing security risks and workplace practices.

» **Endpoint visibility** — You need comprehensive and reliable insights into how all endpoints, including mobile and USB devices, are being used across the enterprise—and especially into how they connect with both the corporate network and the cloud. That will help you understand employee behavior, and it will give you a baseline for endpoint risk. Remember, you can't manage—or get budget for—what you can't measure.

» **Technical control** — A significant portion of data protection maturity is basic "blocking and tackling." Don't overlook the fundamentals. Install software updates promptly to minimize your exposure to known threats. Make sure your antivirus software is enforced and up-to-date. Take advantage of encryption to protect your data in case it's lost or stolen. Conduct a cost-benefits analysis on the value of deploying more sophisticated technologies that can strengthen your security posture. Especially consider application whitelisting, which prevents malware from running and can lower your overall security risk.

» **Corporate culture** — Finally, security managers and corporate executives alike must recognize the strategic nature of data security. Protecting data must become a central part of your organization's processes and even its business strategy. That starts in the corner office, but it must extend throughout the enterprise. Built into your organization's culture, the instinct to protect data will drive the appropriate security investments that can free your organization to leverage data toward business results.

As the *Lumension 2015 Data Protection Maturity Report* confirms, organizations must remain vigilant in safeguarding their mission-critical data—bearing in mind that from a risk perspective, all corporate data is now mission-critical. Doing so might just help you avoid the next negative news cycle. It can also help you achieve the data protection that will position your enterprise for continuous operations and strategic growth.

Continued »

Data Protection Maturity Model

Lumension has developed a Data Protection Maturity Model to aid in the analysis of our annual data protection maturity survey. Like other commonly used maturity models, it offers a framework for assessing organizational and process capabilities.

Within the model we classify survey questions in three categories: Technical Controls, Organizational Motivation, and Administrative Controls. We apply the results in each category to score organizations on their data protection maturity. We display the maturity score by company size, ranging from less than 10 to more than 1,000 employees.

Emphasizing the importance of concrete action, Technical Controls comprise 40 percent of the score. (Planned security measures are important, but they don't protect data.) We also assess technical control effectiveness, based on reported incidents, and adjust scores accordingly.

An organization's intentions are important, however, so Organizational Motivation contributes 35 percent to the score. This highlights the need for cultural commitment and sufficient resources to establish a data security mindset.

The remaining 25 percent of the score we apply to Administrative Controls.

Finally, we assign each survey response a weighted score to create a composite maturity score. Maturity scores are represented by the diamond-shaped points in the Data Protection Maturity chart. (See Figure 14.) The maturity score classifies the organization's level of data protection maturity as follows:

- **Optimal** — Organizations characterized by best-of-breed data security
- **Operational** — Those that demonstrate adequate security
- **Standardizing** — Enterprises that have some organizational commitment and technical controls but are still maturing
- **Ad Hoc** — Those that merely react to security events as they occur

Comparing this year's results to last year's, we see two distinct trends. First, there's a steeper line between small businesses and large enterprises. The starting point for companies with fewer than 10 workers is about the same as in 2014. But the ending point for enterprises with more than 1,000 employees is significantly higher. That suggests that while the smallest companies may be struggling to keep up, the largest increasingly recognize the strategic importance of data protection—and are taking the appropriate steps.

Continued »

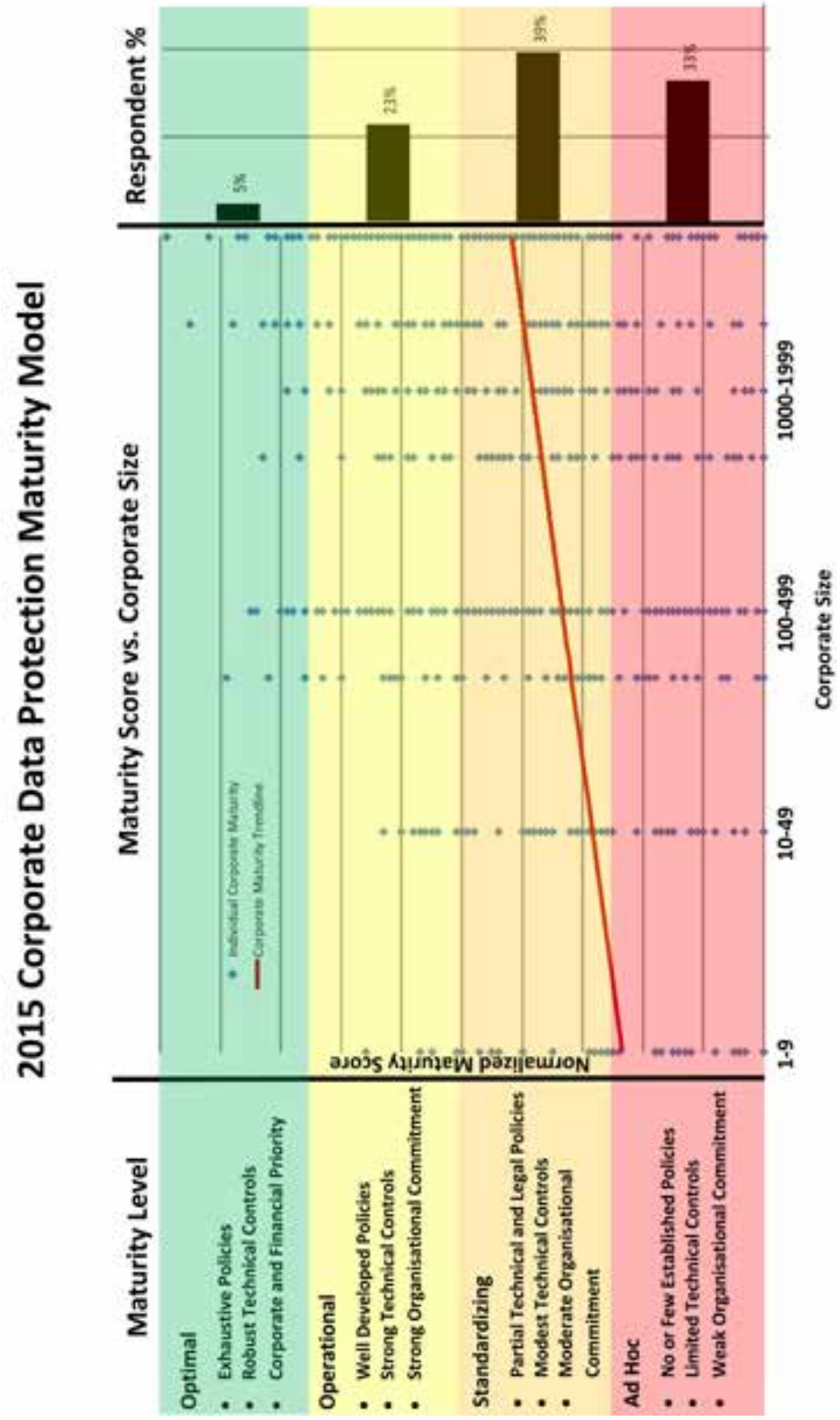


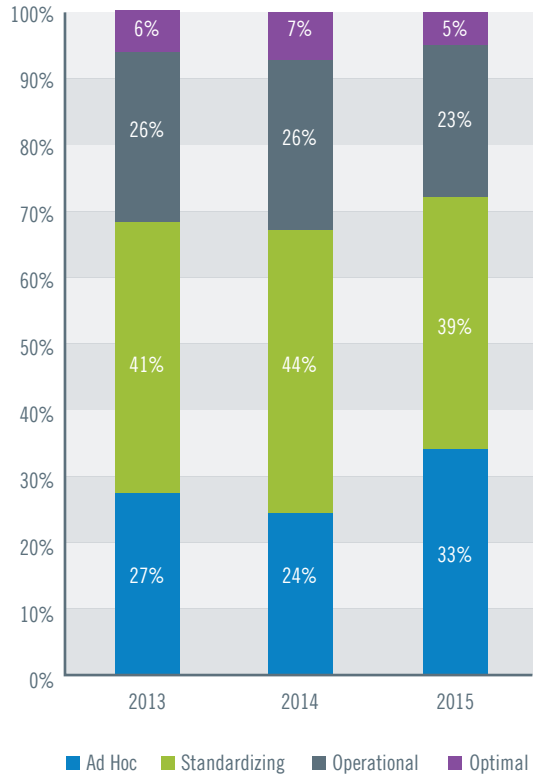
Figure 14

Continued »

Data Protection Maturity Model (cont.)

The second trend is less encouraging. Optimal organizations, at 5 percent of respondents, are down 2 percentage points since 2014. (See Figure 15.) Those considered Operational, at 23 percent, are down 3 percentage points year over year. The Standardizing enterprises, at 39 percent, are down 5 percentage points. But the "Ad Hocs"—those companies that merely react to security events as they occur—rose 9 percentage points, from 24 percent in 2014 to 33 percent this year. It would seem that many organizations still have work to do on their data protection maturity.

Figure 15



Protecting data must become a central part of your organization's processes and even its business strategy.

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 3,000 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.

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

Lumension
IT Secured. Success Optimized.™