Microsoft

Trends in Cloud Computing

Cloud Security Readiness Tool

Trends in Cloud Computing

Authors

Frank Simorjay
Microsoft Trustworthy Computing

Jeff Jones
Microsoft Trustworthy Computing

Contributors

Michael Mattmiller
Microsoft Trustworthy Computing

Sian Suthers
Microsoft Trustworthy Computing

Richard Saunders
Microsoft Trustworthy Computing

Price Oden
Microsoft IT

Cynthia Sandvick
Microsoft LCA

Steve Wacker
Wadeware LLC

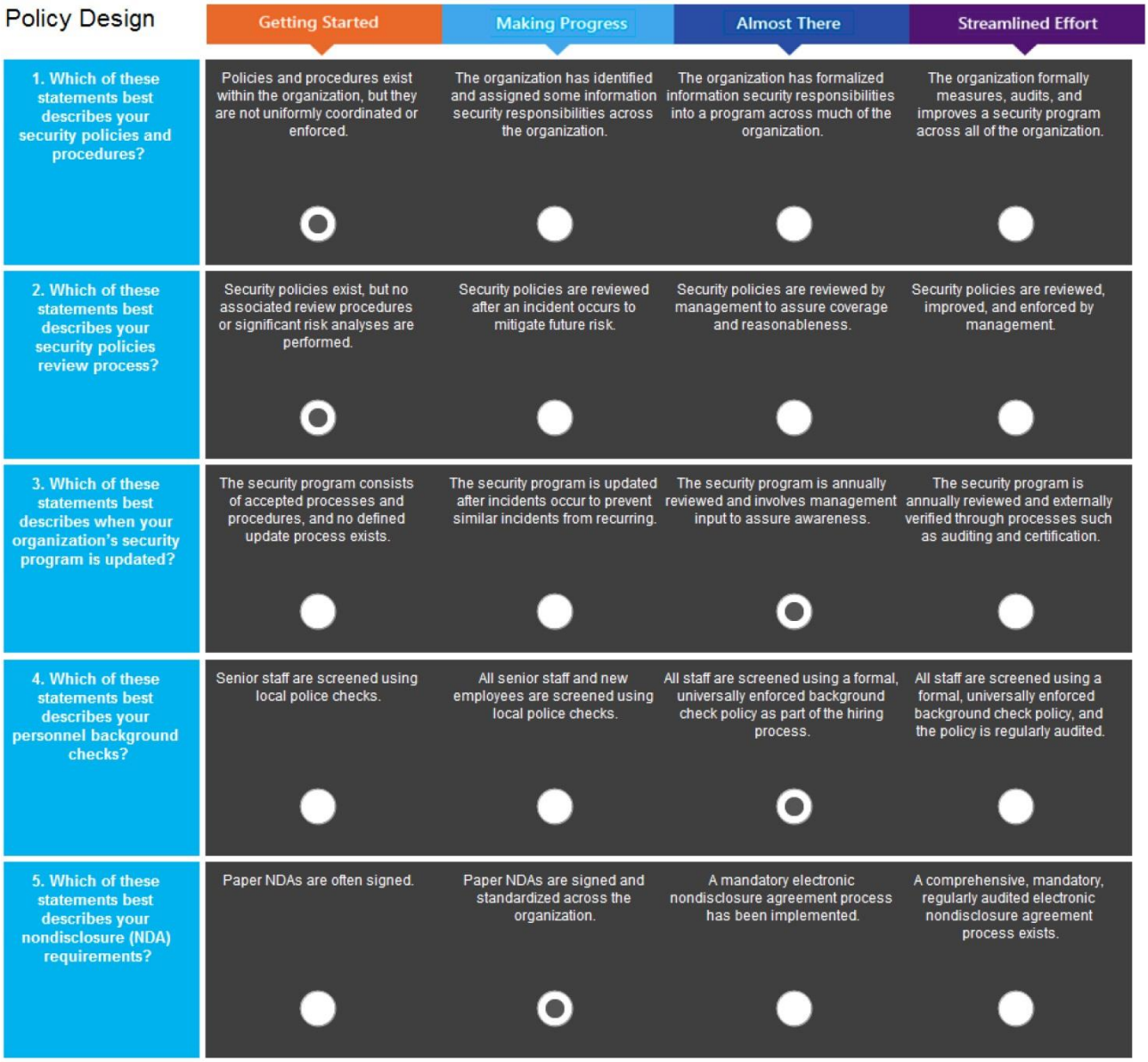
Microsoft

Table of contents

About this report

This report is the result of information collected in the Cloud Security Readiness Tool (CSRT). The CSRT is a brief survey that seeks information about the maturity level of an organization's current on-premises IT infrastructure. Organizations can use the CSRT to better understand their systems, processes, policies, and practices. They can also improve their current IT state, learn about relevant industry regulations, and receive guidance on how to evaluate different cloud options.

Figure 1. Sample CSRT questions and possible answers



Microsoft

This report analyzes data that was collected in the six-month period between October 2012 and March 2013. The data consists of answers provided by people who used the CSRT. Approximately 5700 anonymized responses to the CSRT's 27 questions were received from around the world.

The accuracy of the data in this report is only as accurate as the answers provided by those who used the tool. The answers they provided reflect the relative maturity levels of their IT environments, and although efforts were made to verify the data it is possible that a small number of incorrect entries could have slightly skewed the results. The data was also sanitized to remove obvious "test case" entries and for analysis purposes.

Maturity levels

The following four IT maturity levels of survey respondents are referenced throughout this report. These maturity levels are calculated based on answers provided to the questions in the CSRT.

- **Getting Started**. Undocumented, ad hoc state. Reactive and incident or event response-driven.
- **Making Progress**. Response-driven, following trends, and somewhat repeatable with limited automation in segments.
- **Almost There**. Scaled response, using programs. Limited scaling still segmented.
- **Streamlined**. Centralized, automated, self-service, and scalable. Can allocate resources automatically.

The questions that were used in the CSRT can be read in their entirety in Appendix 1.

Background

Cloud computing

By their very nature, technological changes are jarring. Business as usual gets turned on its head as pioneers work to put potential into practice. Trust is implicit in the vision, although for early adopters that trust can seem uncertain. For those yet to embrace technological change, trust—for various reasons—can be a reason for a more cautious approach. Most revolutionary ideas and practices require time for their impact to be felt—that is, for a critical mass to understand the benefits and risks. Cloud computing is no exception.

After maturing for several years in various forms, the cloud is coming into sharper focus as more people adopt cloud services and gain experience that can be shared with others. As uses of cloud computing have expanded, so has industry expertise in harnessing its potential. In addition to serving as an underlying infrastructural pillar of the Internet, the cloud now supports an array of services and applications. From off-premises storage to running business applications on remote servers, the cloud's applicability to the modern computing experience is being realized.

Concerns and benefits of adoption

A number of benefits are regularly mentioned by cloud providers and customers, including reduced capital costs, economies of scale, time savings, flexibility, and scalability. However, organizations that consider cloud computing have also voiced a number of concerns. In multiple studies over the past several years, security and privacy are commonly cited[1] as top concerns.

These studies echo Microsoft experience as well. In customer discussions—especially with those who have not yet adopted the cloud—one of the very common topics is cloud security.

Many organizations that want to transition to the cloud would like simple, well-organized information to answer two questions: Where are we in terms of our current IT state? And what will be our IT state if we adopt a particular cloud service? Organizations that understand how these questions relate to them are in a better place to make informed comparisons and evaluate the concerns and benefits of cloud adoption.

Cloud Security Readiness Tool

In October 2012, Microsoft Trustworthy Computing released the free Cloud Security Readiness Tool (www.microsoft.com/trustedcloud) to help organizations accelerate their assessment of adopting cloud computing. The CSRT builds on the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) and is an interactive, easy-to-use survey that consists of 27 questions. The questions are designed to obtain information about an organization's industry and the maturity level of the organization's current IT infrastructure. Each question relates to a control area in the CSA CCM.

The CSRT uses respondent information to provide relevant guidance in a custom report that helps organizations better understand their *existing* IT capabilities, more easily evaluate cloud services in critical areas, and learn about compliance issues. It considers several areas, including security policy capabilities, personnel capabilities, physical security capabilities, privacy capabilities, asset and risk management capabilities, and reliability capabilities.

[1] For example, Intel IT Pro Research (May 2012) of 800 IT pros from Germany, UK, US, and China. More than 54% were very concerned and 87% were very or moderately concerned about security and data protection in public clouds. (For private clouds, the percentages were 38% and 69%, respectively.) www.intel.com/content/www/us/en/cloud-computing/whats-holding-back-the-cloud-peer-research-report.html

Microsoft

An additional benefit of the CSRT is that it helps organizations better understand their capabilities and potential cloud benefits with regard to relevant control standards and organizations. These standards and organizations include the Federal Office for Information Security (BSI) Security Recommendations for Cloud Computing Providers, the European Network and Information Security Agency (ENISA) - Information Assurance Framework (IAF), the International Organization for Standardization (ISO 27001), the Payment Card Industry (PCI), the Health Insurance Portability and Accountability Act (HIPAA), and the National Institute of Standards and Technology (NIST).

The CSRT has been available for a little over six months and has been used by hundreds of organizations around the world to help them better understand their current IT state and the potential cloud benefits listed in the Cloud Security Alliance's Security, Trust & Assurance Registry (STAR). This report analyzes the response data from this time period in an effort to learn about the current IT maturity levels of organizations that have used the tool.

The CSRT questions can be reviewed in Appendix 1.

Results overview

The body of the report examines responses to each of the 27 CSRT questions and considers how they reflect the current IT state of respondent organizations. This section provides an overview of the results.

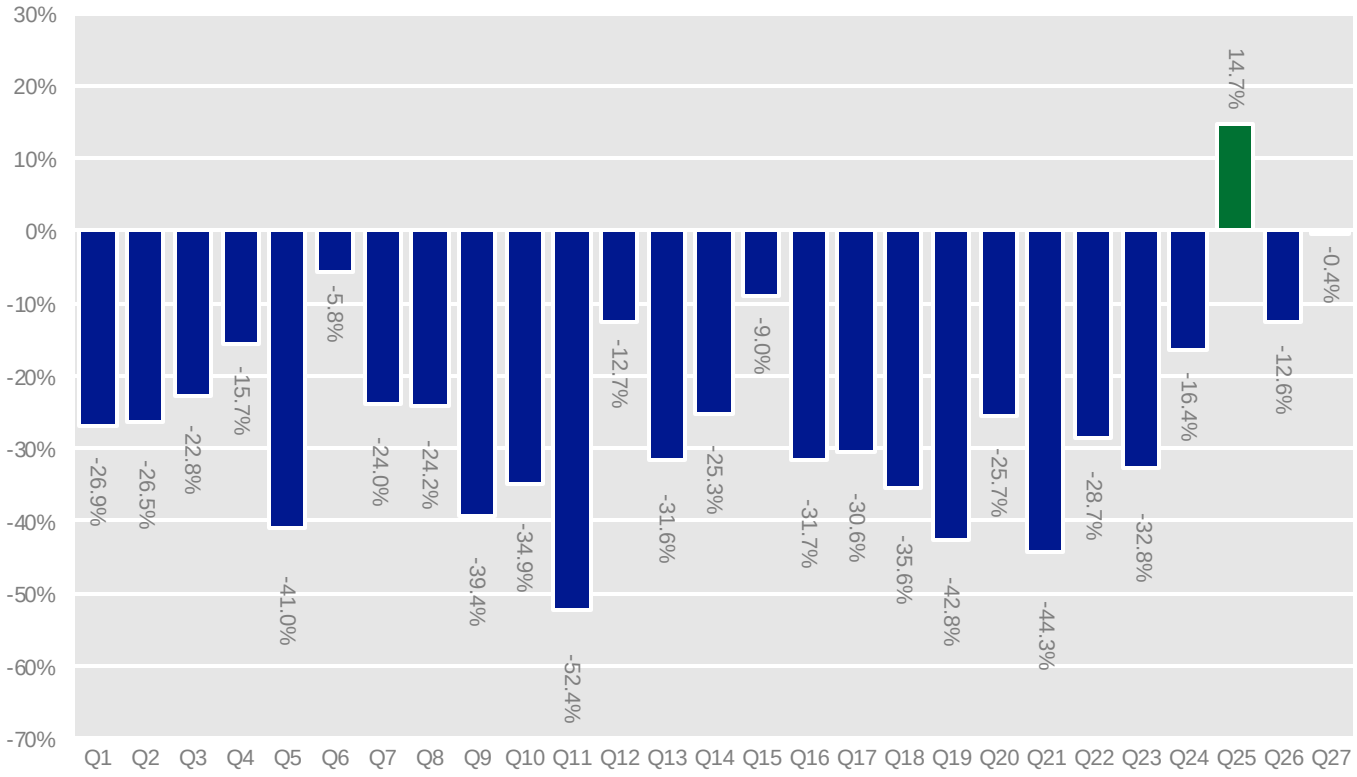
To gauge overall maturity, the following values were assigned to each of the four possible answers for each question:

- If the answer was Almost There or Streamlined, a +1 value was assigned for maturity.
- If the answer was Getting Started or Making Progress, a -1 value was assigned for maturity.

Next, the values for all respondent answers to all 27 questions were averaged and charted so that a positive value indicates organizations that are almost there or streamlined and a negative value indicates organizations that are still getting started or making progress. A zero value indicates that equal numbers of respondents were included in each maturity level pairing.

As shown in the following chart, most respondents indicated that their existing IT states were still getting started or making progress. Respondent answers to only one question (question 25, which relates to deploying antivirus/antimalware software), appears to indicate relative maturity for the average respondent.

Figure 2. CSRT respondent answers to all questions and the IT maturity levels they indicate



The answers that reflected the most advanced maturity levels overall were in the following areas:

- #25. (CCM IS-21). Information Security. Antivirus / Antimalware Software (+14.7%)
- #27. (CCM SA-12). Security Architecture. Clock Synchronization (- 0.4%)
- #6. (CCM FS-02). Facility Security. User Access by Role (- 5.8%)

It is perhaps encouraging that malware protection is relatively mature on average, but less so when you consider that almost 45% of respondents indicated they are getting started or making progress. For more information about these three areas, see the "Information Security," "Security Architecture," and "Facility Security" sections.

The answers that reflected the least advanced maturity levels overall—and therefore the areas in which organizations could most benefit from the cloud—were in the following areas:

- #11. (CCM HR-02). Human Resources Security. Employment Agreements
- #21. (CCM OP-03). Operations Management. Capacity / Resource Planning
- #19. (CCM IS-23). Information Security. Incident Reporting
- #5. (CCM LG-01). Legal. Nondisclosure Agreements
- #9. (CCM OP-04). Operations Management. Equipment Maintenance

Although there is not a clear common theme that ties these answers together, it is noteworthy that these areas all require budget beyond deployment of an IT solution.

Microsoft

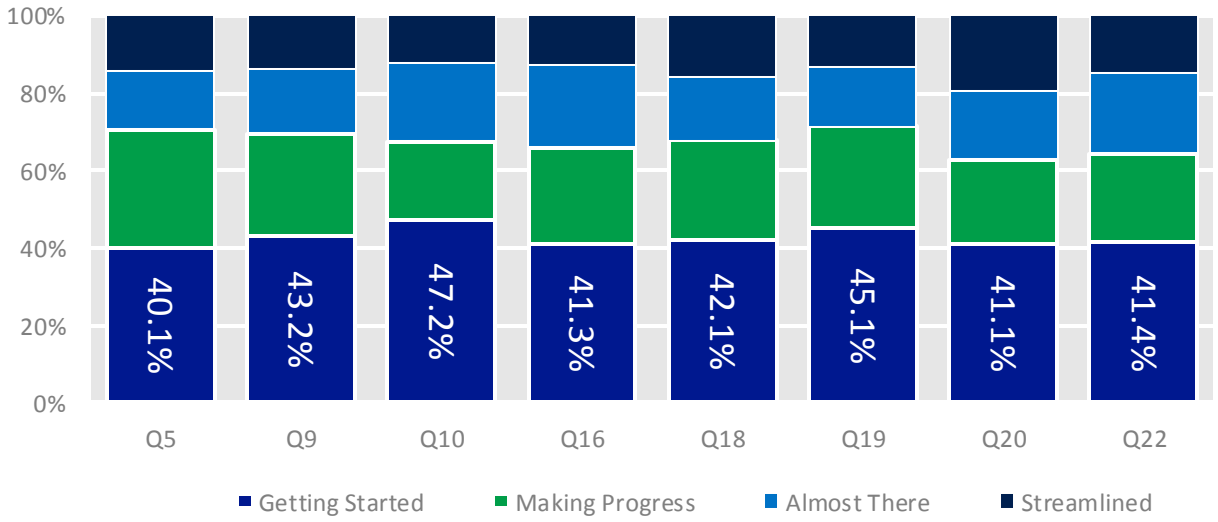
Observations

If one imagines an IT department that has placed a production environment into operation that meets business needs, the following assumptions can be made:

- Employment agreements depend on legal and HR processes.
- Nondisclosure agreements depend on legal and HR processes.
- Equipment maintenance and capacity planning require ongoing, post-deployment processes and budget.
- Incident reporting requires specialized processes and has increasing legal requirements in many regions.

It's also possible to consider the four answers to the questions themselves to get a less simplified view, such as in the following chart.

Figure 3. CSRT answers to eight specific questions and the IT maturity levels they indicate



This figure shows that there are eight areas in which 40% or more of the answers were the least mature, or getting started:

- #5. (CCM LG-01). Legal. Nondisclosure Agreements
- #9. (CCM OP-04). Operations Management. Equipment Maintenance
- #10. (CCM DG-02). Data Governance. Classification
- #16. (CCM FS-08). Facility Security. Asset Management
- #18. (CCM RI-01). Risk Management. Program
- #19. (CCM IS-23). Information Security. Incident Reporting
- #20. (CCM RS-01). Resiliency. Management Program
- #22. (CCM RS-06). Resiliency. Equipment Location

Observations

Most organizations are relatively immature across almost all of the control areas represented in the CSRT.

There is potential benefit in adopting a cloud computing solution from a vendor who has implemented best practices across the CSA's CCM.

Control mappings may provide additional benefits.

These areas of least maturity are also the areas in which organizations would potentially benefit the most from cloud computing, at least if they select services from vendors who are willing to attest to advanced maturity levels in these areas.

In contrast, the same three areas that were mentioned at the beginning of this section were the only ones for which an average of more than 20% of the respondent organizations assessed their own maturity at the highest level, or streamlined:

- #6. (CCM FS-02). Facility Security. User Access by Role
- #25. (CCM IS-21). Information Security. Antivirus / Antimalware Software
- #27. (CCM SA-12). Security Architecture. Clock Synchronization

The data shows that most organizations are relatively immature across almost all of the control areas represented in the CSRT, which emphasizes the potential benefit to be gained from adopting a cloud computing solution from a vendor who has retained skilled personnel and has implemented best practices across the CSA's CCM. Because the CCM and the CSRT report also provide mappings of the controls to some of the most common global industry standards, the potential benefits of cloud adoption may be even greater than previously estimated.

Microsoft

Worldwide observations

Policy design

Organizations' security policies and procedures and their review and update efforts (CCM IS-01, CCM RI-04, CCM IS-05)

Organizations should consider adopting and implementing security policies and procedures as well as formal and measured capabilities to ensure their quality and effectiveness. In addition, organizations should ensure that management is aware of security policies and procedures and includes their regular review as a strategic part of their business strategy.

Observations:

On average, 35 percent of organizations worldwide are still struggling to establish uniform security policies and procedures across their environments. Because such policies and procedures form the backbone of any organization's security posture, it's essential for them to seek ways of maturing their programs to help establish better security postures.

The trend of security policy creation, review, and revision is consistent across the board. In general, only about 17 percent (represented as Streamlined in the relevant graphs) of organizations have security programs that are formally managed, reviewed, audited, and regularly enforced.

Advantage of using a cloud provider:

Typically, cloud providers will have a security update plan in place that provides careful notifications to their customers. Cloud providers should also be able to maintain separate staging and production environments as well as provide access to staging environments so that changes can be evaluated and tested before they are deployed.

Figure 4. CSRT answers RE: information security management programs

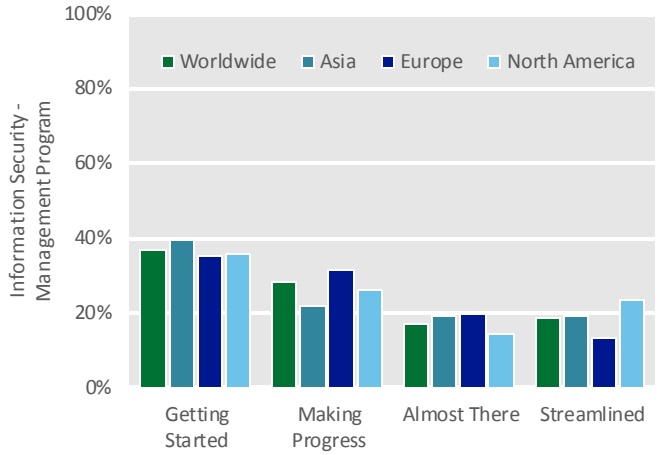


Figure 5. CSRT answers RE: information security policy reviews

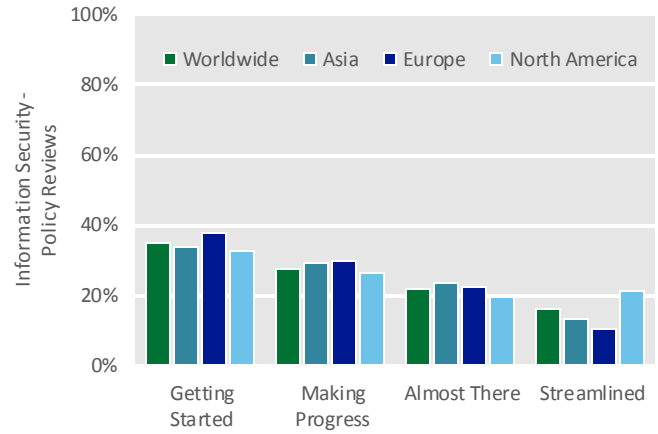
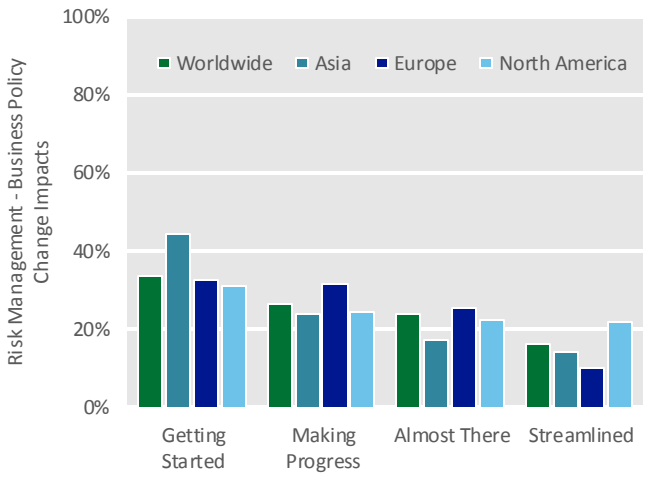


Figure 6. CSRT answers RE: risk management



Organizations' personnel background checks policies, nondisclosure agreement (NDA) policies, and security employment agreements (HR-01, HR-02, LG-01)

It is generally accepted that the human factor is one of the most important contributors to the success of an information security plan, but also presents one of the biggest risks. Malicious or disgruntled personnel with access to important information assets can be a significant threat to the safety and security of those assets. Even people without malicious intent can pose a danger if they don't clearly understand their information security responsibilities. These issues can be mitigated by ensuring that quality background checks are performed and periodically updated, and by ensuring that current NDAs are signed by employees, contractors, and other associated parties before they gain access to sensitive information or resources.

Observations:

Generally, data from Asia and Europe shows trends that minimal effort is expended toward ensuring high-quality processes for background checks, NDAs, and security employment agreements. There is greater general adoption of employee verification in 53 percent of North American organizations, including background screening that uses a formal, universally enforced background check policy as part of the hiring process. These figures may reflect more extensive enforcement of legal and human resource guidance in North America, while European organizations may be limited on what information they can legally collect during their hiring practices.

Advantage of using a cloud provider:

Cloud providers typically conduct regular pre and post-hire background checks on their employees, as well as maintain policies and procedures that define the implementation and execution of NDAs and confidentiality agreements. In addition, such NDAs are typically managed separately and audited at regular intervals, at least on an annual basis.

Figure 7. CSRT answers RE: personnel background checks

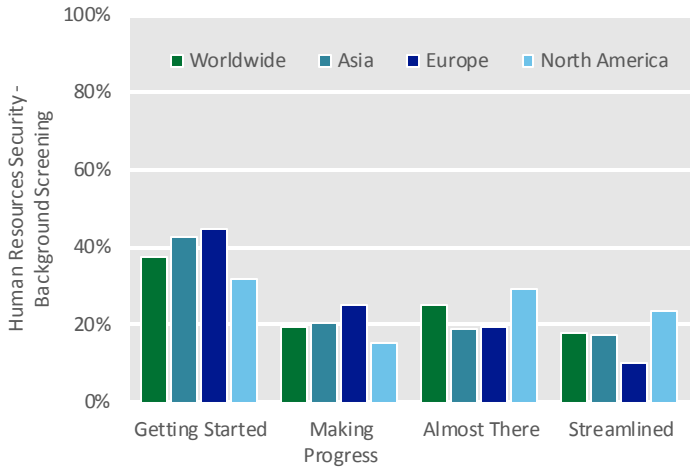


Figure 8. CSRT answers RE: nondisclosure agreements

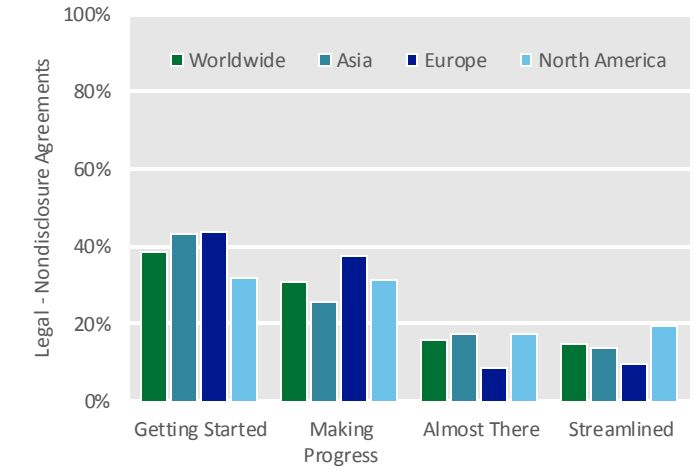
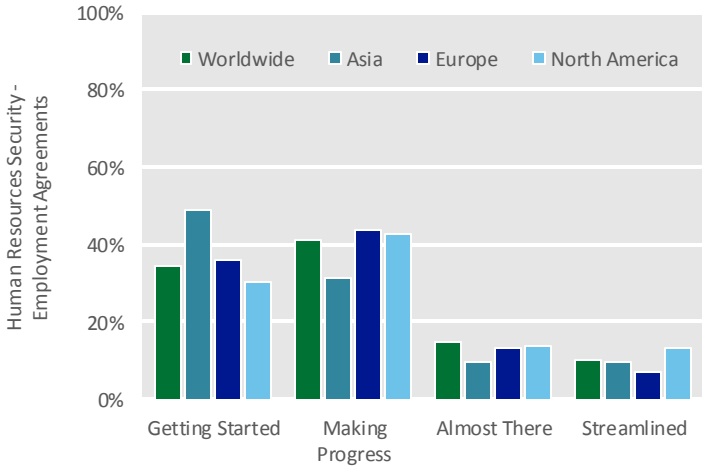


Figure 9. CSRT answers RE: employment agreements



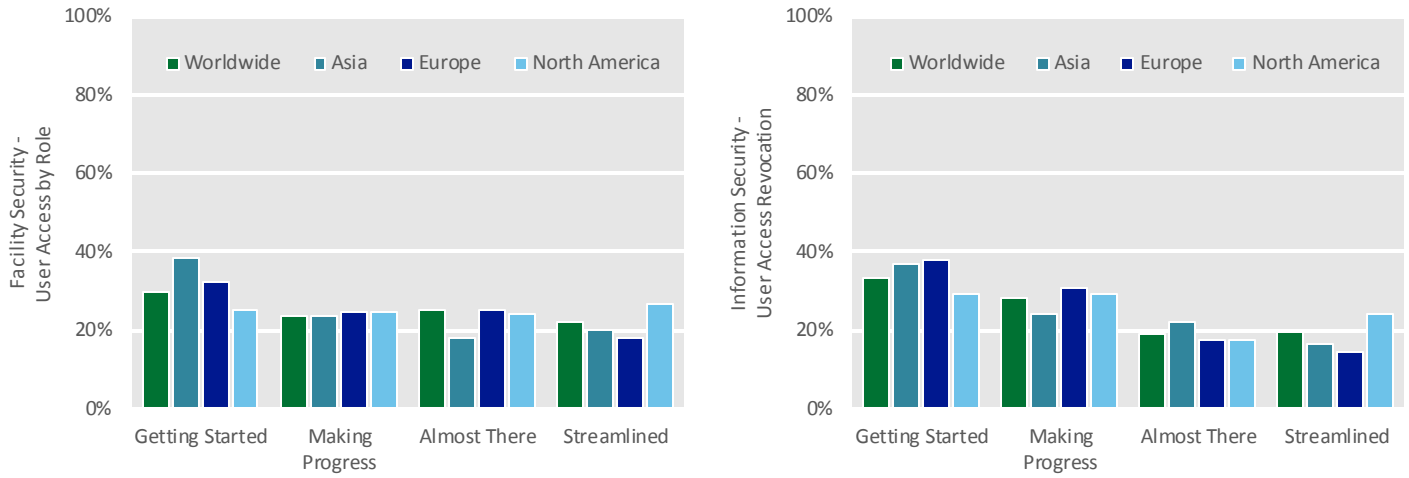
Microsoft

Physical design

Organizations' role-based physical access restrictions and their employee change/termination processes (IS-09, FS-02)

Controlling access is an important part of information security. Physical access to data center environments should be strictly controlled through various security mechanisms and limited to authorized personnel whose identities can be verified. If a malicious party gains unauthorized access to facilities that house sensitive data, hardware, and networking components, information assets could be subject to serious risk of disclosure, damage, or loss.

Figure 10. CSRT answers RE: controlling access to physical facilities



Observations:

Adoption of role-based user access and revocation policies exhibits a general trend that is similar to organizations' security policies; roughly a quarter of the respondents are at each maturity level, with about one-third of the respondents at the Getting Started level.

Advantage of using a cloud provider:

Cloud providers typically maintain strict control over access to important systems, and access is usually restricted by role. Authorizations for access are typically granted by a relatively small set of trusted staff members and tracked using a ticketing/access system. Also, lists of authorized personnel are typically reviewed and updated regularly.

Regular access review audits help ensure that appropriate steps are being taken to manage access. Control of access rights among employees and contractors of the customer organization itself remain the customer's responsibility.

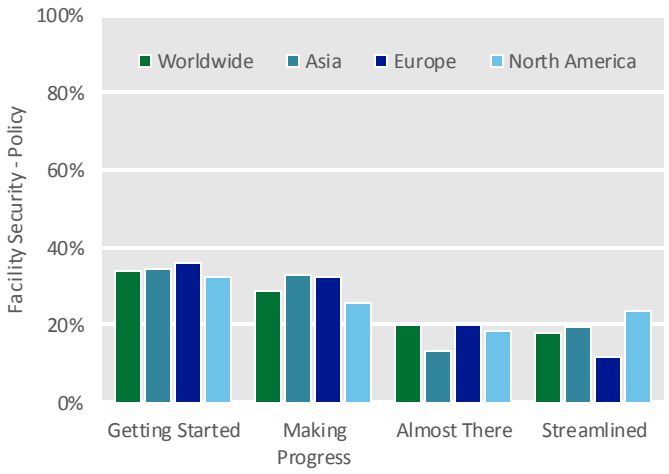
Organizations' physical security access methods (FS-01)

Maintaining physical security is one of the most important steps any organization can take to protect sensitive information assets. Only authorized personnel should have access to data center environments.

Observations:

Sixty-eight percent of organizations worldwide state that there is little managed physical security access in their working environments, with control either at the perimeter (for example, building entry) or through some minimal key-based security access system to more secure locations. Both of these physical security solutions can be security and audit risks because they lack adequate validation, verification, and audit capabilities.

Figure 11. CSRT answers RE: physical access methods



Advantage of using a cloud provider:

Cloud providers typically conduct operations in high-security facilities that are protected by a range of mechanisms that control access to sensitive areas. Providers frequently ensure that common security mechanisms are implemented, such as doors that are secured by biometric or ID badge readers, front desk personnel who are required to positively identify authorized employees and contractors, and policies that require escorts and guest badges for authorized visitors.

Microsoft

Privacy design

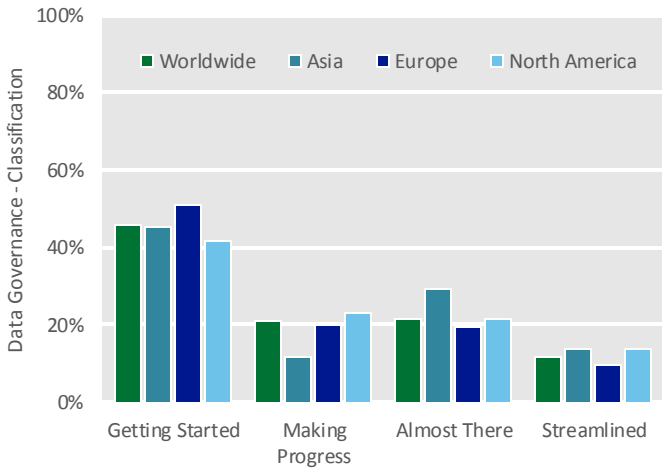
Organizations' data classification efforts (DG-02)

Data classification, which involves associating each data asset with a standard set of attributes, can help an organization identify which assets require special handling to ensure security and privacy protection.

Observations:

Data classification is regarded by 46 percent of worldwide respondents as a mechanism of the local operating system. Classification is typically done on a case-by-case basis, and should be considered a good method of data control and privacy management. Users who attempt to classify data without appropriate guidance will most likely fail to ensure that classified data such as personally identifiable information (PII) is stored, transmitted, or processed with the correct privacy elements in place.

Figure 12. CSRT answers RE: data classification



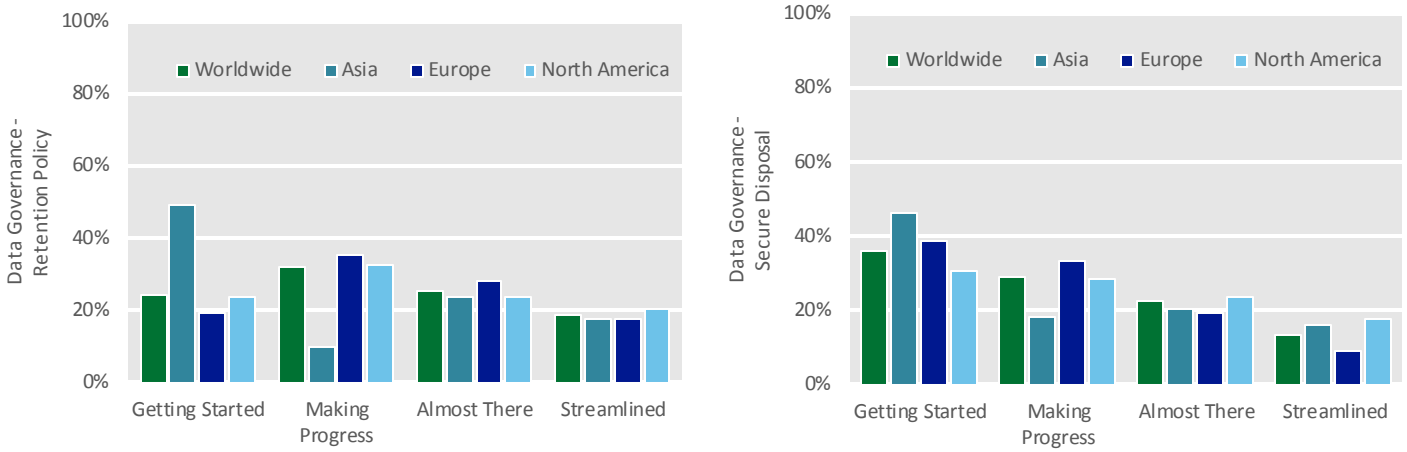
Advantage of using a cloud provider:

Cloud providers typically classify highly sensitive data and other assets according to defined policies that dictate a standard set of security and privacy attributes, among others. In addition, data stores that contain customer data need to be classified as sensitive assets that require advanced security, although customers typically retain responsibility for classifying their own data internally.

Organizations' data retention, recovery, and destruction programs (DG-04, DG-05)

Data backup capabilities should include the ability to restore data on demand as part of an overall backup policy. Comprehensive policies and processes are also needed to govern the proper disposal and destruction of electronic and paper records to help prevent sensitive data from unauthorized disclosure.

Figure 13. CSRT answers RE: data retention and disposal



Observations:

From a worldwide perspective, data retention and disposal efforts are distributed in roughly equal portions among three of the four maturity levels. The exception is Asia, which reported high numbers of organizations with no formal data retention or disposal processes in place. Approximately half of the organizations allow individual employees to be responsible for storing and disposing of data by using local permissions and rights on their computers.

Advantage of using a cloud provider:

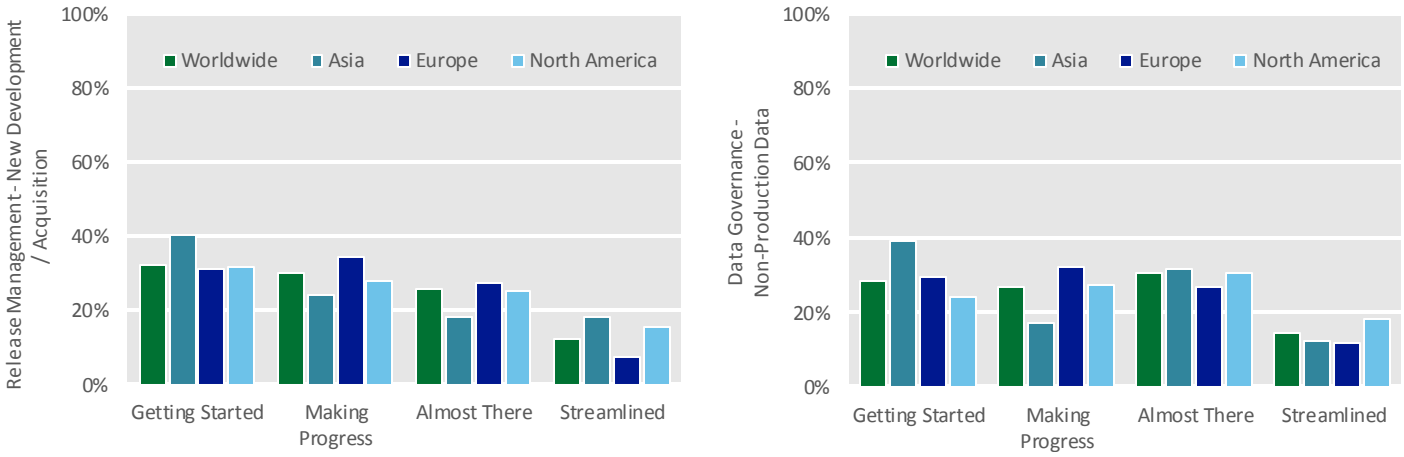
Cloud providers typically maintain a data backup, recovery, and disposal framework that is consistent with industry practices. A typical data backup, recovery, and disposal plan assigns clear responsibilities to specific personnel and defines objectives for backup, recovery, and disposal.

Microsoft

Organizations' procedures for staging data to production and performing application testing using customer data (RM-01, DG-06)

An organization that lacks proper change management procedures creates unnecessary risk when deploying changes to a production environment. Also, it is essential that production data not be used or allowed to leak into non-production environments. If new and modified systems are not adequately tested and validated before deployment, data can be unintentionally lost, altered, or disclosed.

Figure 14. CSRT answers RE: staging data to production and using customer data for testing



Observations:

Sixty-two percent of organizations worldwide are either at the Getting Started or Making Progress maturity level when managing data from staging sites to production sites. Also, 55 percent of those same organizations indicate they are at the Getting Started or Making Progress maturity level with regard to using customer data for testing and development efforts.

Advantage of using a cloud provider:

Cloud providers typically separate production and non-production environments in accordance with widely used technical and industry standards. Cloud providers also use operational change control procedures for system changes, which are communicated to all parties who perform maintenance on the systems. Such procedures consider the following actions:

- Identification and documentation of the planned change
- A process to assess possible impacts of the change
- Change testing in an approved non-production environment
- Change communication plan
- Change management approval process
- Change abort and recovery plan (when applicable)

To ensure that the procedure itself is adequate and effective, management review and approval is typically required. In addition, sufficient notice of potentially disruptive changes is provided with several days' advance notice before any planned maintenance is performed.

Risk management

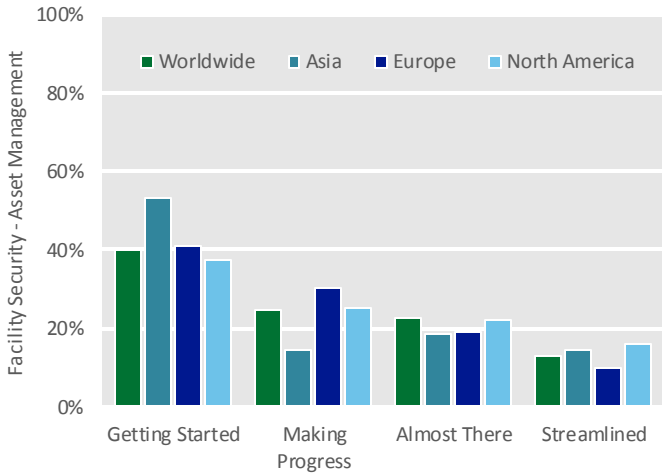
Organizations' asset inventory programs (FS-08)

Asset management makes it possible to keep track of important information about IT assets, including ownership, location, status, and age. A comprehensive asset management program is an important prerequisite for ensuring that facilities and equipment remain secure and operational.

Observations:

Sixty-five percent of worldwide organizations are either at the Getting Started or Making Progress maturity level with an asset management program. This percentage indicates that these organizations either maintain their asset inventories manually or use a policy that only focuses on sensitive assets.

Figure 15. CSRT answers RE: managing asset inventory



Advantage of using a cloud provider:

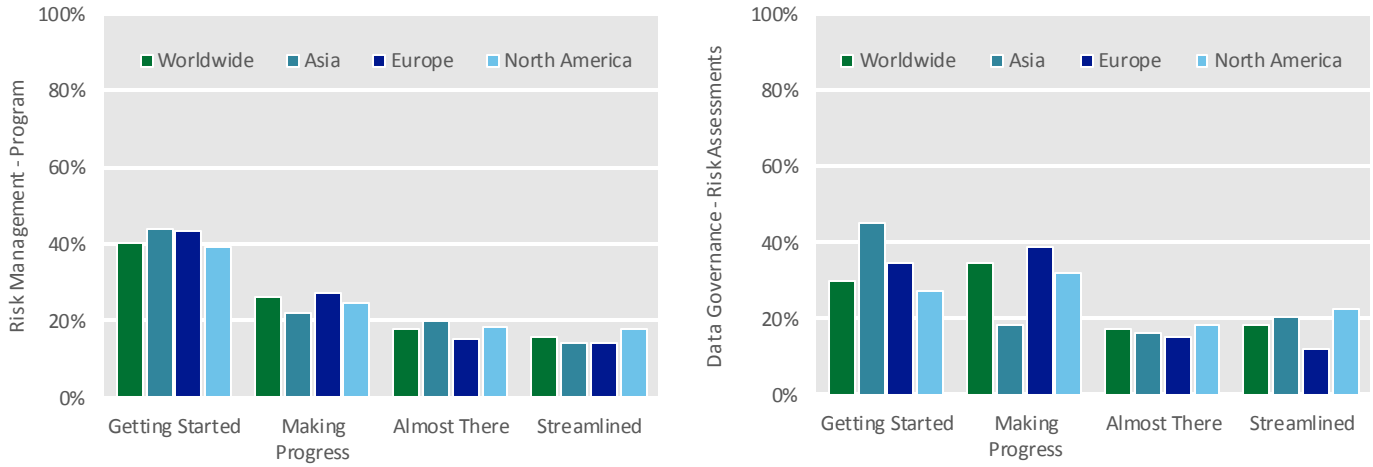
Cloud providers typically use formal asset management policies that require all assets to be accounted for and have designated asset owners. Asset owners are responsible for classifying and protecting their assets and maintaining up-to-date information regarding asset management, location, and security. Cloud providers can also maintain inventories of major hardware assets used in the cloud infrastructure environment and conduct regular audits to verify the inventories.

Microsoft

Organizations' risk assessments and risk management frameworks (DG-08, RI-01)

Organizations of all sizes need to ensure they have in place a documented and repeatable process to conduct information security risk assessments for all IT projects. An information risk management framework needs to be centrally managed and used uniformly throughout the organization to minimize risk to the organization's operational effectiveness. Risk assessments are required by many regulatory and compliance models.

Figure 16. CSRT answers RE: risk assessment and risk management



Observations:

Sixty-five percent of organizations indicated that they have only run risk assessments after a major incident or that they use loosely managed processes. And 70 percent of organizations do not have a basic risk management framework in place to manage risk at acceptable levels.

Advantage of using a cloud provider:

Most cloud providers conduct regular risk assessments that evaluate threats to the confidentiality, integrity, and availability of data and other assets under their control. Cloud providers typically use centrally managed information risk management frameworks built upon versions of the "plan, do, check, act" approach. Also, mitigation plans can minimize the risk from identified threats and help recover business processes if a loss should occur.

Resilience management

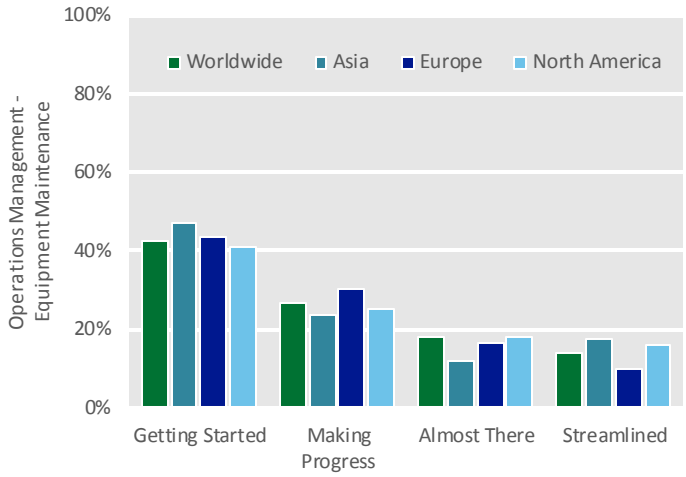
Organizations' equipment support contracts (OP-04)

Keeping equipment such as computers, routers, and other networking devices up-to-date and in working order is essential for ensuring continuity of operations. Without current support contracts, obsolete or inoperative equipment can jeopardize the availability of important systems and information.

Observations:

Worldwide, 42 percent of organizations reported that their efforts to maintain their equipment are conducted on a per-device basis, and that all asset warranty, support, and expiration information is typically tracked on an as-needed basis.

Figure 17. CSRT answers RE: equipment maintenance



Advantage of using a cloud provider:

Cloud providers typically develop and maintain software configuration management (SCM) processes that provide for continuity of operations and ensure ongoing security, compliance, and privacy protections. Also, equipment is refreshed regularly and all systems kept current and operational. Equipment support processes typically involve establishing alternate sites to be used if a failure of the primary service facility occurs.

Microsoft

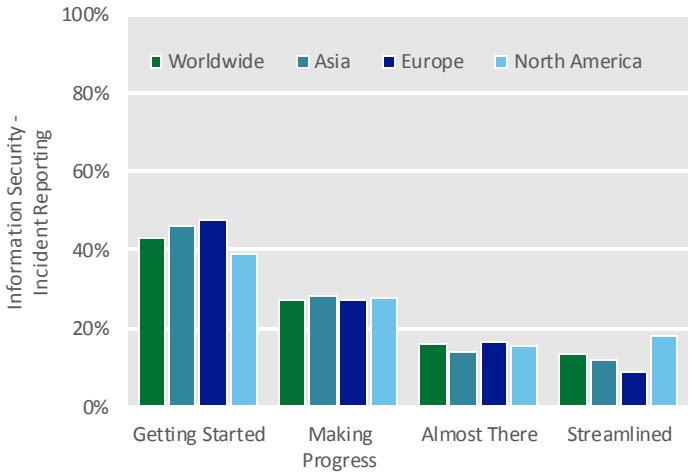
Organizations' incident management programs (IS-23)

When a security incident occurs, proper and timely reporting can mean the difference between containing the damage or suffering a major breach and loss of important information assets. Effective incident response can only occur if information security events are reported to the appropriate parties promptly and clearly.

Observations:

45 percent of organizations worldwide manage incidents such as stolen laptops in an ad hoc manner. Less than 15 percent of organizations worldwide have an incident response program that is in accordance with risk-based policy, processes, and procedures that are regularly updated, tested, and audited.

Figure 18. CSRT answers RE: incident management



Advantage of using a cloud provider:

Most cloud providers require their personnel to report any security incidents, weaknesses, and malfunctions immediately using well-documented and tested procedures.

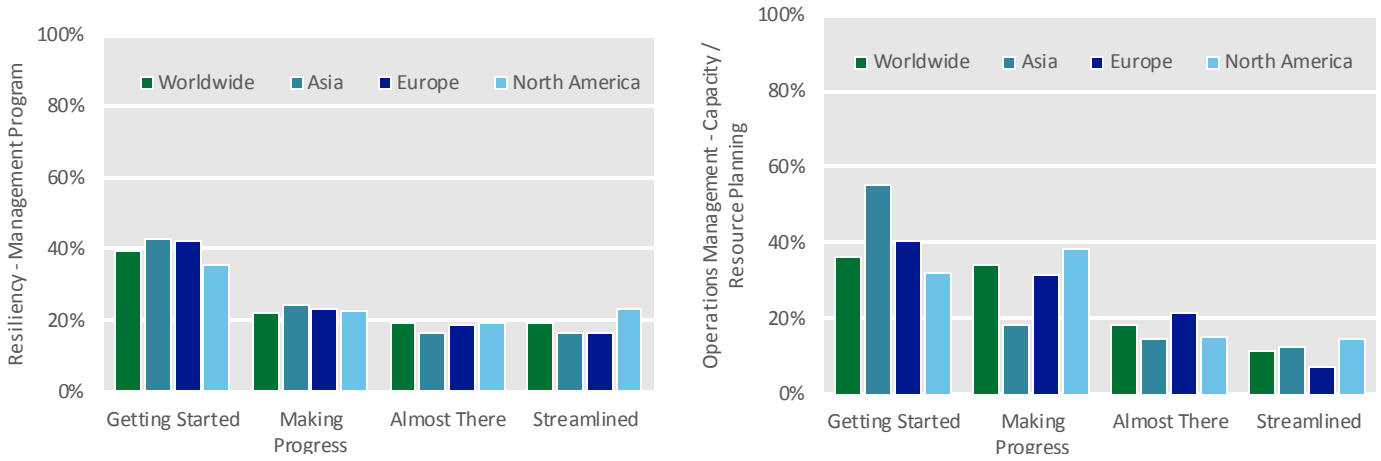
Organizations' disaster recovery plans and capacity planning efforts (RS-01, OP-03)

Effective capacity, resource, and disaster planning are integral to ensuring the availability of information assets in an organization. These efforts attempt to anticipate and prepare for future resource needs to maintain system availability and to provide a means for resuming operations under adverse conditions.

Establishing a formal, approved, and budgeted disaster recovery plan helps ensure the following:

- Assignment of key resource responsibilities
- Notification, escalation, and declaration processes
- Recovery time objectives and recovery point objectives

Figure 19. CSRT answers RE: disaster recovery and capacity planning



Observations:

Resilience management observations show the following trends:

- 38 percent of organizations have stated they are at the Almost There or Streamlined maturity level with regard to creating and implementing a disaster recovery plan.
- 71 percent of these organizations indicated that they have minimal plans in place to adequately support capacity shortages.
- 11 percent of organizations indicated they have formal and regularly reviewed capacity planning efforts in place.

Advantage of using a cloud provider:

Most cloud providers maintain disaster recovery frameworks and processes for governing proactive capacity management that are consistent with industry practices.

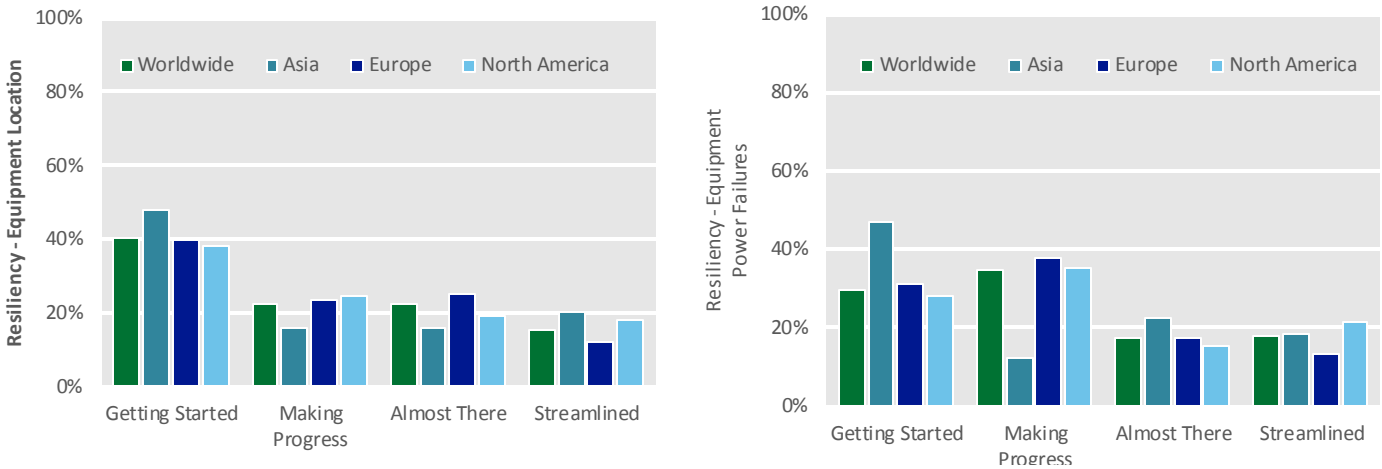
A typical disaster recovery plan assigns clear responsibilities to specific personnel; defines objectives for recovery; delineates standards for notification, escalation, and deceleration; and provides for training all appropriate parties.

Hardware and software subsystem monitoring helps ensure acceptable service performance, CPU utilization, storage utilization, and network latency. A service health dashboard can be used to provide customers and prospective customers with quick web-based access to information about the availability of different cloud resources. Customers typically retain responsibility for monitoring and planning the capacity needs of their own applications and virtual resources.

Organizations' data center locations and their resiliency should utility service outages occur (RS-06, RS-07)

Environmental hazards such as fire, vibration, and weather disasters can threaten systems that store and process important information assets. Whenever possible, these systems should be installed in locations with minimal exposure to such hazards. Also, it is essential that redundant systems be used to provide continuity of operations should disruptions or outages occur. Without redundancy, a data center can become a single point of failure that threatens the ongoing operations of an organization.

Figure 20. CSRT answers RE: data center locations and backup power capabilities



Observations:

Sixty-four percent of organizations worldwide choose their data center locations based on local proximity to the organization's place of business. Thirty percent of these organizations do not have onsite power redundancy and 35 percent only use a generator to ensure power availability if a power failure occurs.

In addition, 50% of Asian respondent organizations have no power failure solutions and select data center locations based on convenience.

Advantage of using a cloud provider:

Cloud providers typically place equipment in environments that have been specifically selected and engineered to protect the equipment from environmental risks such as fire, smoke, water, dust, vibration, earthquakes, and electrical interference.

In addition, most cloud providers have dedicated facility operations centers that monitor power systems and other systems, and that use dedicated 24x7 uninterruptible power supply (UPS) equipment and backup generators.

Power systems include all electrical components, including generators, transfer switches, main switchgear, power management modules, and UPS equipment.

Security architecture

Organizations' patch management, antivirus, and firewall protection efforts (IS-20, IS-21, SA-09)

Malware outbreaks often begin when an attacker successfully exploits a vulnerability in an operating system, application, or browser plug-in on a victim's computer. Most such exploits can be foiled by ensuring that security updates from the affected software vendors are quickly deployed to all computers across the IT environment. Also, using network segmentation and deploying an effective antimalware solution to protect computers will help control malware outbreaks. In addition, all computer systems should be updated on a regular basis.

Observations:

Thirty-nine percent of Asian respondent organizations expect individual users to be responsible for patch management and antimalware protection on their computers. These organizations also rely on their service providers to provide network segmentation, such as firewalls.

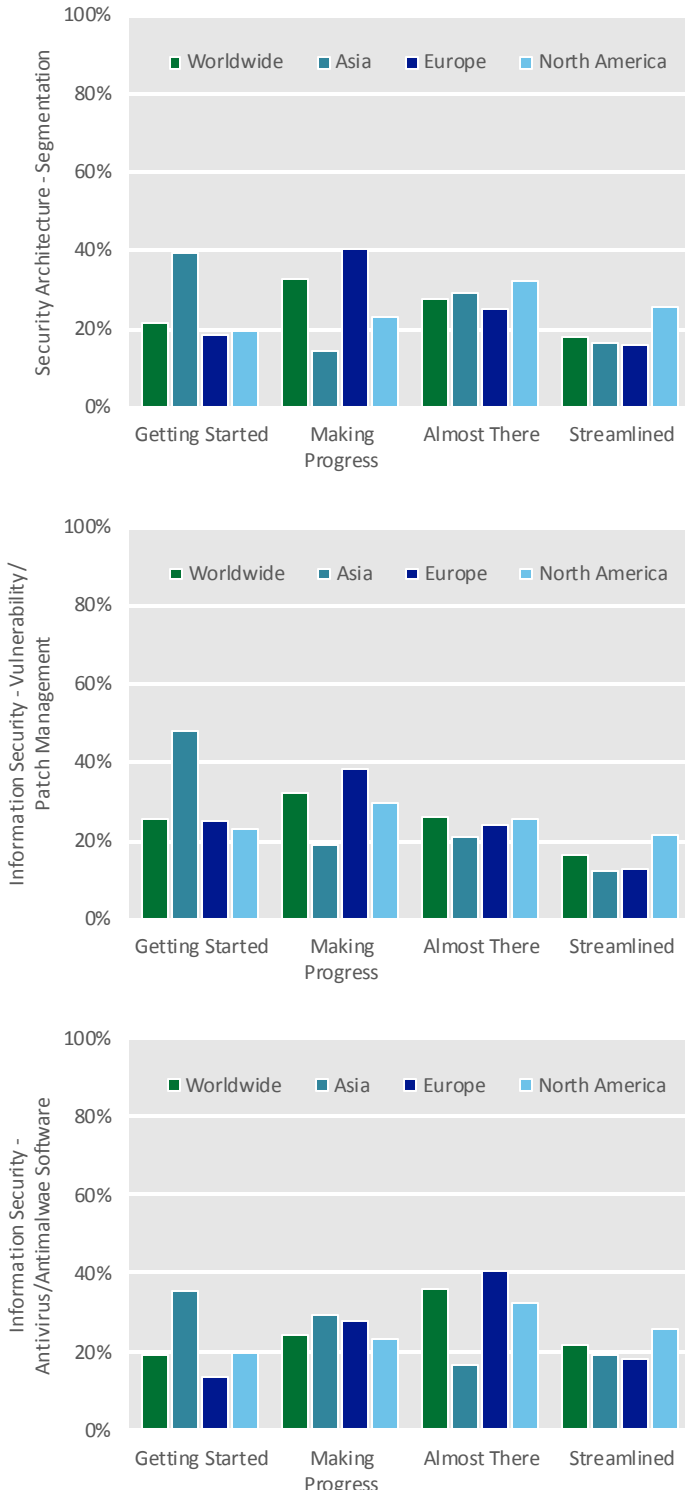
Worldwide, adoption of security solutions indicates better than expected security capabilities. Observations include:

- 68 percent of organizations do not attempt to ensure that patches are configured and installed automatically
- 64 percent of organizations do not run a centrally managed and scheduled antivirus program
- 66 percent of organizations do not make use of a stateful firewall

Advantage of using a cloud provider:

Cloud providers use automated tools and procedures to scan systems for vulnerabilities, along with the latest information available from software vendors and security experts. When vulnerabilities are discovered, mitigations and workarounds are applied to reduce the risk that they pose to systems and data.

Figure 21. CSRT answers RE: security architecture



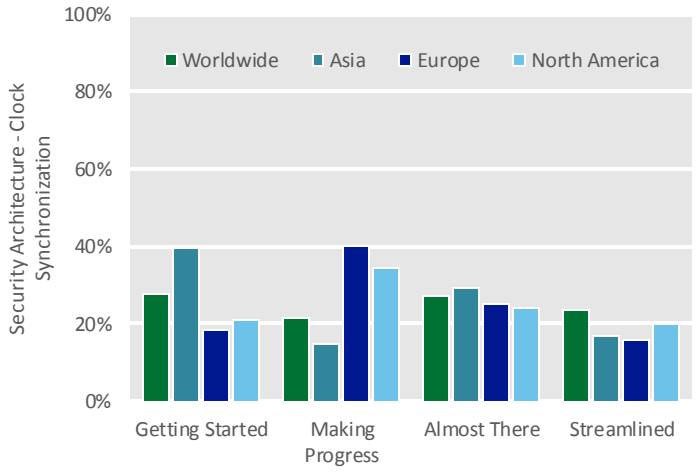
Cloud providers also typically use separate network segments and multiple layers of antivirus software from different vendors to ensure adequate coverage as appropriate. In addition to the real-time protection this approach provides, scheduled scans help ensure that systems remain free from malware.

Effective monitoring is managed using a comprehensive data aggregation solution that can intelligently send alerts when issues are detected.

Organizations' system time setting policies (SA-12)

Precise time synchronization is important for effective investigation of security events that affect multiple computers. Many regulations and best practices require that investigators be able to compare event log timestamps to determine the source of a security incident, such as a breach, or understand how a malware infection spreads to multiple computers. If the system clocks on the affected computers are not synchronized, reconstructing the sequence of events can be difficult or impossible, which can make responding to such incidents much more difficult.

Figure 22. CSRT answers RE: computer clock synchronization



Observations:

Similar to patch management, 43 percent of organizations in Asia and 28 percent worldwide expect users to be responsible for clock synchronization. Worldwide, 79 percent of organizations do not use consistent clock setting standards and approved time sources for their systems; 73 percent of all systems do not use consistent clock setting standards, automatic updating, or use a single, authoritative time source.

Advantage of using a cloud provider:

Typically, cloud providers use Network Time Protocol (NTP) to regularly synchronize system clocks with a central, widely accepted time source to ensure consistent and accurate time synchronization.

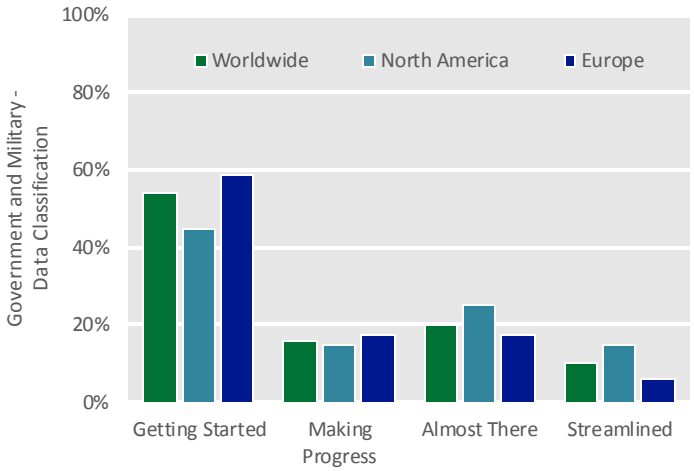
Industry-based trends for government/military organizations

Data governance and classification efforts

Like Cloud Control Matrix (CCM) control DG-09, data classification for governments and military organizations involves associating data assets with a standard set of attributes. Data classification is especially important for agencies and organizations that are responsible for managing sensitive information. Generally, public agencies such as governments and military organizations actively categorize and classify data in an organized, automated fashion.

According to the respondents, an underdeveloped state of understanding exists about data classification in governments and military worldwide. On a worldwide basis, 52 percent of governments and military organizations reported that data classification terminology varies within the organization and is classified as a function of its location (for example, OS File System).

Figure 23. CSRT answers RE: data classification in government and military organizations



Operations management – equipment maintenance and capacity / resource planning

Governments and military organizations have indicated they are making progress with regard to equipment maintenance and capacity planning (OP-04 and FS-08). These controls reflect planning and deployment efforts for load and resilience management. Fifty percent of organizations indicate that no formal capacity planning process exists, but they have some projects that include usage and growth estimation. And 31 percent of organizations have their asset warranty, support, and expiration tracked centrally and reviewed regularly.

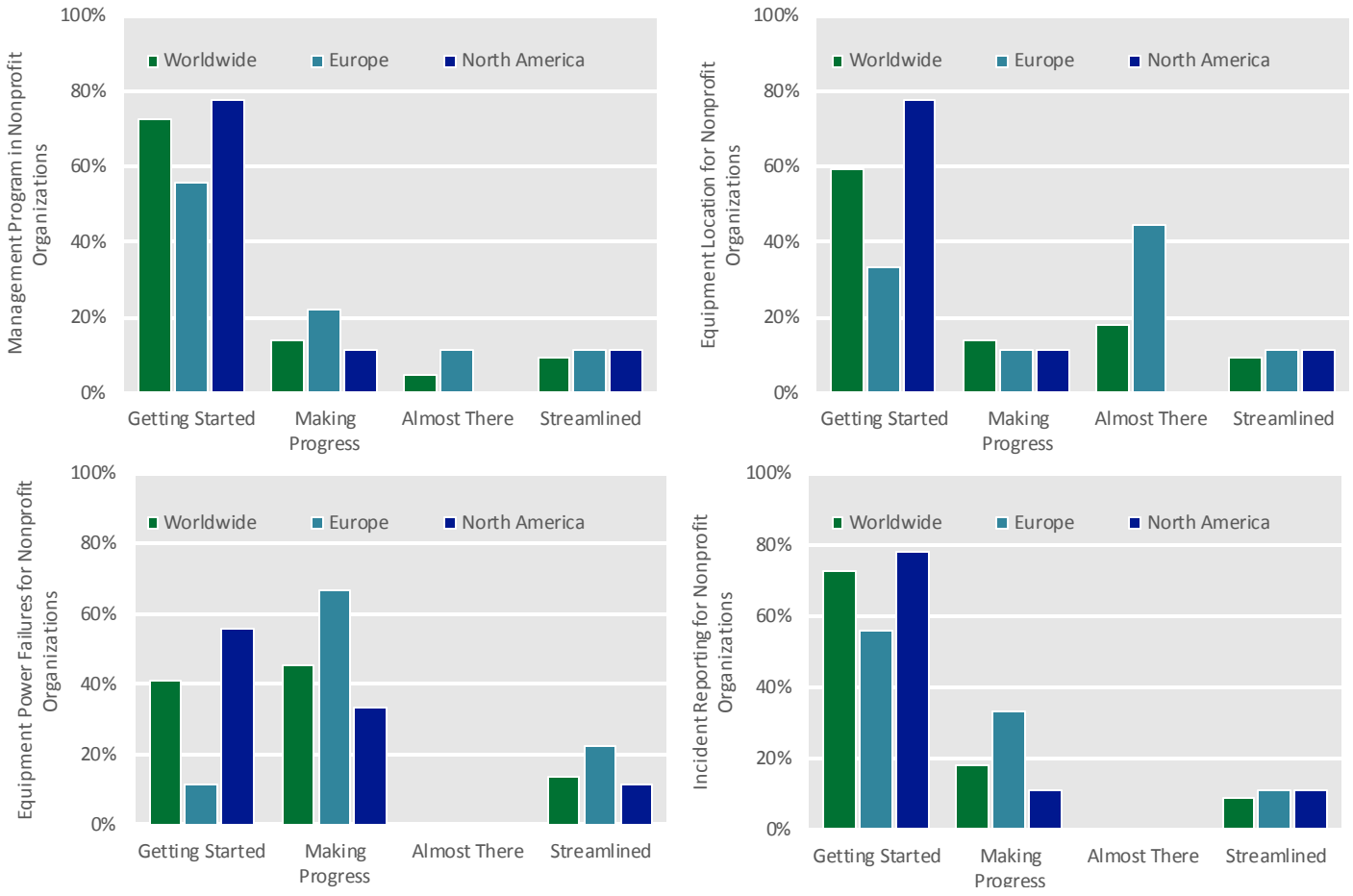
Figure 24. CSRT answers RE: resource planning and equipment maintenance in government and military organizations

Microsoft

Industry-based trends for nonprofit organizations

Nonprofit organizations exhibit a worldwide trend of general immaturity when it comes to resilience management controls RS-01, RS-06, RS-07, and IS-23. This immaturity can be attributed to the high cost of resilience and the operational state of underfunded and highly volunteer-dependent nonprofit organizations.

Figure 25. CSRT answers RE: resilience management in nonprofit organizations



Nonprofit respondents indicated the following:

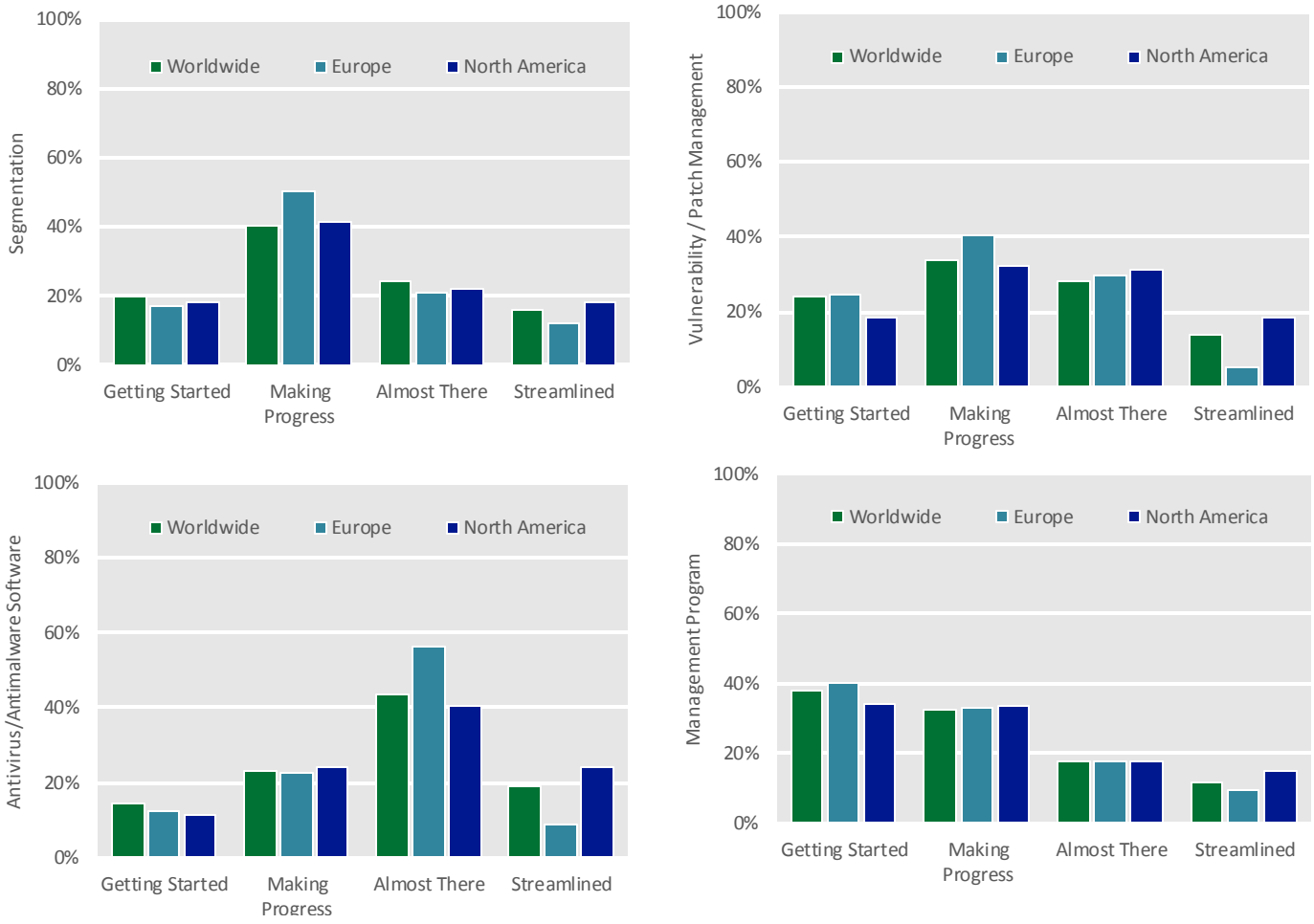
- 73 percent of organizations worldwide have started a disaster recovery plan but no formalized budget has been assigned to implement the program.
- 59 percent of organizations worldwide selected their data center based on local proximity to the organization's place of business.
- 41 percent have no plan in place for redundant power.
- 45 percent have an onsite generator to protect their organization's operations in case of power failure.
- 73 percent of nonprofit organizations worldwide indicated that they respond to incidents in an ad hoc manner, with no formal plans in place.

Organizational trends in small and midsize businesses

When considering physical security as it relates to their security policies, small and midsize businesses with 25-500 PCs (SMBs) worldwide indicated that they are maturing from a very basic state and have not automated their security capabilities entirely. Sixty percent of SMBs have very basic network segmentation (SA-09), or expect their ISP to provide firewall services. Seventy-three percent of SMBs have basic (IS-21) antivirus solutions in place throughout their organizations that are managed by individual employees. Eighty percent of SMBs have (IS-20) patch management capabilities.

However, more than 71 percent of SMBs do not have a formalized information security management program (IS-01). This dichotomy indicates SMBs understand that security technologies are essential to protect their network assets (for example, through the use of firewalls, antivirus programs, and patch management), but that they need to apply more effort toward the development of underlying security standards and policies.

Figure 26. CSRT answers RE: physical security in small and midsize businesses



Microsoft

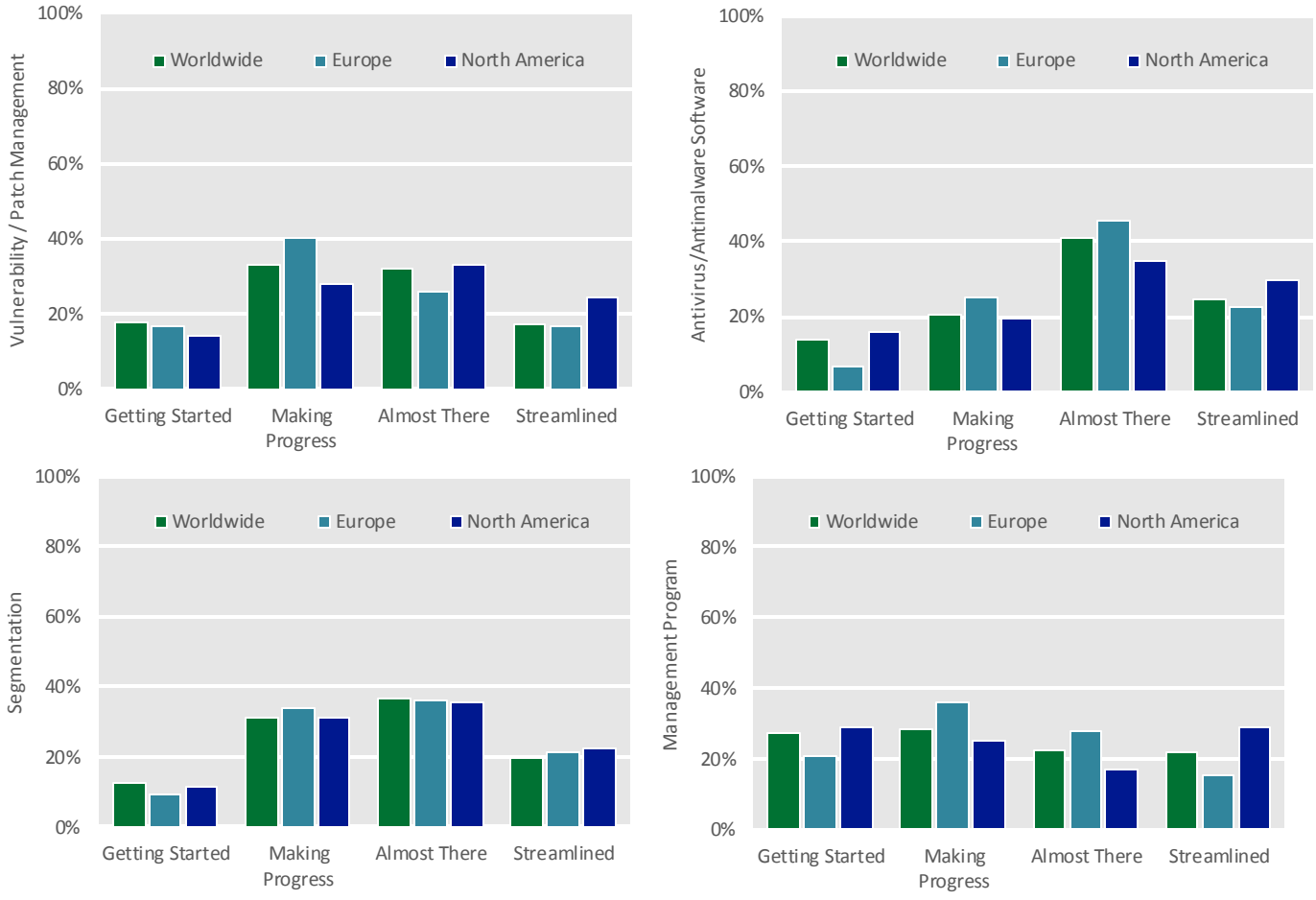
Organizational trends in enterprise organizations

Enterprise organizations (more than 500 PCs) show a solid maturity trend toward physical security adoption. This trend is evident for antimalware, firewalls, and patch management capabilities.

- 66 percent of enterprise organizations have advanced antimalware capabilities
- 49 percent have vulnerability/patch management
- 56 percent have advanced capabilities that include management and auditing of the organization's security policy.

In contrast, enterprise organization security policy distribution data indicates that 55 percent of enterprise organizations have security policies that are not uniform, but that some information security responsibilities have been identified and assigned across the organization.

Figure 27. CSRT answers RE: physical security in enterprise organizations



Conclusion

Considerations about how to benefit from cloud computing must be carefully weighed. These considerations are especially important for harnessing the maximum benefits of cloud computing in earnest, and whether to take advantage of the cloud's rapid deployment and provisioning capabilities or just to reduce costs. There are also benefits to service delivery models as cloud computing becomes more agile and cost effective for organizations that want to optimize time, funds, and resources.

In May 2012, Microsoft released research findings that small and midsize businesses (SMBs) were gaining significant IT security benefits from using the cloud, according to a study in five geographies.[2] Seeing those results, the natural question was: "If the cloud has clear security benefits, what is holding other organizations back?" We found that many of the organizations considering cloud adoption would like simple, well-organized information to help answer where they are in terms of their current IT state and where they will be if they adopt a particular cloud service.

To help the cloud assessment process, Microsoft launched the Cloud Security Readiness Tool (CSRT) (www.microsoft.com/trustedcloud) in October 2012. Organizations can use the CSRT to understand their systems, processes, policies and practices and also to improve their current IT state, learn relevant industry regulations, and receive guidance on evaluating cloud adoption.

With six months of usage data from the CSRT, this report was able to broadly consider the data and compare where organizations are with their current IT states and how they can take advantage of cloud services.

The self-assessment data from organizations around the world indicates that cloud computing has the potential for even greater security value and benefit than had been previously estimated.

[2] The study showed that 35 percent of U.S. companies surveyed had experienced noticeably higher levels of security since moving to the cloud. In addition, 32 percent say they spend less time worrying about the threat of cyberattacks. www.microsoft.com/en-us/news/Press/2012/May12/05-14SMBSecuritySurveyPR.aspx

Microsoft

References for additional reading

Microsoft Trusted Cloud

- *TwC trusted cloud*

Trust Centers

- *Office 365*
- *Windows Azure*
- *Dynamics*

Related Links

- *Microsoft Global Foundation Services*
- *CSA Security, Trust & Assurance Registry (STAR Program)*
- *Microsoft Privacy in the Cloud Site*
- *Microsoft Privacy Information*
- *Trusted Cloud Frequently Asked Questions*

Appendix 1

List of questions used in the Cloud Security Readiness Tool

Question number	Control ID	Control area	Control specification	Question
1	IS-01	Information Security - Management Program	An information security management program (ISMP) has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Which of these statements best describes your organization's security policies and procedures?
2	IS-05	Information Security - Policy Reviews	Management shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy.	Which of these statements best describes your organization's security policies review process?
3	RI-04	Risk Management - Business / Policy Change Impacts	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective.	Which of these statements best describes when your organization's security program is updated?

4	HR-01	Human Resources Security - Background Screening	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors and third parties will be subject to background verification that is proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Which of these statements best describes your organization's personnel background checks?
5	LG-01	Legal - Nondisclosure Agreements	Requirements for nondisclosure or confidentiality agreements that reflect the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Which of these statements best describes your organization's nondisclosure agreement (NDA) requirements?
6	FS-02	Facility Security - User Access by Role	Physical access to information assets and functions by users and support personnel shall be restricted.	Which of these statements best describes how your organization restricts physical access by role?
7	IS-09	Information Security - User Access Revocation	Timely deprovisioning, revocation, or modification of user access to the organization's systems, information assets, and data shall be implemented upon any change in status of employees, contractors, customers, business partners, or third parties. Any change in status is intended to include termination of employment, contract, or agreement, change of employment, or transfer within the organization.	Which of these statements best describes your organization's employee change/termination process?
8	FS-01	Facility Security - Policy	Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.	Which of these statements best describes your organization's physical security access method?
9	OP-04	Operations Management - Equipment Maintenance	Policies and procedures shall be established for equipment maintenance to ensure continuity and availability of operations.	Which of these statements best describes your organization's equipment support contracts?

10	DG-02	Data Governance - Classification	Data and objects that contain data shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization, and third-party obligation for retention and prevention of unauthorized disclosure or misuse.	Which statement best describes your organization's data classification efforts?
11	HR-02	Human Resources Security - Employment Agreements	(v1.0) Prior to granting individuals physical or logical access to facilities, systems, or data, all employees, contractors, third-party users, and customers shall contractually agree and sign the terms and conditions of their employment or service contract, which must explicitly include the individual's responsibility for information security. (v1.1) Prior to granting individuals physical or logical access to facilities, systems, or data, all employees, contractors, third-party users, and tenants and/or customers shall contractually agree and sign equivalent terms and conditions regarding their information security responsibilities.	Which of these statements best describes how your organization grants access to data?
12	DG-04	Data Governance - Retention Policy	(v1.0) Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual, and business requirements. Testing the recovery of disk or tape backups must be implemented at planned intervals. (v1.1) Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual, and business requirements. Testing the recovery of backups must be implemented at planned intervals.	Which of these statements best describes your organization's data retention and recovery program?

13	DG-05	Data Governance - Secure Disposal	Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media to ensure that the data is not recoverable by any computer forensic means.	Which statement best describes how your organization destroys data?
14	RM-01	Release Management - New Development / Acquisition	Policies and procedures shall be established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.	Which of these statements best describes your organization's staging to production requirements?
15	DG-06	Data Governance - Non-Production Data	Production data shall not be replicated or used in non-production environments.	Which of these statements best describes the way your organization performs application testing using customer data?
16	FS-08	Facility Security - Asset Management	A complete inventory of critical assets shall be maintained with ownership defined and documented.	Which of these statements best describes your organization's asset inventory program?
17	DG-08	Data Governance - Risk Assessments	Risk assessments associated with data governance requirements shall be conducted at planned intervals and consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Which of these statements best describes how your organization conducts risk assessments?
18	RI-01	Risk Management - Program	Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level.	Which statement best describes your organization's risk management framework?

19	IS-23	Information Security - Incident Reporting	Contractors, employees, and third-party users shall be made aware of their responsibility to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a prompt and expedient manner in compliance with statutory, regulatory, and contractual requirements.	Which of these statements best describes how your organization responds to an incident such as a stolen laptop?
20	RS-01	Resiliency - Management Program	Policy, processes, and procedures that define business continuity and disaster recovery shall be put in place to minimize the impact of a realized risk event on the organization to an acceptable level and facilitate recovery of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) through a combination of preventive and recovery controls in accordance with regulatory, statutory, contractual, and business requirements and consistent with industry standards. This resiliency management program shall be communicated to all organizational participants on a need-to-know basis prior to adoption and shall also be published, hosted, stored, recorded, and disseminated to multiple facilities that must be accessible in the event of an incident.	Which of these statements best describes your organization's disaster recovery plan?
21	OP-03	Operations Management - Capacity / Resource Planning	The availability, quality, and adequate capacity of resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual, and business requirements. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Which of these statements best describes your organization's capacity planning efforts?

22	RS-06	Resiliency - Equipment Location	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be located away from locations that are subject to a high probability of environmental risks and supplemented by redundant equipment located within a reasonable distance.	Which of these statements best describes how your organization selects its data center location(s)?
23	RS-07	Resiliency - Equipment Power Failures	Security mechanisms and redundancies shall be implemented to protect equipment from utility service outages (for example, power failures, network disruptions, and so on).	Which of these statements best describes your organization's plan for redundancy if utility service outages should occur?
24	IS-20	Information Security - Vulnerability / Patch Management	Policies and procedures shall be established and mechanisms implemented for vulnerability and patch management to ensure that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner. Critical patches shall be analyzed for risk and prioritized accordingly.	Which statement best describes your organization's patch management processes?
25	IS-21	Information Security - Antivirus/Antimalware Software	Ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.	Which of these statements best describes your organization's antivirus efforts?
26	SA-09	Security Architecture - Segmentation	System and network environments are separated by firewalls to address the following needs and requirements: • Business and customer requirements • Security requirements • Compliance with legislative, regulatory, and contractual requirements • Separation of production and non-production environments • Protection and isolation of sensitive data	Which of these statements best describes how your organization uses firewalls to protect data?

27	SA-12	Security Architecture - Clock Synchronization	An external, accurate, externally agreed upon time source shall be used to synchronize the system clocks of all relevant information processing systems within the organization or explicitly defined security domain to facilitate tracing and reconstitution of activity timelines. **Note**: Specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the organization's domicile time reference. If so, the jurisdiction or platform is treated as an explicitly defined security domain.	Which of these statements best describes your organization's system time setting policies?