State of Network Security 2014

An AlgoSec Survey

algosec Managing Security at the Speed of Business

SHARE THIS RESEARCH:

Executive Summary

A survey of 142 information security and network operations professionals and application owners finds that current security management processes make balancing access to the rapidly rising number of business critical applications and reducing system vulnerability increasingly challenging.

- **The need to "fly blind" through convoluted processes continues to hamper business agility and threaten productivity.** Nearly two-thirds of respondents reported that manual processes, limited visibility into security policies and poor change management practices posed the greatest challenge to effective management of network security devices. The inevitable mistakes that arise in this environment have real consequences for a growing number of organizations: more than 80% experienced network or application outages as a result of out-of-process changes, up from just over half in 2012.

- **Internal communication also poses challenges.** Nearly one in five respondents said that aligning priorities and plans between development, security and operations teams created their greatest obstacle, more than double the number citing this problem last year.

- **Business stakeholders should own the risk of their applications**. Three out of five respondents state that their data center includes more than 50 critical business applications and one in five have responsibility for more than 500. With all those applications, the majority of organizations say they struggle to identify vulnerabilities and understand them in the context of the business. Consequently, virtually all the respondents said that business stakeholders should manage the risks of their own applications.

About the Survey

The "State of Network Security 2014" survey was conducted to determine the key risks in organizations' security management practices and access to critical applications in the data center.

142 information security, network operations and application owners completed the survey, conducted in February 2014 at the RSA Conference in San Francisco, CA. Of those respondents, 34% primarily had responsibility for information security, 23% were in network operations, 25% were application owners or developers, and 18% were in risk management or compliance roles.

Respondents represented businesses of all sizes: 32% of respondents worked for businesses with 1-100 employees, 17% for mid-sized organizations of 101-1000 employees, and 51% for enterprises of more than 1000 employees.

- **Insiders pose the greatest risk, but third party security raises significant concerns.** Nearly three-quarters of organizations rated accidental data leakage or malicious behavior by insiders as their number one risk, up from less than two-thirds last year. Half of respondents who outsource management of security controls or sensitive information were less than confident in their provider's ability to provide protection.

- **Pace of cloud adoption picks up, despite concerns about connectivity and security.** Last year one in five organizations expected to move more than 40% of their business applications to the cloud; this year more than 15% already use cloud hosting for the majority of their applications. While the advantages have three-quarters of organizations using cloud hosting to some degree, three out of five still worry about ensuring application availability and security with off-site data centers.

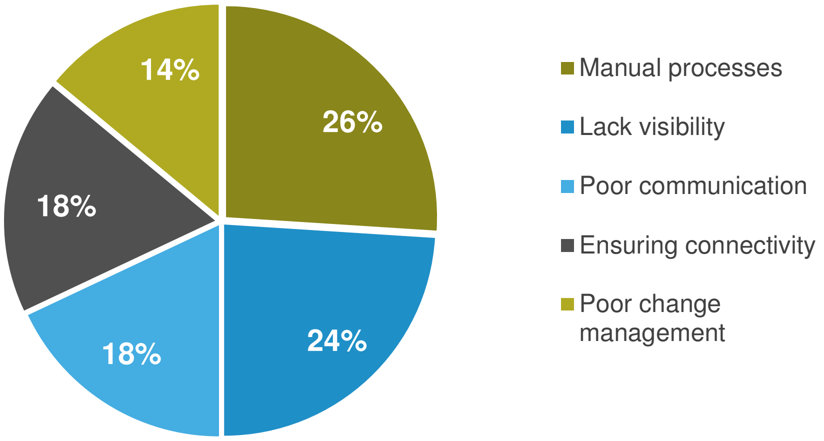
SHARE THIS RESEARCH:

The complex rules and manual processes involved in change management imperil many organizations' ability to ensure system security and stability in an environment with dozens or hundreds of often interconnected business critical applications. The proliferation of applications has made understanding their associated business risk more challenging for information professionals and led to a nearly universal desire to involve application owners more deeply in prioritizing IT risk. At the same time, the increased use of cloud hosting and third-party vendors to manage all those applications have elevated concerns about security breaches and application connectivity. In this environment, the majority of organizations have embraced next-generation firewalls to increase security and control applications.

Manual Processes Plague Security Management

Most organizations (64%) remain hampered by time-consuming manual processes, obscured security policies and poor change management practices (Figure 1). Communication issues rose in importance this year, with 18% saying that aligning the development, security and operations groups was their number one challenge, up from about 9% in 2012 and 2013.

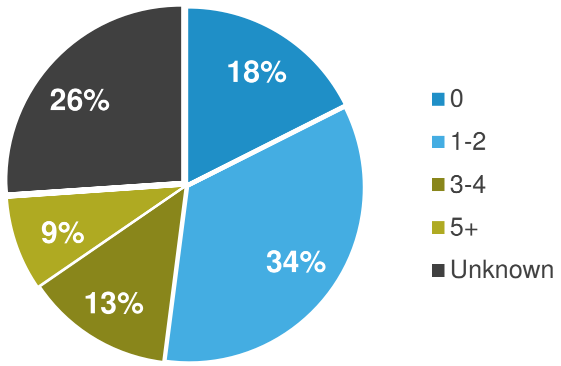
Figure 1: Greatest challenge in managing network security



Almost one in five organizations (18%), report that the details of ensuring business application connectivity posed the greatest challenge in network security management, a nearly 50% increase over the number in 2013. Enabling that connectivity drove more than 40% of all firewall rule changes for the majority of organizations (56%) and accounted for more than 60% of rule changes for nearly two out of five (37%) organizations.

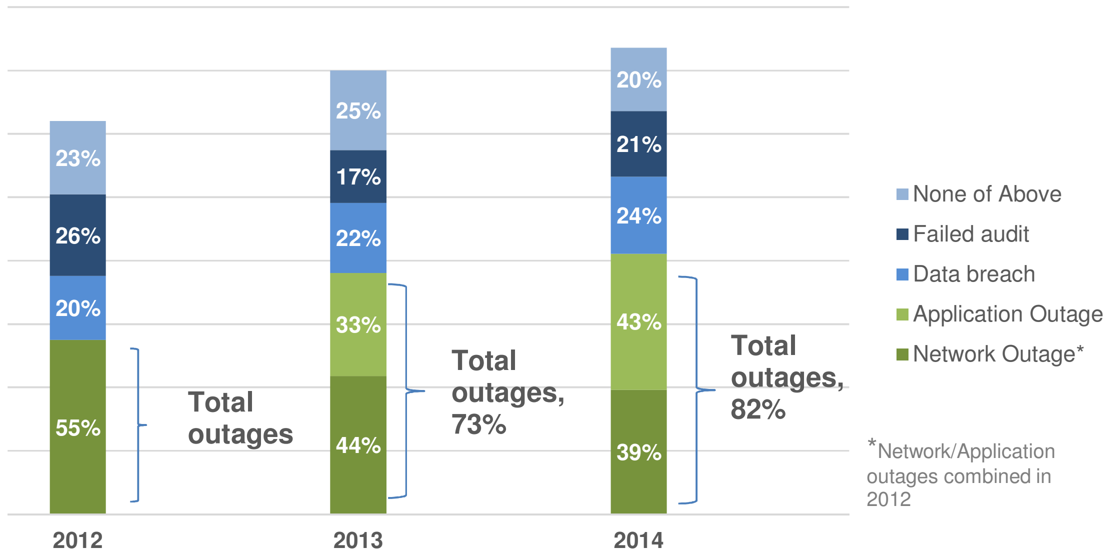
Manually making all those changes without a clear view of the affected security policies puts organizations at elevated risk of outages. The majority of respondents (56%) reported they suffered one or more outages in the last year as a result of security infrastructure misconfiguration and almost one-quarter (22%) said misconfiguration caused three or more data center application outages. Notably, 26% did not know how many outages they experienced, perhaps because their systems lacked centralized reporting functionality (Figure 2).

Figure 2: Outages caused by misconfigured security infrastructure in last year



Out-of-process changes to support business agility further increase the risk of outages. In the last year, the number of organizations reporting application errors as a result of unscheduled changes rose 30%. Network and application outages, experienced by 82% of organizations, occurred nearly four times more often than failed audits and almost 350% as often as data breaches (Figure 3).

Figure 3: Consequences of out-of-process changes



*Network/Application outages combined in 2012

SHARE THIS RESEARCH:

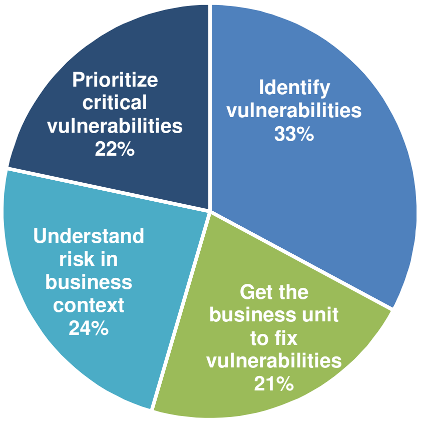
Who Should "Own the Risk"? Business Stakeholders.

The number of business applications managed in data centers continues to rise rapidly. Today, 60% of organizations manage more than 50 business applications in their data center, up from 50% last year. At the high end, the change is more dramatic, with 20% of organizations now managing more than 500 applications and 15% having responsibility for more than 1000 applications. In 2013, less than 19% of respondents reported they had more than 200 applications in the data center.

All those applications have made it harder for organizations to stay on top of vulnerabilities—and eager to involve business stakeholders in risk management.

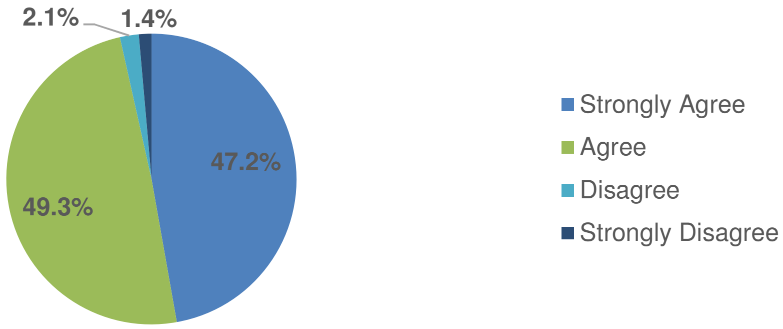
Almost half of organizations (45%) said their biggest challenges are understanding the business context or getting the business unit to fix vulnerabilities. Slightly more than half stated that identifying and prioritizing vulnerabilites are their biggest issues (Figure 4).

Figure 4: Greatest challenge in vulnerability management



With the need for greater business unit involvement to understand and address vulnerabilities, it's little surprise that nearly all respondents thought business stakeholders should "own the risk" of their applications. In fact, only five respondents disagreed—and three of them were application owners (Figure 5).

Figure 5: Business stakeholders should own the risk of applications

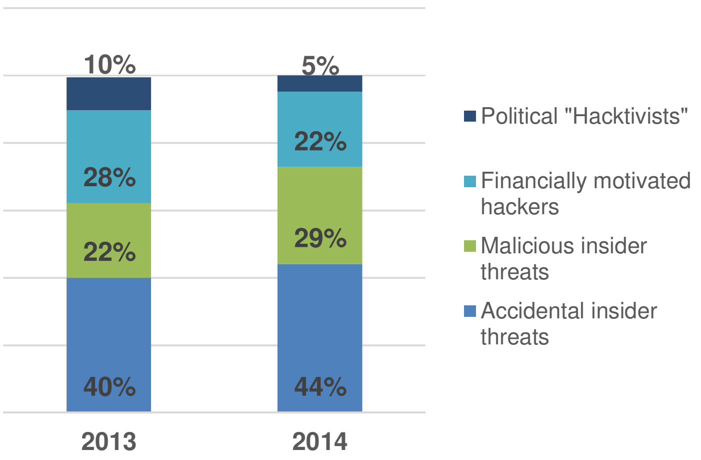


SHARE THIS RESEARCH:

Security Risks Rise on Two Fronts

In 2013, 62% of organizations considered insider threats—both accidental data leakage by employees and malicious breaches—to be their greatest risk. This year, 73% said insiders were their top concern, perhaps driven by the significant press attention to the Edward Snowden revelations and related security concerns. At the same time, the percentage of respondents worried about financially motivated hackers dropped from 28% to 22% (Figure 6).

Figure 6: Greatest area of risk

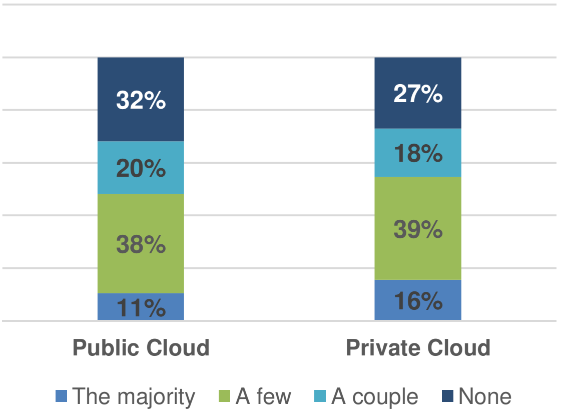


Organizations still don't rest easy about attacks from outside, however, as many lacked confidence in the security of third-party vendors. These concerns may have been heightened this year as a result recent and well publicized breaches, the largest of which originated through vulnerabilities around third-party vendor access. Of those whose organizations outsourced management of any security controls or sensitive information, just 12% said they were "very confident" of the provider's ability to ensure the highest level of protection. Half said they were either "not confident" or only "somewhat confident."

Cloud Migration Picks Up

In a previous survey on the Impact of Security Management on the Business, just 5% of respondents expected to migrate business applications to public clouds. In a dramatic upswing, this survey shows that more than two-thirds have already migrated some applications to a public cloud—and 11% have migrated the majority of their applications to a public cloud already. At the same time, 73% of respondents have migrated some applications to a private cloud and 16% have moved the majority of their business applications to a private cloud (Figure 7).

Figure 7: Percentage of business applications hosted in a cloud

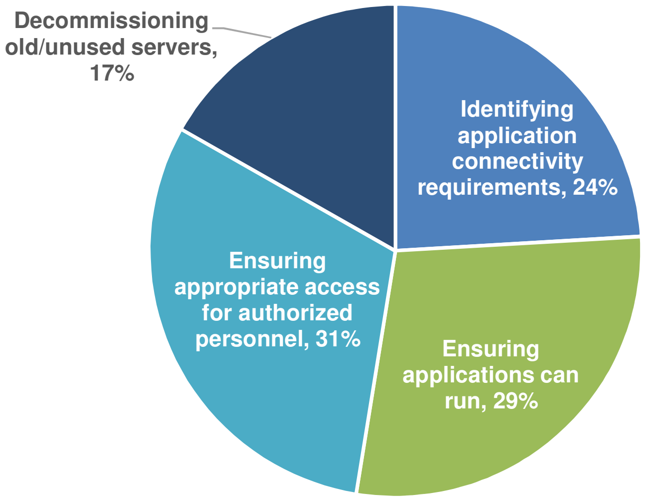


SHARE THIS RESEARCH:

While adoption rates have risen markedly, cloud hosting still raises security concerns for respondents. For 37%, maintaining security remained the greatest challenge associated with migration. One in five worried about ensuring application availability. Overall, just 16% had no concerns with migration.

When consolidating data centers, more than half (53%) expressed concern with application connectivity, with 29% focused on ensuring applications can run and 24% saying that identifying application connectivity requirements was their leading concern. Another 31% rated ensuring appropriate access for authorized personnel as their top challenge (Figure 8).

Figure 8: Greatest security challenge when consolidating data centers

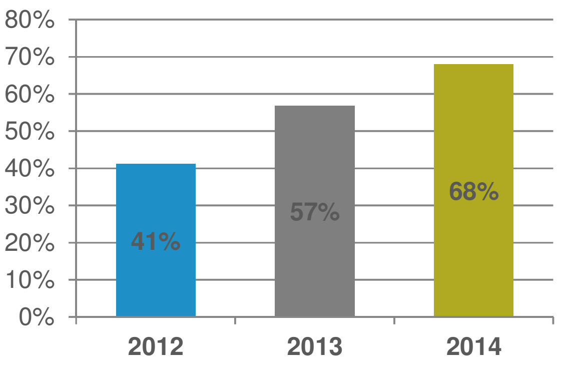


Next-Generation Firewalls Now Dominate

More than two-thirds of organizations have now implemented next-generation firewalls (NGFW), up from just over 40% two years ago (Figure 9). Organizations most commonly used the intrusion protection systems, application control, URL filtering and advanced malware detection features of next-generation firewalls.

The majority of respondents reported that improved protection from attacks drove NGFW adoption, but the desire to reduce IT expenditures also played an important

Figure 9: Adoption of next-generation firewalls



SHARE THIS RESEARCH:

role and 29% of organizations upgraded their firewall to enable “bring-your-own-device” initiatives. With increased adoption has come greater awareness of the challenges associated with defining NGFW policies, which nearly a third of those surveyed (31.2%) said was now their main challenge, up from just 6% last year. The number of respondents reporting that training employees posed the greatest challenge rose 8 points, from 16% to 24% in the last year.

Conclusions

As seen in previous surveys, lack of visibility, time-consuming manual processes, and poor change management practices continue to create significant challenges for IT security and network operation teams as well as application owners. With no easy way to make changes or a clear path to determine their impact on other applications, organizations face a substantial risk of outages. With data centers now often stocked with hundreds to even thousands of applications, the need for frequent out-of-process changes further compounds the problem.

The rapidly accelerating growth in business critical applications is transforming the landscape for organizations as IT teams recognize their need to work closely with business units to identify and remedy application vulnerabilities and with third parties to host those applications or manage data. Organizations readily recognize that involving more people inside and outside the organization in security management increases their level of IT risk, but the sheer number of applications in modern data centers makes distribution of responsibility unavoidable. Aligning priorities and improving communication among IT development, security and operations teams has also become more challenging as the number of applications has grown.

With increased adoption of NGFWs, organizations should focus efforts on automating more security management processes and improving visibility and understanding of policies. These changes will ultimately enable them to more quickly respond to dynamic business imperatives.

algosec

About AlgoSec

AlgoSec is the market leader for security policy management, enabling organizations to simplify and automate security operations in evolving data centers and networks. More than 1000 of the world's leading organizations, including 15 of the Fortune 50, rely on AlgoSec for faster security provisioning of business applications, streamlined change management, continuous compliance and tighter security.

AlgoSec's application-centric approach orchestrates the management of complex policies across firewalls and related network devices, aligning IT teams for improved business agility.

AlgoSec is committed to the success of every single customer, and offers the industry's only money-back guarantee. For more information, visit www.AlgoSec.com.

SHARE THIS RESEARCH:

265 Franklin Street
Boston, MA 02110
USA

T: +1-888-358-3696
F: +1-866-673-7873
E: info@algosec.com

AlgoSec.com