2012 State of the Endpoint

Executive Summary

Independently conducted by Ponemon Institute LLC
Sponsored by Lumension

November 2011

WP-EN-11-10-11

Introduction

The *2012 State of the Endpoint* study sponsored by Lumension® and conducted by Ponemon Institute is the third annual study to determine how effective organizations are in the protection of their endpoints and what they perceive are the biggest obstacles to reducing risk.

At the highest level, respondents report increasing endpoint insecurity year over year since 2009. This year, 66 percent reported their networks are not more secure than a year ago; 64 percent reported they were not more secure in 2010 compared to the year prior and 59 percent reported they were not more secure in 2009.

Malware attacks continue to be a significant risk and operational cost driver for respondents – with more than 50 malware incidents occurring per month within their organizations. However, today's IT security teams are more concerned about threats brought on by their organization's increasing reliance on personal mobile devices, virtualization technologies and cloud computing. While IT's focus on the enablement of business productivity is a mind shift expected by other business leaders, inadequate collaboration and lacking resources for security create a perfect storm for hackers to capitalize on.

Overall, the research reveals that risks to the endpoint environment are growing in scope - no longer is endpoint security about securing a few laptops. It is also apparent to an increasing number of administrators that traditional defenses no longer work and investment in new approaches like application whitelisting are planned in the next 12 months.

Respondents perceive their environment's greatest risks for 2012 as third-party applications, remote employees/mobile devices, cloud computing and removable media. It is interesting to note that areas of increased investment in security in 2012 do not precisely match the areas identified as increasing IT risk.

In this study, IT also reports dissatisfaction with other business leaders' prioritization of security. To implement change effectively, attention must be given to people, process and technology. Survey respondents indicate a need for stronger collaboration with IT operations and other business executives. Only 12 percent of respondents in this study say collaboration between IT operations and IT security is excellent and 40 percent say collaboration is poor or non-existent.

The 688 respondents in this year's *State of the Endpoint* study are deeply involved in their organization's IT function and have at least a moderate involvement in endpoint security. Sixty-five percent are at the supervisor level or higher. Seventy-six percent report directly to the chief information officer (CIO) or chief information security officer (CISO).

Key Findings

The study focused on four topics on the state of endpoint security: risk, productivity, resources and complexity. The findings are presented in this section.

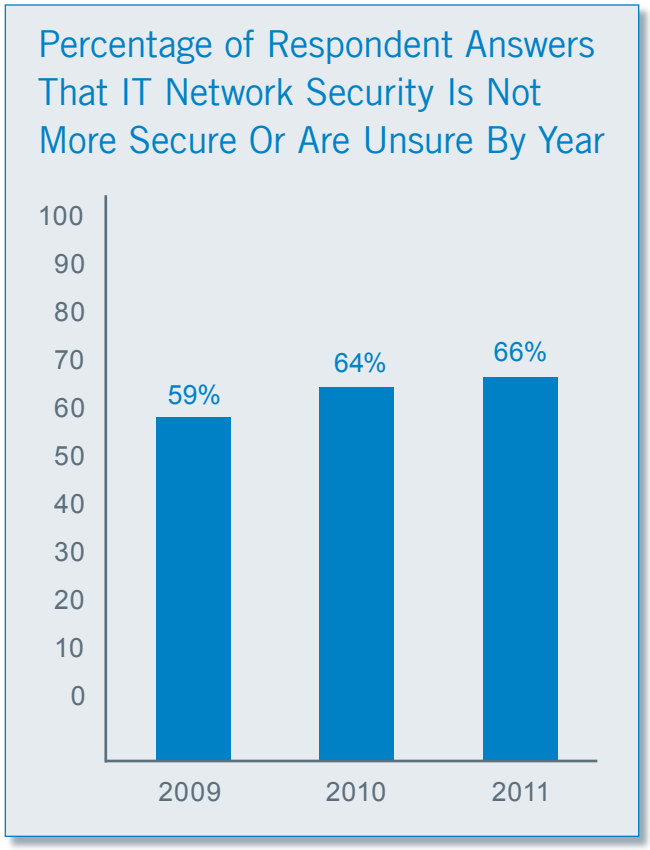
The first part of the study asked respondents their perceptions about the current state of endpoint security within their organizations. In general, the pattern of agree and disagree responses summarized for three attributions about endpoint security suggests many respondents are concerned about support from line of business executives, available IT resources and security risks from mobile data-bearing devices.

Less than half (41 percent of respondents) of respondents agree that non-IT executives are supportive of their organizations' endpoint security operations. Fewer respondents (35 percent) agree they have ample resources to minimize IT endpoint risk throughout their organizations and only 26 percent agree that laptops and other mobile data-bearing devices are secure and do not present a significant security risk their organizations' networks or enterprise systems.

IT's growing insecurity. In this and previous studies, there has been no real improvement in IT network security. As described above, 66 percent say that IT network security is not more secure or are unsure. In 2010, 64 percent said this was the case and in 2009 it was 59 percent.

Malware incidents persist but are no longer the primary concern for IT. According to respondents, on average malware incidents have nearly doubled from 27 percent in 2010 to 43 percent in 2011 with 31 percent reporting they have significantly increased in frequency, specifically when it comes to Web-born malware attack. On average, respondents say they are seeing more than 50 malware attempts per month within their organizations.

The concern of growing malware has decreased significantly from 61 percent in 2010 to 29 percent in 2011. The increased use of mobile platforms, insufficient budget/resources and insecure cloud computing resources are now more of a worry.



Greatest growth in areas of perceived IT security risks for 2012 are vulnerabilities among third-party applications, mobile devices and removable media. Vulnerabilities in third-party applications is ranked as the highest potential security risk in the IT environment by 56 percent of respondents and represents an increase from 45 percent of respondents in last year's study. Mobile/remote employees are the second greatest risk. The risk posed by mobile devices such as smart phones increased dramatically from 9 percent to 48 percent.

Vulnerability assessment continues to be considered the most effective in meeting their organizations' IT risk mitigation requirements according to 55 percent of respondents in this year's study versus 70 percent in the 2010 study. The second and third most effective technologies are device control and endpoint firewall respectively.

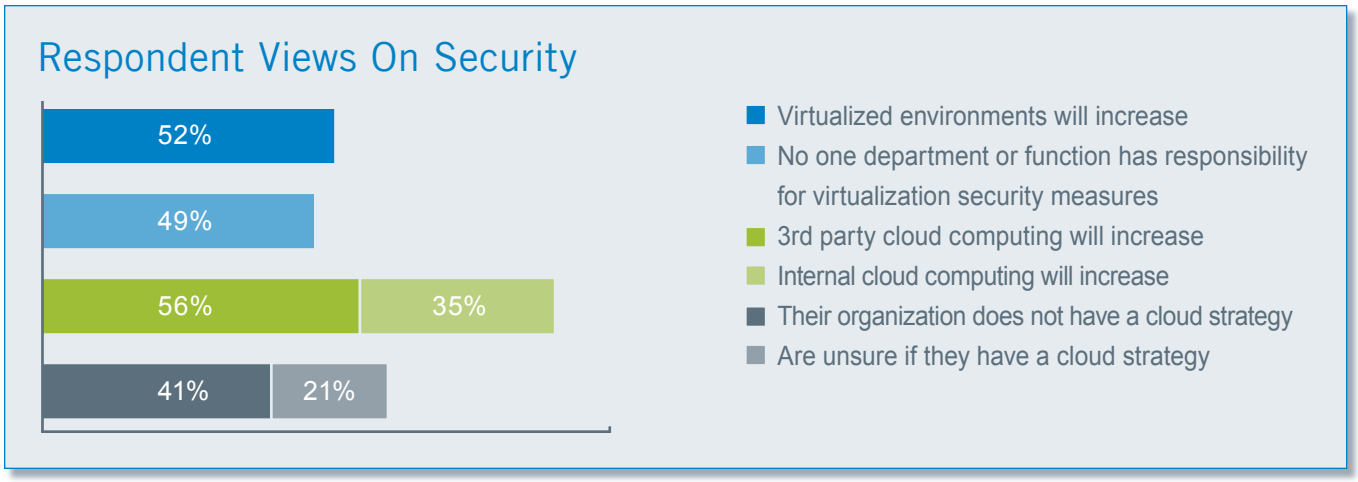
Despite rating third party application risk the top concern for 2012, only 23 percent rate patch and remediation management as a "top five" risk mitigation approach. While all organizations in the study use anti-virus/malware technology, less than half (40 percent) of respondents say it is one of the top five most effective technologies. This is a decline from 57 percent reported in last year's study. Sixty-three percent of respondents say they are certain or likely to pilot or expand their use of application control/whitelisting technologies within the endpoint environment sometime within the next 12 months.

Trust in using the Apple Mac is declining. Forty-one percent are very concerned about Mac malware infections and 44 percent are increasingly concerned.

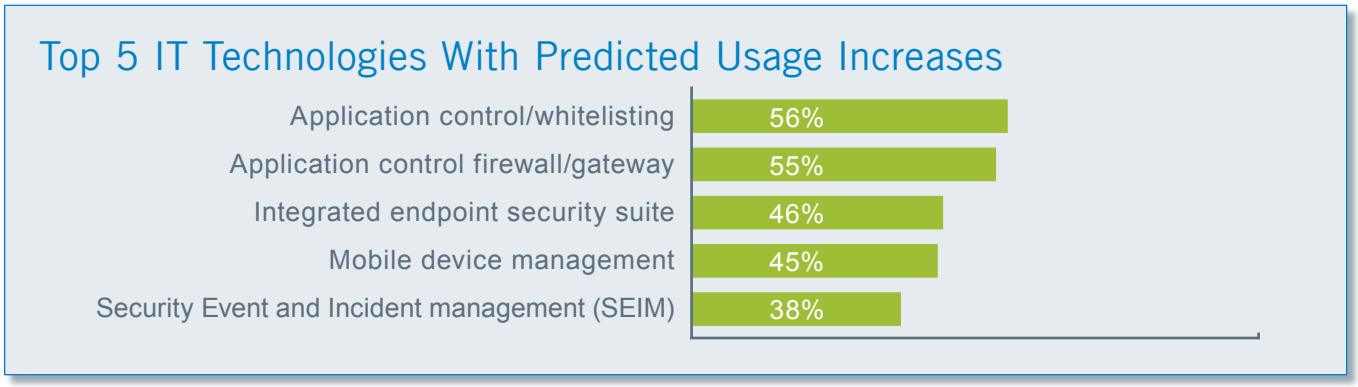
Technologies tied to organizations' productivity are increasing. Social media/Web 2.0, mobile devices/smart phones and use of third-party cloud computing infrastructure are the technologies that are expected to increase substantially in use. On average, 42 percent of employees in respondents' organizations use their personal mobile devices in the workplace. However, 42 percent say that their organization does not have an effort in place to secure them. Forty-six percent say they secure them in a manner similar to that already in place for corporate devices.

The technologies expected to increase most in both use and investment are application control/whitelisting and application control firewall. While respondents identified mobile devices and removable media as increasing IT risk in their organizations, less than half of respondents (46 percent) say investment in mobile device management will increase and only 20 percent say device control will increase. While more than half (56 percent) say their organizations' IT security budget for 2012 will stay the same, 25 percent say it will increase.

Strategies to manage risk are lacking. More than half (52 percent) of respondents say virtualized environments will increase in the next 12 to 24 months. However, 49 percent say no one department or function has responsibility for virtualization security measures. Further, 56 percent say third party cloud computing infrastructures will increase as well as internal cloud computing, according to 35 percent of respondents but 41 percent of respondents say their organization does not have a cloud strategy and another 21 percent are unsure.



Given the impact of new risks associated with remote workers, social media, mobile platforms and cloud computing, organizations are now looking to implement a more robust mix of effective solutions to tackle these mounting endpoint risks. According to those polled, the top five technologies that IT plans to increase usage over the next 12 months are:



Continued »

Implications

The findings of this study reveal the enormous challenges IT practitioners face when trying to improve the security posture of their organizations. Respondents in this study understand how a lack of support from non-IT executives, insufficient resources and the pervasive use of laptops and other mobile data-bearing devices are putting their organizations at risk. However, very often no one function is accountable or in charge of mitigating the risk and collaboration with other executives is often poor.

To better address the difficulties in managing the endpoint risk, collaboration between IT operations and IT security should be improved. As mentioned above, 48 percent say collaboration could be improved and 40 percent say existing collaboration between the two groups is poor or non-existent. Working together might result in a better allocation of resources and the creation of strategies to address risks associated with virtualization, cloud computing, social media and mobile devices.

About Ponemon Institute

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and Risk Management 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 Florida, Texas, Luxembourg, the United Kingdom, Germany, Ireland, Spain, France, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension, Lumension Patch and Remediation, Lumension Vulnerability Management Solution, "IT Secured. Success Optimized.", and the Lumension logo are trademarks or registered trademarks of Lumension Security, Inc. All other trademarks are the property of their respective owners.

Global Headquarters
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.888.725.7828
fax: +1.480.970.6323