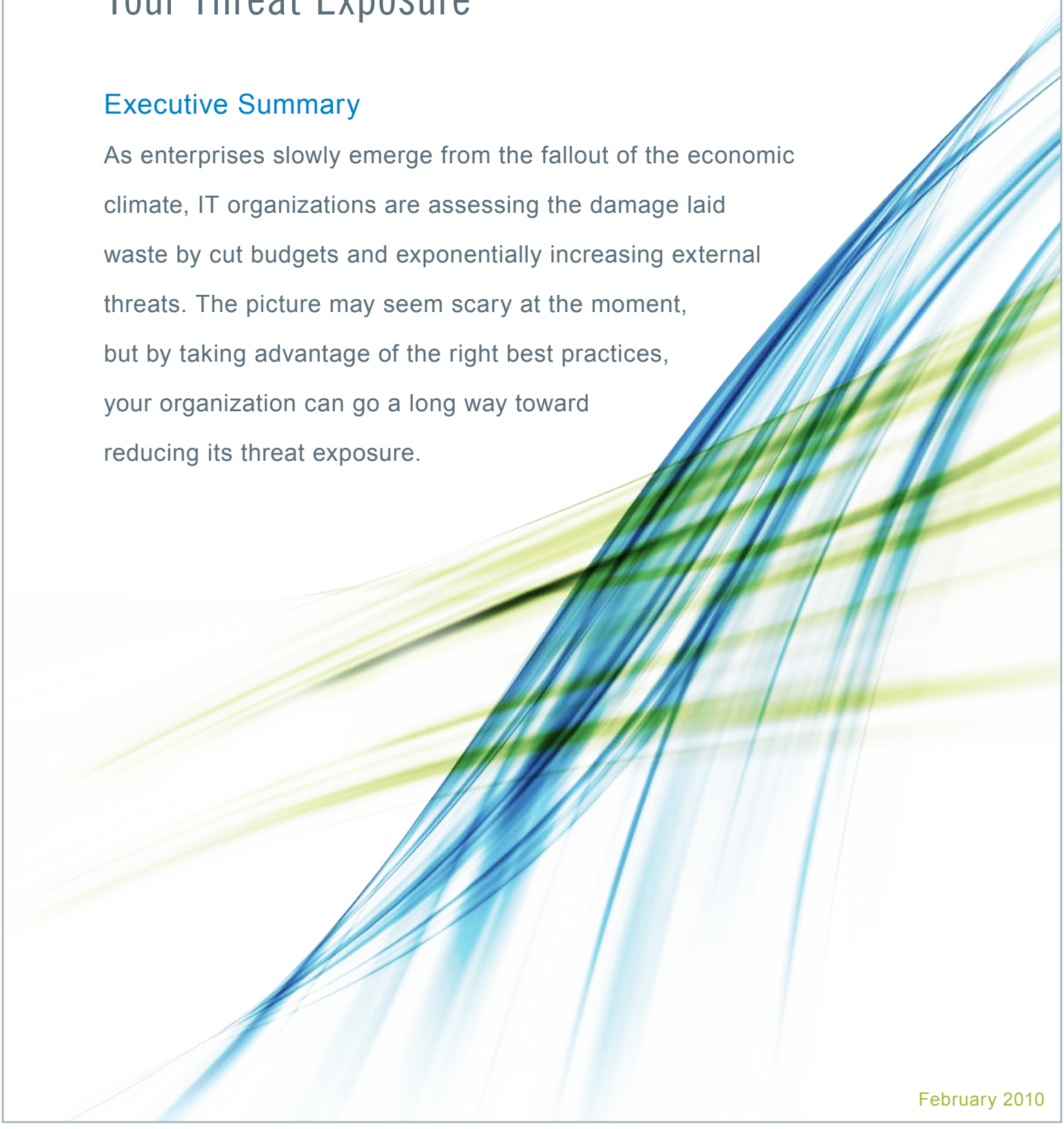
Best Practice Guide to Reducing Your Threat Exposure

Executive Summary

As enterprises slowly emerge from the fallout of the economic climate, IT organizations are assessing the damage laid waste by cut budgets and exponentially increasing external threats. The picture may seem scary at the moment, but by taking advantage of the right best practices, your organization can go a long way toward reducing its threat exposure.



February 2010

WP-EN-02-24-10

Best Practice Guide to Reducing Your Threat Exposure

As enterprises slowly emerge from the fallout of the economic climate, IT organizations are assessing the damage laid waste by cut budgets and exponentially increasing external threats. The picture may seem scary at the moment, but by taking advantage of the right best practices, your organization can go a long way toward reducing its threat exposure.

Even as organizations faced massive IT budget cuts and pressure to spend remaining security monies on skyrocketing compliance costs in 2009, the external forces threatening infrastructure and information did not let up last year. In fact, the risks continued to grow more mature and plentiful than ever before. According to the 2009 Computer Crime Security Survey, the number of organizations that experienced malware infections this year shot up from 50 percent all the way to 64 percent.

And as FBI Assistant Director of Cybersecurity Shawn Henry told a conference crowd in October 2009:

"The threat we see to every piece of infrastructure is significant and continuing to grow. Energy, transportation, banking and finance, information technology, retail — they've all been breached across the spectrum."

Last year, cybercriminals continued to innovate with threats like Koobface that took advantage of the explosion in Web 2.0 applications and others such as Conficker that exploited organizations' and individuals' continuing inability to patch systems and securely configure them.

It's all a continuation of the year's long evolution of cybercrime into a viable business for the unscrupulous. Cybercrime is one of the fastest-growing industries in the world. In 2008, it expanded tenfold. The numbers are still out for 2009, but analysts believe there is no burst bubble in store for the cybercrime economy.

For the law-abiding, the onslaught only continues. Organizations face, on average, five malware events each year or 10 events if there are more than 5,000 users. And it isn't just large enterprises that are at risk. According to FBI estimates from October 2009, cybercriminals have stolen more than $40 million from small- to medium-size businesses since 2004. Clearly, all organizations must find a way to reduce their exposure to these risks, even if budgets remain flat in 2010.

Why Manage Your Critical Risk?

Organized External Threats

Sophisticated criminal networks are now supplying the black market with more than $5.3 billion in stolen corporate and personal information obtained by exploiting known security flaws. This despite remediation being available 90 percent of the time to correct these security flaws.

Consumerization of IT

End users are utilizing personal tools for productivity, both hardware (USB devices) and

software (IM and other Web 2.0 applications) causing additional threats to your network.

Regulatory Compliance

States and countries are becoming stricter about regulations as the risks to computer networks become more intense. Efficiently proving compliance with regulatory or corporate policies, as well as industry best practices, is now vital.

Diversity of Operating Systems and Applications

Network environments have become heterogeneous and therefore more complex to configure and maintain. Within these increasingly diverse networks, the need for an automated security solution that supports multiple OS platforms, applications and vendors is crucial to managing the 13 new vulnerabilities that are released each day, in addition to maintaining security configurations[1].

The Cost of Risks and Threats

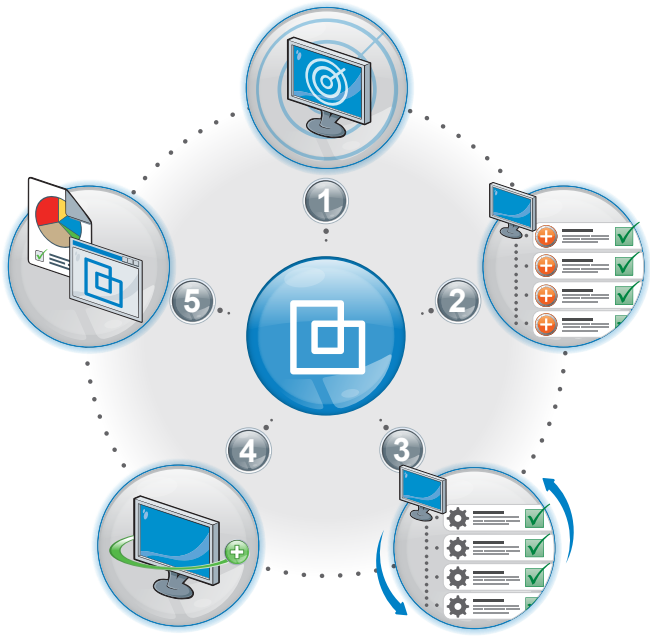
- 72 percent increase in computer replacement costs and increased help desk tickets[2].
- The potential worth of stolen information traded online during 2008 was $5.3 billion[3].
- The average security incident costs an organization $234,000[4].

How to Manage Your Critical Risk

By managing the entire vulnerability management lifecycle with a holistic solution and transitioning from a reactive security model to a proactive risk management approach, you can eliminate the majority of risks to your network environment.

The Vulnerability Management Lifecycle

- Discover: Gain complete visibility of your heterogeneous network environment.
- Assess: Identify known issues before they can be exploited.
- Prioritize: Focus on your most critical security risks first.
- Remediate: Automatically deploy patches to the entire network.
- Report: Gain a holistic view of your environmental risk.



1. National Vulnerability Database
2. William Bell, Director of Security, ECSuite
3. Joan Goodchild, Why Cybercrime is Thriving, CSO - November 28, 2008
4. 14th Annual CSI Computer Crime and Security Survey, 2009

How to Manage Your Critical Risk

Best Practices	How Lumension Helps
1. Find All Assets: Proactively discover all IT assets, both managed and unmanaged, and any vulnerabilities that may exist within your entire network environment to gain visibility of your threat landscape and understand your security posture.	» In-depth inventory scans and flexible grouping and classification of your IT assets provide full visibility into the devices connected to your network. » Discovers silent or hidden network nodes. » Continuous vulnerability assessments of IT assets provide actionable intelligence and help identify vulnerabilities before they can be exploited.
2. Practice Rule of Least Privilege: Set up systems with the most secure configuration that your business will allow.	» Provides out-of-the-box regulatory, standards-based assessment and industry best-practice templates to ensure endpoints and applications are properly configured.
3. Automate Endpoint Management: Automate patch and configuration management to make sure systems maintain their secure configuration, are fully patched and updated with the latest software version (including keeping antivirus software up to date).	» Automatically deploys patches through a single, scalable solution to patch and remediate a heterogeneous network, covering all major applications and operating systems, such as Windows, UNIX, Linux, Apple Mac OS and Novell — as well as customized software applications. » Repository of more than 25,000 patches covers all major applications and operating systems from many vendors. » Enforces application and device use based on granular policies to proactively protect against data leakage and malware. » Identifies high-risk vulnerabilities that are not patch-related, leveraging Lumension's large pre-built vulnerability and configuration repositories, as well as customized vulnerability policies. » Rapid, accurate and secure patch management with comprehensive ongoing vulnerability assessment ensures systems are always up to date and free from vulnerabilities.
4. Develop and Define Policy: Define security policies with global, user-specific and/or machine-specific rules based on organizational needs.	» Easily creates a "whitelist" of authorized applications. » Centralizes policy management per user or user group as well as per computer based on user and/or machine. » Supports hundreds to thousands of endpoints with scalable installation.
5. Demonstrate Compliance: Maintain and demonstrate compliance with regulatory policy requirements (FDCC, PCI-DSS & HIPAA) by mapping security policies to technical controls and continuously measuring configuration results via comprehensive compliance reporting.	» Delivers Security Content Automation Protocol (SCAP)-validated configuration assessments. » Leverages security best practices to ensure secure configurations and simplify compliance. Security configuration checklists are obtained from a variety of sources, including: OVAL Vulnerability Fingerprints, SCAP, FDCC Compliance Checklist, PCI Compliance Checklist, NIST NVD, Microsoft Patch Fingerprint, etc. » Detects systems that have drifted out of configuration policy. » Continuously managing and enforcing security configuration policies ensures that endpoints and applications are properly configured, effectively reducing security incidents and strengthening your security posture.

Key Lumension Solutions

Lumension® Vulnerability Management

The Lumension Vulnerability Management solution delivers automated vulnerability assessment and patch management through an integrated solution that enables businesses to automatically detect risk, deploy patches and defend their business information across a complex, highly distributed environment with greater efficiency and minimal impact to productivity. All of these activities are seamlessly integrated into a single management console for complete visibility into your network.

Lumension® Scan

Complete network-based scanning solution enables assessment and analysis of threats impacting all network devices.

- Complete identification and inventory of all devices on the network.
- Accurate scans of all devices for software and configuration-based vulnerabilities.
- Risk-based prioritization of identified threats.
- Continuously updated vulnerability database for orderly remediation.
- Comprehensive reports of scan results.

Lumension® Patch and Remediation

Proactive management of threats enables automated collection, analysis and delivery of patches across heterogeneous networks (all major operating systems and applications).

- Reduce corporate risk through the timely, proactive elimination of operating system, application and configuration vulnerabilities.
- Decrease IT costs and improve productivity with a highly automated, subscription-based patch management solution.
- Eliminate recurring risks through “patch drift.”
- Demonstrate compliance with regulatory security policies and industry standards through the continuous monitoring and enforcement of mandatory baselines as well as comprehensive reporting.

Lumension® Security Configuration Management

Comprehensive risk assessment of security configurations enables regulatory compliance and improves security posture.

- Delivers Security Content Automation Protocol (SCAP)-validated configuration assessment.
- Enables the standardization of endpoint and application configurations.
- Ensures endpoint and application configurations are continuously secured.
- Maps technical controls to regulatory policies, industry standards or corporate policies.
- Demonstrates policy compliance by reporting configuration status against regulations and industry standards.
- Reduces exposure to operational and financial risk.

Lumension® Content Wizard

Powerful tool that automates tedious and time-consuming system and desktop management tasks to optimize your IT environment and take advantage of cost- and resource-saving options via power management capabilities.

- Reduces power consumption by standardizing system power settings across the organization.
- Optimizes IT efficiencies and improves software usage compliance with policy-based deployment and removal of new and updated software.
- Enforces security configuration policies based on industry best practices.
- Automates time-consuming tasks across the entire network, including disk defragmentation and policy enforcement for system settings.
- Centrally deploys, manages and reports on all scripting actions, including making sure antivirus is installed and distributing third-party patches.

Lumension® Endpoint Protection

Combination of antivirus and behavioral analysis capabilities with policy-based enforcement of application use that secures organizational endpoints from malware, spyware and unwanted or unlicensed software.

- Scan for and remove all known malware to establish a clean environment.
- Define and enforce a trusted application environment throughout the organization.
- Block and remove known malware and use behavioral analysis tools to assess new unknown code which may or may not be legitimate.
- Reduce IT support volume and increase end-user productivity by eliminating unapproved applications.
- Demonstrate policy compliance and ensure software license compliance by drilling down on suspicious behavior for security or legal follow-up.

Additional Resources

Lumension Vulnerability Management Solution: Automating the Vulnerability Management Lifecycle

This whitepaper examines how the Lumension Vulnerability Management solution enables organizations to mitigate their critical risk by integrating the five phases of vulnerability management.

Download Now.

Staying Ahead of Threats: A Look at Lumension Vulnerability Management

Learn how Lumension Vulnerability Management helps organizations effectively minimize security risks through the proactive discovery of IT assets and automated remediation of software and configuration vulnerabilities.

Download Now.

EC Suite Case Study

EC Suite‘s preventive security approach, enforced by Lumension solutions, has yielded a stronger

security profile against malicious attacks, reduced overall IT and security operational expenses, and enhanced operational efficiencies.

Download Now.

About Lumension

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 IT Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Ariz., Lumension has operations worldwide, including Virginia, Utah, 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.