

Exploring the ESG “Outside-In” Confidential Data Security Model

Date: August 2009

Author: Jon Oltsik, Senior Principal Analyst

Abstract: Confidential data resides everywhere—from locked-down data centers to mobile devices—and is increasingly accessed by a wide range of constituents—from employees to contractors and business partners. How can CIOs and CISOs possibly secure confidential data when it is in a constant state of motion? The ESG “Outside-In” data security model seeks to put confidential data security in context by anchoring data security to risk metrics, categorizing risk zones, and recommending security controls. This requires a greater focus on distributed data and controls like endpoint DLP. When properly and consistently applied, ESG believes that the “Outside-In” security model can help organizations improve confidential data security, mitigate information risk, while making this data more productive for global network-based business processes.

Research Overview

In April 2009, ESG published a research report titled *Protecting Confidential Data Revisited*, which builds upon a similar research study conducted in 2006. The objective of ESG’s report was to uncover the confidential data security practices, challenges, and future plans of large “enterprise-class” organizations. To gather data for this report, ESG surveyed 308 North American and Western European information security professionals at enterprise-class organizations (1,000 employees or more) that were responsible for or familiar with their organization’s current policies, procedures, and technologies used to protect and secure confidential information.

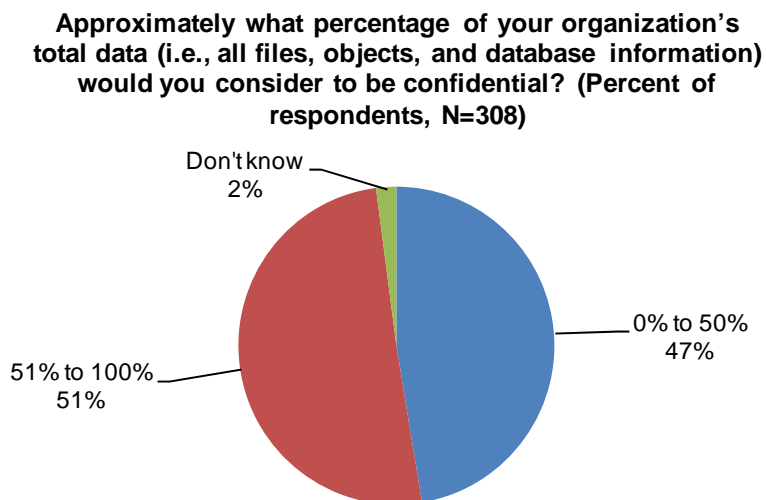
For the purposes of ESG’s research, confidential data was defined as information that can be categorized as:

- Intellectual property.
- Information that is protected by government regulations.
- Non-public private information (NPPI).
- Information that is protected by industry regulations.
- Information classified as company confidential or private.
- Personally Identifiable Information (PII).

Key Research Findings

While an exhaustive discussion of the research findings is beyond the scope of this brief, a few data points can be used to summarize the current state of confidential data security. ESG’s research found overwhelming evidence that confidential data is prolific and spread throughout the enterprise in databases, file shares, and e-mail repositories. This data is strewn across a wide variety of devices including enterprise storage systems, departmental servers, desktop and laptop PCs, and various other mobile devices. As shown in Figure 1, 50% of all respondents consider more than half of their organization’s total data to be confidential (for more detailed information on confidential data trends, see the April 2009 ESG Research Brief *Amount of Confidential Data by Company Size and Industry*).

FIGURE 1. CONFIDENTIAL DATA IS PERVASIVE ACROSS THE ENTERPRISE

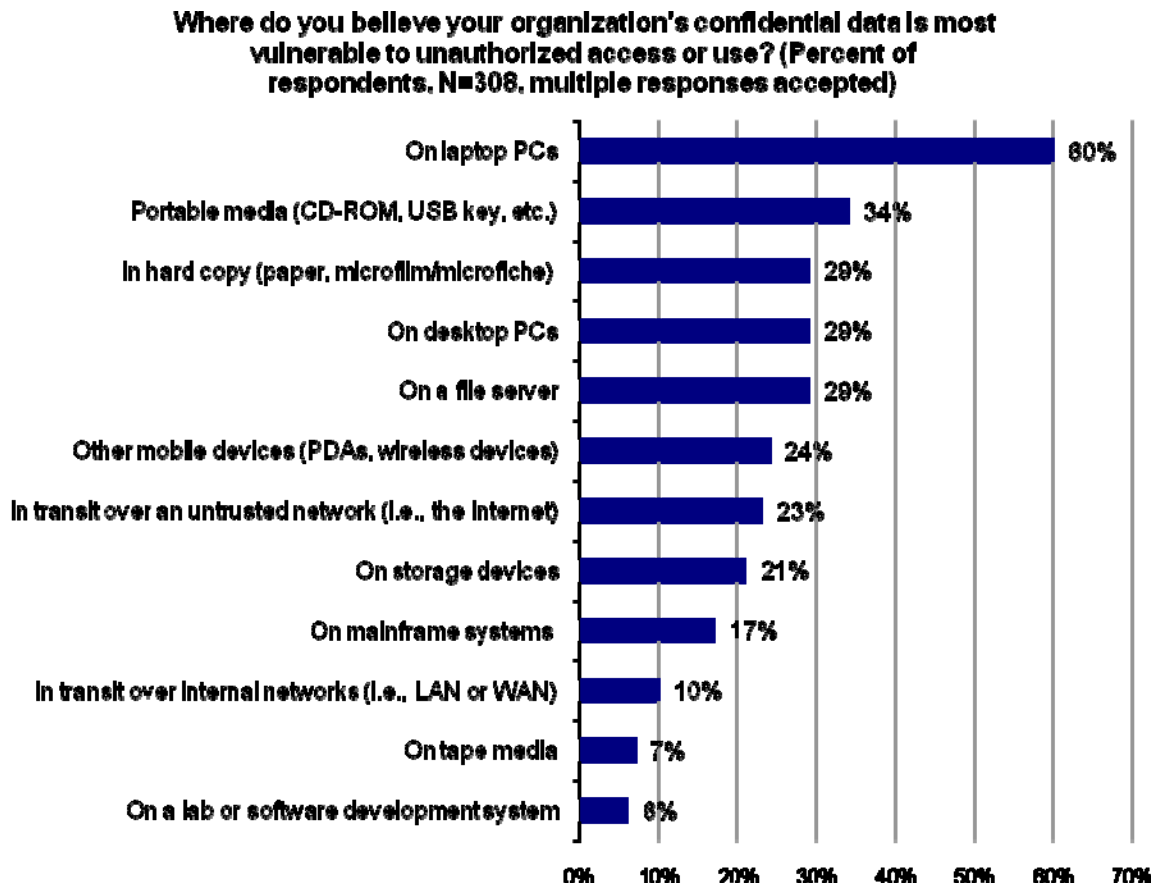


Source: Enterprise Strategy Group, 2009

While this confidential data is vulnerable to a number of different threat vectors, some risk patterns are clearly evident. Ultimately, ESG concludes that risks associated with an accidental or malicious breach of confidential data are a function of three primary factors:

1. **The volume of users and devices with access to confidential data.** Risk is a function of the number of users and devices with the ability to read, write, copy, move, and manipulate confidential data. Simply put, more devices and/or users leads to greater risk.
2. **Data mobility.** Risk is also proportional to data mobility. The more mobile the data, the higher the risk. For example, 60% of security professionals said that their organization's confidential data is most at risk on laptop PCs while 34% said that their organization's data is most at risk on portable media like CD-ROM disks and USB flash drives. In contrast, just 21% of respondents believe confidential data stored on enterprise storage systems is at risk (see Figure 2).

FIGURE 2. LARGE ORGANIZATIONS RANK CONFIDENTIAL DATA VULNERABILITIES



Source: Enterprise Strategy Group, 2009

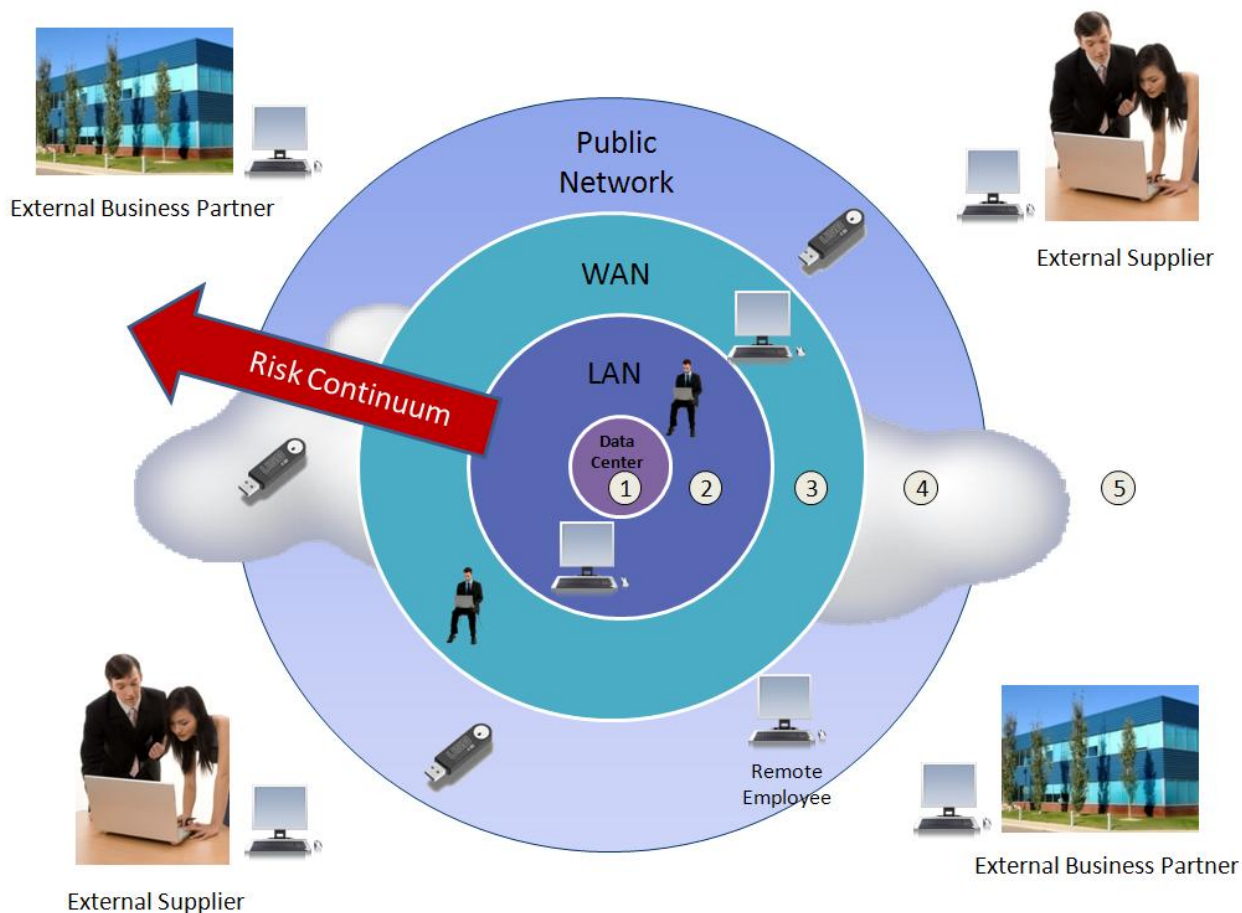
- The data's proximity to IT.** Risk is also a function of the location of confidential data in relation to its proximity to IT. Confidential data with limited or no IT oversight, often in motion over unsecured networks, is most at risk. However, mainframes which contain a high percentage of confidential data, are less at risk since enterprise systems tend to be housed in data centers surrounded by tight security controls, and are in close proximity to IT staff. Security professionals here are generally less concerned with confidential data stored on mainframes than data on other systems. Additionally, corporate employees and external constituencies outside of the purview and controls of the IT department present a bigger risk to confidential security than knowledgeable collocated IT staff.

Taken together, these three criteria can be used to establish a common risk model for any confidential data in the enterprise, regardless of industry, compliance mandates, or business processes. This model can be summarized as follows: Confidential data that is accessible by a large number of mobile users with limited IT oversight is at the greatest risk of a malicious or accidental data breach.

Introducing the ESG “Outside-In” Confidential Data Security Model

ESG has developed its “outside-in” confidential data security model as a framework for security professionals seeking to minimize risk associated with the loss or misuse of sensitive information. Based on this model, security executives should focus their efforts at the edge of the network where confidential data is voluminous, constantly changing, and mobile—and where there is limited proximity to IT personnel and security controls. In other words, multiple vulnerabilities at the network edge should take precedence over incremental efforts and controls in relatively secure corporate data centers (see Figure 2).

FIGURE 3. THE ESG “OUTSIDE-IN” CONFIDENTIAL DATA SECURITY MODEL



Source: Enterprise Strategy Group, 2009

In the ESG model, controls, safeguards, and oversight efforts should begin with confidential data that is accessible to a broad range of distributed users and/or is capable of being or likely to be stored or transported on removable media and portable devices. From this starting point, security efforts should then proceed in a stepwise fashion toward the data center. This model should not preclude a full enterprise data risk assessment nor should it ignore potential security vulnerabilities in the data center. However in general terms, the ESG “outside-in” model maps to the most significant threats, risks, and vulnerabilities identified by enterprise security professionals.

Note that there are five different network zones illustrated. Each of these zones—proceeding in order from zone 1 to zone 5—corresponds to an increasing risk profile and therefore requires a different security model. ESG’s definition of and security recommendations for each zone are displayed in Table 1. These recommendations go beyond security technology tools alone. ESG believes that user training, legal protection, policy definition, and activity monitoring are also essential components in confidential data security for overall risk reduction.

TABLE 1. CONFIDENTIAL DATA SECURITY STRATEGIES BASED UPON THE ESG “OUTSIDE-IN” CONFIDENTIAL DATA SECURITY MODEL

Zone	Location	Volume of users and devices	Data mobility	Proximity to IT	Sample recommendations
5	Public network/ non-employee users	High. Likely to grow as more external users are given network access.	High and uncontrollable	Not available. IT may provide a support role but no security role.	<ul style="list-style-type: none"> Strong authentication Contractual/legal protections Cooperative training with business partners Read-only access or ERM Network/application layer encryption SSL VPN access only DLP
4	Public network/ remote employee access	High. Increase is related to new devices, employee growth, and telecommuting	High. Large population of laptops and unrestrained mobile devices	Low. Users and devices may be invisible to IT for extended periods of time.	<ul style="list-style-type: none"> Specialized user training, frequent updates Employee contract stipulating policies and penalties Strong authentication Entitlement controls based upon employee role User behavior auditing Access policies based upon network location and device health (NAC) SSL VPN access only Full-disk encryption Approved and authenticated mobile devices only with encryption Endpoint DLP or ERM
3	WAN	Medium to high depending upon organizational size	Medium to high depending upon organizational size	Low to medium. May have remote staff.	<ul style="list-style-type: none"> Multi-tiered user training depending upon mobility, quarterly updates Employee contract stipulating policies and penalties Strong password and password management Entitlement controls based upon employee role User behavior auditing NAC policies tailored for local users. Mobile workers inherit controls from Zone 4 above Backhaul all Internet access through data centers Full-disk encryption for laptops Approved and authenticated mobile devices only with encryption Endpoint DLP or ERM Specialized controls for local IT devices (ex. file servers, tape drives, etc.)
2	LAN	Medium to high depending upon organizational size	Medium to high. Use of wireless networks and mobile devices	Medium to high. Ratio of IT/security staff to users varies by organizational size.	<ul style="list-style-type: none"> Strong physical security with links to electronic security controls Multi-tiered user training depending upon mobility, quarterly updates Employee contract stipulating policies and penalties Strong password and password management Entitlement controls based upon employee role User behavior auditing NAC policies tailored for local users. Mobile workers inherit controls from Zone 4 above Full-disk encryption for laptops Approved and authenticated mobile devices only with encryption Endpoint DLP or ERM Network-based DLP
1	Data center	Low. Should be limited to IT staff and approved devices	Low with the exception of backup tapes shipped off-site	High. Non-IT personnel should have limited access.	<ul style="list-style-type: none"> Strong physical security with links to electronic security controls Role-based access controls Administrator authentication linked to Active Directory, RADIUS, etc. Hardened configurations of all systems Approved mobile devices only IT behavior auditing Tape encryption Data destruction of hard drives that leave data center

CISOs Must Address Confidential Data Security Chaos

Think of confidential data security as a complex multi-dimensional matrix where large organizations must somehow manage confidential data access, distribution, and usage by a growing number of users, applications, and devices. How can security officers possibly reign in this chaos? It certainly isn't easy, but ESG believes that smart organizations will begin this effort with:

- **Data discovery and classification.** Before undertaking any confidential data security effort, it is first important to start with a definition of confidential data within an organization. Large organizations must adopt an appropriate taxonomy for confidential data classification. Closely related to data classification is data discovery. As one would expect, data discovery means assessing every digital and physical nook and cranny in the enterprise, finding confidential data, applying a classification, and then aligning classified data with appropriate controls.
- **User education.** As the old security adage goes, "people are the weakest link in the security chain." If users don't know that they shouldn't download software, email private data, or save personal records to portable storage devices, their behavior will likely lead to security incidents. Yes, most large organizations already have some form of end user security training but ESG Research indicates some problems – 28% of security professionals rated their organization as either fair or poor with regard to communicating and training employees on confidential data security policies. Given this, smart CSOs will start by assessing the effectiveness of current security training and communications practices and proactively address all shortcomings.
- **Activity monitoring.** Another time honored saying is applicable here, "you can't manage what you can't measure." In other words, strong confidential data security depends upon logging the distribution and use of confidential data at all times. Armed with this information, security professionals can spot suspicious behavior, adjust security policies, fine-tune enforcement, and determine focus areas for end user security training.

As far as technology, it is worth noting that DLP technology is ubiquitous throughout the ESG outside-in model as it is recommended in each security zone. This shouldn't come as a surprise since DLP technologies are already widely deployed in large organizations. Yet ESG's model is somewhat different than many DLP deployments in its emphasis on endpoint DLP. Many organizations rely on network-based DLP alone. ESG believes that this is a mistake. Since confidential data security risk increases with scale, mobility, and distance from IT, security monitoring and policy enforcement is really dependent upon a myriad of endpoint tools including port blocking, full disk or file and folder encryption, and DLP. What's more, endpoint DLP is a critical component of data discovery, classification, user education, and behavior monitoring. As such, desktop DLP must become a future priority for those organizations that have not already piloted or deployed this technology.

The Bottom Line

With ever-growing volumes of sensitive data spread throughout the enterprise, few would argue that securing confidential data is an uphill climb for most IT organizations. Unfortunately, the technology industry has not provided users with the right contextual model to define and address this problem, choosing instead to sell tactical products rather than end-to-end enterprise solutions.

The ESG "outside-in" confidential data security model is not a panacea, but rather a tool for making data security more manageable by qualifying risk based on three factors: data/device/user volume, data mobility, and data proximity to IT personnel and controls. When applied on a business process basis, ESG believes that the "outside-in" security model and recommendations can help guide CISOs toward a more manageable way to address their confidential data security requirements and focus on areas that will maximize information risk mitigation and return on security investment.

subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.