White Paper

The 2013 Vormetric Insider Threat Report

Written By Jon Oltsik, Senior Principal Analyst, ESG

October 2013

Vormetric

Administered by ESG.

Contents

Executive Summary

The 2013 Vormetric Insider Threat Report, a collaborative research project conducted by Vormetric and the Enterprise Strategy Group (ESG), is based upon a survey of 707 IT professionals responsible for evaluating, purchasing, or managing information security technologies and services for their organizations. Respondents came from companies ranging in size—from less than $250 million to more than $20 billion in revenue—and representing numerous industry and government segments.

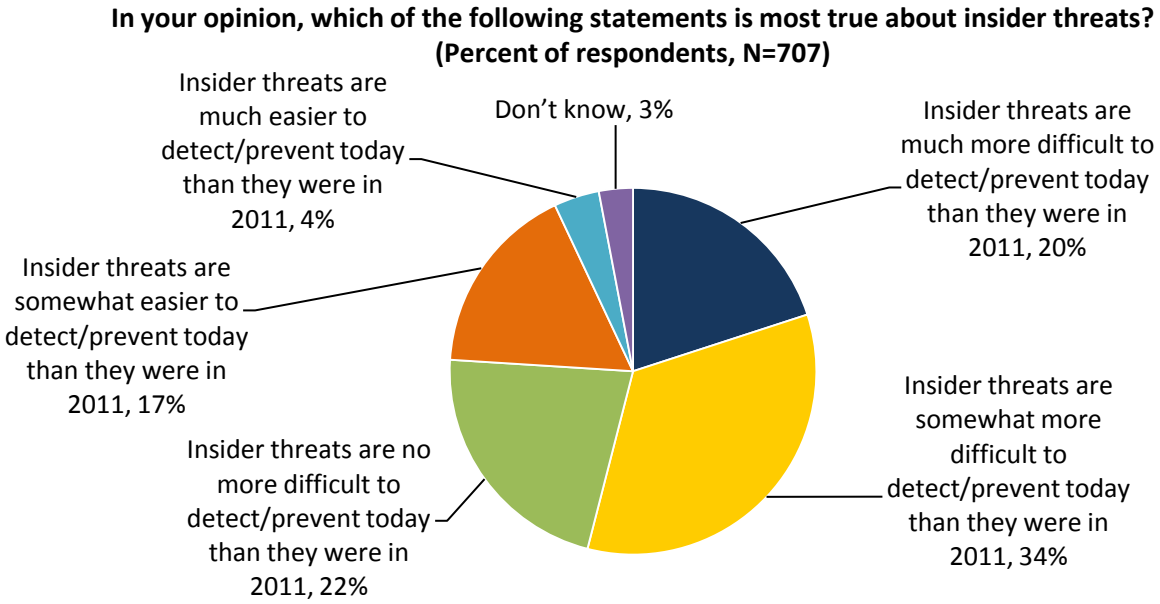
While the security community remains fixated on advanced malware, tried-and-true insider threats and related attacks remain a vexing problem for most organizations. This report concludes:

- Insider threats continue to present a challenge. The majority of organizations believe that insider threats are becoming more difficult to detect/prevent and that they remain vulnerable to insider attacks. Why? IT scale (i.e., number of users, devices, network packets, etc.), cloud computing, and advanced malware threats provide the necessary cover for insiders to hide their attacks among typical IT activities.
- Status quo security is not working well. Organizations continue to invest in perimeter and host-based security technologies like firewalls, IDS/IPS, and antivirus software, but these security defenses are no match for knowledgeable insiders and sophisticated cyber adversaries who have the right access, skills, and tactics to easily circumvent security controls, steal valuable data, and cause massive damage.
- Advanced organizations are moving toward a more data-centric security strategy. ESG data reveals that security-conscious organizations are increasing their investments in technologies for granular data access, encryption, key management, and data security intelligence. This is a leading indicator of the future market direction. Given increasing de-perimeterization, ESG believes that data-centric security will move to the mainstream built upon five key cornerstones: identity, policy, infrastructure-based policy enforcement, data-specific policy enforcement, and situational awareness.

Insider Threats Are Bad and Getting Worse

While the security community has focused its attention on advanced malware over the past few years, insider threats (i.e., threats posed by employees, third parties, or malicious software that uses legitimate access rights to networks, applications, and sensitive data as an attack vector) continue to present a number of challenges for many organizations. In fact, ESG research indicates that more than half (54%) of IT and security professionals believe that insider threats are more difficult to detect/prevent today than they were in 2011 (see Figure 1).

Figure 1. Insider Threat Sentiment



Source: Enterprise Strategy Group, 2013.

What makes insider threat detection/prevention so much more difficult? For the most part, it is a simple matter of arithmetic and scale. For example, ESG research reveals that:

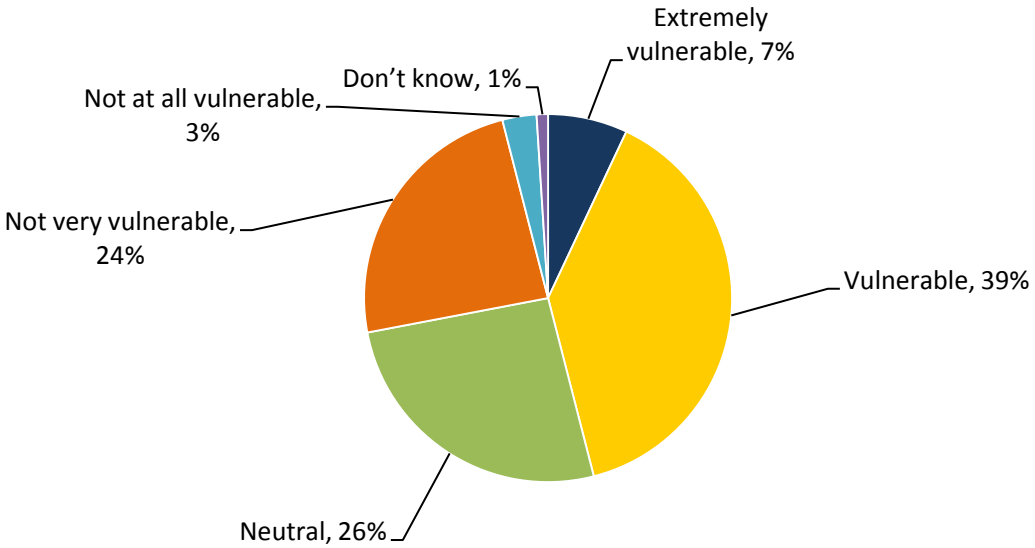
- 37% of respondents point to the fact that there are more people—like employees, contractors, and business partners—with access to the network. The increase in people accessing the network simply makes it more difficult to isolate suspicious behavior.
- 36% say that the growing use of cloud computing at their organizations makes insider threat detection/prevention more difficult. This is understandable because cloud computing distributes sensitive data beyond internal IT control and thus increases the attack surface for insider assaults. Additionally, cloud security is notoriously difficult for many organizations.
- 35% indicate that the growing volume of network activity makes insider attack detection/prevention more difficult. This difficulty is likely related to baselining normal behavior and pinpointing anomalies buried in an avalanche of ports, protocols, and applications traversing the network.
- 27% admit that cyber-attacks like APTs make insider attack detection/prevention more difficult. This may be an indication that insiders are also using sophisticated attack techniques that emulate "normal" behavior, helping them achieve their cybercrime goals.

Many Organizations Remain Vulnerable to Insider Threats

Since insider threat detection/prevention is becoming increasingly difficult (for a multitude of reasons), it is not surprising that many organizations believe they are vulnerable to an insider attack. In fact, ESG research indicates that 46% of organizations believe they are extremely vulnerable (7%) or vulnerable (39%) to insider threats (see Figure 2).

Figure 2. Perceived Vulnerability of Experiencing an Insider Attack

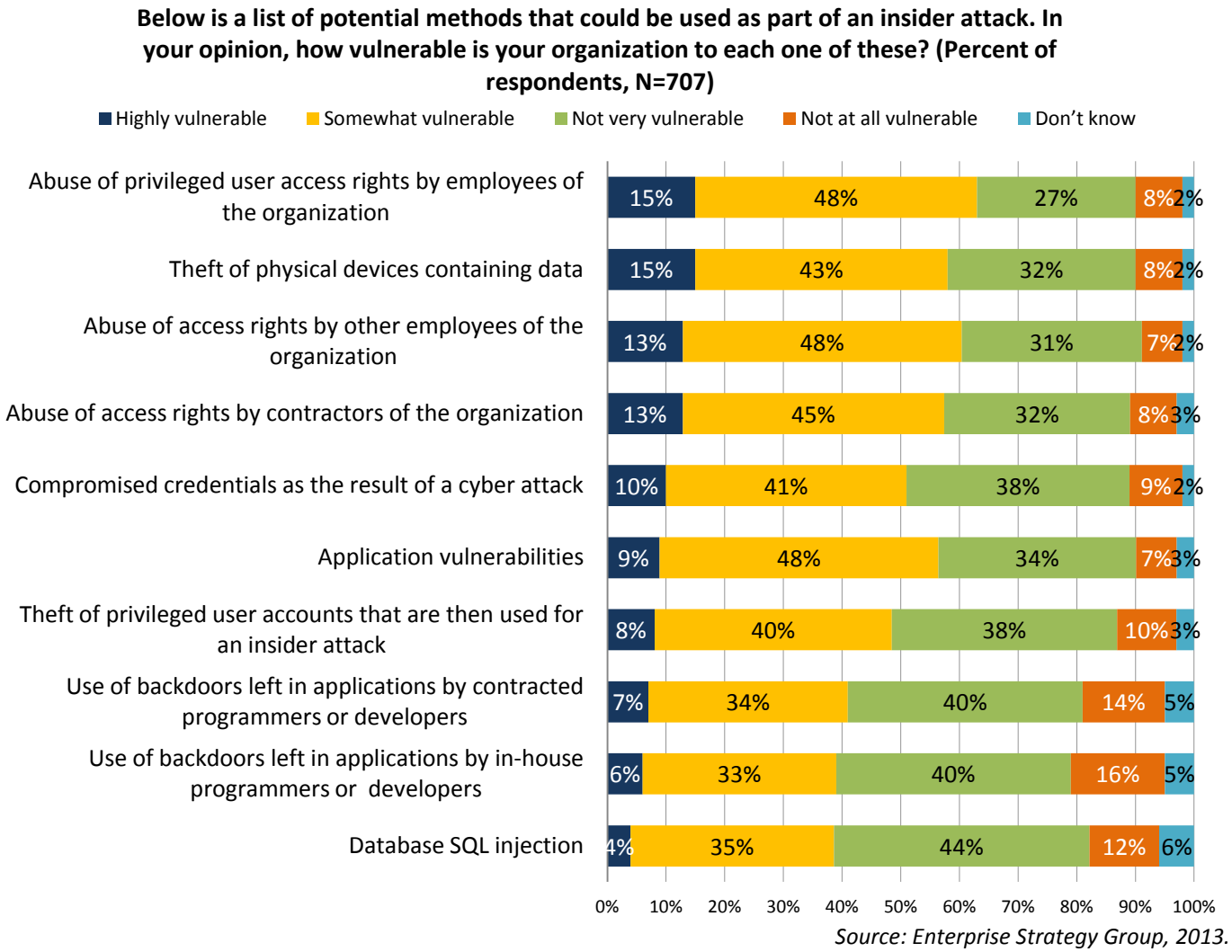
In your opinion, how vulnerable is your organization to experiencing an insider attack? (Percent of respondents, N=707)



Source: Enterprise Strategy Group, 2013.

ESG pushed survey respondents further to identify areas in which organizations believe they are most vulnerable to an insider attack. Alarmingly, the list of vulnerabilities is lengthy and diverse. In aggregate, more than half of all survey respondents believe their organizations are extremely vulnerable or somewhat vulnerable to six different types of attack tactics (see Figure 3).

Figure 3. How Vulnerable Organizations Believe They Are to Potential Methods of Insider Attacks



Source: Enterprise Strategy Group, 2013.

It should also be noted that targeted attacks like APTs are executed so that external cyber adversaries harvest insider credentials and thus perpetrate "insider" attacks. In this case, any of the vectors discussed are fair game in pursuit of a cyber-attack resulting in data exfiltration.

Insider Attacks Emanate from a Variety of Suspects

ESG's data indicates that many organizations are vulnerable to insider attacks in a number of areas, increasing overall IT risk. Just what types of users are most likely to exploit these vulnerabilities for malicious or criminal purposes?

- 51% of security professionals say that non-technical employees with legitimate access to sensitive data are one of the biggest threats to their organizations.
- 48% of security professionals say third-party contractors with legitimate access to their organization's network are one of the biggest threats to their organizations.
- 34% of security professionals say that IT administrators are one of the biggest threats to their organizations.

Security professionals' anxiety about non-technical employees with legitimate access to sensitive data may be rooted in a pair of recent highly publicized security breaches. In August of 2013, U.S. Army private Bradley Manning was found guilty of releasing a large volume of confidential documents to the public through Wikileaks, an international, online, nonprofit organization that publishes secret information, news leaks, and classified media

from anonymous sources. In addition, Edward Snowden, a contractor working for Booz Allen Hamilton, leaked information about NSA surveillance programs to the Guardian and other media outlets.

It seems that these incidents have enlightened business executives and CISOs alike to the risks associated with employees whose responsibilities include analyzing large volumes of sensitive data. In fact, ESG found that nearly half (45%) of organizations say that the Snowden affair did change the organization's perspective on insider threats either substantially or somewhat.

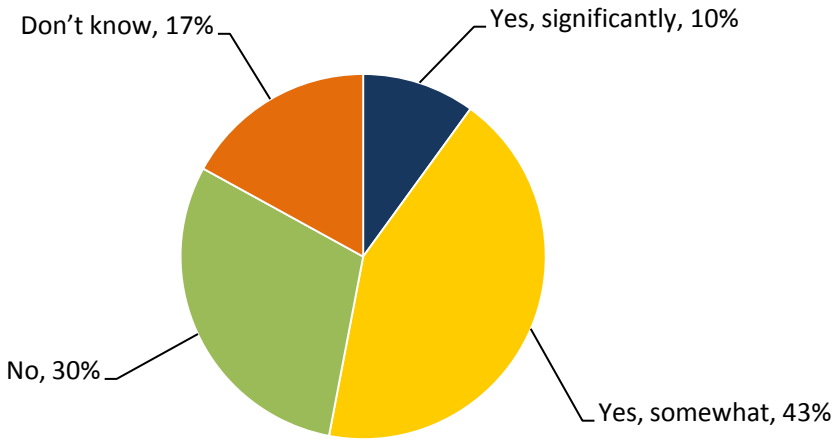
Organizations Are Responding to Insider Threats

The ESG data indicates that risks associated with insider threats should not be underestimated: Insider attacks are more difficult to detect/prevent; organizations point to a list of vulnerabilities; and numerous types of users are well positioned to launch insider attacks with extremely damaging consequences. In the past, these risks were known yet somewhat amorphous to business managers and corporate executives. This is no longer the case as Army Private Bradley Manning and Edward Snowden served to personify insider attacks. The risks have become that much more real, and the devastating results are now widely understood.

The good news is that insider threats have not gone unnoticed. In fact, ESG found that more than half (53%) of all organizations will increase information security budgets in direct response to insider threats (see Figure 4).

Figure 4. Organizations Are Increasing Information Security Budgets in Response to Insider Attacks

To the best of your knowledge at this time, will your organization increase its information security budget over the next 12 months in direct response to insider threats? (Percent of respondents, N=707)



Source: Enterprise Strategy Group, 2013.

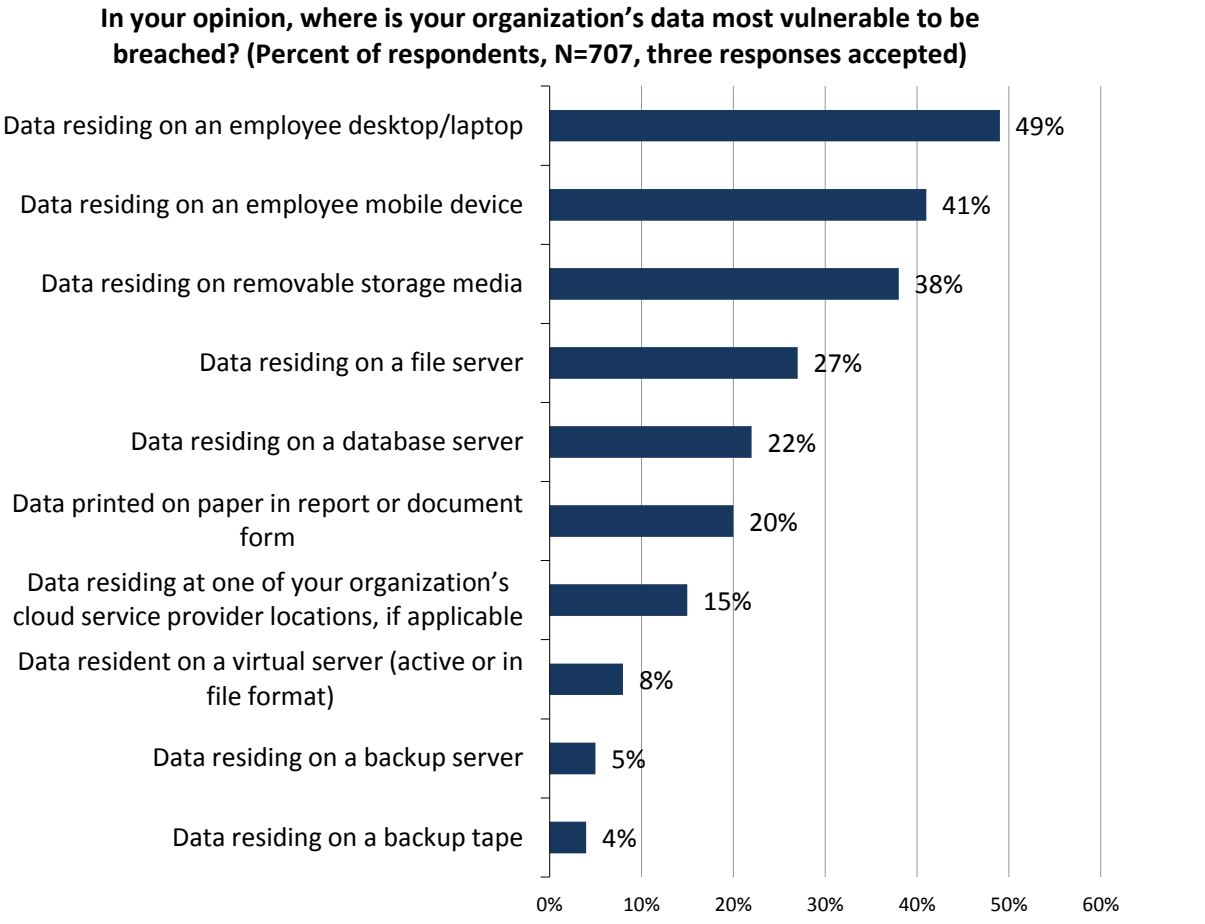
Defending Against Insider Attacks

While some insiders plant logic bombs in order to destroy valuable systems, most insider attacks tend to include data theft as one of the primary objectives. A sales manager takes a new position with a direct competitor and decides that taking the company's customer database might help her accelerate her progress. A disgruntled knowledge worker steals company intellectual property to extort money from his employer. An intelligence officer decides to leak sensitive diplomatic data to WikiLeaks.

To address the risks associated with a rogue or malicious insider, security teams implement compensating security controls in numerous areas. Of course, smart CISOs prefer to focus these controls in the right places—where data is

most at risk. Where are these vulnerable locations? Security professionals pointed to several areas, including data residing on an employee desktop/laptop (49%), data residing on an employee mobile device (41%), and data residing on removable storage media (38%, see Figure 5).

Figure 5. Where Data is Most Vulnerable to Being Breached



Source: Enterprise Strategy Group, 2013.

The obvious pattern here is that mobile data is vulnerable data. Large organizations should certainly address this risk by classifying data on endpoint devices, moving highly classified data from endpoints to more secure repositories, and limiting data storage and usage options.

These are important controls as mobile data is certainly susceptible to loss or theft, but security professionals should not assume that data on file or database servers is better protected. This is especially true since sophisticated "low-and-slow" attacks tend to perform network reconnaissance, locate sensitive data stores, obtain privileged user credentials, and eventually gain access to highly valuable data. To safeguard these assets, ESG recommends a full assessment of existing data security controls. Would these existing security controls really help prevent or detect an APT? Based upon ESG research, the answer is: probably not.

Security Controls Used to Address Insider Threats

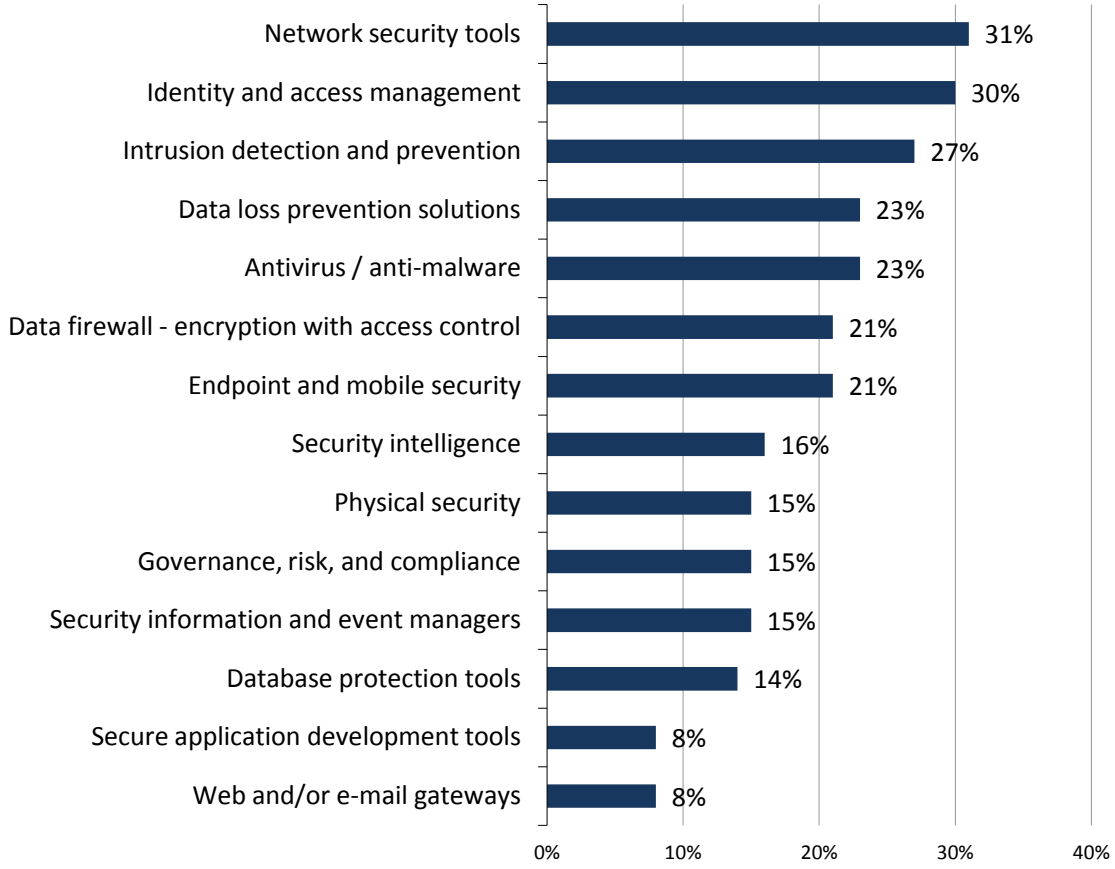
ESG asked respondents to identify the most important security controls used to mitigate the risk associated with insider threats. The top three most-cited security controls were network security tools (31%), identity and access management (30%), and intrusion detection and prevention (27%, see Figure 6).

ESG believes it is noteworthy that two of the top three controls identified by respondents are information security staples that are usually deployed at the network perimeter. Perhaps security professionals pointed to network security tools and intrusion detection/prevention in response to the recent wave of targeted attacks. After all,

attacks emanating in Beijing, Moscow, or Odessa have to penetrate the network from the outside in. While this is true, ESG believes it is another example of security professionals' historical fixation with perimeter defenses. Yes, these defenses remain important, but a combination of cloud computing, globalization, IT consumerization, and mobility has led to a growing trend toward "de-perimeterization." In short, this means that security defenses for prevention and detection must be increasingly layered across networks, systems, applications, and data throughout the enterprise.

Figure 6. Most Important Security Controls for Protecting Data Against Insider Attacks

Which of the following security controls – if any – would you describe as being the most important for protecting your organization's data against insider attacks? (Percent of respondents, N=707, three responses accepted)



Source: Enterprise Strategy Group, 2013.

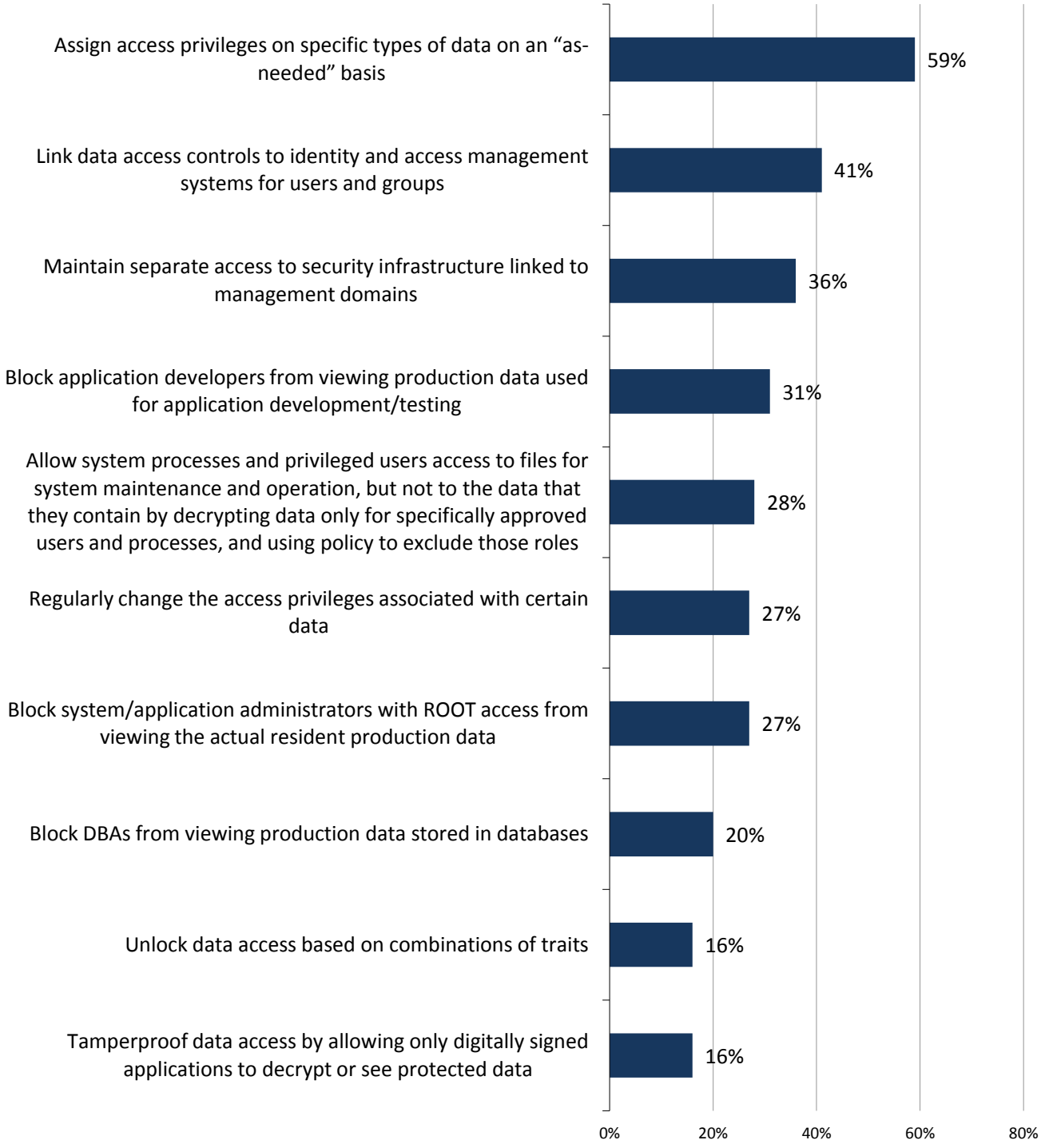
Aside from standard security controls, some organizations are following the information security principal of "least privilege." For the purposes of this report, "least privilege" is defined as:

A basic principle in information security that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions. For example, the restrictive "need-to-know" approach defines zero access by default and then opens security as required. All data in a corporate network would be off-limits except to specific people or groups.

To enforce "least privilege," many organizations are implementing fine-grained access controls in order to limit user access to applications, data, and networks. Alarmingly, 12% of the organizations surveyed are not using fine-grained access controls of any kind. Of the remaining population, 59% assign access privileges to users on an "as-needed" basis. This type of role-based access controls was the most popular response. Security professionals also indicated that they link data access controls to identity and access management systems for users and groups (41%), maintain separate access to security infrastructure linked to management domains (36%), and block application developers from viewing production data used for application development/testing (31%, see Figure 7).

Figure 7. Types of Fine-grained Access Controls Used

Which of the following types of fine-grained access control activities are used by your organization? (Percent of respondents, N=620, multiple responses accepted)



Source: Enterprise Strategy Group, 2013.

Fine-grained access controls are certainly useful, but ESG has observed that they can be difficult to implement, monitor, and manage. To overcome this operational challenge, it is best to use fine-grained access controls exclusively for IT applications and data with "mission-critical" or "sensitive" classifications.

Security Monitoring and Insider Threats

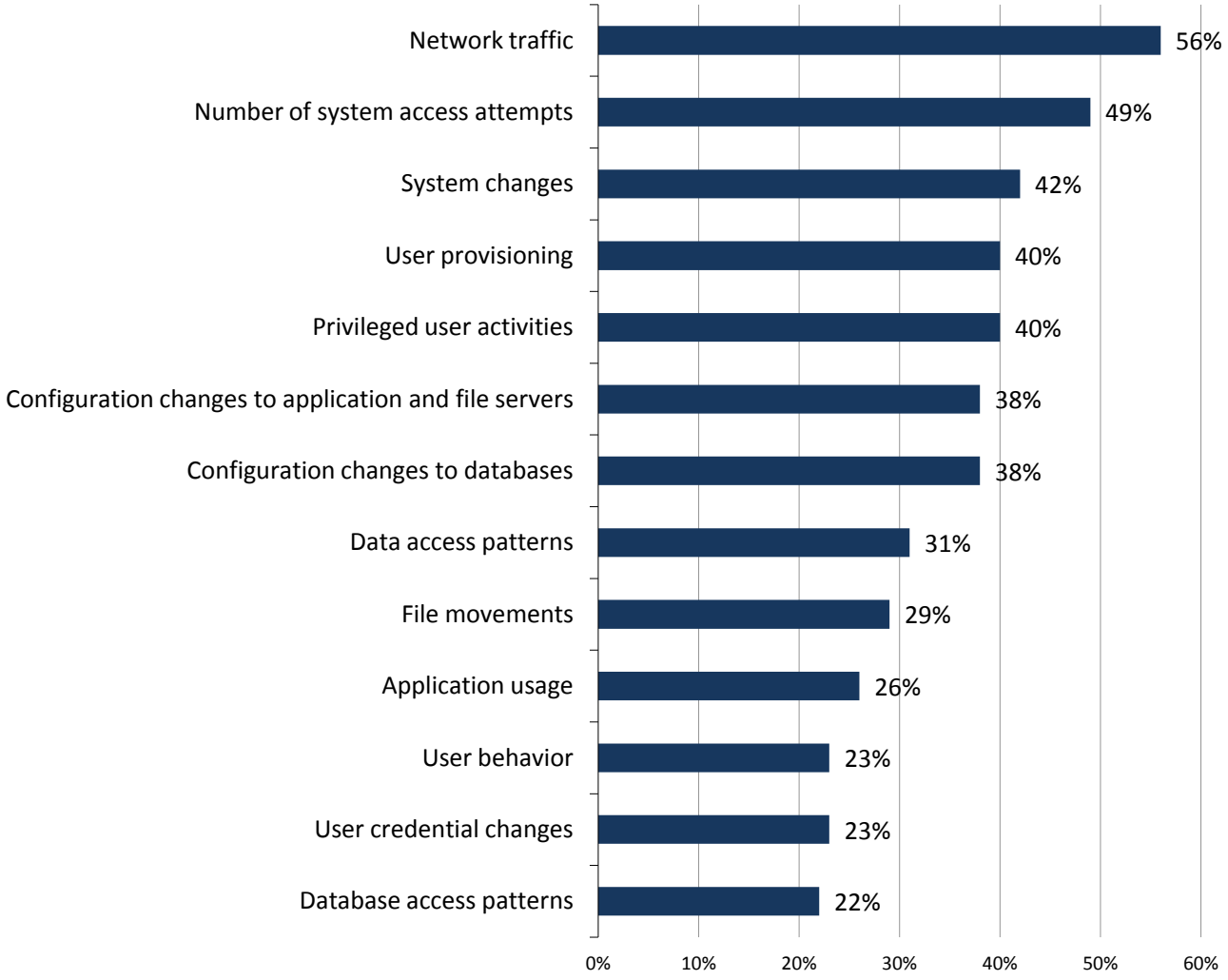
Organizations tend to deploy layers of security controls in order to prevent security breaches and thus mitigate risk. In spite of best efforts however, knowledgeable insiders and sophisticated malware can still elude security controls, compromise critical systems, and ultimately lead to extreme consequences (i.e., DOS attack, data exfiltration, public disclosure, etc.).

To further avoid insider attacks, organizations must complement security controls (i.e., prevention) with security intelligence, IT behavior monitoring, and in-depth analysis. To assess the visibility of insider threats, ESG asked respondents which IT activities they monitor today to identify potential data breaches. Once again, network activity is top of mind—56% say they monitor network traffic (i.e., network flow, applications used, protocols, etc.) to identify and prevent data breaches today, followed by number of system access attempts (49%), system changes (42%), user provisioning (40%), and privileged user activities (40%, see Figure 8).

Security analysts monitor these IT activities looking for the "needle in the haystack" that indicates suspicious behavior. Clearly, network traffic, credentialed users, configuration changes, and data access patterns have grown more voluminous and complex over the past few years as a result of web applications, data center consolidation, and user mobility. Taken together, it's no wonder that 54% of security professionals believe that insider attacks have become more difficult to prevent/detect.

Figure 8. Areas Organizations Monitor to Identify and Prevent Data Breaches

Which of the following areas does your organization monitor in order to identify and prevent data breaches today? (Percent of respondents, N=707, multiple responses accepted)



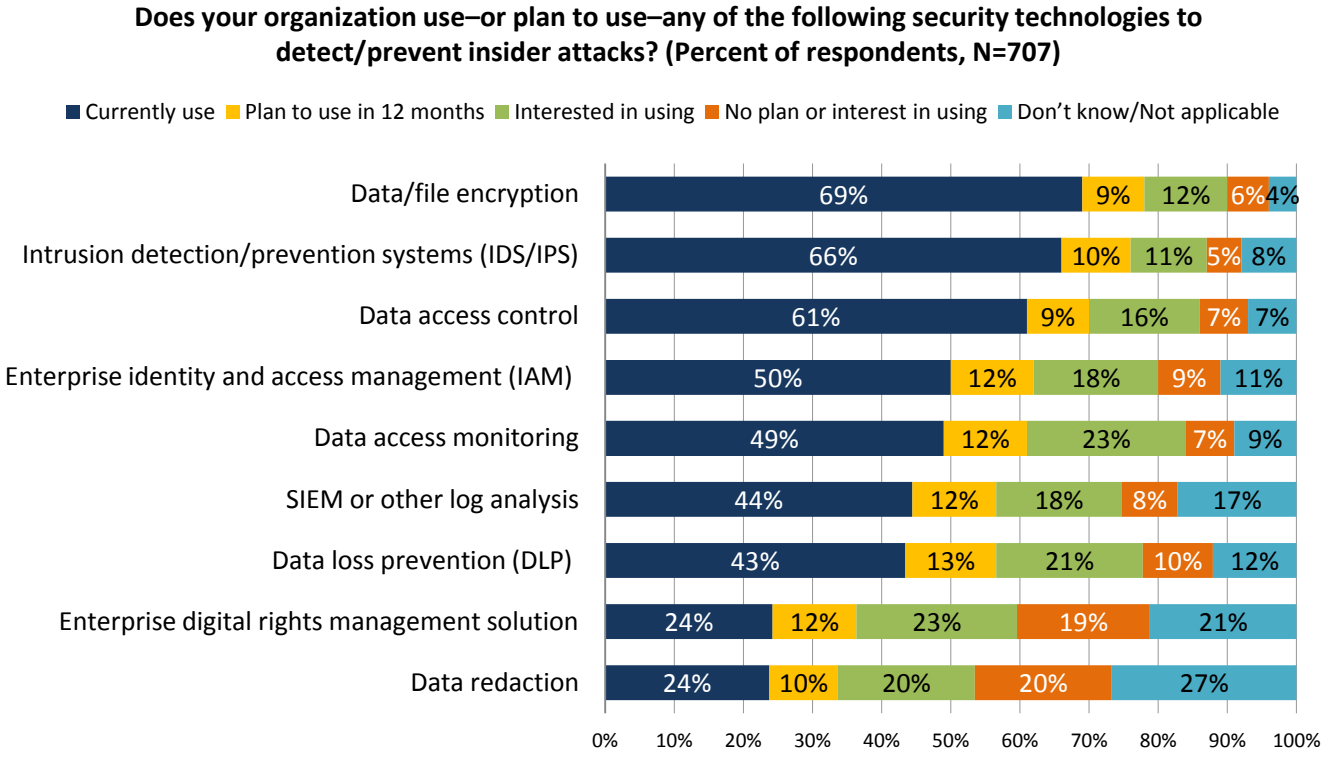
Source: Enterprise Strategy Group, 2013.

Security Technologies Used to Detect and/or Prevent Insider Attacks

Finally, ESG wanted to understand the types of security technologies that organizations depend upon to detect/prevent insider attacks as well as those they plan to deploy in the future. Security professionals pointed to a wide range of technologies across the technology stack, but data/file encryption, intrusion detection/prevention, and data access control (i.e., specific controls for accessing sensitive data) were used most extensively by the organizations surveyed (see Figure 9).

The list is quite interesting in that it is a combination of standard security tools (i.e., IDS/IPS, IAM, SIEM, etc.) and specific types of data security technologies (i.e., data/file encryption, data access control, data access monitoring, etc.). In both cases however, the technologies are a combination of technologies for insider attack prevention and detection.

Figure 9. Use of Security Technologies to Detect/Prevent Insider Attacks



Source: Enterprise Strategy Group, 2013.

Large Organizations Need a Data-centric Security Strategy

Aside from security technologies in use today, Figure 9 also hits at an impending information security trend. Note that a fair number of organizations are interested in using security technologies like enterprise DRM, data access monitoring, and DLP. This data indicates a strategic move toward increasing security protection that resides closer to the data itself.

Just what will this type of solution look like? ESG believes it will surround sensitive data with security lifecycle services including:

- **User and device authentication.** Data security starts with the concept of "least privileges" described previously. To adhere to this principle, data security solutions need a trusted identity infrastructure that can guarantee that the authentication of employees, devices, and privileged users maintains the properties of non-repudiation. This doesn't mean that data-centric security solutions need strong authentication built in, but they must be able to easily integrate into existing strong authentication infrastructure and require multi-factor authentication by default. Aside from user and device identity, these technologies should also offer data classification features and policy enforcement. The overall goal is to be able to align the right user/device with the right data and security protection.
- **User context.** In addition to user and device authentication, data access should take other risk factors into consideration. For example, the CEO should have access to all data when she is connected via the corporate LAN, but it may be too risky to give her access to top-secret intellectual property when she is accessing the files remotely from an Internet café in China. Enterprise organizations need the ability to implement, change, and enforce these kinds of data access policies in order to improve security and automate operations.
- **Data-centric security controls.** Sensitive data confidentiality and integrity depends upon ubiquitous encryption on all key file servers and databases. To streamline operations, organizations should think in terms of tools that can provide centralized encryption and key management with distributed enforcement.

Data-centric security controls should also block IT administrator access to sensitive production data and masking data when it is used by software developers.

- **Continuous monitoring with data security-centric analytics and automation.** Granular access policies and data encryption are effective means for reducing the sensitive data "attack surface," but security professionals must also remain vigilant to detect and minimize malicious insider activities. This requires continuous monitoring of sensitive data access and usage. Data-centric security must provide this type of sensitive data monitoring and alert the security team upon anomalous behavior detection. To provide more extensive security visibility, data-centric security intelligence should also be shared with SIEM and security analytics tools.
- **Pervasive coverage.** CISOs should look for common tools that protect data in file systems and databases, whether they reside on the internal network or in the cloud. Wide coverage will enable companies to create, change, enforce, and monitor consistent data security policies across the enterprise. This can also help the security team reduce risk, adhere to regulatory compliance requirements, and streamline operations.

Conclusion

This paper can be summarized by two important observations:

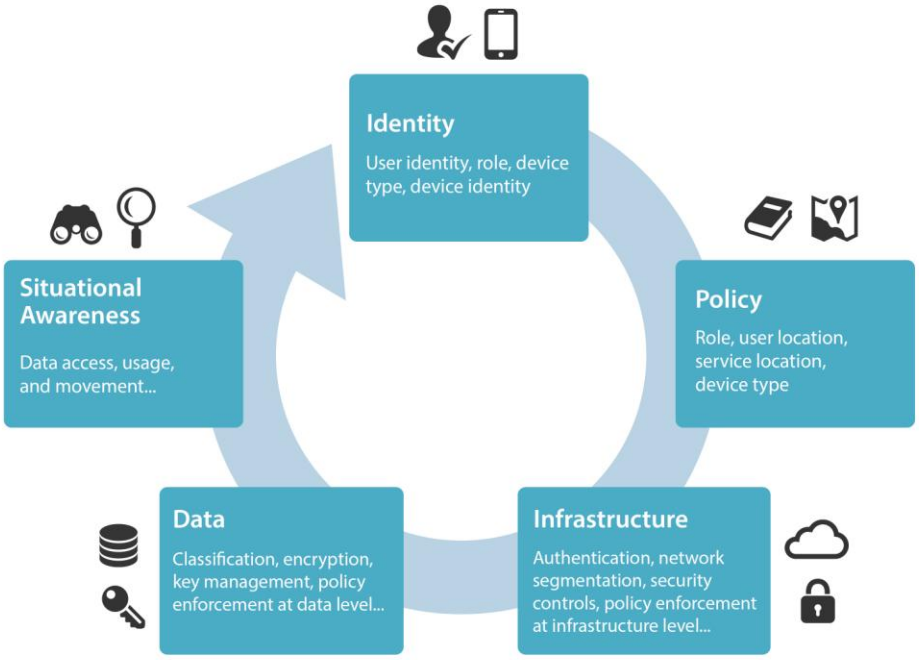
1. Organizations remain vulnerable to an assortment of threats and attack vectors. For insider threats, abuse of privileged user rights by employees is a key concern. Cloud security, network expansion, and APTs that compromise insider credentials are also contributing to this risk.
2. Insider attacks are increasingly difficult to prevent and detect, with organizations feeling that new investments are required to protect against them.

Based upon these conclusions, a determined and motivated insider, or a malware attack that has compromised insider credentials, should have little trouble wreaking havoc by stealing data, interrupting business processes, or disclosing sensitive information to the press, competitors, or cyber adversaries.

Certainly, status quo security controls like firewalls, IDS/IPS, network segmentation, and IAM can help decrease risk by limiting access to IT assets (i.e., applications, servers, networks, data, etc.). That said, these tools should be viewed as a first line of defense only. In truth, a combination of new types of users, cloud applications, and mobile devices continue to drive network de-perimeterization in rapid fashion. As this happens, information security will really move to a data-centric security model dependent upon (see Figure 10):

1. **Identity.** Authentication of users and devices will be strongly considered in data access and entitlements decisions.
2. **Policy.** Organizations will create and manage contextual security policies that allow, deny, or limit access to IT resources based upon situational considerations (i.e., user, location, time, threat level, application/data requested, etc.).
3. **Infrastructure-based policy enforcement.** IT and security infrastructure will help enforce security policies by enforcing rules that limit access to resources (i.e., networks, servers, applications). In this way, contextual server policies will depend upon existing IT and security controls like network segmentation, VLANs, firewalls, ACLs, etc. These infrastructure controls will also extend into the cloud.
4. **Data-specific policy enforcement.** Automated data discovery and classification will align with specific data security controls like data migration (i.e., automated movement of data from insecure to secure repositories), encryption, and key management.
5. **Situational awareness.** Data movement, access, and usage will be continuously monitored and audited. Anomalous/suspicious activities will trigger security alerts.

Figure 10. De-perimeterization Drives Five Key Elements of Information Security



Source: Enterprise Strategy Group, 2013.

CISOs should use the data presented in this report as a warning and a guideline. The report presents an alarming situation where insider attacks (conducted by employees or remote hackers posing as employees) are both routine and extremely damaging. This state of affairs must be addressed soon, but since status quo information security defenses are increasingly ineffective countermeasures, security executives must be willing to try new things and "think outside the box." Given the continuing pattern of cloud computing, mobility, and globalization, a data-centric security strategy may be the best—and only—way to proceed.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com