ESG Solution Showcase

Data-centric Security: A New Information Security Perimeter

Date: March 2015 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: *Information security practices are in the midst of a major transition. Why? Traditional security defenses are no match for targeted attacks that circumvent security controls and steal sensitive data. Furthermore, IT infrastructure (and sensitive data) is more mobile as organizations embrace cloud computing, mobility (i.e., mobile applications, remote/mobile employees, users, etc.), and big data analytics tools. To address modern threats and IT mobility, CISOs must adopt two new security perimeters around identity attributes and data-centric security. In this regard, sensitive data must be continuously monitored for situational awareness and risk management.*

Overview

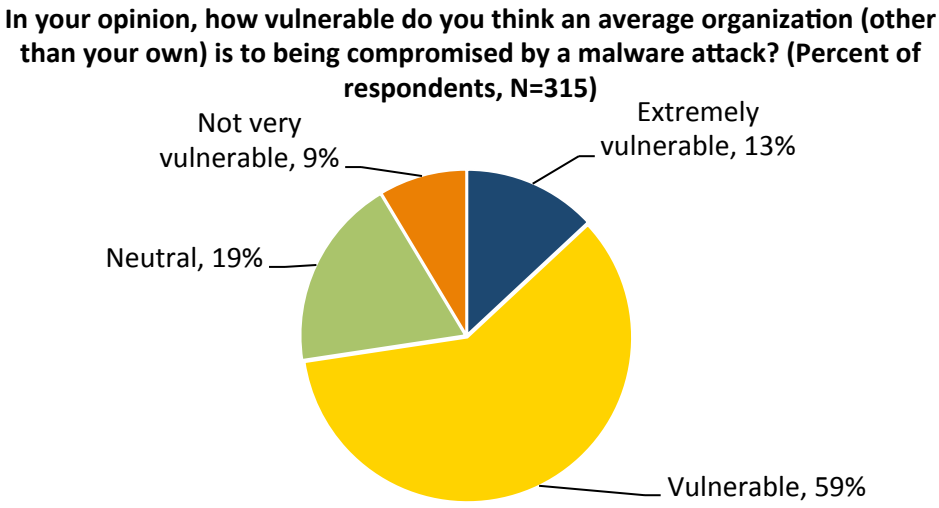
In January 2010, Google announced that it had experienced a damaging cyber-attack the previous year. The attack, dubbed Operation Aurora, was intended to steal Google intellectual property and gain access to several Gmail accounts. Aside from Google, Operation Aurora also targeted numerous others including Adobe, Morgan Stanley, Northrop Grumman, Symantec, and Yahoo.

Operation Aurora also introduced the world to a new concept: the advanced persistent threat (APT). APTs are a type of targeted cyber-attack where sophisticated cyber-adversaries penetrate corporate networks, compromise systems, and steal data over time. This cyber-attack workflow was further described by the Lockheed-Martin Cyber Kill Chain, which progresses through seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on target. Typically, the "actions on target" phase results in sensitive data exfiltration.

In 2014 and 2015, several organizations including Home Depot, Staples, the US Postal Service, Anthem, and Premera suffered damaging data breaches where sensitive data was stolen. Alarmingly, things seem to be getting worse, not better. According to ESG research, a majority of security professionals working at enterprise organizations (i.e., more than 1,000 employees) believe that many organizations remain extremely vulnerable or vulnerable to being compromised by a malware attack (see Figure 1).[1] The results can be devastating: Target estimated last year that the 2013 data breach would cost $148 million, while the Sony Pictures breach will likely lead to years of litigation.

[1] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013.

Figure 1. Perceptions of Average Organization Malware Vulnerability



Source: Enterprise Strategy Group, 2015.

Situational Analysis

Most cyber-adversaries approach their attacks with a distinct objective: steal valuable data as a means for industrial espionage or illicit profits. In addition, insiders pose a perpetual threat. Insiders can inadvertently help hackers obtain credentials via social engineering or initiate their own attacks by commandeering sensitive information for monetary gains, revenge, or other personal objections. Of course, this is well understood by cybersecurity professionals, yet these harmful data breaches continue on a fairly regular basis. Why? Large organizations remain too vulnerable because:

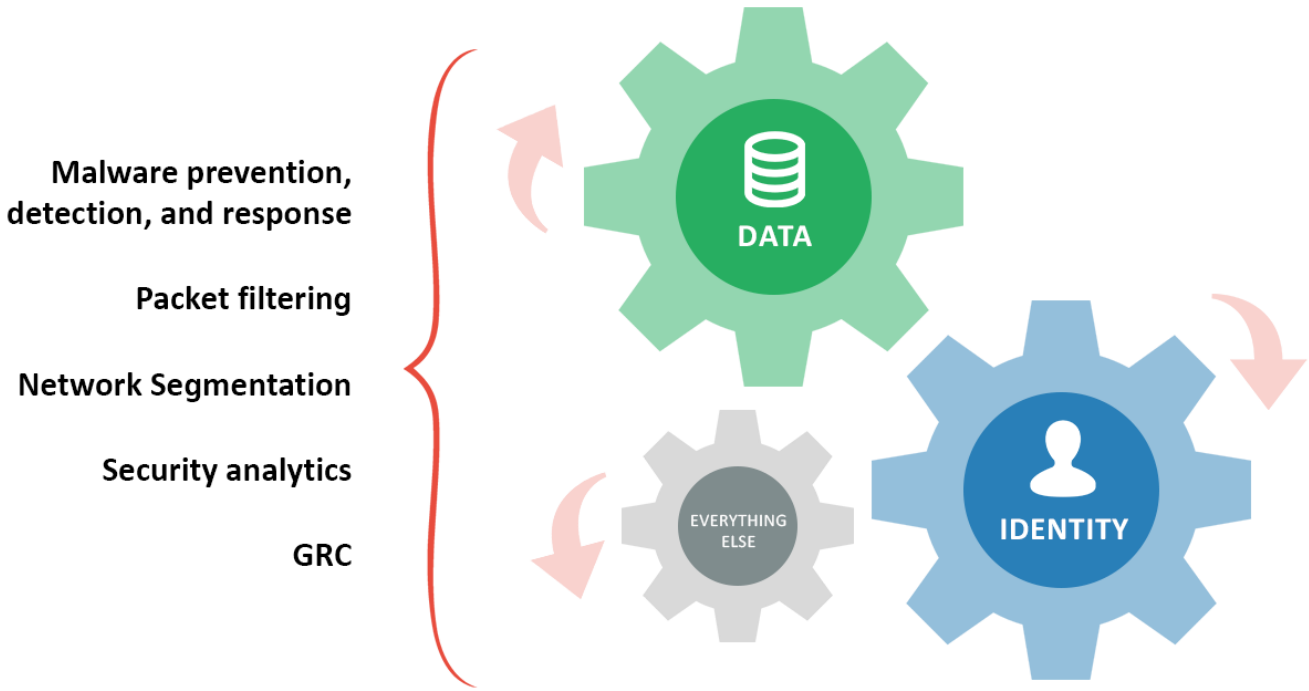
- **Security defenses focus on networks and endpoints.** To defend against APT-style attacks, large organizations rely upon layers of defensive technologies deployed on networks and hosts. These defenses include firewalls, malware gateway appliances, antivirus software, and homegrown security analytics. Standard security technologies can be effective for blocking obvious malware and identifying anomalous behavior, but it is not unusual for APTs or malicious insiders to simply circumvent these defenses and exfiltrate sensitive data. Cyber-adversaries often avoid detection because attack patterns are designed to look like authorized users accessing sensitive data. Network and endpoint technologies looking at packets, files, and flows have limited visibility and understanding into what's happening with the data and the users accessing the data itself.
- **Sensitive data is stored everywhere.** Sensitive data tends to proliferate across the enterprise as it is replicated across databases, copied by employees, and used by software developers to emulate production settings. This problem continues to grow more cumbersome as large organizations move workloads to the cloud, embrace mobile applications, and implement big data analytics technologies like Casandra, Hadoop, MapReduce, and NoSQL. Given this situation, determined cyber-adversaries move laterally across networks, look for vulnerable copies of sensitive data, and then complete their crimes with relative ease.
- **Sensitive data monitoring can be based upon manual processes and assorted reports.** While security teams capture, process, and analyze system logs and network flows, many lack this same level of automated visibility into their sensitive data. In other words, many organizations don't have a clear or real-time understanding of where their sensitive data copies are, who has access to them, and what users are doing with the data. In lieu of this information, CISOs may be "flying blind" without the information necessary for creating the right data security controls.

While these issues make it difficult to stop an APT, they also greatly limit the ability to detect and respond to internal attacks. A malicious individual (i.e., employee, contractor, business partner, etc.) with legitimate access to sensitive data can easily conduct a "low-and-slow" attack by siphoning off a few sensitive files each day. For example, PFC Bradley Manning, an intelligence officer with legitimate access to classified information slowly copied over 200,000 classified documents and then provided them to WikiLeaks. This type of carefully crafted tenacious attack will often go unnoticed as an insider slowly accumulates more and more data for nefarious purposes. The security team frequently remains in the dark until an attack is completed and massive damage is done.

Organizations Are Establishing New Security Perimeters

Large organizations face a difficult situation in a number of areas. The threat landscape continues to grow increasingly dangerous while a wave of new technologies further distribute sensitive data across devices, locations, and data repositories. In the past, many organizations based their security defenses on network- and host-based controls like perimeter firewalls, network segmentation, and antivirus software, but rapid transitions in IT infrastructure make traditional security gates much less effective. As IT changes occur and organizations lose some control over IT, CISOs must increase their oversight in two areas: identity and data-centric security (i.e., data security controls and analytics). In fact, ESG considers these areas as new security perimeters (see Figure 2). Yes, traditional security technologies still play a supporting role, but CISOs will need to focus on identity and data-centric security, and supplement their renewed focus on identity and data-centric security with traditional endpoint/network defenses and security analytics solutions.

Figure 2. Identity and Data-centric security: The New Security Perimeters



Source: Enterprise Strategy Group, 2015.

ESG has observed that many organizations are already moving in this direction with "crown jewels" security projects. In this way, enterprises focus on identifying and protecting sensitive data by limiting user access with least-privilege rules, multi-factor authentication, privileged accounts controls, and by monitoring sensitive data access patterns for anomaly detection. Given this momentum, ESG believes that the market for identity management and data-centric security solutions will grow precipitously over the next three to five years.

What's Needed for Data-centric Security?

While large organizations reinforce their identity management, they must also get their arms around the scale and scope of sensitive data residing across their networks, cloud deployments, and disparate data repositories. To accomplish this, CISOs need the right data security intelligence tool for:

- **Data discovery.** With sensitive data strewn throughout internal networks and external clouds, security professionals need efficient tools to scan systems and databases to discover all copies of sensitive data wherever it resides.
- **Data classification.** To protect sensitive data, organizations need to enforce a rigorous taxonomy for data classification. The "crown jewels" security projects described previously often adhere to a binary classification schema: Data is either sensitive and thus demands additional security controls and oversight, or it is not sensitive and needs no additional protection. This simple model should be enhanced over time to provide more granular classification context and protection for different types of data.
- **End-to-end visibility.** Data discovery and classification projects are often limited to particular data centers, servers, or databases. This makes sense for early stage projects, but organizations ultimately need a more comprehensive perspective. To accomplish this, CISOs need to know about sensitive data anywhere it resides—inside or outside the corporate network.
- **Data security analytics for risk management.** Compliance, privacy, and security are based upon security professionals knowing where sensitive data is, who has access to it, and what they are doing with it. This is not a static requirement that can be satisfied with occasional audits and scans. Rather, CISOs need to collect, process, and analyze data-centric security information continuously to make the appropriate risk management decisions in real time.

Once CISOs know where sensitive data resides and assess risk, they can apply security tactics and implement the right data security controls. As risks change, they can fine-tune existing controls, deploy additional safeguards, or move sensitive data to more secure locations. Finally, data security analytics will likely adopt machine learning algorithms for anomaly detection over time. When an employee suddenly starts downloading sensitive data on a daily basis, data security analytics will alert the security team to launch a more thorough investigation or take some type of risk mitigation action.

Informatica Secure@Source

Data management pioneer Informatica recently introduced a new data-centric security product offering called Secure@Source. Simply stated, Secure@Source is designed to help CISOs identify where sensitive data resides; assess sensitive data history (i.e., access patterns, provenance), proliferation, and protection status; and identify risks to sensitive data in real time. Informatica Secure@Source provides a sensitive data "heat map" that assesses risks to data based upon its sensitivity, its protection (i.e., encryption, masking, anonymization, etc.), proliferation, etc. ESG believes that this type of continuous monitoring of sensitive data could help organizations better manage and protect sensitive data at rest, data in motion, and data in use by applying the right level of controls and oversight based upon real-time risk management calculations. In this way, Informatica Secure@Source can also help streamline compliance audits, improve risk management, and decrease the likelihood of a devastating data breach.

The Bigger Truth

CISOs have spent years building a defense-in-depth security architecture to safeguard networks and systems. Given the changing threat landscape and IT architecture, it's time that they create a layered defense surrounding their most precious digital asset: sensitive data.

An old management saying goes, "You can't manage what you can't measure." In other words, enterprises can't implement the right data security controls if they don't have a complete understanding of where sensitive data resides, who has access to it, and how it is impacted by new types of threats and vulnerabilities.

It's time for a vast improvement in data-centric security that includes data discovery, classification, end-to-end visibility, and data security analytics for risk management and situational awareness. Armed with these capabilities from vendors like Informatica, CISOs can greatly enhance sensitive data security, regulatory compliance, privacy policies, and operational efficiency.