SilverSky
SECURITY FROM THE CLOUD

White Paper

Navigating the Pitfalls of Attack Prevention: A Look at Employee Perception

Situation Overview

In today's day of persistent and ongoing targeted attacks, the need to prevent and prepare for the eventuality of a security breach is of paramount importance. More sophisticated threats, including targeted attacks, zero-day attacks and advanced persistent threats (APTs) are more commonplace and becoming harder and harder to predict and defend against. A new form of protection is needed to take security beyond simple detection to a more complete preventative approach.

According to research from the Online Trust Alliance (OTA) 2014 Data Protection and Breach Readiness Guide, in analysis of nearly 500 breaches in the first half of 2013, 89 percent could have been avoided had simple controls and security best practices been implemented.

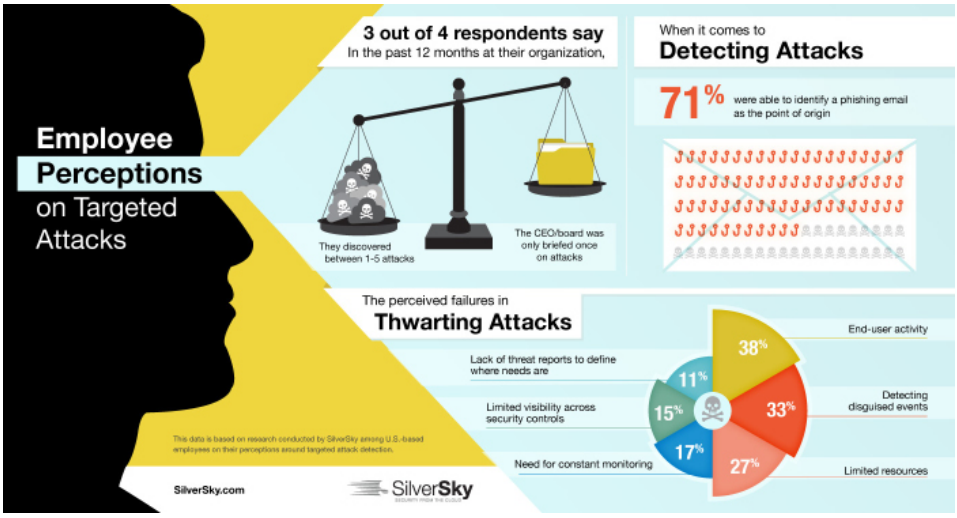
Targeted cyber-attacks, similar to the recent breaches that hit Target, Neiman Marcus and others, are on the rise and organizations are scrambling to up their defenses to ensure digital assets are secure. This protection starts at the ground level with employee awareness of security issues and vulnerabilities.

A Study on Perceptions

In order to understand how employees perceive the abundance of attacks targeting their organizations and the ability to defend against them, we surveyed nearly 200 U.S. based employees on their perceptions around targeted attack detection. The study reveals several inadequacies in detecting and blocking targeted cyber-attacks. In fact, most employees (78 percent) said their organization has fallen victim to 1-5 known attacks in the last 12 months.

The data also indicates that the majority of attacks against organizations have been targeted phishing attacks. Of note, 71 percent of respondents identified a phishing email as the point of origin.

How employees perceive targeted attacks



SilverSky Labs VP Brandon Edwards says, "It is clear that antivirus alone is not enough to address today's sophisticated threat actors." It's widely known that cyber criminals will use multiple methods, such as phishing emails and phony websites, to lure unsuspecting employees into sharing their personal information or clicking on a less than legitimate link.

Corporate Headquarters SilverSky 440 Wheelers Farms Road Suite 202 Milford CT 06461

Other industry findings claim that businesses suffer an average of nine attacks per year, which tells us something we have been regrettably aware of: many attacks go undetected – and unknown compromises are far worse than the known ones.

According to the study, some of the barriers preventing organizations from doing a better job in monitoring for, collecting and analyzing attack information include:

+ Cost (64%)
+ Time constraints (44%)
+ In-house knowledge/skill-sets (42%)

SilverSky Level III Analyst and Team Lead, Richard Westmoreland, says the identified barriers to threat prevention highlight the perception problem.

> *"The return on investment with additional in-house knowledge/skill-sets actually reduces final cost. Fortunately, organizations can benefit from using solution providers like SilverSky, which are equipped with advanced Labs that can provide outbreak intelligence and act as an extension of their IT department."*

The study also reveals that the biggest perceived point of failure in catching targeted attacks lies with a company's end users (38%). Other factors that respondents identified as barriers to protecting against attacks were limited in-house resources (27%), and the inability to detect events disguised behind normal processes, files and traffic (33%).

Other areas of perceived inadequacy in an organization's capacity to protect its network:

+ Socially Engineered Trojans (31%)
+ Botnets (25%)
+ Unpatched Exploits (19%)
+ DDoS Attacks (12%)
+ Zero-day Attacks (12%)

Despite widespread knowledge that the majority of respondents' organizations were victim to a targeted attack within the last year, the study also found that 76 percent of employees claim their board of directors and/or CEO was only briefed once in the same time period regarding attacks to their organization.

> *"Lack of CEO involvement in security matters is not uncommon," added Westmoreland. "The reality is C-Level awareness of targeted attacks is insufficient, and quite shocking considering heightened awareness over the last few years around security and the impact of a data breach. Given the high profile nature of the recent breaches we fully expect this awareness – and the demand for managed security services to climb in 2014."*

Corporate Headquarters SilverSky 440 Wheelers Farms Road Suite 202 Milford CT 06461

SilverSky's Targeted Attack Protection (TAP)

SilverSky's Targeted Attack Protection (TAP) is a highly advanced cloud-based service that stops targeted attacks, spear phishing, "longline" phishing, and advanced zero-day exploits without relying on anti-virus signatures.

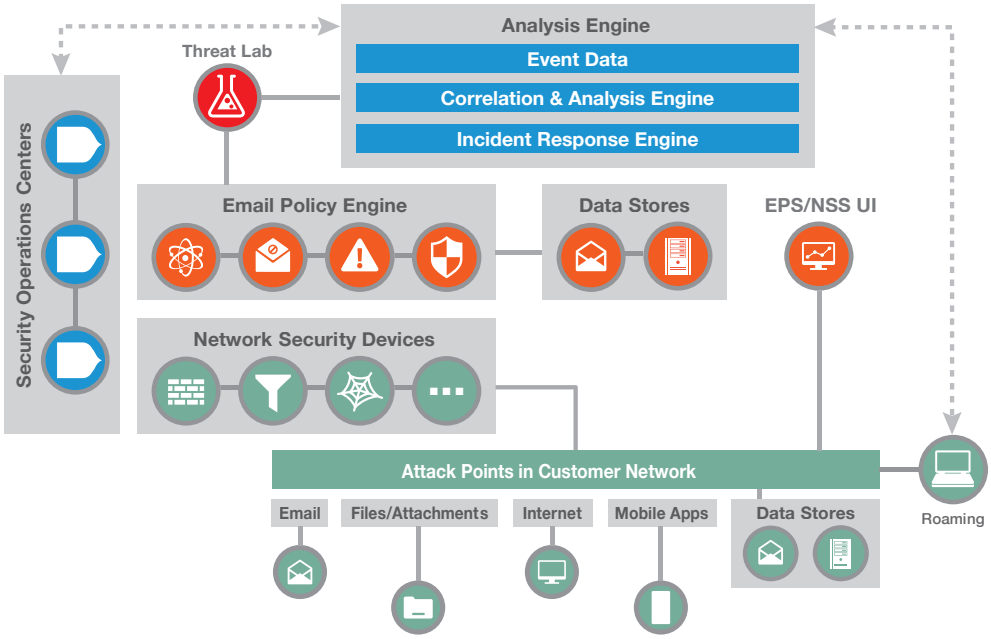
Email is the centerpiece of business communications. It is also the single most important entry point for targeted attacks, spear phishing, "longline" phishing, and advanced zero-day exploits. New data breaches are uncovered almost daily – any one of which can jeopardize your company, place your intellectual property at risk, and cause monetary and reputational damage in minutes.

Cyber-criminlals are increasingly aggressive, well-funded and persistent. No company can ever be perfectly safe from the most determined attackers. But SilverSky's Targeted Attack Protection (TAP) service provides an essential margin of safety for customers seeking to prepare for specific and unusual attack scenarios. TAP arms CIOs and IT managers with new, comprehensive detection techniques to reduce their company's attack surface and vulnerabilities. And because we address the entire kill chain through our complementary portfolio of managed services, we offer more protection than any other solution provider.

Reduce Cost and Complexity	+ SilverSky's Targeted Attack Protection (TAP) is a completely cloud-based service, there is no need to purchase or manage costly hardware or software and no integration or migration is required.
Outsource Time-Consuming Tasks	+ Enjoy 24x7x365 technical support, monitoring, and reporting with Level 2 and 3 technicians
Leverage our Team of Experts	+ SilverSky Labs + 3 Security Operations Centers + SilverSky Labs leverages a massive set of transactional data - nearly 500 million security events and over 50 million emails a day across 6000+ customers - to correlate, analyze and proactively push preventative rules to our customer base. The net result is increased peace of mind and the most up to date protection possible.

Corporate Headquarters SilverSky 440 Wheelers Farms Road Suite 202 Milford CT 06461

TAP in Action



Benefits of SilverSky's Groundbreaking Targeted Attack Protection

+ TAP significantly reduces security exposure for companies and protects them from reputational damage and intellectual property theft from cyber threats with fast and effective attack detection, containment, and response.

+ SilverSky's innovative analysis engines and sandbox simulators quickly identify zero-day malware, malicious network attack activities. TAP pinpoints the probability of an imminent attack or zero-day exploit, confirms the attack is in progress, and suspends message traffic.

+ TAP generates dynamic threat analysis reports for deep inspection and counter-measure activities. And, IT admins can conduct real-time quarantine and remediation of zero-day email attacks.

+ SilverSky Targeted Attack Protection fully integrates with and enhances all SilverSky Email Protection Service solutions for layered defense and real-time correlation. TAP can be deployed rapidly and is easily configured and controlled via the intuitive SilverSky Management Console.

Corporate Headquarters SilverSky 440 Wheelers Farms Road Suite 202 Milford CT 06461

Summary

Perceptions are accurate in indicating the need for more advanced protection. Attackers will constantly try to break down your barriers. The ongoing need for continued awareness, prevention solutions and the critical human element is always going to pose a challenge. Without constant monitoring and expert, 24x7 analysis, as another critical layer to complement security technologies, organizations can never be fully protected.

CEOs, CIOs and IT managers need a better way to equip themselves to prevent today's ongoing and increasingly sophisticated threats. One way to ensure protection is to invest in technologies that reduce security exposure and protect against reputational damage and intellectual property theft with fast and effective attack detection, containment and response.

It is clear that further preparation for these ongoing and increasing outside attacks is needed and advanced new protections need to be put in place to counter the advancing state of adversaries.

About SilverSky

SilverSky is the leading independent cloud-based managed security services provider. Our Security-as-a-Service platform delivers cloud-based software and managed services, such as Email Protection Services, including the recently launched Targeted Attack Protection, advanced Data Loss Prevention, Network Security Services, and Managed Application Services, that protect critical information simply and cost effectively. By tirelessly safeguarding our customers' most important information, we enable growth-minded leaders to pursue their business ambitions without security worry. Our growing customer base includes 6,000 organizations in the financial services, retail, healthcare, energy, critical infrastructure

Corporate Headquarters SilverSky 440 Wheelers Farms Road Suite 202 Milford CT 06461