“Highly publicized breaches rarely result in meaningful security budget increases,” says John Pescatore. “However, they invariably provide strong lessons learned in how to avoid the same problems—often by spending the same amount of money, but focusing on spending in the right places.”

“43% of companies had a data breach within the last year,”
www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197


---

Target, Home Depot, Michaels, PF Chang’s, Jimmy John’s, Goodwill, Sheplers—the list goes on … and on…. In fact, 43 percent of retailers have experienced data breaches thus far in 2014.¹

In September 2014, SANS Institute Director of Emerging Security Trends John Pescatore joined Erick Ingleby, LogRhythm Product Manager, to discuss the ongoing issues of retail security, including point-of-sale (POS) security, in the “Hardening Retail Security: Why and How to Prevent Breaches and Attacks” webcast. The archived webcast, located at www.sans.org/webcasts/hardening-retail-security-prevent-breaches-attacks-98772, offers a number of insights into the root causes of the stream of data breaches and some practical advice for helping prevent them.

Audience members participated in a quick poll during the webcast to share their thoughts around several key areas of retail and POS security: budgets, whether they perform behavioral baselining and whether they collect endpoint forensic data from POS devices.

### Budgets

Does effective security correspond to a larger budget? For many in security who see a big part of their budgets siphoned off for compliance, as much as 38%,² a smaller budget could impact how effectively their security team and tools work. SANS posted the following to listeners of the webcast:

**Has your organization seen increased, decreased or no change to your security budget since Target’s breach became public?**

With the Target breach occurring toward the middle of the budget year, we would expect that by now we would be seeing some changes in budget allocations for security. It is noteworthy that none of the respondents indicated that their security budget was decreased. Figure 1 illustrates the results.

It appears that almost a year after the highly visible Target breach, the majority of practitioners and security staff (69%) are working with the same budget allocation they had previously. SANS will take a closer look at IT spending in a 2015 survey.

---

¹ “43% of companies had a data breach within the last year,” www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197

Behavioral Baselining

The polling then moved to specific activities typical to the threat management arsenal. The first, behavioral baselining, refers to the development of the baseline or standard against which all subsequent changes are measured and analyzed. In the case of POS systems in the retail environment, this means that once a baseline is established for retail networks, authentication and processes, anomalies can be detected and analyzed to determine which are potentially harmful. SANS asked:

**Does your organization have any method of performing behavioral baselining of POS systems running processes, user authentications and file accesses?**

A response of “Yes” means organizations are prepared to identify anomalies; “No” means they have no way to distinguish normal from potentially malicious behaviors. According to the SANS community attending the webcast, 70% do not currently perform such baselining (see Figure 2).

This lack of a baseline standard from which to detect subsequent anomalies could result in attacks, illicit activity or unauthenticated users being undetected, because their behavior is not identified as unusual. The SANS Incident Response Survey recommends baselining as a method to learn about your network and make it easier to detect abnormal traffic and behaviors.

Figure 2. Use of Behavioral Baselining
Endpoint Forensic Data

The polling continued to the final question:

Which method do you typically use/rely on to collect endpoint forensic data from POS devices?

In this informal poll, 70% noted that they do not collect forensic data from the operating system's audit logs of POS devices, and only 30% get data from the endpoints themselves, as illustrated in Figure 3. Of course, until the recent spate of POS hacks and attacks, perhaps there was no perceived need to do so.

Now, of course, the IT and security communities know that it is essential to collect forensic data to aid in resolving and prosecuting breaches. Log data can show registry changes that result from malware infections. Authentications can be found in POS log data as well, confirming who is logging in and when they are active on specific terminals. That information can alert security teams to off-duty employees logging in or downloading data, whether maliciously or not. And log data can indicate if employees or others are siphoning off data from the terminals—the cause of many recent breaches.

Endpoint data can offer additional insights, including who is using them, who the devices are talking to on the network and what kinds of info are exchanged.

The webcast, archived at [www.sans.org/webcasts/hardening-retail-security-prevent-breaches-attacks-98772](http://www.sans.org/webcasts/hardening-retail-security-prevent-breaches-attacks-98772), offers many insights into retail and POS security. These questions specifically indicate that even as the industry increases awareness of vulnerabilities of millions of POS terminals, practitioners are still learning about ways to improve security. Baselining to enhance the ability to distinguish normal and abnormal behavior and collecting forensic data to assist in the incident response process are key steps all organizations can take.

“As the Critical Security Controls effort has shown, focusing on the most effective security controls can increase security without increasing spending,” according to John Pescatore. “Making better use of existing security data to more rapidly and accurately detect attacks in process can be a force multiplier for security budgets.”
SANS would like to thank this paper’s sponsor:

![LogRhythm Logo]