Summary:

Eddie Bauer retail clothing store, a company almost bought out by Jos. A Bank in 2014 for 825 Million dollars, and a company with 370 stores several in Utah was hacked. Eddie Bauer finding out about the hack in July of 2016 which appeared to stretch back to January of 2016. Malware was found on Eddie Bauer Point Of Sale Machines(POS), which captured credit card and debit card Information. Purchases made online were not affected by the malware. Eddie Bauer is working with the FBI and other Forensics firms to determine what happened and to prevent further incidents from occurring in the future.

My Thoughts:

This isn't the first time this has happened to a major company like Eddie Bauer and it won't be the last. The article mentions the data breach at Target that happened late 2013 to early 2014. We learned about this attack in our Hacking and Security Vulnerability Management Class last Spring Semester. Where Target was also targeted(haha) by a Malware based attack to their POS systems also grabbing banking card numbers, an estimated 40 million credit card numbers had been stolen. Target spent over $61 Million dollars in lawsuits as a result of this breach, and Targets stock went down as well. Also unknown losses in future business. What I mean is this also affect current business with a stigma of poor Information Security which causes losses in revenue. With this hack of wendy’s which happened last July, I still dont feel comfortable about eating at a Wendys yet. (Maybe it is the food but point still valid :) ) Wendy’s in July of 2016 also had a POS Malware attack where attackers got credit card information, which affected 12 stores in Utah. One next to my work in Lehi; one in my home town; and one next my house here in orem. Major losses happen as a result of breaches.

Which leads me to the point I’m trying to make. I’m going to preface by saying no system can be completely secure. But by saying this why dont companies learn from other companies mistakes like Target and Wendy’s. Both instances very recent and avoidable including Eddie Bauer. This leads me into my next point why didnt Eddie Bauer, Target, Wendy’s, and every other company that has been hit by a POS attack have monitoring for their POS system. In the case of Target it took Target a months to react and stop the credit card data from being stolen, and it wasnt even caught by Target, it was caught by the FBI. Now that is embarrassing. In the case of Eddie Bauer was never reported, but I assume it was the FBI’s fraud division that caught the issue, and also took months to discover the breach. A majority of my job is to monitor the company I work for site for issues. If I missed something of that magnitude at work I would be fired for sure.

The statement given to us by Mike Egeck CEO of Eddie Bauer’s, “part of a sophisticated attack directed at multiple restaurants, hotels, and retailers.” Is not very comforting to me. Which makes me ask wonder are we more reactive or proactive in dealing with Cyber Security?

The funny thing is in each one of these incidences of a major company being hacked, and disclosing the breach to the public. They all look and sound so similar to one another. I really hope we don't continue to see large amounts of companies fall prey to POS Attacks.

<https://www.youtube.com/watch?v=Jov0LADiX_Q>

<https://www.ksl.com/?sid=40562753&nid=148>

<http://krebsonsecurity.com/2016/08/malware-infected-all-eddie-bauer-stores-in-u-s-canada/>

<http://bgr.com/2014/03/13/target-data-hack-how-it-happened/>