Using RSA Archer to support PCI Compliance by Ted Dziekanowski – CISA, CISSP, RSA-Archer Administrator

To say the Target store chain has had a bad month would be an understatement. As of the time this post the estimated loss due to data breach that occurred starting sometime around Black Friday was approaching [$680 Million dollars](http://www.minnpost.com/glean/2013/12/one-estimate-cost-target-data-breach-could-hit-680-million) and that may not be the final number. Given the proclivity of state’s authority generals to sue over consumer losses, banks recovering the losses remediating customer losses and reissuing cards, the loss of sales and reputation we may be witnessing the first billion dollar breach. Even if mitigated by data breech insurance this event with likely have a significant impact on Target’s earnings on in the time of year when most retailers make the profits that sustain them the rest of the year.

While the actual case of the breech is yet to be determined, this much is known. The Point of Sale System (POS) was the target. It may have either been poorly patched or vulnerable web servers that live on these systems was exploited. The attack was very well planned and executed as demonstrated by the way the stolen information was distributed. A common means of dealing with stolen information is for credit cards companies to identify purchases not clearly identifiable as being in the normal location of the card holder as being potentially fraudulent. In the case of the Target breach, credit card and debit card informations ant the associated csv numbers were being sold in markets where the card holders resided. This is forcing some banks to limit the amount that can be used on debit cards. The attack, as far as we know only impacted the POS systems and not the online sales of Target. Speculation is an insider may exposed the POS to a very sophisticated crime [syndicate](http://www.washingtonpost.com/business/technology/answers-to-questions-about-the-target-data-breach/2013/12/19/bde98d30-68d4-11e3-997b-9213b17dac97_story.html).

Second guessing or speculation is not the intent of this article. What every organization who takes credit cards needs to be asking themselves right now is how I as the head of my company reduce the substantial risk that these new Advanced Persistent Threats are presenting to my organization and how can I get in front of the inevitable regulations that will result from this event. RSA Archer has a specialized solution to deal with PCI compliance and that’s what we will be examining in this post.

## What is PCI Anyway?

The Payment Card Industry Data Security Standard (PCI-DSS) is in its third revision as of [November 2013](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf). The standard’s primary objective is the secure transmission of data between merchants and banks issuing credit cards. Other covered entities include every entity involved in the process including processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Non-compliance can lead to a firm not being able to accept credit cards for business transactions, a death sentence to most firms. PCI-DSS has 12 high level requirements all of which are nicely managed by RSA Archer’s eGRC suite of solutions.

### Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use system defaults for system passwords and other security parameters

### Protect Cardholder Data

1. Protect stored cardholder data
2. Encrypt transmission of cardholder data across open, public networks

### Maintain a Vulnerability Management Program

1. Protect all systems against malware and regularly update anti-virus software or programs
2. Develop and maintain secure systems and applications

### Implement Strong Access Control Measures

1. Restrict access to cardholder data by business need to know
2. Identify and authenticate access to system components
3. Restrict physical access to cardholder data

### Regularly Monitor and Test Networks

1. Track and Monitor all access to network resources and cardholder data
2. Regularly test security systems and processes

### Maintain an Information Security Policy

1. Maintain a policy that addresses information security for all personnel

Now if are familiar with ISO 27001 and 27002 you should immediately notice that many of the controls specified in those documents are requirements in PCI-DSS 3.0. That being said you could download the standard off the internet and construct a word document and excel spreadsheet and be done with it or so you may think. You still need a way to manage and communicate policies but more important are the exception requests you’re sure to receive. There is also the problem of asking the right questions when performing the initial assessment of the environment. There is no centralized repository of content that reflects not only your efforts but a secure place to place evidence of satisfying the requirements of PCI-DSS. Changing your policies should the PCI-DSS standard changes will not be easy. You are also missing one other key feature necessary to properly allocate resources properly, a Risk Management tool. No not only is Archer the better way to manage PCI with Archer’s dedicated solution for PCI but by using a data feed with the right monitoring tools you can better understand any exfiltration attempts on your PCI data.

## Implementing the Archer PCI Solution

First off if you are unfamiliar with what the RSA Archer product does let me give a brief summary. In some respects it’s like Microsoft’s SharePoint product in that it sits on top of a Microsoft SQL server. It offers the data to end users via a web interface that can be customized to display a high level view of compliance for senior management. If you are at all familiar with Domino, Archer has sections that can either be expanded or contracted depending on requirements. I can also conceal data at the record or field level also as required. More importantly RSA Archer comes configured in the PCI solution with authoritative sources that can be used in Questionnaires that will not only help you figure out what needs to be done but the amount of risk your organization is exposed to giving you the opportunity to make strategic decisions on accepting, mitigating or transferring the risk identified in control gaps. You also get workflow to manage the processes that are going to be part of managing the PCI solution.

### Part One – Defining the Scope

What you need to do to satisfy the PCI requirements and what you need Archer to do depends in large part on the volume of transactions you perform annually. As pulled from the [PCI Merchant Compliance Standards](http://usa.visa.com/merchants/risk_management/cisp_merchants.html#anchor_4) here are the thresholds for testing.

|  |  |  |
| --- | --- | --- |
| evel / Tier1 | Merchant Criteria | Validation Requirements |
| 1 | Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region 2 | * Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”) or Internal Security Assessor (“ISA”) if signed by officer of the company * Quarterly network scan by Approved Scan Vendor (“ASV”) * Attestation of Compliance Form |
| 2 | Merchants processing 1 million to 6 million Visa transactions annually (all channels) | * Annual Self-Assessment Questionnaire (“SAQ”) * Quarterly network scan by ASV * Attestation of Compliance Form |
| 3 | Merchants processing 20,000 to 1 million Visa e-commerce transactions annually | * Annual SAQ * Quarterly network scan by ASV * Attestation of Compliance Form |
| 4 | Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually | * Annual SAQ recommended * Quarterly network scan by ASV if applicable * Compliance validation requirements set by merchant bank |

Installing the RSA Archer PCI 2.1 solution will also require

* RSA Archer Platform 5.3.1 or later
* All of the following licenses:
  + RSA Archer Compliance Management
  + RSA Archer Enterprise Management 4.0
  + RSA Archer Policy Management 4.0

The implementation of these solutions are not trivial exercises and before beginning the installation process or constructing a statement of work I’d strongly recommend taking the RSA Archer administration classes and would also consider the separate policy and risk 2 day classes for the best results. Several Practitioner guides are available on the RSA Archer Community pages and reading the latest administration guides will also help you to prepare questions about integrating Archer into your current environment to leverage tools already in your infrastructure.

Other steps in setting up this solution will include once the required Archer components are installed included

* Defining Groups and Access roles for the solution
* Installing the latest version of the package from RSA
* Import the package and perform an Advanced Mapping to add the components to the Archer platform
* Install the solution package
* Create a user account for the web services client
* Add the Solution Data Feeds
* Set a schedule for the feed
* Set up the compliance mail merge template
* Configure the layout the solution fields

Details on how to perform these steps are included in the RSA solution guides for PCI 2.1.

### How This All Works

Using the authoritative sources provided by RSA will be a huge help in meeting your PCI compliance requirements. Here are the activities the solution manages.

* You create the documents that define the cardholder data environment
* Created the documentation that shows your control framework
* Schedule ongoing compliance assessments
* Capture evidence
* Manage issues, exceptions and remediation
* Provide compliance assessment reports

### So the Benefits are…

If you are solving e GRC issues with Archer adding the PCI solution will give you

* PCI requirements met
* Lower Audit costs
* Easier transition to new versions of the PCI standards
* Reduced risk of a data breach
* Maintenance of brand integrity
* Increased Shareholder value
* Lower insurance costs
* Improved capital allocation

### Summary

As the threats increase and the sophistication of attacks grows managing the risk from data loss grows, tools like Archer which still leads all products in this category is a worthwhile investment.

## Resources

### Archer Training –

* RSA Archer Administration - Global Knowledge Course 9738 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=17849&catid=542&country=United+States))
* RSA Archer Advanced Administration – Global Knowledge Course 9739 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=17851&catid=542&country=United+States))
* Getting Started with Enterprise Risk Management – Global Knowledge Course 9781 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=19725&catid=542&country=United+States))
* Getting Started with Policy and Compliance Management - Global Knowledge Course 9780 ([Link](http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=19367&catid=542&country=United+States))

## RSA

### Customer Support –

* Information - <http://www.emc.com/support/rsa/contact/phonenumbers.htm>
* Customer Support E-mail <mailto:archersupport@rsa.com>

### RSA Archer Community –

<https://community.emc.com/community/connect/grc_ecosystem/rsa_archer>

### RSA Archer Exchange –

<https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange>

Access the documentation from the Documents page on the RSA Archer Community at

<https://community.emc.com/community/connect/grc_ecosystem/rsa_archer> (Registration Required)

RSA Archer Demonstrations are also available on [YouTube](http://axp.zedo.com/asw/pfr/305/1523691/8/o.html?cdm=xads.zedo.com&a=1523691&x=3869&g=172&c1=305017112&c2=305017112&i=0&n=305&s=1029&1=4&2=1&tg=1377795314&vr=8&m=24&w=30&os=3&p=6&h=747871&f=1354039&b=30&o=20&y=3&v=1&t=i&u=J3wxkx8zTfWiTUVMptuMWw**~072113&z=0.2998643006620564&mb=29&dm=.zedo.com&pt=3Interactive&q=&sk=&l=&cd=&adm=c5.zedo.com&r=2&ldm=l1.zedo.com&exp=0&cm=&tt=0&wm=Transparent&dnt=1&tsad=0&p1=&p2=&p3=&p4=&p5=&prfl=&ct=0)

## About the Author

I think of myself as a specialist in the area of IT governance, IT risk identification and mitigation as well as managing a broad range of regulatory and statutory mandates along with extensive IT technical skills. I've done things that includes being a session speaker at the 2006 North America Audit, Control and Security Conference, where I presented on the security and the auditing of Active Directory and Exchange. I have 15 years of directory services, identity management and messaging experience providing system designs to numerous clients of varying sizes. Other things includes performing Sarbanes Oxley compliance testing and providing guidance that has helped organizations deal with the compliance and business risk that can come from the use of electronic messaging. Among my certifications include being an IT Systems Auditor (CISA), Certified Information Security Professional (CISSP) along with product certification from IBM, Microsoft and RSA. I also have a BS in Accounting and an MBA with experience in dealing with regulatory issues such as Sarbanes Oxley, BASEL II, FFIEC, PCI and HIPAA as well as numerous privacy mandates. I have been training representatives of large enterprises for Global Knowledge to identify and remediate institutional risk from email and to develop a message management solution using Exchange 2010 and reducing operation risk by using System Center Operations Manager and System Center Configuration Manager I’m currently teaching Archer, System Center, Exchange and SharePoint for Global Knowledge.

You can email me at [ted@chathamtech.com](mailto:ted@chathamtech.com)

Follow me on Twitter – [Tdziekanowski](https://twitter.com/TDziekanowski)

Linkedin:<http://tinyurl.com/bv75fee>

Blog: <http://www.chathamtech.com>