GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Case Study: Critical Controls that Could Have Prevented Target Breach

GIAC (GSEC) Gold Certification

Author: Teri Radichel, teri@radicalsoftware.com
Advisor: Stephen Northcutt

Accepted: August 5th 2014

Abstract

In December 2013 over 40 million credit cards were stolen from nearly 2000 Target stores by accessing data on point of sale (POS) systems. This paper will explore known issues in the Target breach and consider some of the Critical Controls that could have been used to both prevent this breach and mitigate losses. From what is known about the Target breach, there were multiple factors that led to data loss: vendors were subject to phishing attacks, network segregation was lacking, point of sale systems were vulnerable to memory scraping malware and detection strategies employed by Target failed. A possible solution for preventing and mitigating similar breaches using a defense in depth model will be presented using a multi-layered security strategy. Considerations of human factors that contributed to the losses in this case will also be addressed.

© 2014 The SANS Institute Author retains full rights.

1. Introduction

Target shoppers got an unwelcome holiday surprise in December 2013 when the news came out 40 million Target credit cards had been stolen (Krebs, 2013f) by accessing data on point of sale (POS) systems (Krebs, 2014b). Target later revised that number to include private data for 70 million customers (Target, 2014). The breach transpired between November 27 and December 15th 2014 (Clark, 2014). Over 11 GB of data was stolen (Poulin, 2014). Target missed internal alerts and found out about the breach when they were contacted by the Department of Justice (Elgin, 2014).

A series of steps were taken by the adversaries to obtain access to the credit card data and retrieve it from Target's systems. A break down in detection further increased data loss. Sources suggest the breach transpired as follows:

1. Reconnaissance by attackers may have included a Google search that would have supplied a great deal of information about how Target interacts with vendors. Results would have revealed a vendor portal and a list of HVAC and refrigeration companies (Krebs, 2014g). This reconnaissance would have also revealed a detailed case study on the Microsoft web site that describes how Target uses Microsoft virtualization software, centralized name resolution and Microsoft System Center Configuration Manager (SCCM), to deploy security patches and system updates. The case study describes the Target technical infrastructure, including POS system information, in significant detail (Microsoft, 2011).
2. An email containing malware was sent to a refrigeration vendor, Fazio Mechanical, two months prior to the credit card breach. Malware installed on vendor machine may have been Citadel – a password-stealing bot program that is a derivative of the ZeuS banking trojan. The malware stole credentials to an online vendor portal (Krebs, 2014d).
3. Next the criminals accessed Target's systems via Fazio Mechanical's credentials via a vendor portal (Krebs, 2014d).

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

4. From this pivot point the attackers could have further infiltrated the network. The specific details are not available but we can speculate that the criminals used the used the attack cycle described in Mandiant's APT1 report to look find vulnerabilities in the vendor portal move laterally through the network via back doors, reconnaissance and other vulnerable systems (Mandiant, 2014a). Common network tools were used to do reconnaissance once inside the network (iSight Partners, 2014).
5. Another Mandiant report on data breach trends describes how reconnaissance in a retail attack uncovered misconfigured systems. A vulnerable domain controller that could then be used to obtain access to POS systems. (Mandiant, 2014b). The Microsoft Target Case Study states *"*Except for centralized authentication, domain name resolution, and endpoint monitoring services, each retail store functions as an autonomous unit*"* (Microsoft, 2011) so the attacker would know to look for these pivot points.
6. Once access was obtained to the necessary systems, malware was installed on point of sale systems (Steinhafel, 2012). The number of POS machines that were compromised in a short amount of time indicates that the software was likely distributed to them via an automated update process. A Dell SecureWorks report explains how the malware was installled using SCCM (Jarvis & Milletary, 2014). The malware was custom software, undetectable by virus scanners (Krebs, 2014a).
7. The software gathered credit card information from memory as cards were swiped (Krebs, 2014b). The data was saved to a .dll file and stored in a temporary NetBios share over ports 139, 443 or 80 (iSight Partners, 2014).
8. Components used by attackers communicated via an ICMP tunnel (Warner, 2014). The ICMP traffic consisted of PING packets with custom text messages to indicate data movement from POS machines to compromised machine on the corporate LAN (iSight Partners, 2014).

© 2014 The SANS Institute Author retains full rights.

9. Other customized components were used to send raw commands over the network that would not be discoverable by common network forensics tools and bypass network controls (iSight Partners, 2014).
10. Reports indicate data was retrieved using the default user name and password for BMC's Performance Assurance for Microsoft Servers (Krebs, 2014e).
11. Data was moved to drop locations on hacked servers all over the world via FTP. Hackers retrieved the data from drop locations which hackers accessed to retrieve it (Krebs, 2014h).
12. While the attack was in progress, monitoring software (FireEye) alerted staff in Bangalore, India. They in turn notified Target staff in Minneapolis but no action was taken (Elgin, 2014).
13. Credit cards were then sold on the black market (Krebs, 2013c).

The cost of the breach was far reaching to both Target, customers, employees and banks. High-ranking employees lost their jobs including the CEO (Gonsalves, 2014) and CIO (Baldwin, 2014). Members of Target's board of directors were threatened with removal (Lublin, 2014). Banks had to refund money stolen from customers via their credit cards and pay for replacement cards costing more than $200 million (D'Innocenzio, 2014). Banks refunded most funds stolen from credit and debit cards, but identity theft was at an all time high in the first half of 2014 due to large data breaches including Target (Murray, 2014). More than 140 lawsuits have been filed against Target (Webb, 2014). Banks sued Target's PCI compliance auditor, Trustwave (Schwartz M. J., 2014). Target is dealing with investigations involving the Department of Justice (Hosenball, 2014), the FTC (Risen, 2014) and SEC (Michaels, 2014). Individual state laws may result in fines and legal proceedings over and above PCI compliance fines. States are passing even stricter laws as a result of recent breaches (Grande, 2014). Profits dropped 46% in the fourth quarter of 2013 during the critical holiday season (Ziobro, 2014). Customer visits dropped in the new year prolonging the losses (Halkias, 2014).

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

Target passed PCI compliance audits prior to this breach, indicating they had implemented security required by the credit card processing industry (Schwartz M. J., 2013). Fazio Mechanical issued a statement claiming they were compliant with industry standard information security regulations (Fazio, 2014). We can learn from the Target breach that compliance with baseline standards isn't enough (Mellow, Jr., 2014). A comprehensive approach to security will consider all assets, not just those that fall under compliance regulations. Each asset has a specific set of threats and vulnerabilities that can be considered as part of a risk management program, rather than simply implementing what is mandated for a subset of assets. As demonstrated in this breach, many different assets were used to move throughout the network, so consideration of the POS systems alone would not address the root causes that led up to this attack.

This paper explores a more holistic approach to security. Risk management assesses and prioritizes security needs based on what can cause the most damage to a company (SANS Institute, 2014b, p. 217), rather than relying on legal or industry standard compliance. Defense in depth makes use of multiple layers of protection (SANS Institute, 2014a, p. 6). The Critical Controls (SANS Institute, 2014c) are recommended that may have either prevented this breach or mitigated the impact. Controls include not only technology but also people who must audit, analyze and manage systems and perform incident response activities. The Target breach is then replayed to demonstrate an alternate scenario had this strategy been employed.

2. Security Strategy

2.1. Risk Management

PCI compliance alone is not a risk management strategy. Only assets related to payment card processes are considered. Many businesses approach PCI compliance by trying to minimize what is in scope for the PCI audit. Assets and implementation details that may pose the greatest risks to the organization may fall outside of this scope and therefore not be adequately addressed if PCI alone drives a business security decisions. For example, at the time of the breach, the current PCI standard says consideration should be made for data stored in memory but no specific requirements are defined (PCI

© 2014 The SANS Institute Author retains full rights.

Security Standards Council, 2013a). Regulations cannot be developed, written and agreed upon as fast as attackers can change their tactics. In fact, standards may inform adversaries what security measures a business has implemented, so the attacker will likely attack vulnerabilities not on the compliance checklist and assets that are out of scope for PCI compliance audits. Even if the standards tried to define a complete security checklist, auditors would likely not be able to find every infraction.

> Vanessa Pegueros, CISO of DocuSign says: We are going through our PCI audit right now. PCI Auditors cannot be expected to find every vulnerability and security problem. The field is too complex and broad and auditors are not paid enough nor do they have the expertise to go to that level of detail needed to address the true risks. It is just not a cost effective exercise to try and find every problem that exists (V. Pegueros, personal communication, 2014).

Rather than relying on a mandated checklist, organizations will be better able to mitigate losses by performing organization-wide risk management activities on a regular basis. Vulnerabilities are system weaknesses that can be exploited. Threats are events that have negative consequences. Threats and vulnerabilities for all systems, not just those within scope for compliance audits, are identified. Threats and vulnerabilities are then prioritized and fixed to limit risk to an acceptable level (SANS Institute, 2014b, pp. 214-241). Constant re-evaluation is required as the threat landscape is always changing.

After threats and vulnerabilities are identified for all systems, the risk posed by each is carefully analyzed. Generally, the vulnerabilities with the highest likelihood of occurring and most severe consequence in terms of cost to the organization should be prioritized highest and fixed first. This has nothing to do with compliance and everything to do with what poses the greatest risk to the organization.

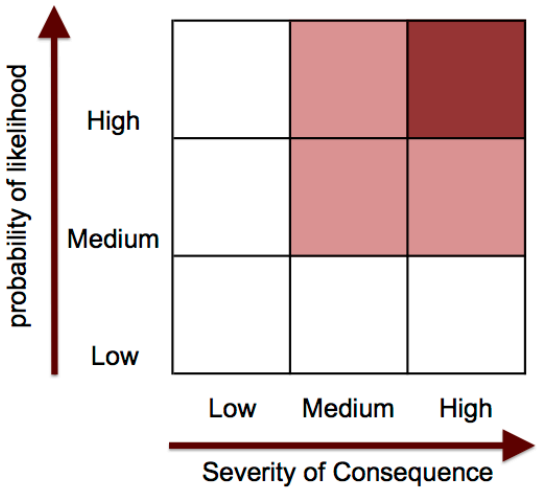


Figure 1 Risk Analysis Matrix
(Sans Institute, 2014b, p. 217)

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

Threat modeling and risk management in entirety is outside the scope of this paper, but it is important to understand that a reliance on mandated compliance guidelines was not enough to protect Target from monumental data loss. *Threat Modeling: Designing for Security* by Adam Shostack (Shostack, 2014) covers this topic in depth. *Hacking Point of Sale: Payment Application Secrets, Threats and Solutions* by Slava Gomzin (Gomzin, 2014) presents specific vulnerabilities for POS systems. Companies can also use common risk frameworks such as ISO 27001/27002/27005 or NIST 800-30/800-53 (J. Popp, personal communication, 2014).

Businesses need to employ an adequate number of security professionals who understand the business, the risks and the potential loss. Security staff needs to be vigilant to understand new potential threats and vulnerabilities when they appear. New attacks may appear in internal system logs or be reported in the industry as vulnerabilities or security incidents or events. Organizations must understand that Advanced Persistent Threats (APTs) are targeting them and the nature of the attacks (Ferraro, 2013).

2.2. Defense in Depth

"A security system is only as strong as its weakest link" (Ferguson, Schneieir, & Tadayoshi, 2010). If you install a large, strong gate at the front of your property, but a hole exists in the back fence large enough for a thief to enter, the gate can easily be bypassed. Installing cameras to watch the hole in the back fence with, but not hiring someone to monitor the cameras 24 x 7 will not prevent a burglary and renders the cameras ineffective. Recent breaches demonstrate that persistent adversaries are constantly seeking the weakest link to obtain access systems to steal data. Defense in Depth is a layered approach to security created by the National Security Agency (NSA). A single protection may fail so multiple levels of protections and controls are employed to protect business assets (SANS Institute, 2014a, p. 6).

Many businesses that have experienced recent major breaches employ encryption strategies. Unfortunately, encryption is often not properly implemented and deployed. Encryption in and of itself does not protect systems. A robust security strategy is required which protects entire systems in a comprehensive way in order for encryption to be effective. For example, an encryption algorithm and large key may become useless if you

© 2014 The SANS Institute Author retains full rights.

have the encryption key stored with the data. The hackers or malicious insiders will simply gain access to the system and use the key to unencrypt the data (Ferguson, Schneieir, & Tadayoshi, 2010, p. 12). For encryption to be effective, you must employ a defense in depth strategy in which you also protect the key and protect access to systems where the data needs to be unencrypted in order to be processed.

Target reportedly spent a great deal of money on security technology (Capacio, 2014). Although systems used encryption, the encryption was rendered useless because the data was accessed in memory where it was unencrypted. Although some level of segregation likely existed, vulnerable configuration and accounts allowed segregation strategies to be bypassed. Despite the fact that they purchased expensive monitoring software, staff was not sufficient, not well-trained or inadequate processes turned those systems into a liability rather than an asset when it was determined that Target was notified, but did nothing to stop the breach.

Defense in Depth requires layers of security, but the weakest link in each layer may provide access to the next. It appears that there were vulnerabilities in each layer of defense employed by Target that ultimately allowed the attackers to gain access to some of their most sensitive data.

2.3. Critical Controls

In 2008, the federal government arranged a consortium of public and private organizations to come up with a list of Critical Controls based on various other cyber security lists and guidelines. Critical Controls are added to the list because they help prevent and detect known attacks effectively (SANS Institute, 2014d). The Consortium for Cybersecurity Action (CCA) regularly updates the Critical Controls (Dell Secure Works, 2014). The following table lists the 20 Critical Controls. The Sans Institute web site provides more details about each control at http://www.sans.org/critical-security-controls (SANS Institute, 2014c).

The 20 Critical Controls
1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops,

© 2014 The SANS Institute Author retains full rights.

Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

Figure 2 The 20 Critical Controls (SANS Institute 2014c)

3. Security Strategy Applied to Target Case

3.1. Risk Management as related to Target and POS systems

A risk-based approach to security would have involved analyzing threats and vulnerabilities of all systems within the company on a regular basis. Risks would have then been prioritized so that some of the vulnerabilities used to attack the systems in this breach may have been prevented. Threat models created for systems throughout the data centers and networks might have uncovered attacks that were used as pivot points to reach the POS systems. Analyzing systems for vulnerabilities would have likely revealed some of the flaws that were exploited by the attackers to gain system access. An understanding of the data as it flowed through the system encrypted and unencrypted might have revealed that data was residing unencrypted in memory where it would be accessible by malicious software. Determining the most critical assets may have led to additional logging, monitoring and log analysis for those systems. Analysis of threats and vulnerabilities for all systems, not just those with most valuable data, could have been used to prioritize security efforts to lower risk.

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

When asked about the Target Breach, Jason Popp says, "Even though the POS system was one of the most valuable systems, the internet-facing vendor system had a higher risk level. Additional controls on that internet facing environment may have prevented the attack." He also commented that the Target case study on the Microsoft web site pointed out exactly what ports were open and what tools were available for the POS exploit (J. Popp, personal communication, 2014).

3.2. Defense in Depth applied as a strategy in this case

Although many security measures were in place throughout the Target infrastructure, additional layers of protection would have stopped the attack at various points along the way. Applying a stronger Defense in Depth strategy would have ensured that each level was not accessible from the next. Additional defenses on the POS system itself could have further protected the data.

Even though encryption was used, the card data was available in memory at some points on the POS systems. This card data was accessible because hackers were able to infiltrate the network through other vulnerable systems to ultimately access the POS machines. Had network controls and other system controls prevented access to the POS machines at all, the card data would have been inaccessible.

Application whitelisting would have allowed only authorized software to run on the POS system. Jason Popp, Group Manager of Security Architecture for a major retailer suggests that a process separate from the POS system and software management tools could have managed whitelisting (J. Popp, personal communication, 2014). Application white listing could be done via hardware or software. Jose Diaz, Director, Business Development & Technical Alliances at Thales eSecurity explains how code signing with an HSM (hardware security module) which protects encryption keys would work: "The code or application running in the POS system could have employed digital signatures, with the signing key protected in a Hardware Security Module (HSM) to ensure only legitimate code from the manufacturer could be installed in the devices" (J. Diaz, personal communication, 2014).

As for the encryption itself, additional layers of protection could have been added to protect card POS operating system memory. A tamper resistant security module

© 2014 The SANS Institute Author retains full rights.

(TRSM) encrypts data in hardware, not software. Some POS models use a TRSM to encrypt the data at point of swipe (Horton & McMillon, 2011). The card data goes directly to the TRSM where it is encrypted. Even if malware got on the POS operating system, it would have been reading encrypted data. Jeremy Eisenman of Thales eSecurity explains, "Secure pin entry devices have been around for 40 years. Requirements are strict around securing PINBLOCKS. Magnetic stripe track data has not been handled with the same security controls even though swiped on the same PED" (J. Eisenman, personal communication, 2014).

For true Point-to-Point Encryption (P2PE) a system would look similar to this diagram from the Payment Card Industry's guide on (PCI) Point-to-Point Encryption (PCI Security Standards Council, 2013b):

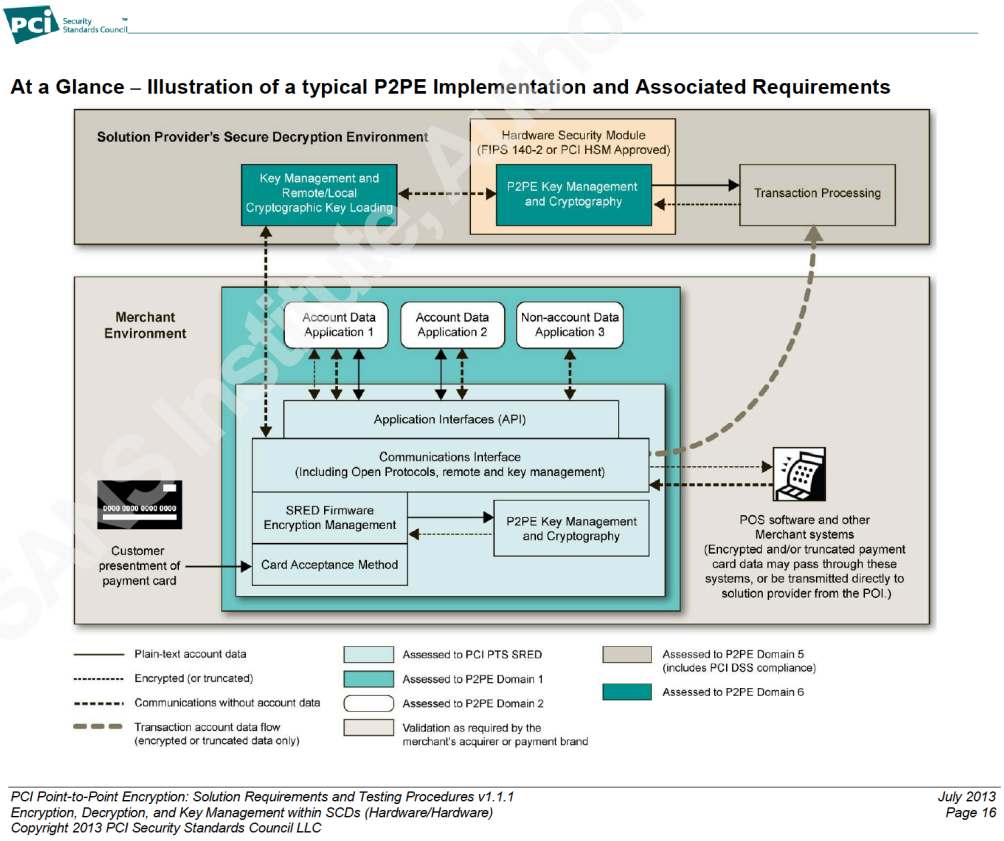


Figure 3: PCI Point-to-Point Encryption Implementation

Jose Diaz of Thales eSecurity explains that payment terminals implemented correctly already encrypt the PIN data on the cards but often not the data on the magnetic

© 2014 The SANS Institute Author retains full rights.

stripe. When the PIN is received an encrypted PINBLOCK is created immediately at entry. The cryptogram is sent over the network to a payment HSM that unencrypts and then re-encrypts the PIN to the processor or issuer that can verify them. The retailer should never store the PIN data.

> He goes on to say: Using a PCI PIN Transaction Security (PTS) approved device for reading the cards and encrypting sensitive data within the device, as described in PCI Point-to-Point Encryption requirements, would have prevented having clear sensitive data in the POS environment similar to what is done for PINs (J. Diaz, personal communication, 2014).

3.3. Possible Implementation of Critical Controls

The Critical Controls are a prioritized list of controls that are chosen to prevent known attacks. By reviewing the Target breach, the effectiveness of the Critical Controls can be evaluated to determine if they would have helped prevent this attack. Each step the hackers took to gain access is a point in the system where the attack could have potentially been thwarted. Analysis of each action can determine if there is a Critical Control that would prevent a similar attack in the future.

Attack vectors used in this breach are listed below. Next to each attack vector the Critical Controls are listed that may have stopped this attack. The full list of 20 Critical Controls are found on the SANS Institute web site at http://www.sans.org/critical-security-controls (SANS Institute, 2014c).

Attack Vector	Critical Control
Reconnaissance	9. Security Skills Assessment and Appropriate Training to Fill Gaps: Use security awareness training to make employees aware of the danger of sharing too much information. 15. Controlled Access Based on the Need to Know: Remove vendor information and Microsoft case study with detailed information about Target technical systems, processes and staff. Network access could restrict access to vendor and technical information.

© 2014 The SANS Institute Author retains full rights.

Email attack, Malware installed on vendor machine	5. Malware Defenses: Require vendors to use commercial virus checking software and other security precautions on the systems used to interact with vendor portals. 9. Security Skills Assessment and Appropriate Training to Fill Gaps: Require vendors to go through basic security training or agree to train staff.
Use of vendor credentials	13. Boundary Defense: Limit network access to vendor portal so anyone who obtained the credentials would not be able to access the vendor portal unless on a network allowed to access that portal. 16. Account Monitoring and Control: Require multi-factor authentication to log into vendor portal. Monitor use of vendor portal logins. Profile accounts for normal activity and usage periods to spot anomalies.
Exploited Vendor Portal Vulnerabilities	3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Weakness may have been in a component running on the vendor portal server that could have been prevented. 6. Application Software Security: A web application firewall, monitoring, scanning for vulnerabilities and testing may have uncovered flaws in the vendor system. Patching the system would have ensured software was up to date with known vulnerabilities patched. 20. Penetration Tests and Red Team Exercises: Since this system is on the perimeter at the first layer of defense chances are a pen tester may have uncovered the weaknesses in this system given a password.
Network Infiltration and Communication	12. Controlled Use of Administrative Privileges: Inappropriate access to administration accounts may have allowed

© 2014 The SANS Institute Author retains full rights.

	attackers to install tools and bypass network segregation boundaries. Monitoring access may have indicated the unexpected activity. 14. Maintenance, Monitoring, and Analysis of Audit Logs: Monitor for anomalies including malformed packets and packets with unexpected sizes or data. Analyze unexpected traffic to and from critical systems. Do not rely on standard tools alone. Custom attacks are designed to bypass known capabilities of technical tools. 19. Secure Network Engineering: Segregate critical systems from the rest of the network with tightly controlled access.
Misconfigured systems and vulnerable Domain Controller	3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Weakness may have prevented inappropriate access or exploitation of systems. Alerts could have been generated by a HIDS when key server configurations were changed. 16. Account Monitoring and Control: Require multi-factor authentication for critical accounts. Monitor accounts. Profile accounts for normal activity and usage periods to spot anomalies. Account privileges should be limited to need to know. Segregate account access across network tiers. Change default passwords. Disable and delete unneeded accounts.
Malware installed on POS systems	2. Inventory of Authorized and Unauthorized Software: Whitelisting would not have allowed the malware to be installed on POS systems. Scanning for configuration changes with a HIDS such as Tripwire would have alerted staff to configuration changes. Tripwire alerted Sally Beauty to a credit card breach however reports do not indicate if the HIDS was installed on POS systems (Krebs, 2014f) . Inventory software and

© 2014 The SANS Institute Author retains full rights.

	require it to provide identification tags in logs. Virtualized instances of systems can be periodically restored to a pristine version. 3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers: Secure configuration of POS machine would have likely turned off NetBIOS. In addition blocking ports related to NetBIOS may have prevented network access and shares used to exfiltrate data. 5. Malware Defenses: Although virus-scanning software would not have prevented this attack, monitoring for malicious software and a HIDS may have helped uncover its existence if whitelisting was not in place. 12. Controlled Use of Administrative Privileges: Limited administrative privileges may have prevented inserting software to get into the deployment process used to infect the POS systems with malware. Monitoring access may have indicated the unexpected activity.
Card data scraped from memory	6. Application Software Security: Developers trained in security should develop systems processing sensitive data. Target software on POS machines was an in-house product (iSight Partners, 2014). 17. Data Protection: P2PE for POS systems from PCI compliant vendors may have helped protect card data in memory. Hardware encryption devices directly connected to the pin pad would have kept credit card data out of memory (Gomzin, 2014, p. 210). POI pin pads with tamper resistant security module (TRSM) implement hardware encryption (Gomzin, 2014, p. 188).
Data removed from POS machines to corporate LAN	3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops,

© 2014 The SANS Institute Author retains full rights.

	Workstations, and Servers: Data could not be moved using NetBIOS functionality. 13. Secure Network Engineering: Implement network segregation that limits access to critical systems to specific addresses and ports. URL filtering for egress capabilities limits datacenter system outbound access.
Data moved to drop locations	17. Data Protection: Employ tools at perimeters to monitor for sensitive data leaving the company in clear text. Use Data Loss Prevention systems if applicable. Monitor traffic. Block known exfiltration web sites.
Failure to respond to FireEye alerts	4. Continuous Vulnerability Assessment and Remediation: continually assess the environment and threats for new vulnerabilities. 9. Security Skills Assessment and Appropriate Training to Fill Gaps: Make sure security staff is adequate to monitor logs appropriately and well trained. 14. Maintenance, Monitoring, and Analysis of Audit Logs: Hiring more staff or better training staff to adequately monitor logs may have helped mitigate losses. 17. Data Protection: Scan for sensitive data and document where it is located. Ensure locations are valid places for sensitive data to reside. 18. Incident Response and Management: Retrospective after incident may indicate how better policies and procedures for incident management could have prevented this breach or minimized the losses. 20. Penetration Tests and Red Team Exercises: Pen testing exercises to mimic attacks and generate alerts could indicate whether or not staff responds to alerts appropriately.

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

Cards stolen on black market	17. Data Protection: EMV (Europay, MasterCard and VISA), otherwise known as chip and pin, is not explicitly named but will add some help for cards used by requiring a pin at the time the card is used to authenticate the transaction. It would not have completely prevented loss by customers because in some cases devices do not support or failover to the magnetic stripe method (Gomzin, 2014, p. 215). This technology protects the customer after the data has been stolen because it prevents using a cloned card in some cases. It does not prevent stealing the data from a POS system.

Figure 4 Critical Controls recommended for each step taken by attackers in Target breach.

4. Target Breach: An alternate outcome

By applying the recommended security strategies, a speculative alternative outcome demonstrates how they may have stopped or mitigated the attack. A risk-based approach to security would have included analyzing threats and vulnerabilities for all systems on a regular basis to determine high-risk systems. Prioritization of risk would have helped determine which Critical Controls to implement first based on possible damage to the business. Risk analysis would have helped the company determine which Critical Controls to implement first. Use of the Critical Controls to implement a stronger Defense in Depth strategy may have stopped the attackers at different points before they reached the credit card data.

Even if Target had not applied every single control listed, one or more of the controls could have blocked each step of the attack. Although the breach is unfortunate and unintended, it provides a case study that other businesses can use to understand the threats and vulnerabilities that led up to it. The table below suggests specific actions that could be taken to apply the recommended Critical Controls for each attack point. An alternate outcome is presented, had the controls had been applied. Using a real world example demonstrates why the Critical Controls are important and how they can help.

Attack Vector	Result With Critical Controls Applied

© 2014 The SANS Institute Author retains full rights.

Reconnaissance	No revealing data such as the list of vendors found on target web site. No access to vendor portal web URL unless coming from an approved network address or VPN. No case study would be published that had details about the infrastructure of the Target stores, systems, software or maintenance processes. Separation of duties would have prevented insiders from having end-to-end system knowledge or access. Result: Hackers would have not known vulnerabilities in advance of attack.
Email attack, Malware installed on vendor machine	Vendor staff is familiar with phishing attacks because Target required vendor training. Require commercial virus scanning software that would have prevented malware used in the attack on the vendor machines (Poulin, 2014). Result: Malware in phishing attack would have failed. Hackers would not have obtained access to vendor portal credentials.
Use of vendor credentials	Requiring a VPN or restricting network access would have prevented an attacker from accessing the vendor portal. Multi-factor authentication would have prevented the vendor from logging into the portal if they did not have the MFA token. This would have prevented exploiting vulnerabilities in the vendor portal. Result: Hacker with vendor credentials could not access vendor portal.
Exploited Vendor Portal Vulnerabilities	Periodically scanning the vendor portal may have uncovered vulnerabilities that could have been fixed such as SQL

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

	Injection, XSS and other web site vulnerabilities (Poulin, 2014). Hardening the machine may have removed vulnerabilities that exploited. Preventing network access to all systems and ports that were not required may have prevented network infiltration. Running applications under a non-administrator account with no access to other portions of the network may have limited access. Result: vendor portal cannot be used as a pivot point.
Network Infiltration and Communication	More staff trained in depth on network traffic and security analysis to inspect traffic and account activity for anomalies. Correlation of logs and analysis of network and account activity may have uncovered anomalies indicative of an attack: Accounts accessing unexpected resources, unexpected traffic between systems, failed login attempts or access, installation of network reconnaissance tools, malformed packets and packets of unusual sizes, unexpected shares, unexpected increase in traffic, traffic sent to unexpected location, unexpected types of traffic (FTP traffic going to Brazil, for instance). Restrict accounts to a single network zone if possible so access to one account does not give access to other portions of the network. Monitor unauthorized access attempts. Set up honey pots and honey tokens if budget allows for detailed and constant monitoring of these resources. Analyze all access for malicious activity. Prioritized logging as relates to traffic in

© 2014 The SANS Institute Author retains full rights.

	and out of POS systems. Additional scrutiny is placed on any traffic changes in or out of systems with critical data. Tuning of alert systems to reduce false positives. Adequate staff to allow review of all alerts in a timely and adequate manner. Strict firewall rules to segregate systems and accounts limited to access specific portions of the network. Separation of duties prevents access across different network layers. Understand ICMP Attacks to determine how they can be prevented (InfoSec Institute, 2012). Result: suspicious activity leads to discovery of infiltration and problem is resolved before hackers reach POS systems. Accounts and systems limited in access cannot be used as pivot points to other parts of network.
Misconfigured systems and vulnerable Domain Controller	Servers are hardened and set up with known good configurations so hacker cannot exploit flaws. Configuration files do not contain sensitive data that can be used by hackers to access other systems, so they cannot determine how to get to POS systems on the network. Any sensitive data in configuration is encrypted when possible. Encryption keys and processing occurs in an HSM so cannot be accessed by hacker directly from files even if get onto the machine. Configurations are monitored for changes and changes are reviewed for flaws so any misconfigurations would be fixed immediately. Critical systems and accounts require

© 2014 The SANS Institute Author retains full rights.

	multi-factor authentication. Accounts are given minimal access for specific purposes. No default passwords would have been accessible for any third party to use. Result: Attacker may obtain access to one machine or account but will be limited in what they can access or do after reaching that machine. Attack would have been limited in scope and not been able to reach POS machines.
Malware installed on POS systems	Systems are patched and up to date so known vulnerabilities cannot be exploited. No remote access is allowed on POS machines so attempts to log in remotely fail. Software is inventoried and white listed on POS machines. New software would be prevented from installing or running. Applications are run under non-administrator account. If hacker got access to accounts running on system they would not have ability to install software. Strong passwords changed regularly prevent attacker from brute force password attack to escalate privileges and install software. A host intrusion detection device alerts to any system changes if the attacker is able to install the malware so it can be uncovered and stopped immediately. Target used custom-built POS software. (iSight Partners, 2014). Software and systems should be designed by people with in depth knowledge of security could potentially build additional protection and logging into software that is processing

© 2014 The SANS Institute Author retains full rights.

	card data. Limit access to centralized build and installation systems. Audit all access to these systems. Place additional controls on gold images used for POS systems. Ensure central management system and any software images are properly signed, managed, secured and audited (J. Popp, personal communication, 2014). Result: Would not be possible to install malware on POS machines. Any changes to POS configurations would generate alerts to quickly resolve the problem.
Card data scraped from memory	P2PE is employed to ensure credit card data is encrypted end-to-end and never accessible in memory to hackers in the POS systems. Consider using approved P2PE vendors from PCI web site, but verify data is not stored in memory or inappropriately with appropriate testing. POI pin pads with tamper resistant security module (TRSM) use hardware encryption to encrypt credit card data so it never enters the memory on the machine and key is protected. A pin pad should be used that encrypts the magnetic stripe data using the TRSM, not just the pin. Result: credit card data would not have been available to the memory scraping malware.
Data removed from POS machines to corporate LAN	Turn off NetBIOS and file and printer sharing unless absolutely needed. Turn off any other protocols not required such as SMB and CIFS unless they are actually needed. Available services can be used for malicious activity. Extraneous protocols, especially if not well monitored, may be used to tunnel through firewalls. Block all ports related to these services if not required.

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

	Inventory network devices and shares, especially on critical systems with sensitive data. Additional logging and alerting for traffic coming in or out of POS systems. Result: NetBIOS ports could not have been used to data.
Data moved to drop locations	Implement strict access for data moving out of the company via FTP or known file transfer protocols. Create a proxy specifically for data movement such as FTP, SFTP and other protocols used to send data to remote locations. Carefully monitor traffic for unexpected activity. Monitor outbound traffic for unexpected changes and anomalies. Result: Data moving out of the organization would have been spotted. Breach would have been stopped sooner.
Failure to respond to FireEye alerts	Separation of duties would have different people monitoring systems than those who have access to make changes to configuration. Adequate staff would be available to look at alerts in detail and respond accordingly. Processes would be appropriate and staff would be well trained to handle alerts in such a way that the breach would have been uncovered. Correlated logging using a SIEM (Security Incident and Event Management) system may have helped uncover the breach sooner. Result: The alerts would have been analyzed differently and the data breach

© 2014 The SANS Institute Author retains full rights.

	would have been terminated sooner.
Cards stolen on black market	Once the card data has been stolen it can be used to create fake cards or facilitate transactions. At that point, requiring a pin that the owner of the card must know would have prevented use of the cards when sold on the black market if the device was used on a card reader that supported chip and pin technology. This is more for fraud than data protection. Protection is thwarted on manual entry and on failover to MSR when the card reader or doesn't support the chip and pin technology and the card still has a magnetic stripe (Gomzin, 2014, p. 214). Result: Some of the data loss due to using stolen cards could have been prevented.

Figure 5 Possible outcome at each step had recommended Critical Controls been in place.

5. Summary

Target invested heavily in security spending, and unfortunately hackers were still able to find a way through their defenses. This breach makes it clear that PCI compliance, legal and industry mandates do not provide adequate security for sensitive data due to limitations in scope and an ever-changing threat landscape. Advanced Persistent Threats are going to seek out and exploit the weakest link in any system, network or process. They will use complex and lengthy attacks to mine data from companies any way they can. They are constantly revising their strategy and seeking holes in the armor of business security implementations. The adversary can adapt faster than the regulations can possibly be put in place. Security must be approached more strategically as a way to protect critical assets, business reputation and profitability.

The security strategy for a business should take into account the specific needs of that particular business. Businesses must consider what assets are most valuable and what threats pose the greatest risk using threat modeling and a risk management program. Resources should be focused on the most critical and highest risk assets. Solutions should be implemented most cost-effectively to mitigate that risk. This strategy requires an analysis of the business impact, not a boilerplate template provided by an external

© 2014 The SANS Institute Author retains full rights.

standards body. The cost and return on investment of various security tactics must be analyzed to help make appropriate security implementation decisions. A complete discussion of risk management is beyond the scope of this paper but resources were provided for further reading.

Businesses should not rely on a single security tool or process to prevent data loss or harm to the business. A layer of defenses including preventative and detective measures should be employed. Due to the complex nature of security and the persistence of the adversary, detection is crucial. A detailed understanding of networks, hardware, software and processes is required to create a comprehensive plan. Using the Critical Controls to implement layers of security helps thwart attacks by guarding against the many different ways attackers gain access to systems.

An alternate outcome for the Target scenario was presented with Critical Controls in place. Steps taken by the attackers could have been stopped at many different points during the attack. Segregating the POS systems, end-to-end encryption, inventory of systems and detailed logging would have kept thieves away from credit card data. Proper encryption would have prevented card data from being read in memory. Adequate, well-trained staff with time to appropriately analyze logs would have uncovered the malware and network traffic to mitigate losses had the breach still occurred.

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

6. References

Baldwin, H. (2014, March 11). The other shoe drops for Target's CIO. Retrieved from Forbes: http://www.forbes.com/sites/howardbaldwin/2014/03/11/the-other-shoe-drops-for-targets-cio/

Capacio, S. (2014, March 13). Target breach: Security warning ignored before heist. Retrieved from myFOX9.COM: http://www.myfoxtwincities.com/story/24968693/report-target-ignored-signs-of-breach

Clark, M. (2014, May 5). Timeline of Target's data breach and aftermath: How cybertheft snowballed for the giant retailer. Retrieved from International Business Times: http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

Dell Secure Works. (2014). The 20 critical security controls. Retrieved from Dell Secure Works: http://www.secureworks.com/resources/articles/other_articles/the-20-critical-security-controls/

D'Innocenzio, A. (2014, 2 18). Target data breach cost banks more than $200 million. Retrieved from THE HUFFINGTON POST: http://www.huffingtonpost.com/2014/02/18/target-data-breach-cost_n_4810787.html

Elgin, B. (2014, March 13). Missed alarms and 40 million stolen credit card numbers: How target blew It. Retrieved from Bloomberg Businessweek: http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Fazio, R. E. (2014, February 6). Statement on Target. Retrieved from Fazio Mechanical Services: http://faziomechanical.com/Target-Breach-Statement.pdf

Ferguson, N., Schneieir, B., & Tadayoshi, K. (2010). Cryptography Engineering: Design Principles and Pracctical Applications. Indianapolis: Wiley Publishing.

Ferraro, P. (2013, April 01). You are an APT target. Retrieved from SC Magazine: http://www.scmagazine.com/you-are-an-apt-target/article/284408/

Gomzin, S. (2014). Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions. Indianapolis, IA: Wiley.

Gonsalves, A. (2014, May 5). Target CEO resignation highlights cost of security blunders. Retrieved from CSO: http://www.csoonline.com/article/2151381/cyber-attacks-espionage/target-ceo-resignation-highlights-cost-of-security-blunders.html

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

Grande, A. (2014, May 8). Post Target breach laws ratchet up pressure on companies. Retrieved from Law 360: http://www.law360.com/articles/536057/post-target-breach-laws-ratchet-up-pressure-on-companies

Halkias, M. (2014, March 7). Survey says: Target data breach still having an impact on customer shopping decisions. Retrieved from Dallas News: http://bizbeatblog.dallasnews.com/2014/03/survey-says-target-data-breach-still-having-an-impact-on-customer-shopping-decisions.html/

Horton, T., & McMillon, R. (2011). Security technologies: Encryption and tokenization. Retrieved from First Data: http://files.firstdata.com/downloads/thought-leadership/primer-on-payment-security-technologies.pdf

Hosenball, J. F. (2014, January 29). Target says criminals attacked with stolen vendor credentials. Retrieved from Reuters: http://www.reuters.com/article/2014/01/30/us-usa-justice-target-idUSBREA0S1AE20140130

InfoSec Institute. (2012). ICMP attacks. Retrieved from InfoSec Institute: http://resources.infosecinstitute.com/icmp-attacks/

iSight Partners. (2014, January 14). KAPTOXA Point of sale compromise. Retrieved from Security Current: www.securitycurrent.com/.../KAPTOXA-Point-of-Sale-Compromise.pdf

Jarvis, K., & Milletary, J. (2014). Inside a Target point of sale breach. Austin: Dell SecureWorks.

Krebs, B. (2014a, January 14). A closer look at the Target malware, part II. Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/#more-24401

Krebs, B. (2014b, January 14). A first look at the Target intrusion malware. Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

Krebs, B. (2013c, December 12). Cards stolen in Target breach flood underground markets. Retrieved from Krebs on Security: http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

Krebs, B. (2014d, 02). Email Attack on Vendor Set Up Breach at Target. Retrieved from Kerbs On Security: Email Attack on Vendor Set Up Breach at Targethttp://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

Krebs, B. (2014e, January 14). New clues in the Target breach. Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/

Krebs, B. (2014f, March 14). Sally Beauty hit by credit card breach. Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/03/sally-beauty-hit-by-credit-card-breach/

Krebs, B. (2013g, December 13). Sources: Target investigating data breach. Retrieved from Krebs on Security: http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

Krebs, B. (2014h, February 2014). Target hackers broke in via HVAC company. Retrieved from Krebs On Security: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Lublin, P. Z. (2014, May 28). ISS's view on Target drectors is a signal on cybersecurity. Retrieved from THE WALL STREET JOURNAL: http://online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278

Mandiant. (2014a). APT1: Exposing one of China's cyber espionage units. Alexandria: Mandiant.

Mandiant. (2014b). M Trends: beyond the breach. Alexandria: Mandiant.

Mellow, Jr., J. P. (2014, March 18). Target breach lesson: PCI compliance isn't enough. Retrieved from Tech News World: http://www.technewsworld.com/story/80160.html

Michaels, D. (2014, July 3rd). SEC launches investigations of hacked firms. Retrieved from The Boston Globe: http://www.bostonglobe.com/business/2014/07/02/hacked-companies-face-sec-scrutiny-over-disclosure-and-controls/rH1MlfdmqyKNHMu2yrusHP/story.html

Microsoft. (2011). Large retailer relies on virtual solution to deliver optimal shopping experience. Retrieved from Microsoft Download Center: http://download.microsoft.com/download/3/A/D/3AD464EA-F2B4-4E62-B11F-14E37727557C/Target_Hyper-V_CS.PDF

Murray, T. D. (2014, 07 09). Six months after the Target security breach, report says cases of identity theft are increasing. Retrieved from cleveland.com: http://www.cleveland.com/business/index.ssf/2014/07/six_months_after_the_target_se.html

NSA. (n.d.). Defense in depth. Retrieved from NSA: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

PCI Security Standards Council. (2013a, July). Payment Card Industry (PCI). Retrieved from PCI Security Standards Council Point-to-Point Encryption Solution Requirements and Testing Procedures: Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware : https://www.pcisecuritystandards.org/documents/P2PE_v1-1.pdf

PCI Security Standards Council. (2013b, November). Payment Card Industry (PCI) data security standard: Requirements and security assessment procedures. Retrieved from PCI Security Standards Council: https://www.pcisecuritystandards.org/security_standards/index.php

Poulin, C. (2014, January 31). What retailers need to learn from the Target breach to protect against similar attacks. Retrieved from Security Intelligence: http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.U8sthsLn-pp

Risen, T. (2014, March 26). FTC investigates Target data breach. Retrieved from US News & World Report: http://www.usnews.com/news/articles/2014/03/26/ftc-investigates-target-data-breach

SANS Institute. (2014a). 401.2 Defense In-Depth. Bethesda: The SANS Institute.

SANS Institute. (2014b). 401.3 Internet Security Technologies. Bethesda: The SANS Institute.

SANS Institute. (2014c). Critical security controls for effective cyber defense. Retrieved from SANS Institute: http://www.sans.org/critical-security-controls

SANS Institute. (2014d). Critical security controls: A brief history. Retrieved from SANS Institute: http://www.sans.org/critical-security-controls/history

Schwartz, M. J. (2013, December 21). Target breach: 10 facts. Retrieved from Dark Reading: http://www.darkreading.com/attacks-and-breaches/target-breach-10-facts/d/d-id/1113228

Schwartz, M. J. (2014, March 26). Target, PCI auditor Trustwave sued by banks. Retrieved from Dark Reading: http://www.darkreading.com/risk/compliance/target-pci-auditor-trustwave-sued-by-banks/d/d-id/1127936

Shostack, A. (2014). Threat Modeling: Designing for Security. Indianapolis: John Wiley & Sons, Inc.

Steinhafel, G. W. (2012, January 12). Target CEO: We are accountable for the breach. (B. Quick, Interviewer)

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.

Target. (2014, January 20). Target provides update on data breach and financial performance. Retrieved from Target: http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance

Warner, G. (2014, January 19). Target "hacker tools" provide breach insight. Retrieved from Malcovery Security: http://cdn2.hubspot.net/hub/241665/file-466107501-pdf/Target.Lessons.Learned.pdf

Webb, T. (2014, June 25). Target lawyer suggests mediation for resolving data breach lawsuits. Retrieved from TwinCities.com: http://www.twincities.com/ci_26032089/target-lawyer-suggests-mediation-resolving-data-breach-lawsuits

Ziobro, P. (2014, February 26). Target earnings slide 46% after data breach. Retrieved from THE WALL STREET JOURNAL: http://online.wsj.com/news/articles/SB10001424052702304255604579406694182132568

Teri Radichel, teri@radicalsoftware.com

© 2014 The SANS Institute Author retains full rights.