Interested in learning more about security?

SANS Institute InfoSec Reading Room

Security Skills Assessment and Training: The Critical Security Control that can make or break all others

Data breaches and identify theft have arguably occurred since information has been stored and utilized in modern times. As the nature of information has shifted from hard copy forms and print materials into digital format stored, accessed and transmitted across the globe in the blink of an eye, the ease in which that information is used and misused has changed dramatically. The evolution of technology has given rise to the information assets, electronic bits and bytes that create value. Information as an asset has f...

Security Skills Assessment and Training: The "Make or Break" Critical Security Control

GIAC (GSLC) Gold Certification
Author: Paul Hershberger; pjhersh13@gmail.com
Advisor: Barbara Filkins
Accepted: Oct 24, 2014

Abstract

Data breaches and identify theft have arguably occurred since information has been stored and utilized in modern times. As the nature of information has shifted from hard copy forms and print materials into digital format stored, accessed and transmitted across the globe in the blink of an eye, the ease in which that information is used and misused has changed dramatically. The evolution of technology has given rise to the information assets, electronic bits and bytes that create value. Information as an asset has fueled the growth of cybercrime organizations and driven innovation in the way those cybercrime organizations operate. The perceived ability to create almost limitless cash flow through theft of information assets has resulted in the crime known as a data breach.

As the criminal organizations have been developing their skills and honing their craft, the information security industry has been thriving as well. The information security industry responded with a never-ending supply of processes, technology and frameworks, that for a price will solve all of the victimized companies' cybercrime problems, of course until the cyber criminals change their attacks. As information protection spending has exploded, little has been done to effectively slow the tide of data breaches. Although tools, technologies and frameworks are critical to the ability to protect against data breaches, the fact remains that this is a battle being waged between intelligent individuals, people behind tools on both sides of this fight. This paper explores recent data breaches and discusses how the technology deployed to protect the information

worked as intended; however, the persons behind the tools became the weak link resulting in the loss of personal information.

1. Introduction

Across the security community, 2013 has been noted as the year of the breach. Symantec reported 8 breaches with more than 10M identities exposed per breach representing a 700% increase from the year prior(Symantec Corporation, 2014). The year was filled with salacious headlines pulling readers across into the latest exploits of cyber crime and espionage rings. Setting the tone for the year was the Mandiant APT-1 report released in Feb 2013. The team at Mandiant released detailed documentation and analysis of the APT-1 threat group and publicly identifying China's 2nd Bureau of the People's Liberation Army General Staff Department 3rd Department (Military Cover Designator 61389)(Mandiant, 2013). The year continued with reports of password database breaches on an almost monthly basis. On top of it all there was the periodic resurfacing of Anonymous and their string of #op flavor of the day, the continued expansion of the Blackhole exploit kit, the rise of the Crypto Locker ransom ware and the Syrian Electronic Army. News reporters and the information security community were busy, dazed, and possibly, a little confused. Rounding out the blurring haze of the year were reports of breach at Neiman Marcus and the loss of 110 million identities by Target. As details became public on the multitude of breaches and incidents throughout the year, an extensive amount of effort went into identifying the gaps in security controls that allowed the attackers to operate unnoticed by the victims' organization(s). Through all of the detailed analysis, the primary focus has been on the technical controls such as network segmentation, data loss prevention, least privilege access, audit logging and boundary defenses, but very little focus on the people behind those controls. The focus on tools and technology reflects a general bias toward a tools based approach to information security. The tools based approach is one that measures the level of security by the tools and a technology deployed, and is rooted in the assumption that the company with the largest inventory of the latest tools must be the most secure. Although tools and technical controls are critical to protect sensitive data within an organization, they are only as

effective as the people designing and operating them. Using historical information about data breaches, the information security industry and publicly available information about the Target Corporation and Neiman Marcus breaches this paper will discuss how the tools based approach to security has failed the security community, the companies and individuals who entrust their most sensitive data to the care and protection of that community. Additional discussion will show how the SANS Critical Security Control #9 Security Skills Assessment and Appropriate Training to Fill Gaps(CSC 9)(SANS Institute), is critical to changing the current direction of the information security community.

1.1 SANS Critical Security Controls

In 2008 the National Security Agency (NSA) initiated an effort to shift security focus away from compliance centric security programs and began to identify a set of controls that are designed around the threat and focused on controls that directly address the way attackers operate. In collaboration between public and private organizations across the globe a set of Critical Security Controls were identified, coordinated by the SANS Institute, those controls became known as the SANS 20 Critical Security Controls (Institute). The 20 Critical Controls are:

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, 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

Like most information security frameworks the 20 Critical Security Controls can be tied back to the National Institute of Standards and Technology (NIST) SP 800-53. What differentiates the 20 Critical Security Controls from other frameworks developed over the years is the focus on what is effective in defending against advanced attackers rather than what is auditable. An important part of what makes this framework one that focuses on operational effectiveness is the inclusion of CSC 9, the skilled people behind the tools and processes.

1.2 The Lockheed Martin Kill Chain Analysis

Driven by the growing Advanced Persistent Threat (APT) and the need to change how they approached information protection, researchers at Lockheed Martin Corporation published a paper entitled Intelligence-Driven Computer Network Defense (Hutchins, Eric M.; Coppert, Michael J.; Amin, Rohan M., 2011). The paper defined a framework to incorporate threat intelligence driven by attacker activities into the defensive strategies of an organization. The approach defined within the framework was to learn as much as possible about your attackers, through the course of incident investigation and remediation. The security analyst can then identify patterns in attack activities and use those patterns to anticipate the next attack, and in turn stop that attack before it can start. The framework, as detailed in the report relies heavily on the incident responder and their ability to learn the objectives, tactics and techniques of the adversaries they face. One of the most widely discussed and adopted elements of the Lockheed Martin framework is the intrusion kill chain. The intrusion kill chain defines the attack cycle into seven phases of activity; Reconnaissance, Weaponization, Delivery, Exploitation, Installation, C2, and Action on Objectives. Among the elements of security operations and control activities detailed in their research, the team from Lockheed Martin published a matrix of actions defenders can take to disrupt the attackers at various stages of the kill chain as shown in Figure 1.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Figure 1.Lockheed Martin Courses of Action Matrix. Reprinted from "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain" by Eric M. Hutchins, Michael K. Cloppert, Rohan M. Amin, Ph.D., Lockheed Martin Corporation, 2011 p.5

The course of action matrix provides a high level overview of technical capabilities although the narrative and focus of the Lockheed Martin report was a balance of capabilities from the technology, process and people perspective. The security industry bias toward tools and technology has caused the narrative around the Lockheed Martin framework to become slanted away from that balance and focuses primarily on the tools and technology. By removing the industry bias and looking at the concepts outlined in the framework, the need for skilled people at all levels of the organization becomes evident. An adaptive security posture and program driven by attacker intelligence requires people who can analyze and interpret the intelligence and make changes to the defensive posture accordingly. That adaptation simply cannot be configured into a tool. This balanced approach closely aligns the Lockheed Martin framework with the SANS 20 Critical Security Controls.

1.3 Information Technology (IT) and Cyber Security Leadership (CSL):

The information security community faces a dilemma of its own making and one that could be argued to stem from a broader IT community problem. Leadership in IT and

cyber security is often viewed as a general management function in which the requirements for success is a base level of managerial competencies. In the wake of the Target breach the Chief Information Officer (CIO) at Target, Beth Jacob, resigned from the role that she held since 2008(Press, 2014). Prior to being appointed as the CIO, Jacob started with Target as an assistant buyer and continued to hold several positions within Target in the area of guest contact and operations. Jacob was noted as an accomplished executive and business leader, the lack of direct experience in IT can be seen as a contributor to the problems at Target that resulted in one of the largest data breaches in history. The realization of the value of relevant IT experience at the CIO level by Target was highlighted by the replacement of Jacob with Bob DeRodes, an executive with more than 40 years of IT experience (Target Corporation, 2014).

In a recent interview with Gov Info Security (Chabrow, 2014), Michael Daniel, White House Cyber Security Coordinator, stated that his lack of technical expertise was a key asset to his position overseeing the government cyber security strategies and policies. Daniel goes on to say "Being too down in the weeds at the technical level could actually be a little bit of a distraction," (2014). An argument can be made that Mr. Daniel is correct in his assessment of being "too down in the weeds" as detrimental to the role and that at the senior leadership level, the position needs general leadership qualities and the ability to bring together a team capable of meeting the challenges faced by the organization. In order to accept that argument, one must overlook the importance of strategic leadership and how top level strategy influences and shapes the organization and operation under that leadership. Organizational culture, external influencers, market trends and personal background and experience all play in integral part in shaping the strategic direction of an organization. Without direct relevant experience to build upon, leadership is left with culture, external factors and market trends to influence strategic direction. Strategic direction driven by culture and market trends remains susceptible to industry bias which can degrade operational effectiveness. When applied to information security this bias and can lead to the propagation of a tools based approach to security.

1.4 The Information Security Market

In 2002 the information security industry was estimated to be $3.5 billion and clearly dominated by five vendors focused primarily on providing anti-virus solutions (Gordon, 2014). Since 2002 the information security industry has grown and is projected to reach $73 billion by the end of 2014(Gordon, 2014). This market has expanded to cover over 80 unique product types and by one account is projected to grow to become a $639 billion industry by 2023(Stiennon, 2013). With this large of a market at stake and the continued optimistic outlook for growth, the software companies have their marketing teams in high gear driving home the message that their latest tool is the answer to all your security problems. The message is "buy our product and protect your information".

The FireEye products solution overview discusses the FireEye Threat Prevention Platform stating (FireEye):

> *The FireEye Threat Prevention Platform combats today's advanced cyber attacks. The FireEye platform is designed from the ground up to stop advanced malware used by cybercriminals and advanced persistent threat (APT) actors. Each FireEye platform features the patented Multi-Vector Virtual Execution (MVX) engine that provides state-of-the-art, signature-less analysis along with proprietary virtual machines within its core to identify and block cyber attacks that may leverage one or more threat vectors to infect a client (e.g., targeted emails with embedded URLs or malicious documents).*

Blue Coat markets their Advanced Threat Protection solution stating(Blue Coat):

> *The Blue Coat Advanced Threat Protection solution integrates technologies from the Blue Coat Security and Policy Enforcement Center and the Resolution Center to deliver a comprehensive lifecycle defense that fortifies the network. The solution*
>
> - *Blocks known advanced persistent threats*
> - *Proactively detects unknown and already-present malware*
> - *Automates post-intrusion incident containment and resolution.*

The constant barrage of skillful marketing drives the information security industry harder and harder toward the tool based solution to information protection. As a senior leader responsible for information protection within an organization, it can be difficult to ignore

the marketing when there are gaps in personal skills and cyber security experience. When skill gaps in senior level IT and CSL exist, the information security industry marketing machines have a potential to drive cyber security strategies in their direction.

The marketing machines are driving home the message that their associated tool(s) are the answer to all of the security problems plaguing companies. They paint a picture that their tools are user friendly enough that anyone can operate them with a minimal amount of training on how to navigate the user interface. The resulting mind set is that you can simply plug it in, set it up and gain instant, lasting protection. The marketing targets senior level executives who define strategy, but often lack the personal experience to filter out the marketing noise. As a result the level of security for a company becomes defined by the tools implemented rather than the skills and capabilities of the security team.

2 Data Breaches

An information security breach or data breach is commonly known to be an event in which an unauthorized party gains access to sensitive information such as medical, financial or identity related information, such as social security, credit card, or drivers' license numbers. Although data breaches have likely been occurring since computers were connected to the internet, they have been formally tracked and recorded since roughly 2005. Two noted non-profit organizations who compile information and statistics on date breaches are The Identity Theft Resource Center (ITRC), and The Privacy Rights Clearinghouse (PRC). The IRTC reports 4,579 data breaches covering 630,870,450 records exposed between 2005 and June 2014(Identity Theft Resource Center). Their analysis of recent data breaches by the ITRC show that the largest single percentage of breaches (26.1%) in 2013 were a result of hacking activities (ITRC Breach Statistics: 2005-2013). The PRC publishes details on 4,311 data breaches which have exposed 867,647,607 records (Privacy Rights Clearinghouse, 2013). Additionally the PRC classifies 24% of the breaches from 2005 to present as being attributed to hacking. Although the numbers differ between the two organizations, the message is the same, an astonishing amount of data continues to be exposed and hacking is the most common

path to exposure. The information security industry is driving an approach for protecting the sensitive information that simply isn't working and something has to.

2.1 Targeting Target

On Dec 18, 2013, investigative reporter Brian Krebs published a story on his web site KrebsonSecurity (Krebs, Sources: Target Investigating Data Breach, 2013)sighting multiple reliable sources, stating that Target Brands Inc. was investigating a data breach. At the time of publish it was unclear as to how large the breach exactly was, however speculation was that it could rank up there with some of the largest breaches recorded to date. On Dec 19, 2013 Target Corporation published a press release on their Corporate Internet site confirming "unauthorized access to payment card data in U.S. stores"(Target Corporation, 2013). The acknowledgement by Target of the breach set the wheels in motion for what is arguably the most publicly discussed and documented breaches to date. The results of the multiple independent reports and analysis by a host of information security vendors was used by the U.S. Senate Committee on Commerce Science, and Transportation to produce a Majority Staff report for Chairman Rockefeller on March 26 2014 entitled A "Kill Chain" Analysis of the 2013 Target Data Breach(Committee on Commerce, Science, and Transportation, 2014). The detailed analysis by the U.S. Senate Committee included the creation of a timeline of attacker and Target activities over the course of the breach as see in figure 2.

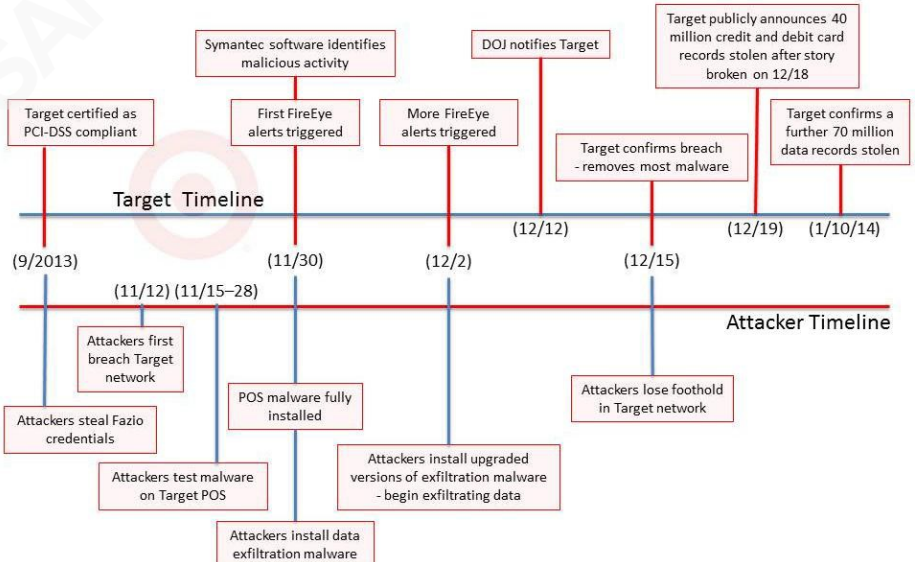

Figure 2.Target Attack Timeline Analysis. Reprinted from "A "Kill Chain" Analysis of the 2013 Target Data Breach" By the United States Senate Committee on Commerce, Science, and Transportation, 2014 p. 12

The report to the U.S. Senate Committee on Commerce and Science and Transportation included and analysis of the Target breach, based on the Lockheed Martin Kill Chain framework that highlighted the security gaps that allowed the Target attackers to be successfully. (See Figure 3.) The analysis specifically identifies four key control failures within the Target security program.

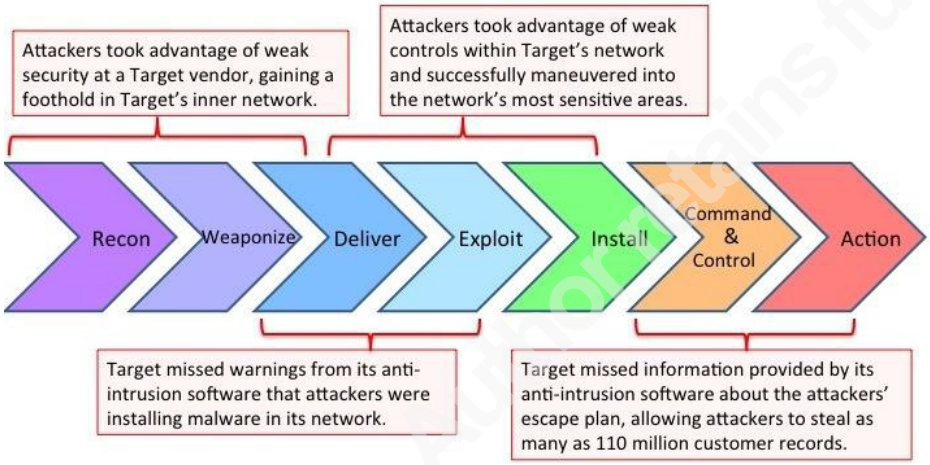

Figure 3. Target kill chain analysis. Reprinted from "A "Kill Chain" Analysis of the 2013 Target Data Breach" By the United States Senate Committee on Commerce, Science, and Transportation, 2014 p. 11

The first opportunity missed by the Target security team was an alert by the anti-intrusion software that created when the attackers installed malware on the Target network. As reported by Bloomberg Businessweek (Riley, Elgin, Lawrence, & Matlack, 2014) six months prior to the breach, Target had deployed an anti-malware solution produced by the security technology firm FireEye. The FireEye solution is an advanced malware detection and prevention tool that enables the customer to identify malware across large dispersed networks. The FireEye solution is known for its shared intelligence model in which information and indicators of malware identified by one customer is rapidly shared with and used in the protection of all customers globally. On Nov 30th the FireEye solution issued an alert for unfamiliar malware with a label of "malware.binary". The alert was reported to be categorized at the top of the FireEye severity scale and acknowledged by the Target monitoring center in BangaloreIndia, which in turn escalated the alert to the Target Security Operations Center (SOC) in Minneapolis MN, the SOC took no action (Riley, Elgin, Lawrence, & Matlack, 2014). The FireEye solution again

generated alerts on Dec 2nd when the attackers installed a new version of malware on the Target computers in preparation for ex-filtration of the data collected over the weeks they were operating freely within the Target network; yet again the alerts resulted in no response from the Target Security team.

The two remaining control failures noted in the Senate report focused on the areas of remote access controls and network segmentation of the Target network. As reported by Brian Krebs (Krebs, Target Hackers Broke in Via HVAC Company, 2014) the target attackers accessed the Target network after compromising the user credentials for an employee of Fazio Mechanical Services, a Pennsylvania based refrigeration and HVAC systems service provider. The credentials compromised were used by the staff at Fazio to connect to the Target vendor management system for the purpose of billing, contract submission and project management. Once a foothold was established on a Target system, via the Fazio Mechanical Services user account, the attackers reportedly leveraged a service account used by the BMC Software IT management software product installed on Target's network (Krebs, New Clues in the Target Breach, 2014). The service account password appeared to have been compromised by the attackers and allowed them to gain access into the most sensitive areas of the Target network including access to the Point of Sale systems which allowed them to collect and steal credit card data at will.

Looking at Target through the lens of the security industry and applying the bias of tools based approach to security one would have to conclude that they were a very secure organization. Target deployed some of the latest tools to protect their systems, they invested significant amounts of money in their security operations and met all of their compliance requirements to include Payment Card Industry (PCI) security standards, yet those tools failed to stop the actions of an attacker that compromised 110 million identities. The tools were all in place and operated as intended, they created alerts, they raised the alarm, they notified the people they were supposed to notify and that's where the protection ended. The people entrusted to operate the tools and translate the data into action failed to recognize the importance of what they were presented by the tools and in turn the attackers accomplished their mission.

Paul Hershberger, pjhersh13@gmail.com

2.2 Neiman Marcus

Target wasn't alone in this. Upscale retailer Neiman Marcus was reported by Brian Krebs (Hackers Steal Card Data from Neiman Marcus, 2014) to have acknowledged an investigation into a potential data breach in which they were working with the U.S. Secret Service on. Neiman Marcus acknowledged at that time they were notified in mid-December 2013 of the potential breach. Bloomberg Businessweek published an overview of the breach after reviewing a detailed report prepared for Neiman Marcus by the consulting firm Protiviti (Elgin, Lawrence, & Riley, 2014). The Bloomberg report went on to provide an alarming story of missed opportunities by the security team at Neiman Marcus. Reportedly the attackers gained access to the Neiman Marcus network in March of 2013. Once inside the network they spent four months performing reconnaissance of the environment and designing their approach to stealing credit card data. They moved into action on July 16 when they installed their malware and started collecting credit card data. From July until Dec 2013 attackers operated malware and collected credit card data within the Neiman Marcus network. Like Target, Neiman Marcus had deployed a host of anti-malware tools and technologies. Those tools were configured to remove malware from systems when it was identified, however they did not have their solutions configured to block the malware from operating. Although this slowed the progress of the attackers, the attacker had an answer. The attackers assessed the environment and proceeded to simply re-install the malware on a daily basis. During the time in which the attackers were operating in the Neiman Marcus network they triggered roughly 60,000 individual alerts but those alerts resulted in no response by the Neiman Marcus security team.

Much like Target, the tools and technologies did everything they were supposed to do, they removed malware from the Neiman Marcus environment on a daily basis like clockwork, but they were working against people on the attackers' side. The people behind the malware adapted and found ways to overcome the technology put in place to stop them. With no one to adapt the protection, the attackers continued to operate at will and victimize the customers of Neiman Marcus. Again the tools based approach to information protection broke down. That breakdown was not a failure of the tools, the

tools performed as designed; they did exactly what they were deployed to do. The failure was a result of the people who configured them and subsequently failed to take action when the tools generated alerts about the attacker actions.

2.3 A View from the Top

Feb 4th 2014 the United States Senate Committee on the Judiciary convened for a session entitled Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime. As part of the session included testimony from John Mulligan, Chief Financial Officer from Target Corporation and Michael Kingston Chief Information Officer for Niemen Marcus. Both officers addressed the committee with prepared remarks, Mr. Mulligan stated (Mulligan, 2014):

> *"For many years, Target has invested significant capital and resources in security technology, personnel and processes. We had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools. We perform internal and external validation and benchmarking assessments. And, as recently as September 2013, our systems were certified as compliant with the Payment Card Industry Data Security Standards."*

While Mr. Kingston stated (Kingston, 2014):

> *"Our security measures included numerous firewalls at the corporate and store level, network segmentation, a customized tokenization tool, numerous encryption methods, an intrusion detection system, a two-factor authentication requirement, and use of industry-standard and centrally-managed enterprise anti-virus software."*

In their testimony, both executives focused heavily on the technical aspects of the organization's information security program with only minimal reference to the human aspect of information security. It was widely reported that neither organization had a Chief Information Security Officer (CISO) with responsibility for the information security program. In the case of Target Corporation, information security responsibility was said to be distributed across multiple executives and driven mainly by compliance requirements. The lack of leadership at the executive level was the initial failing of both

organizations. Executive leadership with a clear understanding of the challenges faced by information security teams sets the tone for the organization. Understanding the risks of cyber threats and how to deploy teams of skilled practitioners to address those risks is crucial to an organization's ability to protect the information entrusted to them. In the absence of executive level leadership the information security team is most likely to struggle with the ability to obtain organization support, budget and staffing to adequately protect the environment.

The lack of executive level security leadership cascaded across those organizations and negatively impacted the effectiveness of the teams responsible for executing the mission of protecting the information entrusted to the organization. As referenced earlier both Target and Neiman Marcus deployed technical solutions that alerted their security teams when the attackers were operating within their corporate environment, though neither company recognized or acted on those alerts. Both organizations had the tools and technology deployed to protect their data, but the apparently lacked the skills to make those tools effective. The organization issues continued to surface at Target, as reported by the Wall Street Journal (Yardon, Ziobro, & Barrett, 2014), members of the information security team within Target warned about vulnerabilities to the Point of Sale (POS) terminals months before the breach. The warnings were reportedly "brushed off" by Target management and no action was taken. The identification of potential issues prior to the breach by Target staff indicates that there were skilled security professionals within the organization that were capable of assessing potential issues and defining a need for action. The apparent lack of action taken to address the potential vulnerabilities highlights the breakdown in the organization's information security leadership. For concerns to go unaddressed within the organization it is presumed that gaps in the security skills at multiple levels within the organization must have existed, beyond the publicly emphasized absence of a CISO providing leadership to the information security team.

Although there are less public reports about the internal struggles of the Neiman Marcus information security team, the lack of a CISO and the high volume of missed alerts can be assumed to exemplify a systemic lack of information security understanding. This

lack of understanding resulted in one of two potential scenarios. Either nobody was monitoring the alerts from their tools or the people monitoring the tools didn't have the necessary skills to interpret the data and recognize malicious activity. They appeared to have an approach of configuring tools and walking away from them. This approach can be attributed to a lack of understanding of the threat actors and the level of diligence they will place on their efforts to execute an attack. The reported 60,000 alerts generated by the technical solutions deployed by Neiman Marcus (Elgin, Lawrence, & Riley, 2014) highlights the shortcomings in the tools based approach to information protection.

3 Capabilities Based Security

There is no shortage of frameworks, models, standards and checklists intended to guide the development and implementation of security controls within organizations today. Each framework adds value in one way or another; however their true potential is difficult to achieve unless the capabilities and skills of the team behind the frameworks are developed. When working for the Defense Information Systems Agency (DISA), Tim Treat developed a model of information security operations that focuses on the key capabilities needed in any type of cyber operation (Treat, 2014). The framework is built around the following 11 core capabilities;

- Command and Control
- Situational Awareness
- Visibility (Network, Device and Endpoint)
- Event/Attack identification and Triage
- Configuration Control and Governance Monitoring
- Collaboration
- Continuity of Operations
- Active Isolation
- Hunting
- Threat Intelligence and Indicator Management
- Critical Information Identification and Tracking

Defining the capabilities needed by an information security team, allows CSL continue to define the skills necessary for the team members who support those core capabilities. The National Institute for Science and Technology (NIST), National Initiative for Cybersecurity Education (NICE) campaign, created The National Cybersecurity

Workforce Framework (The NICE Framework)(National Initiative for Cybersecurity Education). The Framework provides guidance around the skills necessary for all levels of cyber security from CISO down to the network cabling technician. Understanding the skills through the NICE Framework and mapping those skills to the organizational capabilities creates a foundation on which CSC 9 can be implemented across an organization. The implementation guide for CSC 9 starts with the need for a gap analysis of the organization, this gap analysis is only possible once the capabilities and skills needed by the organization are understood. Using the inventory of required skills CSL can identify the gaps, define strategies for remediating the gaps and start the process of implementing the intent behind CSC 9. By fully implementing CSC 9 aligned to the NICE framework and supporting organizational capabilities, an information security team can move beyond a focus on tools and build the capabilities to meet the attackers on equal ground. Providing effective information protection and turning around the trends of data breaches as we know them today.

4 Conclusion:

The collective information security community comprised of vendors, service providers, technicians and leadership across all types of organizations globally is facing a dilemma. Business is good as a security vendor and service provider, the market is booming and projected to continue to grow for the foreseeable future. That growth has done little to slow the rate of data breaches because the strategies put in place to stop them simply don't work. There are a multitude of arguments as to why the strategies don't work and many of those arguments focus on dollars spent or tools deployed at companies but evidence shows that the issue is much greater than that. The information security teams continues to focus outward for solutions rather than directing attention inward at the people behind the strategies and those who are charged with configuring and operating the multitude of high priced tools deployed across organizations. The CSC 9, "Security Skills Assessment and Appropriate Training to Fill Gaps" provides guidance on how to change the current direction. Skills assessment supported by The NICE Framework, provides guidance around the skills necessary for all levels of Cybersecurity from CISO

down to the network cabling technician. Ensuring the right knowledge and skills supports the development of organizational capabilities at all levels is critical to building an effective information protection program. This starts at the top, with a senior leader that has a solid foundation in technology and understands the threats faced by the organization. They must be able to filter through the marketing buzz words and news headlines to develop strategic direction that balances tools and technology with the people capable of leveraging that technology effectively. A focus on skills starting at the top helps ensure that skills based capabilities cascade down through the organization and fosters an environment of innovation and continual skill development. Only through this level of organizational commitment to skills development, organizations will realize the continually evolving defenses as intended by the Lockheed Martin Kill Chain Analysis. When you step back and review the full breadth and depth of the SANS 20 Critical Security Controls, they lay out a comprehensive capability based framework for effective information security programs. An organization can certainly implement each of the other 19 controls to the letter of the framework and be proud of what they have accomplished. They will also miss the mark on the intention of the framework unless they focus on the people behind those controls and ensure that CSC 9 is fully implemented across all levels of the organization.

Although the headlines may sound like there is no hope for the security community and there is no way to stop the constant barrage of data breaches, all is not lost. Yes, there are significant changes that must happen across the security community, those changes start with a focus on skills at all levels of the organization. The SANS Critical Control, Security Skills Assessment and Training is the key to realizing those changes and altering the course of data breaches.

Paul Hershberger, pjhersh13@gmail.com

References

Blue Coat. (n.d.). *Blue Coat*. Retrieved September 6, 2014, from Advanced Threat Protection: https://www.bluecoat.com/advanced-threat-protection

Chabrow, E. (2014, August 21). *Michael Daniel's Path to the White House*. Retrieved September 6, 2014, from Gov Info Security: http://www.govinfosecurity.com/interviews/michael-daniels-path-to-white-house-i-2422

Committee on Commerce, Science, and Transportation. (2014). *A "Kill Chain" Analysis of teh 2013 Target Data Breach.* Washington: United States Senate.

Elgin, B., Lawrence, D., & Riley, M. (2014, February 21). *Bloomberg Business Week*. Retrieved June 14, 2014, from Neiman Macus Hackers Set off 60,000 Alerts While Bagging Credit Card Data: http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

FireEye. (n.d.). *FireEye*. Retrieved September 6, 2014, from FireEye Products and Solutions Overview: http://www.fireeye.com/products-and-solutions/

Gordon, R. (2014, May 8). *The Cyber Security Market is Hot! Here's why*. Retrieved September 6, 2014, from Dark Reading: http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128

Hackers Steal Card Data from Neiman Marcus. (2014, Jan 10). Retrieved July 19, 2014, from krebson Security: http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/

Hutchins, Eric M.; Coppert, Michael J.; Amin, Rohan M. (2011, March). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain.* Retrieved June 28, 2014, from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Identity Theft Resource Center. (n.d.). Retrieved June 28, 2014, from itrc: http://www.idtheftcenter.org/images/breach/20052013UPDATEDSummary.jpg

Institute, S. (n.d.). *Critical Security Controls*. Retrieved July 19, 2014, from SANS Institute: http://www.sans.org/critical-security-controls/

ITRC Breach Statistics: 2005-2013. (n.d.). Retrieved June 28, 2014, from itrc: http://www.idtheftcenter.org/id-theft/data-breaches.html

Paul Hershberger, pjhersh13@gmail.com

Kingston, M. (2014, Feb 14). *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime.* Retrieved July 19, 2014, from United States Senate Committee on the Judiciary: http://www.judiciary.senate.gov/imo/media/doc/02-04-14KingstonTestimony.pdf

Krebs, B. (2014, Jan 29). *New Clues in the Target Breach*. Retrieved July 19, 2014, from KrebsonSecurity: http://krebsonsecurity.com/2014/01/new-clues-in-the-target-breach/

Krebs, B. (2013, December 13). *Sources: Target Investigating Data Breach*. Retrieved June 14, 2014, from KrebsonSecurity: http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/

Krebs, B. (2014, Feb 5). *Target Hackers Broke in Via HVAC Company*. Retrieved June 14, 2014, from KrebsonSecurity: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Mandiant. (2013). *APT1 Esposing One of China's Cyber Espoinage Units.* Alexandria: Mandiant.

Mulligan, J. (2014, Feb 14). *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime.* Retrieved July 19, 2014, from Uinted States Senate COmmittee on the Judiciary: http://www.judiciary.senate.gov/imo/media/doc/02-04-14MulliganTestimony.pdf

National Initiative for Cybersecurity Education. (n.d.). *The National Initiative for Cybersecurity Education.* Retrieved September 6, 2014, from The National Cybersecurity Workforce Framework: http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf

Press, T. A. (2014, March 5). *Target's Chief Information Officer Resigns*. Retrieved Sepember 6, 2014, from The New York Times: http://www.nytimes.com/2014/03/06/business/targets-chief-information-officer-resigns.html?_r=0

Privacy Rights Clearinghouse. (2013, December 31). Retrieved June 28, 2014, from PRC: https://www.privacyrights.org/data-breach

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 13). *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*. Retrieved July 19, 2014, from Bloomberg Businessweek Technology: http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

SANS Institute. (n.d.). *Critical Security Contorl: 9*. Retrieved June 14, 2014, from SANS: http://www.sans.org/critical-security-controls/control/9

Paul Hershberger, pjhersh13@gmail.com

Stiennon, R. (2013, August 14). *IT Security Industry to Expand Tenfold*. Retrieved September 6, 2014, from Forbes: http://www.forbes.com/sites/richardstiennon/2013/08/14/it-security-industry-to-expand-tenfold/

Symantec Corporation. (2014). *Internet Security Threat Report 2014.* Symantec Corporation.

Target Corporation. (2014, April 29). *Target Appoints New Chief Information Officer, Outlines Updates on Security Enhancementss*. Retrieved Oct 8, 2014, from Target Press Room: http://pressroom.target.com/news/target-appoints-new-chief-information-officer-outlines-updates-on-security-enhancements

Target Corporation. (2013, December 19). *Target Press Room*. Retrieved June 14, 2014, from Target Confirms Unauthorized Acess to Payment Card Data in U.S. Stores: http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores

Treat, T. (2014, Sepember 15). Capabilities Based Securty. (P. Hershberger, Interviewer)

Yardon, D., Ziobro, P., & Barrett, D. (2014, Feb 14). *Target Warned of Vulnerabilities Before Data Breach.* Retrieved July 20, 2014, from The Wall Street Journal OnLine: http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690

Paul Hershberger, pjhersh13@gmail.com

Last Updated: May 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced