Global Information Assurance Certification Paper

Corporate Identity Fraud:

Life-Cycle Management of Corporate Identity Assets

GSEC Gold Certification

Author: Bryan K. Fite, bryan.fite@lexisnexis.com

Adviser: Lori Homsher

Accepted: January 23rd 2006

Outline

1.Introduction

The advent of the World Wide Web has provided many new and innovative ways for organizations to conduct business. It has also exposed organizations to new and innovative forms of trademark & brand abuse.

Corporate Identity Fraud can be defined as the abuse of traditional and non-traditional identity assets with the intent to divert, deceive or defraud consumers.

Trademarks and brands are traditional corporate identity assets. Trademark enforcement and brand protection programs are governed by legal precedence and legacy business procedures. These mature practices are based on very narrow criteria. The litmus test being: Is it "actionable"?

This archaic approach is no longer adequate, because it is steeped in the "brick and mortar" world of the recent past. In the new marketplace, many assets are not kept in bank vaults or protected by fences and guards. In addition, standards of conduct and laws are not universally defined or enforced.

Organizations have created new non-traditional corporate identity assets by embracing the Internet. Websites, domain names, email addresses and subscribers are just a few of these new assets. It is imperative that they be afforded protection commensurate with their value. Any comprehensive trademark and brand protection program must address these evolving threats.

2.Threats

Trademarks, brands, logos, mascots, registered domains, email addresses and even key personnel can all be classified as **Corporate Identity Assets**. Once viewed as an asset, we can use traditional risk assessment techniques to identify our exposure and formulate an appropriate response.

In order to determine the residual risk within in an existing program or to define the requirements for a new program, it is important to understand the threat landscape. Essentially, these are all of the known "bad things" that COULD happen to your corporate identity asset.

Spoofing is the term used to describe the electronic impersonation of an IP address, email address or other electronic identity asset. The use of this technique is usually malicious in nature since its purpose is to deceive.

Example: A forged email is sent to someone from their boss's boss asking them to take some kind of action. If the victim executes the action then the fraud attempt was successful. This type of fraud is not new and can be executed using alternative communications methods including fax, telephone, paging and others.

This can be a highly effective attack and is typically easy to execute especially for the skilled attacker.

Phishing is a form of SPAM (unsolicited commercial email). In this case, the commercial enterprise is illegal; identity fraud, credit card fraud and bank fraud just to name a few. At its core, phishing is designed to steal privileged information by using a combination of social engineering techniques and technology.

Example: An email is crafted to look like an official message from a credit card company's fraud abuse department (irony). The message asks the potential victim to provide privileged information: social security number, address, birth date, passwords, bank account numbers and/or credit card numbers. If the recipient responds with the sensitive information the ruse has achieved its objective.

Many Phishing attacks attempt to contact the largest possible number of targets. Therefore, harvested email addresses are often indiscriminately "Phished". The idea being; the wider you cast your net the more victims you will catch. A recent study conducted by America Online and the National Cyber Security Alliance found 61% of online users have received a phishing attempt in the past.

Another method criminals use involves highly targeted attacks that do not indiscriminately send email to unrelated targets. This type of Phishing is called "Spear Phishing". These scams sometimes use malicious software, called "Crimeware", to capture privileged information or take command & control of a victim's computer. Keyboard loggers are a favorite piece of Crimeware. By monitoring each keystroke the criminals can obtain privileged information.

Pharming is the practice of creating a forged website or other online forum designed to deceive the potential victim. By impersonating a trusted partner, criminals trick victims into revealing privileged information: social security numbers, addresses, birth dates, passwords, bank account numbers and/or credit card numbers.

Example: An attacker registers a dot com domain name that is a variation or misspelling of a trusted Corporate Identity Asset. In this case, a home banking

service is impersonated. Legitimate users of the home banking services are duped into believing that the bogus site is legitimate. Victims enter their usernames and passwords which are captured at the bogus site.

This is a highly effective attack because the bogus websites are exact duplicates. They can even broker transactions between the victim and the legitimate website. This allows the attacker to compromise sensitive information without causing the victim to become suspicious and possibly report the problem to the legitimate trusted partner's help desk. This technique is commonly referred to as a "Man-in-the-Middle" attack.

In addition, criminals use Spyware and malicious Adware to modify host files, DNS queries or DNS responses. This allows the criminals to divert victims from the legitimate partner site to a comprised site controlled by the criminal. According to scans performed by AOL/NCSA in support of their recent study, 61% of all respondents had some form of Spyware or Adware installed on their computer.

3. Asset Valuation

To develop a reasonable approach for addressing these threats, Corporate Identity Assets must be identified and recognized as assets by the organization. A relative value should be assigned to each asset. This will aid in the prioritization exercises that inevitably occur during management discussions. High, medium and low are perfectly acceptable classifications for this purpose.

Corporate Identity Assets can include but are not limited to:

- Trademarks/Service Marks/Logos
- Domain Names & Email addresses

- SSL Certificates,
- Cryptographic Keys/Digital Signatures
- IP Address Space
- Vanity Phone Numbers
- Online Forum Identities
- Personal Identities of Key Human Associates

Asset valuation should take into account the impact of losing that asset or having its value diluted. One way to view the problem is to consider the impact in terms of revenue, reputation, regulation and overall strategic importance of the asset. If you have a business continuity plan, it makes sense to incorporate these assets into the Business Impact Analysis section of the plan.

If a brand is considered to be a high-value Corporate Identity Asset then all of the Corporate Identity Assets related to that brand must also be classified as high-value.

It is important to recognize that these are not traditional physical assets but rather virtual and intangible in nature. This creates new and unique challenges for those responsible for protecting Corporate Identity Assets. However, this paper will describe practical and effective practices that can be employed to mitigate risk.

4. Roles and Responsibilities

An effective asset protection program must have clearly defined roles and responsibilities.

Regardless of the organizational structure there are two basic roles:

- Asset Owners are responsible for asset valuation, defining custodial requirements and authorizing custodians. Asset valuation should determine the required security controls. Security control requirements should be prescribed by organizational policy.
- Asset Custodians must understand their responsibilities and agree to perform their duties. It is important to formalize and document what is expected from owners and custodians. This can be accomplished through organizational procedures, Service Level Agreements (SLA's) or legally binding contracts.

The traditional practice of Brand Protection is the remit of corporate counsel and/or the marketing department. However, ultimate responsibility for protecting identity assets belongs to the asset owner. Traditional custodian ranks may need to be augmented as the threat evolves. Custodians should expect more requirements to be levied against them and be prepared to refine their practices to accommodate the changing requirements.

5.Identifying Threats

In general, securing assets require us to identify exposures to Confidentiality, Integrity and Availability of a given asset. When we apply this methodology to our Corporate Identity Assets we come up with these high-level threats sometimes referred to as "Bad Outcomes".

If an asset is vulnerable to a threat then a decision must be made to mitigate the risk, accept it or transfer it. We then can look at the likelihood of a particular Bad Outcome occurring. This can be used to create a risk profile associated with a particular asset or group of assets. As discussed early, the asset owner must communicate to the asset custodian(s) what is an acceptable level of risk and the appropriate control requirements.

Corporate Identity Fraud poses significant security challenges. These challenges are compounded by the economic motive fueling this "cottage" industry. Profit is the motivation behind most of these crimes. According to the November 2005 Anti-Phishing Work Group (APWG) Phishing activity report, more than 90% of all Phishing activity is targeted at the financial services sector. This is a great example of Gangster Commerce (G-Commerce). It is organized, effective and profitable!

Unauthorized Access is the end-game of much of the Corporate Identity Fraud activity being perpetrated. Usernames and passwords are the primary control used to provide access to online resources (e-commerce websites, collaboration forums, email and other IP enabled services). Phishing and Pharming for access credentials are effective and can compromise the Confidentiality, Integrity and Availability of online resources.

Theft of Service is a way compromised authentication credentials can be abused by criminals. Normally, this type of fraud is perpetrated against online services that are fee based. It is also a technique used to mask criminal activity.

Brand and Reputation Damage can result from abuses of Corporate Identity Assets. Forged emails can confuse the market place. Bogus websites can defraud clients and partners, while reflecting poorly on the genuine asset owner.

Distributed Denial of Service (DDoS) attacks can be perpetrated by compromising a corporate identity asset. Legitimate customers could be duped into executing large numbers of inquires or connection attempts to organizational resources causing service outages. This class of threat impacts availability of

resources.

Sensitive Data Compromises can result from a successful Corporate Identity Fraud scam. Sensitive data includes personally identifiable information, usernames, passwords, account numbers, access credentials, credit ratings, medical information and others. The Confidentiality of data is impacted in this class of attacks.

Data Corruption can occur when access controls are compromised. This impacts the integrity of the data.

Civil Litigation is a threat to any organization or individual residing in a litigious environment. As it relates to Corporate Identity Fraud, the threat primarily revolves around "due diligence" questions. If owners or custodians fail in their fiduciary responsibility to safeguard organizational assets they could be exposed to monetary penalties.

Regulatory Fines and Sanctions could result by being out of compliance with government or industrial regulations. Sanctions, fines and imprisonment are all potential penalties for not performing the appropriate "due diligence" or exercising proper custodial control.

It is important to note that any successful attack on Corporate Identity Assets could require public disclosure based on legal interpretation or organization policy. This can impact an organization's reputation, finances or their ability to conduct normal business.

These risks should be clearly understood by the business. If intangible

assets are valuated through sale or acquisition, it is reasonable to use that value for purposes of financial reporting. If the value is significant, corporate governance demands prudent controls. For publicly traded companies this could put Corporate Identity Assets in scope for SOX auditing.

"Corporate Identify Fraud is becoming the perfect crime for cyber criminals due to a failure at the corporate governance level of many banks and other consumer-focused corporations to comply with federal standards for preventing, detecting and reporting criminal acts or infringements against corporate identity assets, i.e., brands and trademarks in the form of domain name owned and registered by cyber criminals.", TrademarkBots.com, Inc.

6.Security Controls

Individual Corporate Identity Assets have different risk profiles. Certain security controls are more effective at mitigating specific risks than other security controls. While a security control may be available, it may not effectively mitigate the right level of risk. On the other hand, the control could be very effective but could prove too costly which would make it unacceptable to the organization. It is important to understand the organization's tolerance for risk and select the most appropriate controls.

Controls come in two categories: Proactive and Reactive. Proactive controls are primarily preventive, while reactive controls are primarily concerned with containment and resolution. Vendor solutions can be further divided into four basic categories; prevent, detect, respond and manage. Appendix B contains a list of some

of the major vendors and solution providers in this space.

Properly implemented these controls have a high affinity for mitigating the associated risk:

Strong Authentication is designed to verify a user's identity in a highly reliable and accurate manner. This control is effective in preventing Unauthorized Access and Identity Spoofing. Multi-Factor authentication (MFA), like RSA's 2 Factor token based authentication and One Time Passwords (OTP) are forms of MFA that are effective in defeating keyboard loggers. Because the password changes every logon or every sixty seconds, the authentication system does not depend on the secrecy of the password. User experience is an important consideration when selecting and implementing strong authentication systems. Systems that are not user friendly will breed user resentment and lead to the development of unsafe user practices like writing passwords on Post-it™ notes.

Policy, Awareness and Accountability is one of the most important classes of control. Organizations must clearly define their security policies and engage in aggressive awareness campaigns to educate their associates, employees and customers. Organizations must constantly enforce their policies by holding all responsible parties accountable. This is imperative to demonstrate proper "due diligence" and custodial control. SANS has numerous sample policies available at their public website.

Registration of key global and country specific domain names can insure they are not available to cyber criminals for abuse. High-value Identity Assets warrant special consideration. Registering misspelled, novel spelling or

purposefully confusing domain names may be an appropriate response. Vendors, like MarkMonitor and Verisign, provide Top Level Domain (TLD) registration, tracking and management tools. Sometime referred to as, "Portfolio Management Portals", these tools are an efficient and effective way to manage large numbers of domain registrations

Monitoring and Watch Services are required for any effective Corporate Identity protection program because Identity Asset abuse can occur on many fronts. These services monitor domain registrations looking for possible abuses of the protected Identity Assets. They can also monitor trademark, service mark and logo use on the Internet in an automated fashion. By using the same techniques that search engines use to catalog the Internet these services can identify possible abuse. Watch services can be developed in-house using open-source resources, by a 3rd party or a combination of the two. A reasonable approach could be some combination of the two based on organizational needs and constraints.

Intelligence Capabilities should be developed and/or acquired to provide decision support to owners and custodians of Corporate Identity Assets. These services should focus on a specific industry or vertical market attack vectors. They attempt to describe and predict specific methods, techniques and tactics used by attackers. This is a form of trend analysis and can be attached to the monitoring & watch services or included in the awareness program.

Baselining services can be a great way to detect anomalous activity. DNS is a service that can be abused to re-direct legitimate web requests to a bogus website. Assuming there is an accurate DNS route baseline, periodic DNS route checks could be performed to expose DNS hijacking attacks.

Legal Protection should be sought for all high-value Identity Assets. Traditional trademark and service mark protections can be leveraged to impose monetary penalties on violators and can form the foundation of an effective Corporate Identity Protection Program.

Law Enforcement is normally engaged after a crime has been committed but can certainly be leveraged in a preventative fashion if there is reasonable indication that a crime is going to be committed. This control normally takes the form of legal action. If the attacks are criminal in nature law enforcement should be involved. Clear criteria for engaging law enforcement should be in place and some understanding of jurisdiction issues should be developed.

Audits should be used to verify compliance with all policies and procedures of record. Audit deficiencies can identify vulnerabilities proactively or uncover existing fraud. A Corporate Identity Rating system should be developed as part of the standards creation.

End-Point Security is an important consideration. It represents the first and last line of defense. Anti-malware fit into this class of controls. They attempt to keep "Crimeware" from infecting user's workstations, thereby protecting them from attack. In addition, a new type of end-point control is emerging. They take the form of browser toolbars or plug-ins. They provide easily identifiable visual queues and rate the "trustworthiness" of a website.

Risk Assessments should be developed to provide a systematic and consistent organizational approach to categorizing Corporate Identity Assets and defining the appropriate security controls.

Gateways and Network Controls have visibility to network service requests and responses. Therefore, proxies, firewalls, intrusion detection systems and intrusion prevention systems can be used to restrict access to known phishing sites, stop "Crimeware" infection, contain compromised workstations and alert staff of malicious activity.

7. Corporate Identity Protection Program

A comprehensive and effective program will incorporate many of the controls previously discussed. Because most Corporate Identity Fraud is perpetrated directly against end-users, customers and partners, organizations might not have direct knowledge that an attack is taking place or has succeeded. The advantage is currently with the criminals. However, a clearly defined organizational wide program that understands the nature of the evolving threats can reduce residual risk.

While it is out of the scope of this document to provide a detailed tutorial on the creation of a custom Corporate Identity Protection Program, it is useful to look at a sample program and the rationale used for security control selection. We will explore the basic elements of a comprehensive program initiated by a fictitious company named HACME.

HACME Corporate Identity Protection Program

Assumptions:

1. This organization has existing high-level security policies
2. This organization's existing brand protection program was antiquated
3. The organization recently ratified program requirements

4. This organization uses the Internet to conduct business
5. Upper management considers this a priority

Protect

1. Business units must identify assets, asset owners and asset custodians [*Action: A series of meetings with the existing owners and custodians take place to create a definitive list of assets, owners and custodians. This list is converted to an authoritative centralized database which references the assets, owners and custodians*]
2. Asset owners must declare a relative asset value [*Action: Asset owners define three basic valuation categories; high, medium and low. They are relative value ranges- Low<=$5,000 Medium=$5,000-$99,000 High>=$100,000. Asset values are assigned and the authoritative database is updated with the values*]
3. Business units must clearly define roles and responsibilities of owners and custodians [*Action: All asset owners are senior executives and will not play a role in the operational aspects of the program. They set the value of the assets, sponsor/fund the program, provide program oversight and act as an escalation path. Custodians handle all other aspects of the program. There are several custodians across three groups; Legal, technical operations and marketing*]
4. Business units must define, implement and formalize a comprehensive Identity Asset Protection Program.
    a. Must be role based [*Action: Owners and custodians agree to setup a formal governance model. They document requirements and assumptions. An internal SLA is drafted. It identifies the specific operational duties, the parameters of their delivery and service commitments. HACME is a large global entity. As such, they have decided to implement a global council to manage their Identity Asset Protection Program. This council reports to Executive management and asset owners*].
    b. Must be auditable and repeatable [*Action: Procedures are properly documented and clearly communicated. All council meetings are recorded for posterity.*]
    c. Should include automation and management tools for managing asset portfolios [*Action: The business units were all using different domain name registrars. The council decided it made sense to consolidate the management of domain names to a single vendor. By*

doing this the business was presented with a central online domain management portal and realized the value of bulk rate domain name pricing.]

5. Business units should develop a metric to articulate the risk profile of an asset or group of assets relative to other assets being managed [*Action: The council decided to leverage an external brand audit to determine their current security profile. This audit was reviewed. A target rating was agreed to and remediation work was performed. Subsequent audits show signs of improvement and or on plan.*]
6. Assets must be secured based on standard/published criteria

Detect

1. Monitoring of all High-value assets must be performed [*Action: Third party monitoring services were secured for all High-value assets.*]
2. Monitoring of Medium-value and Low-value assets must be considered and should be implemented based on a business risk analysis. [*Action: Council sessions were scheduled to discuss securing monitoring services for Medium-value and Low-value assets. It was decided to use a combination of third-party monitoring services, existing domain registrar services and open-source tools to provide a tiered monitoring capability.*]
3. Asset abuse alerts should be tracked centrally and communicated to owners and custodians based on business rules. [*Action: Alerting business logic was defined by the council and implemented across monitoring services.*]
4. There must be a way for associates, customers, partners and employees to report possible asset compromises or exposures. [*Action: Internal and external websites were created to report abuse.*]

Respond

1. Business units must have a documented response procedure. It should be automated and follow a standard process. [*Action: The council endorsed a basic incident response workflow based on assessing risk, asset value and the event itself. Legal must evaluate the event to answer the traditional question "Is it actionable?" Internal risk analysts rate the threat*

based on the source and type of attack. In cases where the workflow does not accommodate an appropriate response, the operational arm of the council can invoke an emergency meeting and/or escalate.]

2. The response procedure must accommodate a feedback mechanism that updates the authoritative asset database or list with status information. [*Action: Additional fields were added to HACME's Corporate Identity Asset Database to accommodate detailed status information for any asset that is being actively attacked or compromised.*]
3. The response strategy must consider traditional legal remedy as well as immediate technical responses.

In addition, an overall awareness and education campaign should be launched to explain the program to employees, customers and partners. [*Action: The council promoted its creation of the Corporate Identity Asset Protection Program websites as part of a comprehensive education and awareness campaign.*]

8.Summary

As organizations move from the "bricks and mortar" way of doing business to the modern market place of bit and bytes, new intangible corporate assets are being created. These assets must be protected. Traditional protections are not appropriate or effective. Therefore, new techniques, technologies and protections are warranted.

It is unlikely that law enforcement, technology or identity asset stakeholders will be able to deal with this growing epidemic alone. It is equally unlikely that criminals will voluntarily stop taking advantage of the current security deficiencies. Therefore, it is imperative that organizations take proactive steps to identify and protect Corporate Identity Assets before an attack.

9.Appendix A: References

National Cyber Security Alliance, (2005). AOL/NCSA online safety study. Retrieved Jan. 22, 2006, from http://www.staysafeonline.info/pdf/safety_study_2005.pdf.

Anti-Phishing Working Group, (2005). Phishing activity trends report. Retrieved Jan. 22, 2006, from http://www.antiphishing.org/reports/apwg_report_Nov2005_FINAL.pdf.

US Department of Justice, (2005). Operation cyber sweep. Retrieved Jan. 23, 2006, from http://www.fbi.gov/cyber/cysweep/cysweep1.htm.

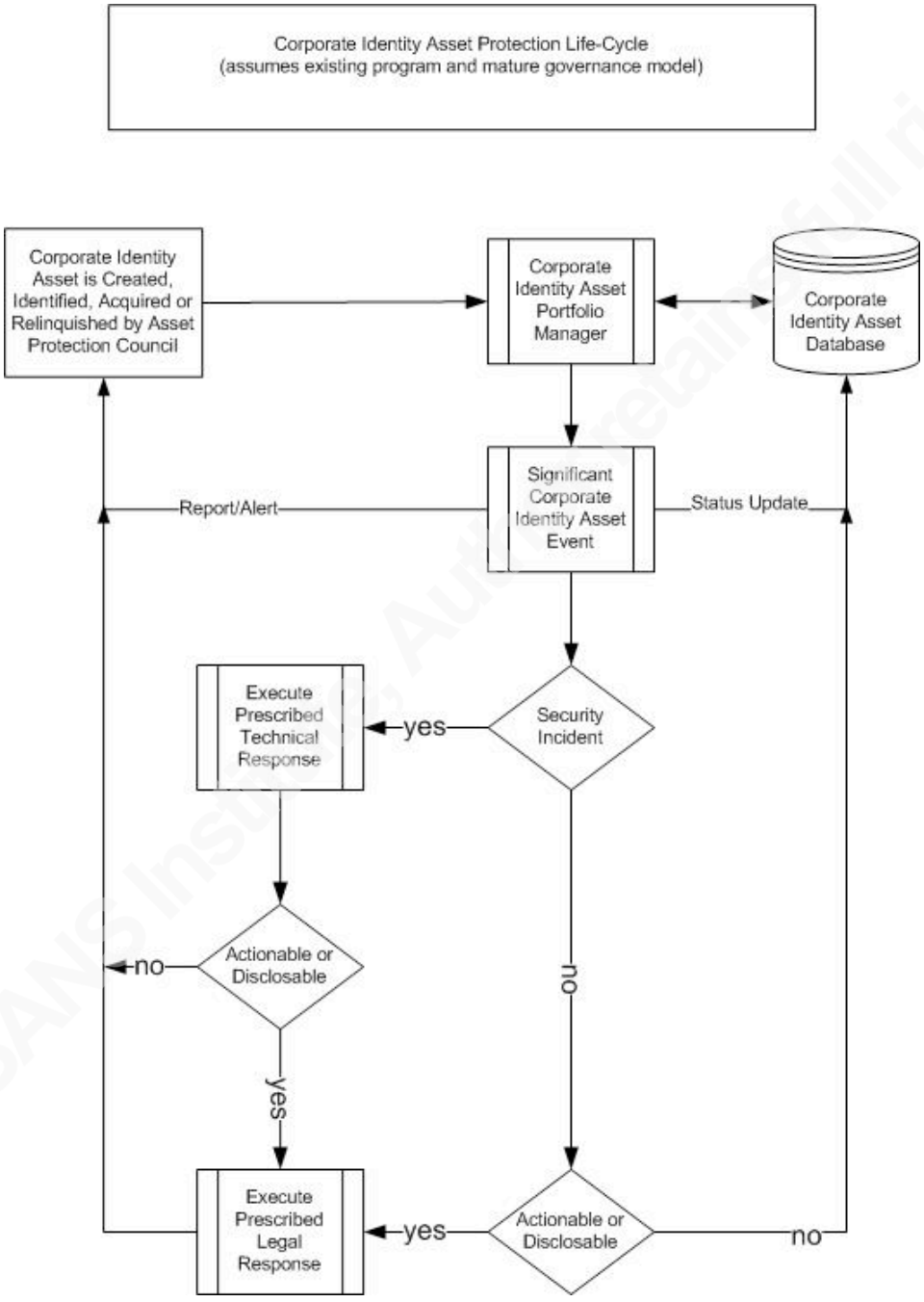
TrademarkBots.com, Inc., (2005). Online brand rating. Retrieved Jan. 23, 2006, from Corporate Governance Web site: http://onlinebrandrating.net/governance.pdf.

SANS, (2002). The SANS security policy project. Retrieved Jan. 23, 2006, from http://www.sans.org/resources/policies/.

10. Appendix B: Vendors and Solution Providers

Actividentity	Strong Authentication	Protect
Bluecoat	Gateways and Network Controls	Protect and Detect
Mark Monitor	Monitoring and Watch Services	Protect, Detect, Respond and Manage
McAfee	End-Point Security	Protect and Detect
Microsoft	End-Point Security	Protect and Detect
Netcraft	End-Point Security	Protect and Detect
RSA	Strong Authentication	Protect
Trademarkbots	Monitoring and Watch Services	Detect and Manage
Vasco	Strong Authentication	Protect
Verisign	Registration	Protect, Detect, respond and Manage
Websense	Gateways and Network Controls	Protect and Detect

11. Appendix C: Corporate Identity Asset Protection Life-Cycle



12. Appendix D: HACME Corporate Identity Asset Database

Asset ID	Description	Category	Value	Status
21001	hacme.com	TLD	HIGH	SECURED
21002	hacme.org	TLD	HIGH	SECURED
21003	hacme.net	TLD	HIGH	SECURED
21004	hacme.biz	TLD	HIGH	SECURED
21005	hacme.tv	TLD	HIGH	SECURED
21006	hacme.info	TLD	HIGH	SECURED
21007	hacme.biz	TLD	HIGH	SECURED
21008	hacme.cc	TLD	HIGH	SECURED
21009	hacme.us	TLD	HIGH	SECURED
21010	hacme.de	TLD	MEDIUM	DISPUTE
21011	1-800-10-HACME	Phone #	LOW	SECURED
21012	HACME™	trademark	HIGH	SECURED
21013	HACME X.509	certificate	HIGH	SECURED
21014	order@hacme.com	email	MEDIUM	MONITORED
21015	hacme Skype™	P2P/VOIP	MEDIUM	SECURED