ISSUE 3Q2013
Published: July 2013
Quarterly News Review
www.savanture.com/newsletter

Contributors in this Issue.

Dennis Devlin, CISO, CPO, and SVP Privacy Practice for SAVANTURE

Rick Rumbarger, Industry Expert and advisor to SAVANTURE

Doug Howard, CEO, SAVANTURE

THE SECURITY SAVANT
relevant news for business
Americas

Exploring High Risk IT Security Threats

SAVANTURE's Efforts

In ***The Security Savant*** we focus on identifying the high risk areas within IT Security and the role of Chief Information Security Officer. We expose you to information we track. We have fulltime researchers focused on security business trends, evolving risk, and threats. We combine this with our security team's experience and best practices we are establishing in the SAVANTURE CISO Practice which are most relevant to you.

Security focuses on ensuring confidentiality, integrity and availability. An example of recent impacts on availability was through Distributed Denial of Service (DDOS) attacks that impact many businesses, but have often targeted gaming, retail, banks and financial services websites.

Google and Arbor recently collaborated on consolidating some carrier data that shows, in non-real-time, origination of high volume DDOS attacks. It's very pretty and certainly has the wow factor when it comes to graphical illustration of an attack, but it provides only country level graphics (no physical address level, or even city level details. The forensics value is questionable, but at least it's a good step in having carriers share some data. Some interesting links:

www.Digitalattackmap.com

http://atlas.arbor.net/cc/US#sources

We Need You

This newsletter is for you, so we need your feedback. We also welcome countering opinions and contributions. We need to understand if we are

Top 5 threats we are tracking:

1. The Futility of Passwords
   a. Like using one skeleton key to open every lock
   b. Social engineering, phishing, social network overshare, etc.
   c. Need more multi-factor authentication for critical applications
2. Advanced Persistent Threats
   a. Lack of network visibility into outbound traffic
   b. Lack of alerts for connections with known bad actors
   c. Need for better SIEM and event correlation
3. Ignorance of Privacy
   a. Organizations don't know how to respect it
   b. Individuals don't know how to expect it
   c. Need awareness and enforcement of privacy regulations
4. Lack of Information Management
   a. Most digital information is not life cycle managed by the enterprise
   b. When compromises occur, "you can't lose what you don't have"
   c. Need life cycle management to destroy information that is no longer needed
5. Inadequate Identity and Access Management
   a. For any asset an enterprise should know all of the identities that can access it
   b. For any identity an enterprise should know all of the assets that it can access
   c. Need timely, accurate and consistent enforcement of law of least privileges

Over time we will report on each of these high risk threat areas. Many resources are available on our website to allow you quick access to real-time updates.

Getting Help with Security

We will limit the advertising in the newsletter to this section. We won't end each article with "call us now" or even "We are Savanture. We can help". Rather, we will update you on our offerings in this small little, tiny, non-descript, almost unnoticeable section. But if you read it … THANKS!

SAVANTURE offers a suite of security services to help with IT Security and Compliance. These include SIEM, LMS, VMS, 2FA and of course Genesis5. We also offer consultancy services including CISO and Chief Privacy Officer services.

War of the World-Wide Internet

Every conflict tagged as a "war" historically has been of the physical world. So why is the conflict over the internet with nation-states attacking each other electronically not a war? Many arguments can be made that few lives have been lost, no mass destruction has resulted, and so forth. Yet, we believe these catastrophic events are coming. Call it World War C (Cyber), World War I (Internet) or any other creation … the cyberwar is coming. Planes, trains, and ever increasingly automobiles, utilities, financial systems, and even our homes are all connected and subject to external influences via the internet. Few in the industry would argue that within 2 years, life loss and physical damage will be caused due to a cyber attack. – Doug Howard

this issue

Advanced Persistent Threat (APT). A Primer. A Refresher.

Advanced Persistent Threat (**APT**) refers to a group, such as a government or an organization, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information but applies equally to other threats such as that of traditional espionage or attack. APTs typically are achieved over a long period of time where patience leads to obfuscation of low impact activities.

The term, like many within IT, has become as much of a marketing term as a clear technical definition. Many IT Security vendors have simply added their ability to protect against APT to their list of capabilities with no improvements in their products; sometimes accurately, while most products are relatively ineffective. Most agree that, an individual hacker, is not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target. Most individuals are motivated by monetary gain, not in disruption or intelligence gathering.

There are several ways APT may penetrate a customer's network to deploy an automated propagating malware through a wide variety of vectors, even in the presence of properly designed and maintained defense-in-depth strategies:

- **Internet-based malware infection** such as drive-by download, phishing, and file sharing.
- **Physical malware infection through external device connections** such as a USB.
- **External exploitation** such as vishing, rogue access points, or remote access through a trusted third-party

APT attacks are inherently difficult to detect and protect against. Most solutions cover some very, very small aspect of APT detection and protection. Monitoring at the registry level is difficult which is often the most effective level of detection, but as you know software changes, updates, and even particular activities create registry changes. To date we have seen no complete solution that truly protects against APT. There are professional services companies that can come in and identify APT activities that have already occurred and what information the perpetrator had access to. Many companies can help you reduce risk to APT, and we will cover these in more detail in the future as we continue to report on this topic.

Guiding Principles for protecting critical information

From the beginning . Basics.

The tactical steps that will serve you well are:

1st, prioritize you information assets by determining their impact on revenue, reputation and regulation. Many information assets impact all three areas and you can move it to the top of the list.

2nd, identify the systems and paths which the data will transit. Outside the organization data it is possible that data will be captured from a network path, but typically encryption (via VPN or data encryption) is your only real option for control. Most risk resides on the servers and viewer systems that your data will come to rest on (temporarily or for an extended period of time. Using your prioritization list, you can then classify the prioritization of systems as well.

3rd, identify how to best protect the most important data that poses the highest impact to your organization. Often this is not just applying security, but changing processes, rearchitecting data storage, or reworking information handling.

Don't buy more technology until you've leveraged the capabilities of what you have.

THE DOMAIN NAME SERVICE ACHILLES HEEL

Why you're at risk and what to do about it.

Rick Rumbarger, Industry Expert

Most people, even seasoned IT professionals, don't give the Domain Name System (DNS) the attention it deserves. As TCP/IP have become the dominant networking protocols, so has the use of DNS. Most organizations use DNS to not only direct customers to their website, but to conduct almost every aspect of their day-to-day business operations. DNS is the hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network that converts complicated IPv4 & IPv6 device addresses into easy to understand names (e.g. mail.domain.com) that humans can use and understand. On private networks it is used to address even the most mundane things like printers and servers. On the Internet we use it to address websites (A records), VoIP phone calls (SRV records), email servers (MX records) and a myriad of other critical connections. Advanced organizations even use DNS to load balance, failover and geographically redirect connections. DNS has become so pervasive it is hard to identify a modern TCP/IP connection that does not use DNS in some way.

"The World's largest and most used directory. DNS is the internet's critical linchpin and demands the highest degree of availability and integrity. "

Due to the reliability built into the fundamental RFC based design of DNS most IT professionals don't spend much time worrying about it, but this can be a huge mistake! If your DNS is maliciously attacked altering the addresses it gives out or taken offline your business is not only stopped in its tracks, but your brand can be damaged for years to code. End users seldom take the time to understand the security issues your business has had, this public facing issue can be. They simply go to your competitor. Whether conducted for financial motives, political gain, or the notoriety of the attacker, the damage from a DNS attack can be devastating for the target business.

To understand the risk to which your business is exposed, you must understand the security threats that exist. The most common security issues for DNS are:

- **Unauthorized Authoritative DNS Record Changes** – Changes to authoritative DNS records which point end users to computer systems outside of your control can have the most damage to a business's brand. This type of attack is typically done to either send an end user to a site, which either provides a negative marketing message the attacker wants to promote or a location mirroring your site where account credentials can be harvested, many times without the end user even being aware it has happened.

- **Denial of Service Attacks** – Denial of Service (DoS) or Distributed Denial of Service Attacks (DDoS) are simply done to make your DNS service unavailable and thus create the impression your business is offline or closed down (website, portals, VPNs, FTP, VoIP, email, etc.). This type of attack is one of the easiest to perform and can be one of the hardest to defend against. One of the seldom known impacts to a business that suffers a DNS outage from a DDoS attack is the negative effect it has on your search engine rankings.

- **Recursive DNS Spoofing/Cache Poisoning** – Outside of a business's control, the Recursive DNS server an end user utilizes is typically set at a network administrator's level or an individual device level. Recursive DNS servers communicate Authoritative DNS records a business sets to an end user's device. Unfortunately many Recursive DNS servers are not well maintained or protected and can be easily compromised to give out false responses. This has the same downstream effect of an Unauthorized Authoritative DNS record change.

Obviously there are many more, but this is a good start in understanding the broad risk to DNS and you.

Test your DNS

There are a lot of services to help you secure your DNS, however one of the best and most comprehensive ways to check the health of your DNS is with a free tool from Neustar.

Previously I had the honor of working at Neustar and leading up product for the UltraDNS service and we brought this tool to the market to help everyone understand how their DNS was operating at a specific point in time. In addition to the web version, we also created mobile versions as well. Happy to see its still relevant. Rick.

Security best practices for DNS:

- **Registrar Lock Your Domain Names** – One of the simplest protections you can do is lock all of your domain names at your registrar.

- **Outsource Your DNS Services** – In today's world it is generally accepted that it is unrealistic to maintain your own DNS name servers in a way that both protects them from attacks and maintains global performance and naive to use the free DNS services of a domain registrar. Cloud based managed service providers are your best bet for both Authoritative & Recursive DNS. Neustar (UltraDNS), DynDNS, VeriSign, Amazon (Route 53), and Community DNS (European focused) are top IP Anycasted Authoritative DNS providers to consider. OpenDNS, Neustar (UltraDNS), DynDNS & Google are top Recursive DNS providers to consider.

- **Utilize Strong Access Controls** – As with any critical IT infrastructure only allow users access to DNS administration for what they need to manage, lock down access to these critical accounts to known IP ranges, utilize strong password controls and whenever possible use two factor authentication.

- **Activate DNSSEC On Your Domain Names** - DNSSEC counters cache poisoning attacks by verifying the authenticity of responses received from name servers. It effectively prevents responses from being tampered with, because in practice, signatures are almost impossible to forge without access to private keys. If your DNS provider is not DNSSEC capable… make a switch.

- **Continuously Monitor Your Critical Services & DNS Records** – Utilize an advanced SIEM like the one available from Savanture to monitor all of your critical services and monitor your DNS records for changes from outside your network. UltraTools.com provides a free DNS monitoring service that many top organizations use.

- **Promote The Use of Protected Recursive DNS Servers** – If you are not already using one of the top Recursive DNS providers listed above for your business's network, make the switch now. Many times there is no cost to this, only a configuration change. After you select a provider, promote it to your end users, inside & outside of your business.

- **Protect Your DNS Service Against DDoS Attacks** – If you aren't using one of the top Authoritative DNS providers listed above that also provides DDoS protection for your DNS service, add it. For your other public facing services that require DDoS protection lower your DNS Time to Live (TTLs) settings to 300 (5min) so you can redirect traffic quickly if you come under attack and need protection.

BREACHES

In 2Q2013 there were over 140 breaches representing more than 30M exposed records

LivingSocial

29 million records exposed due to a cybersecurity compromise.

Administrative Office of the Courts
Olympia, Washington

1,000,000 court records with PII information compromised when the courts servers were hacked.

Indiana University Health Arnett

10,300 records compromised when an employee's laptop was stolen outside of work.

City of Akron (OH)

47,452 records compromised in a network breach by a hacker (or foreign organization)

Lutheran Social Services of South Central Pennsylvania

7,300 records compromised due to malware on internal servers.

U.S. Army Corps of Engineers' National Inventory of Dams

Server compromise due to cyber attack which resulted in hackers obtaining 8,100 major dams. Dam vulnerability was taken that could be used in terrorist attacks.

Pentagon

500,000 emails were exposed from a Pentagon server. Data and compromise details were not disclosed

comScore

Two comScore panelists filed a lawsuit after downloading comScore software. Allegedly, comScore collected and sold consumers' Social Security numbers, credit card numbers, financial information, retail transactions, and other personal information. 2011 case proceeding after judge denied dismissing.

Who does the CISO typically report to?

The size and degree of regulatory controls of the organization clearly defines the stratification level of titles and responsibilities within any organization. Looking at a sampling of CISOs within the Fortune 1000, the majority of CISOs report to the Chief Information Officer (CIO) while a few, especially in regulated industries, recognize the necessity for the CISO to report outside of the CIO area; such as to the CEO or CFO. If no CPO or CCO exist, most often the responsibility for Privacy falls to the CISO to manage.

Three R's of Privacy. No, four!

By no coincidence, the three R's of Privacy are the same three R's of Security that we use. Privacy impacts an organization by putting at risk its Revenues, Reputation, and ability to meet Regulatory Requirements. Add to the costs of Ramification when you must remediate the situation when you provide notice to those impacted (or everyone if you can differentiate) and then fees for services to protect your clients or worse, the fees to repair the situation should the compromised date be used.

The Role of the Chief Information Security Officer Defined

The evolving position of the CISO

Dennis Devlin, SAVANTURE

A generally accepted definition for the role of Chief Information Security Officer (CISO) is a senior level executive within a business or organization who is responsible for managing the risks and business impacts of IT security. The CISO is responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining security across the organization including people, processes and technology to reduce information and information technology (IT) risks. They respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information technology security related regulatory compliance.

The Chief Information Security Officer (CISO) is a challenging and highly demanding role in most organizations. It's a function that carries significant enterprise-wide responsibilities, yet the function is often underfunded and does not have the executive level influence that it should. If IT weren't complex enough, at least the threats to availability caused by change are relatively manageable compared to threats to confidentiality and integrity caused by criminal attackers and well intentioned staff members making bad decisions about how to protect information.

"Promoting the value and importance of Security to all users is critical"

Like many corporate executive roles, it carries differing responsibilities depending on the industry, size of company, and reporting structure. And like many executive roles, the smaller the organization the less likely that the formal roll even exists at all.

The role of the CISO has evolved from being primarily a technologist who established a cyber-demarcation between the enterprise and the outside world to a member of the executive leadership team who both understands the business and the potential risks to revenues, reputation and compliance with applicable regulations caused by inadequate information security. There is not one single "right" answer when it comes to risk management. Business is about taking risk. An effective CISO helps the board of directors and senior executive leadership to measure the risk, decide on their risk tolerance, and then to manage that risk through policies that align people, process and technology appropriately. Good policy is a statement of informed executive management intent. The role of the CISO is help leadership to manage risk to the enterprise in a way that is consistent with the risk tolerance of the organization.

Information security is the responsibility of every user with system access. The role of the CISO is to help them make the more secure choice every time.

The Chief Information Security Officer is responsible for enterprise information security, including:

- Educating the board of directors, senior executives, IT leadership, Human Resources, Office of General Counsel, Corporate Communications, Investor Relations, Marketing, etc. on the security status of the organization and high risk threats.
- Assessing security readiness by determining the maturity of current security plan and controls.
- Developing and maintaining security policies, standards, best practices, communications, etc.
- 7x24 monitoring for evidence of anomalies that could indicate a breach or increase in the risk to the organization's IT security systems and applications (MSSP, SIEM, VMS, LMS, 2FA, etc.)
- 7x24 management of security staff and Security Operations Centre (SOC)
- Business Continuity and Disaster Recovery (BCDR) planning to enable high availability
- Identity management, authorization management and access control
- Perimeter, network, server, application and workstation vulnerability management
- Business process risk management including supply chain, transaction systems, etc.
- Computer Emergency Response (CERT) and Computer Security Incident Response (CSIRT)
- Establishing and promoting a culture of compliance when it comes to security that will enable the organization to potentially leverage information security as a competitive differentiator.
- Digital information discovery (eDiscovery), digital forensics, digital investigations

This Month's Security Q&A with newsletter subscribers

Q: What security standard is the best to use as the foundation for my Security Plan?

Security standards are just that – a benchmark of industry standard best practices used to measure the maturity and completeness of an organization's security practices.

There are many different organizations who have published security standards, including:

- British Standards Institute (BSI 7799)
- International Organization for Standardization (ISO 17799)
- National Institute for Standards and Technology (NIST 800 Series)
- PCI-DSS (for credit card industry)

The "best" standard for your security plan is based on:

- which standard your industry uses.
- which standard your customers use.
- which standard meets your regulations.

For small organizations t with no regulatory requirements a good starting point might be:

- SANS 20 Critical Security Controls

EYE ON IT Highlighted Regulatory Changes

Americas

2013 HIPAA regulator changes. due to willful neglect, instead of first attempting to resolve the matter through informal means. Penalties for HIPAA violations are significant. Penalties for violations caused by willful neglect, which are corrected, range from $10,000 to $50,000 per violation. The minimum penalty for an uncorrected HIPAA violation caused by willful neglect is $50,000 per violation. The penalties are capped at $1.5 million for all violations of an identical requirement in a calendar year. HIPAA.

Changes to Children's Online Privacy Protection Act (COPPA)

Updates are to continue to strengthen the laws to protect children that go in effect in July 1, 2013.

99 Countries with Privacy Laws. Read more.