Cybersecurity: Emerging (and Re-Emerging) Issues

Steven Roosa, Co-Chair, Data Privacy & Security Team

April 23, 2015
Introduction
Introduction

» There is no such thing as perfect security

» The world is increasingly reliant on the Internet and connected devices

» The “bad guys” are smart, patient, and able to quickly adapt to defensive measures
  - A recent survey showed that cyber-attackers went undetected for an average of 243 days
  - Adversaries are evolving faster than detection and response capabilities

» No industry is off limits

» It only takes one “click” or one failed security protection

» This new threat is creating unique legal challenges, not readily addressed by traditional frameworks
Federal Legislation Update & Forecast
Congress is intently focused on cybersecurity legislation, and information sharing bills are moving quickly on the Hill

Last night, the House of Representatives passed the Protecting Cyber Networks Act (H.R. 1560)

This morning, the House also passed the National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731)

The Cybersecurity Information Sharing Act of 2015 (S. 754) also passed out of Intel Committee and is expected to be on the Senate floor after Memorial Day, if not sooner
Protecting Cyber Networks Act (H.R. 1560)

(Subject to Change)

» Designed to promote public-private sharing of cyber threat indicators or imminent/ongoing cybersecurity threats

» Enables private companies to voluntarily share cyber threat indicators with each other and with Federal Government entities other than NSA or DoD

» Contains liability protections for private entities acting in good faith in accordance with the Act

» Allows for private right of action against Federal Government for intentional/willful violations of privacy and civil liberties guidelines
National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731)

(Subject to Change)

» Designed to promote public-private sharing of cyber threat indicators, defensive measures, and cybersecurity risks
» Enables private companies to voluntarily share cyber threat indicators with each other and with Federal Government entities
» Establishes the Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) as the central vector for the information sharing process
» Contains liability protections for private companies acting in accordance with the Act
» Allows for private right of action against Federal Government for intentional/willful misuse of shared information
Will this be the year Congress acts?

» Congress has unsuccessfully considered cybersecurity legislation for years, but many think this year may be different

» The recent high-profile cyber attacks, especially those involving state actors, has put pressure on Congress to act in this space

» President Obama has urged Congress to act and issued an Executive Order in February 2015, promoting a public-private information sharing relationship

» This week, the White House also publicly backed the two House cyber bills

» Passing out of the House is the first major step for the bill to become law

» The bills will now be combined and go to the Senate for approval and, if passed, to the President to be signed into law
Federal Guidance on Due Diligence for Third Parties
Subject: Third-Party Relationships  
Date: October 30, 2013

To: Chief Executive Officers and Chief Risk Officers of All National Banks and Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Description: Risk Management Guidance

Summary

This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise.¹

The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank’s use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.²

New York State
Press Release

December 10, 2014
Contact: Matt Anderson, 212-709-1691

NYDFS I S SUES EXAMINATION GUIDANCE TO BANKS OUTLINING NEW TARGETED CYBER SECURITY PREPAREDNESS ASSESSMENTS

DFS-Regulated Banks to be Examined Based on Cyber Security Protocols, Governance, Third-party Vendor IT Security, Other Issues

Targeted Cyber Security Assessments Will Be Integrated As Ongoing, Regular Part of DFS Exam Process

Benjamin M. Lawsky, Superintendent of Financial Services, today issued an industry guidance letter to all New York State Department of Financial Services (DFS)-regulated banks outlining the specific issues and factors on which those institutions will be examined as part of new targeted, DFS cyber security preparedness assessments. These banks will be examined on their protocols for the detection of cyber breaches and penetration testing; corporate governance related to cyber security; their defenses against breaches, including multi-factor authentication; the security of their third-party vendors, and a number of other issues.

The new cyber security assessments will become regular, ongoing parts of all DFS bank examinations moving forward.
TO: All NYS-Chartered or Licensed Banking Institutions

FROM: Benjamin M. Lawsky

DATE: December 10, 2014

RE: New Cyber Security Examination Process

In an effort to promote greater cyber security across the financial services industry, the New York State Department of Financial Services (the “Department”) plans to expand its information technology (“IT”) examination procedures to focus more attention on cyber security. The Department encourages all institutions to view cyber security as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology. To that end, the Department has incorporated into the examination new questions and topics, which will be embodied in pre-examination “First Day Letters.”

In particular, IT/cyber security examinations will now include, but not be limited to, the following topics:
- Corporate governance, including organization and reporting structure for cyber security related issues;
- Management of cyber security issues, including the interaction between information security and core business functions, written information security policies and procedures, and the periodic reevaluation of such policies and procedures in light of changing risks;
- Resources devoted to information security and overall risk management;
- The risks posed by shared infrastructure;
- Protections against intrusion including multi-factor or adaptive authentication and server and database configurations;
- Information security testing and monitoring, including penetration testing;
- Incident detection and response processes, including monitoring;
- Training of information security professionals as well as all other personnel;
- Management of third-party service providers;
- Integration of information security into business continuity and disaster recovery policies and procedures; and
- Cyber security insurance coverage and other third-party protections.
In addition to the revised First Day Letter, the Department is updating its examination process, including the procedure for assessing and scheduling IT/cyber security examinations. Going forward, the Department will schedule IT/cyber security examinations following the comprehensive risk assessment of each institution. To aid in that assessment, the Department will be seeking, by separate request, responses to the following questions:
1. Provide the CV and job description of the current Chief Information Security Officer or the individual otherwise responsible for information security, describe that individual’s information security training and experience, and identify all reporting lines for that individual, including all committees and managers. In addition, provide an organization chart for your institution’s IT and information security functions.

2. Describe the extent to which your institution maintains information security policies and procedures designed to address the information security goals of confidentiality, integrity, and availability. Provide copies of all such information security policies.

3. Describe how data classification is integrated into information risk management policies and procedures.

4. Describe your institution’s vulnerability management program as applicable to servers, endpoints, mobile devices, network devices, systems, and applications.

5. Describe the organization’s patch management program including how updates, patches, and fixes are obtained and disseminated, whether processes are manual or automated, and how often they occur.

6. Describe identity and access management systems employed by the organization for both internal and external users, including all administrative, logical, and physical controls and whether such controls are preventive, detective, or corrective in nature.
7. Identify and describe the current use of multi-factor authentication for any systems or applications.

8. Describe your institution’s due diligence process regarding information security practices that is used in vetting, selecting, and monitoring third-party service providers.

9. Describe all application development standards utilized by the organization, including the use of a secure software development life cycle, and the extent to which security and privacy requirements are assessed and incorporated into the initial phases of the application development process.

10. Provide a copy of, to the extent it exists in writing, or otherwise describe, the organization’s incident response program, including how incidents are reported, escalated, and remediated.

11. Describe the extent to which information security is incorporated into the organization’s BCP/DR plan, how and how often the BCP/DR is tested, and the results of the most recent test.

12. Describe any significant changes to the institution’s IT portfolio over the last 24 months resulting from mergers, acquisitions, or the addition of new business lines.
The New York State Department of Financial Services issued a Report this month regarding cybersecurity practices for third-party vendors in the financial services sector.

The Report identified continuing challenges with the industry’s reliance on third-party vendors for critical banking functions.

The Report was based on survey responses from approximately 40 financial organizations and revealed some key vulnerabilities:

- Less than half of surveyed organizations require on-site assessments of third-party vendors.
- 21% do not require vendors to represent that they have established minimum information security requirements.
- 64% of organizations do not require information security requirements to be extended to subcontractors.
- 21% of organizations do not require the right to audit their vendors.
- 30% do not require vendors to notify them in the event of an information security breach or other cybersecurity breach.
Third-Party Vendors – Selection Process

» Vendor candidates’ information security practices should be a specific component of the vendor selection process, especially of those vendors with access to sensitive information.

» Companies may consider conducting an on-site assessment of the vendor prior to engagement.

» Vendor selection criteria should be reduced to writing in internal policies so that information security risk assessment procedures are memorialized and available to those involved in the selection process.
Contracts that enable effective vendor risk management typically include:

- Minimum requirements for security controls, log retention, incident response cooperation (consistent with your company’s policies/requirements)
- Explicit treatment of regulatory requirements and the vendor’s responsibilities for compliance
- Audit rights that enable you to conduct regular (annual) on-site audits of the vendor’s policies, processes, and controls
- Adjudication process for resolving concerns that are identified as a result of those audits
- Requirements for participation in cyber risk management activities including training, exercises, information sharing, and breach notification
Third-Party Vendors – When to Engage

» The time to establish relationships and/or establish information security protocols with third-party vendors is not mid- or post-breach.

» These procedures should be clearly established and agreed upon before an incident occurs.

» Similarly, companies should establish relationships with vendors relevant to the incident response process, such as credit monitoring companies, forensic firms, law firms, public relations firms, etc., in advance of a major incident.

- During a cyber incident, the company will be consumed with mitigating the threat and determining its scope.
- You do not want to be negotiating contract provisions with vendors while trying to manage a live cyber event.
Observations About the Threat Landscape
The Certificate Authority Trust Model Which Secures the Entire Web
Device/Browser/OS

ROOT CA

Website/App Server

SSL Cert: “I am ABC Bank”

Who are you?

SSL Cert

Root Cert

Root CA

Website/App Server

SSL Cert

Who are you?

Root Cert

$$$

Relying Party / End User

Holland & Knight
Final Report on DigiNotar Hack Shows Total Compromise of CA Servers

by Dennis Fisher

The attacker who penetrated the Dutch CA DigiNotar last year had complete control of all eight of the company's certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified. The final report from a security company commissioned to investigate the DigiNotar attack shows that the compromise of the now-bankrupt certificate authority was much deeper than previously thought.

In August 2011 indications began to emerge of a major compromise at a certificate authority in the Netherlands, previously unknown to most of the Internet's citizens, and the details quickly revealed that the attack would have serious ramifications. The first public acknowledgement of the attack was the discovery of a large-scale man-in-the-middle attack against Gmail users in Iran. Researchers investigating that attack discovered that the operation was using a valid wildcard certificate, issued by DigiNotar, for *.google.com, giving the attacker the ability to impersonate Google to any browser that trusted the certificate.
DigiNotar is not Google’s CA.

But the CA Trust Model allows ANY Root CA to issue an unauthorized, but technically valid cert for ANY domain.
Man-in-the-Middle (MITM) Enabled by Unauthorized Certs Issued by DigiNotar
The Attack Surface, in Light of DigiNotar, Includes the Trustworthiness and Security of Every CA.

So, the fewer I trust by default, the better.
Thank Goodness There Aren’t Many
iOS

JPKI
Entrust
A-Trust
Japanese Gov.
AOL
AdTrust AB
AffirmTurst
America Online, Inc.
LGPKI
Baltimore CyberTrust
Buypass
CNNIC
Comodo
Dhimyotis
Chunghwa Telecom
Digital Signature Trust Co.
Deutsche Telekom AG
DigiCert Inc.
U.S. Gov.

Echoworx Corp.
Entertrust, Inc.
Equifax
Go Daddy Group, Inc.
GTE Corp., CyberTrust
GeoTrust Inc.
Hongkong Post
IZENPE S.A.
Japan Certification Services, Inc.
KMD
NetLock Kft.
Network Solutions
Unizeto Technologies S.A.

Camerfirma SA
RSA Security Inc.
VISA
SECOM Trust.net
Starfield Technologies, Inc.
Sonera

SwissSign AG
TDC OCES CA
Thawte Consulting
Trustis Limited
SecureTrust Corporation
UniTrust

Unizeto
VAS Latvijas Pasts
WISeKey
Wells Fargo Wells Secure
Xramp Security Services Inc.
CertiNomis

Sociedad Cameral de Certificaci
Belgium Root CA
Certplus
Cisco Systems
FNMT
KISA
StartCom Ltd.
Swisscom
Introducing CNNIC:

China Internet Network Information Center
From Wikipedia, the free encyclopedia
Jump to: navigation, search

The China Internet Network Information Center (simplified Chinese: 中国互联网络信息中心; traditional Chinese: 中國互聯網絡信息中心; pinyin: Zhōngguó Hùlián Wǎngluò Xìnxī Zhōngxīn), or CNNIC, was founded as a non-profit organization on June 3, 1997.

CNNIC is the administrative agency responsible for Internet affairs under the Ministry of Information Industry of the People’s Republic of China. It is based in the Zhongguancun high tech district of Beijing.
Welcome > Blog Home > Cryptography > Google, Mozilla Drop Trust in Chinese Certificate Authority CNNIC
OWASP Top 10
# OWASP Top 10

## OWASP Top 10 – 2013 (New)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>A2</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A3</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A4</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>A5</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>A6</td>
<td>Sensitive Data Exposure</td>
</tr>
<tr>
<td>A7</td>
<td>Missing Function Level Access Control</td>
</tr>
<tr>
<td>A8</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A9</td>
<td>Using Known Vulnerable Components</td>
</tr>
<tr>
<td>A10</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>
The Exploit and Vulnerability Market
Observations and Conclusions
Steven B. Roosa is a partner in Holland & Knight's New York office and co-chair of the Data Privacy and Security Team. He is also the director of Holland & Knight’s internal testing Lab and a fellow emeritus at the Center for Information Technology Policy (CITP) at Princeton University. His practice focuses on advising companies on a wide spectrum of technology and legal issues pertaining to privacy and data security. Representative issues include: mobile app privacy compliance; leveraging anonymity solutions to help clients safely unlock the value of large data sets; Internet tracking; web security; geo-fencing; data breach and incident response; Children's Online Privacy Protection Act (COPPA); Computer Fraud and Abuse Act (CFAA); FTC compliance; privacy considerations of modified network protocols; California best practices for websites and mobile apps; compliance with wiretap statutes and the Electronic Communications Privacy Act (ECPA); public-key infrastructure (PKI); certification authority matters pertaining to online trust; and web-based reputation and defamation issues. Mr. Roosa is a regular contributor to Holland & Knight's Privacy Blog.