Online Trust Alliance

"Security By Design"

Data & Information Security Recommended Best Practices

Published: April 20, 2011   Revised: October 10, 2011
For updates visit https://otalliance.org/securitybydesign.html

This paper is intended for all business segments including members of the interactive messaging ecosystem most recently victimized by breaches and data loss incidents. OTA suggests organizations create a cross-functional team to review these recommendations and develop a prioritized game plan based on their assessment of risks associated with their current data flows and practices.

Few events can damage a company's brand and the trust of its customers more than a data incident, either the loss or misuse of customer data. We've witnessed in recent months cybercriminals targeting the email and interactive messaging ecosystem with increased malice and precision. Every brand and service provider in this ecosystem needs to understand the nature of these attacks, recognize their data is at risk and plan accordingly. Left unchecked, multiple data incidents across an industry and online can trigger a meltdown in consumer trust and damage the viability of online communication and commerce.

The 'Security by Design' framework is a holistic approach to security. It is predicated on the belief that all members of the messaging community have a stake in the preservation of consumer trust. Data stewardship is everyone's responsibility and creating a culture of security is a critical priority as we move into an era of data-driven cross-channel communications and platforms.

OTA believes all businesses must take security and privacy seriously, and not wait for government regulation to force our hand. Effective self-regulation and transparency will enhance the vitality of our industry and advance the interests of all legitimate stakeholders, but its absence will have the opposite and significantly detrimental effect.

This document provides a security framework that every business and technical leader should carefully consider. To assist in the development of a plan, a series of twenty questions are included to stimulate internal review. These security best practices are presented as a starting point for security professionals and operations managers as they seek to assess their data and operational security requirements.[1]

[1] Note: these recommendations do not override other standards that apply to specific industries, such as the financial services, PCI credit data and health care sectors. Those recommendations deemed appropriate should be included in internal operating guidelines and stipulated in RFPs and agreements with third parties.

To be successful, “security by design” needs to be part of the culture of every organization and functional group. Security is no longer an option and businesses need to accept three fundamental truths: 1) the data you collect includes some form of personally identifiable information (PII) or “covered information”; 2) if you collect data you will experience a data loss incident at some point; and, 3) data stewardship is everyone’s responsibility. Businesses that accept these “laws of data collection” and structure themselves accordingly will be better positioned to protect their customers and brands from harm.

In the past five years, over 525 million records containing sensitive personal information have been compromised. These high profile data breaches and cyber security incidents caused by human error or malice confirm that all businesses and government agencies are at risk.

Data breach incidents damage a company’s brand, and increase scrutiny and potential liability. According to the 2010 Cost of Data Breach Report published by the Ponemon Institute, data incidents cost companies $214 per compromised customer record with an average cost-per-incident of $7.2 million. Data loss incidents, often due to security lapses have not gone unnoticed in the United States by the FTC and state regulators. Recently, the Massachusetts Attorney General stated that she would continue to take action against companies that fail to implement basic security measures to protect consumers.

OTA has identified best practices to help businesses address many common causes of data loss. Many of the guidelines may be regarded as security ‘101’, they are often the most overlooked. While there is no silver bullet, the attached recommendations serve as an aid to help develop an appropriate security program for businesses who maintain consumer data or manage a messaging infrastructure. The recommendations should be considered with knowledge that the effort to build a security program will produce positive benefit for all concerned.

The definition of “personal data” or “personally identifiable information” (PII) is continuously evolving as the regulatory landscape has become increasingly complex. Today we no longer compile files consisting of a single data type, such as email address. Instead, through data appending, data mining and other processes we now have data files that include many data fields, including email addresses which sometimes serves as the primary key. Service providers can have little or no visibility into what data elements are being used or created in their systems. In these cases, OTA recommends that both in-house marketers and service providers assume their lists include some PII.

Security by Design Objectives

1. Provide an assessment framework for businesses to review their internal systems, processes and data management practices – for their own systems as well as their service providers.
2. Accelerate the development of a comprehensive security strategy, including security and privacy best practices for the capture, storage, transmission and use of customer, with the goal of enhancing consumer trust and confidence.

Steps to Security by Design

1. Create a cross-functional security team headed by a chief security officer (or equivalent) as a single point of authority with security accountability.
2. Map the data workflows within your organization and vendors to identify points of vulnerability. Examine how you handle data, from collection and storage to transmission, usage and destruction. Define who should have access to the data, how and why.
3. Include security review milestones in the product development process, from concept development, functional specification development, design, testing and launch.
4. Audit your network infrastructure, mapping both internal and external facing sites and all points of connection. Implement processes to monitor your network and data assets to detect unauthorized access or unusual patterns of activity.
5. Develop an incident response plan and team. Include pre-defined action items and communication strategies that can be easily executed should a breach occur.

Top 20 Self-Assessment Questions

To assist in the development and implementation of an effective security strategy plan and incident response plan, organizations are encouraged to audit their level of preparedness by surveying their team and vendors with the following questions.

1. Do you know what sensitive information is maintained, where it is stored and how it is kept secure? Do you have an accounting of all information stored including backups and archived data?
2. Do you know what data elements or attributes are being stored?
3. Who has access to each data set and data elements? Is access limited by account or client responsibility? (Limited vs administrative rights, read only, etc.)
4. How do you provision new user accounts, audit user rights and revoke them on job changes or termination? Do you have a comprehensive password management system?
5. Do you have intrusion detection systems? How often do you review and test them?
6. How do you monitor outbound systems for abnormal or malicious usage?

7. What logs are maintained, how are they secured and used for intrusion detection? Do you have a process and procedure for regular review?
8. Is your definition of personal information current and in line with both applicable industry regulation and customer's expectations?
9. Do you have a trained incident response team in place ready to respond 24/7?
10. Is your executive management aware of security, privacy and regulatory requirements related specifically to your business (including breach notifications requirements in the US, Canada and the EU)?
11. Have you conducted a comprehensive audit of your data flows across the enterprise and vendors including a privacy and security review of all data collection and management activities?
12. Are security disclosures and requirements included in your terms of service and service contract with customers and vendors? Do your contractual requirements account for exceptional risk and liability due to nature of the work or service provided by third party vendors?
13. Are you prepared to communicate to customers, partners, shareholders and the community at large in the event of a data incident?
14. Are employees equipped to notify management of security incidents, including intrusion, breach, data misuse or data loss?
15. Have you coordinated with all departments with respect to an data loss incident? (for example information technology, corporate security, marketing, governance, fraud prevention, compliance, HR and regulatory teams) with respect to breach readiness?
16. Have you developed relationships with law enforcement and forensics services in advance of an incident and understand their data requirements and how to work with them?
17. Do you have a privacy review and audit system in place for all data collection, storage, manipulation or usage activities, including those of third-party service providers and partners? Have you taken necessary or reasonable steps to protect customer confidential data?
18. What processes do you have in place for data minimization, secure archiving and data destruction?
19. Have you considered updating your Terms of Use to provide an ability to examine customer data files and share information with forensics specialists and law enforcement officials and to investigate reports of misuse?
20. Have you developed a mutual understanding with your service providers of the security requirements they must adhere to in managing or processing your data?

Information Security Recommended Practices

The attached list provides recommendations to help fortify your security defenses, detect exploits, and to implement plans to remediate data loss. As the security landscape is ever changing, plans need to be re-assessed on an ongoing basis.

Security Infrastructure	Immediate	Within 90 days
1. Enable multi-layered firewall protection from the public Internet via multiple and distinct firewalls. By default deny on inbound and outbound. As access control lists are validated such connections can be added.	✓	
2. Install a network and host based intrusion detection system with staffing, monitoring and processing of data.		✓
3. Initiate planning to support DNS Security Extensions (DNSSEC). DNSSEC adds security to the DNS and is designed to help address man-in-the-middle attacks and cache poisoning.[2]		✓
4. Maintain comprehensive system and application logs to review traffic patterns and abnormalities (Key logs should be written to a separate server including but not limited to application, DNS and servers).		✓
5. Require employees to use the most current version of browsers. Terminate support for end-of-life browsers with known vulnerabilities. (*For testing purposes the use of end-of-life browsers should be limited to test machines, https://otalliance.org/browser).*	✓	
6. Adopt Email Authentication including both SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to help reduce the incidence of spoofed and forged email. Drive adoption to include sub-domains and top level domains as possible.[3]	✓	
a) Initiate corporate inbound authentication checks, quarantining, blocking or junking unauthenticated email often attributed to spear phishing and malicious payloads.		✓
7. Scan outbound marketing, transactional and other email streams to detect malicious content and links or unauthorized use. Implement the capability to suspend sending and take other correction action including quarantining email as necessary.		✓
8. Encrypt all data files containing PII, customer profiles or email addresses which are transmitted externally or stored. Consider restricting or prohibiting any data to be stored on client systems, portable devices or media including flash and USB. Data which includes PII should be prevented from standard user access.		✓
9. Use Transport Layer Security, such as Secure Socket Layer (SSL) for all data collection forms and web applications. SSL invokes for your web sites and applications, encrypting data in transit between the users browser and your server. Consider always on SSL or HTTPS to provide end-to-end security and minimize risk of wireless snooping.	✓	

[2] https://otalliance.org/resources/dnssec.html

[3] https://otalliance.org/resources/authentication/index.html

10. Upgrade client login sites to Extended Validation Secure Socket Layer Certificates (EV SSL) for all sites requesting sensitive information including registration, ecommerce, online banking and any data which may request PII or sensitive information.[4]		✓
11. Develop and test a data loss incident response plan to be prepared for quick handling and response to best minimize risk and impact of an incident to customers and business partners.[5]	✓	
12. Maintain an aggressive program of software patch management where patches are tested and implemented immediately to prevent exploitation. Where possible, consideration should be given to implementing automated patch management, for operating systems, applications, add-ons and plugins. Prohibit employees from using end-of-life applications or limit use to secure sessions. (Complete a rapid test for compatibility.)	✓	
13. Continuously monitor third-party code, links and advertising on your site to help prevent malicious content and ads from being served on your site. Request third-party content providers and ad networks to adopt anti-malvertising guidelines.[6]	✓	
14. Enable secure encryption such as WPA2 on all wireless routers and access points. Hide your SSID (Service Set Identifier Names) or name it to help ensure that SSID does not provide identifying details. Change your encryption keys frequently to help prevent key disclosure or unauthorized use. If providing public wireless, limit how and when the network can be used, monitor usage and keep the network isolated from your business network.	✓	
Password Access Management & Provisioning		
1. Require strong passwords for employees and restrict customers from using weak passwords. Prevent old passwords from being reused. Consider preventing common and specific password from being used.	✓	
2. Consider forcing password resets every 30 to 60 days, ensuring services accounts are not used by staff or are not able to be used through customer facing application. Educate employees and customers on effective password management to minimize the risk of account takeovers.		✓
3. Implement an access policy management or rule-based permission client access system, limiting user access specific to their areas of responsibility.		✓
4. Perform regular entitlement reviews and remove terminated employee accounts immediately. Disable or remove any account unused after a predefined number of days	✓	
5. Consider modernizing password/passphrase requirements. Include security questions with highly variable answers which are not discoverable on social networking sites.		✓
6. Limit access attempts and force account shut down requiring administrative interaction.	✓	

[4] https://otalliance.org/resources/EV/index.html

[5] https://otalliance.org/resources/Incident.html

[6] https://otalliance.org/resources/malvertising.html

Password Access Management & Provisioning (continued)	Immediate	Within 90 days
7. Limit the number of login attempts by any one IP and/or block ranges of unknown IPs or out of band solutions for remote employees or customers		✓
8. Implement additional identity verification for system access including 2-factor security, IP address verification and security pins. Consider using on screen keyboard input.		✓
9. Inventory system access credentials, employ least required privilege policies.	✓	
10. Update privacy policies to state what is collected, who it is shared with and how it is used.	✓	

Employee Recommendations	Immediate	Within 90 Days
1) Consider the risks of social engineering (listing yourself as an ESP employee on LinkedIn makes you a target) and establish a social networking policy for employees. You cannot force people to stay off social networks (effectively) but you can make them aware of the risks.	✓	
2) Enable whole disk encryption on company computing device(s) which contain customer data or login credentials.		✓
3) Require company issue or reimbursed mobile phones to have remote wipe capabilities.		✓
4) Require and limit use of only approved browsers (see above)	✓	
5) Document best practices for employees to use on their home computers.	✓	
6) Establish a program for security awareness training and require employee completion of training modules.	✓	
7) Consider providing employees that have access to customer data only be on machines that do not have a data portability capability.		✓
8) Prohibit employees from saving data files or require automatic notification to management of any file being downloaded.		✓
9) Disable shared folders on all client systems.	✓	

Committee Members & Supporting Organizations

Supporting this initiative is a broad range of industry and business leaders who share a belief in the need for increased security and data stewardship. Committee members include American Greetings Interactive, Anti-Phishing Working Group, Campaigner, Concise Consulting, Constant Contact, Cypra Media, PulsePoint, Delivera, DigiCert*, eCert, e-dialog, Epsilon, Exact Target, FedEx, Iconix, Implex, Internet Identity, Intersections*, LashBack, MailChimp, MarkMonitor*, Marketo, Message Systems*, Microsoft, National Cyber Forensics & Training Alliance, PayPal*, Publishers Clearing House*, Return Path*, The Relevancy Group, Responsys, Reputy, QuePasa, Secunia, SilverPop, SimplyCast, Stopbadware.com, SubscriberMail, Symantec*, TRUSTe*, TrustSphere*, WhatCounts and Zynga. * OTA Board member.

OTA & Industry Resources - Security By Design Updates - https://otalliance.org/securitybydesign.html
OTA recommends a review of related best practices to develop a holistic security program suited to their business and industry.

- 2011 OTA Data Breach and Data Loss Incident Planning Guide https://otalliance.org/resources/Incident.html
- Why Your Browser Matters – https://otalliance.org/browser
- 2011 OTA Top 10 Tips to Protect Business & Consumer Data https://otalliance.org/resources/2011Top10Tips.html
- Anti-Malvertising https://otalliance.org/resources/malvertising.html
- DNSSEC https://otalliance.org/resources/dnssec.html
- Email Authentication https://otalliance.org/resources/authentication/index.html
- EV SSL Certificates https://otalliance.org/resources/EV/index.html

- Cloud Security Alliance https://cloudsecurityalliance.org/Research.html
- Federal Trade Commission – Keeping Your Business Data Secure http://www.ftc.gov/bcp/edu/microsites/infosecurity/
- Email Sender & Provider Coalition (ESPC) Data Security Best Practices http://www.espcoalition.org/
- Message Systems- Safeguarding Message Streams for Enterprises and Email Service Providers http://www.messagesystems.com/resources-white-papers-safeguarding-message-streams.php
- Microsoft Corporation – Enterprise Security Best Practices http://technet.microsoft.com/en-us/library/dd277328.aspx
- National Cyber-Forensics & Training Alliance http://www.ncfta.net/
- StopBadware http://stopbadware.org/
- Symantec - http://service1.symantec.com/SUPPORT/ent-security.nsf/7bc18d1a4d5824eb882573410063493f/755da16cf23f663a88257538005b03bf?OpenDocument
- U.S. Cert http://www.cert.org/governance/
- U.S. Department of Homeland Security https://buildsecurityin.us-cert.gov/bsi/home.html

Material in this publication is for educational and informational purposes only. The Online Trust Alliance (OTA) does not assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use. OTA and OTA members make no assertions or endorsements regarding the security or business practices of companies who may choose to adopt such recommendations outlined. For legal advice, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of all OTA member companies or affiliated organizations. OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. No part of this publication may be reproduced or distributed in any form or by any means, or stored without the written consent of OTA. For updates visit https://otalliance.org/resources/index.html Send comments and suggestions to staff@otalliance.org