Prepared by Future of Privacy Forum
July 2015

Security Quick Tips for Vendors

1. Risk: Data Interception
Solution: Encrypt Data in Transit
End-user network traffic is easily monitored or intercepted on open WiFi or over the wire by the operator of the network. To prevent sensitive information from being accessible to unintended parties, use HTTPS (SSL/TLS). Do not send passwords in clear text! (Also encrypt data at-rest; see 4. below)

2. Risk: Vulnerable Software
Solution: Regularly Patch and Update Software, Servers and Endpoints
Many data breaches are caused by the exploitation of vulnerabilities for which there are known fixes. In other words, the breach didn't have to happen. Require appropriate personnel to patch and update systems, quickly, routinely, programmatically, and often, in accordance with policy. Commonly, operations personnel apply patches, and version updates, while security analyst/engineers run scans to confirm that patching has been applied and vulnerabilities are remediated. (Keeping the distinction between the two roles provides a check and balance within the process.)

3. Risk: Database Compromise (Injection Attacks)
Solution: Use Accepted Secure Coding Practices
Code can masquerade as data, and the resulting "injection" attacks are the source of many data breaches. Thankfully the necessary secure coding practices to prevent injection attacks are well known, such as parameterized queries and sanitizing inputs. See https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

4. Risk: Lost or Stolen Laptops and Workstations
Solution: Require Full Disk Encryption
Require your security team to use full-disk encryption on all laptops and workstations. All information at rest in your control should be encrypted. This includes your servers, third party servers, but especially when it lives on a machine that can be tucked under an arm and carried out the door. If you use or allow portable storage media (thumb drives, any portable media), they should also be encrypted. Train employees to report lost or stolen equipment immediately.

5. Risk: Password Compromise
Solution: Deploy 2-factor authentication.
Require development teams to deploy 2-factor authentication on web-accessible log-ins. Yes, this is not always possible, or practical. Strive for it where possible; when it is not feasible, employ strong password rules and controls; apply practices appropriate to the level of risk of the data involved.

6. Risk: Relying on Hashing to De-Identify Data
Solution: Use Properly Salted Hashes
Although many hash outputs or "digest" values inputs cannot be easily reverse-engineered to determine the hash input, calculating look-up tables for certain types of uniform data is very easy. For example, a look-up table for all U.S. phone numbers can be calculated very quickly and used to look up "hashed" phone numbers. The solution is to use salted hashes and consult with a computer scientist to verify strength of resulting de-identification

7. Risk: Cloud Services (reminder, there is no "cloud" – it's just someone else's computer)
Solution: Do Your Due Diligence.
Determine if you can even use a cloud solution based on legal requirements. If you don't encrypt student data *before* it is sent to the cloud, the cloud provider has physical access to the data.

8. Risk: Third-Party Management and Hosted Solutions
Solution: Due Diligence and Contractual Constraints
Your responsibility and authority for data in your possession/control extends to its management while under the control of a third party providing you a service.
Contractual constraints –

- Seek third party audits or audit reports
- Verify insurance requirements and comply
- Include relevant reps and warranties
- Require incident response provisions

9. Risk: Browser Compromise Through Java Plug-In
Solution:

- **Disable the Java Plug-In in all Browser Software Enterprise-Wide**
- **Never Publish Software that Requires the Java Plug-in to be Installed in Order to Run**

Many instances of browser compromise occur because of security issues with the Java Plug-in for browsers. Block and disable the plug-in.

10. Risk: Other Browser and App Compromise
Solution: Require In-House and External Developers to Satisfy the Appropriate ASVS Standard
Consider using the ASVS standards – the aim of the OWASP Application Security Verification Standard (ASVS) Project is to normalize the range in the coverage and level of rigor available in the market for Web application security verification using a commercially-workable open standard. The standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection.
https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf

Additional Steps for Security Policy and Practices

- Incident response planning and preparation – have a breach response plan. Your contract may require it, but regardless, you should have (and test, and train for, regularly) your procedures for how to respond in the event of a breach, of different magnitudes
- Insurance
- Establish, update and regularly conduct training for employees, both those directly involved in security systems and those who simply need to understand their own responsibilities
- Employ a system or process for logging and monitoring of all activities

Additional Resources
https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet
https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
https://www.ftc.gov/datasecurity