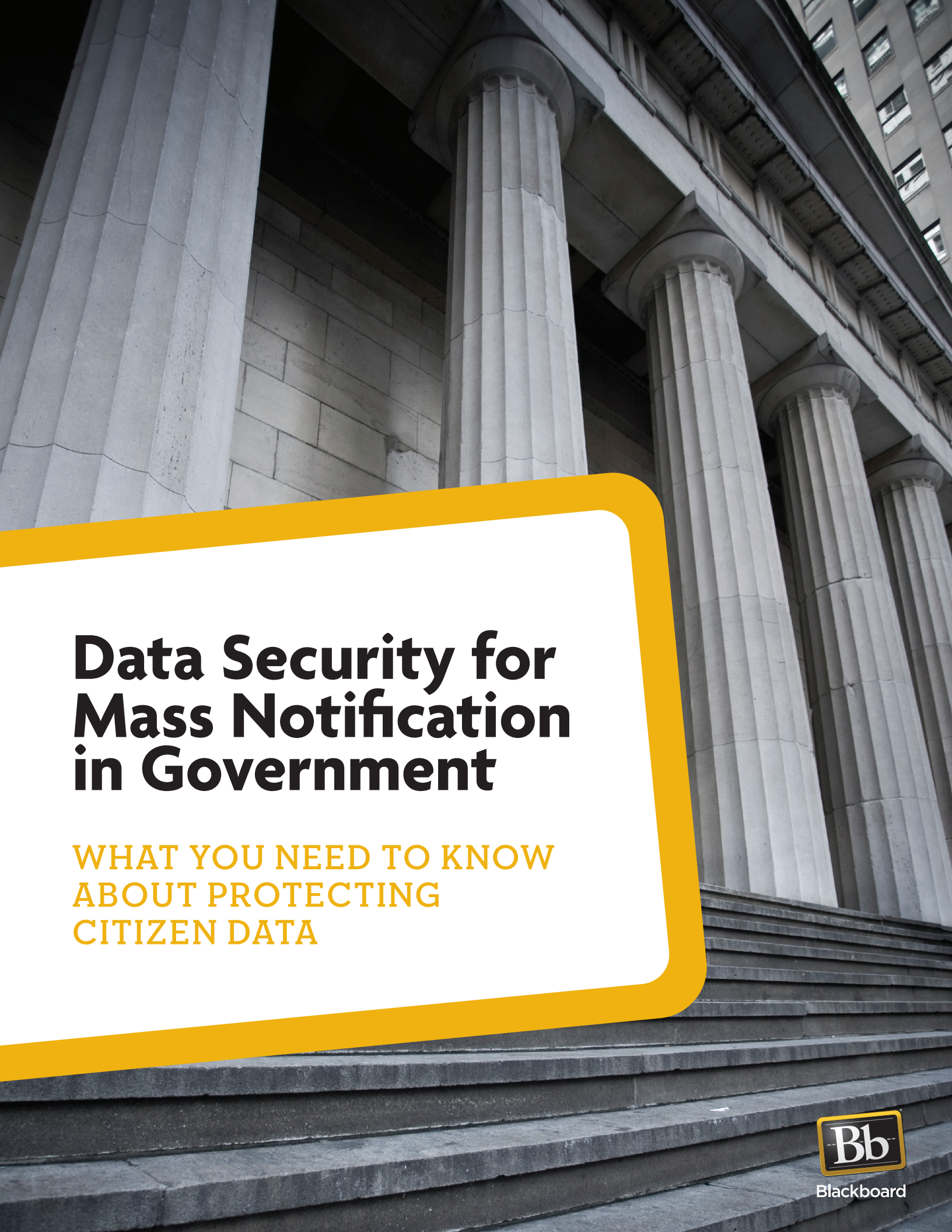


Data Security for Mass Notification in Government

WHAT YOU NEED TO KNOW ABOUT PROTECTING CITIZEN DATA

Blackboard

Executive Summary

The rise of notification technology has coincided with an increase in citizen demands for transparent communications from their leaders. Residents are expecting immediate and accurate information about the events and issues that affect their community.

As a result, mass notification systems have gained a significant foothold in local governments. It has now become the norm for local officials to reach out to citizens via phone, email, text – even social media – at a moment's notice. With this new emphasis on transparent communications, local governments must carefully assess their methods for protecting increasing volumes of citizen information.

What are the ramifications of this data falling into the hands of unauthorized parties? And how can government leaders ensure this personal information is protected? The risks and challenges cannot be underestimated.

Several factors affect the ability of a mass notification system to protect citizen contact data and deserve careful consideration when reviewing your security measures. These include physical data sites, data transmission, application security, backup policies, audits, and personnel. By asking the right questions and listening carefully to the answers, municipalities can determine which mass notification system offers the highest level of personal data protection. With years of proven performance in the mass notification industry, Blackboard understands how to meet and exceed security requirements. The Blackboard Connect™ for Government platform is helping local, state, and federal agencies across the country balance mass notification with secure communications.

Why Securing Personal Contact Information Is Important

The adoption of mass notification systems to keep the public informed has been on the rise and these systems are now used by more than half of all municipalities, according to a May 2010 study by Galain Solutions. These systems are driven by gigabytes of personal contact information including names, phone numbers, and email addresses. Governments must be vigilant stewards of this data.

Unfortunately, data breaches are not rare events. According to the Privacy Rights Clearinghouse, more than 500 million "records" of all types have been breached in the U.S. since January 2005.

Mass notification systems are built upon a foundation of trust between government and its citizens -- trust that the information sent will be accurate and timely and trust that the contact information will not be shared with unauthorized parties. Preserving this trust is paramount to the ongoing effectiveness of these systems.

Unfortunately, data breaches – in both the private and public sectors – are not rare events. According to the Privacy Rights Clearinghouse

(www.privacyrights.org/data-breach), as of November 30, 2010, more than 500 million "records" of all types have been breached in the U.S. since January 2005.

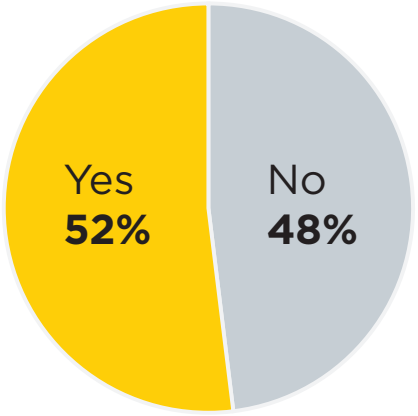
In addition to loss in confidence and trust, a data breach can be costly to a municipality. According to a PGP-sponsored 2009 Ponemon Institute survey, the average cost of a data breach increased last year to $204 per compromised record. These costs include those associated with detection, escalation, notification, and response. The average total cost of a data breach rose from $6.65 million in 2008 to $6.75 million in 2009, with a cost range per breach of approximately $750,000 up to nearly $31 million. Based on these statistics, it is possible that for a town of 50,000 citizens where half are affected, the breach could cost the town several million dollars to counter the incident.

Breaches of personally identifiable information (PII) can have far reaching effects for individuals, including identity theft, financial loss, and personal hardship. While any one piece of mass notification data—a name, a phone number, or an email address—may not alone expose an individual to significant risk, someone may cause injury with such information. Savvy criminals have a variety of means by which to compile additional personal data. When multiple pieces of data are used in concert, this information can lend credibility to someone seeking to gain information for identity theft purposes. Telephone scams initiated by knowledgeable callers are more successful in getting targets to share personal information. The same is true of email scams.

According to M86 Security Labs, the global volume of spam is approximately 200 billion messages per day. The 2009 Symantec Global Internet Security Threat Report finds that 15 percent of all spam messages contain money making scams, including "phishing" attacks that attempt to convince recipients to provide passwords or bank account details. Emails that include personal information are more likely to be opened and trusted.

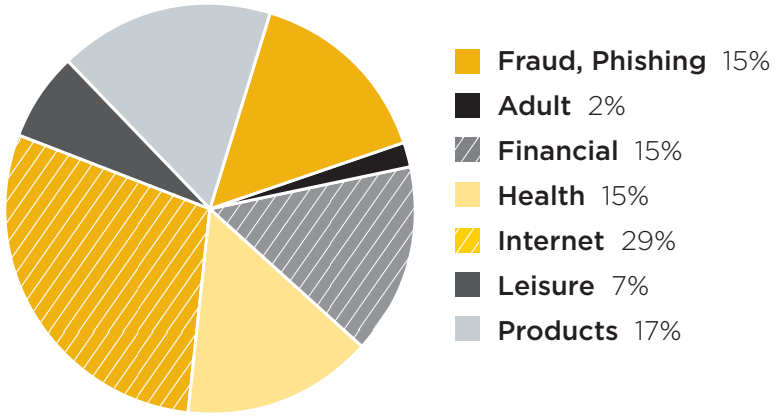
Organizations such as the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST) and a range of regulations including PCI DSS (Payment Card Industry Data Security Standard), FISMA (Federal Information Security Management Act), and HIPAA (Health Insurance Portability and Accountability Act) encompass PII protection mandates. While actual laws vary from state to state, by leveraging a set of industry-standard best practices for technology and processes set forth by these organizations and regulations, municipalities can take significant steps to protect individuals' data and preserve public confidence in mass notification programs.

MUNICIPALITIES THAT MANAGE OR HAVE ACCESS TO TELEPHONE-BASED ENS



Source: Galain Study

SPAM BY CATEGORY



Source: Symantec

Six Elements of a Secure Mass Notification System

Several physical, technological, and procedural factors affect the security of a mass notification system and deserve careful consideration when reviewing an organization's security posture. Government agencies should ask potential mass notification service vendors the following six questions:

1. What measures do you implement to support physical data security?

A comprehensive approach to data security should include:

- **Redundant physical data locations geographically dispersed across multiple power grids and time zones.**
- **Data facilities equipped with redundant power feeds and data connectivity.**
- **Data facilities that are fireproof, flood proof, and have level 4 rating earthquake protection.**
- **Data centers with 24/7/365 manned monitoring by experienced security personnel.**
- **Controlled data access limited to specific authorized personnel with valid identification, handprint identification, and key cards to enter the facility.**
- **Databases that are segregated into isolated Virtual Local Area Networks (VLANs) with stringent access control lists (ACLs) to protect data entering and exiting the network.**

2. How do you secure transmissions for all data transferred to and from clients' sites?

Secure transmissions should utilize industry-standard protocols and tools including:

- ***HTTPS/SSL/SFTP.*** **All data transmitted to and from a client administration website should offer secure transmissions that use 128-bit Secure Socket Layer (SSL) encryption or better. All data transfer should be performed using either SSL or SSH File Transfer Protocol (SFTP) at the client's preference.**
- ***Firewalls.*** **All database servers should be behind a firewall, inaccessible from the outside, and secured on a separate VLAN with non-routable IP addresses to the Internet. All firewalls should be monitored 24/7/365 by experienced security personnel using the latest industry standard tools.**
- ***Web Application Firewalls.*** **In addition to standard firewalls, web application firewalls add another line of defense, filtering all requests, and inspecting all traffic for malicious content (e.g., SQL injections; cross-site scripting).**
- ***Intrusion Prevention Systems (IPS).*** **A layered approach to data security also includes IPS hardware, which monitors and detects malicious activity and attacks, preventing unauthorized access to data servers.**
- ***Controlled Access.*** **Employee access should managed with stringent access control lists and require domain-level authentication for access.**
- ***DMZs.*** **As further protection, web servers should reside in a perimeter security network called a demilitarized zone (DMZ) that separates the internal network from the outside world.**

SIX ELEMENTS OF A SECURE MASS NOTIFICATION SYSTEM

- Physical data sites
- Data transmission
- Application security
- Backup policies
- Audits
- Personnel

3. How do you ensure application access remains secure?

Password and verification security should include robust password requirements like alpha-numeric passwords that must be changed frequently and the addition of a security profile that includes questions that must be answered in order to reset the password.

4. What are your backup policies?

To ensure data recovery, data backups should be conducted on both an incremental and weekly basis. All data should be encrypted, backed up nightly, and removed to an off-site location. Client data should only be duplicated for the creation of authorized back-up copies.

5. What risk assessment tools and processes do you have in place?

Organizational security controls should incorporate all aspects of internal and external risk assessment, including:

- **Internal audits conducted at minimum on a bi-annual basis to ensure security measures are maintained across the organization.**
- **Annual third-party audits and scoring by an accredited organization to rate the mass notification system provider against widely accepted security best practices and standards.**
- **System logging, monitoring, and reporting practices and tools to identify potential security threats and immediately notify personnel in the event of any suspicious activity.**
- **A combination of vulnerability scanners, security baseline analyzers, and robust application scanners to identify potential network vulnerabilities.**
- **Monitoring industry-issued security advisories and bulletins on a daily basis to keep apprised of the latest threats.**
- **Frequent reviews of operations and business practices to maintain compliance with corporate policies and procedures governing the security and confidentiality of information.**
- **Professional staff trained and certified in data security best practices.**

6. What types of qualifications and certifications do your security personnel hold?

Security is not just a hardware or software issue. Personnel must be screened to ensure they have the qualifications and credentials necessary to maintain security best practices, for example:

- **All employees should undergo and clear a rigorous comprehensive pre-employment background and reference check conducted by third-party independent professionals.**
- **Upon hire, all employees must sign a Confidentiality Agreement, a Code of Business Conduct Policy, and other policies which govern the use of electronic communications and technology resources.**
- **During the orientation process and throughout the employment period, each employee should receive education on the latest security, confidentiality, and privacy protocols and processes.**
- **Security personnel should be required to seek and maintain widely-respected industry certifications such as the NSA-IEM certification (National Security Agency-Infrastructure Evaluation Methodology), and the CISSP accreditation (Certified Information Systems Security Professional), which is overseen by the International Information Systems Security Certification Consortium or (ISC).**

How a mass notification vendor answers these questions will provide government leaders with the information they need to determine if their citizens' personal contact data is protected or exposed.

How Blackboard Connect Measures Up

The Blackboard Connect mass notification platform delivers robust and effective alert capabilities while protecting client data around the clock. Blackboard's comprehensive approach to security has been validated by recognized third-party assessors.

Foundstone Certification and AAA Rating

For the fourth year in a row, the Blackboard Connect platform has been awarded a AAA security certification from Foundstone Professional Services, a division of McAfee, Inc. Foundstone issued its AAA rating for the Blackboard Connect platform after thoroughly testing the system's external and internal network connections, as well as its web applications, for best practices among Software-as-a-Service (SaaS) providers. Foundstone is the industry leader in network security consulting, serving a large segment of the Fortune 500 and many U.S. government agencies. Blackboard is the only mass notification service provider to hold Foundstone certification and the AAA rating.

U.S. Department of Commerce Certification

The Blackboard Connect solution is certified with the U.S. Department of Commerce's Safe Harbor program, which ensures compliance by U.S. firms with the European Union (EU) directive on privacy and the use of personal data. EU standards for digital communications are among the most stringent in the world and the recently announced EU Digital Agenda continues member nations' active focus on privacy and data protection.

FOUNDSTONE SECURITY CERTIFICATION CRITERIA

Grade	Security	Criteria Description
A	Highly Secure	Attention to security exists and policy is implemented effectively and consistently. No high risk vulnerabilities were identified and there is clear recognition of asset criticality and threat likelihood in the defense measures taken.
B	Moderately Secure	Attention to security exists, but there are issues with the completeness of the organization's security policy or the organization's ability to execute its security objectives consistently for lower priority assets. This is reflected in a small number of vulnerabilities being identified, with no high risk issues associated with critically important assets.
C	Marginally Secure	Attention to security exists, but there are issues with the completeness of the organization's security policy or the organization's ability to execute its security objectives consistently for all assets. This is reflected in a small number of high risk vulnerabilities being identified that could be exploited to compromise critically important assets.
D	Unsecure	Attention to security requires improvement. Significant gaps in security policy exist and/or execution issues prevent the organization from securing its critical assets from attack. A large number of high risk vulnerabilities associated with critically important assets were identified.

For the fourth year in a row, Blackboard received 'Highly Secure' ratings in all three categories: Web Application Testing, External Penetration Testing, and Internal Penetration Testing.

Blackboard Connect for Government

The Blackboard Connect solution allows state and local government officials to provide millions nationwide with time-sensitive information – via voice, text, email, Facebook, Twitter, and more – while keeping contact information secure. The Blackboard Connect solution makes security a top priority through a proactive, robust security program that constantly researches and implements the latest security best practices to protect personally identifiable information. Current comprehensive, industry-standard security features and practices include:

- **A security posture driven by ISO and NIST standards for business continuity planning; system access control; system development and maintenance; physical and environmental security compliance; human resources security and personal security; and computer network management**
- **Fully-certified Security Managers (NSA-IEM, CISSP, Watchfire- and Qualys-certified engineers)**
- **Background checks on all employees conducted by third-party professionals and ongoing personnel training**
- **State-of-the-art software and hardware to protect all data involved in any transaction**
- **Industry-leading password and verification procedures, including new password requirements, security questions, lockout based upon multiple attempts, and password expiration**
- **Secure transmissions with 128-bit SSL encryption or better, with all data transfers performed using the highest security protocol possible**
- **Fully-redundant, state-of-the-art facilities that require photo identification, thumb-print recognition, and keyed access and are manned 24/7 with experienced security personnel**
- **Firewalls, intrusion prevention systems, and demilitarized zones for every database server that separate the internal network from the outside world**
- **Regular internal and external audits**
- **Adherence to the strictest possible privacy policies and protocols to ensure data protection**

The Blackboard Connect solution's comprehensive approach to security has been validated by recognized third-party assessors.

Moreover, Blackboard will never sell, trade, lease, or loan any data about its customers to any third-party.

Conclusion

The importance of securing citizen contact information cannot be underestimated. Disclosure of contact data through a breach can have a long-term negative impact, for both impacted citizens and government agencies.

Six factors must be considered when evaluating a mass notification system to ensure it measures up to security best practices and standards: physical data sites, data transmission, application security, backup policies, audits, and personnel.

As a proven leader in mass notification systems, Blackboard is committed to satisfying the security requirements of local, state, and federal agencies across the nation through its Blackboard Connect platform. If your organization is interested in finding a government to citizen mass notification solution that makes security a top priority, contact Blackboard Connect to learn more.

blackboard.com/connect • 650 Massachusetts Avenue, NW 6th Floor Washington, DC 20001 • 1.800.424.9299, ext. 4

Copyright © 1997-2011. Blackboard Inc. All rights reserved. Blackboard, the Blackboard logo, BbWorld, Blackboard Learn, Blackboard Transact, Blackboard Connect, Blackboard Mobile, Blackboard Collaborate, the Blackboard Outcomes System, Behind the Blackboard, and Connect-ED are trademarks or registered trademarks of Blackboard Inc. or its subsidiaries in the United States and/or other countries. Blackboard products may be covered by one or more of the following U.S. patents: 7,493,396, 7,558,853, 7,816,878.