Content Encryption: Key Issues to Consider

An Osterman Research White Paper
Published September 2015
EXECUTIVE SUMMARY

Encryption of electronic content is an essential best practice, despite the fact that many organizations and individual users do not encrypt email, files stored behind their corporate firewall, files stored in the cloud, and in other venues. However, most IT administrators understand the benefits of encrypting content to protect sensitive or confidential information, to protect their organizations against data breaches, to satisfy regulatory obligations, and to protect against various types of legal liabilities, as shown in Figure 1.

Figure 1
Top Reasons for Using Encryption
% Responding a “Driver” or “Major Driver”

<table>
<thead>
<tr>
<th>Reason</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>The need to protect sensitive/confidential</td>
<td>70%</td>
</tr>
<tr>
<td>information</td>
<td></td>
</tr>
<tr>
<td>To protect against data breaches</td>
<td>56%</td>
</tr>
<tr>
<td>Regulatory requirements we must satisfy</td>
<td>55%</td>
</tr>
<tr>
<td>Protection against legal liabilities</td>
<td>52%</td>
</tr>
<tr>
<td>To reduce overall corporate risk</td>
<td>43%</td>
</tr>
<tr>
<td>The need to protect intellectual property</td>
<td>34%</td>
</tr>
<tr>
<td>To protect against insider threats</td>
<td>19%</td>
</tr>
<tr>
<td>To reduce costs with more efficient workflow</td>
<td>16%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

It is important for decision makers to understand that encryption is more than simply a defensive strategy to protect against data breaches or to comply with regulations. Organizations that encrypt content can create new business opportunities and create competitive differentiation that can contribute significantly to their bottom line and provide new ways of attracting and keeping customers.

KEY TAKEAWAYS

- Most organizations do not provide the ability for users to encrypt email manually or through administrator-created, policy-based mechanisms, although one-half of users are expected to have policy-based encryption by mid-2016, as shown in Figure 2 on the next page.

- A failure to encrypt content can create a variety of legal, regulatory and other problems. The trend toward increasing use of employee-owned mobile devices, mobile apps and cloud-based applications is making the problem significantly worse.

- There are a number of barriers to adopting encryption that must be overcome before its use becomes more common.
• The consequences of failing to encrypt content are serious and can create debilitating problems for any organization.

• All organizations should place a high priority on encrypting content sent through email, stored locally, on mobile devices and stored in the cloud.

ABOUT THIS WHITE PAPER
This white paper discusses the results of an in-depth, primary market research survey conducted with 150 IT professionals who are knowledgeable about the use of encryption within their organizations. The survey was conducted during August 2015. The paper also discusses the key issues surrounding encryption, offers some best practice recommendations for decision makers to consider, and provides information about Alt-N, the sponsor of this paper.

CONTENT MUST BE ENCRYPTED
EMAIL IS TYPICALLY NOT ENCRYPTED
Most emails and other electronic communications sent by users in the typical organization are not encrypted. Moreover, a significant proportion of application-to-human content, such as bank statements or airline itineraries are also sent unencrypted. The primary reason for this is that the majority of email users do not today have their email processed through a secure email gateway or have access to manual encryption capabilities, despite the fact that the secure email gateway market is relatively mature. However, the proportion gateway processed email is expected to increase significantly by 2016, as shown in Figure 2.

Figure 2
Penetration of Encryption Capabilities, 2015 and 2016

![Penetration of Encryption Capabilities](source: Osterman Research, Inc.)

It is important to note that encryption is very definitely a “two-way street”. While many organizations focus on outbound encryption of email and other content that is sent outside the firewall, there needs to be an equal focus on inbound communications, as well. For example, if an outside party sends sensitive or confidential information to someone inside an organization, it is essential to manage
that information properly to prevent its storage on file servers, in cloud storage, in the user’s mailbox, or in other venues in an unencrypted state.

**USER PROBLEMS: ERRORS AND OTHERWISE**

Although we discuss the consequences of not encrypting content later in this white paper, it is important to note here that one of the fundamental problems that occurs when failing to encrypt content is much greater susceptibility to user mistakes. For example, it is not uncommon for users to send sensitive or confidential information to the wrong party when they are rushed and fail to recognize this. The “type-ahead” feature in most email clients is a common culprit in these types of mistakes, as is managing files via a file sync and share service like Dropbox. Here are just a few examples of users mistakenly sending unencrypted content that have occurred during 2015:

- An employee at Nationstar Mortgage mistakenly emailed copies of customers’ W-2 forms to an employee at Greenlight Mortgage, revealing Social Security numbers, names, addresses and other sensitive information.
- 845 patients of Tulare County Health received information on how to access protected health information (PHI) via the administration’s medical portal due to an employee mistake.
- Graduate students at the South Dakota School of Mines and Technology were inadvertently sent an email attachment that included the student identification numbers, grade point averages and other information of about 350 fellow students.

There is a need to encrypt a wide variety of communications and content types that today are typically sent and stored unencrypted. A number of information types that traditionally are sent in clear text – such as financial statements, presentations, purchase orders, press releases and the like – should be sent so that the sensitive or confidential content within them cannot be accessed. Plus, there is value in revoking decryption rights for ex-employees, former business partners, contractors and others who should no longer have access to encrypted content after the organization’s relationship with them has changed or been terminated. However, most users do not have available to them any sort of rights-management capability that will allow them to control the lifecycle of, or actions that can be taken on, the content they send.

Although not really an email or communications issue, decision makers must address the less common occurrence of a disgruntled contractor, employee or other individual who can steal confidential information that lies unencrypted on corporate file servers, on FTP servers or in various databases. For example, in a case that started innocently with an email sent to the wrong party, Planet Fitness alleged that one of its former employees had accessed and stored confidential corporate information on his home computer and “threatened to release it publicly right before Planet Fitness went public, in an attempt to disrupt the IPO.”

**CONSUMERIZATION IS WORSENING THE PROBLEM**

Much has been made of the various BYO (Bring Your Own) problems, such as BYO Devices, BYO Applications and BYO Cloud, and for good reason: these various BYO-related issues are contributing significantly to the problems that a lack of encryption can create. For example, the proportion of personally-owned devices used in the workplace to access sensitive corporate resources like email, CRM databases, ERP systems and the like is growing at a significant pace. However, as shown in Figure 3, only a fraction of personally owned devices, when compared to company-supplied devices, are managed by any sort of IT-managed encryption. Add to this the significant proportion of employees who use various personally managed mobile apps, social media tools, telephony tools, and other cloud-based applications without IT management or oversight of any kind.
A key element in making the encryption problem worse is the proliferation of cloud-based file sync and store tools that are commonly used by employees, many of which are used without any endorsement from corporate IT, as shown in Figure 4.

The BYO phenomenon is a key element in the trend toward multi-platform, mobile interaction with corporate applications and cloud-based services, only some of which are actually sanctioned by corporate IT. The trend toward BYO is being driven by a number of factors, including employees’ desire to use the latest and greatest, budget constraints within many IT departments, increased employee mobility that motivates employees to adopt productivity tools that may not yet be sanctioned by IT decision makers, and IT being hampered by the rather sensible notion that new capabilities should be vetted properly before they are used to access and modify sensitive corporate data.
The BYO phenomenon increases the possibility that sensitive or confidential information will be breached in some fashion. For example, in a somewhat dated, but still relevant study, researchers acquired 49 mobile devices that had been resold through various secondary markets. The forensic examination of these devices found information on every device and more than 11,000 pieces of potentially important information from all of the devices in aggregate.

From an encryption perspective, the BYO problem is a serious and growing concern for decision makers because it permits an increasing proportion of employees to send and access corporate information independently of any IT-managed encryption capability. This increases the risk of data breaches and the problems that accompany them.

EMAIL ENCRYPTION GATEWAYS
An email encryption gateway is conceptually simple: it’s a platform that will process content based on corporate policies so that emails are automatically encrypted before they are sent. Key elements of an email encryption gateway generally include the following:

• Policies are pre-defined so that outbound content will be automatically encrypted based on pre-defined policies that are dictated by regulatory obligations, legal requirements or corporate best practice.

• Multiple applications are supported so that content sent to Gmail, Salesforce.com, Office 365, custom applications built on the Amazon.com infrastructure or any other service will be automatically encrypted.

• Data formats are preserved so that content is not modified by the encryption process.

• Data is encrypted both in transit and at rest so that any content outside of the organization’s direct control cannot be accessed by third parties.

• Multiple device types are supported so that users can employ the gateway to encrypt content sent from their desktop computer, smartphones, tablets, home computers or any other platform that they might employ.

While there are many encryption gateways available that have been on the market for a number of years, many of these solutions take a somewhat different approach to managing email. For example, many legacy gateway encryption solutions do not permit users to receive emails using their native email client, but instead require messages to be retrieved from a secure portal. While this is functionally acceptable in that it allows content to be received securely, it represents a barrier to the adoption of encryption simply because many users do not want to use two different interfaces to receive email. Moreover, many of these solutions encrypt content only in transit or when stored remotely, not in each user’s inbox. This can create the potential for a data breach if a device is lost or stolen. Many end-to-end encryption solutions also provide robust functionality, but they require the use of desktop software or email client plug-ins, complicating the management of the solution for IT.

BARRIERS TO ENCRYPTION
There are a number of factors that inhibit the use of encryption, even in situations where encryption is required or would otherwise provide demonstrable benefits. Among the factors slowing the use of encryption are the following:

• Encryption and archiving of content
  A growing proportion of organizations archive their content because of regulatory obligations to do so, eDiscovery requirements, advice from legal counsel, or simply a desire to preserve content for access by employees. However, if an
organization has not coordinated its archiving and encryption strategies, there can be problems. For example, encrypted content stored in an archive for which keys are no longer available creates the real possibility that some archived data will not be accessible, such as after an employee leaves the company. However, if the right technology is used, emails can be encrypted on a per-user basis to ensure that information is protected from someone with keys to the entire archive having access to all archived email. Plus, if the contents can be decrypted to ensure that content can be indexed, this permits a search of encrypted email without compromising the integrity of the archived content.

• **Encryption and mobile don’t always get along**
  Mobility is becoming a critical issue because of the growing trend for employees to use mobile devices and because of increasing use of personally owned devices. When IT decision makers evaluate email encryption solutions, it is essential for them to consider how these solutions’ support users sending, receiving, encrypting and decrypting messages across a wide range of mobile devices. The best encryption solutions will support all of the mobile devices in use in an organization without requiring the installation of plug-ins or additional software.

  From a usability perspective on mobile devices, encryption can be a difficult experience. Typing a strong password on a smartphone screen is cumbersome and error-prone. The use of PINs is also difficult, plus they are relatively easy to guess because of their predictability. For example, one analysis found that 10.7% of PINs are “1234” and 6.0% are “1111”. In fact, although there are actually 10,000 different combinations of four digits, the analysis found that one-half of those used were concentrated in just 426 different combinations. That said, PINs are generally preferable to passwords because mobile devices autocorrect text, making their entry tedious and time-consuming (up to 30 seconds for the typical password on a mobile device).

• **Encryption used to be difficult (and many still perceive it to be)**
  Some legacy encryption solutions were difficult to use and were more of an impediment to productivity than a benefit. While current-generation encryption capabilities are generally much easier to use, the legacy of difficult encryption continues. For example, in the survey conducted for this white paper, we found that only 26% of IT professionals agree or strongly agree with the notion that encrypted emails are easy for recipients to open in the context of the desktop experience; this figure is only 28% when IT professionals are asked about the use of encryption on mobile devices. When IT professionals were asked to rate the end user experience for encryption, only 17% agreed or strongly agreed that encrypted emails are easy for end users to open in the context of the desktop experience, and only 16% felt this way about the mobile experience.

• **Key management schemes are lacking**
  An encryption capability must include robust key management, but its cost and ease of administration can vary between solutions. Some encryption solutions offer basic key management that requires a minimum of infrastructure and IT staff time to manage, while others employ cloud-based key management to entirely eliminate on-premises infrastructure requirements.

• **Efficient automation and policy definition are not available**
  In most cases, email encryption should be policy based and solutions will automatically encrypt content based on various keywords, character strings and pattern matching in the subject line or body of the message. However, some encryption solutions lack efficient automation schemes and so do not offer the ability to define policies easily. In most cases, IT wants encryption policy definition to be part of a larger policy management system instead of a separate tool that requires its own interface and learning curve.
Encryption can make monitoring more difficult

Messages that are encrypted end-to-end present a dilemma for content monitoring: does IT allow the message to flow through unchanged, or does it decrypt messages to check for policy and content violations? If encryption is employed to hide intentional violations of corporate policy or the law, that increases corporate risk. On the other hand, if messages are legitimately encrypted to comply with policies or regulations for confidential or sensitive information, unnecessarily decrypting those messages creates the risk that the decrypted message will be accessible to unauthorized individuals. On balance, Osterman Research believes the most appropriate course of action is to decrypt inbound messages to check for policy violations, but decision makers must understand the risk of either option.

That said, properly designed and integrated gateway encryption solutions take this issue into account. For example, inbound messages that are encrypted with an "approved" encryption scheme are decrypted in memory at the gateway, scanned for compliance with various policies, and sent in encrypted form to the proper destination based on policy. By default, the gateway and the intended recipient have access to the unencrypted contents of the message and its attachments. In this type of system, inbound messages encrypted with other forms of "unauthorized" encryption are typically handled by an "acceptable encryption policy". Normally, these policies specify a set of trusted recipients that may be allowed to receive arbitrary encrypted messages, but these messages will be quarantined if directed to others.

THE CONSEQUENCES OF NOT ENCRYPTING

As shown in Figure 5, 25% of organizations have attempted to deploy an email or content encryption solution that either has failed or was not adopted. Moreover, 5% of organizations have been fined or warned about the leakage of confidential information, while 3% have been fined or warned about their lack of an encryption solution.

Figure 5
Encryption-Related Problems That Have Occurred

<table>
<thead>
<tr>
<th>Problem</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not respond/has not happened</td>
<td>69%</td>
</tr>
<tr>
<td>We have attempted to deploy an email or content encryption solution that has failed and/or was not adopted</td>
<td>25%</td>
</tr>
<tr>
<td>We have been fined or warned for the leakage of confidential information</td>
<td>5%</td>
</tr>
<tr>
<td>We have been fined or warned for the lack of an encryption solution</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.
What this data highlights is that a fairly significant proportion of organizations admit to their formal censure for leakage of sensitive or confidential information and/or their failure to implement an encryption solution. It is more likely, however, that the numbers of those who have had problems are significantly greater than those shown in the figure above because many decision makers are reluctant to share information about corporate sanctions, data leakage and other, similar types of unpleasant occurrences.

The consequences of failing to encrypt content can be several and severe, as discussed below.

**DATA BREACHES**

As of early September 2015, PrivacyRights.org had catalogued 857.7 million records breached across 4,597 publicly announced individual data breaches since 2005. This equates to an average of roughly 86 million records breached per year, more than 230,000 records breached on a typical day, and about 187,000 records lost per breach incident. The Verizon 2015 Data Breach Investigations Report shows even more depressing numbers: 79,790 security incidents that resulted in 2,122 confirmed data breaches during 2015 alone.

Data breaches can be enormously expensive to address because 47 US states, Washington DC, Puerto Rico, Guam and the US Virgin Islands have all passed legislation that requires the full disclosure of data breaches involving personal information. California began this movement back in 2003, but most North American governments have followed their lead in the ensuing 12 years.

"Addressing" a data breach can mean several things:

- The cost of notifying those whose data was breached, even if no financial or other loss has occurred.
- The cost of providing credit-monitoring services for at least a year to those who were affected.
- The negative publicity that follows many data breaches. This can include questions from regulators, investors, stockholders, customers and prospects that can seriously damage an organization's standing in its industry.
- The long-term, ongoing impacts from customers that no longer want to do business with a firm that cannot protect its own or customers' sensitive or confidential information. Because customers are less likely to do business with an organization they cannot trust, this results in potentially severe impact to corporate revenue in the short term and even larger impacts over the long term.

It is important to note two important caveats about data breaches in the context of encryption: a) not every data breach results in actual data loss or an impact on the entities whose data was lost, and b) many data breaches are the result of factors that encryption does not directly address, such as phishing and malware. However, a substantial proportion of data breaches can be minimized or eliminated by the use of email encryption and/or device encryption.

**LOSS OF SENSITIVE OR CONFIDENTIAL DATA**

Frankly, the bulk of email or other electronic content is not of sufficient interest to third parties to warrant their attention in trying to intercept it even if it’s not encrypted. However, there are cases in which interception of data can be incredibly damaging even if it won’t trigger a regulatory obligation to report the breach. For example, engineering drawings, financial projections, marketing plans, corporate health plan changes, legal opinions and a host of other information should be encrypted to prevent its accidental or intentional disclosure. Unfortunately, much of it is not.
Exacerbating the problem is the growing number of file sync and share tools that are used in the workplace, as discussed earlier. An Osterman Research survey revealed that 13% of corporate data is stored on employees’ laptops, 5% is stored on smartphones and tablets, and 1% is stored on employees’ home computers. A significant proportion of this data is synced with these platforms using file sync and share tools.

The primary implication of the growing use of non-IT sanctioned (commonly referred to as “shadow IT”) file sync and share tools is that organizations are losing much of their control over corporate content because copies of these assets are stored with a variety of third party providers and managed solely by employees. Moreover, IT is less able to control the management of information in their organizations for purposes of legal and regulatory compliance. Plus, because many file sync and share tools do not encrypt data at every point during the data transfer or storage process, this leaves corporate data subject to interception and loss.

REGULATORY VIOLATIONS
Most organizations have corporate governance obligations with which they must comply. Although these requirements are particularly stringent in heavily regulated industries like financial services, energy, healthcare and life sciences, among others, all organizations have some level of regulatory obligation to satisfy. Examples of these obligations, which are focused mostly on the archiving, encryption and monitoring of certain types of communications, include:

- **Payment Card Industry Data Security Standard (PCI-DSS)**
  This is a set of requirements for protecting the security of consumers’ and others’ payment account information that primarily impacts retailers. It includes requirements for building and maintaining a secure infrastructure, encrypting cardholder data when it is sent over public networks, and assigning unique IDs to each individual that has access to cardholder information.

- **Health Insurance Portability and Accountability Act (HIPAA)**
  This regulation applies primarily to healthcare, but also a variety of other organizations, to protect sensitive health information about patients. However, the “new” HIPAA that took effect during the first quarter of 2010 greatly expands the impact of the law. While HIPAA previously applied mostly to medical practices, physicians, hospitals and the like, now business associates of these entities are required to comply with HIPAA’s rules about the security and privacy of protected health information (PHI). That means that benefits providers, accountants, attorneys and others that are given access to PHI are now fully obligated to comply with HIPAA.

- **Financial Industry Regulatory Authority (FINRA)**
  This organization sets forth a variety of strict and detailed requirements for supervising, archiving and managing the communications of registered representatives and others involved in the financial industry. As just one example of FINRA’s oversight in the context of encryption is Rule 8210, which governs how member organizations are obligated to provide information to FINRA during investigations, examinations or proceedings. Rule 8210(g) states, “Any member or person who, in response to a request pursuant to this Rule, provides the requested information on a portable media device must ensure that such information is encrypted.”

- **Gramm-Leach-Bliley Act (GLBA)**
  This regulation obligates financial institutions to protect private information about individuals, including their names, addresses, phone numbers, bank and credit card account numbers, information about income and credit histories, and Social Security numbers.

- **Family Educational Rights and Privacy Act (FERPA)**
  This is a US federal law focused on protection of student records in schools that
receive funds from the US Department of Education. The majority of the requirements in FERPA are focused on maintaining the accuracy of student records and providing parental access to them, but there are provisions in the law for sending these records, as well. In cases where a school needs to disclose student records to another school, an accrediting organization or the courts, encryption plays a key role in maintaining the privacy of these records.

RECOMMENDATIONS

BEFORE IMPLEMENTING TECHNOLOGY, DEVELOP AN ENCRYPTION PLAN

For organizations that have not fully embraced encryption, perhaps the place to begin the process is by targeting the areas that are most obviously in need of it. Decision makers should identify privileged communications, as well as content that could greatly harm the company’s standing with business partners and other key constituencies if intercepted. This includes emails that contain clearly sensitive documents like financial projections or draft policy statements; and content that contains obviously confidential information like bids, tenders, acquisition information, employee medical records or customer financial information. This content typically represents the vast majority of the risk in most organizations and is the easiest to address. This can be followed by the less obvious use cases that might require more effort and integration.

QUANTIFY THE RISKS OF A FAILURE TO ENCRYPT

It is essential that decision makers understand the significant consequences that can result when sensitive or confidential data is not encrypted. These consequences include lost internal data like financial projections or trade secrets, lost customer information that can trigger data breach notification obligations, large fines, or damage to corporate reputation. It is useful for decision makers to quantify the cost of a data breach as a starting point. For example, if there is only a 1% chance per month of a data breach that could cost an organization $500,000 (a rather small impact of a single data breach) in remediation and other costs, that represents a $5,000 monthly potential cost to the organization.

CAN YOU CREATE A BUSINESS CASE FOR ENCRYPTION?

As a corollary to the point above, there are two ways to justify the deployment of encryption capabilities:

- Defensively, to mitigate the risks associated with failing to satisfy statutory obligations, defending against data breaches, protecting intellectual property, and the like. This is the “basic” business case for encryption and perhaps the easiest to sell to senior decision makers.

- However, the business case for encryption does not have to be based solely on regulatory compliance and data breach prevention. While the defensive argument helps to avoid fines or lost business, encryption can also create new business opportunities that would not otherwise be available. As just one example, this might include the ability to provide customer statements electronically, which can not only reduce the cost to the vendor, but also provide an improved and “stickier” customer experience. Sending statements encrypted also provides an added benefit of easily tracking delivery of the statement, and when and if it was opened. Plus, in the case of email, encryption can enable secure communications and transactions over low-cost, well understood and easy-to-use communication channels in a variety of industries, such as healthcare, mortgage processing and banking.
CREATE POLICIES AND REVISIT THEM OFTEN

Next is to create detailed and thorough policies based on legal, organizational and regulatory obligations to protect content using encryption. This should include a discussion of the important business risks that need to be mitigated, consequences for violating corporate data protection policies, and should also provide a thorough perspective on BYO-related policies. The last point should include devices, operating systems and applications that can and cannot be used by various roles within the organization.

As part of the policy development phase should be employee education about the policies that have been created and the dangers of not using encryption where it needs to be used. For example, encryption capabilities should be used to provide feedback and indirectly train employees about handling sensitive information, such as via notifications when sensitive content is included in an unencrypted email or file transfer.

Employees who regularly deal with sensitive or confidential content that should be encrypted when sent externally should have encryption handled automatically through a policy-based system. In this approach, a pop-up message to the offender shouldn’t be required, but instead automated systems should handle the encryption activities automatically, or at least route the message through a secure channel.

EVALUATE THE DEPLOYMENT OPTIONS

The last step is to evaluate the available deployment options for encryption solutions. These include traditional, on-premises software deployed on IT-managed servers; physical and virtual appliances; cloud-based services; and combinations of two or more of these using a hybrid approach. Many organizations will want to consider a hybrid approach to encryption, perhaps deploying an on-premises solution for some staff and a cloud service for others.

As shown in Figure 6, roughly one-half of organizations view on-premises email encryption provided as part of the email system to be the most secure encryption model, followed by cloud-based email encryption.

Figure 6
Views on the Most Secure Encryption Delivery Models

Source: Osterman Research, Inc.
SPONSOR OF THIS WHITE PAPER

Alt-N Technologies develops email and email security software for the global SMB market. Founded in 1996, its products are trusted by small-to-medium businesses in over 90 countries and 25 languages. The company’s flagship products, MDaemon Messaging Server and SecurityGateway for Email Servers can be deployed in hosted cloud or private on-premise environments. Alt-N products include the latest email encryption and security technologies and require minimal support and administration to operate and maintain. The company uses a network of global distributors and resellers for the sale and support of its products.
Content Encryption: Key Issues to Consider

© 2015 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader’s compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

i http://oag.ca.gov/ecrime/databreach/reports/sb24-57381
ii http://www.databreaches.net/ca-email-error-exposes-845-tulare-county-patients-email-addresses/
iv http://www.fosters.com/article/20150811/NEWS/150819917
v Electronic Retention: What Does Your Mobile Phone Reveal About You?
vi http://EzineArticles.com/7068075
vii Source: PrivacyRights.org
viii http://www.datagenetics.com/blog/september32012/index.html