Why Your Organization Faces Risk from the Epsilon Email Breach (Even if They Are Not Your Vendor)

04.08.2011

Elizabeth H. Johnson

If you have an email account, then you by now have received one or more emails from companies notifying you that their email communication provider, Epsilon, suffered a security breach that resulted in unauthorized parties accessing your name and email address. Since Epsilon purports to send 40 billion emails annually, and boasts over 2,500 corporate clients including 7 of the Fortune 10, the impact has been widespread. The companies affected include Best Buy, Capital One, Citi, Dell, Disney, Hilton, Home Shopping Network, JPMorgan Chase, Kroger, Marriott, Ritz-Carlton, Target, TiVo, Verizon and Walgreens. (For a fuller list click here). So many people have received multiple notifications about this single incident that "Epsilon Bingo" cards have sprung up on the Internet (if you collect notifications from each company on the card, you win the game). Although much larger in scope, this breach is similar in nature to those suffered by other email providers in the past six months (click here and here), implying a pattern of attacks by fraudsters.

So why should your business care about this event? The most imminent reason is that it may pose a direct security threat to your organization. It has been widely assumed that the emails stolen from Epsilon were taken to perpetrate phishing attacks, send spam, or infect recipient systems with malware. (Reports of phishing attempts have been reported by affected individuals, but it is somewhat common for fraudsters to wait until the news cycle has cooled before they start exploiting the information.) It is very likely that your

employees provided their corporate email address to one or more of the companies affected, such as to the hotel chains for purposes of booking corporate travel. If they did, that means that your corporate email system may be the recipient of these incoming, harmful emails. In that case, to protect your corporate email and information systems, you may want to ensure that your information security personnel are aware of this incident and have appropriate spam filters and malware detection software in place. You may also want to remind your employees of the following security precautions:

- Do not provide personal information in response to, open attachments from, or click links sent by email messages (even if it appears to be from a company with which you do business). Phishing emails are designed to look like they come from a reputable business. If it is an email you were expecting (for example, a business that has attached an invoice that you expected to receive), this is more likely to be safe.
- Be suspicious of e-mails or phone calls threatening to close your account or take other action if the recipient fails to provide personal information (including user names and passwords).
- Be wary of phone calls from businesses claiming to know you and that ask for personal information to verify your identity, your account or otherwise. You should hang up and call that business at a number you know to be theirs (such as the customer service number on your account statements) to verify the call.
- If you see a significant uptick in spam at your work email account, report it to appropriate information security personnel.

Additional tips are available from the Federal Trade Commission here.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

The second reason you should care about this event is that it emphasizes the need to perform diligence and contract appropriately with **any** service provider handling personal information on behalf of your organization. Historically, businesses have been most concerned with vendors that handle Social Security numbers, credit card numbers, bank account numbers, and other types of data expressly covered by state laws, HIPAA, PCI DSS, etc. Although those types of providers certainly do hold sensitive personal information governed by strict information security requirements (many of which require specific contract provisions be included), other types of providers can be equally troublesome even if the information they hold is less sensitive in nature. The Epsilon breach illustrates, for example, that a provider handling largely public information like name and email address can, nevertheless, cause businesses to suffer significant productivity impacts, sustain reputational damage, and incur legal and PR expense.

Although there are a plethora of appropriate diligence and contracting issues to consider, some of the more crucial items include the nature of the provider's information security program, whether their employees are trained regularly, whether they employ encryption and in what circumstances, their notification to you in the event of a breach, their responsibility to mitigate that event, whether they will securely return or dispose of the information upon conclusion of the services and, of course, the nature and scope of indemnifications they are willing to offer you in exchange for your business. It is also appropriate to ask about (and contractually restrict) your provider's use of subcontractors. Too often, the contracting entity does not know its vendors are using subcontractors until a subcontractor experiences a breach that must be reported.
The moral of this story? It's time to identify all of the contractors that handle your employees' or customers' personal information (any personal information). Conduct diligence and contract appropriately regardless of whether privacy and security laws directly require you to do so. These laws have largely failed to keep pace with emerging

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

threats to personal information and so do not necessarily require your providers to secure your information appropriately. The risks borne out by the Epsilon breach are a good reminder that proactively mitigating risk is just as important as following the letter of the law.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075