

Information Security Breach Disclosure

When, How Much, and To Whom

By M. Scott Koger

ISSA member, Upstate South Carolina, USA Chapter

Join the Discussion
Connect

This article discusses suggested best practices for planning the timing, amount, and appropriate target audience of post-incident disclosure in light of legal, regulatory, and ethical obligations faced by information security professionals in medium to large organizations.

Abstract

How much information should be shared externally after a computer security incident or a data breach? If we ask our friends in the legal profession the answer is usually “it depends.” While that is not a big surprise, it is not much help either. Given the constantly evolving threat landscape and the shifting regulatory and reporting requirements faced by our organizations, how can we proceed with any reasonable degree of confidence? A list of suggested best practices will be given for planning the timing, amount, and appropriate target audience of post-incident disclosure in light of legal, regulatory, and ethical obligations faced by information security professionals in medium-to-large organizations.

For most IT security professionals the issue has come up at least once during their careers – how soon and how much information should be divulged regarding a data breach? The industry in question and the security culture of the organization that experienced the breach will be the most significant factors in determining the answer to this question. Obviously there will be differences in the responses between industry sectors, but there are wide variations between organizations as well. We all have our preconceived notions of what a particular industry’s response will be – financial institutions are conservative, universities are open, etc.

Not the response that one would expect

These preconceptions are based on stereotypes, and as such are frequently incorrect. For instance, the breach notification approach in Higher Ed can be a lot closer to what might be considered a corporate stance than what would be expected from a public agency – examples of this conservative approach have been seen at major universities in Georgia and North Carolina in recent years. After news of the September 2009 UNC Chapel Hill patient data breach, an excerpt from the *Raleigh News Observer* newspaper story about the incident was posted on the *UNC News* site, but no further comment was immediately offered by the university.¹ After a breach in 2007 involving 3000 credit card numbers and other sensitive data, Georgia Tech was relatively tight-lipped as well; at the time the rumor within the Higher Ed information security community at conferences and in online news groups was that the details were withheld as part of a settlement with the payment card industry.

The author of this paper was not able to find any information to support or refute those rumors, and little official comment from Georgia Tech related to this incident was available online other than the initial statement to the press at the time of the incident: “Georgia Tech regrets that this potential loss

¹ “Women’s data breach probed,” *The News & Observer* (Raleigh) October 14, 2009. Retrieved from <http://uncnews.unc.edu/content/view/3001/103>.

The VA was among the first to offer credit monitoring for those directly affected by data breaches in their organization.

of data occurred and will work with the affected individuals to mitigate their exposure,” said James Fetig, associate vice president of Institute Communications and Public Affairs. “Our investigation is continuing, and we apologize for any inconvenience this incident may cause.”²

In direct contrast to the reticent stance taken by these public universities, the Veterans Administration (VA) has been much more forthcoming with the details surrounding the data breaches they have experienced during the last few years, and the VA was among the first to offer credit monitoring for those directly affected by data breaches in their organization.³

What exactly constitutes a breach?

While the various regulations and statutes each have a formal definition, a practical definition emerges. A breach is commonly understood to be some violation of an organization’s information security policies that results in the unintentional exposure of sensitive information – usually personally identifiable information (PII) of customers, students, or patients. The *Internet Security Glossary*, RFC 2828, defines a security incident as follows: “a security-relevant system event in which the system’s security policy is disobeyed or otherwise breached.”⁴ In the event of a data breach, it is up to the organization responsible for that data to determine which, if any, of the many statutes apply to its circumstances. In what jurisdiction was the data housed? Where and how was it collected? For what purpose was it being used: was it part of an educational record, a loan application, or a medical record? Where are the primary residences for those affected? Are any of them in an area covered by one of the state or national breach notification laws? These are just a few of the factors that must be considered.

In the U.S., regulations are usually focused on particular industries. Public utilities, FDIC insured financial institutions, federal government agencies, and their information technology contractors all have their own sets of breach notification requirements based on their industry – usually one, or at most two sets. Higher Ed has the unique situation of crossing multiple regulatory domains, requiring compliance with

overlapping and sometimes contradictory sets of regulations and statutes.

Regulations, statutes, and contractual obligations

The Graham Leach Bliley Act (GLBA)⁵ is intended to regulate organizations involved in credit and lending activities; the Health Information Portability and Accountability Act (HIPAA)⁶ and its extension into the recent HITECH Act⁷ for health care providers; the Fair and Accurate Credit Transactions Act (FACTA) ID Theft Red Flag rules⁸; and the Family Educational Rights and Privacy Act (FERPA)⁹ (U. S. Department of Education) for educational institutions are the most frequently cited regulations that university security offices have to deal with, but the list increases almost daily. Another common compliance criteria is triggered when any contracts or research grants involving data or connections to the information systems of the Department of Defense, DARPA, or federal agencies, which can trigger FIPS and FISMA¹⁰ compliance requirements. There are also contractual obligations like the Payment Card Industry Data Security Standard (PCI-DSS)¹¹ for merchants who accept credit card payments.

Finally there are those laws that follow the individuals across jurisdictional boundaries that all organizations have to be concerned with. Regardless of industry sector – if an organization collects data about individuals, then its information systems probably fall under one of these privacy statutes. California’s SB 1384 and the European Union’s Directive 95/46/EC protect their citizens’ personally identifiable information, *regardless of where the breach actually occurred*. For some privacy laws, it depends on where the data was collected; for others, the specifics or the geographic location where the data was stored determines applicability, and for others the primary concern is to clearly identify where the data was used when one attempts to determine which law applies. At the time of this writing all but six states within the U.S. and

2 “Hackers hit Georgia Tech and Steal personal info,” *The Atlanta Business Chronicle* (2007, February 21). Retrieved from <http://atlanta.bizjournals.com/atlanta/stories/2007/02/19/daily20.html>.

3 “Secretary Nicholson Announces VA to Provide Free Credit Monitoring” [Press release], Department of Veterans Affairs. (2006, June 21). Retrieved from <http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1143>.

4 R. Shirey, “Internet Security Glossary,” Internet Engineering Task Force (May 2000). RFC 2828. Retrieved from <http://www.ietf.org/rfc/rfc2828.txt>.

5 “The Gramm-Leach Bliley Act,” Federal Trade Commission. Retrieved from <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>.

6 “The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule,” Office of Civil Rights, Department of Health and Human Services. Retrieved from <http://www.hhs.gov/ocr/privacy/index.html>.

7 Majority Staff of the Committees on Energy and Commerce, Ways and Means, and Science and Technology. United States House of Representatives. (2009, January 16). Title IV – Health Information Technology for Economic and Clinical Health Act Health Information Technology for Economic and Clinical Health Act or HITECH Act. Retrieved from <http://waysandmeans.house.gov/media/pdf/110/hit2.pdf>.

8 “Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy” [Press release], Office of Public Affairs, Federal Trade Commission. (2007, October 31). Retrieved from <http://www.ftc.gov/opa/2007/10/redflag.shtm>.

9 “Family Educational Rights and Privacy Act (FERPA),” United States Department of Education. (2009, June 16). Retrieved from <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

10 “Federal Information Security Management Act of 2002,” 44 U.S.C. § 3541 (2002).

11 “Welcome to the PCI Security Standards Council,” PCI Security Standards Council. Retrieved from <https://www.pcisecuritystandards.org>.

...now “covered entities” must notify major media outlets and the director of Health and Human Services “promptly” in cases...

some 51 nations have separate privacy laws.¹² Usually all of this dizzying complexity has to be dealt with while the people responsible for the IT infrastructure are still trying to determine the scope of the compromise – was it a single server that was compromised, a lost laptop, an intercepted communication? Was the data encrypted? Usually the information security or compliance office does not have the luxury of waiting until they have a complete picture of what happened before one of these reporting requirements kicks in.

What triggers a notification?

The various regulations and statutes have their own event triggers for notification, usually having to do with the number of individuals potentially impacted. These event triggers can and do change even within existing statutes. For instance HIPPA compliance has changed significantly after the passage of the HITECH Act of 2009. In addition to notifying all those whose information had been exposed, now “covered entities” must notify major media outlets and the director of Health and Human Services “promptly” in cases where more than 500 individuals are affected. In cases involving fewer than 500 individuals, the event must be reported to each individual whose information was directly involved and as part of an annual report to the director of HHS. Another significant change with the HITECH Act is that now these breach notification requirements extend to “business associates” who are required to notify the covered entity of breach events “at or by the business associate.”¹³

In the case of the GLBA, breach notification requirements refer to a breach notification response program; while there is a direct notification requirement to the relevant regulatory agencies, there is no direct customer notification requirement. Commonly, the only notification a customer receives after an information compromise is a new credit card in the mail with a new account number.

“At a minimum, an institution’s response program should contain procedures for: (1) assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused; (2) notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or

use of sensitive customer information ... (3) immediately notifying law enforcement in situations involving federal criminal violations requiring immediate attention; (4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, ... (5) notifying customers when warranted.”¹⁴

For those who accept credit card payments, compliance with the PCI-DSS is a contractual obligation. PCI-DSS does not directly include individual breach notifications; those activities are covered under GLBA guidelines. Rather the notification requirements discussed as part of PCI-DSS are focused on notification of the card issuer and card processors.¹⁵

Who gets notified?

Once an incident has been identified, and a determination of which law or regulation has been violated, the response team will be able to determine what the formal reporting requirements will be. It is crucial that the IT staff engage the appropriate legal counsel early in this process. The lawyers responsible for the organization need to determine whom to contact: local, state, federal, and possibly even international law enforcement; the relevant federal regulatory agencies – each has its own reporting criteria and requirements. Initial attention should be focused on maintaining the chain of custody and following the documented computer security incident response team (CSIRT) procedures while maintaining an audit trail. These steps will ensure that any legal obligations are being met, and providing an audit trail can later establish due care and diligence on the part of the incident responders.

After the legal requirements have been met, the question of ethical obligations must be addressed. Just what are our ethical obligations? Again, the interpretation will vary by industry and by institution, but as information security professionals we have an obligation to shape those decisions based on criteria that should span industries and organizational cultures. Many professional associations and certification bodies directly address the issue of ethics, and as members of these organizations or holders of these certifications we are bound by these statements of principal. For publicly traded companies and privately held corporations, cases like Heartland Payment Systems indicate that transparency and openness will be rewarded in the marketplace. The predictions of the demise of Heartland have not been borne out by their share price in the medium- to long-term, despite the understandable volatility after the initial reporting of their data breaches. For public institutions the open approach taken by the Veterans Administration seems to be much more well regarded by the public, the media, and information security

12 S. Berinato, “CSO Disclosure Series | Data Breach Notification Laws, State by State,” CSO Magazine (2008, July 28). Retrieved from http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_by_State.

13 “HITECH Breach Notification Interim Final Rule,” Office of Civil Rights, United States Department of Health and Human Services. Retrieved from <http://www.hhs.gov/ocr/privacy/hippa/understanding/coveredentities/breachnotificationifr.html>.

14 “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. 68 FR 47954,” retrieved from <http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf>.

15 “About the PCI Data Security Standard (PCI DSS),” PCI Security Standards Council, retrieved from https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Ultimately those who were directly impacted deserve to know what happened.

industry professionals than the markedly less transparent path followed by the Department of Energy or certain public universities.

(ISC)² and the ISSA both have clearly stated codes of ethics, as well as the governing body for the Internet, the Internet Engineering Task force, which also spells out the ethical obligations of users of the Web in RFC 1087. All three documents reflect the character of the organizations which created them in their specifics, but they all share common elements – to honestly and diligently discharge our obligation to protect the confidentiality, integrity, and availability of the informational assets entrusted to our care, to develop and promote information security best practices, and to treat the privacy of the individual with all possible care and diligence.¹⁶

How much to share?

Once the legal obligations are taken care of, the ethical issues need to be addressed. After we determine whom we need to notify based on ethical considerations, the next issue is how much detail do we really need to share? As information security professionals the last thing we want to do is to provide insight into our defenses for the next villain, or to let the bad guys know which specific tools and techniques were effective and why. At the same time, as a community of information security practitioners, ideally we would be able to share lessons learned, discuss emerging threats, collaborate on possible response approaches, etc. Ultimately those who were directly impacted deserve to know what happened. Javelin Research has just completed a study which shows that individuals who have received a notification letter indicating that their personally identifiable information was involved in a corporate data breach are four times more likely to be the victim of identity theft. The study included data across multiple years, including breach incidents as recent as 2009.¹⁷ Was their PII accessed when a server was breached? Was an unencrypted laptop left in a cab? Was it a poorly written web application? While internal understanding of the details and nature of the breach are important for developing defenses against future attacks, is it necessary or desirable to share those details externally?

Doing the right thing

The behavior of Heartland Payment Systems executives may be the best example of how to handle these decisions. At the time of this writing, the Heartland Payment Systems incident is potentially the largest and is thus far the most openly discussed data breach to date. Company officials still maintain that the breach announcement and the Obama inauguration just happened to coincide, and that it was not a deliberate effort on their part to bury the item in the news cycle.¹⁸ They maintain that the timing of their announcement represented the first opportunity that they had to call a press conference after consulting with their board, internal counsel, law enforcement, and other relevant entities. Since the incident Bob Carr, CEO of Heartland, has hit the speaking circuit to share lessons learned and to advocate for refinements to the PCI-DSS, particularly in the area of “end-to-end” encryption. The transparency and proactive approach of Heartland’s management may well have saved the company. As a publicly traded company whose entire business is built upon the perceived security and accuracy of processing transactional data for merchants and credit card issuers, most industry analyst had openly questioned the survivability of the company after their January 20, 2009 announcement of a data breach of unknown proportions.¹⁹

The most readily available metric, the share price of Heartland common stock, serves as a ready indicator of how the markets have responded to the incident and the company’s actions since. Before the announcement, Heartland had been trading at \$15.16 per share. Immediately after the breach announcement it dropped to \$8.18. A few weeks later, as part of their annual SEC filings, Heartland included a statement to the fact that they did not know the scope of the incident and that they were unsure just how long the breach had existed before it was detected. This was true in spite of the fact that just before the breach Heartland had been re-certified as compliant with PCI-DSS guidelines for the sixth straight year. No one could say at that point how long the problem had existed. This uncertainty pushed the share price down to \$3.43. On March 14, 2009 Heartland was delisted on the stock exchange but by April 30 it was re-certified as a card processor and re-listed on the stock exchanges. As of this writing, the share price is at \$10.43, but had been as high as \$14 per share.

In October of 2009, Mr. Carr spoke to the information security press and security practitioners as part of the 2009 SC World Congress.²⁰ During his presentation he shared details of the time line, some of the particulars of the attack,

16 “ISSA Code of Ethics,” Information Systems Security Association, retrieved from <http://www.issa.org/Association/Code-of-Ethics.html>; “(ISC)² Code of Ethics,” International Information System Security Certification Consortium (ISC)², retrieved from <http://www.isc2.org/ethics/default.aspx>; “Ethics and the Internet,” Network Working Group, Internet Activities Board, RFC 1087, retrieved from <http://www.ietf.org/rfc/rfc1087.txt>.

17 T. Wilson, “Corporate Breaches Increase Chances of Consumer ID Theft, Study Says,” Dark Reading (2009, November 4), retrieved from http://www.darkreading.com/security/privacy/showArticle.jhtml?article=221600348&cid=n_DR_WEEKLY_H.

18 B. Acohindo, “Hackers breach Heartland Payment credit card system,” *USA Today* (2009, January 23). Retrieved from http://www.usatoday.com/money/perfil/credit/2009-01-20-heartland-credit-card-security-breach_N.htm.

19 E. Mills, “Payment processor Heartland reports breach.” *Cnet News* (2009, January 20). Retrieved from http://news.cnet.com/8301-1009_3-10146275-83.html.

20 “Securing the Cloud,” SC Magazine eConference and Expo, *SC Magazine* (2009, November 10). Retrieved from <http://events.unisfair.com/microsite24.jsp?eid=474&seid=173&language-code=en&country-code=US&logon-form-state=0&login-return-state=1&code=Direct%20Access>.

the company's actions since the announcement, and suggestions to other organizations and the payment card industry in particular. Among the numerous recommendations was a call for a framework for anonymous sharing of information about the methods and means used to attack information assets between the institutions and most importantly among those charged with certifying our information environments as secure or charged with post-event investigations.

Within the payment card industry there is a finite list of approved forensic examiners; only seven companies are deemed Qualified Incident Response Assessors (QIRAs) and are approved for use by the payment card industry. Until the recent formation of the Payment Processor Information Sharing Council (PPISC)²¹ there was no mechanism for these examiners or the institutions they review to share information about the methods and means by which they are being attacked. The SQL injection used against Heartland was part of an attack used against at least 300 companies, many of whom had been review by the same QIRAs, but no details of the attacks were shared, and the individual examiners had to start their analysis from scratch with each engagement. It would be like an antivirus program having to develop a signature library from scratch each time a computer was started – the least efficient possible model, and the most likely to produce false negatives.

Emerging best practice

Based on the actions of Heartland Payment Systems, the Veterans Administration, and others who are providing leadership in the area of breach disclosure, there is an emerging set of best practices which were codified into a simple list by *SC Magazine* in a recent article:

Be prepared: Breach checklist

Before a breach happens...

- **Write a policy** – This should detail how an organization would respond in the event of a breach.
- **Teach end-users** – Do not just teach employees how to avoid threats, but also educate them on how to distinguish when a breach has occurred – and whom they should tell about it.
- **Management must get it** – Business leaders should recognize the risk potential of a breach to a company's bottom line.
- **Prepare for federal legislation** – It's coming. States should ensure they have their IT procedures in place so they are not rushing to fix any holes when Congress finally passes a law. Use the state notification laws as guidance.

And after...

- **Do not rush to judgment** – Depending on what was exposed, notification may not be required. But if it is,

21 "Welcome To The Payments Processing Information Sharing Council," Financial Services Information Sharing and Analysis Center (2009). Retrieved from <http://www.ppisc.com>.

The only group that is not served by disclosure is the attackers.

do not try to keep the situation quiet. Fines could result.

- **Tap into a team of experts** – Because a data-loss incident is wide ranging in its effect, a representative from each business division should be tapped. That includes legal, IT, and human resources.
- **Care about the customer** – The most successful organizations have been as up front as possible with their clients after an incident, offering remedies such as free credit monitoring and following up with them months later.
- **Learn from your mistakes** – If they didn't have effective security in place to start, organizations should use a breach as an opportunity to improve their posture."²²

Conclusion

As the old saying goes – sunlight is the best disinfectant. These pre- and post- breach recommendations are straightforward, as are the ethical guidelines provided by the IETF, ISSA, and (ISC)². The cases of Heartland and the VA demonstrate that transparency, the sharing of lessons learned, and a customer-centric focus are not only a theoretical ideal, but are sustainable in the long-term. Shortsighted efforts to "keep a lid on it" only help to provide cover for those who are attacking our information assets. For those of us in the public sector, these recommendations may be easier to implement, since most states have a sunshine law or public records law that would apply to the public disclosure of a breach. Even for publicly traded organizations that have to be ever mindful of preserving shareholder value, the Heartland Payment Systems example demonstrates that doing the right thing can protect the long-term interest of all the legitimate stakeholders. The only group that is not served by disclosure is the attackers, and they have benefited from our collective silence for far too long.

About the Author

M. Scott Koger currently serves as the security analyst for the Information Technology group at Western Carolina University (WCU) in Cullowhee, North Carolina. Prior to joining WCU, he served as the systems development project lead for the Sewerage and Water Board of New Orleans during the eventful months following Hurricane Katrina in 2005. He may be reached at m.scott.koger@gmail.com.



22 D. Kaplin, "Data breach defense: Response ability," *SC Magazine* (2009, July 1). Retrieved from <http://www.scmagazine.com/Data-breach-defense-Response-ability/article/139460>.