PCI Data Breach Preparedness – How To Prevent Your Organization From Becoming the Next Data Breach Headline

Presented by the Bryan Cave Payments Team and
Special Guest Speaker Andi Baritchi

Agenda

- Introduction - Judie Rinearson (NY)
- Reducing Business Risk – Jena Valdetero (CH)
- Minimizing Exposure from a PCI Breach – Courtney Stout (DC)
- On PCI Compliance vs. Breach Risk – Andi Baritchi (Verizon)
- Moving Beyond Legal Documents – Linda Odom (DC)
- Conclusion – Linda Odom (DC)

Can you prevent a breach?

No more than you can prevent theft…vandalism… violence…or any other type of crime…

There is a misperception that data breaches can be prevented if an organization invests enough money, hires the right people, implements the right technology.

The truth is that you can no more prevent a data breach than you can prevent a robbery. Some aspects are within your organization's control; others are not.

Can you help prevent being a headline?

BRYAN CAVE

Reducing Business Risk

JENA VALDETERO (CHICAGO)

BRYAN CAVE

What factors influence the impact a breach will have on an organization?

Outside of Organization's Control

- The size of the breach.
- The type of data breached.

Within Organization's Control

- How quickly an organization identifies the breach.
- How quickly an organization investigates the breach.
- How quickly an organization remediates the breach.
- What an organization communicates to partners.
- What an organization communicates to impacted individuals.
- What an organization communicates to regulators.
- What an organization communicates to the media.
- Complying with contractual obligations.
- Complying with regulatory obligations.

What factors influence the impact a breach will have on an organization?

How do you prepare your organization to handle these?

Within Organization's Control

- How quickly an organization identifies the breach.
- How quickly an organization investigates the breach.
- How quickly an organization remediates the breach.
- What an organization communicates to partners.
- What an organization communicates to impacted individuals.
- What an organization communicates to regulators.
- What an organization communicates to the media.
- Complying with contractual obligations.
- Complying with regulatory obligations.

Evaluating the level of the legal department's preparation for a breach

The top 10 legal documents to review

1. Data security representations / privacy policies.
2. Agreements with subcontractors that hold your data.
3. Data breach incident response plan.
4. Whistleblower policy.
5. Agreements with breach response providers.
6. Payment processing agreement (credit / debit / prepaid card).
7. Reports on compliance (credit / debit / prepaid card).
8. Agreement with independent forensic investigator.
9. Agreement with PFI forensic investigator (credit / debit / prepaid card).
10. Cyber-insurance.

1. Data security representations

Where you find them:

- Internet privacy policy.
- Marketing material to other organizations or consumers.
- Contracts with other organizations or consumers.

What should you be concerned about:

- Language that suggests “guaranteed” security.
- Language that suggests encryption in all situations.
- Language that suggests a standard of care which is higher than that which is legally required.

What to look for:

- Consistent messaging concerning the organization’s level of security.
- Any exceptions to that messaging are understood and appropriately recorded within the organization.
- Representations of specific security technology.
- Data breach notification provision that permits flexibility.

2. Agreements with subcontractors (vendors) that hold your data

Where you find them:

- HR / accounting / processing outsourcing agreements.
- Marketing outsourcing agreements.
- Partnerships and joint ventures.

What should you be concerned about:

- Vendor has adequate security.
- Vendor will notify you if something goes wrong.
- Vendor will pay for the cost of notifying individuals if they have a breach.
- Vendor has little, or no, liability.
- Vendor is effectively judgment proof (start-ups / holding company).

What to look for:

- Clear representation concerning the level of security that is applied to the data. According to one study, 70% of companies now require third party vendors to abide by standard / model security contract terms.*
- Level of security represented “fits” the sensitivity of the data that you provide to the vendor.
- Data breach notification obligation.
- Agreement that they will pay cost to notify the impacted individuals and / or cost for providing credit monitoring and other related services.
- Exceptions from any liability cap.
- Cyber-insurance.

* Ponemon Institute, "Is your company ready for a big data breach?” (Sept. 2014) at 8.

3. Data breach incident response plan

Where you find them:

- 26% - Number of companies that don't have a written incident response plan.*
- Some organizations' IT departments may have developed a plan in a vacuum.

* Ponemon Institute, "Is your company ready for a big data breach?" (Sept. 2014) at 8.

Data breach incident response plan (cont'd)

What should you be concerned about:

- 47% - number of companies that reported that they weren't sure if their plan was effective, or affirmatively felt that their plan was not effective.*
- 78% - number of companies that reported that their plan has either never been reviewed or updated, or there is no set schedule for conducting such a review.
- Plan is not well understood by organization.*
- Organization is not trained on the plan.
- If a breach occurs, plan will be overlooked or ignored.
- Plan creates obligations or timelines that may not "fit" your organization or be realistic.

* Ponemon Institute, "Is your company ready for a big data breach?" (Sept. 2014) at 8.

Data breach incident response plan (cont'd)

What to look for:

1. Assigns specific person or group to lead an investigation. (21% have no designated person)*
2. Provides a clear internal escalation plan for information about an incident.
3. Discusses the need for preserving evidence, and provides resources for accomplishing that.
4. Incorporates Legal where appropriate to preserve privilege.
5. Includes an external communications plan that takes into account the organization's contractual and regulatory obligations.
6. Includes contact information for internal resources.
7. Includes contact information for pre-approved external resources.
8. Includes communications plan for dealing with media.
9. Is reviewed periodically (e.g., annually).

* Ponemon Institute, "Is your company ready for a big data breach?" (Sept. 2014) at 8.

4. Whistleblower policy

Where you find them:

- Employee handbook
- Sharepoint / Intranet site
- HR
- Privacy policy

What should you be concerned about:

- If organization does not have an internal policy, employees may be discouraged from early reporting of a data security incident.
- If organization does not have an external point of contact, consumers report a data security incident to a third party (press or government), instead of the organization.

What to look for:

- Employee-facing policy is broadly worded to include the reporting of data-related issues.
- Employee-facing policy includes a mechanism for anonymous reporting.
- Employee-facing policy accurately describes level of confidentiality afforded.
- Consumer-facing policy provides multiple points of contact (e.g., email, telephone, mail).

Minimizing Exposure From a PCI Breach

COURTNEY STOUT (DC)

BRYAN CAVE

5. Agreements with breach response providers

What they are:

- Mailing notification letters.
- Call-center support.
- Credit monitoring.
- Identity restoration services.
- Identity theft insurance.

What should you be concerned about:

- Service provider has not had its own data security related problems.
- Service providers do not have a history of consumer protection related problems that might “re-victimize” the people that you are trying to notify, or further jeopardize your reputation.
- Service providers apply adequate security to the data that you provide to them.

What to look for:

- No exclusivity within service provider agreement.
- Data provided to them is not retained for other purposes (e.g., marketing).
- Service provider is prevented from marketing or upselling.
- Indemnification for unfair or deceptive practices by service providers.
- No onerous liability caps.
- Copy of any materials that would be provided to the impacted individual (e.g., insurance policies).

6. Payment processing agreements (network branded prepaid / debit card)

Where you find them:

- Legal? Finance? Accounting?
- There should be an agreement with (a) your merchant bank and / or (b) a third party payment processor.
- The agreements almost always incorporate by reference separate operating “rules.”

What should you be concerned about:

- Obligation to notify your processor in the event of a network branded card related breach.
- Liability for any “fines or assessments.”
- Bank / processor does not have the same level of responsibility as does your organization.
- You don’t have all amendments to the agreement.
- You don’t have all incorporated-by-reference documents.

What to look for:

- Is the organization liable for “fines,” “assessments,” “chargebacks,” or “recoveries” imposed by the credit card company on your bank / processor?
- Do you have a right to contest those fines / assessments / penalties?
- Is there any cap to your organization’s liability?
- Is the bank / processor reciprocally liable to you if a breach happens on their system?
- How quickly do you need to notify them of a suspected incident?
- To whom is notice given?

BRYAN CAVE

7. Reports on compliance (network branded card)

What they are:

- Depending on how many network branded card transactions you process, the credit card companies require different levels of auditing for “PCI” compliance (called “Reports on Compliance” or “ROCs”).

Where you would find them:

- Sometimes these are housed in Legal; sometimes in IT.

What should you be concerned about:

- If a ROC does not exist, but should, based upon the PCI rules.
- If a ROC indicates an area of deficiency or non-compliance which is exploited by a hacker, it may be used as evidence to establish the organization’s “knowledge” of deficient security.

What to look for:

- What “level” merchant are you (Level 1, Level 2, Level 3 or Level 4)?
- Who conducted your ROC assessment?
- Do you have a current ROC assessment (as required by your level)?
- Are there any areas of “non-compliance” noted?
- How long has an issue been noted as “non-compliant?” Has it been remedied?

8. Agreement with independent forensic investigator

What it is:

- If you have a security incident, the organization may require the assistance of a forensic specialist to help identify the scope and nature of the incident, and remediate any vulnerability.

Where you would find them:

- Sometimes these are housed in Legal, but more often they are housed in IT.
- Oftentimes a written service agreement may not exist.

What should you be concerned about:

- The level of security that your investigator applies to data that it takes out of your environment.
- Maintaining attorney client privilege if appropriate.
- Guaranteed access to their services.

What to look for:

- Strong representations of security for any data that is taken from your environment into their environment.
- Indemnification for any breach of their security.
- Notification obligation for any breach of their security.

9. Agreement with PFI forensic investigator (network branded card)

What it is:

- The operating rules for VISA, MC, AMEX and Discover require that an organization retain a forensic investigator that is certified by the Payment Card Industry if you experience a network branded card related data breach. These are referred to as “PCI” or “Payment Card Industry Forensic Investigators.”

Where you would find the contract:

- If one exists, it may be housed in Legal, but more often they are housed in IT.

What should you be concerned about:

- PFI’s are required to report their findings to the credit card brands; as a result, there is no claim of attorney client privilege.
- PFI findings are typically used by the credit card brands to issue fines, penalties or assessments.

What to look for:

- Strong representations of security for any data that is taken from your environment into their environment.
- Indemnification for any breach of their security.
- Notification obligation for any breach of their security.
- Strong representations of confidentiality (at least to the extent consistent with the PCI-PFI Rules).

On PCI Compliance vs. Breach Risk

ANDI BARITCHI (VERIZON)

Andi Baritchi

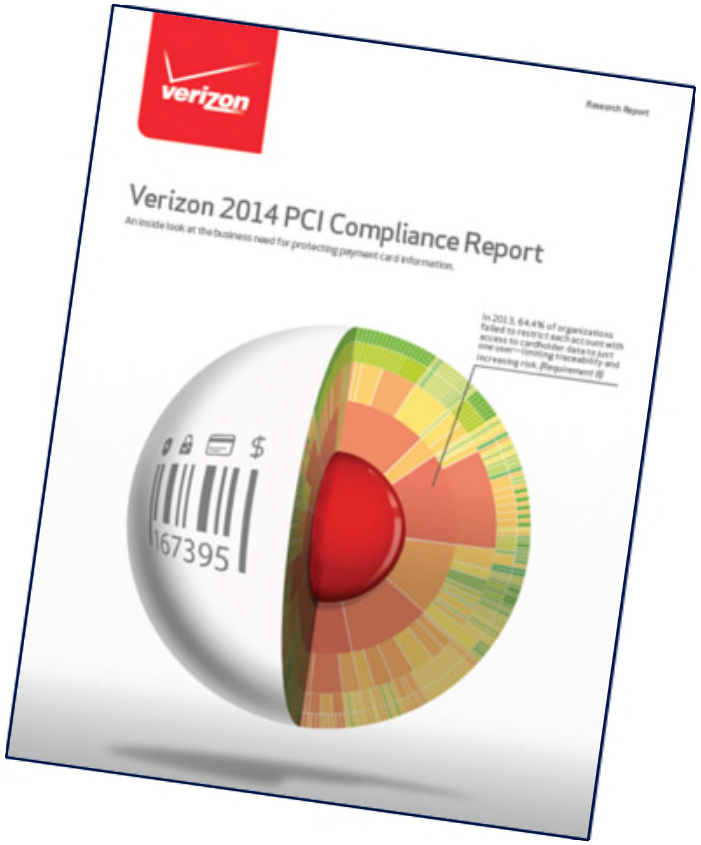
Andi Baritchi is the Global Managing Principal in charge of Verizon's PCI Practice. He is a recognized expert in cybersecurity, payment security and regulatory compliance.

Andi Baritchi
Global Managing Principal
PCI Consulting Services
Verizon Enterprise Solutions
andi.baritchi@verizon.com
+1.972.489.4289

Verizon 2014 PCI Compliance Report

Based on a unique data set — the only report of its kind in the world

- 2014 (3rd edition)
- PCI v2.0 assessments from 2011 – 2013
- 500 PCI Assessments across 250 organizations
- ~300 control tests per assessment
- ~150,000 controls analyzed



2015 Edition Coming February 23!

http://www.verizonenterprise.com/pcireport/

What are the non-breached companies doing differently?

BRYAN CAVE

PCI compliance of QSA vs PFI customers