Risk. Repercussions. Reputations.

Data Protection and Reputation Management for Today's Business Enterprise

A publication of: vehr communications

Index

Published April 2015

Introduction

To succeed in business today, corporations need customers to buy and recommend their products and services, suppliers to support the enterprise and employees to deliver on the company strategy. They may also need regulators to provide a license to operate or industry analysts to recommend their stock. And, they likely will need media to report on company successes, whether online, broadcast or print.

But, what do customers, suppliers, employees, regulators, politicians, reporters, bloggers, and others need from today's corporate enterprise?

TRUST

They need to trust that the business will deliver on its promise to them and their customers.

They need to trust in the reputation of the company and its product or services.

They need to trust the leader to do what he or she says they'll do.

A company's reputation is based on trust. Trust is at the core of the value exchange; it is the promise between corporation and customer and is often considered the essence of the company's brand.

For today's enterprise, data breaches are as real and potentially damaging as any risk ever faced by corporations. The repercussions of a breach are far from settled in modern case law and the regulatory environment is changing as you are reading this document.

A company's reputation – its promise to its customer – is still the company's most valuable asset. In the event of a data breach, a company's reputation is at risk.

THE VALUE OF REPUTATION

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

Warren Buffett,
CEO, Berkshire Hathaway

This eBook is intended to help its reader on three levels:

- **Risk:** Understand the risk companies face when collecting and managing confidential corporate information and personally identifiable data and how to reduce that risk.

  Sandy Hughes, former Global Privacy Officer at Procter & Gamble, challenges readers to consider "Privacy by Design" for all businesses collecting personally identifiable information. Put differently, to think first before collecting data, only gather what you need and have a plan for how to protect it before it is in your possession.

- **Repercussions:** Be aware of the shifting legal landscape and the general "unsettledness" of current law pertaining to the ramifications of a corporate data breach and to understand how the government is going to be paying more attention to this area of modern commerce.

  Jack Greiner, who leads the law firm Graydon Head's Communications and Industry Group and represents various media organizations, discusses how the current lack of regulation in the area of data breaches and data protection means there are few "safe harbors" for today's business enterprise, and that's not necessarily a good thing. He also discusses how, and how rapidly, regulation in this area is evolving.

- **Reputations:** Realize the importance of being prepared when a data breach occurs – because it will – so that the hard-earned and well-deserved trust of your customer can be preserved.

  Nick Vehr, President and Founder of Vehr Communications, a Cincinnati-based strategic communications firm with a global presence, shares how enlightened businesses have a plan to protect and preserve their hard-earned reputation from the fall-out certain to follow the data breach that is bound to happen.

Cybersecurity is part of doing business in today's connected world. Whether internal or contracted IT support, whether specialized insurance or data security specialists, whether new and changing business protocols to new employee policies, data privacy and security is fast becoming standard operating procedure for businesses large and small.

You cannot afford to be left behind or to be a step behind those who care little for the trust you have developed with your mission-critical audiences.

About the authors

This publication has evolved from a collaboration of three experienced professionals with expertise in data privacy, communications law and reputation management. Those professionals are:

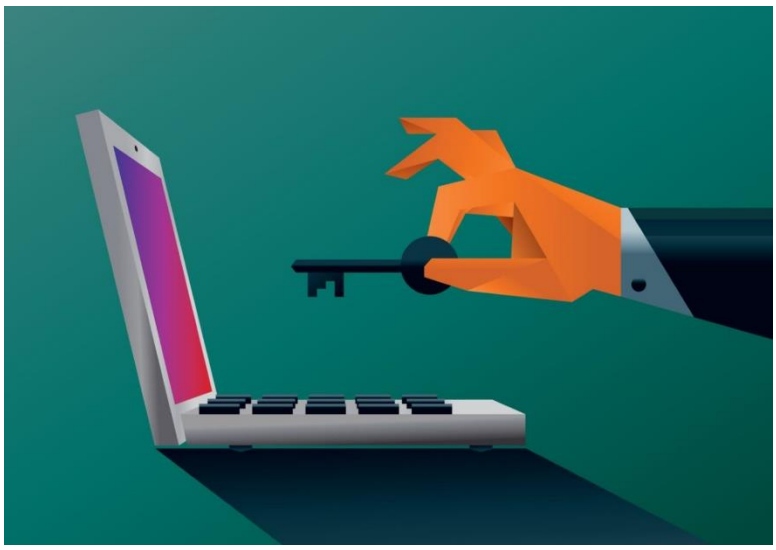
Sandra R. (Sandy) Hughes: Sandy retired in 2012 after a 25+ years with Procter & Gamble, the world's largest consumer products company. Sandy served as Global Privacy Executive and lead global programs in Ethics & Compliance, Information Governance, and Competitive Intelligence. She was recognized by the International Association of Privacy Professionals (IAPP) with the Vanguard Award (best Corporate Practitioner) and the Executive Women's Forum for Risk Management, Information Security and Privacy (Woman of Influence, Lifetime Achievement Award). Sandy is a Business Strategy and Executive Coach, serves on the corporate board for Future of Privacy Forum and advisory boards for International Privacy Day and Executive Women's forum.

Jack Greiner: Jack is a partner at Graydon Head. He is a lifelong Cincinnati resident and a graduate of the University of Notre Dame Law School. Jack heads up Graydon Head's Media Communications and Information Industry Group. Jack has practiced in the field of communications law for nearly 20 years, and his clients have included The Cincinnati Enquirer, Courthouse News, ESPN and Vogue Magazine. Jack writes a column for The Cincinnati Enquirer Business section called "Strictly Legal." In addition, Jack is an adjunct professor at the University of Cincinnati Law School and maintains a blog – "Jack Out of the Box" – that comments regularly on data privacy.

Nicholas J. Vehr: In 2007, Nick founded Vehr Communications, now one of Cincinnati's leading strategic communications firm and a partner in IPREX, a $270 million global communication network of more than 75 firms in 33 countries. Nick was an elected member of Cincinnati City Council and was appointed to various boards, task forces and commissions by the Mayor of Cincinnati and Governor of Ohio. Active in nonprofit service, Nick served as Chair of the Cincinnati USA Convention & Visitors Bureau and was the volunteer managing director of the 2012 World Choir Games. While Vehr Communications specializes in many areas, it is especially recognized for its work in issues management and crisis communications.

Risk … consider "Privacy by Design."

By: Sandra Hughes



Back when the Internet was young, a privacy policy and a compliance program were enough to minimize the risk of regulators bringing enforcement action, customers filing civil lawsuits, and/or hackers causing data breaches.

But our rapidly developing information society and the astronomical possibilities of advanced technology make it nearly impossible to succeed in the marketplace without capturing some type of personal information.

Today, savvy CEOs know that their creative and engineering employees must practice Privacy by Design.

What is "Privacy by Design"

Privacy by Design is a user-centric approach to an initiative, application and/or systems development which takes privacy into account from concept throughout the whole lifecycle of development. See (https://www.privacybydesign.ca/).

To illustrate, consider how selling something as innocuous as a "Window" evolves over time.

a. A Web site provides information. It recognizes the computer every time it clicks, along with other websites it has visited.

b. Email capability is introduced. Address lists you purchased or received from interactions with customers allow you to deliver advertising straight to customers. Now you know specifically who is receiving your messages and a bit about their community based on how they forward your messages.

c. Online purchase capability adds convenience. Customer service interaction, combined with social media chat and online reviews, creates a relationship between you and your customers but also an indirect relationship with their community (perhaps not intentionally). Behind the scenes, this is the 'mother load' of information: Personal and financial information can be matched with behaviors to not only know "who" uses your Window (and when why and how they use it) but also "who else" uses it (and when why and how they use it).

d. Mobility Apps provide convenience. They also add the "where" dimension about your customers, and even more data about their habits and practices.

e. Sensors introduced into your Window design simplify and improve your customers' lives when they communicate directly with your HVAC system to control air quality or electricity expense, given your customers' pre-set criteria. This brings you up close and truly personal with your customers' lives.

Now, instead of "Window" in this scenario, substitute something else like a personal fitness monitor, toilet, car, jewelry, greeting card, or even something you ingest like a sensor in a pizza!

In each step, the information collected, processed, retained, analyzed, dispersed, shared and managed expands exponentially. And the number of people and third parties who touch that or could come in contact with that information does as well. This increases the likelihood for human error, technical holes and misuse contributing to the possibility of data breach, deceptive claims and fraud.

User mistrust, and the perception of surveillance and "creepiness" – all on top of the risks of government fines and civil lawsuits, can damage your brand and company reputation – maybe even the CEO personally.

Companies must give deep thought and ask questions about how personal information of their customers (and employees) will be protected from end-to-end and hand-to-hand. Companies also need solutions which incorporate the desired level of privacy for each customer. (Just like color and fit, every customer has a different desire for privacy.)

This is Privacy by Design. In the near future, your customers will demand it. Regulators in the United States and Europe will require it.

Privacy by Design – 7 Foundational Principles

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles.

1. *Proactive* not Reactive:

The *Privacy by Design* (*PbD*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the *Default Setting:*

We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. Privacy *Embedded* into Design:

Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – *Positive-Sum*, not Zero-Sum:

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security and demonstrates that it is possible to have both.

5. End-to-End Security – *Full Lifecycle Protection:*

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data is securely destroyed in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. *Visibility* and *Transparency* – Keep it *Open:*

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. *Respect* for User Privacy – Keep it *User-Centric:*

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

(Source: https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/)

Repercussions … a regulatory vacuum gets filled and what it means for you.

By: Jack Greiner

In the world of privacy law, business owners may find the absence of regulation more problematic than thousands of pages on the topic in the Code of Federal Regulations. And since that sounds counterintuitive at very least, it bears some explaining.

There are federal privacy regulations that impact any number of businesses across the country. The two privacy regulatory schemes that come to mind almost immediately are HIPAA in the world of health care and the Graham Leach Bliley Act in the world of banking and finance.

So if you're a hospital CEO or bank president, you know a lot about detailed regulations and you probably have compliance people either on your payroll or on your speed dial. Or both.

But what if you own a pizza company or a window business, or any operation not covered by HIPAA or GLB? You probably collect and store personally identifiable information. So are you off the hook? Short answer? No.

The Federal Trade Commission (FTC) has stepped into this regulatory vacuum and has gotten very active in recent years. The FTC is able to do this, it contends, under the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices." That language is the extent of any written regulation on the topic. But relying on that simple language, the FTC has prosecuted a number of enforcement actions involving car dealers, restaurants and market research companies. In the two instances where FTC targets have challenged the FTC's authority to proceed, the federal courts have sided with the Commission.

And what is the problem exactly with the FTC looking into a company's privacy practices?

Well, the remedy that the FTC extracts, often via a "settlement" can be pretty onerous. Resolution of a FTC complaint typically involves an order compelling the company to cease and desist from whatever practice the FTC doesn't like. But it likely also includes a monetary penalty. Penalties have ranged from one thousand dollars to 35 million dollars. The company will likely be required to delete whatever data it collected via its "unfair" or "deceptive" practice and provide consumers with notice of the problem and their remediation rights. The FTC may also require the company to develop a comprehensive program to address the issue, and require assessments by independent professionals (on the company's dime). And the FTC will likely retain the right to monitor for 20 years.

And so what draws the FTC's attention? According to the FTC, companies have allegedly engaged in "deceptive acts" when their actions haven't matched their promises. Companies that copy a privacy policy off the Internet without ensuring the policy aligns with their actual practices are at risk. And companies that decide to make unilateral changes to existing privacy policies may land on the FTC's radar.

Even those companies that limit their promises may not be risk free. The FTC has increasingly found that companies that don't use state of the art privacy protocols may be engaging in "unfair practices." Companies whose procedures for encrypting or disposing of data, for example aren't up to par, may have a problem. And that "problem" could take the form of a consent decree that requires FTC monitoring for over 20 years.

No regulation means no "safe harbors" and no clear guidance. But clearly no regulation does not mean no teeth. And with the attention on this issue generated by the breaches at Target, Home Depot and more recently Anthem, there is little doubt that the government's scrutiny will only increase.

The Target Breach, by the Numbers

40 million	The number of credit and debit cards thieves stole from Target between Nov. 27 and Dec. 15, 2013.
70 million	The number of records stolen that included the name, address, email address and phone number of Target shoppers.
46	The percentage drop in profits at Target in the fourth quarter of 2013, compared with the year before.
200 million	Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards — about half of the total stolen in the Target breach.
100 million	The number of dollars Target says it will spend upgrading its payment terminals to support Chip-and-PIN enabled cards.
0	The number of customer cards that Chip-and-PIN-enabled terminals would have been able to stop the bad guys from stealing had Target put the technology in place prior to the breach (without end-to-end encryption of card data, the card numbers and expiration dates can still be stolen and used in online transactions).
0	The number of people in Chief Information Security Officer (CISO) or Chief Security Officer (CSO) jobs at Target (according to the AP).
18.00 – 35.70	The median price range (in dollars) per card stolen from Target and resold on the black market (range covers median card price on Feb. 19, 2014 vs. Dec. 19, 2013, respectively).
1 – 3 million	The estimated number of cards stolen from Target that were successfully sold on the black market and used for fraud before issuing banks got around to canceling the rest (based on interviews with three different banks, which found that between 3-7 percent of all cards they were told by Visa/MasterCard were compromised actually ended up experiencing fraud).
53.7 million	The income that hackers likely generated from the sale of 2 million cards stolen from Target and sold at the mid-range price of $26.85 (the median price between $18.00 and $35.70).
55 million	The number of dollars outgoing CEO Gregg Steinhafel stands to reap in executive compensation and other benefits on his departure as Target's chief executive.

(**Source:** Brian Krebs (May 6, 2014) - http://KrebsOnSecurity.com)

Reputation … why you need to protect it.

By: Nicholas J. Vehr

When it comes to data privacy, the risks have never been greater, legal repercussions have never been more uncertain and severe and effectively managing and protecting your brand's reputation has never been more important.

Reputation matters, whatever business you're in. It's the foundation of your relationships with shareholders, employees, vendors, suppliers, regulators, communities, and more.

Reputation is linked to your company's valuation and cash flow. According to a Weber Shandwick and KRC Research study in 2011 (*The Company Behind the Brand: In Reputation We Trust*), "60% of a company's market value is attributed to company reputation."

Just ask the CEO of Target (not the current one but the one who lost his job after its massive data breach). Just ask the CEO of Sony (the first time they were breached and the second time), Home Depot, Anthem, Uber, JPMorgan Chase and many, many more.

Even more important, ask the CEOs of small and mid-sized businesses out there who are even more tempting targets.

You may not have known this: when it comes to data breaches, mid-sized businesses are the ideal target for cyber-sleuths. Think car dealers, restaurant chains and marketing firms … any business that collects personally identifiable data (DOB, SSN, credit card #s, driver license #s, addresses, etc.).

So, what's a mid-sized business that collects customer data to do?

Prepare.

Most experts will tell you that it's not whether a data breach happens, but when. And when it does happen, here are seven steps to protect your hard-earned reputation:

1. **Move quickly:** Nature abhors a vacuum. If you don't communicate, someone else will. Chances are, it won't be in your best interest. Activate your data breach crisis communications plan (assuming you have one).

2. **Be transparent and truthful:** You can handle the truth, really, you can. Share what you know and what you don't. Put yourself in the shoes of those whose information was pilfered and empathize with sincerity. Social media puts a premium on truth so don't nudge, fudge or lie. You'll just get caught and it will erode that hard-earned trust even further.

3. **Open multiple channels with audiences that matter:** Open two-way communications channels with internal and external audiences. Let everyone know you're working on the problem. Clarify and agree on what's to be said; understand what's being heard.

4. **Be flexible and responsive:** Be available and on-call. News cycles today are 24/7/365 … there's no break in the action because all news is broken instantaneously on social media.

5. **Over-communicate and be consistent:** Say what you think, at the time, is appropriate and responsible and then say it again. We have yet to hear about the company that lost the trust of its customers because they heard from it too often.

6. **Assess, measure and prepare to do better the next time:** Assess all media coverage for tone, story approaches and comments. Monitor social media discussions. Use what you learn to inform and improve your next communication.

7. **"Close" the crisis, if you can:** Inform the audiences that matter to you of the causes and fixes to the problem from a perspective that matters to them.

Reputation matters. Value it. Protect it.

Have a system in place to protect the data you collect. And, remember, also have a plan in place for when your data is breached.

Six Tips to Reduce Your Risk and Be Prepared For a Data Breach

Here are six tips to help you do all you can to prevent a business-disrupting, trust-breaking data breach *and* be prepared for when the data breach actually happens, because it will.

1 **Assume it will happen:** There are many things you can do to prevent a data breach (see 2, 3 and 4 below), or reduce the damage for when it does occur (see 5 and 6 below). The most important tip, though, is this one: assume it will happen. A bad guy will find a way around any and every protection you put in place. An employee laptop will be stolen from their car. An associate will accidentally hand over an unencrypted memory stick loaded-up with confidential client information. Your colleague will access protected customer data files from an unsecured Wi-Fi site.

2 **Ask your IT guy, then ask again:** For the leaders of companies large and small, you should regularly ask what is being done to protect whatever data is in your possession. If your IT guy says, "No problem. We've got it covered," you may need a new IT guy. No one has it covered. Well prepared enterprises seek to be one step ahead of the bad guys while assuming they are likely always one step behind.

3 **Get insurance:** Cybersecurity insurance is available. If you have it, review it regularly with your insurance carrier. If you don't, ask carrier for your other business insurance to recommend several options. Just applying for cybersecurity insurance will be an eye-opening experience. You'll quickly realize how at risk and far behind you really are. Bade news: the forms are long, there are lots of questions it takes a ton of time. Good news: cybersecurity insurance is very reasonably priced.

4 **Put workplace policies in place:** Your insurance carrier will recommend, and you should comply, to put in place a data management, computer and internet policy for your workplace. It is important for everyone in your company to understand the role they play to protect confidential information. It is important for your business, when a data breach occurs, to demonstrate that you have policies in place and employees are trained appropriately.

5 **Plan for when it happens:** It is one thing to assume it will happen and another to plan for when it does. Typically, the largest cost to a company for a data breach comes from lost business indirectly attributed to the break in trust with long term clients and customers. You invested a lot in developing, nurturing and growing mission-critical business relationships, you should do the same to preserve and protect them. This is all about communications which we all know is at the core of any business relationship.

6 **Practice what to do:** It's good to have a plan. It's silly to simply check that box then place the plan on a shelf. Best-in-class companies plan, practice and adjust on a regular basis. For some this may be quarterly. For others, it may be annually. What looks good on paper doesn't always work well in practice, but you'd never know that unless you practiced in advance.

About Vehr Communications

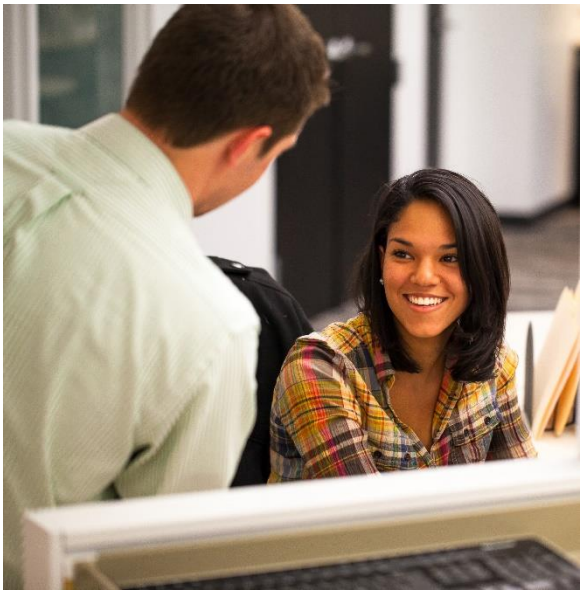
Managing Reputations, Building Relationships, Delivering Results … That's PR. That's What We Do.

Our Mission:

We will be a strategic partner with our clients to help them manage their reputations, build valued relationships and deliver meaningful results.

Our Principles:

- Passion to serve the clients.
- Driven to work hard … really hard.
- Creativity that challenges and is disciplined.
- Commitment to listening, learning and growing.
- Honesty, always, with clients, colleagues and each other.
- Desire to have fun and find balance in our lives.



Our Difference:

- **Refreshing Attitude:** We partner, we listen, we challenge. We learn. We work hard. We make a difference. And we have fun in the process.
- **Resourceful Approach:** We approach each client opportunity with creativity, energy and discipline to build relationships that matter.
- **Global Reach**: We're an IPREX partner … 77 communications agencies with 1,850 staff and 100 offices in 30 countries working as one to support global communications programs for our clients.

Connect with Vehr Communications online at: www.vehrcommunications.com

Contact us at: Vehr Communications, LLC
700 Walnut Street, Suite 450
Cincinnati, OH 45202
T: 513.381.8347