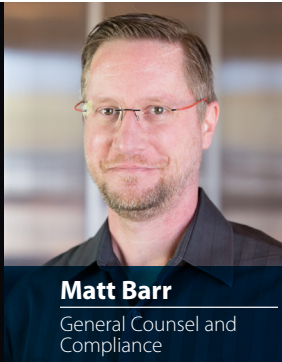


DATA SECURITY

GET TO KNOW YOUR VENDORS

Sponsored by **Mercury Network**

The software chosen by over 700 lenders and AMCs www.MercuryVMP.com 1-800-434-7260



DATA SECURITY

You're responsible for your third party vendors.

Matt.Barr@MercuryVMP.com
www.MercuryVMP.com

Mercury Network

Feedback? We'd love to hear it at info@MercuryVMP.com.

For the latest appraisal workflow and compliance news, subscribe to our blog: www.WorkflowGeeks.com

“

Hundreds and maybe thousands of breaches go unreported.

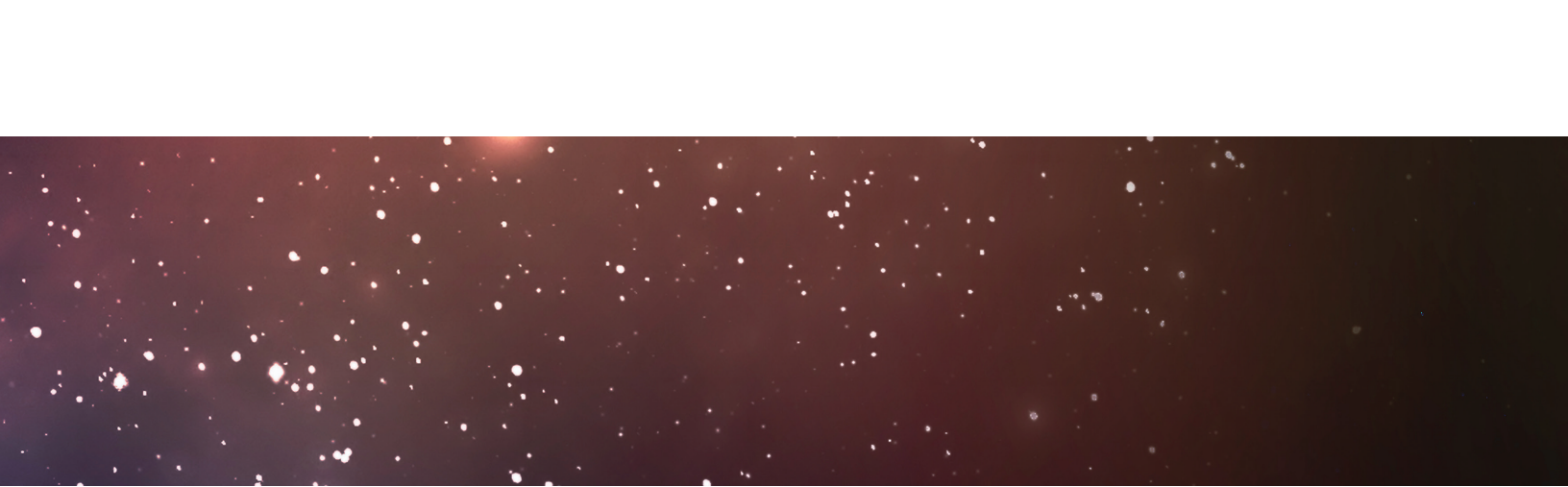
”

You can't go a week without hearing about a new high-profile data breach at a retailer, health care company, financial institution or other business. The targets (I could capitalize the t there and make a bad pun about Target Corp.'s infamous 2013 data breach) seem scattershot, but patterns do form, and they're not unexpected. Twenty-two percent of all data breaches involve financial institutions, a close second-most after health care companies.

In a recent FTI Consulting survey, 90% of directors and 86% of general counsel said they are concerned about cybersecurity. Seventy-seven percent of both directors and general counsel say the risk of cyber liability has increased at their companies.

It's shocking how often you hear executives say they're safe from data breaches because they're too small or not widely known enough to pique the interest of hackers. Be assured that the data breaches you hear about on the news are only the highest-profile ones, generally ones that happen to companies with large footprints. In a typical year, about 1,500 data breaches will be publicly reported. Hundreds and maybe thousands of breaches go unreported.

Hackers are responsible for less than half of those breaches. System glitches (29%) and human error (25%) combined account for more than half. The hugely expensive Countrywide Financial data breach, settled in 2010, was an inside job, an employee downloading customer information and selling it to rival mortgage companies.



Changes in technology and workflow are making you more susceptible to breaches. In a survey of 703 IT security practitioners involved in endpoint security—an endpoint is a desktop, laptop, phone, etc.—68% agreed that employee-owned mobile devices (BYOD) significantly increased risk to endpoints. Cloud applications? 73%. Employees working remotely? 63%.

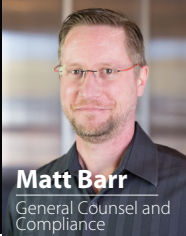
So the data breach you may suffer is very possibly going to be a well-meaning mistake, or a glitch, or a result of the evolution of technology policy. You've literally got people who are paid to worry about those kinds of things in your organization, and as a team I'm sure you're making your own company as secure as it can reasonably be.

But one often overlooked soft spot in data security is your vendors. You're paying more attention to your third party vendors than ever before, with regulators' recent emphasis on third party oversight. But are you paying extra attention to your vendors' information security programs? To the extent you share data with them, your vendors' data security measures are every bit as important as your own.

So what due diligence is desirable when it comes to third party data security?

Get it in writing.

A vendor providing services directly to financial institutions should have a written information security program. Evaluate it, considering the risk if data is compromised, what kind of data it is, and what the vendor does with it. A comprehensive policy should have technical (for example, access control and transmission security), administrative (for example, assigned security responsibility), and physical (for example, facility access control) components.



DATA SECURITY

You're responsible for your third party vendors.

Looking at it through the data life cycle, a policy should address:

- **Access control.** The most effective security measure is preventing access to areas where sensitive data resides in the first place. Some things to consider: where a vendor has access to sensitive data, its workstations should be as secure at its office as they are at yours. How do customers log on to retrieve their data, if applicable? Are measures in place to prevent fraudulent customer access, such as locking the account after a certain number of failed login attempts? What measures are taken when access control is compromised (for example, a possible stolen password)?
- **Restricted access.** Access to sensitive data should be rigorously restricted. There should be a hierarchy of access to sensitive data, both internally in organizations and throughout the data life cycle, that resembles need to know. Which managers, employees, and contractors have access to the most sensitive data? Do they undergo a background check prior to or during their employment? Employees should also undergo comprehensive security training, including learning what data they have access to, and how to manage it when it's in their possession.
- **Security in transit.** Sensitive data should be protected in transit, for example by reliable encryption. Certain data just shouldn't be conveyed via e-mail in the first place. And for goodness' sake, we need to stop using fax machines, at least shared ones and at least for sensitive data.
- **Data retention.** Sensitive data should be kept no longer than necessary. If a vendor has a backup system, which is responsible business continuity planning, it should have only a limited time in storage before it's finally destroyed. Is backed-up data as secure as real time data? Ideally, it should reside on media that's not connected to the vendor's network where the original data resides.
- **Data disposal.** Paper with sensitive information should be shredded. Data on electronic media should be irretrievably erased after a certain date. When there is employee turnover, the computer the former employee used should be wiped clean.

Your own organization deals with these issues. Your vendors do, too.



Written contracts

Where there is a contractual relationship, are provisions in place protecting you and your data? Again, appropriate to the level of risk. There's no better place to spell out obligations than the contract you have to enter into anyway.

Many vendors will have a boilerplate contract or license agreement—should you negotiate? How deep into the weeds do you want to go? To reiterate, it depends on the risk to the data, what data they see, and what they do with it. But if the vendor has a standout information security policy, that helps you evaluate the potential for security concerns, so you can prioritize your highest-risk vendors and contracts.

One route some companies go involves drafting a standard data security addendum which they append to their vendor contracts when appropriate. A couple of pointers. It's tempting to throw in language obligating vendors to “comply with all relevant laws and regulations”, but vague provisions like that are just asking for trouble. Cite chapter and verse: the Gramm-Leach-Bliley Act, 15 U.S.C. §6801 et seq., for example.

When it comes to detailed security procedures, there are certainly items you want to make sure are covered in a contract, such as incident response. However, unlike the catch-all “all laws and regulations” you want to avoid, it's better to be nonspecific here. You want your vendor to modify its security policy as threats evolve, not make it adhere to a snapshot of the policy on the date you signed the contract.

The SSAE-16

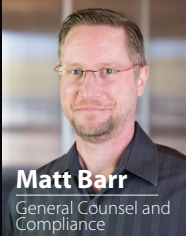
Your priority vendors should have a report of the results of an annual security audit. The SSAE-16 was developed by the American Institute of Certified Public Accountants to provide an in-depth audit of a company's security objectives and activities. It allows a vendor to disclose its processes to an independent auditor in a uniform format.

The report has its limitations—the vendor has a great deal of input into what their systems are, how they work, and what they're meant to accomplish. But it's a valuable tool for evaluating a vendor's security measures. It includes

“

You can't have too much information about a vendor's security policies and practices.

”



DATA SECURITY

You're responsible for your third party vendors

comprehensive descriptions of the controls the vendor has in place that might go into more detail than a written security policy. If your priority vendor has had a SSAE-16 audit, definitely grab a copy of the report as part of your due diligence, and then read it (or have someone responsible for reading it). You can't have too much information about a vendor's security policies and practices.

Business continuity and disaster recovery

Separate from a written security policy, even though they touch on the issue of security, are business continuity and disaster recovery plans. A business continuity plan will tell you that a vendor has thought about and put controls in place to mitigate incidents that might disrupt normal operations. How will the vendor respond to a total power outage, or a comprehensive systems failure, or half the staff not showing up for work due to weather? A disaster recovery plan, along the same lines, spells out the vendor's response to more catastrophic incidents, when systems and data might be irretrievably lost, such as an earthquake or tornado.

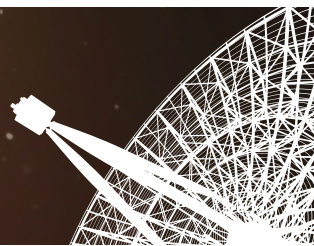
Has responsibility for coordinating BC/DR been allocated in advance? Is the plan granular enough that managers know who's responsible for what? Are there generalities—"make sure everybody is safe"—or specifics—"require everyone to text a number we've given out in advance to say they're OK?" More directly, does the plan specify how and when its customers can expect to be back up again after an incident?

Retention and destruction of data

Of course you want your vendors who deal with your sensitive data to back everything up; you're trying to avoid data loss, just as you are data compromise. Keeping backup data safe and inaccessible often involves the same measures the vendor has in place for the original data. Where are the backup files stored? Offsite? On site, but separate from the system where the data lives in real time? Is it backed up in the cloud, and if so, what measures are taken to prevent unauthorized access? Who has physical access to the place where the backup data resides?

Your own organization works hard to maintain your own data security. You know that your vendors do too. They should be able to prove it with a comprehensive, written, audited security policy, including plans for business continuity and disaster recovery.

FREE COMPLIANCE RESOURCES



www.MercuryVMP.com/Resources

More than 700 lenders and appraisal management companies choose Mercury Network to power their appraisal operations. How are they handling all the new compliance challenges while keeping expenses down?

Each download is packed with strategies to help you avoid expensive mistakes and reduce your risk, with expert interviews and links to the regs. Get them today for free insight on the appraisal compliance challenges we all face.





Free additional resources: Industry best practice guidelines and news

www.MercuryVMP.com

Get expert recommendations for compliance, efficiency, and maximizing profit.

www.workflowgeeks.com

Subscribe to get the latest in your inbox.

Mercury Network

The software chosen by over 700 lenders and AMCs

www.MercuryVMP.com or call **1-800-434-7260**