The data breach has come of age. Looking back from 2016, companies representing all industries and sizes have now experienced a major data breach. Whether your company stores valuable intellectual property or sensitive customer information, securing your company’s data is now a prerequisite to protecting your company’s bottom line. This article serves as a practical guide to understanding and managing your company’s data breach risk. It will help you to assess your company’s exposure to data breach liability and take proactive and reactive steps to prevent and mitigate data breach costs.
Data breaches are events where a company’s confidential or sensitive data is accessed by an unauthorized party or is unintentionally exposed to the public. While companies in the health care and financial industries have long made data security a top priority, the new legal and business reality is that every company must now take data security at least as seriously as it takes any major threat to its bottom line. Not all data breaches are sensational, highly-publicized cyberattacks resembling the Sony or Target breaches. Smaller and lower profile companies now form a prime target for attacks by sophisticated criminal organizations. In fact, 62% of all data breach victims are small and medium sized businesses.

Because data breach costs are often excluded from traditional insurance, smaller companies may have great difficulty absorbing the loss of goodwill and professional fees resulting from a data breach. Likewise, data breaches can result in serious career damage to the executives responsible for protecting data. Consider that the average cost to a U.S. company for a data breach in 2015 was $6.5 million and the average cost to a U.S. company for each lost or stolen record containing sensitive or confidential information in 2015 was $217.

Don’t make the mistake of relying solely on security software packages and stop-gap technical fixes. Data thieves routinely exploit human judgment lapses, physical security weaknesses and business process loopholes to steal sensitive data.

Part one of this article explains the types of costs and disputes companies face as a result of a data breach. While reading this part, I urge the reader to think about the risks applicable to their company. Part two covers the fundamentals of establishing a data security program. Part three discusses the steps necessary to contain and mitigate losses when reacting to a data breach.
Protecting against data breaches is far from a simple matter with a simple solution. Data can be compromised intentionally or unintentionally, by international criminal rings or well-meaning employees, through physical theft or by technological subterfuge. For example, a careless employee may mistakenly forward a sensitive email to the wrong person; a thief may steal an executive’s laptop on a train; and so-called ‘ransomware’ attacks hold data hostage until the company pays an overseas hacking group thousands of dollars to unencrypt it.\(^3\) As if that weren’t enough, data breach threats will only continue to rise, especially for companies that allow ‘bring your own device’ programs (BYOD), migrate their data to cloud-based systems or connect new kinds of devices to their network.

Losses from a data breach can be devastating to a company, many times resembling a death by a thousand cuts as consumers stop patronizing retail outlets, business partners sever ties and legal costs accumulate. The loss profile of each data breach will differ depending on the amount and type of data stolen, the company’s efforts to secure the data prior to the breach, and the federal and state laws implicated in the breach.

Most data breach costs will fall into the following categories in varying amounts, depending on the nature of the breach:

- **Reputational damage and lost profits**
- **Legal and other professional costs from defending lawsuits and managing investigations** (see sidebar on this page)
- **Forensic investigations and business continuity expenses**
- ** Destruction of a company’s competitive advantage from exposure of trade secrets**
- **Costs to comply with cumbersome data breach notification statutes**
- **Adverse court judgements, legal settlements and regulatory fines**

The most common type of stolen data relates to consumers’ personally identifiable information, or PII, which can easily be monetized by identity thieves for profit. Not all data breaches relate solely to PII or similar information, however. Far less reported, likely because of a reluctance to go public, are breaches of intellectual property, such as source code or internal communications. In the Sony breach, for example, movies, scripts, employee emails and executive salaries were all stolen and released to the public, resulting in massive damage to the company’s reputation.

While there is no perfect data breach solution, by establishing a data security program, or DSP, a company can minimize the risk of a data breach. The basics of DSPs are discussed in the next section.

---

**CONSUMER AND CONTRACTUAL LAWSUITS**
A company that has experienced a major data breach can expect to face claims from a wide variety of litigants. The most common type of claim is one by a consumer or class of consumers alleging injuries related to compromised private information. These lawsuits allege that the company violated its contractual obligations, duty of reasonable care to protect confidential information, or both. Regardless of the ultimate merits of the case, defending against a consumer lawsuit can result in significant legal expenses, along with fines and damages.

If compromised data includes a business partner’s confidential information, a company can become the target of a lawsuit for breach of vendor contract. Similarly, if credit card data is stolen, companies may face claims from issuing banks for recoupment of fraudulent charges and related damages. While less common, companies should potentially be *more* concerned about these types of lawsuits given the ability of well-capitalized plaintiffs to fund a long-term legal assault versus that of consumers.

Finally, boards of directors may face shareholder derivative litigation for damages to share value resulting from data breach costs. While the law is still developing in this regard, it is plausible that a board’s fiduciary duties will one day include an express duty to develop and implement some form of DNP.

**STATE AND FEDERAL INVESTIGATIONS**
The Federal Trade Commission, or FTC, has emerged as the national leader in bringing enforcement actions against companies who have experienced a data breach. In these actions, the FTC asserts that a company’s cybersecurity policies and practices are ‘unfair’ or ‘deceptive’ acts, giving the FTC so-called Section 5 authority to take legal action against virtually any company that has experienced a data breach. The FTC usually alleges a failure to use reasonable security measures (unfairness) or misrepresentations by the company about its existing security procedures (deception). Defending against an FTC enforcement action can come at great expense to a company and can result in fines and a requirement that the company adopt new security safeguards. Along these lines, you should ensure your company’s customer privacy policy accurately reflects its actual security procedures, or risk unnecessary ‘deception’ liability in an FTC enforcement action.

Similarly, state attorneys general offices have brought their own enforcement actions relating to data breaches, both on their own or in partnership with other state attorneys general. Smaller companies may find themselves off the FTC radar, but well within the sights of a state attorney general after a data breach. For example, in 2013 the Vermont Attorney General’s office reached a settlement with a local grocery store over the failure of the store to promptly notify its customers a data breach had occurred and a failure to expeditiously correct security vulnerabilities.\(^4\)
Part 2: The Data Security Program

"An ounce of prevention is worth a pound of cure" – Benjamin Franklin

The most important step your company can take to guard against data breach risk is to develop and implement a comprehensive data security program, or DSP. One study found that a staggering 90% of data breaches in 2014 could have been prevented by the adoption of widely accepted best security practices. A DSP may also form proof your company maintained reasonable and appropriate security measures to protect its data when defending against lawsuits or regulatory enforcement actions.

As much as a DSP is a set of written policies, it is also an organic process requiring continual review, revision and commitment. A successful DSP is also an interdisciplinary endeavor requiring representation from each functional group within the company. At a minimum, your DSP should leverage the expertise, and influence the policies, of your company’s management, legal, operations, human resources, risk management and information technology departments.

The following considerations are essential when crafting an effective DSP:

Identify Data Assets and Risks to Data
Before your company can determine what safeguards to use, it needs to understand the data it stores or handles. During this process, you should pinpoint your company’s ‘crown jewel’ data, such as important trade secrets or credit card data, as you will likely want to prioritize and orient your DSP around these assets. Do not neglect to consider your own employees’ data in this assessment. Personnel files are often a treasure trove of valuable information for hackers.

After cataloging your company’s data assets, identify security threats to that data. For each threat, your company should evaluate the risk posed to the data by analyzing the likelihood of the threat, the potential damage from the threat and the sufficiency of security safeguards to guard against the threat.

Implement Security Controls
Following the risk assessment, your company should work with its information technology, operations, legal and human resources departments, together with an outside technical advisor or advisors, to determine the security controls necessary to protect sensitive data. Security controls will form the foundation of the DSP and can take the form of technical, administrative and physical safeguards. A robust, effective DSP will provide for, among many other things, sophisticated encryption technology, user privilege policies, key card locks on server rooms, document shredding, data destruction, password management, email authentication and mobile device management.

A word of warning: do not become a victim of technology! Many companies become so dependent on data security software that they neglect or fail to implement other important security safeguards. A security software package is not a magic bullet. To the contrary, technology is but one important component of the overall DSP.

Employee Training
Data security should be a core value of company culture. To that end, employees must be properly trained about their security responsibilities. The most sophisticated and expensive security safeguards can be circumvented when a careless employee opens a malware-laden email attachment or gives her password to a tech support imposter. Routine employee training should include instruction on data management policies, breach recognition, security policies and privacy policies. Employees should be instructed about how to report data security concerns with assurance they will not face retaliation.

Legal Considerations
It is no secret that government contractors, healthcare providers and financial institutions must meet certain government regulations relating to data security. What about companies in other sectors? While there is no federal ‘Data Security Act’ generally applicable to all companies (yet), there is a patchwork of state and federal laws, regulations, regulatory enforcement actions and common law theories that directly or indirectly relate to data security. Several states, including Massachusetts, Texas and California, have even enacted laws requiring all businesses active in their state to implement certain data security procedures and practices. If the state or states you are operating in have not enacted an express data security law, your company is by no means safe. Obscure statutes, regulations and common law theories of negligence have successfully been used to sue companies for poor security practices.

The bottom line is that bad security is a legal quagmire. Companies that fail to provide reasonable security for their customers’ or business partners’ data risk losing big if a breach occurs. In summary, you should always provide reasonable security measures for your company’s data. You also need to work with your legal advisor to ensure you are meeting the specific requirements of applicable state and federal laws.

Appoint a Chief Data Protection Officer
It is important to appoint an employee to take ownership of your company’s data security. In smaller organizations, this might not be a full-time position. The most important job of this data chief is to ensure compliance with the DSP.
**Part 2: The Data Security Program**

**Cyberinsurance**

Cyberinsurance isn’t just for your robot collection. Your company should review cyberinsurance options with different insurers to ensure it has the desired liability backstops in place should a data breach occur. Because it is a development-phase insurance product, data breach insurance policies vary widely from carrier to carrier. The selected policy should provide some type of coverage for forensic investigation, costs of restoring data, consumer notification costs and defense costs. Your company’s cyberinsurance policy should be carefully tailored to the data security risks it identifies when crafting its DSP. For example, a company anchored by its intellectual property will be more concerned about data restoration and forensic investigation expenses, whereas a consumer driven company will want to focus on consumer lawsuits and data breach notification coverage. Do not expect to rely on your commercial general liability (CGL) policy for data breach claims; those claims are likely excluded. Avoid policies with encryption, cloud and software update exclusions. You should periodically reevaluate cyberinsurance coverage to ensure it offers the desired levels of protection as the data needs of your company change.

**Review Commercial and Transactional Contracts With Counsel**

As outsourcing of business functions continues to rise, so too is the sharing of customer or other confidential data with outside service providers. For example, your company’s relationship with its cloud services provider or managed services provider often requires the sharing of sensitive internal data over the internet. If one of these service providers is hacked, it is often other companies’ data that is exposed. In such a case, it is unlikely the service provider will readily step up and accept responsibility for its own negligence. Therefore, it is important that your contracts with those vendors detail the data security duties owed to your company and require the service provider to indemnify your company for data breaches where it was at fault.

In addition, if your company is seeking to purchase another business it should analyze data security issues as part of its transactional due diligence. Foremost, you should review the target’s DSP and assess the level of compliance with its DSP. You should also inquire about any recent data breaches or other security events and review the target’s cyberinsurance policies.

**Data Collection, Retention and Disposal**

Limit data collected to what is necessary to your company’s operations. Each item of data collected or stored means more potential liability. Delete unneeded data; hackers can’t steal what you don’t have. The data-happy company should know that keen data management is not necessarily at odds with robust data collection and data usage. Data management does, however, involve tying data collection to legitimate business needs and disposing of data after it is no longer needed.

**Breach Response Plan**

Many security experts recognize that it is not a matter of *if* but *when* a company has a data breach, which is why your company needs a breach response plan. Following the creation of a breach response plan, you should conduct a breach response ‘test run’ to ensure company-wide familiarity with the plan. Each company’s breach response plan will vary depending on specific business needs, but should include the following at a minimum:

- **Definition of a data breach.** A data breach in progress doesn’t look like an alarmed IT worker agape at a flashing red monitor. Employees should be trained to recognize and report activity that forms or could form a data breach, such as a misdirected email containing sensitive information or a stolen laptop.

- **Internal reporting procedure.** Provide specific instructions about who to notify within the organization about the breach or possible breach.

- **Incident response team.** Allocate responsibilities for responding to the breach among a team of ‘first responders.’ Just like any disaster, the response team must be trained and equipped to handle the situation. The team leader should be someone who has the requisite authority to make quick decisions.

- **Notification procedures.** Describe in detail your company’s notification obligations in the event of a breach.

**Third Party Vendor Requirements**

Most companies would never entrust their physical inventory to a third party without asking questions about their insurance, employees and facilities, yet companies often hire cloud services vendors and outsourcing agents with little or no due diligence. When engaging a third party for cloud storage services, software as a service, or other IT need, you should ensure these service providers’ technical and physical safeguards are at least equal to, or greater than, your company’s own security safeguards.

**Audit and Update**

A DSP is never ‘complete.’ As part of its ongoing commitment to update and refine its DSP, your company’s chief data protection officer should administer a periodic audit of the DSP. In the audit, the company will reassess risks, implement and update safeguards, run tabletop exercises, train and retrain employees, review insurance policies and contracts, and update other security policies as necessary.
Part 3: Responding to a Data Breach

“*I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.*” – Robert Mueller III, Former Director of the FBI

It would make little business sense to rule out the possibility of a fire following the installation of a new sprinkler system and a few fire drills. In the same way, no matter how well-defended your company might be, a major data breach always remains a distinct possibility. Even the most secure systems are still susceptible to hackers through previously undisclosed and uncorrected software vulnerabilities (so-called ‘zero-day’ exploits).

Once it is certain there has been a data breach, company officers should consult the company’s breach response plan for the procedures necessary to mobilize the breach response team. The data breach response can be largely separated into three stages: containment, investigation and notification. These stages will likely overlap.

**Containment**

Following a data breach, your company’s most time sensitive need will be to limit further data loss by containing the incident. Often times, IT employees and consultants are under immense pressure to fix the problem and restore functionality to the system. This results in a panic mode where key evidence regarding the nature of the data breach is lost. Therefore, in the immediate aftermath of a data breach, the breach response leader should take steps to ensure all evidence about the breach is preserved and your company’s initial response actions are thoroughly documented in writing. Then, as the IT team is working to restore service, a designated record keeper should collect information about how the breach was discovered, what data might have been affected and which individuals have knowledge of the breach. Steps should be taken to save and preserve your company’s server logs as soon as possible following discovery of the breach.

**Investigation**

A thorough, well-documented investigation must take place before your company can make sensible business decisions about how to respond to the breach. In the investigation, your company will determine exactly what data was compromised in the breach and why data security measures failed to prevent the unauthorized access. In light of this information, your company should analyze the legal and business implications of the breach, including the risk of litigation and any notification requirements.

It is important the investigation be headed by your company’s legal counsel. Counsel will be able to best determine how to assess and manage liability relating to vendor contracts, statutory notification requirements and governmental investigations. Of perhaps greater importance, the investigation process may be protected by attorney-client privilege if lead by an attorney. This protection may prove an invaluable advantage in an ensuing lawsuit or regulatory investigation. Any outside technical consultants, such as forensic specialists, should be engaged by counsel to extend the attorney-client privilege.

Law enforcement agencies, such as the FBI, can prove a valuable resource or annoying obstacle following a data breach. Whether to contact law enforcement will depend on the circumstances of the data breach, including the seriousness of the event and the company’s desired amount of control over the investigation.

**Notification**

An important decision your company will need to make following a data breach is when and how to notify the public, shareholders and the company’s business partners about the breach. While state and federal data breach disclosure laws may require some specific deadlines and disclosure formats (see sidebar on the next page), it is likely that many details of how to disclose the breach to the public will be left up to the company’s discretion. Once you are confident of the scope of the breach and your company’s respective legal obligations, you should consider going public.

For the most part, the sooner the data breach is disclosed the better, unless there are obvious reasons why your company should hold off. Knowledge that sensitive information has been compromised allows customers and companies to take proactive measures to prevent or mitigate their losses, such as alerting their payment card banks and upgrading their security systems. In addition, the longer a company waits to disclose a data breach the more likely it is that an injured party will find out about the breach from an unofficial source, such as a wayward employee or disgruntled vendor, in turn fostering resentment and disloyalty towards the company. By the same token, being forthright can engender loyalty and transparency with customers and business partners.
Part 3: Responding to a Data Breach

DATA BREACH NOTIFICATION STATUTES
At the time of this article, 47 states and the District of Columbia have enacted some form of data breach notification statute. These laws require a company to notify consumers if sensitive information, such as social security numbers or credit card information, has been compromised. Navigating each state’s unique notification statute can be a legal nightmare for companies. For example, in Florida, notification of the data breach must be made within 30 days, while in Connecticut the notification window is 90 days. Florida defines personally identifiable information to include an individual’s military ID number and passport number while Wisconsin does not, so it is possible that—for the same data breach—a notification might need to be made in Florida but not in Wisconsin and may be considered late if mailed within 60 days to a Florida resident but not so if mailed to a Connecticut resident. Confused yet? As if that were not enough, depending on industry or other factors, companies may be subject to state and federal regulations requiring them to report the data breach to the Securities and Exchange Commission, the Department of Health and Human Services, state attorneys general and other federal and state agencies.

Many experts believe this patchwork of state laws will one day give way, and must give way, to a uniform national standard. Legislative proposals have been made to that end. Until such time, your company must take note of each state’s unique notification requirements when reporting a data breach, as a failure to correctly follow the law can result in civil liability or statutory penalties.

1 “Small, mid-sized businesses hit by 62% of all cyber attacks,” Property Casualty 360, May 27, 2015 (last accessed March 7, 2016).
3 “California Hospital Pays $17,000 To Hackers In ‘Ransomware’ Attack,” CBS SF Bay Area, sanfrancisco.cbslocal.com (last accessed March 8, 2016).
6 At a minimum, your company should implement the “SANS 20” critical security controls, available at www.sans.org/media/critical security-controls/CSC-5.pdf.

This article is not intended as legal advice or as a substitute for the specific advice of your own counsel and should not be relied upon as legal advice. The advice appropriate for your company will be dependent upon the particular facts and circumstances of your situation. The transmission or receipt of this article does not create an attorney-client relationship. Attorney Advertising.
Data storage and use is not only a powerful tool and asset, but full of risk. No company, including yours, can completely eliminate these risks. Your company can, however, manage and minimize its data breach risk by implementing a DSP. An effective DSP will include employee training initiatives, security safeguards, contractual provisions and insurance coverage, among many other things. Data security will also require ongoing input and collaboration from the management, legal, operations, human resources, information technology and risk management departments of your company. Should a data breach occur, your company will need to respond swiftly and effectively to mitigate its losses.

Further Information
If you would like further information on any aspect of this article, please contact Ryan S. Replogle, Esq.

replogle@beckmanlawson.com
T 260-403-9845
www.linkedin.com/in/replogle1

Ryan advises small businesses on cybersecurity and privacy issues, including legal risk assessments, mitigation strategies and organizational data security programs.

Ryan also has a broad background in corporate, commercial and securities law, representing companies and investors at all stages of corporate growth. He advises clients regarding their commercial agreements, contract disputes, merger and acquisition transactions, shareholder agreements and supplier-distributor relationships.