DATA BREACH

COMPLIMENTS OF MRINSURABILITY.COM

Introduction

Businesses today are responsible for all kinds of data. Common types of data include credit card information, employment records, healthcare records, company financial data and often time's confidential corporate information.

Even those companies with the most sophisticated IT security systems, are susceptible to a data breach. The loss of this data and the associated costs could be devastating to a business.

Last year alone 429,000,000 records were compromised. That's an increase of 23% over the previous year. On average, 29,611 records are lost per breach. The average cost of dealing with each record is $221. Just talking about an average breach, that comes to just over 6.5 million dollars.

So you can see that when it comes to a threat such as a data breach and its potential impact on your business, it pays to be prepared. This means having the right information, as well as the right insurance coverage.

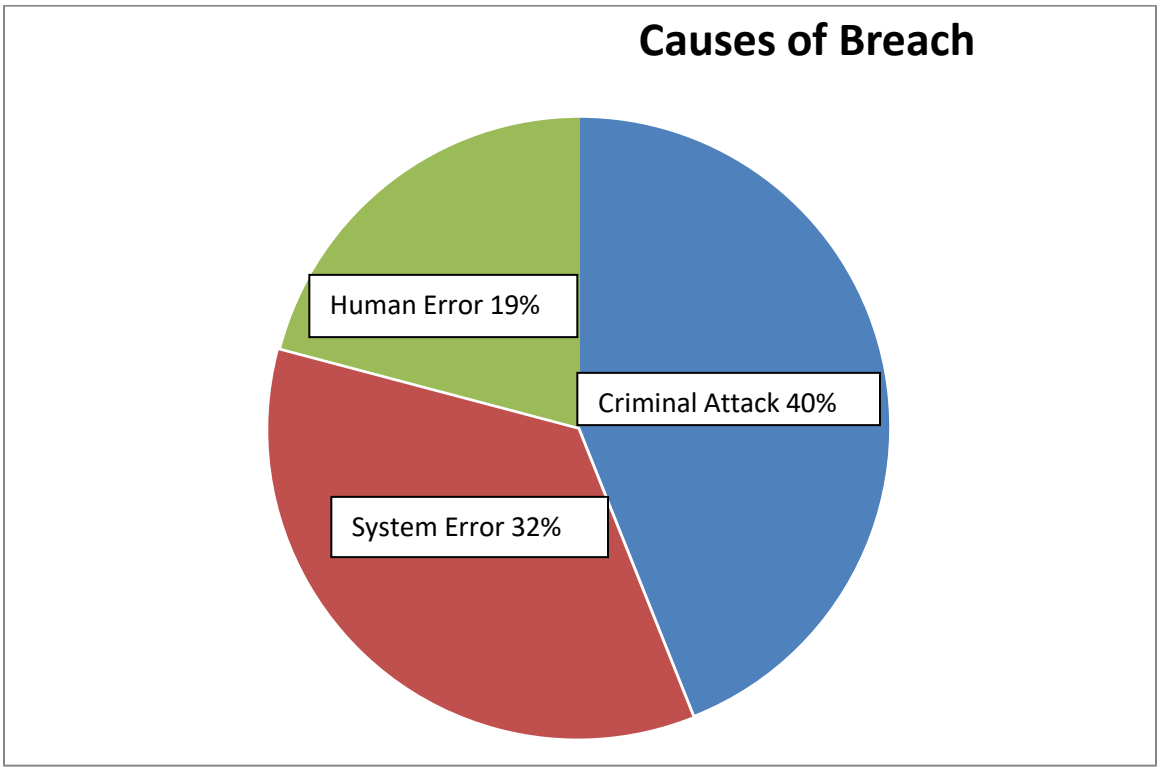
How Breaches Occur

Technology is a major component of today's business operations and as it becomes more complex and sophisticated, so do the risks. Let's look at some of the ways that data breaches can occur. The following is a list of some of the most common methods.

- Solicitation – Simply asking for information
- Password Sniffing – Software scans and records passwords
- Human Error – Documents with one (or more) person's nonpublic personally identifiable information were mistakenly sent to someone else (e.g. emailed, faxed, mailed, etc.)
- IT Security Error – Typically involves a system misconfiguration
- Missing or Stolen Mobile Devices – contain unencrypted nonpublic personally identifiable information (e.g. laptops, smart phones, USB flash drives, CDs, etc.)
- Exploitation – Abuse or misuse of access to company information
- Unapproved Devices – Using hardware or software not approved by the company
- Hacking – Unauthorized individuals gain access to your computers or servers (often due to inadequate firewalls or weak passwords) and gain access to nonpublic personally identifiable information you store
- Laptop Theft – Stealing a company owned laptop to access vital information
- Pretexting – Person lies to gain access to privileged data
- Social Media –Use of social site to identify employees and gain information through fake friendship
- Denial of Services – Render website and other resources unavailable to intended user
- Malware Infection – Infect data system with a virus
- Hoax – Access information through deception
- Wireless Network – Hackers use flaws in wireless routers to access users information
- Social Engineering – Deceive people into performing actions or divulging confidential information

- Abuse of Access – User with more than normal access to company network steals information
- Improper Data Disposal – Not destroying hardware, software, paperwork in a proper manner
- Ransomware - Malicious software blocks access to a computer system until money is paid
- Bots on the Network – Software allowing a computer to receive instructions from a different computer
- Phishing – Emails appearing to be legitimate are actually fake and typically ask for personal information under some false pretext
- Data Misuse – Data used for things other than the reason it was initially collected
- Erroneous Data Posting - Someone unintentionally posts private or sensitive company or customer information
- Breach Caused by a Vendor - Exposing your customer's and/or employee's nonpublic personally identifiable information
- Payment Card Fraud - Nonpublic personally identifiable information is stolen from a point-of-service credit card or payment terminal
- Missing or Stolen Paper Documents - containing nonpublic personally identifiable information
- Stolen Computers or Servers - Containing unencrypted nonpublic personally identifiable information

Now that we've looked at a variety of the causes of data breaches, we can narrow it down a bit further. They fall into 3 basic categories: human error, employee error and criminal activity. The following chart gives us a more accurate look at the percentages involved.



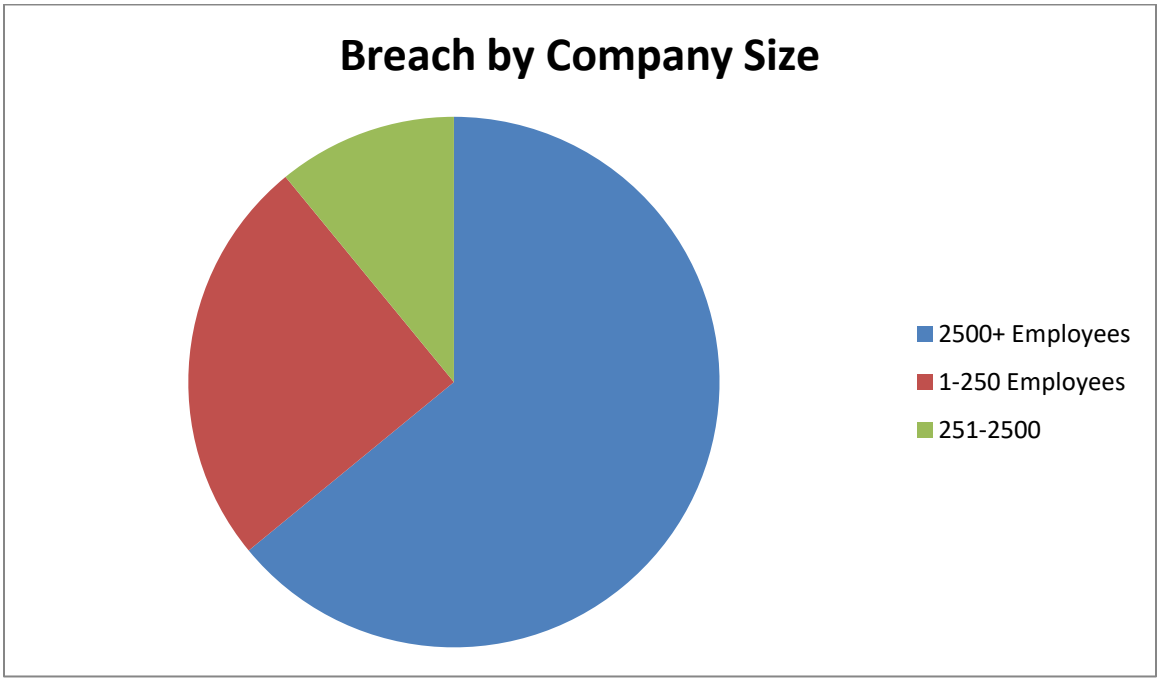
As the percentages show, there are still a few unknowns, but for the most part we can see that criminal attack is actually less than one-half of the overall cause of the problem.

So, in order to get an even better handle on things, let's take a look at some of the misconceptions that company owners and officials have about data breaches.

Misconceptions about Data Breaches

When it comes to cyber-risk, there is a lot at stake: data, customers, reputation and a businesses' bottom line. **The truth is that no business is too big, too small or too well protected to fall victim to a data breach.** Let's take a look at some common misconceptions about a company's safety.

The first one is that only large companies are at risk (Let's see if that's true.)



Companies with 1-250 employees had 34% of the data breaches last year
Companies with 251-2500 employees had 25% of the data breaches last year
Companies with 2500+ employees had 41% of the data breaches last year

So, it would seem that small and medium size companies actually account for more of the data breaches than large companies do.

We have state-of-the-art security systems in place

IRS -724,000 records hacked

Centene Health- care 950,000 records hacked

FBI/Homeland Security-20,000 FBI, 9000 Homeland records hacked

Linkedin – 167M records hacked

MySpace-6.5M records hacked

Office of Child Support Enforcement Wash DC-21M records hacked

Verizon-1.5M records hacked

Yahoo-500M records hacked

The above was just for the year 2016

We've never had an issue, so we probably won't have one

See above

We outsource our data and they have coverage

The original owner of any data is liable for it – if you outsource to a cloud, vendor, supplier, payment processor or any payment service, it doesn't matter.

We can handle the cost of a breach

Cost of data breach $217 per record, average cost 6.53Million per breach

We're already covered for cyber-events

As of October 2016 only 29% of businesses had any cyber coverage. Current cyber policies are filled with exemptions and the coverage that does exist still leaves companies severely underinsured when compared to the cost of damages from today's data breach.

Just What is Nonpublic Personally Identifiable Information?

Just about all businesses, no matter the size, collect data about their employees, customers and tenants. So, just what is nonpublic personally identifiable information? Below is a list of the most common items. If your company collects any of these, then you need to have safeguards in place.

Nonpublic Personally Identifiable Information includes, but is not limited to:

- Employee Information
- Social Security Number
- Contact information
- Government-Issued ID
- Birth Date
- Birth Place
- Payment Information
- Account Numbers
- Online Information
- Loyalty Cards
- Password Verification Data

Protected Health Information includes, but is not limited to:

- Physician's Health Records
- Medical Records for Workers' Compensation
- Drug Test Results
- Prescription Information
- Patient Billing and Insurance Records

Data Breach Response Expenses Coverage

Now, let's take a brief look at what kind of coverages a typical company should be looking into getting.

The first thing to be aware of is that the majority of states have breach notice laws that require notification to individuals, if their nonpublic personally identifiable information or protected health information has been exposed.

The cost of providing notice and responding to a data breach can be expensive, depending upon the number of impacted individuals and compromised records. In reality, **this will probably be your most expensive portion of the cost of recovering from a breach.**

Typical Data Breach Response Expenses coverage provides:

- Expenses to notify affected individuals of the breach
- Legal and forensic costs to determine the extent of the breach and how best to respond
- Services to impacted individuals, such as credit monitoring, a help line and identity restoration case management
- Access to a data security resource website

Typical Data Breach Liability provides coverage for:

- Damages the Insured is legally obligated to pay due to fraudulent use of nonpublic personal information of others that is lost, stolen or accidentally released
- Costs to defend suits seeking such damages, including investigation or settlement of a covered data breach suit

Typical Commercial Identity Recovery coverage provides:

Individual business owners and, if selected, their employees, with recovery services incurred as a result of a theft of their personal identity. These services typically include:

- A case manager who will assist the individual in recovering control over their personal identity by contacting authorities, credit bureaus and businesses in the process of correcting records
- Reimbursement of necessary and reasonable expenses incurred as a result of identity theft, including lost wages, mental health counseling and child and elder care supervision costs
- One-Stop policyholder support is provided, including

a) Seamless integration of response services
b) Documentation of every stage of the breach response process

I use the term “Typical” in these sections because today’s Data Breach coverage is something very new and because of the variety of needs that businesses may have, the coverage is also quite customizable.

When you contact an organization such as MrInsurability, for information on coverage for your company, you should expect to receive a plan that is customized to every aspect of your industry, as well as to your particular business.

Let’s close out with a few ideas on where to get started assessing your company’s needs.

Where to Begin

In deciding where to begin, first ask whose information do you store or have stored? The answer will most likely be one or more of the following:

- Customers
- Employees
- Other businesses
- Other individuals

The next thing to determine is what kind and how sensitive that information is:

- Financial
- Medical
- Intellectual property
- Personal

Next you'll need to determine how that information is

- Collected
- Protected
- Shared
- Used – you, your partners and assoc, others that host or have access to your data

Identifying the systems and data most critical to your operation, as well as your organization's vulnerability, is the first step toward helping to prevent, respond to and recover from a data breach or cyber-attack of any kind.

Implementing, maintaining and enforcing procedural and technological controls to protect critical data and systems are a key element to the success of a winning cyber-security strategy for your company.

Being prepared to respond quickly when a suspected data breach or cyber-security incident is reported, as well as planning your company's response and recovery, are the most critical steps that you can take, prior to a breach ever taking place.

In Conclusion

Information Security Risks, Data Breaches and Identity Fraud are not disappearing trends. As a matter of fact we have all read about the fact that these types of attacks are becoming more frequent and more complex in nature.

New legislation, along with ever changing contractual requirements, has added to the complexity of managing all types of cyber-threats for the business owner.

The one constant in all of this is insurance. It remains that insurance is the one tool that businesses can use to manage risk!

If you find that you're most likely underinsured or if you're in that 71% of businesses with no cyber-threat insurance at all, then please contact us. At MrInsurability we work with only the top insurance carriers in this industry and have the ability to customize coverage to meet the particular needs of your company!

We can be reached by using the contact form on our website MrInsurability.com, by email at info@mrinsurability.com, by phone at 630-385-2448 or toll free at 1-800-869-9194.

The next 2 pages contain a short questionnaire. In case you are not sure, it will let you know for sure if you are in need of insurance coverage against a data breach or other cyber-threat. It's very easy and if you find that you are indeed in need of coverage, then, you already know what to do!

Your Cyber Exposure

1. Does your business retain physical or electronic records of employees or other third parties with any of the following? (Check any that apply)

a. Social security numbers _____

b. Drivers' license information _____

c. Tax identification numbers _____

d. Birth dates _____

e. Medical/health records _____

f. Court records _____

g. Police records _____

h. Banking information (checking/savings accounts)_____

i. Email addresses or home addresses _____

If you checked any of the above, your organization is in control of "Personally Identifiable Information" and therefore, required to protect that data subject to State and Federal privacy and data breach notification laws.

2. Does your business have employees? Yes ___ No ___

3. Does your business have an active website? Yes ___ No ___

4. Does your business use third-party vendors (e.g., cloud, IT services)?
Yes ___ No ___

5. Does your business use mobile technology (e.g., smartphones, tablets, laptops)?
Yes ___ No ___

6. Does your business accept credit card payments, other electronic payments or have online bill pay? Yes ___ No ___

7. Does your business allow employees to use personal devices to connect to your network? Yes ___ No ___

8. Does your business train employees on proper email use and other privacy issues?
Yes ___ No ___

9. Does your business store your customers' corporate confidential information?
Yes ___ No ___

10. Does your business have access to online cyber risk management tools?
Yes ___ No ___

If you answered "yes" to one or more of questions 1–9, your business has exposures which may lead to a data breach or some other cyber-related loss. This leaves your business open to claims or lawsuits. Can you afford to self-insure these types of losses?

If your answer is that you cannot, then please contact MrInsurability for help.

We can be reached at 1-630-385-2448 or 1-800-869-9194 or by email at info@mrinsurability.com.

These questions were provided by Traveler's Insurance and
Ponemon Institute 2015 Cost of Data Breach Study
NetDiligence Cyber Claims Study 2014
Ponemon Institute 2015 Cost of Data Breach Study