Our World Today

Technology allows us to connect in previously unimaginable ways, where we can schedule doctor appointments, order food, shop, pay credit cards, and more with the touch of a finger. Our digital fingerprints are everywhere, and businesses collecting all this personal information need to be aware of the risks they face in doing so.

Businesses are retaining and using an exponentially increasing amount of interconnected data, and they have a public responsibility and legal obligation to keep it secure. Opportunistic and innovative cyber criminals have more access than ever before and legislation, individuals and businesses seem one step behind when it comes to protecting their data.

What data is at risk?

PII

Personally Identifiable Information, e.g., social security and driver's license numbers, bank account information, online account user names and passwords, medical and health insurance information.

PHI

Protected Health Information, which is information relating to the provision and payment of health care that can be used to identify an individual.

PCI

Payment Card Information, including debit and credit cards.

Why do cyber criminals steal PII?

In simple terms, PII is valuable. Whether it's stealing employee social security numbers to fraudulently establish new lines of credit or extracting other confidential information to sell on the black market, access to personal and confidential information can be easily monetized.

To protect individuals' personal information, strict requirements have been placed on businesses to pay the costs associated with responding to a data breach. The overwhelming costs and confusing legislative requirements make it difficult for businesses to overcome the fallout of a data breach without assistance.

Key Facts

Malicious actors continually seek new security vulnerabilities to exploit and access valuable and sensitive information. Many companies believe privacy and data breaches won’t happen to them, but three key facts stand:

Fact 1: Breaches are bigger and more costly than ever before

Fact 2: Every industry and size of business is at risk

Fact 3: All organizations are susceptible to both internal and external threats

FACT 1: Breaches are bigger and more costly than ever before

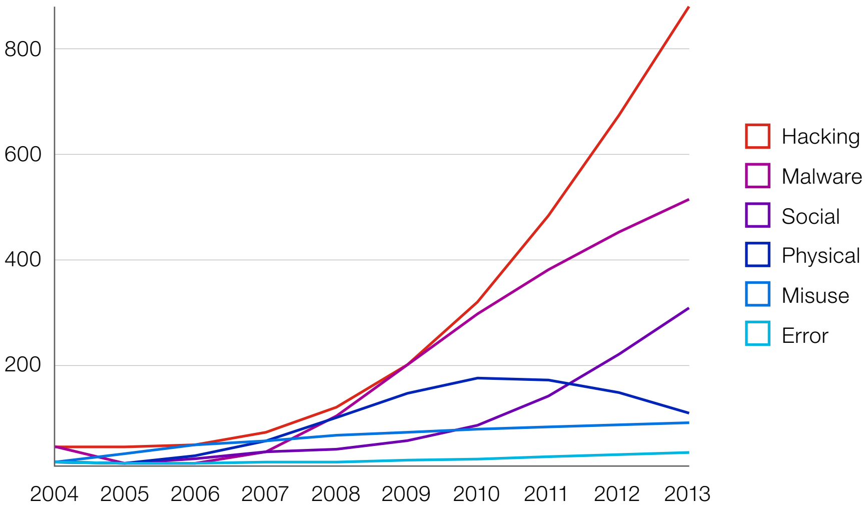
Data breach incidents are becoming larger, affecting more records at one time.

2,144,583,675 records lost to breaches in 2014[1]

375% more breaches compared to 2013[1]

TYPES OF BREACHES OVER TIME

Hacking has become the most prevalent cause of data loss, and the number of hacking incidents is rapidly increasing.[2]



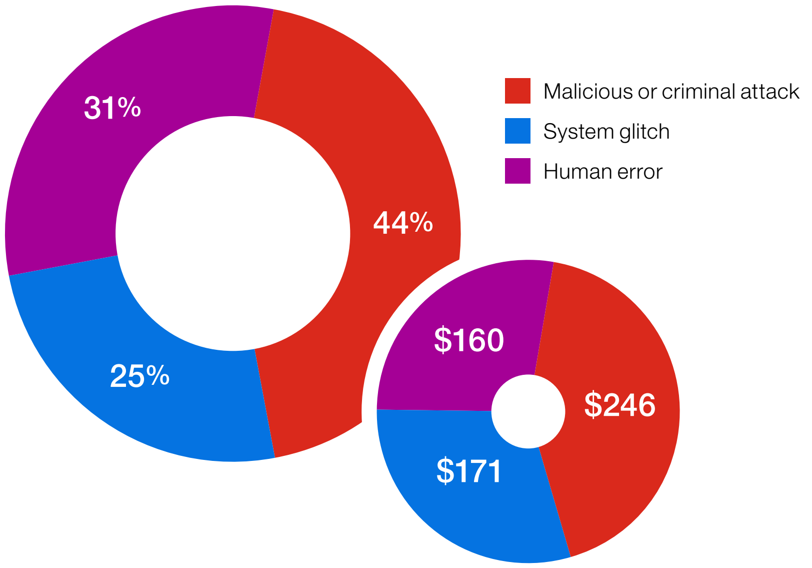
The costs of resolving a data breach are daunting, no matter what size the business. Sources of costs include: detection, escalation, notification, remediation and lost business in both income and reputation.[3]

$

- 2014 average post data breach costs: **$1.6M**
- 2014 average lost business costs: **$3.3M**
- 2014 average records lost per breach: **23,647**
- 2014 average cost per record breached: **$201**

MOST COMMON TYPES OF BREACHES & RELATED COSTS PER RECORD

Malicious hacks are the most common and costly root cause of data breaches. Other breaches are simply errors caused by a system or employee.[4]



[1] Source: http://blog.mint.com/how-to/data-privacy-day-how-to-keep-your-information-safe-infographic012815/?display=wide
[2] Source: verizonenterprise.com/DBIR/2014
[3] Source: Ponemon Institute LLC 2014 Cost of Data Breach Study: United States
[4] Source: Ponemon Institute LLC 2014 Cost of Data Breach Study

FACT 2: Every industry and size of business is at risk

Several industries have emerged as notable targets, making up **nearly half (49%)** of all breaches in 2014.[1] Costs per record breached are higher in certain industries than others.

INDUSTRY	2014 %	COST PER RECORD[2]	INDUSTRY	2014 %	COST PER RECORD[2]
Business & Professional Services	17%	$223	Legal Services	7%	n/a
Retail	14%	$125	High-Tech & IT	7%	$181
Financial Services	10%	$236	Healthcare	6%	$316
Media & Entertainment	8%	$183	Transporation	5%	$286
Construction & Engineering	8%	n/a	Aerospace & Defense	3%	n/a
Government & International Organizations	7%	$172	Other	8%	n/a

60% of small to medium-sized businesses close six months after suffering a breach

Unfortunately, most small organizations also lack the resources to rebound from the costs of managing a data breach.[3]

22% chance of a breach of 10,000 records or less over a two year period

Organizations of all sizes can be affected. Small to medium-sized businesses are especially susceptible since most lack the resources needed to manage their cyber security.[4]

[1] Source: FireEye M-Trends 2015 Report
[2] Ponemon Institute LLC 2014 Cost of Data Breach Study
[3] Source: Stockton, Gary. 'Experian Data Breach resolution Advises Small Businesses to be Prepared for a Data Breach'. Experian Business Information Services. November 2013.
[4] Source: Ponemon Institute LLC 2014 Cost of Data Breach Study

Fact 3: All organizations are susceptible to both internal and external threats

State-sponsored

A group employed by the government of a nation state.

- Chinese government hackers.
- Russian government hackers.
- Syrian Electronic Army.

Script Kiddies

A usually inexperienced person or group acting on their own, and not a member of any other threat category.

- Kid brings down school network ‘for fun’.
- People who deface sites in the hope of impressing someone (rather than for political reasons).
- Unsophisticated groups using pre-fabricated malware or botnets to be malicious.

Hacktivist

An individual or group who performs attacks to draw attention to or hinder support of a cause such as free speech.

- Anonymous.
- Lulzsec.
- WikiLeaks.

Organized Crime

Groups of criminals engaging in illegal activity to extort money or hired to carry out an attack.

- Producers of ransomware.
- Black-market data thieves.

Insiders

Employees or other privileged users associated with an organization.

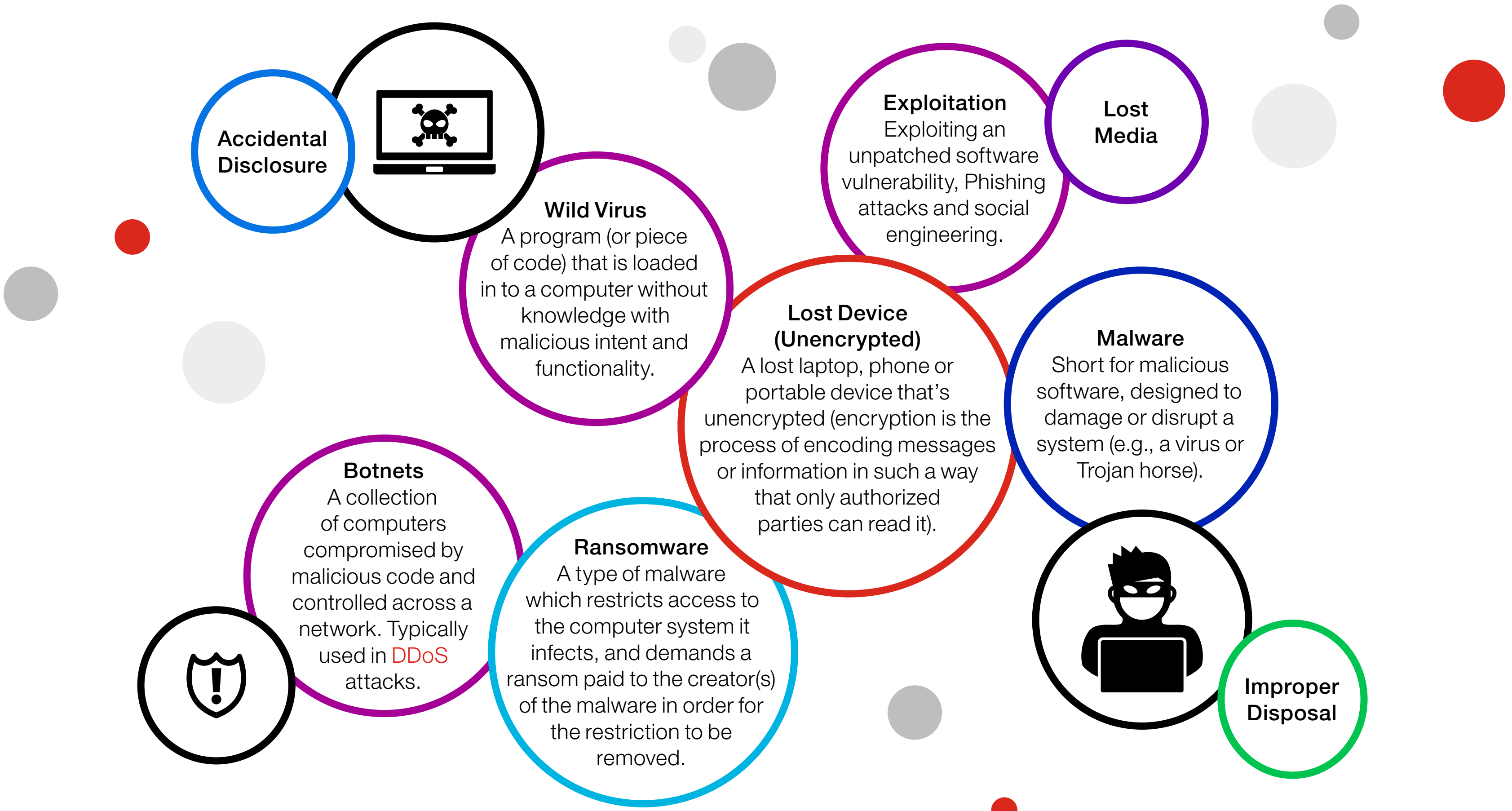
- Contractors.
- Employees.

Cyber terrorist

One who carries out attacks of the purpose of causing fear or panic. Individual is motivated by ideological or political goals or is associated with a known terrorist group.

Source: https://www.surfwatchlabs.com/threat-categories
https://www.surfwatchlabs.com/threat-categories#Actor

Through various methods, cyber criminals infiltrate entities and take advantage of a system malfunction or human error.



Accidental Disclosure

Wild Virus
A program (or piece of code) that is loaded in to a computer without knowledge with malicious intent and functionality.

Exploitation
Exploiting an unpatched software vulnerability, Phishing attacks and social engineering.

Lost Media

Lost Device (Unencrypted)
A lost laptop, phone or portable device that's unencrypted (encryption is the process of encoding messages or information in such a way that only authorized parties can read it).

Malware
Short for malicious software, designed to damage or disrupt a system (e.g., a virus or Trojan horse).

Botnets
A collection of computers compromised by malicious code and controlled across a network. Typically used in DDoS attacks.

Ransomware
A type of malware which restricts access to the computer system it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.

Improper Disposal

The above is not exhaustive of all ways and means used by cyber criminals

Exposures

What are the main exposures individuals and risk managers need to be aware of?

First Party Exposures

Include any expenses resulting from a breach but not requiring a lawsuit:

- Computer forensics expenses (to identify the size and scope of a breach or loss of information) – costs can vary greatly depending on breach size/complexity
- Notification of affected individuals - rates can vary, but many carriers have negotiated rates that range from $1.25 to $5/head
- Credit monitoring after loss of social security numbers - widely available on the open market at upwards of $20/year, but many carriers have negotiated rates in the $9-$13/head/year range
- Regulatory fines and penalties
  - HIPAA – enforced by Health and Human Services and the Office of Civil Rights
  - Fines/Penalties vs. Compensatory Awards
- Public relations expenses
- Ransomware payments for cyber extortions

Third Party Exposures

Include any expenses triggered after a lawsuit is filed by a third party:

- Class-action lawsuits
- Payment card reissuance expenses
- Payment card fraud expenses
- PCI Fines/Penalties
- Identity theft lawsuits
- Loss of third party intellectual property or confidential corporate information lawsuits
- Network disruption suits
- Bodily injury arising from lost data
- Mental distress due to exposure of privacy information
- Negligent transmission of a computer virus/worm or malicious code

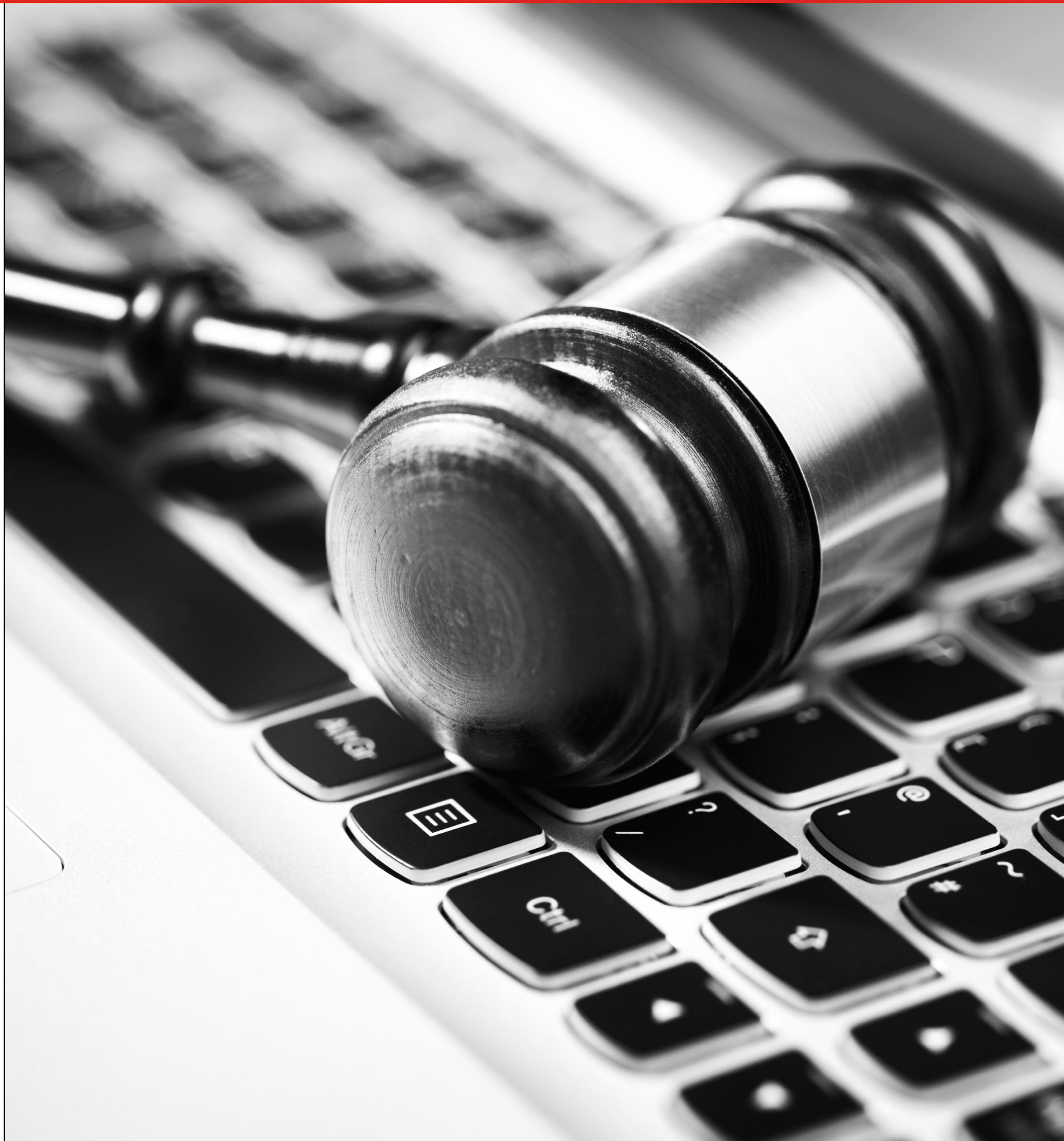
Understanding regulatory exposures

The landscape of federal and state regulations, as well as PCI requirements is constantly evolving based on new exposures and threats.

Federal Regulations

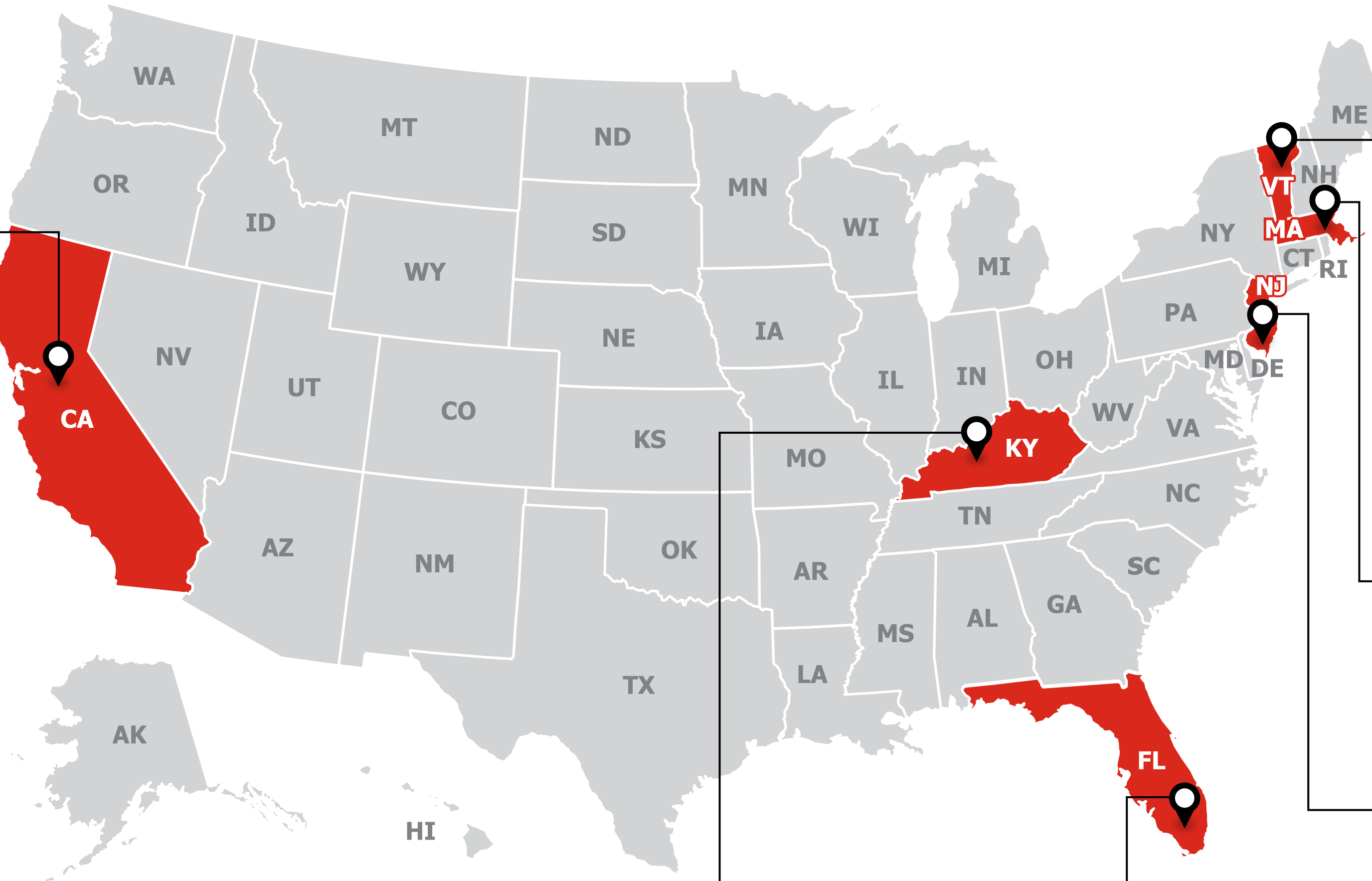
The legislation crafted by the Federal Government to protect individuals and their Personally Identifiable Information (PII). HIPAA, for example, is a set of national standards to protect Protected Health Information (PHI). It applies to 'covered entities' and 'business associates' and considers any unauthorized access of PHI a 'breach'. HIPAA may require notice within 60 days.

Source: John Mullen, Lewis Brisbois Bisgaard & Smith LLP, www.lewisbrisbois.com



State Exposures

Forty-seven states, including Puerto Rico, Washington, D.C. and the Virgin Islands require notice to customers after unauthorized access to PII/PHI, and each state may define PII a bit differently. Notice is typically due ‘without unreasonable delay’ and businesses are subject to high fines for non-compliance or delay. Some states require notification to the state attorney general and/or state consumer protection agencies.



CALIFORNIA

Considers a username or email address and password to be PII.

Now requires the entity providing notice to offer appropriate identity theft prevention and mitigation services if the entity was the source of the breach

Mandates strict health information protection including notice to DPH and affected individuals within 5 business days of learning of breach (an amendment in effect in 2015 changes this to 15 days)

KENTUCKY

Became 47th state with breach notification law in April 2014.

FLORIDA

Requires notice to those affected within 30 days.

VERMONT

Requires notice to affected individuals within 45 days of breach and discovery; notice to AG within 14 business days of breach discovery or affected individual notice (whichever is sooner).

MASSACHUSETTS

Requires a ‘written information security plan’ for businesses storing local personal information.

NEW JERSEY

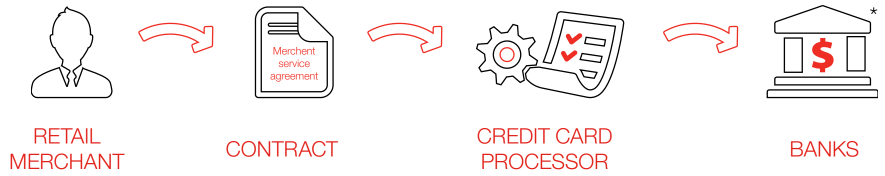
Considers a username or email address and password to be Personally Identifiable Information (PII).

Payment Card Industry (PCI)/ Data Security Standard (DSS) Regulations

The Payment Card Industry Security Standards Council, comprised of Visa, Mastercard, AmEx, Discover and JCB International, is a non-governmental entity requiring merchants and service providers to abide by certain protocols. Fines can be charged to clients who aren't PCI/DSS compliant. Small states have also incorporated PCI/DSS requirements into data protection laws.

Violations of PCI/DSS have multiple consequences: payment brands will fine acquiring banks $5,000 to $100,000 per month for non-compliance and banks will often pass these fines off to the merchant.

The payment processors have a motive not to get stuck with the indemnities in the event of a breach and banks want to pass on the liabilities to other parties. If one's merchant services or payment processing agreements aren't in his or her favor, the business could incur all indemnification costs, including fraudulent charges and costs of re-cutting cards.



RETAIL MERCHANT

CONTRACT

CREDIT CARD PROCESSOR

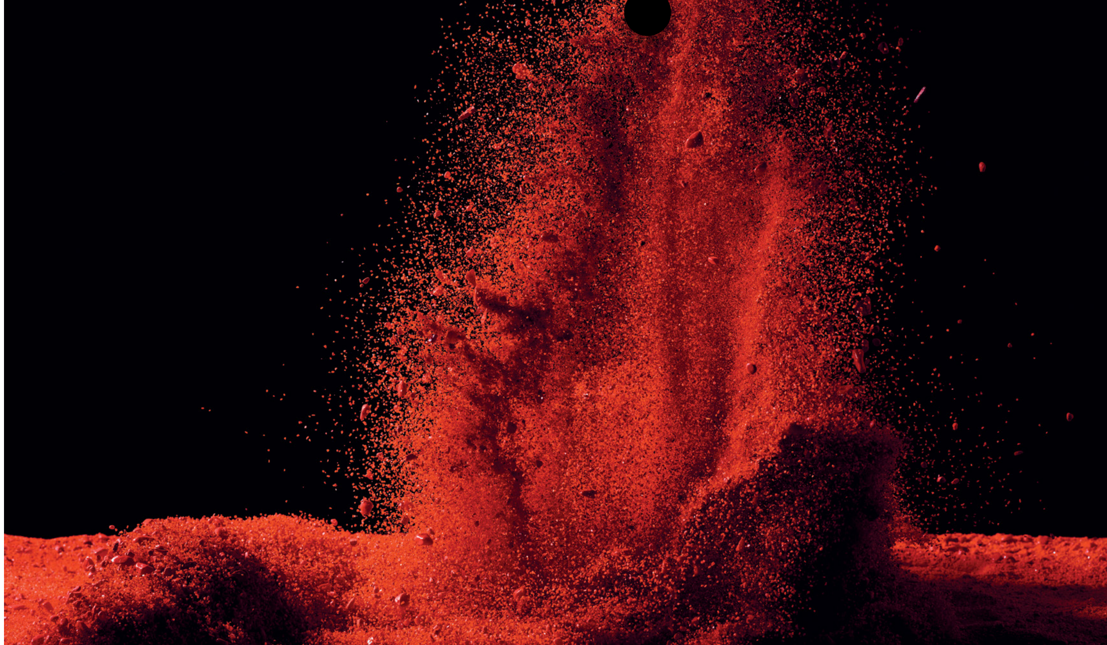
BANKS

I only process 100 cards annually, must I be PCI compliant? How do I become PCI compliant?

According to the PCI Compliance Guide, PCI applies to ALL organizations or merchants that accept, transmit, or store any cardholder data, regardless of the size or number of transactions. Companies that are found to be out of compliance can be subject to fines and penalties from the payment card brands. Consult the PCI webpage to determine the applicable merchant level as well as the steps needed to be taken to satisfy the compliance requirement.

I am PCI compliant, so if there is a breach I won't be held responsible, correct?

Not necessarily. Being PCI compliant means the appropriate controls are in place to secure payment card transactions and storage, including regular audits of these controls to be up with the evolving industry. Being PCI compliant will lessen the punitive costs imposed by the card issuers, and will more importantly keep security up to date.



Consult the PCI website to determine the applicable level of compliance required as well as the steps required to become compliant https://www.pcisecuritystandards.org/

*the chart is a sample and is oversimplified. Other intermediaries or arrangements may be present.

Coverage

What coverage is needed to insure the many exposures facing businesses today?

There is no 'one size fits all' approach to adequately insure privacy exposures. Companies must each assess their own exposures and purchase coverage that specifically caters to the risks inherent to their specific business.

Privacy protection

Covers costs to defend and resolve claims with regard to the handling of personally identifiable or confidential corporate information. Covers negligence, violation of privacy or consumer protection law, breach of contract and regulatory investigations. Covers issues resulting from the failure of network security, including the negligent transmission of a virus and the inadvertent participation in a DDoS attack against a third party.

Breach costs

Coverage for costs associated with responding to a breach, such as forensic costs to confirm and identify the breach, costs to notify affected individuals, credit protection services including costs to staff a call center for redemption of monitoring offers, and crisis management and public relations costs.

Cyber business interruption

Covers financial loss, such as business income when a company has its network-dependent revenue interrupted. Traditionally, this has been for fire, flood, etc. but technology growth has created new BI perils (viruses, tech failures, programming errors and computer hacking).

Hacker damage

Covers costs to recreate or repair damaged or destroyed data, systems or programs. In a digital world, property is no longer exclusively tangible, so specialized coverage is needed to pay for intangible data recovery costs.

Cyber extortion

Covers the response costs and financial payments associated with network-based ransom demands. With the proliferation of ransomware such as Cryptolocker and anonymous currencies such as Bitcoin, network extortion demands are on the rise. In the digital world, intangible assets are 'kidnapped' and extorted with threats to shut down a system or divulge sensitive or proprietary information.

Multimedia liability

Costs to defend and resolve claims related to online content, such as defamation or trademark or copyright infringement.

Risk Management

A holistic approach to privacy security is necessary to mitigate the risk of a data breach and decrease the damage when a breach occurs. A strategic approach to data breach prevention and response involves a combination of best practices, insurance and a response plan.

Why does Risk Management matter?[1]

- Having a strong security posture has been shown to reduce the average cost of a data breach by $14.14 per record
- Appointing a CISO has been shown to reduce the average cost of a data breach by $6.59 per record

How can companies mitigate their risk?[2]

- ✓ Make privacy and data security a part of the organization's corporate culture
- ✓ Assign ultimate data privacy and security responsibility to one person
- ✓ Implement a continuous workforce training and awareness program
- ✓ Strengthen contracts with vendors and business associates
- ✓ Identify and classify the types of information collected and stored by the organization
- ✓ Collect and retain the minimum amount of personal information necessary
- ✓ Review and update existing data security policies, plans and procedures
- ✓ Conduct continual risk assessments and consider ways to avoid or mitigate the risks identified

    — Administrative safeguards
    — Physical safeguards
    — Technical safeguards

- ✓ Prepare for data security incidents
- ✓ Mitigate risks with cyber insurance

[1] Ponemon Institute, 2014 Cost of Data Breach Study
[2] ePlace BreachProtection™

Claims Scenarios

Every company has risks associated with privacy. Consider these scenarios in which a company might incur losses if privacy is breached.

Accounting firms
A backup drive containing the names, addresses and social security numbers of all of the tax preparation clients of an accounting firm is lost. Because the drive contained personally identifiable information, each client has to be contacted and offered credit monitoring services, even though the information is never disseminated.

An accounting firm's computer system is hacked, compromising payment information of hundreds of clients. The firm is required to absorb the cost of notifying all of the affected clients and the cost to issue new credit cards.

The computer system of an accounting firm is hacked. The social security numbers and other financial information from the tax returns of several thousand customers is compromised, as is the employee information from all of its regular and seasonal employees. The firm must notify all of the affected parties and provide credit monitoring services.

Advertising firms
A disgruntled employee at a digital advertising agency provides confidential per-click tracking data to a competitor of the agency's client. The client sues the agency for breach of contract and negligence.

An advertising agency creates a new ad campaign for a high-profile client. The campaign is inadvertently leaked prior to the planned launch date, and the client sues the agency.

Agriculture
An employee of a feed supplier loses a laptop computer that contains sensitive data, including billing information, of its customers. Even though it is never proven that the data was ever used, the supplier is responsible for notifying all of the companies whose data was affected.

The computer system of a large commercial farm is hacked. Sensitive data, including names, social security numbers and dates of birth, is compromised. The farm must notify all of its regular employees and well as seasonal workers, and provide credit monitoring services.

Biotechnology and Pharmaceutical firms
A pharmaceutical company is in the midst of a large clinical trial for a promising drug. Their computer system is hacked, and sensitive patient information, including social security numbers and medical information, is compromised. The company has to notify all of the affected patients and offer credit monitoring, and they have to cancel the study and start again.

A biotechnology firm is working on a new genetically modified food product. Details of the research are inadvertently leaked by email to a media outlet prior to the completion of the study. The food manufacturer sues the lab.

Construction
A construction company's computers are infected with a virus that is inadvertently transmitted to its prospects, customers and suppliers. The company is liable for the costs that those companies incur to remove the virus and restore their data.

The confidential design plans for a new multi-use development are leaked to a competitor by a disgruntled employee of the company that has the construction contract. The developer sues the contractor for breach of contract since they signed a non-disclosure agreement.

Consulting firms
A laptop belonging to a human resources consulting firm is lost. The data on it includes names, addresses and social security numbers of hundreds of contract employees. Even though the information is never disseminated, the consulting firm is required to notify the affected employees and offer them credit monitoring services.

A management consulting firm places several consultants at a client site during a project. One of the consultants inadvertently circulates a confidential memo to a large email list including internal and external recipients. The client sues the consulting firm.

Energy
The computer system of a solar energy provider is hacked and the payment information of all of its customers, as well as sensitive personnel information, is compromised. The company must bear the cost to notify everyone affected and to provide credit monitoring services.

Entertainment
An employee at a recording company inadvertently releases the new single of a popular artist to several free music sharing sites. The artist sues the company for lost royalties for the song.

Gaming
A game hosting company is hacked, and several popular gaming sites are down for several days. The game designers sue the hosting site for lost royalties.

A popular online game franchise is preparing for the release of a new version of its flagship product. A demo version is supposed to be available for download, but the full version is made available instead, and thousands of users are able to download it for free. The developer, marketer and others suffer lost revenue.

Government agencies
The computer system of a government agency that oversees a program for adults with disabilities is hacked. The personally identifiable information of the clients of the program is compromised. The agency is required to notify the affected clients and their caregivers or guardians, and provide credit monitoring services.

Labor management trusts
The computer system of a labor management trust is hacked and sensitive data on all of the members is compromised. The trust is responsible for

notifying all of the affected members and providing credit monitoring services.

Law firms

The computer system of a law firm is hacked, and confidential information about a high-profile divorce case is leaked to the media. The firm is sued by both parties in the divorce.

A new employee at a law firm disposes of a printout of confidential client payment information in the office building's communal recycling bin rather than shredding it. The firm was responsible for notifying the clients that their information may have been compromised and was required to provide credit monitoring.

A laptop belonging to a law firm that specializes in class action suits is stolen. It contains sensitive information, including social security numbers and medical history, of a large number of claimants in a suit against a medical device manufacturer. The law firm is liable for notifying the claimants and providing credit monitoring services.

Manufacturing

An inventor contracts with a manufacturing company to do a small production run of a product on which the inventor does not yet have a patent. An employee of the manufacturing firm inadvertently sends an email which includes the product's specifications to a list that includes potential competitors. The company is sued for breaching the non-disclosure agreement and other damages.

The computer system of a manufacturing firm is hacked, and the sensitive data of all of its full time employees and contract workers is compromised. The company must notify all of the affected workers and provide credit monitoring.

Media firms

A media firm develops a comprehensive media plan for a client's new product. An email that includes confidential details about the product, intended for the client, is inadvertently sent to the firm's press distribution list instead, and the product details are publicized well ahead of the launch. The client sues the media firm for breach of contract and other damages.

The computer system of a media firm contains large amounts of data on its clients' analytics, including search engine optimization keywords, pay-per-click campaigns, etc. The system is hacked and all of the data is at risk. Several clients files lawsuits alleging negligence.

Not-for-profit organization

A laptop that contained the donor list of a not-for-profit organization is lost. The agency is required to notify everyone whose name is on the list and provide credit monitoring, even though the information is never disseminated.

Professional service firms

An architectural firm produces plans and specifications for a new office building. The general contract misreads the specifications and uses inferior quality materials. The problem is not discovered until after the building is occupied. The building owner sues the architect for negligence.

Publishing firms

A well-known author writes a new book in a different genre using a pen name. The firm that publishes the book signs an agreement not to reveal the author's true identity, but the information is leaked to the press by a disgruntled employee. The author sues the publishing firm for breach of contract.

The computer system that processes the orders of an e-book publisher is hacked and sensitive payment information is compromised. The company is liable for the costs to notify all of its customer and offer one year of credit monitoring.

Retail merchants

A retail store's point of sale system is hacked, and the credit and debit card numbers of thousands of customers are exposed. The store is required to notify the card issues, pay to replace the cards, and offer credit monitoring services to those whose account numbers were compromised.

Tech developers

A developer loses a back-up drive that contained the code for a new application. The client sues the developer for negligence and for the delay in the project's schedule that resulted.

Tech service providers

A technology service provider has a service outage that caused the websites and intranets of several clients to crash. The service provider is sued for business interruption costs and the cost of recovering lost data.

Telecommunications

A telecommunications provider's computer network is hacked and the payment information of thousands of customers is compromised. The provider is required to notify all affected customers, pay for the cost to reissue credit cards, pay for fraud charges, and provide credit monitoring. It is also subject to fines for failing to encrypt sensitive data.

Unions

A laptop containing personally identifiable information about retired union workers and their pensions is lost. Even though the information is never disseminated, the union is required to notify all of the affected retirees and provide them with credit monitoring services.

Website development

A developer designs a new website for an ecommerce company. When the site is launched, it immediately crashes. The site is down for three days while the developer fixes the problem. The company sues the developer for the lost revenue.

A health insurance broker launches a new website and the password requirement does not work properly, allowing anyone to access personally identifiable information about members. The insurer sues the developer for their costs to notify members and provide credit monitoring.

FAQs

A lot of confusion exists around privacy. Our underwriters are here to help answer the most common questions clients ask brokers regarding privacy exposures and coverage.

PRIVACY INSURANCE 101

What is a client's exposure? Generally, the typical exposure includes personally identifiable information in their custody – from employee social security numbers and drivers license numbers, to payment cards accepted for fees, goods and services, exposure to clients' sensitive data, healthcare records collected, etc.

Why do you need to know how many records a company has? The higher the number of records, the higher the exposure and the higher the potential costs post-breach.

WHY DOES MY CLIENT NEED A PRIVACY POLICY

I got an endorsement to my other policy for this. Isn't that enough? Maybe, but usually not. Most endorsements are for a very small dollar amount with very limited coverage. For example, only third party costs may be covered, or the maximum coverage for first party costs may be only $50,000. Every company would benefit from a full privacy/data breach policy, providing the peace of mind that comes with knowing that the costs of a potential breach won't be catastrophic to the business.

If my only real exposure is first-party data (such as. employee data), do I really need a policy? All companies have the duty and obligation to safeguard the information they hold on behalf of their employees as well as any confidential information about the business itself. No company is immune from attacks. A Hiscox policy provides coverage for employee data.

I am not a target like Sony, Anthem or Home Depot. Why should I worry? Large corporations make the news. Small ones don't. It's a matter of 'when', not 'if' a company will have a breach of data. There's a black market where these records are sold and bought, and hackers are only getting savvier. Target, Home Depot, Anthem, and other large organizations have entire departments devoted to analyzing the risks the company could face and helping set policies and procedures to protect against them, and their systems and data have still been breached. Smaller companies without someone responsible for network security and the resources to protect their data are easy targets for hackers

Who buys cyber coverage? Companies who are mitigating this growing risk. It is becoming a must-have coverage.

Why shouldn't I trust my IT Department when they say they have it covered? Target, Sony, and other large corporations have entire departments devoted to IT security, and they did not have it covered. A simple error or omission like not updating software, not setting appropriate user authentication procedures for third party vendors, losing an unencrypted laptop that stores sensitive data, or a rouge employee with malicious intent can all lead to a breach. Exposures grow as technology expands, and hackers are only getting smarter and better.

Do I need this coverage if I don't store any client information on my network? Yes. You may not store client data, but you may have access to it. You may cause a breach of your client's data, consequentially breaching a contract. Corporate information is also covered under a privacy/data breach policy. Employee data is also a liability.

My company is really small. Am I still at risk of a data breach? Every company has data breach and privacy exposures, either through employee sensitive information, payments accepted from third parties, services provided, etc. Some have more exposure than others, but it's important to emphasize that every company with employees is liable for third party data (including employee data). A breach costs an average of $188k, for the smallest companies with the smallest exposure. Costs add up very quickly.

I outsource my payment card processing to a third party. I don't have any payment card exposures do I? According to the PCI Compliance Guide, PCI applies to ALL organizations or merchants, regardless of the size or number of transactions, that accept, transmit, or store any cardholder data. And merely using a third-party company does not exclude a company from PCI compliance. It may cut down on the risk exposure and consequently reduce the effort to validate compliance but it doesn't mean a merchant can ignore PCI.

If my client information is stored in the cloud, the liability rests with the cloud provider, right? Not exactly. It would be in the insured's best interest to carefully review those contracts with their legal counsel. Even if the risk is mitigated, the liability may still fall on the shoulders of the insured.

KEY FACTS

What industries traditionally buy, and what industries are newly buying? Currently the most heavy users of liability insurance are in the banking, healthcare, and technology fields. New purchasers are businesses of all sizes and industries, including governments, schools, and manufacturers.

What is the average cost of a data breach? The average cost of a data breach continues to fluctuate but reputable cyber security and information sources peg the average breach at roughly $188,000. The bigger the company, the bigger the costs. Also, the more sensitive data the company collects (regardless of the size of company), the higher the costs.

EXPOSURES

What does cyber crime cover? Cyber crime contemplates the following scenario: A hacker disguises themselves as a vendor, client, or employee and tricks the Insured's employee into transferring funds to the hacker's account. This deception can be perpetrated through phishing, spearphishing, and other tricks perpetrated through email, text message, instant message, telephone, or other electronic means.

What is considered a record? What if I have multiple files for the same person in my possession? Do you require the total number of records or just the number of individuals? Non-public individually identifiable information as defined in any federal, state, local, or foreign statute, rule or regulation, may include but is not limited to unsecured protected health information, social security number, individual tax ID number, driver's license number or state ID, passport number, financial account number or credit or debit card number. We would like to know the total number of pieces of individual information an insured possesses. If multiple pieces of information for the same individual are stored within the insured's network or on the insured's premises, we would like details on the retention and duplication procedures in place.

How much does the coverage cost? It depends on size and exposure. A $1M policy could cost as little as $1,000.

Do privacy policies matter for websites? Yes, because they are in many ways constructively a contract with your customers. More importantly, if you do not disclose your data privacy procedures and who you share others' data with you could be in violation of several privacy related laws.

What is the difference between regulatory defense and the regulatory compensatory award? The regulatory action defense addresses claims brought by a regulatory body, such as the Office of Civil Rights for HIPAA violations. If a breach does indeed occur, the regulatory body will set up something that acts a lot like a trust for the affected individuals of the violation. In practice, if individuals' data was breached and an entity violated HIPAA, the OCR will levy a fine for their violation. The fine will be paid directly to the OCR, and will not address "victim" compensation. The OCR will then set up a this trust-like fund for the medical group to pay into that will be distributed to those individuals for their "damages."

Generally, what regulations are companies subject to? For payment card data, PCI DSS. For healthcare data, HIPAA. These, in addition to social security numbers, financial records, etc., are also subject to state and federal regulations.

Why is PCI compliance important? What happens if I'm not PCI compliant? Outside of the specific fines and penalties levied by the card brands, a non-compliant business would open themselves up to various third party suits from angry consumers whose information was breached.

My POS vendor says they're PCI compliant. That makes me compliant, right? Not necessarily, most merchants have some exposure. The only way to totally eliminate the need to become PCI compliant is through full outsourcing of your entire payment handling process. In most cases the processing uses at least some of your network infrastructure. This subjects merchants to the standard of PCI compliance.

What is the difference between a PCI fine and an assessment? The payment brands (Visa, Mastercard, etc.) may, at their discretion, fine $5,000 to $100,000 per month for PCI compliance violations. These amounts are intended to be punitive in nature and don't address indemnifying the banks for their losses resulting from a payment card breach. PCI Assessments are liabilities and costs detailed in a Merchant Services or Payment Processing Agreement, which may include costs associated with card reissuance and fraudulent charges experienced post-breach.

COVERAGE

What is the difference between first party and third party coverage and when is each important? First party coverage includes costs incurred by the insured, such as notifications sent out to each individual, computer forensic specialists hired to figure out how the breach occurred, remediation, business interruption, etc. Third party costs may include class action suits, and other claims brought by those outside the company

What is considered confidential corporate information if you exclude trade secrets? Confidential corporate information would refer to information that if disclosed may harm the business. This may includes sales and marketing plans, product plans, notes associated with various designs and inventions, customer and supplier information, financial information, etc., that is non-public in nature.

What coverage should I consider? First and third party coverage. This includes costs for notification, forensics, regulatory fines and penalties, PR consultants, third party suits, etc.

What limits should I consider? That depends on they company's size and exposure. The larger the company and the more sensitive data they hold, the higher the limits.

What is "Per Person" coverage? Rather than setting a dollar value to notification and credit monitoring costs, the insurer sets a number of maximum individuals they would cover for these costs (no dollar value set).

Does a cyber insurance policy cover the direct loss of funds? Most cyber insurance policies are crafted to cover the loss of information, not money (directly). At Hiscox, we can cover certain perils via endorsement to respond to these exposures. Our Cyber Crime offering is built for "data" events where banking credentials are stolen and utilized to transfer uninsured funds from a corporate bank account or other institution. Other coverage is also evolving to respond to instances where hackers trick employees into voluntarily releasing funds on behalf of the organization, but the funds are sent to the hacker due to a spoofed invoice or other method of deception.

Does the policy cover 'social engineering?' Social engineering can be defined as an attempt to obtain otherwise secure data by conning an individual into revealing secure information. Victims of social engineering attacks are typically vulnerable due to the innate desire to trust other people and be helpful. Most insurance policies cover the loss of data regardless as to how it is obtained, though the policy wording should always be checked.

Does the policy cover a rogue employee event? Most insurance policies cover the loss of data regardless of how it is exposed. With that said, certain policies may exclude rogue employee events. Under the Hiscox suite of privacy insurance policies, a standard rogue employee event is covered subject-to policy terms and conditions, but certain events involving executives of the organization may be excluded.

Does the policy cover paper records? Most all privacy insurance policies cover paper records, but policy wording should always be reviewed. The Hiscox Privacy Protection insurance policy defines Personally Identifiable Information as information in any form, that is in your care, custody or control, or in the care, custody or control of any third party for whom you are legally liable. A breach of paper records would be covered by the standard Hiscox policy wording.

If paper records are destroyed is coverage considered under the Hacker Damage module or does that consider the destruction of digital assets only? Our Hacker Damage Module is triggered by a Hacker Damage Event whose definition includes "…data you hold electronically." Paper records would not be covered. These events include the malicious authorized access of a website, intranet, network, computer system, etc.

Is coverage worldwide? What does that mean? Must the suit be handled in a court in the USA? We provide worldwide coverage but our jurisdiction in claims handling is restricted to the United States courts.

Does the policy cover offline exposures too? Policies cover online and offline/paper data.

Can you offer drop down sublimits when writing excess insurance policies? Yes; we can drop down over primary policy sub-limits. Terms and conditions will need to be underwritten by your regional Hiscox underwriter.

RISK MANAGEMENT

Why does employee training matter? A significant number of losses actually arise from employee negligence, whether it's leaving a laptop in a cab or plane, accidentally emailing PII to the wrong email address, or simply verbally disclosing private information about individuals in a public setting. Employees must learn to treat such information with discretion and care.

Why do merchant service agreements matter? The agreements you sign with payment processors will often pass through liability owed to banks in the event of a payment card breach. The fine print may have you agreeing to much more than you think.

What is encryption? It's the process of encoding information in such a way that only authorized parties can read it. Encryption is very important in evaluating a company's risk and exposure, since a breach of encrypted data is significantly less costly than a breach of unencrypted data Encryption is a safeguard in many cases with regard to privacy protection law obligations.

Our laptops are password protected. Isn't this enough? Does that mean they're encrypted? No. Encryption is the process of scrambling the actual data on a hard drive so that it is unusable unless accessed with an encryption key. Only password protecting a laptop simply means a hacker can bypass the password to access intact data that hasn't been encrypted.

What is the difference between encryption and password protection? How does my company encrypt data? Encryption is a method of encoding messages or data with coded strings of symbols. It is commonly used to secure online banking sessions and protect credit card data. When you bank online, a 'lock' icon routinely appears in the address bar which means the browser session is encrypted by the bank. Often on mobile devices, passwords are used to enable encryption. Apple has started encrypting personal data on the latest operating system, iOS 8, if the correct settings are enabled. A number of vendors offer encryption of corporate data and insureds should consult their risk manager for further information on how to implement this additional security protocol.

What are your value added services? We have partnerships with BreachProtection.com and the eRisk Hub, all complementary to our insureds. BreachProtection.com provides comprehensive risk management policies, procedures, training, and other tools for pre-breached insureds. This includes online compliance material, email updates, procedures and sample forms, workforce training, data breach response plans, and full phone support. Our eRisk Hub, powered by NetDiligence, provides breach response resources and tools to help our insureds understand the exposures, establish a breach response plan, and minimize the effects of a data breach organization. They include a Breach Coach and a Breach Response Team as well.

Glossary of Terms

Here are some key terms related to data breach and privacy insurance.

APT (Advanced Persistent Threat) – An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objective by using multiple attack vectors (cyber, physical and deception). APT attacks can be conducted by foreign nation-state actors that have a continual focus on penetrating a specific target.

ASP (Application Service Provider) – A third-party entity that manages and distributes software-based services via the internet from a central data center.

Authentication – The process of verifying the identity or other attributes of an entity. May also be utilized in Multi-Factor Authentication, which refers to the process in which multiple factors are utilized when identifying and authenticating an individual.

Blackhat – Used to describe a hacker who breaks into a computer system or network with malicious intent.

Blacklist – A list of entities or individuals who are blocked or denied privileges or access.

Bot – A computer connected to the Internet that has been secretly compromised with malicious code to perform activities under remote command and control of a remote administrator (or hacker).

Botnet – A collection of computers compromised by malicious code and controlled across a network. Typically used in DDoS attacks (definition below).

Breach (Data) – A security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches are also subject to state specific definitions that may also govern when certain types of breach responses are required.

Breach Costs – The costs associated with Breach Response services. These (typically) insurable amounts can include computer forensics services, notification services and credit monitoring services. Breach costs are considered a “first party” insurance coverage and are typically triggered by a breach event, rather than a lawsuit. Insurance policies may offer these services on a voluntary basis or only in response to a breach of information that triggers certain state or federal data breach laws.

Breach Response – The act of responding to a data breach. Companies may have predefined breach response plans that articulate a step-by-step plan of action to respond to a breach.
The scope of these plans typically include many escalation phases, including Incident Analysis, Incident Disclosure, Loss Mitigation and Communication/Remediation. Insurance carriers may provide third party vendors to navigate this process in the event of a breach.

Brute Force Attack – A trial and error method used by applications to decode encrypted data such as passwords by checking all password combination options by methods such as a dictionary attack. This primitive hacking/cracking method is very time consuming and can be thwarted by basic security controls.

Children’s Online Privacy Protection Act (COPPA) – Federal Trade Commission (FTC) legislation governing websites that are collecting information from children under the age of thirteen.

Cloud Computing – The general term to describe the delivery of hosted services over the internet. Cloud computing enables businesses to consume computing resources as a utility, similar to a telephone service, rather than building and maintaining their own hardware infrastructure.(See Infrastructure as a Service and Platform as a Service)

Cloud Hosting – The general term to describe a service where data and resources are stored by a hosting facility. Cloud infrastructure may be set up as public, private or hybrid deployments. Benefits typically include redundant data storage, no single point of failure, flexibility and affordable pricing.

Collocation (or Co-location) – Refers to the practice of businesses leasing real estate, cooling, power and bandwidth from a hosting facility that allows them to place their own resources (servers, storage) with the hosting facility’s environment (typically in secured cages). Most collocation facilities also offer high-security, fire detection, filtered power and backup generators to ensure business continuity.

Computer Forensics – The application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. These investigations are the first line of defense when identifying the size, scope and cause of a data breach.

Credit Monitoring – A service offering that involves monitoring credit activity for individuals. Service is typically offered based on a monthly charge and will notify individuals of suspicious credit activity pertinent to their identity.

Critical Infrastructure – Terminology referring to the underlying framework of facilities, systems, sites and networks necessary for functionality.

Cryptography – The act of protecting information by transforming it into an unreadable format (cipher text). The cipher may be converted into legible formats (decrypted) through the usage of a secret key. There are various forms of encryption and key distribution that may be utilized, including the widely-distributed format, PGP (Pretty Good Privacy).

Cyber Deception – The act of deceiving an individual into releasing sensitive data or funds through the usage of various techniques such as spear-phishing, phishing and e-mail hacking.

Data Aggregation – The concept of enormous volumes of sensitive information being centrally transmitted or stored in a centralized repository.

DDoS – Acronym for Distributed Denial of Service Attack. This is an attack where multiple compromised systems are used to flood a target with network traffic, thus causing the targeted network to experience an outage.

Dumpster Diving – The act of physically trolling through trash in an attempt to discover improperly discarded sensitive information.

EMR – Acronym for Electronic Medical Records. The term is typically utilized when referring to electronic records management systems employed by the healthcare industry.

EMV – Acronym for Europay, MasterCard and Visa. It is a global standard for inter-operation of integrated circuit cards (or “chip cards”) deployed by the payment card industry for use with card-present point of sale (POS) systems.

Encryption – The process of encoding messages or information in such a way that only authorized party can read it. This tactic does not necessarily thwart interception, but denies the interceptor access to deciphering the content. *See: Cryptography*

Exploit – Term referring to a security vulnerability. A security exploit is an unintended and unpatched flaw in software code that exposes the software to potential unauthorized access or compromised integrity.

Firewall – A system utilized to prevent unauthorized access to or from a private network. Firewalls may be implemented through both hardware and software.

First Party (Insurance Coverage) – Coverage granted to indemnify an insured for losses not triggered by a third-party lawsuit. In general, this classification refers to notification, credit monitoring, cyber business interruption, data asset and cyber extortion coverage grants.

Firmware – Software written onto read-only memory (ROM), which is integrated into hardware components.

FTP – Acronym for File Transfer Protocol, which is a methodology for exchanging/transmitting files over the internet.

Hacktivism – Terminology referring to the motivations behind certain hacking events. Hacktivists may be politically or socially motivated, rather than acting with financial gain as a primary motivator.

Hardware – Computer hardware typically refers to objects that you can physically touch, such as drives, screens, boards and chips.

Hashing – Transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is commonly used to index and retrieve items in a database because it is quicker to find the item using the shorter hashed key. It is also utilized in many encryption algorithms.

HIE – Acronym for Health Information Exchange. Refers to the mobilization of healthcare information electronically across organizations within a region, community or hospital system. The term may also refer to the organization that facilitates the actual exchange.

HIPAA – Acronym for Health Insurance Portability and Accountability Act of 1996. Portions of this law are dedicated to the protection of confidential health information, in addition to helping the healthcare industry control administrative costs.

HITECH (HIPAA) – Acronym for the Health Information Technology for Economic and Clinical Health Act. Enacted as part of the American Recovery and Reinvestment act of 2009, it was created to stimulate the adoption of electronic health records.

IaaS – Acronym for Infrastructure as a Service. Defined as computer infrastructure being delivered as a service (over the internet).

Incident Response Plan – A plan put in place by an organization with the intent to organize the approach to addressing and managing the aftermath of a security breach or attack. These plans typically define what constitutes an incident and step-by-step processes regarding timelines, roles/responsibilities, contact information and other components required to manage a breach situation.

Intrusion – Refers to evidence of a system intrusion by an outsider not permitted to have access. May be identified utilizing an intrusion detection system, or IDS.

Key – With regard to encryption, the key refers to the information required to decrypt an encryption cipher and convert the information to legible data.

Keylogger – Malware (Virus) used to log the keystrokes input into a computer. This surveillance software usually has the capability to encrypt the key logs and hide the transmission of this data to a hacker.

Malware – Shortened verbiage referring to malicious software. This software typically is designed to damage or disrupt a system, such as a virus or Trojan horse.

Notification – In cyber insurance terms, notification refers to the notice given to the affected pool of individuals whose information has been exposed in a data breach. As of March 2015, 47 states have notification laws governing what constitutes personally identifiable information and when notification of the affected individuals is required. There are also various forms of proposed federal legislation currently being debated.

PaaS – Acronym for Platform as a Service. This is an internet-delivered model for a computing platform being delivered as an outsourced service, in place of a company managing their own hardware/software.

PCI – Acronym for Payment Card Information. The PCI SSC defines 'cardholder data' as the full Primary Account Number (PAN) or the full PAN along with any of the following elements: Cardholder name, Expiration Date, Service code. Sensitive Authentication Data also requiring protection includes full magnetic stripe data, CAV2, CVC2, CVV2, CID and PINs, amongst other information.

PCI DSS – Set forth by the PCI SSC, the PCI Data Security Standards define the minimum level of security required of any organization handling payment card transactions. As of March 2015, there are four levels of PCI DSS, each of which is derived from the annual volume of payment cards handled by a business. PCI Level 1 is the highest standard of compliance required by the PCI SSC, with PCI Level 4 being the least onerous (due to light payment card volume). Additional information can be found here: https://www.pcisecuritystandards.org/

PCI (Standards Council) – The governing body of PCI. The PCI Security Standards Council (PCI SSC) was formed in September of 2006 by American Express, Discover Financial Services, Japan Credit Bureau, MasterCard Worldwide and Visa International. As of August of 2014, the PCI SSC website lists 688 "Participating Organizations".

PCI Assessments (Compliance) – An audit for validating compliance with the PCI DSS (defined above). In certain circumstance, self-assessments may be allowed for lower volume merchants. In most higher card volume situations, full (or on-site) assessments may be required. Compliance assessments may be conducted by a qualified security assessor, or QSA (defined below).

PCI Assessments (Charges) – Monetary amounts that breached businesses are compelled to pay as a result of a payment card breach. These amounts may include card reissuance fees and unrecoverable fraud charges experienced on the stolen cards. These amounts are typically passed to the breached business through their contracts, specifically Merchant Services Agreements (MSA) or Payment Processing Agreements. Since the banks issuing payment cards do not contract directly with businesses accepting payment cards from customers, these charges are typically passed through a contractual chain, with the payment processor sitting in the middle. Certain insurance policies will expressly cover these breach of contract-driven expenses, while others may not.

PCI Fines and Penalties – Monetary fines/penalties acquiring banks levy as a result of PCI compliance violations. Fines may range from $5,000 to $100,000 per month, details of which are not openly discussed nor widely publicized.

PCI QSA – Approved businesses that can offer PCI Compliance Assessments to certify a businesses compliance with the PCI DSS. Approved Qualified Security Assessors, or QSA companies, may be found here: https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Packet – A unit of data routed between an origin and a destination of a network (or the internet).

Penetration (Pen) Testing – The act of utilizing a "White hat" hacker (or script) to attempt a network penetration. This preparedness technique can expose vulnerabilities otherwise unknown to a business.

PHI – Acronym for Protected Health Information. This constitutes any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

Phishing – A technique utilized by hackers or other individuals with dubious intentions where the perpetrator falsely claims to be a legitimate contact in an attempt to scam the user into surrendering private or sensitive information. Other types of phishing techniques include "spear phishing" (focusing on a single user or department) or "whale phishing" (focusing on individuals of high importance or worth).

Phreaking – Using a computer or other device to trick a phone system. Typically, phreaking is used to make free phone calls or to have calls charged to a different account. This is one of the earliest forms of "hacking".

PII – Acronym for Personally Identifiable Information. This typically refers to any information that can identify an individual, though various states, laws and regulations have their own definitions as to what constitutes "PII". PII may include PHI (protected health information), PCI (payment card information), social security information, amongst a plethora of other sensitive data.

POS – Acronym for Point of Sale, referring to the capturing of data and customer payment information at a physical location where goods or services are bought and sold. Depending on the context, POS may also refer to the software platform utilized to capture and/or transmit this information.

Ram Scraping – A technique utilized by various Malware (namely, the BackOff variant) where payment card information is extracted from a machines memory prior to being encrypted.

Ransomware – A type of malware which restricts access to the computer system it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed

Redundancies – Duplicate copies of data, infrastructure or other sensitive/critical information or infrastructure. Typically, off-site and geographically diverse redundancies serve as the gold standard.

Rogue Employee – Refers to an employee who has nefariously accessed information that they were not granted access to or an employee who nefariously transacts sensitive information, typically for financial gain. Rogue employees may also seek to attack a company network when seeking retribution for various perceived indecencies (amongst other rationale).

SaaS – Acronym for Software as a Service. This delivery method allows for software functionality to be delivered over the internet (or cloud) rather than being installed locally on the end-user's machine.

SCADA – Acronym for Supervisory Control and Data Automation. These systems can be used in controlling industrial and manufacturing processes.

Social Engineering – The act of attempting to obtain otherwise secure data by conning an individual into revealing secure information. Victims of social engineering attacks are typically vulnerable due to the innate desire to trust other people and be helpful.

SPAM – Electronic junk mail or postings.

Spoofing – Describes a variety of ways in which hardware and software can be fooled. Spoofing may also refer to faking a certain telephone number, IP address or other unique identifier.

Spyware – Software that covertly gathers user information without their knowledge, usually for advertising purposes.

SSL – Acronym for Secure Sockets Layer. SSL is a protocol for transmitting private data via the internet by utilizing cryptographic systems that use two keys to encrypt data. Many internet browsers indicate a connection protected by SSL by displaying a padlock or security certificate near the URL field.

Third Party (Insurance Coverage) – Typically refers to coverage triggered by a claim filed by a third party. In a privacy/cyber context, these claims usually arise from allegations of mental anguish, identity theft, exposure of information or network security attacks.

Threat Agent – A term used to indicate an individual or group that can manifest a threat. These threats typically want to exploit the assets of a company for various purposes.

Tokenization – The process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token.

Trojan Horse – A program (Malware) designed to breach the security of a computer system and, when executed, carry out actions determined by the nature of the Trojan (typically theft of data or computer harm).

Virus – A program (or piece of code) that is loaded onto a computer without knowledge with malicious intent and functionality.

Vulnerability – An unintended flaw in software or systems that leave it open to potential exploitation.

White hat – A term referring to "ethical hacking". White hat hacking attempts are typically requested by the target themselves, in an attempt to discover vulnerabilities previously unknown to them.

Worm – A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Zero-Day – An exploit that takes advantage of a security vulnerability on the same day that the vulnerability becomes publicly or generally known. These exploits are typically thwarted at later dates through security patches/updates released by the software vendor.