Global Data Breach Notification Laws: Meeting Requirements and Mitigating Risks with Endpoint Security

ABSOLUTE™

Whitepaper

Global Data Breach Notification Laws: Meeting Requirements and Mitigating Risks with Endpoint Security

Introduction

A common nightmare scenario for security leaders today is having a laptop, tablet, or smartphone – loaded with sensitive information – go missing. When devices are lost or stolen and personal data is breached, organizations face increasing obligations to disclose incidents to the affected individuals and/or government agencies. Disclosure requirements partly explain why, according to recent research, 72% of business and security professionals say their top mobile security concern is data loss due to lost or stolen devices.[1]

Ongoing massive data breaches have driven many recent updates to legislation, with a trend towards more stringent requirements and higher penalties for non-compliance

Rooted in privacy law, data breach notification requirements are based on the philosophy that notification can mitigate the risks for individuals who are affected by breaches. With notification, individuals or government agencies may be able to take actions to protect those affected and avert for example, identity theft, financial loss, or injury to personal character. Another major driver behind these rules is to compel organizations to prevent breaches by implementing security controls that adequately protect information.

This white paper is intended to help security teams understand the basic requirements of data breach notification rules worldwide, including the specific expectations pertaining to mobile incidents, in order to develop effective risk management and compliance strategies.

THE ESCALATING COST OF BREACHES

According to the latest *Cost of a Data Breach Study: Global Analysis*, the average total cost of a data breach for the companies surveyed increased by 15%, up to $3.5 million USD, over the previous year. As well, a lost or stolen device was the number one factor in increasing the cost of a data breach. The study also looked at the potential risks of having a data breach and predicted that over the next two years, the probability that an organization will have a material breach involving a minimum of 10,000 records is more than 22%.[7]

The cost of a data breach includes immediate costs for investigation, remediation, and notification; public relations costs to manage the reputational damage; and legal and regulatory expenditures. A company may face legal action on multiple fronts, including consumer and shareholder class actions, business partner lawsuits, and government enforcement actions. Some of the most significant costs are in lost business caused by the loss of customers' trust in the organization.

Table of Contents

When devices are lost or stolen and personal data is breached, organizations face increasing obligations to disclose incidents to the affected individuals and/or government agencies

Highlights

- A growing number of laws globally require organizations to make timely notifications if personal information has been involved in a data breach
- It is estimated that in the next two years, 22% of organizations will have a material data breach, with a lost or stolen device being the number one factor increasing the cost
- Ongoing massive data breaches have driven many recent updates to legislation, with a trend towards more stringent requirements and higher penalties for non-compliance

Data breach notification rules expect organizations to be prepared for and respond to any type of incident involving the exposure of personal information including specific expectations regarding mobile incidents

- As an example, the European Union (EU) is poised to introduce a new data protection regulation; penalties for non-compliance are 5% of an organization's annual global turnover or €100 million, whichever is greater
- Organizations that operate in multiple jurisdictions may be subject to a multitude of notification requirements
- Jurisdictions vary in their definitions of what is covered by the law, their criteria for reporting a breach, and their obligations for who, how and when to notify
- The trigger for notification can be any breach as defined by the requirements but many jurisdictions include a specific harm threshold
- Mobile devices pose significant risks as these devices often contain sensitive data and are frequently lost or stolen
- Data breach notification rules expect organizations to be prepared for and respond to any type of incident involving the exposure of personal information including specific expectations regarding mobile incidents
- Key requirements related to endpoint security can be derived from government guidance documents as well as the ISO/IEC 27002 standard
- Recommended practices include ensuring the destruction of sensitive data once it is no longer required and being able to remotely retrieve or destroy information on mobile devices
- When responding to a particular mobile incident, a key challenge is determining if and how notification is applicable
- Generally organizations are expected to look at incidents on a case-by-case basis and, working with legal counsel, make decisions according to a risk assessment
- Organizations should be able to determine facts such as what data is on the device, whether it has been lost or stolen, where it is, who is in possession of the device, the status of encryption, and if any personal information was actually accessed by unauthorized users
- Absolute Data & Device Security (DDS), formerly Computrace, helps organizations to successfully meet the key requirements related to endpoint security and to mitigate the risks of a data breach involving missing devices
- It arms them with a range of powerful capabilities to remotely control and monitor devices, protect the data they contain, and gather the necessary evidence to make informed risk management and compliance decision

Data Breach Notification Requirements: A Global Overview

Data breach notification requirements call for organizations to notify affected individuals and/or government agencies in a timely fashion when the organization becomes aware of a breach of personal information. Since the first data breach notification law was passed in California in 2002, similar laws have been passed across the U.S. and around the world (see table).

The requirements take various forms; they can be issued as stand-alone laws, clauses within overall data protection legislation or regulations, or corresponding guidance. Many jurisdictions have established mandatory requirements, and others have put forth recommended requirements while strongly encouraging organizations to comply in order to maintain trust with government agencies and consumers. Organizations operating in multiple jurisdictions may be subject to a multitude of notification requirements.

Since the first data breach notification law was passed in California in 2002, similar laws have been passed across the U.S. and around the world

NEW DEVELOPMENTS

Governments worldwide continually add or revise legislation and regulations; or publish updated guidance. Lately there has been a lot of activity in response to ongoing breaches of vast amounts of personal information and demands for better protection. Examples include:

- In the U.S., new federal legislation has been proposed that would create a national standard to replace the patchwork of state laws (2015)
- 24 states and counting have introduced or are considering security breach notification legislation this year; mostly to strengthen existing laws (2015)
- In Canada, where there is currently an assortment of provincial laws, draft legislation at a federal level would revise the national privacy law to require mandatory breach notification (2014)
- The EU is poised to introduce the new General Data Protection Regulation, which includes data breach notification requirements. Penalties for non-compliance are significant: fines of either 5% of an organization's annual global turnover or €100 million, whichever is *greater* (2015).
- In Korea, recent amendments to the IT Network Act include notifying affected individuals within 24 hours of discovering a breach. For violations, companies may face fines equivalent to 3% of their revenue (2014).

For a more complete look at the current state of evolving requirements in key geographies, see the "Snapshot" on page 13.

JURISDICTIONS WITH DATA BREACH NOTIFICATION REQUIREMENTS –

Examples from various regions worldwide

North America	
USA	State laws Federal industry-specific legislation, regulations and guidance
Canada	Provincial laws Federal Privacy Commissioner Guidelines Federal draft legislation
Mexico	Federal Data Protection Law
South America	
Brazil	National draft data protection legislation
Columbia	National data protection law
Europe	
EU	ePrivacy Directive (e-communications) Pending General Data Protection Regulation
France, Italy, Netherlands	National sector-specific laws (e-communications)
Germany	Federal data protection law
UK	National sector-specific laws and regulations Information Commissioner Office (ICO) Guidance
Asia Pacific	
Australia	Office of the Australian Information Commissioner Guidance National sector-specific laws
Hong Kong	Privacy Commissioner Guidance
Indonesia	National regulation
Japan	Various Ministry and Agency Guidelines
Phillipines	National data privacy law
South Korea	National data protection law
Taiwan	National information protection law

Organizations that operate in multiple jurisdictions may be subject to a multitude of notification requirements

THE BASICS

Although rules vary, many share the same basic components, including:

- Definition of what is covered by the rule (organizations, breaches and information)
- Threshold for notification
- Process for notification
- Consequences of non-compliance
- Recommended practices to prevent, anticipate, and handle data breaches

Many jurisdictions, including many U.S. states, qualify the definition of "breach" or "personal information" by excluding encrypted data. This exemption is particularly significant in managing the risks of mobile devices; for more information see the sidebar on page 7.

As with all laws, breach notification requirements are open to interpretation on, for example, what constitutes a "breach," what triggers notification, and when to notify. It is advisable for all organizations to consult legal counsel for legal guidance regarding the requirements.

TYPES OF ORGANIZATIONS COVERED

Typically, if an organization is governed by the jurisdiction's privacy laws, it would be subject to the corresponding breach notification requirements. However many rules base the application of the requirements on the place of residence of the data subjects and not on the location of the data owner/processor. In many cases, organizations that conduct business with a jurisdiction's residents, or otherwise process personal data about those residents, are subject to the jurisdiction's requirements, even if the organizations do not have a physical presence there. Some rules are industry-specific and only pertain to organizations in certain industries, such as healthcare, finance or electronic communications.

DEFINITIONS OF "BREACH"

In general "breach" is defined broadly. For example, a compilation of U.S. state law definitions defines a breach as: *"The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information."*[8] Government guidance sometimes offers specific examples of types of breaches such as:

- Lost or stolen IT equipment – missing laptops, tablets, smartphones, etc.
- Hacking – malicious attacks on computer networks
- Technical error – unforeseen complications in an IT system
- Unauthorized access – employees exploiting privileged access

However not all breaches trigger notification (see "Thresholds for Notification" next page 6).

Breach can be defined as: *"The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of personal information,"* according to a compilation of U.S. state law definitions.

TYPES OF INFORMATION COVERED

Fundamentally, the information covered by the rules is "personal information" but the definition of this term varies. Some rules (especially in the EU) use a broad definition such as *"Any information relating to an identified or identifiable natural person..."*[9] Others (such as in the U.S.) specify categories of information about individuals that can be used for identity theft and fraud such as: *"An individual's first name or first initial and last name plus one or more of the following data elements:*

i) Social Security number

ii) Driver's license number or state issued ID card number,

iii) Account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account..."[10]

Many definitions also include medical information pertaining to history, condition, diagnosis or treatment and so on.

THRESHOLDS FOR NOTIFICATION

The trigger for notification can simply be any breach as defined by the requirements. However many jurisdictions include a specific harm threshold: if as a result of a data breach, there is a real risk of serious harm, the affected individuals and/or government agencies should be notified. This requires the organization to perform a risk-of-harm analysis.

Ultimately the onus is on the organization to prove that the encryption was operational, in accordance with current generally-accepted standards for effective encryption

In most cases, government agencies do not offer any formal criteria for measuring the risk of harm. But several provide guidance on the factors to consider such as:

- What kind of information was breached?
  - How sensitive is the data?
  - Could the information enable identity theft or fraud?
- Whose data was breached?
  - How could they be adversely affected by the breach?
  - Are some of the data subjects minors?
- To whom was the data disclosed?
  - Was it disclosed to unauthorized users with malicious intent to use the data?
  - What is the likelihood that third parties will maliciously use the data?
- What steps were taken to mitigate the risk to the data?
  - Was the data immediately destroyed before it could be viewed?
- Was the data actually accessed or viewed?
  - Was the data sufficiently encrypted so that it would not be readable

ENCRYPTION EXEMPTIONS CALL FOR PROOF-OF-ENCRYPTION CAPABILITIES

Often data breach requirements include an encryption exemption. In essence, if an incident which involves personal information occurs but the organization can prove the data was encrypted as specified by the requirements, then an exemption applies and notification is not expected. Deciding if exemption applies will involve working with legal counsel to interpret requirements and evaluate the particular situation.

Exemption is dependent on proving the encryption meets the requirements, however most rules don't define "encryption" precisely. Some offer a generic definition such as, "an algorithmic process that renders the data unusable." Ultimately the onus is on the organization to prove that the encryption was operational, in accordance with current generally-accepted standards for effective encryption.

Factors to consider include strength of the encryption (e.g. algorithm and key size), quality of implementation (e.g. key management), and end user conformance to policy. If the encryption method uses an outdated algorithm, the encryption could be broken by an unauthorized user. Or if encryption is poorly implemented, the unauthorized user can gain access to the key and unlock the data. Common end user practices can thwart encryption such as posting passwords on sticky notes, sharing passwords, or deactivating encryption because it decreases device performance. Some notification rules actually state that the exemption only applies if the key has not been compromised.

PROCESS FOR NOTIFICATION

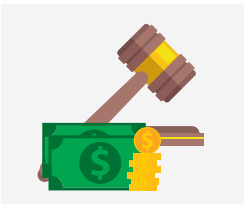
Breach notification rules typically outline who, when and how to notify.

Who to notify?	
Most rules	• Require notification of government agencies such as: ◦ State attorney general ◦ Regulatory body ◦ Data protection authority ◦ Privacy officer
Many Rules	• Require notification of data subjects ◦ The decision to notify data subjects may be made by the organization, or may be based on a directive from a government agency after it has reviewed the facts of the incident
Some Rules	• Require notification of law enforcement or credit reporting agencies
When to notify	
Most Rules	• Are unspecific such as "as soon as possible," or "without unreasonable delay" ◦ Government agency and/or courts determine if notification has been issued in a timely manner
Some Rules	• Give organizations a matter of hours (e.g. 24 or 48) or days (e.g. 14, 30, 45) • Permit organizations to delay notification pending an investigation
How to notify?	
Many Rules	• Indicate means of communication ◦ Methods range from written letters and email to notices on web sites and/ or press releases (for data subjects, depends on quality of contact information available)
Some Rules	• Suggest content to include in the notification • Provide templates or standard forms to fill out

CONSEQUENCES OF NON-COMPLIANCE

Government enforcement agencies take a range of approaches to non-compliance. Not meeting requirements, such as failure to notify or delayed notification, may result in the following consequences:

Possible Consequences	Notes
Penalties and/or fines	• Amounts vary greatly and are often determined up to a maximum and/or are calculated per record
Regulatory action	• Investigations into the causes of the breach can be to prosecute criminals and/or protect consumers • Regulators could impose periodic audits over a period of many years • Some agencies have powers of inspection including seizure of documents and equipment • States attorney generals can apply suspensions so that an organization is unable to conduct business
Private cause of action	• Individuals who suffer damages may be permitted to seek compensation through the courts
Imprisonment	• Under some data protection regimes, individuals who willfully commit offences may be subject to imprisonment
Blacklists	• Agencies may highlight serious abusers of personal information on public websites



If organizations do not meet requirements, consequences may include penalties, regulatory action, or lawsuits

RECOMMENDATIONS TO PREVENT, ANTICIPATE, AND HANDLE BREACHES

In conjunction with establishing notification requirements, some government agencies provide recommendations on specific practices for preventing, anticipating and handling data breaches. Often they also call for the adoption of recognized standards such as IEC/ISO 27001/2.

For preventing a data breach, suggested practices include:

- Catalog sensitive data and keep track of where it is stored
- Conduct ongoing risk assessments in order to determine necessary security measures
- Develop and periodically review and update data security policies
- Implement security controls to ensure information is properly protected
- Train/test employees and contractors on proper security procedures

For anticipating a data breach, suggested practices include:

- Create an incident response team and plan of action for when a breach occurs
- Form a multi-disciplinary team with, for example, senior management, IT, security, legal, and public relations personnel
- Develop procedures for containing the breach, investigating the cause, analyzing the implications, and notifying relevant parties

For handling a data breach, suggested practices include:

- Respond quickly and proactively by assembling the response team and implementing the plan of action as soon as the breach is discovered
- Take the necessary steps to secure the system to prevent further data loss
- Investigate the cause of the breach and implement corrective action
- Analyze the legal and regulatory implications of the breach and notify relevant parties (working with legal counsel)

When responding to a particular mobile incident, a key challenge is determining if and how notification is applicable

Specific Expectations for Mobile Incidents

Data breach notification rules expect organizations to be prepared for and respond to any type of incident involving the exposure of personal information. Given the significant risks of lost or stolen mobile devices, it is not surprising that breach notification guidance often highlights mobile security.

For example, the California Office of Privacy Protection warns organizations to, *"Pay particular attention to protecting notice-triggering personal information on laptops and other portable computers and storage devices."*[11] The UK Information Commissioner's Office provides examples of reportable incidents including a *"Theft or loss of an unencrypted laptop… holding names addresses, dates of birth and National Insurance Numbers of 100 individuals."*[12] Specific expectations related to mobile incidents can be derived not only from breach notification guidance but also best practice standards (see next page on ISO/IEC 27002 Controls).

ENDPOINT PROTECTION

According to breach notification guidance, organizations should implement information security controls that guard against loss or theft of computer equipment or devices containing personal information — including accidental or inadvertent loss. Effective security requires specific measures to protect the hardware as well as the data it contains from misuse, interference, loss, unauthorized access, modification, and disclosure.

Recommended practices include:

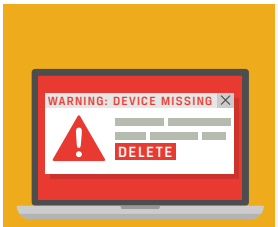
- Minimize the collection and storage of sensitive personal information on mobile devices
- Ensure destruction of sensitive data when it is no longer required
- Use encryption on mobile devices
- Restrict the number of people permitted to carry sensitive personal information outside the office
- Have the capability to remotely retrieve or destroy information in cases where a device goes missing or an employee is terminated

RELEVANT CONTROLS FROM THE ISO/IEC 27002 STANDARD

To protect endpoints and the information they contain, organizations should implement policy and supporting security measures to:

- Prevent loss, damage, theft or compromise of information storing and processing equipment* such as:
  - Ensure removal of equipment is authorized
  - Institute time restrictions on the removal of assets and record removals and returns
  - Undertake spot checks to detect unauthorized removal
  - For off-site assets, take into account the different risks of working outside the organization's premises
  - Maintain a log which details the chain of custody for the equipment
- Manage the risks introduced by using mobile devices such as:
  - Put in place registration of mobile devices
  - Ensure physical protection of devices
  - Restrict software installation on devices
  - Deploy access controls for devices
  - Protect devices with cryptographic techniques
  - Have the ability for remote disabling, erasure, or lockout
  - Protect against the unauthorized access or disclosure of the information stored and processed by devices

* Includes all forms of personal computers and mobile phones, etc.



Organizations are advised to have the capability to remotely retrieve or destroy information in cases where a device goes missing or an employee is terminated

EVIDENCE-BASED RISK ASSESSMENT

When responding to a particular mobile incident, a key challenge is determining if and how notification is applicable. Generally organizations are expected to look at incidents on a caseby-case basis and, working with legal counsel, make decisions according to a risk assessment. Compounding the challenge is if data was actually breached and notification applies, the organization will be under pressure to notify the government agencies and/or affected individuals in a timely manner, possibly in a matter of hours.

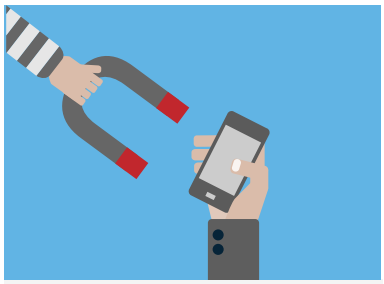
In the case of a lost or stolen endpoint device, gathering the facts needed to decide if a breach of personal information has occurred and if notification is necessary is particularly difficult, given that the endpoint device is no longer under the organization's physical control. Yet the organization should be able to answer such questions as:

- What personal information was on the device?
- Who may be affected by the disclosure of this personal information?
- What parties have gained unauthorized access to the device?
- Have they viewed the personal information on the device?
- Is there a risk of ongoing breaches or further exposure of the information on the device?
- Is there evidence that someone stole the device?
- Can it be determined whether the thief specifically wanted the information on the device, or
- the hardware itself?
- Is the personal information adequately encrypted on the device?
- Can the device and personal information be recovered?
- Who is in possession of the device and the affected information?

Some rules are very specific about how the risk assessment should be conducted such as the omnibus final rule on Breach Notification for Unsecured Protected Health Information (PHI) in the U.S. Under this rule, covered entities must demonstrate that there is a low probability that PHI has been compromised by performing a risk assessment that considers four factors:

1. The nature and extent of the protected health information involved;
2. The unauthorized person to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Covered entities need to determine if the PHI was actually acquired or viewed or, alternatively, if only the *opportunity* existed. The rule provides an example scenario involving a stolen laptop computer. If an investigation shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed, however it is not an explicit exception. The example demonstrates how important it is for organizations to be able to gather detailed evidence, and work with legal counsel, in order to make risk and compliance decisions



In the case of a lost or stolen endpoint device, gathering the facts needed to decide if a breach of personal information has occurred and if notification is necessary is particularly difficult, given that the endpoint device is no longer under the organization's physical control

IMPLEMENTING EFFECTIVE RISK MANAGEMENT AND COMPLIANCE STRATEGIES WITH TECHNOLOGY FROM ABSOLUTE

Mobile device usage provides significant business benefits to organizations yet poses increasing security and compliance risks. Security leaders today recognize that managing these risks involves not only attempting to prevent mobile incidents, but also being able to handle the inevitable incidents when they occur.

A major component of incident response today is meeting data breach notification obligations. This involves working with legal counsel in order to precisely understand the relevant requirements, evaluate if personal data has been exposed, and decide if and how notification applies.

In cases where a device has been lost or stolen, deciding if and how notification is applicable can be a particularly thorny problem. It is dependent on the organization's ability to gather evidence. They must know for example, exactly what data is on the device, if encryption is functioning or has been compromised, and if any sensitive data was actually accessed and by whom. Without physical control of the device, it can be very difficult to get the information needed.

A major component of incident response today is meeting data breach notification obligations. This involves working with legal counsel in order to precisely understand the relevant requirements, evaluate if personal data has been exposed, and decide if and how notification applies.

Absolute DDS is an adaptive endpoint security solution. It provides customers with a persistent connection to all of their endpoints and the data they contain. This means they are always in control, even if a device is off the network or in the hands of an unauthorized user. This connection to each device provides customers with the insight they need to assess risk and apply scenario-appropriate security measures.

- **Significantly reduce the chances of devices being lost or stolen:**
  - Control and secure the complete range of devices in today's IT environment such as servers, workstations, desktops, laptops, notebooks, tablets, and smartphones
  - Track the physical location of devices using geolocation
  - Build geofences whereby administrators are alerted when the device strays out of bounds
  - Monitor suspicious devices to pre-emptively respond to security incidents

- **Effectively implement risk management and governance strategies for corporate assets:**
  - Retain a connection to all devices, on or off the network
  - Run reports on device status to prove that device location, hardware configuration, installed software programs, encryption and security software, etc. are in compliance
  - Know with certainty what is on the device and whether it is secure
  - Remotely delete sensitive information from devices at end-of-life
  - Produce an audit record or end-of-life certificate to prove data was deleted
  - Create customized alerts that indicate if unauthorized changes to the device have been made, or in cases of anomalous device behavior
  - Track device location history and chain of custody
  - Identify devices that might be at risk
- **Capably handle events involving missing devices:**
  - Protect the personal information on the device by remotely preventing access to the device
  - Secure devices that have gone dark and that remain offline
  - Freeze the device so that it becomes unusable and send a message to the user
  - Remotely retrieve or delete personal information from the device
  - Detect whether the device is adequately encrypted
  - Determine if sensitive information on the device has been viewed
  - Perform remote forensic investigations to understand how and why a device was breached
  - Obtain detailed information on the device such as IP address, user name, and call history
  - Work with law enforcement to recover the device and/or possibly identify and charge the individuals associated with the event
- **Ensure the security of the device and protection of information:**
  - Augment safeguards such as encryption and passwords which can easily be thwarted and maintain oversight to ensure these complementary endpoint security measures are in place and working properly
  - Protect the organization from risky end-user behaviors such as posting their password on the device, sharing their password, lending or giving corporate equipment to unauthorized users, or leaving their device unattended in public and susceptible to theft or tampering
  - Preventing non-compliant behavior that can be caused purposely by rogue employees
  - Add a layer of defense to encryption programs that are vulnerable to a variety of attacks including human error

Absolute helps security leaders to enable the use of mobile devices while ensuring their organizations are able to comply with data breach notification laws globally

Conclusion

The growing problem of lost and stolen mobile devices is focusing attention on the risks of data breaches and the ensuing notification obligations. The best approach to complying with data breach notification laws is, of course, to avoid losing devices in the first place. But it is essential to plan for inevitable mobile security incidents and be able to successfully meet notification requirements.

Persistent endpoint technology is an essential component of a layered security strategy. It allows organizations to monitor and control devices, preventing them from going astray. And in the case of missing devices, organizations have the means to gather evidence, assess risks and possibly avert notification.

Absolute helps security leaders to enable the use of mobile devices while ensuring their organizations are able to comply with data breach notification laws globally. By mitigating the risks of data breaches, organizations can safeguard their reputation and avoid significant costs. Not only can they protect devices that hold personal information but also devices that contain other types of sensitive data such as intellectual property and financial records.

Absolute: The Trusted Expert in Persistent Endpoint Security and Data Risk Management

- Absolute is the industry standard in persistent endpoint security and management solutions for computers, laptops, and smartphones — and the data they contain
- Absolute has been a leader in device security and management for over 20 years
- Persistence® technology by Absolute is proven technology that is built into hundreds of millions of devices around the world
- Absolute enables a variety of forensic functionality to assist the investigation and recovery of stolen computers, or confidential insight into internal criminal activity or corporate non-compliance
- Absolute allows administrators to remotely engage with devices, which includes the ability to delete sensitive data or remotely freeze a device that is at risk
- The Absolute Investigations team has recovered more than 30,000 stolen devices in over 110 countries

PATENTED PERSISTENCE TECHNOLOGY

Persistence technology works because it provides the organization with a trusted lifeline to each device, regardless of user and location. This is possible because the Persistence module is embedded into the firmware of computer, tablet, and smartphone devices at the factory. It is built to detect if the software agent has been removed. If the agent is missing, the Persistence module will ensure it automatically reinstalls even if the firmware is flashed, the device is re-imaged, the hard drive is replaced, or if a tablet or smartphone is wiped clean to factory settings.

Snapshot: Status of Breach Notification Rules in Key Geographies

The following section summarizes the status of rules in key geographies in early 2015. It is intended as a representative sampling, not an exhaustive catalog of legislative initiatives. Data breach notification requirements are continually changing. Organizations should seek legal counsel on the latest statutes.

NORTH AND SOUTH AMERICA

UNITED STATES	
State Laws	
Current Situation	• 47 states have enacted data breach notification laws modeled after California's original statute; each with some variation • Basically they require organizations to notify state residents when their personal information has been breached
Recent Developments	• Kentucky is the most recent state to enact a law; its law includes provisions to protect student data stored in the cloud (2014) • Washington state recently amended its law to impose new obligations including an explicitly-defined timeframe: a breached entity must provide notice of the data compromise to the affected individual within 45 days. (2015)
Proposed Legislation	• Alabama, one of the only states without a law, has proposed legislation that would require businesses and government entities to notify the Alabama Attorney General and impacted individuals about a data security breach (2015) • According to the National Conference of State Legislatures, 24 states and counting have introduced or are considering security breach notification bills or resolutions. Many are amendments to existing laws, such as extending definitions of personal information. (2015)
Federal Standard	
Current Situation	• Despite ongoing calls for uniformity to replace the patchwork of state laws (considered a burden for business), there is no federal standard • Proposals for a federal security breach notification law have been on the congressional agenda since 2005
Recent Developments	• The President has put forward a proposal for a federal law and numerous bills are being debated in the House and Senate. Lawmakers have varying views over issues such as preemption of state laws and/or the timing and content of notices. (2015)
Federal Industry-specific Rules	
Current Situation	• There are industry-specific laws, regulations and guidelines at a federal level, for example in the healthcare and financial services industries • Under the Gramm-Leach-Bliley Act, financial institutions have obligations to notify based on the requirements outlined in the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notices • Under the Health Insurance Portability and Accountability Act (HIPAA) and the companion Health Information Technology for Economic and Clinical Health Act (HI-TECH), organizations in the healthcare sector have notification obligations

CANADA	
State Laws	
Current Situation	• Alberta was the first province with mandatory breach notification: Organizations subject to Alberta's *Personal Information Protection Act* (PIPA) must notify the province's information and privacy commissioner of breaches to personal information, where a real risk of significant harm exists. The commissioner then determines whether affected individuals need to be notified. • Several other provinces have included mandatory notification requirements in health-sector privacy legislation such as Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador. In the event of unauthorized disclosure of health-related personal information, organizations must notify the applicable privacy commissioner and in certain cases the affected individuals.
Recent Developments	• Manitoba was the second province to put forth mandatory breach notification. The province enacted the Personal Information Protection and Identity Theft Prevention Act (PIPITPA), which requires organizations to notify individuals in the event their personal information has been breached, if the organization has determined there is a reasonable possibility the personal information would be used unlawfully. (2013) • Still awaiting royal proclamation, PIPITPA is not currently in force.
Federal Standard	
Current Situation	• At a federal level in Canada, there is no mandatory breach notification requirement; organizations can currently report breaches voluntarily • The Office of the Privacy Commissioner of Canada has issued a set of best practices guidelines outlining steps to take after a privacy breach, strongly encouraging notification of the affected individuals
Proposed Legislation	• The federal government has proposed amendments to the *Personal Information Protection and Electronic Documents Act ("PIPEDA")* which includes mandatory breach notification (2014) • The bill — also known as the Digital Privacy Act — states that if an organization suffers a breach of privacy that creates a real risk of significant harm to an individual, the organization will be required to report the breach to the Privacy Commissioner and affected individuals

MEXICO	
State Laws	
Current Situation	• Under the Mexican Data Privacy Law and Regulations, data controllers must notify data subjects of any security breach significantly affecting data subjects' financial and moral rights. The data subject does not need to be a national of Mexico; the law may be applicable to a controller located outside of Mexico

BRAZIL	
State Laws	
Current Situation	• Brazil does not currently have breach notification in place but is in the process of establishing privacy related legislation, with a proposal to adopt a data breach notification regime.
Recent Developments	• The recently enacted Brazilian Internet Act (Marco Civil da Internet) deals specifically with issues of collection, maintenance, treatment and use of personal data on the Internet. (Effective 2014) • The Brazilian government issued the Preliminary Draft Bill for the Protection of Personal Data (2015)
Proposed Legislation	• The draft bill is comprehensive legislation requiring, among other things, consent for the processing of personal data. The bill mandates that organizations notify authorities when a data breach occurs.

ASIA PACFIC

AUSTRALIA	
State Laws	
Current Situation	• Under the Personally Controlled Electronic Health Record Act 2012 (PCEHR), there is compulsory data breach notification for breaches involving PCEHR data. • Outside of the healthcare sector, breach notification is not mandatory, however the Australian government strongly encourages notification and has laid out their expectations for organizations in the Data breach notification guide. The guide states that in general, if there is a real risk of serious harm as a result of a data breach, the affected individuals and the Privacy Commissioner should be notified.
Recent Developments	• An updated Data breach notification guide was released. (2014) • The Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended that the Government introduce a mandatory data breach notification scheme before the end of the year. (2015)
Proposed Legislation	• Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 requires telcos to retain metadata for two years and includes mandatory notification in the event of a security breach. (2015)

JAPAN	
State Laws	
Current Situation	• Although Japan's Act on the Protection of Personal Information (APPI) does not explicitly require notification in the event of a breach, a ministry may request that a report be submitted. • Businesses regulated by the Japan Financial Services Agency (JFSA) must adhere to the JFSA Guidelines which include breach notification. According to the JFSA Guidelines, when a leakage of personal information occurs, organizations must immediately produce a report outlining the facts related to the event and steps taken to prevent recurrence; as well as notify the affected individuals. • The Ministry of Economy, Trade and Industry (METI) have also created guidelines regarding the APPI which include suggested measures to take in cases of a breach notification. Businesses, subject to the METI Guidelines, should notify the individuals whose personal data may have been compromised, depending on the specific facts, and considering the harm (including potential harm) to the individuals concerned
Recent Developments	• METI announced plans to amend their guidelines to reinforce provisions related to data breaches. (2014)

SOUTH KOREA	
State Laws	
Current Situation	• According to the *Personal Information Protection Act* (PIPA) and the Act on *Promotion of Information and Communications Network Utilization and Information Protection* (IT Network Act), affected individuals and/ or relevant regulators must also be notified of a data breach of personal information • Under PIPA, the duty to report to the relevant regulator arises only if the number of the affected individuals is at least 10,000 • Under the IT Network Act, notification is triggered upon occurrence of any data loss, theft or leakage affecting personal information
Recent Developments	• In the wake of several massive data breaches in Korea, recent amendments to the IT Network Act include: an increase in fines, a lower liability threshold for regulators to levy fines, allowing compensation of individual plaintiffs without a showing of damages; and requiring notification of affected individuals within 24 hours of discovering a breach. For any violation of the data protection provisions, companies may face fines equivalent to 3 percent of their revenue. (2014) • Under the recently enacted Cloud Computing Development and User Protection Act, cloud computing service providers will have to notify users of any data breach or service outage (2015)

EUROPE

EUROPEAN UNION

State Laws	
Current Situation	• A data breach notification requirement for the electronic communication sector introduced was introduced by the EU in the revised ePrivacy Directive. • When a personal data breach occurs, electronic service providers must report this to a specific national authority. The provider must inform the concerned subscribers directly when the breach is likely to adversely affect personal data or privacy. To ensure consistent implementation of the data breach rules across Member States, the Commission has adopted practical rules to complement the existing legislation – on the circumstances, formats and procedures for the notification requirements.
Proposed Legislation	• Although European Data Protection law is already one of the most stringent laws in the world, Europe is set to have an even more rigorous law with the introduction of the new General Data Protection Regulation. • The Regulation will apply to all processing of personal data by a business operating in the European Union (EU) market, whether or not the business is physically based in the EU. • It includes data breach notification requirements. There will be a compulsory reporting obligation on a data controller to report a breach to its DPA without undue delay (in contrast to the previous proposed timeline of 24 hours). Affected individuals must be notified where the breach is likely to affect adversely their data protection rights. • The penalties for non-compliance are significant. The data protection authority ("DPA") will be able to impose fines of either 5% of its annual global turnover or €100 million whichever is *greater*. (Proposed Regulation to be finalized in 2015.)

GERMANY

State Laws	
Current Situation	• Under the German Data Protection Act (*Bundesdatenschutzgesetz*) ("BDSG"), depending on the type of data and the severity of the breach, both the affected individual and the regulator have to be informed. • The notification obligation relates to controllers that are subject to the BDSG, irrespective of the location of the affected data subjects. • The obligation is triggered when certain types of personal data is unlawfully transferred or otherwise unlawfully disclosed to third parties, and as a result there is a threat of serious harm to the rights or legitimate interests of data subjects.

UK

State Laws	
Current Situation	• There is no general requirement under the UK's Data Protection Act to notify breaches to either affected individuals or the DPA. • Certain sectors however (such as financial services) have sector specific notification requirements with notifications usually to be made to the sector regulator. • Providers of public electronic communications services (e.g. internet service providers, telecoms providers, netc.) must notify the Data Protection Authority if there is a personal data security breach as required by the Privacy and Electronic Communications Regulation (PECR). • Even though it's not a requirement of the Data Protection Act, the Information Commissioner recommends in guidance that for "serious breaches" the Commissioner should be notified; with the overriding consideration being the potential harm to individuals as a result of the breach (depends on the volume and the sensitivity of the personal data that was breached).

FOOTNOTES

[1] 2014 Mobile Security Survey, InformationWeek, March 2014

[2] The Impact of Mobile Devices on Information Security: A Survey of IT and Security Professionals, dimensional research, October 2014

[3] The Cybercriminal's prize: Your Customer Data and Competitive Advantage, Forrester, August 2014

[4] Brief: Stolen And Lost Devices Are Putting Personal Healthcare Information At Risk, Forrester, September 2014

[5] Coca-Cola in the Dock After Massive Laptop Theft infosecurity, November 14, 2014

[6] Privacy commissioner says Medicentres failed to protect health info CBC News, August 29, 2014

[7] 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014

[8] Data Breach Charts, BakerHostetler, June 2014

[9] Article 2, Directive 95/46/EC

[10] Data Breach Charts, BakerHostetler, June 2014

[11] Recommended Practices on Notice of Security Breach Involving Personal Information, California Office of Privacy Protection, January 2012

[12] Notification of data security breaches to the Information Commissioner's Office (ICO), ICO, July 2012

BIBLIOGRAPHY

2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014

2014 International Compendium of Data Privacy Laws, BakerHostetler, February, 2014

Complying with the GLBA Privacy and Safeguards Rules, Scott & Scott LLP

Data Breach Charts, BakerHostetler, June 2014

Data Breaches and the Encryption Safe Harbor, Storage Networking Industry Association, October 2012

Data Breach Notification Guide: A Guide to Handling Personal Information Security Breaches, Australian Government Website

Data Breach Notifications in the EU, The European Network and Information Security Agency (ENISA), January 2011

Global Guide to Data Breach Notifications, The World Law Group, Ltd., May 2013

ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls, ISO Website

The Impact of Mobile Devices on Information Security: A Survey of IT and Security Professionals, dimensional research, October 2014

Information Security and Security Breach Notification Guidance: Preventing, Preparing for, and Responding to Breaches of Information Security, Office of Illinois Attorney General, January 2012

Notification of Data Security Breaches to the Information Commissioner's Office (ICO), ICO, July 2012

Recommended Practices on Notice of Security Breach Involving Personal Information, California Office of Privacy Protection, January 2012

Security Breach Notification Laws Data Privacy Survey 2014, Weil, Gotshal & Manges LLP, May 2014

NOTE: The information contained in this document on data breach notification requirements is provided as general summary information only and is limited to a subset of the extensive requirements from all of the various jurisdictions. Organizations must refer to the specific legislation, regulations and guidance for more comprehensive information on the requirements. It is essential for organizations to consult legal counsel in order to understand the full extent of their legal obligations and formulate an appropriate response when faced with an incident. Information on the Absolute technology solution and how it can help organizations to implement security controls for endpoint security are provided as general summary information only. Organizations must work with legal counsel and/or privacy and information security auditors to determine if their particular implementation of security controls meets the requirements of the law.

ABT-NA-Global-Data-Breach-WP-E-0811115