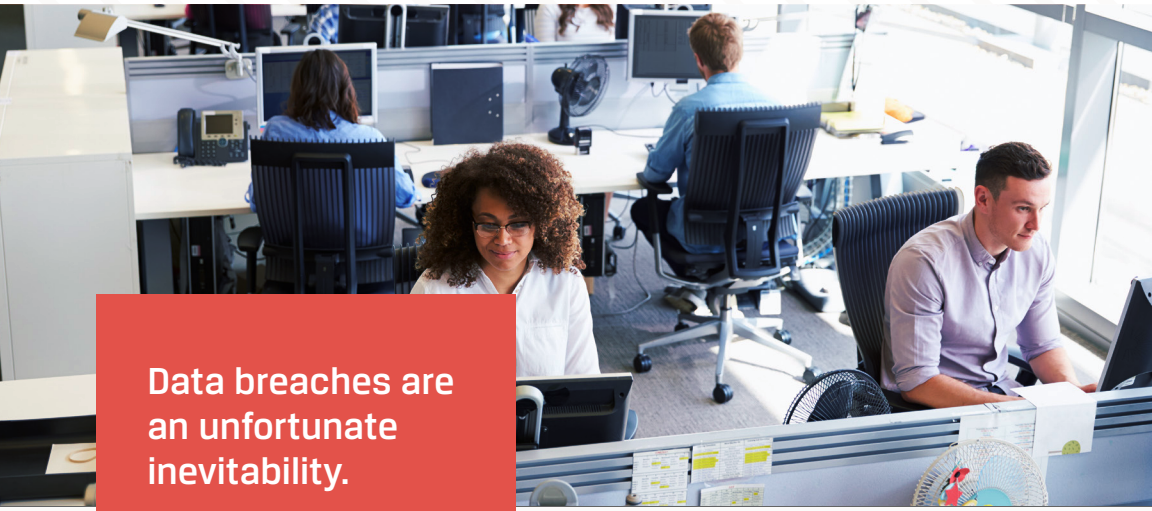


# Data Breach Response Revisited

Refining Best Practices in Incident Response



## SUMMARY



Data breaches are an unfortunate inevitability.

It doesn't matter if you're Google, Facebook, or an independent insurance broker, your data is valuable – and therefore attractive to cybercriminals. Data breach prevention is extremely important, of course, but equally vital is how prepared you are to respond when an incident occurs.

This short eBook examines the latest response requirements outlined by the world's strictest regulators and details breach response best practices in accordance with the NIST Cybersecurity Framework. It focuses particularly on incident response procedures in scenarios where the breach originates on the endpoint – results from a recent [Forrester security survey](#) found that 70 percent of breaches can be traced back to the endpoint.<sup>1</sup>

Read on to learn how your organization can revisit your incident response plans and be prepared to detect, respond, and recover as quickly as possible.

---

<sup>1</sup> IDC, 2016.

## CONTENTS

DATA BREACH PREPARATION	04
GLOBAL DATA BREACH RESPONSE MANDATES	06
REVISIT YOUR DATA BREACH RESPONSE PLAN	11
DETECT	12
RESPOND	13
RECOVER	13
NEXT STEPS	14



# DATA BREACH PREPARATION

Since 2005, more than [1,643,148,162 records have been compromised in 9,668 separate breaches](#)<sup>2</sup>. And that's just in the U.S. — the global tally is far greater. These staggering numbers prove that when it comes to data breaches, it's more a question of 'when' than 'if' it will happen.

Even organizations with seemingly infinite security resources at their disposal are not immune to attack. A vulnerability in Google+ was cited as being [partially responsible](#) for the company's decision to shut down the platform indefinitely,<sup>3</sup> and a recent breach of Facebook's network security may have compromised the personal information of [almost 50 million users](#).<sup>4</sup>

For large organizations like Google and Facebook, a breach is an embarrassing moment in time. To a small business, it could be devastating. According to the National Cyber Security Alliance, [60 percent of small businesses](#) are forced to close their doors less than six months after a cyberattack.<sup>5</sup>

While nothing will protect you completely, you can implement some practical measures to deal with the consequences of an attack efficiently, helping to safeguard your business and your customers. The best way to handle any emergency is to be prepared — a good incident response plan is the most valuable asset to have in the event of a data breach.

---

<sup>2</sup> 2018. [Identity Theft Resource Center](#)

<sup>3</sup> The Verge. 2018. [Google is shutting down Google+ for consumers following security lapse.](#)

<sup>4</sup> New York Times. 2018. [Facebook Security Breach Exposes Accounts of 50 Million Users.](#)

<sup>5</sup> Inc. 2018. [60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself.](#)



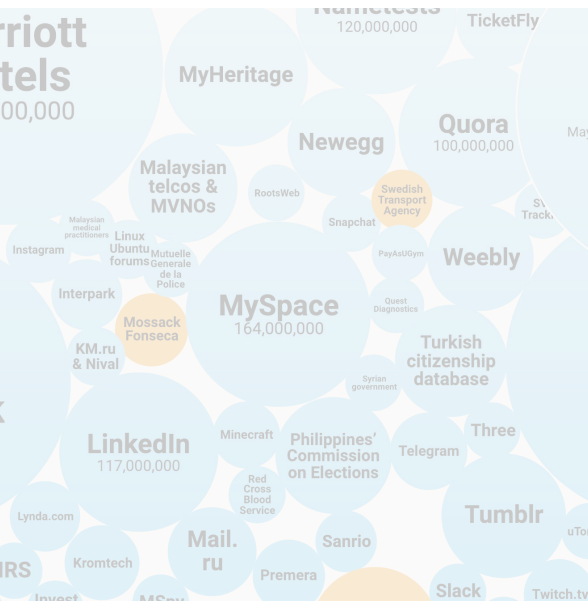
## PROVING COMPLIANCE IS HALF THE BATTLE

Part of surviving an attack is the ability to prove that you had appropriate protections in place. If you can demonstrate that you were proactively taking measures to protect your customers' data, they will be much more understanding in the event of a breach. On the other hand, if your cybersecurity strategy involves lackluster efforts and/or negligence, it's unlikely that your customers will ever trust you again.

**When breaches originate on an endpoint device, you must be able to prove that:**

- All security technology was in place and functioning at the time the device went missing
- No data was accessed post incident
- The device was remotely disabled and all personal data was deleted

If you don't have visibility into your devices, you must presume that the data on that device was breached and follow the relevant breach notification processes in your industry or region.



***SINCE 2005, MORE THAN 1,643,148,162 RECORDS HAVE BEEN COMPROMISED AS THE RESULT OF A DATA BREACH.***

**SOURCE: IDENTITY THEFT RESOURCE CENTER<sup>6</sup>**

<sup>6</sup> 2018. Identity Theft Resource Center.

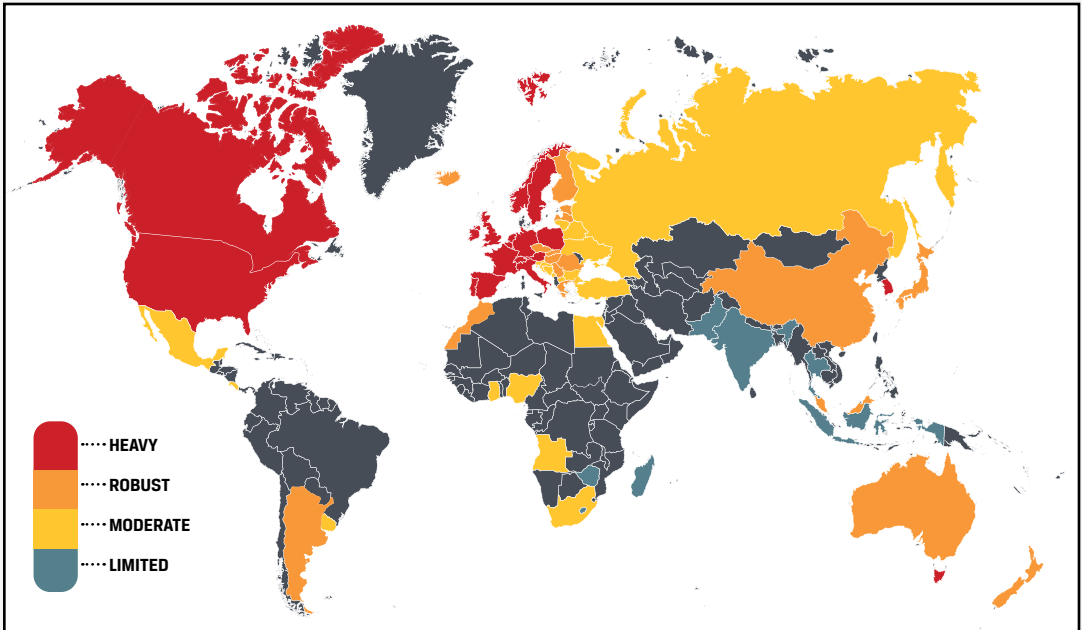


# GLOBAL DATA BREACH RESPONSE MANDATES

Considering both the volume and the range of regulations governing data privacy and security, compliance is becoming more complex and costly every year.

In the largest economies alone, the variation in data breach notification requirements creates profound uncertainty around the obligations of organizations handling personal data. Sweeping regulations such as the [EU General Data Protection Regulation \(GDPR\)](#) are prompting regulators around the world to implement compatible standards and, in some cases, to start levying their own fines.

## GLOBAL REGULATIONS AND ENFORCEMENT



SOURCE: DLA PIPER INTELLIGENCE





Europe, Australia, Canada, and the USA have the heaviest data protection regulations in place today. If you are doing business (or have customers located) in these areas, you must be familiar with the local breach response guidelines.

## USA'S STATE AND SECTOR-SPECIFIC LAWS



Rather than a comprehensive legal protection for personal data, the United States has [a patchwork of state and sector-specific laws that must be adhered to.](#)<sup>7</sup> The laws generally require notification to both consumers and regulators within a stated time period and are based on a broader range of data, including online account credentials, health information, passport numbers, and biometric data.

Outside of the state-level laws, federal laws like HIPAA (Health Insurance Portability and Accountability Act), the Federal Trade Commission Act, and the Gramm-Leach-Bliley Act govern specific industry sectors. Lately, HIPAA enforcement has been particularly unforgiving, with the [average settlement with Office for Civil Rights \(OCR\)](#)<sup>8</sup> quadrupling in the past decade.

Following any breach of PHI, the HIPAA Breach Notification Rule requires you to:

- **Notify affected individuals within 60 days of the discovery of the breach**
- **Notify the OCR within 60 days of the end of the calendar year in which the breach occurred**
- **For breaches involving 500 or more records, notify the OCR immediately, submit a notification to a prominent media outlet, and post a notice on your homepage**



<sup>7</sup> Perkins Coie. 2018. [New Data Breach Notification Laws Spring 2018: What You Need to Know.](#)

<sup>8</sup> Beazley. 2018. [2018 Breach Briefing.](#)



## AUSTRALIA'S PRIVACY AMENDMENT ACT



Since February 2018, organizations with a turnover of \$3 million or more will fall within the scope of [Australia's Privacy Amendment \(Notifiable Data Breaches\) Act](#).<sup>9</sup>

Where a data breach that could cause 'serious harm' has occurred, organizations must:

- **Notify affected individuals with a description of the breach, the kinds of information concerned, and recommendations about next steps**
- **File a report with the Privacy Commissioner**

The term 'serious harm' may include physical, psychological, economic or financial harm, but wouldn't include individuals being distressed or upset.

[Non-compliance may attract fines](#) for both the individual company director(s) (up to \$340,000) and the company itself (up to \$1.7 million).<sup>10</sup> This does not include reparation costs for any customers who may be impacted by the breach by professional firms and their clients.

## CANADA'S PIPEDA



Canada's [PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#) describes how private-sector organizations collect, use, and disclose personal information.<sup>11</sup>

In the event of a breach, organizations subject to PIPEDA are required to:

- **Notify the Privacy Commissioner of Canada where the breach involves personal information that pose a 'real risk of significant harm' to individuals**
- **Notify affected individuals**
- **Keep records of all breaches**

Factors that are relevant to determining whether a breach creates a real risk of significant harm include the sensitivity of the personal information involved in the breach and the probability the personal information has been or will be misused.

<sup>9</sup> Office of the Australian Information Commissioner. 2018. [Australian Privacy Amendment \(Notifiable Data Breaches\) Act](#).

<sup>10</sup> Australasian Lawyer. 2018. [Compliance with the Notifiable Data Breaches Scheme](#).

<sup>11</sup> Office of the Privacy Commissioner, Canada. 2018. [What you need to know about mandatory reporting of breaches of security safeguards](#).





## EUROPE'S GDPR

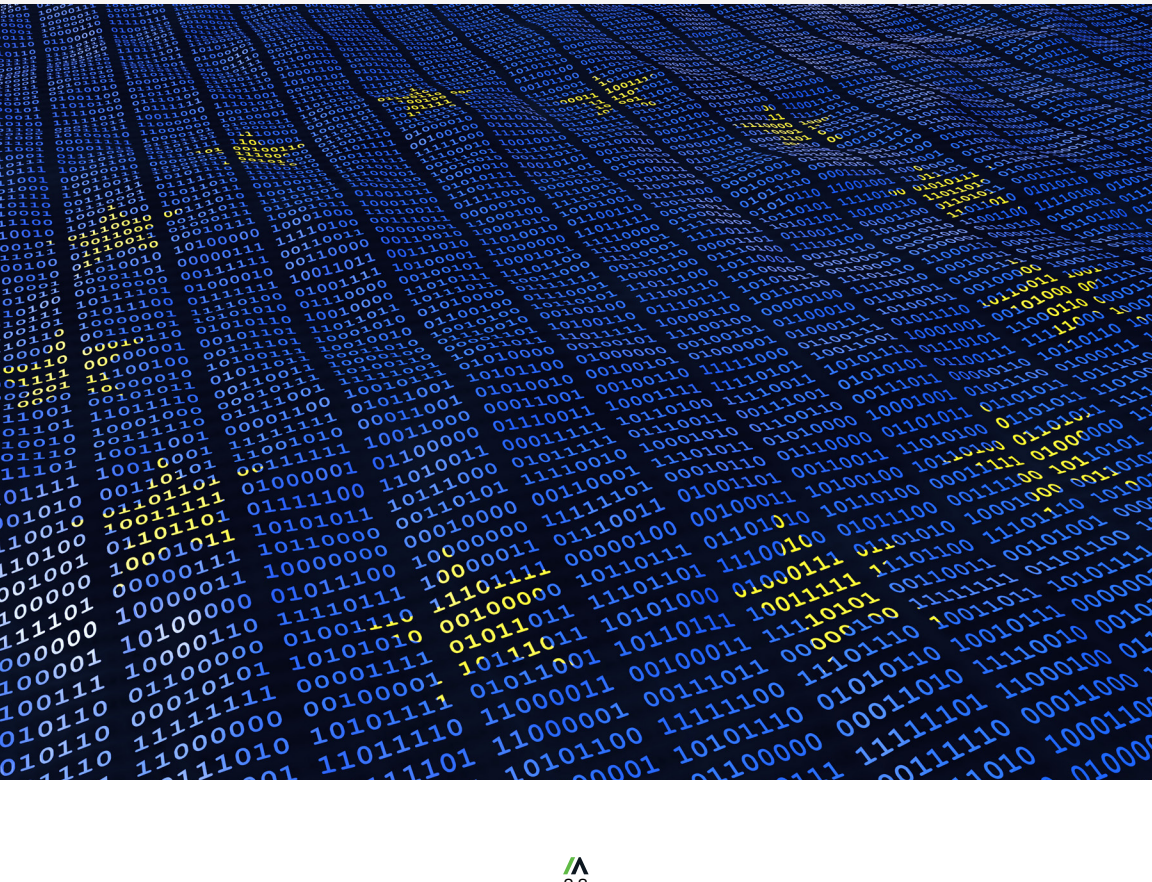


The [GDPR \(General Data Protection Regulation\)](#) is today's highest benchmark for data protection regulation. It is thorough, prescriptive, and complex.

Where a data breach is likely to 'result in a risk for the rights and freedoms of individuals,' organizations must:

- Carry out an investigation
- Notify authorities within 72 hours of breach discovery
- Notify affected individuals 'without undue delay'
- Be specific with respect to what data was impacted and how the issue will be addressed moving forward



One of the biggest challenges for organizations is complying with the [72-hour](#) data breach notification window.





## GENERAL BREACH NOTIFICATION CHECKLIST

Although breach notification timelines and requirements vary, the following checklist can help you in any scenario.

 <b>DURING THE BREACH</b>	 <b>AFTER THE BREACH</b>
<ul style="list-style-type: none"> <li>• Determine the nature of the breach (i.e. the number and types of data records)</li> <li>• Document contact details for your data protection officer or point of contact</li> <li>• Outline the likely consequences of the data breach</li> <li>• Describe measures taken or proposed to be taken to address the data breach</li> <li>• Detail the effects of the breach and remedial actions taken (this will be required by the supervisory authority after the breach so, preparing it proactively saves time)</li> </ul>	<ul style="list-style-type: none"> <li>• Notify authorities within the relevant breach notification response window</li> <li>• Provide all the necessary information</li> <li>• Explain the data breach, including what security measures were already in place</li> <li>• Describe how you plan to prevent future breaches (postmortem analysis of the situation is a requirement under the GDPR)</li> <li>• Develop a plan to update the incident response process and resume best practices for testing and updating the plan</li> </ul>



# REVISIT YOUR DATA BREACH RESPONSE PLAN

The responsibility for data breach response has expanded beyond the IT team and now sits on the shoulders of the board of the executives. Cybersecurity is now deemed to be as important as any other business risk – and board members are responsible for ensuring the proper people, processes, and technologies are in place to manage that risk.

As the regulatory landscape becomes increasingly difficult to navigate, companies need more than just a generic incident response plan. A thorough and customized data breach response plan plays a huge part in this risk management and mitigation. The plan should be regularly updated and practiced to ensure it remains relevant and effective. Many organizations are adopting the cybersecurity framework recommended by the National Institute of Standards and Technology (NIST). The [NIST Cybersecurity Framework](#) can help you evaluate your security posture by implementing five functions to ensure data security and business sustainability.<sup>12</sup>

The framework is cyclical and encourages continuous improvements to adapt to new threats and ever-tightening regulations. It outlines five functions, three of which are directly related to data breach detection, response, and recovery.

## INCIDENT RESPONSE FUNCTIONS OF NIST CYBERSECURITY FRAMEWORK



SOURCE: NIST CYBERSECURITY FRAMEWORK

<sup>12</sup> National Institute of Standards and Technology (NIST). 2018. [The NIST Cybersecurity Framework](#).



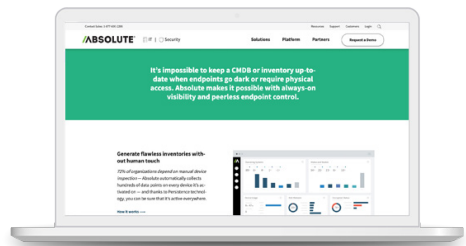


## DETECT

The Detect function of the framework focuses on detecting issues, paying attention to changing circumstances, and also to negligent users to identify suspicious endpoint activity. Once a security incident has been identified, asset intelligence plays a central role in the Detect function. Ensure you can answer these questions:

- **Where is the device located? Is the location unusual?**
- **Is there additional behavior (machine or human) happening simultaneously?**
- **Is the current anomaly outside the bounds of the security policy?**
- **What was happening on the device immediately before the event?**
- **Which data is at risk?**

Intimate knowledge of the device, data, users, apps, and behaviors allows you to satisfy the Detect function and prepare your response more efficiently.



To learn more about how Absolute can help you stop a cybersecurity threat from becoming a data breach, visit: [absolute.com/automate-hardware-audits](https://absolute.com/automate-hardware-audits)



## RESPOND

The actual discovery of a data breach is not the time to decide who will be responsible for leading and managing the response. It's critical to assemble your response plan well in advance.



### PRE-INCIDENT RESPONSE PLANNING

1. Assign a specific person or group to lead the investigation – ensure everyone knows the role they will play
2. Build incident reporting procedures including a clear plan for escalating information about an incident internally
3. Have a clear communications plan (based on your region or industry breach notification requirements). Always ask three questions before any communication – Is it true? Is it helpful? Is it necessary?
4. Document contact information for internal resources and pre-approved external resources
5. Detail how evidence will be analyzed, preserved, and documented
6. Test the plan to identify weak points and document lessons learned
7. Review response plan annually to make improvements

In conjunction with an incident response plan, organizations need to provide adequate cyber awareness training for all employees, not only explicitly telling everyone what to do, but what not to do, in the event of a data breach or cyber-attack.

## RECOVER

Once the incident has been through the post-incident cycle – recover and iterate – question assumptions, change security controls, and use new knowledge to influence future cybersecurity decisions.

***"RECOVERY PLANNING IS IMPROVED BY INCORPORATING LESSONS LEARNED INTO FUTURE ACTIVITIES."***

- THE NIST CYBERSECURITY FRAMEWORK



## NEXT STEPS

Follow these four steps to prepare yourself to be able to respond to any breach originating on the endpoint.

# 1

**Know the laws:** Ignorance is not an acceptable argument when defending your data breach to a regulatory body. It's your responsibility to research the compliance rules that your organization is tied to based on location or industry (and often both). Understand how far reaching the laws are that govern the data for which you are responsible. For example, if you've customer data from European customers, you must comply with GDPR, etc.

# 2

**Apply the NIST Cybersecurity Framework:** Frameworks like the NIST Cybersecurity Framework help to foster a culture of security within an organization from the top down. They create efficiencies in response times as everyone knows what to do and who is responsible for doing it.

# 3

**Develop customer-facing breach response plans:** According to Forrester, almost half of global security decision makers see customer concerns over privacy issues as a risk to their organization.<sup>13</sup> How your firm responds to customers when you've compromised their data will affect public trust and, in turn, your ability to recover from the incident.

# 4

**Implement technology and enforcement controls:** Without visibility and control, security policies are meaningless. When a breach occurs and you can't prove that you had controls in place, it undermines trust and attracts the attention of the regulators. Persistence<sup>®</sup> technology by Absolute offers unparalleled control over any device. Maintain regulatory compliance by providing proof that encryption or other security measures were in place at the time a security incident occurred. By reporting on the status of the data on the device, Persistence enables organizations to identify whether data was accessed post-breach, and consequently, if a breach notification must be made.

<sup>13</sup> Forrester, 2018. [Forrester Analytics Global Business Technographics Security Survey](#)





Are you ready to start implementing the NIST Cybersecurity Framework in your organization? Find out by using our checklist.

GET IT NOW

## ABOUT ABSOLUTE

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications and users against theft or attack – both on and off the corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT to enforce asset management, security hygiene, and data compliance for today's remote digital workforces. Patented Absolute Persistence™ is embedded in the firmware of Dell, HP, Lenovo, and other leading manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at [absolute.com](https://absolute.com) and follow us at [@absolutecorp](https://twitter.com/absolutecorp).



**EMAIL:**  
[sales@absolute.com](mailto:sales@absolute.com)



**SALES:**  
[absolute.com/request-a-demo](https://absolute.com/request-a-demo)



**PHONE:**  
North America: 1-877-660-2289  
EMEA: +44-118-902-2000



**WEBSITE:**  
[absolute.com](https://absolute.com)