BEST PRACTICES

A data breach can happen anytime.
Be ready to respond.

LifeLock BREACH SOLUTIONS

It only takes one stolen laptop, one employee's USB stick, one hacker, one virus, or one careless error to compromise your company's reputation and revenue. The threat of data breach is real and it's critical that your company is prepared. A thorough plan that can be executed quickly is essential to comply with relevant regulations, maintain customer loyalty, protect your brand and get back to business as soon as possible.

QUESTIONS TO ADDRESS WHEN A BREACH OCCURS

WHAT IS THE TOTAL SIZE OF THE BREACH?

It is important to establish the forensics capabilities necessary to rapidly determine the size of the breach BEFORE a breach occurs.

WHAT TYPE OF DATA LOSS OCCURRED? WAS IT ACCIDENTAL DATA LOSS OR CRIMINAL INCURSION?

Understanding the reason for the breach will help understand your risk, and the corresponding risk to the affected population with respect to likelihood of near-term criminal use of the compromised identities, and knowing that can help you determine your communications, as well as breach response product selection/capabilities.

WHAT ARE OUR LEGAL AND REGULATORY OBLIGATIONS? WHO MUST BE NOTIFIED?

47 states have laws stipulating who must be notified in breach situations.[1] Financial institutions must notify consumers and regulators.[2] Healthcare providers must provide public and industry notification of any data breach.[3] Breached merchants must comply with all applicable state, federal and industry security and notification requirements.

WHAT LEGAL AND PUBLICITY EXPOSURE DO YOU ANTICIPATE AS A RESULT OF THE DATA BREACH?

Consider the cost of breach response and the cost of lost business. A data breach can put your financial stability at risk by increasing costs and decreasing revenue. Studies have shown that one of the biggest losses from data breaches result from lost consumer confidence and resulting lost business.[4]

WHAT IS THE SCOPE OF THE BREACH? WHAT TYPES OF INFORMATION WERE COMPROMISED?

Social security numbers? Addresses? Credit card information? Bank account information? Knowing the type and extent of the lost data can guide your selection of a breach service offering and your communication plans.

1 in 4

One in four consumers received data breach notifications in 2014[5]

6X

People notified of a data breach were nearly six times more likely to be victims of fraud than those who were not notified[5]

2/3

Two-thirds of identity fraud victims had received data breach notifications that same year[5]

62,000,000 62M

Nearly 62 million consumers were notified of a data breach in 2014.

More than 2 and half times more than the year before[5]

2.5X+

4/5

Four-fifths of executives at healthcare providers and payers say their information technology has been compromised by cyber-attacks[6]

No one can prevent all identity theft. † LifeLock does not monitor all transactions at all businesses.

[1] ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[2] ithandbook.ffiec.gov/media/resources/3372/frb-sr-05-23.pdf.
[3] hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.
[4] reuters.com/article/2014/04/04/us-target-lawsuites-idUSBREA3309J20140404.
[5] 2015 Identity Fraud, Javelin Strategy & Research, March 2015.
[6] KPMG, Health Care and Cybersecurity: Increasing Threats Require Increased Capabilities, August 2015.

WHAT IS YOUR COMMUNICATIONS STRATEGY?

Understanding your communications strategy begins with understanding the SIZE, TYPE, REGULATORY requirements, EXPOSURE implications, and SCOPE of the breach in question. A firm understanding of those elements of the breach can position you to answer the 'how,' 'what,' 'when,' and 'where' questions related to breach response.

HOW YOU HANDLE A BREACH SAYS A LOT ABOUT YOU.

To facilitate a fast response, your institution should have developed an incident response playbook and appointed a leader to be in charge of it. The team to carry out the plan should be cross-functional with heavy emphasis on communications and public relations, since reaching out to the affected population will be the most important aspect.

BREACH RESPONSE NEGOTIATION CONSIDERATIONS

CAPABILITIES

What are the product capabilities of your preferred response provider and do those products support monitoring and alerting the data you may be at risk of losing? For example, if you maintain payroll data (account and routing information) does the preferred response provider offer services capable of monitoring bank accounts and alerting on potential account takeover incidents?

PRICING AND PRICING MODELS

What is the 'cost per activated member' (your cost for each enrollment) for the service(s)? Can the response provider support a "Population" pricing model wherein the entire affected population has access to enroll in the identity theft protection service at a net cost per member that is less than "cost per activated member" model?

COMMUNICATIONS

Can the response provider work with your team to create a communication template for immediate use in the event of a breach?

ENROLLMENT PROCESS

What enrollment vehicles can the response provider make available (online, phone, or both)? If phone enrollments are available, where is the provider's call center(s) located and during what hours can individuals call to enroll? What are the average phone hold times?

POST-ENROLLMENT MEMBER EXPERIENCE

Which metrics does the preferred response provider use to measure member satisfaction? What is the provider's annual member retention rate for PAYING members?

ALERTING FREQUENCY AND IMMEDIACY

How many and what types of alerts are issued to the members of the breach response product; and how soon after an new application is opened does the response provider issue the alerts?

How to act in a crisis if a breach occurs:

1. Fulfill Federal & State notification requirements.
2. Calm victims and investors.
3. Have a proactive plan in place: if identities are compromised, help protect against further damage.

REPORTING

What kinds of reports will the response provider make available to your company with respect to member enrollment totals and information on the frequency and types of alerts issued to the affect population? To what frequency of reporting will the provider commit?

Regaining trust is hard to do after a breach. Don't make it more difficult by offering only limited protection for your customers. With LifeLock Breach Solutions, you can industry-leading identity theft protection available to help protect against criminals who can sell their credit and wreak havoc on their lives. When you provide more than just limited protection, like credit monitoring alone, you'll increase the potential to regain trust.

The law dictates what you must do, but your employees and customers expect more. Meeting only minimal legal requirements could mean maximum damage to your brand.

Call 877-511-7906, option 4 or send an email to find out how LifeLock can help you prepare and protect your business.

BREACHRESPONSE@LIFELOCK.COM

LIFELOCK.COM/BREACH