

Keeping Customers When Your Data Is Stolen

Businesses face two major threats when data is stolen – the first from thieves – the second from customers and stakeholders.

A SIGNIFICANT DATA BREACH CAN DAMAGE YOUR REPUTATION, stop all momentum, and cause you to lose your smartest customers – all within a few days – unless you are prepared to act quickly.

Why thinking ahead matters. Leaders once thought that simply safeguarding data was enough. Today, it's not.

Recent experience has shown that when a significant data theft occurs customers feel victimized and lose confidence in the company. They stop buying or shift to competitors – often permanently.

That's why the ability to act quickly and decisively is vital – not within days while you figure out what to do – but within minutes and hours. Customers, vendors, and other stakeholders need to know that you care about them and are working tirelessly to protect and help them.

Delays of even a day or two make you look disorganized and indifferent – and can be fatal to important customer relationships.

Critical facts about critical situations.

The data breach won't stay secret.

Hoping it will stay quiet is naive. If news makes its way to the media or directly to customers from outsiders instead of from you – you will have absolutely no control over what is said or how it is said. Once lost, control of the communication process is usually impossible to regain.

The issue will become such a distraction that it often stops everything else.

Uncertainty over what to do can cloud judgment and inhibit sound decision-making. Fear of what might happen often paralyzes you from taking action at all or leads you to make mistakes in those first critical moments – which cannot be easily undone. In panic mode, organizations tend to either under-react or over-react to the situation – both can be very costly.



No one likes to think about disaster. But not anticipating a very real danger means you could be totally unprepared should your data be compromised.



Carl Francis, CEO
A leading strategist, instructor, and thought leader, Carl has advised hundreds of area

business leaders for nearly 30 years. He is also an Adjunct Professor and Lecturer at Drexel's LeBow College of Business.
CFrancis@envisian.com
610.640.4600 x 1



Lisa Howell, Senior Strategist
An expert in market presence and brand development, Lisa has advised leading

area businesses and non-profits for many years. She has a Master's degree from Villanova University.
LHowell@envisian.com
610.640.4600 x 2

About Envisian

Envisian advises CEOs, Boards, and senior leaders on strategic matters such as problem-solving, decision-making, increasing market presence, brand development, and handling critical situations -- including leadership or ownership changes.

Envisian Incorporated

12 Chester County Commons
Malvern, PA 19355-1942

610.640.4600 p
610.640.4601 f
ask@envisian.com
envisian.com



The longer things muddle, the worse they will get. And apparent inaction and indecision could mean that you have little or no defense in the event charges are filed or enforcement actions are brought.

Is there a better approach? Consider the advantage you may have by anticipating likely scenarios and having key assets prepared and in place – such as a plan, a team, and a few key tools.

Imagine this scenario instead.

10:00 am You learn of the breach and alert your team. Your plan is ready and both you and your team know exactly what to do – and in what order.

10:10 You call your team members in for an emergency meeting, thereby activating the plan. Team members at other locations are alerted and conference in. You review highest priority items first.

10:20 You agree on immediate action steps and confirm responsibilities – including actions that will be taken to protect customers. Messages – already prepared for the media, customers, and other important stakeholders, including employees – are reviewed and adjusted to fit the exact situation. A timeline of notifications is established, depending on the circumstances.

10:30 A series of specific actions are already underway by your team to assess the extent of the loss and to involve the proper authorities.

11:00 The first alerts have been delivered, with more planned. You are ready to respond to inquiries from the media and concerned customers. You have initial facts available and can demonstrate clarity, confidence, and control over the situation.

11:10 The first inquiries from the media and customers begin. You know what to say and what NOT to say.

Rapid response is only possible when you are fully prepared – in advance.

Communicating rapidly and comprehensively in the event of a data breach is only possible when you plan ahead.

It's no more complicated than that. You have to plan and prepare your team, your plan, your messages, and key parts of your strategy (such as lists, distribution media, and so on) well ahead of time.

Having a well-crafted action plan, supported by the necessary tools and training, and skilled support from specialists allows you to take control of a situation that is likely to feel out of control. To have confidence in the midst of chaos.

FIND OUT WHAT'S INVOLVED TO BE PREPARED

Learn how you can respond rapidly and professionally, reduce your exposure, and minimize the risk of losing valuable customers and the reputation you've worked so hard to build.

Call Carl Francis at 610.640.4600 ext 1 or email CFrancis@envisian.com today.