


FIGHTING BACK

Before a Hack Attack

A data security breach can occur at any time, triggering confusion and panic among account holders. Because trust is central to your business, it's vital to establish a proactive communications strategy that lets you speak promptly, knowledgeably and empathetically to account holders whose personal records have just been compromised. A crisis communications plan helps rebuild loyalty and confidence in financial institutions damaged by a cyber attack.



How your financial institution responds publicly after a cyber attack may have a lasting effect on its reputation.

At this exact moment, there's a chance hackers are trying to exploit the vulnerabilities in your organization's computer system. Some suggest it's just a matter of time before they succeed. Cyber attacks against financial institutions are increasing in frequency and sophistication, and becoming more widespread.¹

While no organization is immune from cyber crooks, banks and credit unions can help mitigate real and perceived threats that follow the theft of personal information by creating a communications management plan before an online break-in occurs.

Timing is essential

How your financial institution responds publicly after a cyber attack may have a lasting effect on its reputation. You don't want rumors spreading or customers attempting to use frozen or compromised cards at checkout registers because your message was slow to reach them.

Among other things, a comprehensive communications strategy should identify the key personnel and processes needed to help ease the immediate fallout from a cyber hit. A proactive response can ease anxieties that weaken confidence in your recordkeeping system and hinder future growth.

Developing a crisis communications plan


Quickly disseminating accurate information to affected account holders is at the core of any effective communications strategy. Following simple best practices when developing your plan ensures effective, timely communications.

Establish reporting protocols. Your first line of defense against cyber infiltration, of course, is your Information Technology (IT) team. Work closely with your IT professionals — especially third-party service providers — to establish protocols that define:

- What constitutes a data breach
- Root cause analysis of system vulnerabilities
- Regulatory compliance requirements
- How to alert other stakeholders
- Remediation needs, including how and when to begin the process

Prioritize internal chains of command. To involve key personnel early and reduce internal confusion, create a list of departments and individuals to immediately contact when a breach is discovered. Teams might include IT, compliance, legal, insurance/risk management, accounting, back-office

¹ New York State Department of Financial Services, *Report on Cyber Security in the Banking Sector*, May 2014



A professionally managed, 24/7 inbound-outbound call center should be the cornerstone of your communications plan.

operations, communications, branch staff and C-suite executives.

Backup external contacts. A cyber breach could compromise your ability to contact account holders through normal channels. Prepare emergency lists of customers, as well as employees, merchants, banking authorities and media outlets that you can access at a moment's notice.

Prepare for the expected. When hackers break into a company database, they are usually seeking names, social security numbers and other account holder information, as well as that of employees and third-party vendors. To prepare for potential breaches, some questions you might ask include:

- What's the nature of the breach?
- Who and how many people are affected?
- What are the immediate consequences and risks?
- What can be done to prevent further damage? What is the projected timeframe for remediation?
- Should debit and credit cards be reissued? If so, how will account holders be notified? When will they receive new cards and how should they be activated?

- Will we offer free credit monitoring services to account holders?
- Will we need a toll-free hotline for customers to report suspicious account activity?
- What actions and upgrades will be taken to ensure the future safety of account holder information?

Use multiple communication channels. Because account holders typically have communications preferences, consider a "first wave" that includes direct mail, phone, email and web messaging.

A professionally managed, 24/7 inbound-outbound call center should be the cornerstone of your communications plan. Live call center specialists provide a high level of personal care, reinforcing your institution's commitment to customer service. In fact, there is a positive correlation between the quality of personal interaction and long-term customer loyalty.²

A responsive **email** service can aid in rapidly responding to the surge of inquiries that typically follow a cyber attack. Be sure to also include texts and social media, since a growing number of younger account holders prefer these channels.

² Forrester Research, Inc., *What Drives Retention and Sales in U.S. Banking?*, October 2012



To keep abreast of evolving threats, technology and techniques, revisit your crisis communications plan at least once a year.

Your **website** should feature an emergency messaging capability with an interactive web-chat format. Prepare a landing page with common questions and answers, an 800 number and a form to request additional information if desired.

Throughout the remediation process, **direct mail, newsletters, e-seminars** and **statement stuffers** can be used to help promote a sense of normalcy. This “second wave” of communications may focus on computer safety, data protection techniques and how to avoid online scams. Such topics educate account holders, and you will strengthen your relationship and rebuild trust in your institution’s brand.

Deliver consistent messages. The first priority of your crisis communications plan should be reducing anxiety by sharing credible and cohesive information that account holders need and want. The key is to assure them that you’re on top of the crisis without being dismissive of their concerns. Depending on your client base, you may want to translate certain messages into multiple languages.

Keep your cool and your customers

In times of distress, it’s imperative to the success of your institution to communicate to account

holders, employees and associates in a courteous, professional and forthright manner. Conveying a reassuring message through multiple channels can help minimize business disruptions and deliver a more positive experience to account holders.

As a key decision-maker, ask yourself: In case of a data security breach, do we have the internal communications resources — including technical infrastructure and experienced staffing — to assuage fears and reduce customer attrition?

To keep abreast of evolving threats, technology and techniques, revisit your crisis communications plan at least once a year. Doing nothing can make a bad situation worse.

Ask how Harland Clarke can help you develop a crisis communications plan that addresses the specific needs of your financial institution following a cyber breach.

For more details call **1.800.351.3843**, visit **harlandclarke.com/DataBreach** or email **contactHC@harlandclarke.com**.