Rebuilding Customer Trust in Breach Response:

A plan for secure email communications post breach

AGARI

100 S. Ellsworth Ave | 4th Floor | San Mateo, CA 94401 | 650.627.7667

Breaches have become the new normal for today's organizations. Research from the Ponemon Institute revealed that 43% of surveyed companies reported suffering a data breach that affected at least 1000 customer records in 2014.[1]

Against an unrelenting drumbeat of increasingly sophisticated security attacks, most organizations now understand that a professional, efficient response to a data breach is the difference between a customer uprising and an opportunity to quickly re-establish trust. However, every minute matters and every enterprise needs to be prepared with a response plan to counter any successful attacks. According to Forrester Research Inc., "Customer-facing communication following a breach is a critical component of incident response and the first step in reassuring consumers that your organization is handling the incident appropriately. Botch the response, and you'll never be able to regain customer trust. Nail the response, and you have an opportunity to not only regain their trust but also strengthen the relationship."[2]

Before an enterprise even goes public with an official announcement, the breach has to be contained, the impact assessed, law enforcement notified and a message developed with organizations often relying on the ubiquity of email to inform customers and citizens. However, criminals know this too and look to do further damage to customers by hijacking email domains after a data breach. This type of post-breach spoofing attack on unsecured domains is inevitable. In some instances, the threat can be so severe that it entirely eliminates email as a secure communication channel.

Yet, it doesn't need to be this way. This guide provides practical steps to ensure an organization's email remains a secure communication channel in the event of a breach.

> *"Customer-facing communication following a breach is a critical component of incident response and the first step in reassuring consumers that your organization is handling the incident appropriately. Botch the response, and you'll never be able to regain customer trust. Nail the response, and you have an opportunity to not only regain their trust but also strengthen the relationship."*
>
> *- Forrester Research, Inc.*

1 *The Second Annual Study on Data Breach Preparedness, conducted by Ponemon Institute and sponsored by Experian, September 2014.*

2 *Market Overview: Customer Data Breach Notification And Response Services, Forrester Research Inc, August 2015.*

THE NEW NORMAL

As cybercrime continues to rise at an unprecedented rate, and in a multitude of forms, collective responses to the problem have struggled to keep pace. In 2015, breaches have already hit healthcare, financial services, higher education institutions and the public sector. In recent months, the news has been full of data breaches. Anthem, the second largest US health insurer, revealed the personal information of approximately 80 million individuals was compromised after hackers broke into its database and the U.S. Federal Government's Office of Personnel Management (OPM) revealed that the personal information of 21.5 million Americans was compromised in a hack of its databanks.

Organizations of all size need to assume that they will be affected by a data breach at some point and plan accordingly by developing a risk strategy. According to the Ponemon Institute and its data breach preparedness study, more companies are already taking basic steps to prepare themselves for the increasing likelihood of a breach. The majority of surveyed organizations (73%) have a data breach response plan in place, while in the last 12 months nearly half have increased investment in security technologies.

EMAIL IS KEY TO EFFECTIVE COMMUNICATION

Today, any organization without a data breach plan is behind the curve. In the event of a data breach, timely and effective communication is absolutely critical. According to Forrester, "a botched breach response undermines customer trust, reputation. A disjointed, disorganized notification response raises questions about whether a business knows what to do in order to recover or is capable of appropriately executing the response" [3]. Customers and citizens want to know what's going on, assess the impact and understand what options are available to limit exposure. This means crisp, clear messaging with the appropriate balance of confidence and contrition. And it means a channel of communication that reaches your customers, wherever they are, in a timely fashion.

Every minute matters in post-breach communications and the prevalence of email makes it a key channel for communicating and advising victims on next steps. Unfortunately, cyber criminals anticipate this process, which means every publicized data breach

> *"A botched breach response undermines customer trust, reputation. A disjointed, disorganized notification response raises questions about whether a business knows what to do in order to recover or is capable of appropriately executing the response."*
>
> *- Forrester Research, Inc.*

3 *Market Overview: Customer Data Breach Notification And Response Services, Forrester Research Inc, August 2015.*

becomes another chance to take advantage of email and steal further personal information. This is the one-two punch of a data breach followed by phishing resulting in identity theft rates exceeding 25% for customers of breach organizations[4], further damaging customer perception of the brand.

HOW NOT TO DO IT: ANTHEM

Following the data breach at Anthem in February 2015, the company had to publicly advise customers that its emails were being spoofed. Piling damage on top of damage, messages purporting to have come from the company and asking for personal information were actually fraudulent.

In Anthem's case there was no indication the email scam was connected to those who perpetrated the security breach. Instead, after Anthem disclosed that its systems had been compromised, phishers and phone fraudsters took advantage of response efforts to trick customers into handing over financial and personal information by using links to fake identity theft monitoring services.

Unfortunately, this is not uncommon. Cyber criminals often use the confusion that follows in the wake of a data breach to initiate phishing campaigns. Often, the phishing emails will look more professional than legitimate notifications, containing one clear call to action and a limited number of web links to convince users of their authenticity. Successful phishing campaigns can be so debilitating that email becomes practically unusable as a communication channel.

Anthem's email notification plan failed on a number of fronts: firstly, they had not taken the necessary steps to secure their outbound email ecosystem prior to the breach, and secondly, the emails they did send were poorly constructed and less crisp than those of the criminals. Finally, consider the lingering impact this will have on Anthem's top-line by disrupting their email marketing engine, reducing consumer spend and increasing customer acquisition costs.

“Often, the phishing emails will look more professional than legitimate notifications, containing one clear call to action and a limited number of web links to convince users of their authenticity. Successful phishing campaigns can be so debilitating that email becomes practically unusable as a communication channel.”

4 *2014 Data Protection & Breach Readiness Guide, Online Trust Alliance April 2014*

As we've seen time and time again, the prevalence of data breaches makes customers more distrustful of the web, causes considerable damage to corporate reputations, dilutes brand equity and impacts revenue. When Anthem was breached, its CEO, Joseph Swedish, acknowledged the damage such a compromise had on customer trust and confidence in the brand claiming that: *"We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can* ***earn back your trust and confidence.***" To limit the impact that data breaches have, a breach notification plan is key.

HOW NOT TO DO IT: OFFICE OF PERSONNEL MANAGEMENT

Further evidence of the complexities surrounding best practice in post-breach management were once again highlighted when the OPM hired a third-party vendor to provide notification and credit monitoring services to victims of its database hack. OPM realized that email was important and included it as a central pillar of the communication plan, but failed badly in its execution.

At the outset, OPM communicated publicly that it would be sending all notifications from a specific email address: "opmcio@csid.com". The notification wasn't a bad thing in itself. However, OPM and CSID made a couple of key mistakes:

- First, they used a third-party domain, csid.com, rather than their own. This is confusing for the people being notified, who don't understand the relationship of CSID to OPM. It opens the door for other, similar third-party domains to make similar claims of being authorized.
- Second, and even more critical: the address was not secure. Anyone could send emails claiming to be from it, and the recipients couldn't tell the difference. So, in effect, they told the criminals exactly what address to spoof to be as effective as possible.

The content and structure of the notification emails, when sent, were also fatally flawed from a security standpoint. The call to action was an embedded marketing tracking link. First, obscuring the destination address behind a large button made it much easier for criminals to create convincing phishing messages. Second, the marketing tracking links referring to third party domains looked so suspicious to those

"Further evidence of the complexities surrounding best practice in post-breach management were once again highlighted when the OPM hired a third-party vendor to provide notification and credit monitoring services to victims of its database hack."

who did look that legitimate messages were incorrectly flagged as phishing. In one example made public, the U.S. Army warned personnel to delete the real notifications.

As a result of these mis-steps, the notification program had to be suspended until the issues could be resolved, and a more secure communication path established. Additionally, within weeks of the data breach, Katherine Archuleta, head of the OPM, announced that she was stepping down, demonstrating the significant repercussions that security compromises--and poorly crafted response to them--can have.

DOING IT RIGHT

Following identification of an attack, organizations need to secure the services of a cybersecurity firm to enhance defence against further attacks and notify the relevant law enforcement agencies. In most cases, data breach notifications are legally required within a specific timeframe that is mandated by the state, country or industry regulatory bodies.

Enterprises also need to publicly disclose the breach and start notifying clients. It is during this period that email becomes key to every data breach notification plan, and should include steps to ensure a secure and authenticated email channel to communicate through. Agari recommends:

- **Keep it simple:** Choose one, simple, easily communicated email address for breach notification. Use a primary brand domain and a short email address, e.g. update@yourcompany.com that is easy for your customers to recognize and remember. Use the same, simple domain as the destination URL for the customer call to action and avoid any embedded links. We strongly advise against using third-party domains or sub-domains, as they will introduce confusion that criminals will exploit.

- **Make it clear how you will direct them to take advantage of any offers**, specifically that you will provide URLs but never ask them to click a link in the email

- **Turn on DMARC for visibility and protection:** Gain visibility into current email traffic on the target domain now, then bring it to a protected status to lock the phishers out and assure that only you can send to your customers.

“Enterprises also need to publicly disclose the breach and start notifying clients. It is during this period that email becomes key to every data breach notification plan, and should include steps to ensure a secure and authenticated email channel to communicate through.”

- **Identify secure vs. insecure email addresses:** Configure your email sending software to deliver important information only to recipient email domains that validate DMARC, and thus are secure. A list of secure domains—covering the vast majority of consumer inboxes in the U.S. and much of Europe—is available at www.agari.com/DMARC-ISPs
- **Use web, press, and social to communicate the plan:** These one-to-many channels are great for setting expectations of what and to whom you'll be communicating personalized information via email. Include:
  - When and from which email address you will communicate
  - Which email domains you will send to and why (it's secure!), and make it clear that no other domains will receive email
  - Set expectations for the content in the emails
  - Clarify how you will direct them to take advantage of any offers, specifying that you will provide URLs but never ask them to click a link in the email
- **Take credit for your readiness:** Regularly update and test your email notification process end-to-end, using the opportunity to tell customers what you're doing to help keep them secure.

Ideally, organizations will have made incremental investments before a breach to ensure that their email channel is ready in the event of a crisis and has been thoroughly tested. By maintaining complete control of the email ecosystem, after a breach, organizations can share data more proactively and build a holistic view of the threats operating in real-time. Only then is it possible to use the cutting edge intelligence available on brand abuse to effectively authenticate email and allow customers to trust that every email landing in their inbox is legitimate in the event of a breach.

Breach is the new normal - plan for it. Your response makes all of the difference.

"Ideally, organizations will have made incremental investments before a breach to ensure that their email channel is ready in the event of a crisis and has been thoroughly tested. By maintaining complete control of the email ecosystem after a breach organizations can share data more proactively and build a holistic view of the threats operating in real-time."

ABOUT AGARI

At Agari we don't think it's ok for cyber criminals to send emails claiming to be you and defraud your customers. Agari Customer Protect is an email security and data analytics product that helps secure your customer email channel by establishing trust and making sure that the only emails your customers get from you will actually be from you. The most respected brands in the world - including Facebook, LinkedIn, Chase and Aetna - have chosen Agari to re-establish trust in their email channel and protect their customers from email based attacks. Rather than relying on the email receivers abuse filters to figure out what's bad, Agari Customer Protect allow you to explicitly tell them what's good, ensuring that email cyber attacks don't reach your customers. With Agari Customer Protect, you can achieve a trifecta win of providing a better customer experience resulting in increased revenue, defending the value of your brand and reducing the financial impact of an attack. Founded by the thought leaders behind Cisco's IronPort solutions, Agari, a recipient of the JPMorgan Chase Hall of Innovation Award and recognized as a Gartner Cool Vendor in Security, is headquartered in Silicon Valley. Learn more at **http://www.agari.com**