Firestorm Founders Forum –
Crisis Lessons Learned in 2015

Firestorm Insights
January 2016

1000 Holcomb Woods Parkway | Suite 130 | Roswell, GA 30076 | 770-643-1114 | **Fax:** 1-800-418-9088
www.firestorm.com

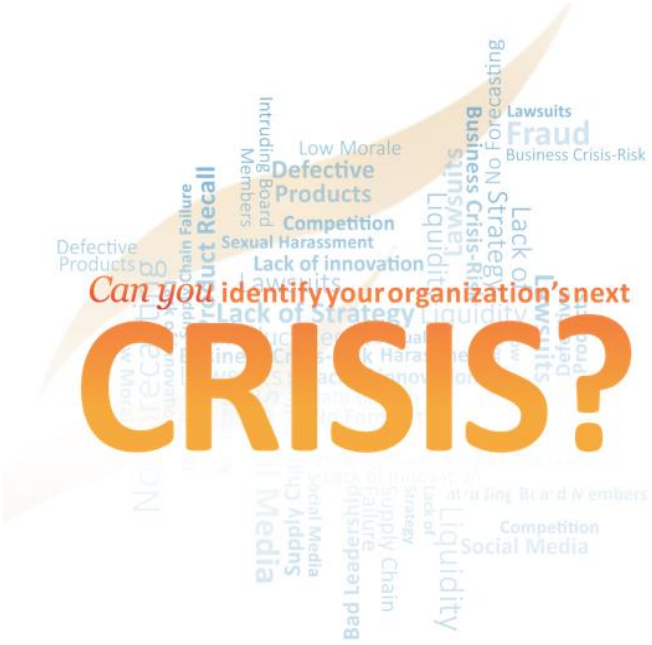
Page Intentionally Left Blank

Firestorm Founders Forum – *Crisis Lessons Learned in 2015*

January 2016

This brief is based on the webinar "Firestorm Founders Forum – Crisis Lessons Learned in 2015" presented by the three Firestorm Founders: Jim Satterfield (President, COO); Harry Rhulen (CEO) and Suzy Loughlin (EVP/CAO).

What Comes to Mind?



Crises of 2015:

> *"The worst disaster you'll ever see is the one that happens to you."*
>
> *-Jim Satterfield*
> *Firestorm President, COO and Co-founder*

Crises of 2015 were significant issues – and issues you might not have seen coming.

- Systemic fraud
- Subway scandal
- San Bernardino Shooting

This last year, however, revealed that communication (or lack thereof) continued to become an organization's next crisis. Initial communication messages that are typically very definitive turn out to be inaccurate.

Every crisis is a human crisis. You must be focused on the consequence management from the beginning of a crisis, as opposed to the crisis itself. A crisis may be very short – it might last seconds or minutes or days – but the consequences will last for an extended period.

All Hazards??

Do you really have an *'all hazards'* plan? Have you identified all the hazards that can, and will, impact your organization? Thinking you have an all hazards plan could cause a false sense of security because there will be issues that you have not planned for.

- Many plans lump all vulnerabilities and threats into one basket.
- 'All hazards' tends to minimize the assessment process.
- 'All hazards' creates a false sense of preparedness.

When creating an 'all hazards' plan, organizations try to combine the vulnerability and threat assessment process into one basket to say that *"we're going to develop plans that are applicable across the board"* to almost any crisis that may arise.

> *"The failure for many organizations and their planning processes is that plans tell people what to do, not how to do it."*
>
> *-Harry Rhulen*
> *Firestorm CEO and Co-founder*

"Employees do things beyond comprehension in a crisis. They do things you could have never envisioned because *you don't tell them how to do the action you're asking them to do*. Although I understand the 'all hazards' approach, I think it's very important that you DO NOT minimize the assessment process."

-Harry Rhulen, Firestorm CEO and Co-Founder

Technology is changing our world so fast, that the business impacts that face your business today are so different than what they were three years ago. The bigger issue is not the false sense of preparedness – it's allowing people to slip back into *"disaster denial."* If you haven't looked at the specific risks- communicable illness, communication planning, etc. - that's a mistake.

Brand Reputation?

*Every crisis is a **human** crisis.*

In 2015, we continued to see a rapid change in technology and communication – specifically social media.

> *"You should presume that whatever the event was, it was captured on video, someone has it and it **will** be shown."*
>
> *-Suzy Loughlin*
> *Firestorm CAO, EVP and Co-founder*

We also saw issues magnified by events that were occurring on the national stage. There were tremendous racial issues in 2015. For our clients, issues that may have been picked up by the media for only a few days - or taken lightly by shareholders or customers - became bigger issues because of the national focus on news stories, a focus enabled through social media channels. ***Crises became magnified for our clients.***

"It's not just you and what you do, but it's the stage on which you're playing that may actually have an effect on your corporation or organization." – Harry Rhulen

In 2015, not enough time was spent talking about victims and the impacts they faced. Such was a theme we saw in the NFL and Subway crises. One of the takeaways has to be that the victim and the attention to the victim should take priority to the disruption that the company has experienced. Talking about the confidence you have in the person who perpetrated the act [and if they did indeed commit the act] shouldn't be the initial commentary of the company.

"Rather, the right thing to do is 'how do we embrace the people who were impacted – the victims'. That's really what the public wants to see and where the communication efforts should initially focus from a brand and reputation perspective."

-Suzy Loughlin

Cyber Breach?

Disaster Due Diligence

It's nearly impossible to 'keep the bad guys out,' [hackers], so being ready on the response side is vital.

What are the tools your organization has in place to detect threats so you are ready to respond when a breach occurs? Unfortunately, many threats will pass through filters. The questions become:

1. What do we do with those [threats that penetrate]?
2. Are we prepared?
3. Have we developed our communication response strategy?
4. Do we know how to protect the individuals that were breached?

Violence

PREDICT.PLAN.PERFORM.®

We want to focus on what can be done before the gun comes to a school or workplace. Focus on:

- Intelligence
- Identification of behaviors of concern

Workplace violence is a huge issue every year – it always has been and always will be.

When you look at statistics, you will see that workplace violence happens everywhere in every industry. More than two million incidents happen annually. If you are not completely aware of what your organization's workplace violence plan looked like, and what the testing and training was from 2015, you need to get familiar with all of that because it is such an important issue.

It is very easy to dismiss some acts of workplace violence (San Bernardino) as episodes of terrorism. That thought process leads people back to 'disaster denial.' If you compartmentalize such acts and think, *"It's terrorism, what can you do?";* you begin to think you are 'off the hook.'

"We want to focus on what to do before the gun comes to a school or workplace."

-Jim Satterfield
Firestorm President, COO and Co-founder

In the case of San Bernardino, the perpetrator had been an employee for five years, who had showed warning signs.

"The question becomes *'how do you recognize behaviors that are exhibited by a person who may be on a path of violence?'"*

-Suzy Loughlin

Discrimination

Actual client crises of 2015:

- Hospitality employee uses a racial slur and customer files complaint with BBB, Human Rights Commission, and political representatives, triggering Attorney General, state legislators and Human Rights investigation across multiple states. Brand and reputation were under attack.
- Employee includes discriminatory language in an advertisement, triggering a national media event, political demonstrations, death threats, etc. Not only are brand and reputation under attack, but municipal healthcare contracts risk being terminated, which would trigger the demise of the company employing 500 people.

Neither one of the discriminatory statements were actually made by a client's employee. The statements, however, were attributed to the organization and still caused a crisis of significant proportions. You must train your employees on how to deal with a discriminatory comment, even if made by a vendor or customer. If it comes back to your organization, you end up owning the statement. Once a legislature or any other public figure gets ahold of the information, they don't care about you or your organization, they use ***YOU*** as the platform.

When you are handling events that center on discrimination, you need to know your stakeholders. You must know who it is you need to communicate with and most importantly, what are the impacts? Are the impacts legal, reputational, regulatory and/or financial?

You HAVE to be prepared before an event occurs – message maps, talking points, key stakeholders and impacts.

Sexual Abuse

Actual client crises of 2015:

- Staff member arrested for possession of ***child pornography***, triggering media inquiries and the need for crisis communications and crisis PR, to prevent injury to brand and reputation.
- Employee installs **cameras in a rest room**, filming children. Criminal proceeding against employee. Brand and reputation under attack.

- Camp doctor gets charged with **sexual abuse** of a student at a school where he also works. Media references camp, although there is no allegation of abuse of any child at the camp. Investigation required. Parents fearful. Brand and reputation under attack.

> *"How do we identify if there is sexual abuse? How do we know if company computers are being used inappropriately?"*
>
> *-Jim Satterfield*
> *Firestorm President, COO and Co-founder*

What type of employment screening was conducted prior to hiring an employee? In most sexual abuse cases Firestorm was called upon, it was the first offense. Perpetrators had clean records because they had never committed an act prior, or because it was the ***first time they were caught.***

Employee background checks are important, but so is supervision of employees and Behavioral Risk Threat Assessment (BERTHA).

Violence

- **Suicide** of prominent physician takes place at the large medical practice where he works. Grief counseling needed for employees; communications required for patients.
- **Home invasion**- murder of patient, injuries to home health aide. Communications required for all stakeholders who don't feel safe at work.
- **Shootings** at public high schools. Communications needed for all stakeholders. Aggressive media involvement. Strategies developed to honor victims and mitigate damages.

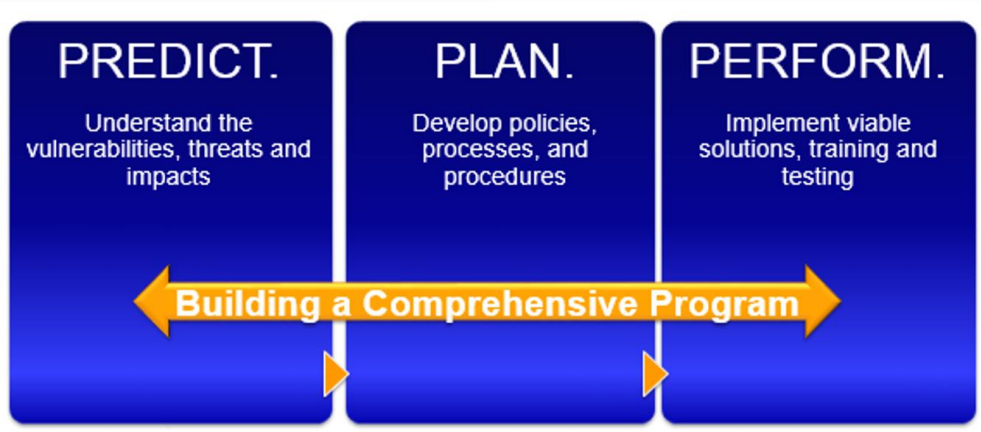
> *"Up to 60% of your employees could turn over in the following 18 months following a workplace death related to violence."*
>
> *-Suzy Loughlin*
> *Firestorm CAO, EVP and Co-founder*

What Did We Learn in 2015?

- **Communications during a crisis continues to become the next crisis for the organization.** We must have pre-identified stakeholders, message maps and pre-determined channels for communication by trained spokespersons.

- **Cyber risk is a business problem, not an IT problem. It affects everyone.** We must do the predictive work to understand how a cyber breach will affect what each of us is doing.
- **Violence is ever-present.** Warning signs are exhibited- -we need to watch for them.
- **Rate of change- results in emerging threats and new risks.** We need to monitor for them via predictive intelligence capabilities.

Advice?



- ***Continue down the path*** - Don't assume that where you are is adequate. Rate of change requires that you are constantly 'moving the ball down the field,' and looking at vulnerabilities, threats and changes. ***Understand the world around you is changing. – Harry Rhulen***

- ***Broaden the involvement -*** Broaden the involvement of who is included in your planning initiatives. The answer is: *everyone*. What we want to see is a culture of preparedness. This results from predictive work (**predict**); steps to mitigate (**plan**); and finally, if confronted with a threat, people know what to do (**perform**). ***– Suzy Loughlin***

Next Steps

Do you want to know what will happen tomorrow?

Can you afford not to know?

Contact Firestorm to learn how to:

Participate in a Virtual Workplace Violence/Active Shooter Exercise with your team:

February 8th (Businesses)

Let Us Help You Identify Threats Before a Crisis Occurs

- Risk of Harm
- Compliance/Legal Risk
- Operating Risk
- Reputation Risk

February 18th (Schools)

Align your plans to best practices

Create your own ***Intelligence Network***

Schedule *CRISIS COACH*® training

Attend any of our other webinars by registering here.

View previous Webinars on our YouTube Channel.

No-Fee Self-Assessment

Receive a no-fee, Self-Assessment & Expert Analysis ($2,500 value).
Link: http://www.firestorm.com/engage-us/contact-firestorm

Contact Us

www.firestorm.com | (800) 321-2219 | 1000 Holcomb Woods Parkway Suite 130 Roswell, GA USA 30076