Firestorm and Black Swan Solutions Presents: Cyber Attack: *Human Impact Lessons*

Firestorm Insights
September 2015

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

Page Intentionally Left Blank

Cyber Attack: *Human Impact Lessons*

September 2015

The webinar "Cyber Attack: Human Impact Lessons" was presented by Jim Satterfield, President, COO and Co-Founder of Firestorm and Michelle Colosimo, Black Swan Solutions Director.

We discussed lessons learned from bad things happening, communications breakdown and today, Cyber Attack: *Human Impact Lessons.*

Previous Webinar discussions:
Firestorm and Black Swan Solutions Present: Crisis Management – Tools for the 21st Century
Firestorm and Black Swan Solutions Present: Communication Breakdown (It's Always the Same)

What do YOU need to know?

- Cybersecurity is a Business issue and NOT an IT Issue.
- Most Breaches are the Result of People not Following Protocols.
- What are your Organization's 'Crown Jewels'?
- What 'Other Records' do Thieves Want and Why?
- Does your Board, Senior Management and Employees Understand:
  - Situational Awareness?
  - Your Corporate Strategy and Operations?
  - Incident Response Plan?
  - Crisis Communications Plan?

> *"The FBI categorizes companies into two categories: Companies that know they have had a cyber breach and those that have had a cyber breach, but don't know it yet."*
>
> *-Jim Satterfield*
> *Firestorm President*

More Information About Breaches

- The Average Breach in U.S. involves **29,087 records**
- Average Breach is undetected for **240 days**
- Average Breach Notification Costs **$509,237**
- Average Lost Business Costs **$1,599,996**
- **Industries most Targeted:**
  - Pharmaceutical
  - Financial
  - Healthcare

- Services
- Technological
- Retail is small, but had most 'catastrophic breaches'

Costs of a Data Breach – 2014 Ponemon Cost Study

- **Each stolen record costs $201 per record**
- **Higher costs:**
  - Stolen Devices $16.10
  - Third Party Involvement in Breach $14.80
  - Quick Notification $10.45
  - Engaging Consultants $2.10
- ***Reduce this cost by:***
  - *Strong Security Posture -$14.14*
  - *Incident Response Plan -$12.77*
  - *CISO Appointment -$6.59*

> *"Today, 80 percent of the assets in a company are information only oriented."*
>
> *-Jim Satterfield*
> *Firestorm President*

This Data is for the Average – Not a Catastrophic Loss!

Facts about Intrusions

- **62%** of all companies breached learned about the breach from customers.
- **42%** of the CISO's say they lack the budget and personnel to effectively detect and prevent breaches.
- **70%** of all retail respondents said they had been breached.
- **57%** retailers said suppliers were liable for breach.
- **2 of 3** victims of identity theft are informed that their PII data had been breached and did nothing about it.

Most threats come from the inside

- **Most Cyber Breaches come from Intrusion, *not* outsiders.**
- **According to experts Sony was most likely an inside job.**
- **Most companies overwrite their systems making prosecution impossible.**
- **Cyber Security comes down to 2 questions:**
  - What information and secrets are you protecting?

- Who are the actors that want them?

- **Knowing what to do and say <u>before it happens</u> is critical.**

Large Business Data Breaches – 2013-2015: A Quick Glimpse

Target	Date	Impact
Premera Blue Cross	3/2015	Approx 11 million records affected
Anthem	2/2015	Approx 80 million records affected
Sony Pictures	11/2014	To Be Determined
Staples	10/2014	1.16 million credit cards impacted
Home Depot	09/2014	56 million credit cards impacted

Target	Date	Impact
JP Morgan Chase	07-08/2014	83 million households and small businesses were impacted
Community Health Systems	06/2014	4.5 million patients impacted
Michaels Stores	04/2014	3 million payment cards
Target	12/2013	40 million credit/debit cards impacted

Three C's of Crisis Communications

- ***<u>Coordination</u>*** **–** communications internally to direct coordination activities regarding cyber breach response and recovery.
- ***<u>Crisis</u>*** **-** communications to address the potential crisis impacts on brand and reputation.
- ***<u>Compliance</u>*** **-** communications responsibilities related to compliance notification to those parties who are impacted (or potentially impacted) by a cyber breach. These communications serve the duel purposes of notification and remedy actions to mitigate or prevent potential impacts.

Lessons Learned from 2015 Breach Event

Today, Black Swan Shares Lessons Learned

What to do ***BEFORE*** an attack occurs:

- Know state notification regulations:
  - Who gets notified?
  - When do they get notified?
- Prepare key teams – ensure everyone knows roles and responsibilities.
- Collaborate with your vendor partners.
  - *"If you don't talk to them ahead of time and understand what they can do for you and what they cannot do for you… it is going to be problematic [during a crisis]."* – Michelle Colosimo, Black Swan Solutions Director

> ***Know state notification regulations:***
> ***"It's not a one-size-fits-all."***
> *-Michelle Colosimo*
> *Black Swan Solutions Director*

What to do ***After*** an attack occurs:

- Early involvement and transparency with key teams and/or departments.
- Be cautious in messaging – but not too cautious!
    - Do not spend too much time crafting a message.
        - This action causes time delay – potentially causing further implications.
    - Have messages pre-written and pre-approved so they are readily available.
- FAQ document/Message Maps – provide early, update often.
    - Avoid having too many documents – create a 'universal FAQ' document.
- Identify internal go-to contacts.
- Communicate regularly with response vendors – especially call center.
- Address NEEDS – it's more than just script reading.
- Maintain centralized location – and process – for documents.
    - Know:
        - Who was the last one to revise a document?
        - When was the last time a document was updated?
    - Get the right message to the right person at the right time.
- Focus must be on impact to organization, not feelings.
    - Make decisions based on the impact on the organization, not whose feelings you may hurt.
    - Do not make decisions based on emotions.
- Remember – employees impacted, too.
- Be compassionate. Always.

> *"You can't be worried about hurting someone's feelings when responding to a [crisis] event."*
>
> *-Michelle Colosimo*
> *Black Swan Solutions Director*

Cyber Event Communications

- **PREDICT.PLAN.PERFORM.®**
- **Why**
  - Coordination
  - Crisis
  - Compliance
- **What**
- **When**

Advantages of having someone on the outside help you handle a crisis:

Internally, people want to help and be supportive before, during and after a crisis. People who are involved, however, are personally impacted by the events. Even if they were not necessarily hurt or injured, they are tied to that organization.

When organizations use their own internal resources to respond to crises, people do not come back to work because it creates a secondary trauma. You want to protect your employees; you want to help and support them. You want to make sure you have people who are trained and have expertise to be able to help employees and the situation.

Companies like Black Swan have the ability to respond instantly and give support to organizations in need. They ensure you get your organization's message relayed to the public and stakeholders.

Firestorm also encourages you to learn more about Black Swan Solutions by visiting blackswancrisissolutions.com or contacting Michelle Colosimo directly at 888-723-2466.

Next Steps

Do you want to know what will happen tomorrow?

Can you afford not to know?

Contact Firestorm to learn how to:

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.

Download a Brief from previous sessions.

Thanks to Black Swan Solutions

888-723-2466
Blackswancrisissolutions.com

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