But it Was Such a Little Phish

February 2016 Webinar

Firestorm Insights
February 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

But It Was Such A Little Phish

February 2016

This brief is based on the webinar "But It Was Such A Little Phish" presented by Jim Satterfield, Firestorm President, COO and Co-Founder.

Phishing is a Means to a Cyber Breach

- The chance of a cybersecurity breach to your business increases every day.
- Phishing is one of the means to a cyber breach.
- If this happens, your business will be impacted at many levels: the human level, the operational level, the reputational level and the financial level.

In this brief, we will discuss what you need to know and do to prepare for the phishing.

Today

- Cyber Breach
- Phishing
- What to look for
- Types
- What to do
- Next Steps

> *"I literally work with rocket scientists, and I can't get them to stop clicking the wrong links, so what chance does your organization have?"*
>
> *Michael Redman, U.S. Army Missile Defense*

"Run the business…no matter what"

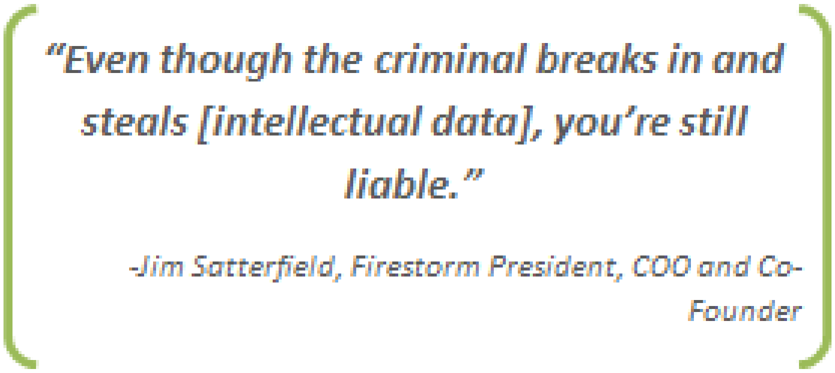
Today, 80 percent of the value of corporate assets has shifted from physical to virtual.

Definition of Cyber Breach

The term **cyber breach** represents the events that could negatively impact your organization with respect to the following:

- All your information assets including hardware, network infrastructure, software, data in electronic and physical form (e.g., paper) and human knowledge.

- Communication, storage and processing of data by any means resulting from your actions/obligations.
- Unauthorized security events resulting from intentional or unintentional electronic or human actions.



> *"Even though the criminal breaks in and steals [intellectual data], you're still liable."*
>
> *-Jim Satterfield, Firestorm President, COO and Co-Founder*

Phishing

- ***Every crisis is a human crisis***
- PICNIC (Problem In Chair Not In Computer)
  - It is not the computer's fault; the computer worked how it was supposed to
- Fishing is always good; it's the catching that matters
- Criminal
- Lure / Fake Bait
- The criminals are looking for your information so they can use it to commit fraud
- Why do criminals do it? It works

Attributes of a Cyber Breach

- ***Criminal Act** of others that you can be liable for*
- Escalating flow of events
- Insufficient & inaccurate information
- Intense scrutiny - highly personal
- Loss of command and control
- How you respond can create a second crisis
- Brand & reputation are under attack
- Every crisis is a human crisis
- Silence = Guilt
- ***Surprise***

Phishing

- Phishing email messages, websites and phone calls are designed to steal money.
- Criminals seek to install malicious software on your computer or to steal personal information from your computer.

- Criminals leverage social engineering to convince you to install malicious software, download something or hand over your personal information under false pretenses.
- Phishing takes advantage of ***your trust*** since you may not be able to tell that the site being visited, link, email or program being used, is ***not*** real.
- As a result, the criminal has the chance to gain the personal information of the targeted user, such as passwords, usernames, security codes and credit card numbers, among other things to gain access.

Sensitive Information

HR and other employee data such as:

- Resumes existing and new
- Employment applications
- Background tests
- Direct deposit voided checks
- Disciplinary actions
- Addresses
- Health insurance applications and claims
- Rehab participation
- Personal information that may make them unemployable
- Unpublished phone numbers
- Private email addresses
- Passwords and login credentials
- Certificates
- Encryption keys
- Tokenization data
- Network and infrastructure data

Commercial Information

- Bank account and transit routing data
- Credit/debit cards
- Financial banking\trading account data
- ACH (Automated Clearing House) credentials and data
- Designs, plans, diagrams
- Merger, acquisition, divestiture documents
- Marketing plans and customer lists
- Strategic plans
- Intellectual property
- Product designs, plans, formulas, recipes
- Legal investigations conducted by the organization
- Sealed bids
- Contract information between company and third parties
- Trade secrets or intellectual property such as research activities
- Location of assets
- Linking a person with the specific subject about which the user has requested information or materials
- Configuration of technology assets (e.g., network diagrams, firewall configurations, etc.)

What do you look for?

- **Spelling and poor grammar.** Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not allow a mass email with errors to be distributed to its users. If you notice mistakes in an email, it might be a scam.
- **Beware of links in email.** If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message.
- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message?
- **Spoofing popular websites or companies.** Scam artists use graphics in emails that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.

Examples of Phishing Messages

- *“You won a $100 gift card from Walmart, please click here.”*
- *“We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*
- *"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."*
- *“Our records indicate that your account was overcharged. You must call us within 2 days to receive your refund.”*

Spear Phishing

- ***Spear Phishing –*** threats directed at specific, targeted individuals or companies.

- Attackers may gather personal information about their target to increase their probability of success.
- This technique is, by far, the most successful on the Internet today, accounting for the majority of attacks.

Clone Phishing

- ***Clone Phishing*** uses a legitimate, and previously delivered, email containing an attachment or link and has had its content and recipient address(es) taken and used to create an almost identical or cloned email.
- The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender.
- It may claim to be a resend of the original or an updated version to the original.

> ***"The FBI tells us there are two types of organizations: those that know they have been breached, and those that have been breached and do not know."***
>
> *-Jim Satterfield, Firestorm President, COO and Co-Founder*

Whaling

- ***Whaling*** directed specifically at senior executives and other high profile targets within businesses.
- The content will be crafted to target an upper manager and the person's role in the company.
- The content of a whaling attack email is often written as a legal subpoena, customer complaint or executive issue.
- Whaling scam emails are designed to masquerade as a critical business email, sent from a legitimate business authority.
- The content is meant to be tailored for upper management, and usually involves some kind of falsified company-wide concern.

Phishing Phone Calls

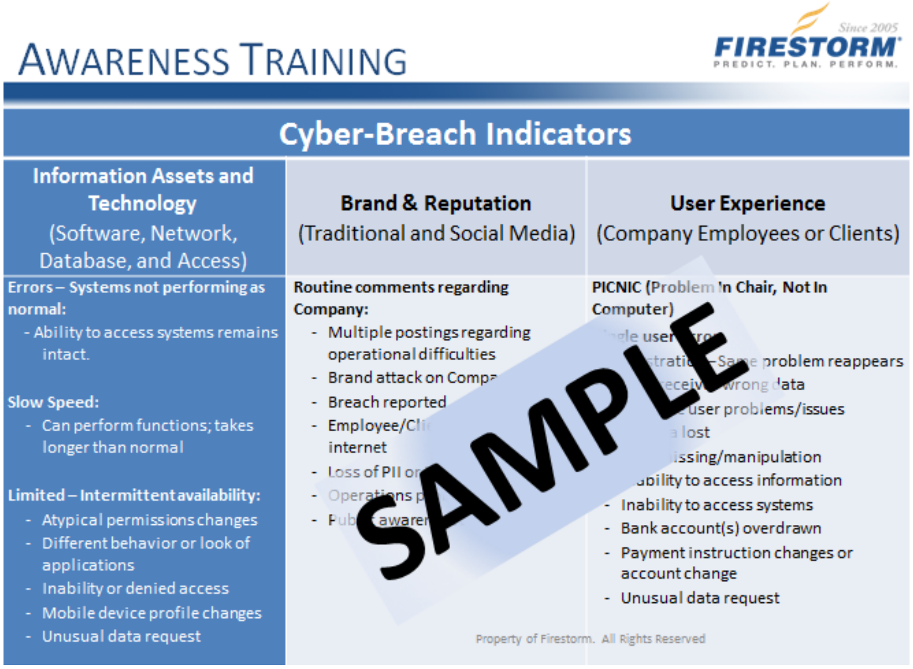
- Criminals call you to offer to help solve your computer problems or sell you a software license. Apple, Microsoft or their affiliates make unsolicited phone calls (also known as cold calls) to charge you for computer security or software fixes.
- Gaining your trust, criminals ask for your user name and password or ask you to go to a website to install software that will let them access your computer to fix it. Once you have given the information, your computer and your personal data are vulnerable.
- Treat all unsolicited phone calls with skepticism. Do not provide any personal information.

How to Deal with Phishing

- ***Use*** trusted security software and set it to update automatically. **(70% of breaches occur within 5 days after a patch is announced).**
- ***Do not email*** personal or financial information. Email is ***not*** a secure method of transmitting personal or corporate financial information.
- **Provide** personal or financial information ***only*** through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins **https** (the "s" stands for secure). Unfortunately, no indicator is foolproof; criminals can forge security icons.
- **Review** credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.
- **Use** caution opening attachments or downloading files from emails, regardless of who sent them. These files can contain viruses or other malware.

> ***"On average, the criminal is inside your network for 240 days prior to detection."***
>
> *-Jim Satterfield, Firestorm President, COO and Co-Founder*

Awareness Training



AWARENESS TRAINING

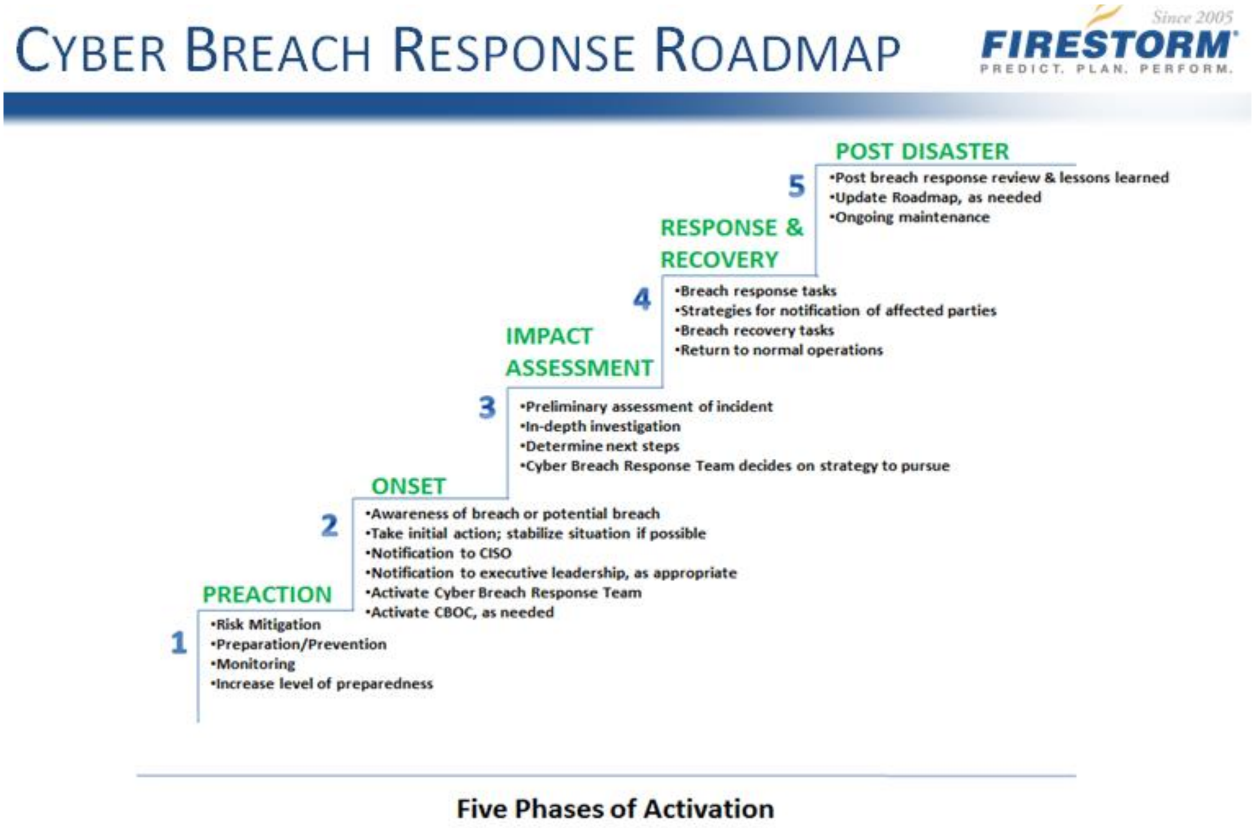
FIRESTORM Since 2005 PREDICT. PLAN. PERFORM.

Cyber-Breach Indicators

Information Assets and Technology (Software, Network, Database, and Access)	**Brand & Reputation** (Traditional and Social Media)	**User Experience** (Company Employees or Clients)
Errors – Systems not performing as normal: - Ability to access systems remains intact. **Slow Speed:** - Can perform functions; takes longer than normal **Limited – Intermittent availability:** - Atypical permissions changes - Different behavior or look of applications - Inability or denied access - Mobile device profile changes - Unusual data request	**Routine comments regarding Company:** - Multiple postings regarding operational difficulties - Brand attack on Compa[illegible] - Breach reported - Employee/Cli[illegible] internet - Loss of PII or [illegible] - Operations p[illegible] - Pub[illegible] awarer[illegible]	**PICNIC (Problem In Chair, Not In Computer)** - Single user error - Frustration – Same problem reappears - Receive wrong data - [illegible] user problems/issues - [illegible] lost - [illegible] missing/manipulation - Inability to access information - Inability to access systems - Bank account(s) overdrawn - Payment instruction changes or account change - Unusual data request

Property of Firestorm. All Rights Reserved

Cyber Breach Response Roadmap



CYBER BREACH RESPONSE ROADMAP

FIRESTORM® Since 2005 PREDICT. PLAN. PERFORM.

5 POST DISASTER
- •Post breach response review & lessons learned
- •Update Roadmap, as needed
- •Ongoing maintenance

4 RESPONSE & RECOVERY
- •Breach response tasks
- •Strategies for notification of affected parties
- •Breach recovery tasks
- •Return to normal operations

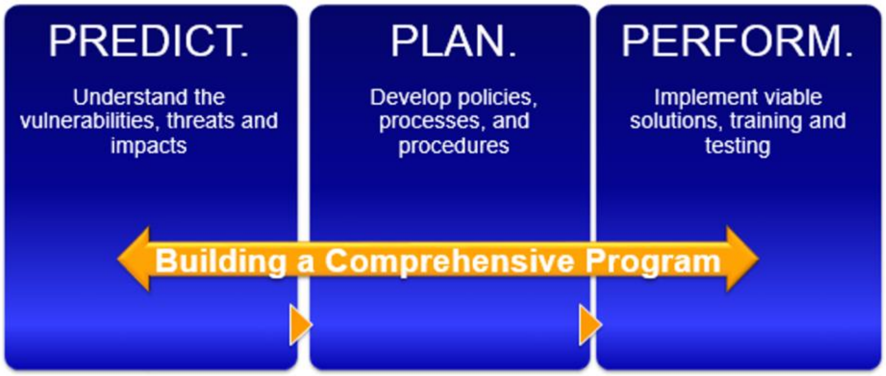
3 IMPACT ASSESSMENT
- •Preliminary assessment of incident
- •In-depth investigation
- •Determine next steps
- •Cyber Breach Response Team decides on strategy to pursue

2 ONSET
- •Awareness of breach or potential breach
- •Take initial action; stabilize situation if possible
- •Notification to CISO
- •Notification to executive leadership, as appropriate
- •Activate Cyber Breach Response Team
- •Activate CBOC, as needed

1 PREACTION
- •Risk Mitigation
- •Preparation/Prevention
- •Monitoring
- •Increase level of preparedness

Five Phases of Activation

PREDICT.PLAN.PERFORM.® Methodology



PREDICT.
Understand the vulnerabilities, threats and impacts

PLAN.
Develop policies, processes, and procedures

PERFORM.
Implement viable solutions, training and testing

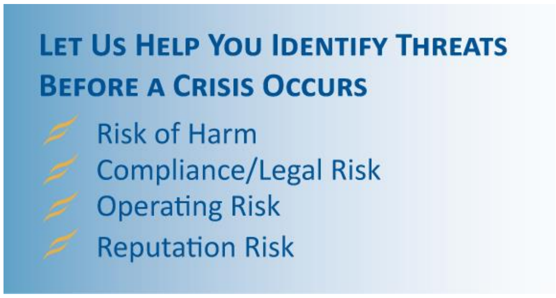
Building a Comprehensive Program

What Must You Do?

- Have good processes and controls based on
    - Need to know access ***only***

    - Internal monitoring of access
- ***Train, Train, Train***
- Identify all software and devices used in business:
    - BYOD policies make organizations susceptible to breach
    - Unauthorized devices and software need to be eliminated
- All experts agree that all companies have been hacked, ***being prepared is more important than believing you can stop it***
- Demonstrate *"Degree of Reasonable Care"*

Next Steps



LET US HELP YOU IDENTIFY THREATS BEFORE A CRISIS OCCURS

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

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 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