SEFF
CYBER BREACH
WORKSHOP & EXERCISE

Presenters

- **David Bridges**
  President
  The Leavitt Group of Atlanta, Inc
- **Jack Healey**
  Managing Director
  Business Crisis Prevention & Performance Group
  Firestorm Solutions, LLC
- **Jim Satterfield**
  President/Founder
  Firestorm Franchising, LLC

Attributes of a Crisis or Disaster

- Escalating Flow of Events
- Insufficient & Inaccurate Information
- Intense Scrutiny
- 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

Southeast Franchise Forum

Can you identify your organization's next CRISIS?

We Can.

What do YOU need to Know

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

Test Exercise

Disclaimer

Definition of Cyber Breach

For the purposes of this test exercise, the term **cyber breach** represents the events that could negatively impact your franchise system 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; and/or
- Unauthorized security events resulting from intentional or unintentional electronic or human actions.

This cyber-breach test exercise is architected to be conceivable, while not specifically addressing your technical, information-security controls. This exercise is designed to simulate and test the Cyber-Breach Response Team's response to a cyber-breach incident. It is not designed to detect gaps in technical security controls currently in place.

Test Exercise Objectives

1. ***Validate and understand*** the monitoring process for a cyber-breach incident
2. ***Identify*** the impacts of a cyber breach on franchise system, its franchisee, employees, clients, subsidiaries & their employees/clients, shareholders, regulators, and the public at each phase
3. ***Understand*** the communications process and content throughout the phases
4. ***Determine*** how to adjust the communications strategy throughout the cyber breach
5. ***Define*** opportunities to improve plans
6. ***Use*** your plans

Rules of the Road - Assumptions and Instructions

- Respond based on ***your*** understanding of current plans.
- Make ***your*** best decision based on situations given.
- Draw upon ***your*** own understanding of how well your franchise system and law enforcement work together in emergencies.
- Decisions do ***not*** reflect the position of your franchise system on any given issue.
- There is ***no*** predetermined solution to this exercise.
- ***You*** **are *"On-the-Clock"***

Group EXERCISE

Rules:

- Quick Data Breach Escalation Event
- **No wrong answers**

Your Franchise System

- Your are the Franchisor CFO
- Your franchisees provide in home services in all 50 States and are regulated in all 50 States
- You are on the Business Crisis Response Team for your System
- CEO is breathing down your neck for numbers for Board meeting

Phase 1 – 4 AM EST Charlotte/West Coast Franchisees Not Available

Situation(s)

- All network traffic/systems running extremely slow to include: Outlook, Oracle, Internet, website etc.
- RTB (run the business) at this time

- IT begins running diagnostics (operating at one-third capacity)
- Security experts estimate 24-48 hours to resolve

king News Breaking News Breaking News Breaking News Brea

Phase 1 – March 1st

Situation(s)
Typical First Quarter Pressures - Annual Report, FDD Filings, and upcoming Board and Committee Meetings are immediate priorities
While everyone is hustling and focusing on the final numbers, Operating Systems, email, and Franchisee Link seem slower than normal.

reaking News   Breaking News   Breaking News Breaking News   Br

Phase 1 – Exercise Decisions

- What do you know?
- Are you concerned?
  - If so, about what?
- What is your plan?
- What are you going to monitor?
  - How? Who?
- What are you going to communicate?
  - How?

__You__ are "On-the-Clock"

PHASE 2

SITUATION(S)
Strange call from a Franchisee '*I got your notice*' where is it that you need me to upload all the information again?
Systems are non responsive. Board member calls and asks why Franchise website is down.

reaking News   Breaking News   Breaking News Breaking News   Br

Phase 2 – Exercise Decisions

- What changed?
- What do you know?
- Are you concerned?
  - If so, about what?
- What is your plan?
- What are you going to monitor?
  - How? Who?
- What are you going to communicate?
  - How?

You are *"On-the-Clock"*

Phase 3

Situation(s)

Internet Customer Lead Service cannot access systems. ERP System and Oracle are not working.

Illinois Commissioner calls and asks, “*why is Franchisor closing all franchisees in Illinois and leaving the state?*”

Law Enforcement contacts Franchisor and asks Franchisor to leave servers alone for potential evidence and not announce cyber-breach publically. General Counsel informs leadership that Franchisor must include the cyber-breach in the FDD.

eaking News   Breaking News   Breaking News Breaking News   Bre

Phase 3 – Exercise Decisions

- What changed?
- What do you know?
- Are you concerned?
  - If so, about what?
- What is your plan?
- What are you going to monitor?
  - How? Who?
- What are you going to communicate?
  - How?

__You__ are "On-the-Clock"

Phase 4

Situation(s)
Hundreds of customer cancellation notices are received.
Financial Reporting is unable to verify information and numbers.
Reporter calls for background on a story regarding personal and medical information being posted on social media related to franchisees, employees, and customers.
Multiple calls received asking why no one showed up for their appointments with customers.
Critical Supplier exercises option for *'immediate termination for clause'* provision in contract.

aking News   Breaking News   Breaking News Breaking News   Bre

PHASE 4 – EXERCISE DECISIONS

- What changed?
- What do you know?
- Are you concerned?
  - If so, about what?
- What is your plan?
- What are you going to monitor?
  - How? Who?
- What are you going to communicate?
  - How?

You ***are "On-the-Clock"***

POST-EXERCISE HOTWASH

Southeast Franchise Forum

- A hotwash is the "*after-action*" discussions and evaluations of performance following an exercise, training session, or major event.

- The main purpose of a hotwash session is to identify strengths and weaknesses of the response to a given event.

- The "*lessons learned,*" will guide future response direction in order to avoid repeating errors made in the past.

Hotwash/Test Exercise Debrief

1. Did the exercise reveal any weaknesses in your planning, readiness, and recovery?
2. What tasks must you complete to improve preparedness, planning, response or recovery?
3. What are your top 3 priorities?
4. What were the impacts?

Hotwash Actions

- **Review** and evaluate the cyber-breach incident
- **Obtain** feedback from all participants on what worked and what didn't work
- **Note** issues of command, control, coordination, and communication
- **Have** each function/business unit chairs report on their experiences
- **Identify** and prioritize key lessons learned
- **Gather** cost accounting detail
- **Gather** visual records of event, e.g. digital or hardcopy photos, newspaper reports, internal and external communications
- **Evaluate** the existing plans
- **Identify** the need for further training and tests
- **Make** suggestions for improvement
- **Provide** feedback
- **Document** a summary of the current state of your plan including processes included, excluded, and any open items (or planning gaps). Emphasis should be given to potential issues and the results expected.

ONE BILLION…

- Electronic records breached and reported in the media in the past twelve months!

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 supplier were liable for breach
- 2 of 3 victims of identity theft are informed that there PII data had been breached and did nothing about it.

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 Report

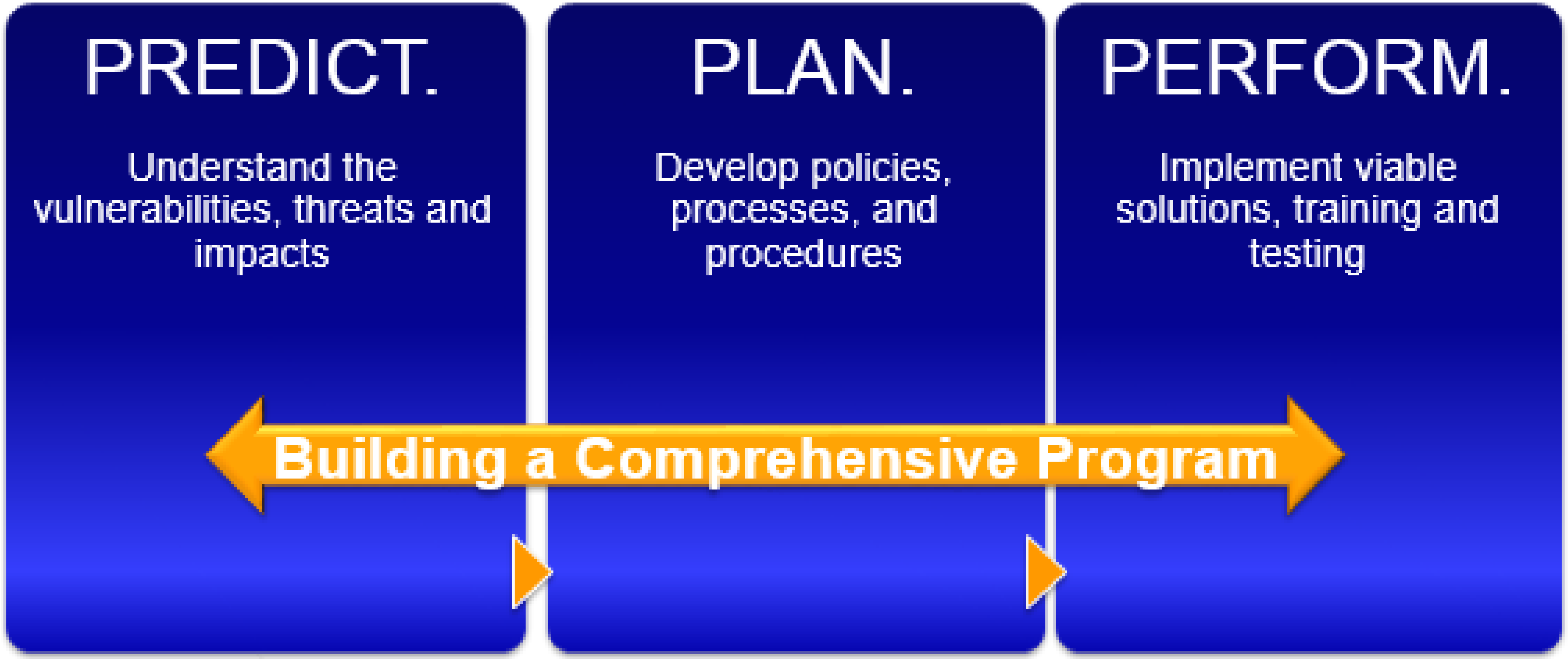
- Each stolen record costs $201 per record
- Higher costs:
  - Stolen Devices $16.10
  - Third Party Involvement in Breach $14.80
  - Quick Notification $10.45
  - Engaging Consultants $2.10
- *Reduce this cost by:*
  - *Strong Security Posture -$14.14*
  - *Incident Response Plan -$12.77*
  - *CISO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

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

So What Should You Know?

- ***Recognize*** Data Breach is NOT an IT Problem, But a Human Problem
- *Know* What Data you have, who would want it, how to protect it, and what to do if you lose it!
- *Need* to be PREPARED! Data Breach Business Crisis-Risk Plan
- *Train* Organization to recognize the *INDICATORS* of a Breach
- *Test* your Plans
- Understand the risks you should transfer
- *Establish Intelligence Network*

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

CYBER RISK

- Cyber Risk takes on many faces, but the common element s are the tools, tactics and motivations amount to fraud.
- Cyber Risk is a Business Crisis Risk, which means the methodology to PREDICT.PLAN.PERFORM® is similar to any other business risk
- Good news is the tactics used will equal the defenses an organization has in place
- Bad news is that the human element will always be a factor, so prevention is almost futile

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 over write there 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 *before it happens* is critical

What Data is Susceptible?

- Intellectual Property- ‘Crown Jewels’
  - Franchisor’ and Franchisees’ *most critical* assets
  - What you need to run your system will vary
- Personal Identifiable Information (PII)- worth $6-$40
- Protected Healthcare Information (PHI)- worth $60-$125
- Where do they reside- One system or multiple systems
- How are they accessed? Who has permission

What is a Franchisor Do?

- Need to have good processes and controls based on
  - Need to know
  - Internal monitoring of access
- 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*
- Franchisor’s and Franchisees’ duties: *“Degree of Reasonable Care”*

What is a Data Breach?

- An event which an individual's name/medical record and/or a financial record/ debit card is put at risk
- An event where business records/data including IP, employee PII, PHI information is stolen or altered
- Three main causes:
    - **Criminal Attack**
    - **System Glitch**
    - **Human Error**

Cyber Threat Drivers: MICE

M.I.C.E

- Money
- Intelligence
- Coercion
- Ego
- (R)etaliation

SYSTEM "GLITCH"

- The 'accidental' disclosure or release of Data
- Unintended access to systems by third parties (Target, HD)
- Monitoring Controls are vital to know what data is accessible
- Myriad of IT Systems raises risk of inadvertent access (Fazio)
- Most likely poor controls, lack of testing
- *HUMAN ERROR is root cause. – **'PICNIC'***

The Future of Business Continuity & Resilience

- Business Crisis-Risk™ is the risk(s) imbedded in an organization due to ***structural*** *design or a breakdown in* ***operational*** *and/or* ***functional*** *processes*.

- If not eliminated, these risks will result in a disproportional adverse event that will impact ***people, profitability, brand and/or reputation.***

- Preparing for these risks is the responsibility of management; unfortunately most management teams do not know how to ***identify these impending risks before they occur***.

Before *Now*™

Embedded Business Crisis-Risk™

- **Structural**
  - Refers to the organization of management, the communication of information and the behaviors of senior leaders.
- **Operational**
  - Refers to how a company handles basic business processes.
- **Functional**
  - Refers to the normal silos that you find in an organization.

Why is Business Crisis-Risk™ Important?

- Study of business crisis-risk indicate that ***most crisis can be foreseen*** and management chooses not to prepare.

- Our research has shown that *business crisis-risk falls into identifiable patterns '**INDICATORS**' shaped* by severity and frequency

- Identifying these risks ***empowers management to avoid or mitigate*** the financial and human impact events which have crippled many companies

Attributes of Crisis- Complexity

A targeted crisis:

- Easily identifiable
- Only become complex due to ineffective crisis management
- Mitigate is more straight forward

A complex crisis:

- Many attributes
- Attributes maybe competing (data breach)
- Requires a much more sophisticated response
- More pressure on management to '*get it right*'.

Attributes of a Crisis - Time to React

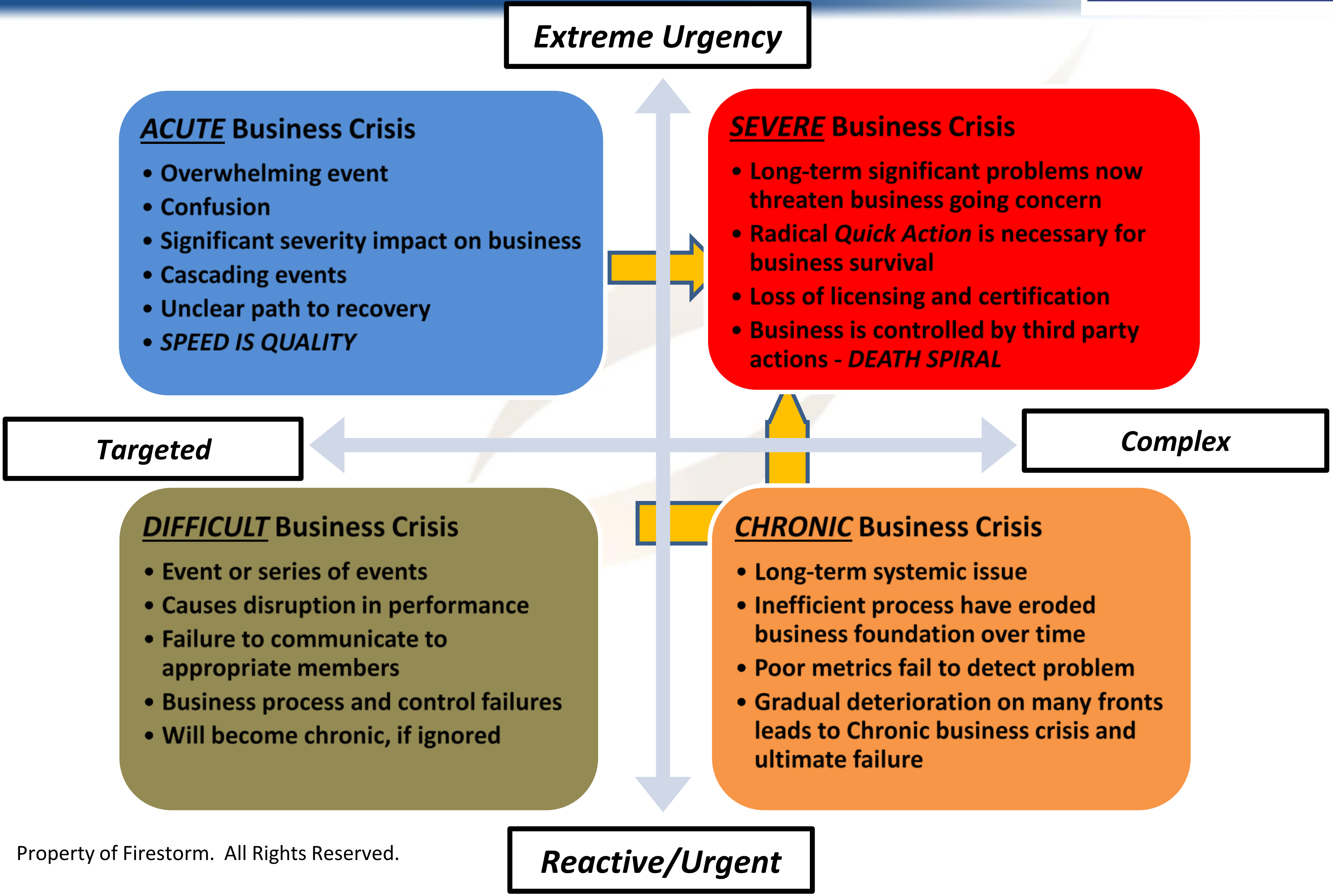
Reactive/Urgent

- *You* are focused on the event
- The organization is not '*all consumed*'
- Able to carry on most other business functions while the crisis is occurring.

Extreme Urgency

- Organization is consumed by the event.
- All business processes are involved in the mitigation
- The organization is not functioning in an efficient manner
- The event is an all-consuming activity.

The Business Crisis Predictive Diagnostic Model™



Extreme Urgency

ACUTE Business Crisis

- Overwhelming event
- Confusion
- Significant severity impact on business
- Cascading events
- Unclear path to recovery
- *SPEED IS QUALITY*

SEVERE Business Crisis

- Long-term significant problems now threaten business going concern
- Radical *Quick Action* is necessary for business survival
- Loss of licensing and certification
- Business is controlled by third party actions - *DEATH SPIRAL*

Targeted

Complex

DIFFICULT Business Crisis

- Event or series of events
- Causes disruption in performance
- Failure to communicate to appropriate members
- Business process and control failures
- Will become chronic, if ignored

CHRONIC Business Crisis

- Long-term systemic issue
- Inefficient process have eroded business foundation over time
- Poor metrics fail to detect problem
- Gradual deterioration on many fronts leads to Chronic business crisis and ultimate failure

Reactive/Urgent

BUSINESS CRISIS-RISK ***INDICATORS***

'INDICATORS' are clue cues that give you more information about business crisis-risk. They can be *behavioral*, *transaction* or *process* changes that are transmitted by verbal and non-verbal means.

Data Breach Indicators include:

- System runs slower than normal
- 'Emergency' requests which circumvent normal protocol
- Large data transfers from non-routine associates
- Multiple 'portals' for suppliers, customers
- Non-segregated point of purchase programs
- Social Media disclosures of leaked information

Do you see the potential Business Crisis-Risk?

Sensitive Information

Well Known Types of 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

Sensitive Information

Southeast Franchise Forum

Commercial Information

- Bank account and transit routing data
- Credit/Debit Cards
- Financial banking\trading account data
- ACH 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 University
- 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.)

Network Security

- Does the insured store Personally Identifiable Information (PII), Personal Health Information (PHI), or Confidential Corporate Information on their network?
- Could a Rouge Employee cause a breach?
- Is the insured subject to any Regulatory Standards? HIPAA, HiTech, GLB, PCI?
- Does this insured use a third party hosting site to store data?
- Could the insured pass on a virus to a third party?

Privacy Liability

- Does the Insured store sensitive information in paper files?
- Does the insured store paper files off-site?
- Are laptops and pda's used, and do they store sensitive information?
- Does the insured have a Privacy Statement?

Content/Media Liability

- Does the insured create any digital content through their website or other electronic means?
- Does the insured create any non-digital content?
- Does the insured store any 3rd Party Intellectual Property on their website?
- Could the insured be brought in to any Domain Name disputes?

Why Prepare for a Breach? SPEED!!!

Target Announces Breach- 40 Million Cards

Day 3- Federal Trade Commission announces probe

Day 4 – Three Class Action Suits

Four State AG's Lunch Investigations

Day 5- 15 Class Action Suits

Day 8- 30 Class Action Suits

Within First 90 Days, Company Testifies to Senate, CEO, CIO ultimately terminated

Spear Phishing vs Phishing

Phishing is a very common form of hacker attack. Hackers send millions of emails out that appear to be from a trust source that is asking for you to download something or reset your credentials(ID and Password). This allows them to install malicious code on your network. Then they search for your bank account info and attempt to extract money. $40mm loss per year for U.S. banks.

Spear phishing seeks to deploy the above technique to specific organizations and/or persons where they know there is a high likelihood of a huge payoff. Basically they get access to your email and impersonate you. They then send email to a third party that trusts you. They solicit that persons credentials to gain access to data or a bank account.

Every Email you Send Receive and Store is at Risk

- Email is often over looked but is a very significant exposure of both personal and corporate information. Most people have sent and received enormous amount of email.
- Almost every company requires a confidentiality statement at the footer of every sent email. This implies that the recipient maintain the confidentiality of this content.
- Hackers are now using sophisticated tools to capture your email as you send it. Then they use your email to impersonate you or others in spear phishing attacks.
- When they get an email from a known source, they do not expect to be accidentally downloading malicious code.
- A breach of your email exposes everyone you communicate with to spear phishing attacks

1ST PARTY COVERAGE

- Business Interruption
- Data Restoration
- Notification Costs
- Credit Monitoring
- Crisis Management/Public Relations Expense
- Forensics Costs
- Cyber Extortion
- Cyber Crime/Phishing
- Reputational Damage

Buyer Beware Clauses
(These could come back to bite you!)

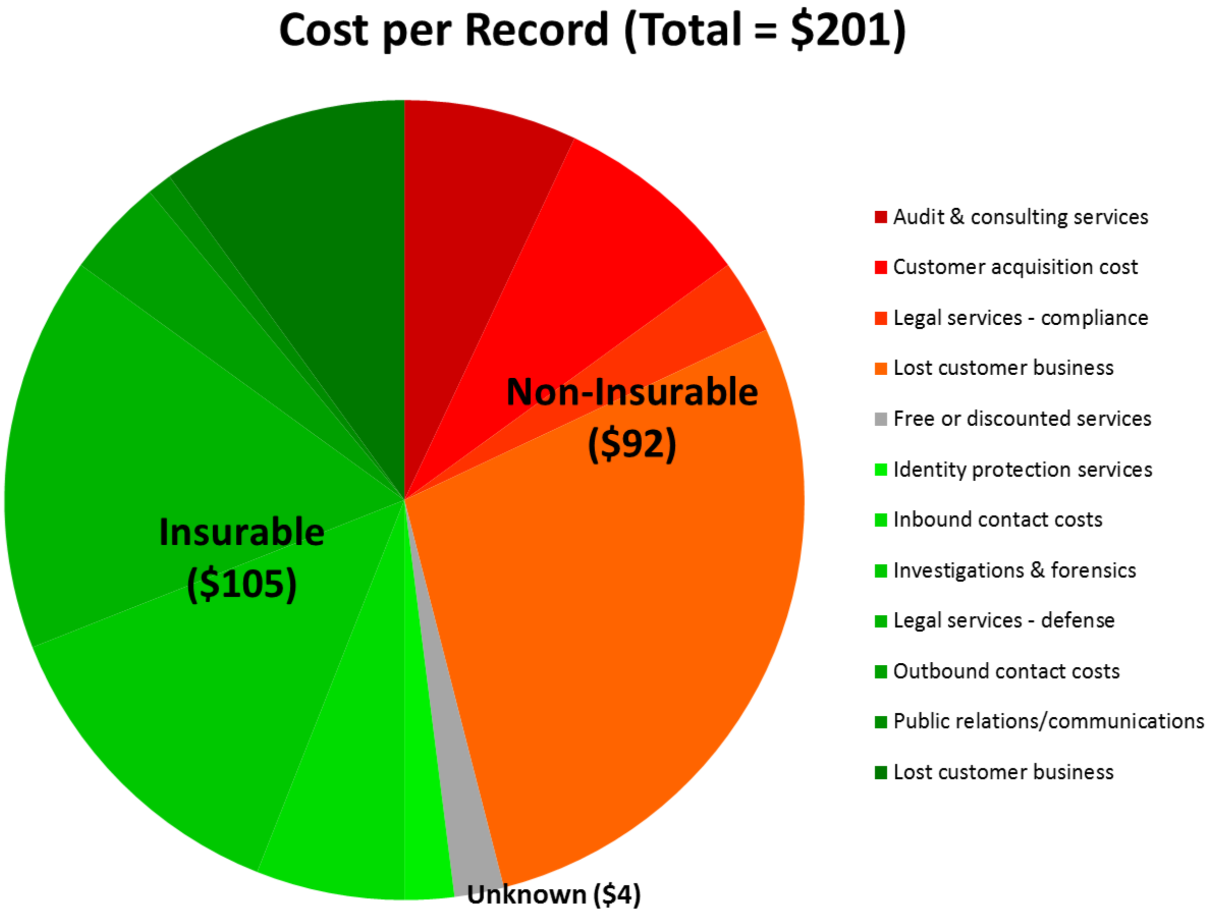
- Unencrypted data Exclusion for laptops and portable devices
- Rogue employee – intentional act exclusion
- No coverage for corporate information protected by N.D.A’s or Confidentiality agreements
- Requirement to “maintain security level” wording.
- Definition of covered network is limited to data within your “care, custody and control”.
- Fraud Exclusion with no add-back for innocent insured for Security Breach or Privacy event

Who Buys Insurance?

Revenue Range (£)	% Purchasing Cyber
<1.5M	3.8%
1.5M<3M	4.8%
3M<6M	6.6%
6M<15M	7.2%
15M<60M	10.0%
60M<180M	17.6%
180M<600M	20.5%
600M<3B	21.8%
3B+	25.9%

Breach Notification Costs
the Real Numbers

- What would your company do if breached?



Data derived from *Ponemon 2014 Cost of Data Breach Study: United States*

Cost Variation –
Dependent on Vendor Selection

- Breach of approx 50,000 records, including social security numbers
- Two years of credit monitoring services provided to victims

	Insured's Vendor Cost	Carrier Vendor Cost	Savings
Legal Assistance with Notification Letters	$24,190	$10,000	$14,190
Print/Mail Letters	$63,551	$56,341	$7,209
Call Center Services	$118,642	$66,852	$51,790
Credit Monitoring Services *	$34,199.80 - $683,996	$15,864.85 - $317,297	$18,334.95 - $336,698
Totals	$240,583 - $890,379	$149,058 - $450,490	$91,524 - $409,887

What is foreseeable?

Today

Everything is foreseeable

Tomorrow

Anyone may be Held accountable

Business Intelligence

- Is a set of theories, methodologies, architectures, and technologies that *transform raw data into meaningful and useful information* for business analysis purposes.
- Allows for the *easy interpretation* of volumes of data.
- Identifies *new opportunities*
- Implements an effective strategy to provide a competitive market advantage and *long-term stability*.
- Provides historical, current and *predictive views* of business operations.

BUILDING AN INTELLIGENCE NETWORK

Southeast Franchise Forum

Define **Framework**

- What are your requirements to manage Social Media ***Risk***?
- What are the objectives of your Social Media use?
- What are the performance drivers and what is their relative importance?
- Managing overlaps and gaps?
- How will we add new tools? Who will lead discovery?
- What role should each team member play?

Identify **the Risks involved**

- What are the specific risks to each stakeholder group?
- What risks are inherent to Social Media?
- What risks are associated with each application or tool?
- What is the likelihood of each risk occurring?
- What potential impact do these risks pose?
- What tools will you use to track, predict and manage?

Manage **and** ***Mitigate*** **Risks**

- Can your Social Media approach be designed to reduce or eliminate risks?
- What are strategies that have a lower risk profile?
- What mitigation strategies are possible for each risk?
- What are the risk tradeoffs involved?
- What strategies exist to minimize disruption risk?
- What techniques and approaches are thought leaders using?

Do you want to know what will happen tomorrow?

Can you identify your organization's next

CRISIS?