Best Practices for Business Continuity: Client RFP's, Client Audits and Vendor Risk Management

Responding to Client/Customer Requests, and Other Considerations

Kathy Scourby, CBCP

K·N·S Consulting

ACP – ODU Chapter Meeting – September 28, 2021

Introduction

Kathy Scourby, CBCP

K·N·S Consulting

- **Kathryn Scourby, CBCP is the Principal of KNS Consulting, LLC.** Kathy works with professional service firms to achieve their goals in the areas of business continuity, disaster preparedness, risk management and compliance.
- **A Certified Business Continuity Professional (CBCP),** she consults with and trains management professionals and all levels of staff at private service firms by facilitating table-top exercises and other training in these focus areas, as well as conducting Business Impact Assessments (BIA's) and overall business continuity planning.
- **Kathy's experience includes thirty-three years with international law firm Hunton Andrews Kurth, LLP**, including over five years as the firm's only Business Continuity Manager, as part of her experience in the legal industry.
- **She continues to receive outstanding reviews as a frequent presenter at legal management conferences** and local chapter meetings of the Association of Legal Administrators (ALA), state and local Bar Association meetings, other professional association meetings and with private service firms and businesses.

Agenda

- Defining disaster/crisis the need for a Business Continuity Program in a Pandemic world
- Responding to RFP's and Due Diligence Questionnaires
- Client Audit Requests and the Importance of Standards
- Vendor Risk Management Program
- Principles for a successful Vendor Risk Management Program
- Best practices and information for a thorough Business Continuity plan
- Q&A session

Defining Disaster / Crisis

"Any situation that threatens the integrity or **reputation** of a firm or business, usually brought on by adverse or negative media attention."

MAJOR DISASTERS 2018-2021

Hurricane Ida
Louisiana & Mississippi
08/2021

Mass Shootings
Atlanta, Boulder & CA
3/2021

Civil Unrest/Capitol Attack
National
5/2020 – 2021

Coronavirus Pandemic
International
2/2020 – To Date

Hurricanes Laura, Marco and Delta
Gulf Coast
8/2020 – 10/2020

Hurricanes Laura, Marco and Delta
Gulf Coast
8/2020 – 10/2020

Wildfires and PG&E Power Outages
California
10/2019 and 9/2020

Christmas Bombing
Nashville, TN
12/25/2020

Mass Shooting
El Paso, TX
8/2019

Hurricane Barry
Louisiana
7/2019

Earthquakes
California
7/4 & 5/2019

Jersey City Mass Shooting
Jersey City, NJ
12/2019

Parkland School Shooting
Parkland, FL
2/14/2018

CYBER-SECURITY BREACHES

T-Mobile
Cyber Breach
8/2021

Microsoft
Exchange/Hafnium
Cyber Breach
3/2021

Universal Health System
unknown accts exposed
9/2020

Marriott (Starwood)
5.2 million
accts exposed
2/2020

Citrix
400k companies & organizations info
accts exposed
3/2019

Walmart
unknown
accts exposed by contractor
2/2019 – 2015

Capital One
100 million
accts exposed
7/2019

Marriott (Starwood)
500 million
accts exposed
11/2018

Facebook/LinkedIn
Up to 214 million
accts exposed
10/2018 and 1/2021

The Need for a Comprehensive

Business Continuity Plan for Any Disaster

Compliance issues
(Client audits and RFP's)

Regulatory Requirements
(government or ISO certification)

New hardware or operating systems and applications that are now in the Cloud

Cyber or Business Interruption insurers

Facility and/or personnel changes/moves/ relocation

Changes in voice/data networks

Third Party suppliers – vendor risk management program

Pandemic Planning

Responding to RFP's & Due Diligence Questionnaires

Companies are increasingly asking potential clients to complete Request for Proposals (RFP's) and Due Diligence Questionnaires **PRIOR** to hiring a client to take on the work or representation :

- **Definition of Due Diligence:**
  "an investigation or audit of a potential investment or product to confirm all facts, such as reviewing all financial records, plus anything else deemed material. It refers to the care a reasonable person should take before entering into an agreement or a financial transaction with another party."

- **RFP and Due Diligence process reduces risk** that a company can incur with hiring a potential client.

- **Companies can gather information** about financial information, security, personnel, pending legal matters and regulatory compliance that can be used to evaluate and compare potential clients.

- **Many companies will now require RFP's or DDQ's** be issued to anyone who may be bidding for work.

Client Audit Requests

Companies are increasingly auditing their clients to ensure their business continuity programs are effective and security protocols are in place:

- **Any large companies (e.g., financial institutions) that are audited themselves**, will audit their own clients/customers who work with them or represent them.
- **What an audit can look like:**
  - Review of written business continuity plan documents
  - Review of cyber security and business interruption insurance documents
  - Review of actual testing and drills that have been scheduled and completed.
  - Review of testing timetable
  - Review of Business Impact Analysis if completed
  - Interviews with Business Continuity Manager, CIO and other managers responsible for disaster preparedness and business continuity
  - Assessment by auditor and review of findings with timetable to fix and mitigate any findings or gaps.

Client Audit Requests

2017 Survey from LogicForce in which 200 law firms were surveyed showed:

- 18 firms said they lost a client for failing an IT audit
- 1 firm lost an entire practice group
- 95% of law firms were not compliant with their own cybersecurity polices
- 77% of law firms did not maintain cyber insurance coverage
- 134 firms reported a cyber breach and 40% of firms suffered a breach that they were not aware of until much later

Client Audit Requests & the Importance of Standards

Importance of ISO (International Organization for Standardization)

ISO 27001 – global management system standard that provides specification for establishing, implementing, maintaining and continually improving an information security management system. Ensures protection, confidentiality, integrity and availability of data.

ISO 27032 –an overview of Cybersecurity and an explanation of the relationship between Cybersecurity and other types of security within a firm. The standard provides a definition of stakeholders and a description of their roles in Cybersecurity and guidance for addressing common Cybersecurity issues. The overall framework of this standard ensures a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

Client Audit Requests & the Importance of Standards

Importance of ISO (International Organization for Standardization)

ISO 22301 – This standard provides a framework to plan, establish, implement, operate, monitor, review, maintain and continually improve a business continuity management system (BCMS). It is expected to help organizations protect against, prepare for, respond to, and recover when disruptive incidents arise.

Certification to ISO Standards can eliminate the need to continually undergo IT audits in a company because the ISO certification auditor has already completed an audit and is certifying compliance.

Client Audit Requests & the Importance of Standards

Importance and benefits of ISO (International Organization for Standardization)

Certification to ISO Standards can:

- **Eliminate** the need to continually undergo IT audits in a company because the ISO certification auditor has already completed an audit
- **Ensure** that businesses are compliant with data security laws and taking steps to protect all data and information entrusted to them by clients

- **Benefits** include:
  - ✓ Adopting international best practices
  - ✓ Avoid penalties and losses due to data breaches
  - ✓ Improve corporate reputation and possible competitive advantage
  - ✓ Build awareness of the need for strict information security

Some clients are requiring ISO certification prior to hiring a company to work with them

Vendor/Business Partner Risk Management Program

Considerations for a Vendor/Business Partner Risk Management Program

- **How well are your cloud-based applications protected** by your vendor and their partners/vendors?
- **How would your company be impacted if your vendor's IT systems** are down for a period of time?
- **Could your vendor's behavior or lack of security** affect your company's reputation?
- **Does your vendor have access** to your firm's intellectual property or clients' data?

Vendor/Business Partner Risk Management Program

Four Principles of a Vendor Risk Management Program

1. **Identify potential vendor risk**
2. **Develop effective strategies** for higher risk vendors
3. **Align vendor environments** with business internal framework
4. **Implement ongoing oversight of vendor program** with metrics and external alerts

Vendor/Business Partner Risk Management Program

1. Identify Potential Vendor Risks

- ✓ **Determine how deeply you need to investigate your vendor** (categorize and prioritize vendors) (payroll/payments vendor vs. a small vendor providing office supplies)
- ✓ **Assess vendor prior to relationship beginning or at time of contract renewal** so there is time to engage with the vendor to understand their business
- ✓ **Are there regulatory requirements or strategic decisions** to make as to the level and need to scrutinize the vendor?

Vendor/Business Partner Risk Management Program

2. Develop Effective Strategies for working with High-risk vendors

- ✓ **Know which areas of your firm's business you need to protect** and focus on mitigating any risks. (Risk Mitigation should be part of the SLA)
- ✓ **Work closely with vendor to identify and resolve issues** early on to lessen any risks
- ✓ **Assess vendor prior to contract renewal** or more frequently
- ✓ **Gather external information about the vendor** (assess their financial health)
- ✓ **Use metrics to benchmark performance of the vendor** over time (is their performance improving?)
- ✓ **Have a plan if vendor's risk exceeds your risk tolerance level** or goes out of business

Vendor/Business Partner Risk Management Program

3. Align vendor environments with your firm's internal framework:

- ✓ **Review internal controls for your firm** (control areas and standards such as ISO, NIST, etc.) and overlay these controls on vendor's program
- ✓ **Perform a gap analysis** of vendor's internal controls
- ✓ **Stipulate need for vendor audits** if necessary, to determine how they are performing and what they need to fix or change

Vendor/Business Partner Risk Management Program

4. **Implement ongoing oversight utilizing metrics and external alerts:**

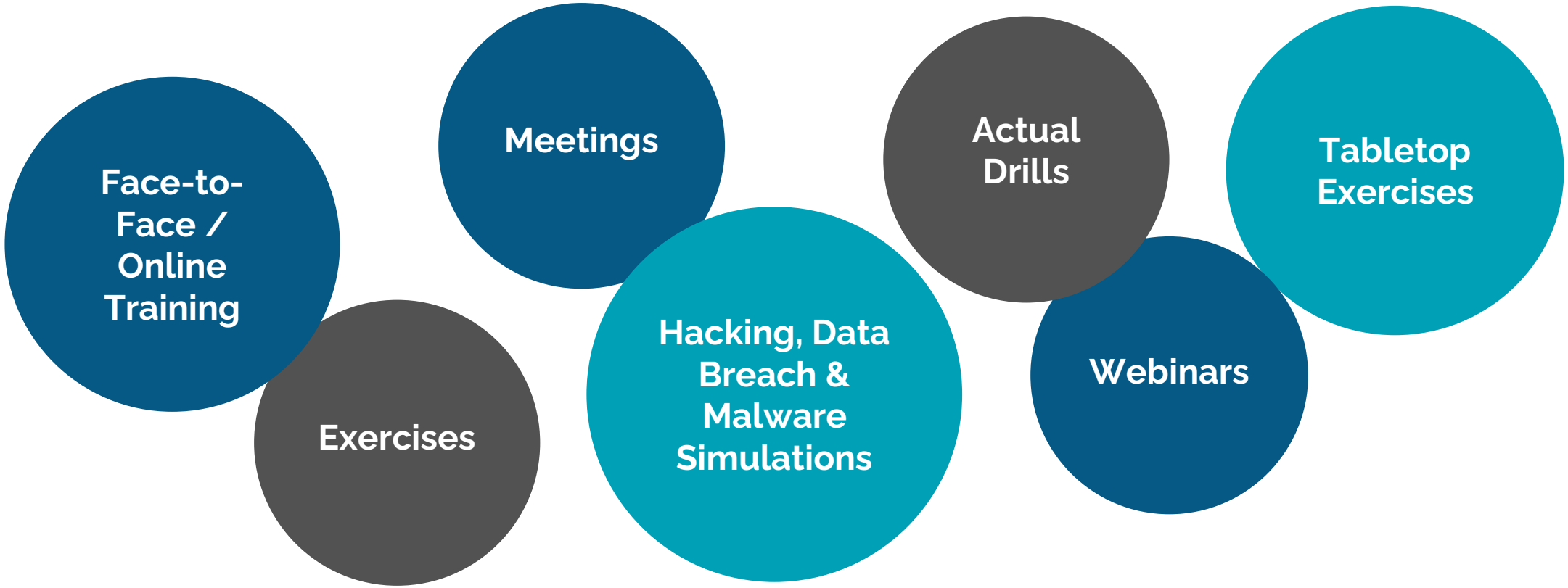
- ✓ **Use metrics to measure performance of vendor** (for example: using a staffing service that has a high turnover in workers being sent to work for you)

- ✓ **Using external alerts can help firm understand if a vendor has an issue** that may impact your firm's business or reputation (for example: if vendor is being acquired by another company or a lawsuit has been filed)

- ✓ **Measurements can include:**
  - Performance or Service Level Agreements (SLA's)
  - Disruption based on vendor performance or non-compliance with rules, regulations or policies
  - Vendors issuing warning for business disruption
  - Breach of vendor network, systems or facilities

Training – Crisis Teams and All Employees

Consistent training for all employees and crisis team members is essential.



Thanks for Joining Us!

www.knsbusinessconsulting.com

(865) 789-7694

Contact Kathy at

kscourby@knsbusinessconsulting.com