PORZIO
BROMBERG&NEWMAN P.C.

PORZIO
COMPLIANCE SERVICES

Incident Response Process: Streamlined

James G. Mottola, MS, CPP, CISM
Vice President of Data Privacy, Investigations and Security
Porzio Compliance Services

Deirdre R. Wheatley-Liss, Esq.
Principal
Porzio, Bromberg & Newman, P.C.

Identification and Evaluation Phase

- **Investigate** early warning indicators that a process is not functioning as usual, unless signs are obvious.
- **Communicate** with key stakeholder to gather additional information in order to verify findings.
- **Determine** operating status within the business units and criticality.
- **Loop** in board, senior management and general counsel.

"The art of communication is the language of leadership"

James Humes

Triage and Immediate Incident Response Phase

- **Refer** to Incident Response Plan or begin to formulate an initial plan with internal team as a priority.
- **Stop** information technology processes to safeguard critical data.
- **Contact** outside legal counsel to manage the response and create umbrella of confidentiality with response service providers.
- **Contact** insurance provider for coverage services, if applicable.

Triage and Immediate Incident Response Phase

- **Coordinate** internal or external information technology and security provider through legal counsel for immediate priority response and first steps.
- **Implement** immediate Communication Plan with stakeholders - Board of Directors, senior management, customers, vendors, employees, lenders.
- **Review** contracts for notification requirement and damage mitigation provisions.
- **Investigate** breach point of entry and impact.
- **Determine** various points within the business process each unit is currently operating.

Incident Response and Business Continuity Phase

- **Assign** internal technical team to work with external consultants to prioritize containment, investigation, and remediation.
- **Assign** internal business team with external business units, if available, to determine back-up process to meet client needs.
- **Refer** back to Incident Response Plan and Business Continuity Plan for available business process resources.
- **Set** daily briefing to incident response leader and board members.
- **Formulate** breach notification messaging to employees, clients, media, and law enforcement with counsel.

Business Continuity and Recovery Phase

- **Verify** with internal team technical and external consultants to validate effective containment, investigation, and remediation.

- **Determine** with internal business team current status of process to meet client needs and prepare for restoration of IT systems.

- **Document** measures taken to refer back to Incident Response Plan and Business Continuity Plan for process review.

Business Continuity and Recovery Phase

- **Continue** to message employees, clients, media, and law enforcement with counsel for legal compliance.
- **Investigate** anomalies with appropriate personnel.
- **Communicate** with key stakeholder to gather additional information.
- **Determine** various points within the business process each unit is currently operating.

Recovery Phase and Resilience Planning

- **Validate** with external consultants on effective containment and remediation, through a vulnerability assessment and testing.
- **Determine** with internal business team current status of back-up processes to meet client needs.
- **Review** measures and practice improving incident response and business continuity plans.
- **Continue** to communicate with employees, clients, media, and law enforcement with counsel for ongoing security awareness, policy development, and legal compliance for maturation of enterprise.

Questions?

Porzio Compliance Services

James G. Mottola, MS, CPP, CISM

jmottola@porziocs.com

973.889.4277

Porzio, Bromberg & Newman

Deirdre R. Wheatley-Liss, Esq.

drwheatleyliss@pbnlaw.com

973.889.4278

Porzio, Bromberg & Newman

William J. Hughes, Esq.

wjhughes@pbnlaw.com

973.889.4308

Porzio, Bromberg & Newman

Robert M. Schechter, Esq.

rmschecter@pblaw.com

609.524.1838.