COMPASS
IT Compliance

Business Resilience

ADAM CRAVEDI, CISSP, CISA
DIRECTOR BUSINESS OPERATIONS

Secure. Comply. Save.

Agenda

COMPASS IT Compliance

- What is Business Resilience?
- Key Components of Business Resilience
- Methods to Achieve Business Resilience
- Q&A

Business Resilience

COMPASS IT Compliance

- Business resilience is defined as the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.
- This is essentially the culmination of having a solid BCP and IT Security Program.
- Both must include your critical business processes AND third-party providers.

Cyber Resilience

COMPASS IT Compliance

- Cyber resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events.
- The term cyber resilience is an evolving perspective that is gaining recognition.
- It essentially brings the areas of information security and business continuity together and yields organizational or business resilience.

Key Components of Business Resilience

COMPASS IT Compliance

- Enterprise Risk Management
- Incident/Crisis Response
- Business Continuity/Disaster Recovery

Key Components of Business Resilience

COMPASS IT Compliance

- Enterprise Risk Management
  - Identify, assess, and prioritizes different risk that could affect the business.
  - Develop plans to minimize or eliminate the impact of negative events associated with those risks.
  - Types of risks include: operational, financial, organizational, strategic, technology and legal.
  - The Goal is to anticipate the business processes with the largest impact to the organization and minimize the impact.

Key Components of Business Resilience

COMPASS IT Compliance

- Enterprise Risk Management
  - Related objectives include:
    - Annual Risk Assessment Program
    - Strategic Plans (corporate + technology)
    - Strong Information Security Program
    - Vendor Management

Key Components of Business Resilience

COMPASS IT Compliance

- Incident/Crisis Response
  - Identify, analyze, and correct events to prevent a future reoccurrence.
  - An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions.
  - Incident Response is the process of limiting the potential disruption caused by such an event, followed by a return to business as usual.
  - Crisis management is a large scale, incident response. It is the process by which an organization deals with major events that threaten to harm an organization, its stakeholders, or the general public.

Key Components of Business Resilience

COMPASS IT Compliance

- Incident/Crisis Response
  - Related objectives include:
    - Incident Response Plan
    - Incident Response Team
    - Emergency preparedness planning
    - Incident Response Plan testing
    - Incident Response Team training

Key Components of Business Resilience

COMPASS IT Compliance

- Business Continuity/Disaster Recovery
  - Broad, enterprise-wide approach to the recovery of the entire business process
  - Disaster Recovery was historically the IT recovery only
  - BCP includes people, process, and technology
  - The goal is to be able to continue business operations after an interruption of services minimizing downtime

Key Components of Business Resilience

COMPASS IT Compliance

- Business Continuity/Disaster Recovery
  - Related objectives include:
    - Business Impact Analysis
      - Identify critical business processes
      - Identify critical systems and hardware
      - Identify critical business dependencies
    - Risk assessments
    - Plan to operate during an event
    - Recovery procedures

Key Components of Business Resilience

COMPASS IT Compliance

- Business Continuity/Disaster Recovery
  - Related objectives include:
    - Testing is an important part of Business Continuity
    - Test your BCP, make adjustments, retest your plan
    - Business Continuity is an ongoing process, not a "one and done" activity
    - Prepare for the worst and hope for the best
    - This is not only a recommendation, but a requirement in most industries/verticals

Methods to Achieve Business Resilience

COMPASS IT Compliance

- Risk Management Strategy
  - Develop a business risk assessment testing and review program
    - Identify threats and impacts across the organization
    - Rank risks based on criticality and impact to business
  - Review and update
  - This is an organizational wide exercise not just for IT
    - Executive management and Board level support is vital
    - Includes strategic planning

Methods to Achieve Business Resilience

COMPASS IT Compliance

- Business Continuity Program (BCP) and Testing
  - Develop a comprehensive BCP
    - Start with a Business Impact Analysis
  - Test, Train & Maintain
  - Again, not only is this a recommendation, but a requirement in most industries/verticals

Methods to Achieve Business Resilience

COMPASS IT Compliance

- Incident Response Planning Program and Testing
  - Focused on perceived and actual information security incidents (Malware, Virus, Ransomware, etc.)
  - Incident Response is very different from Business Continuity
  - Test, Train & Maintain
  - As with BCP, this is not only a recommendation, but a requirement in most industries/verticals

Methods to Achieve Business Resilience

COMPASS IT Compliance

- Digital Forensics Retainer
  - Suspected Loss of Sensitive Data
  - Suspected Breach
  - Suspected Insider Threat
- Proactive vs. Reactive
- Determine Root Cause of Incident

Case Study

COMPASS IT Compliance

- https://coca-colahellenic.com/en/about-us/business-resilience-and-risk-management/business-resilience/

Summary

COMPASS IT Compliance

- Organizations must have resiliency and incident response built into the security framework – these are not nice to have – they are a must have.
- Build, train and maintain a viable:
  - Organizational Risk Management Program
  - Business Continuity Program
  - Incident Response Plan
  - IT Security Program
  - Vendor Management

Resources

COMPASS IT Compliance

- https://www.compassitc.com/blog
- https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx
- https://www.xmatters.com/business-continuity/four-things-you-need-to-know-about-business-resiliency/
- https://fmlink.com/articles/five-things-need-know-business-resilience-planning/

COMPASS
IT Compliance

Questions?

Secure. Comply. Save.

Contact Information

COMPASS IT Compliance

Adam Cravedi, CISSP, CISA

Director Business Operations

acravedi@compassitc.com

Secure. Comply. Save.