RESHAPE THE EXPERIENCE

Cybersecurity – A Risk Based Approach

About Expedient Technology Solutions

MISSION : RESHAPE THE EXPERIENCE

- Founded in 2004, 38 Team Members
- Managed Service Provider
- Cybersecurity and Compliance Services
- Cloud Hosting and Managed Backup

EXPEDIENT TECHNOLOGY SOLUTIONS, LLC

Strategic vs. Tactical Approach

Strategy defines your long-term goals and how you are planning on achieving them. Strategy gives you the path you need to achieve your mission.

Tactics are generally smaller steps and a shorter-term actions taken. They involve best practices, specific plans, resources, etc.

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

Tactical Cybersecurity

- Tactical approach does not look at the entire scope of a mature cybersecurity program, only threats and vulnerabilities.
- Tactical approach does not prioritize defense or recovery based upon criticality of asset or system.
- Tactical approach does not consider laws, regulations, or contractual obligations the organization is required to comply with for cybersecurity or privacy.

Tactical Cybersecurity Examples

- ***CIS Controls*** (https://cisecurity.org) – Prioritized set of actions to protect your organization and data from known cyber-attack vectors.
- ***NIST Cybersecurity Framework*** (https://www.nist.gov/cyberframework) - Voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.
- ***Cybersecurity & Infrastructure Security Agency (CISA) Ransomware Guide*** - Best practices and ways to prevent, protect and/or respond to a ransomware attack.

Case Study #1 - Ransomware

Business: Manufacturer

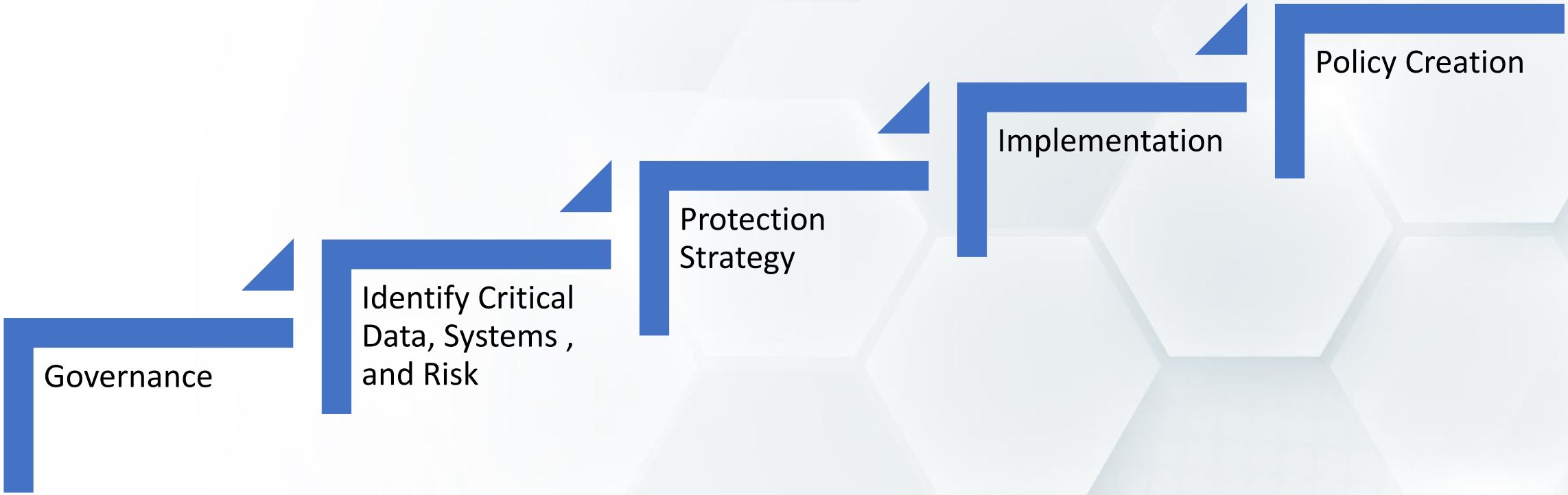
Incident: Network-wide Ransomware Infection

Affect on Business:

- Discovered offsite backups were not functional for 6+ months.
- Software needed to rebuild applications were stored electronically.
- Forced to pay ransom of $75k due to insufficient restore capability.
- Additional costs for investigations, recovery, etc.
- Multiple weeks of business interruption.

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

Cybersecurity – A Risk Based Approach



GOVERNANCE

Objective: Establish a governance strategy.

Target Audience: The executive team.

Actions:

- Identify External Program Influences
  - Statutory Cybersecurity and Privacy Requirements (Laws)
  - Regulatory Cybersecurity and Privacy Requirements
  - Contractual Cybersecurity and Privacy Requirements
  - Industry Recognized Practices

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

GOVERNANCE

Actions (cont.):

- Identify Internal Program Influences
  - Aligning IT to business strategy
  - Goals and objectives (e.g. customer satisfaction, SLA's, quality metrics, competitive advantage)
  - Budget constraints
  - Corporate policies
- Identify Risk Tolerance

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

IDENTIFY CRITICAL DATA, SYSTEMS, AND RISK

Objective: Identify critical data / systems and establish a risk-based protection strategy.

Target Audience: Data / system owners and IT / cyber lead.

Actions:

- Identify Assets
  - Data
  - Personnel
  - Physical Devices
  - Software / Applications
  - External Information Systems
  - Facilities / Locations

EXPEDIENT TECHNOLOGY SOLUTIONS, LLC

IDENTIFY CRITICAL DATA, SYSTEMS, AND RISK

Actions (cont.):

- Identify Business Environment
  - Role in the supply chain.
  - Suppliers and third parties related to IT
- Development of a Risk Assessment
- Development of a Business Impact Analysis
- Gap Analysis of any Identified External Influences

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

Case Study #2 - Ransomware

Business: Multi-Location Services Business

Incident: Network-wide Ransomware Infection

Affect on Business:

- Rebuild of entire server infrastructure, rebuild of all workstations.
- Lost all ERP history and rebuilt the current month from paperwork.
- At least $150k in hard costs.
- Did not pay ransom.

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

Risk Assessment Concepts

Process of analyzing potential threats and vulnerabilities to your assets to establish what loss you might expect to incur if certain events happen.

Risk = Threat * Vulnerability

EXPEDIENT TECHNOLOGY SOLUTIONS, LLC

Risk Assessment Concepts

Quantitative Risk Assessment

Measures risk using monetary amounts, providing the value of expected losses of a specific risk.

- Asset Value
- Frequency of Risk Occurrence
- Probability of Associated Loss

Single Loss Expectancy x Annualized Rate of Occurrence = Annual Loss Expectancy

Risk Assessment Concepts

Qualitative Risk Assessment

Measures risk using opinion-based judgement to determine risk based upon probability and impact. Rating Scale:

- Low – unlikely to occur or impact
- Medium – possible to occur and impact
- High – Likely to occur and impact significantly.

Probability	Harm Severity		
	Minor	Major	Critical
High	High	High	Very High
Medium	Medium	High	Very High
Low	Low	Medium	High

Business Impact Assessment Concepts

- Maximum Tolerable Period of Disruption
- Recovery Time Objective
- Recovery Point Objective
- Dependencies Related to Critical Systems and Functions
- Scenarios Most Likely to Impact Critical Systems and Functions
- Potential Loss from these Scenarios

Business Impact Assessment Concepts

Payroll Example

Dependencies – Internet connectivity, Timekeeping and Accounting Systems, Payroll Provider SaaS Platform

MTPD – 2 Weeks

RTO – 72 Hours

RPO – 24 Hours

Likely Impact Scenarios – Loss of Internet connectivity, payroll provider SaaS platform downtime, timekeeping and accounting systems downtime.

Potential Loss – No attributable financial loss expected. Downstream issues expected if payroll window is missed, and employees are not paid timely.

PROTECTION STRATEGY

- Objective: Develop a strategy to protect assets based upon their classification, priority, and risk.

Target Audience: IT / cyber lead and key team members.

Actions:

- Risk Responses
  - Risk Mitigation
  - Risk Assignment or Transference
  - Risk Acceptance
  - Risk Deterrence
  - Risk Avoidance
- Expense of Responses Justified by the Risks and Impact Shown in the RA / BIA.

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

IMPLEMENTATION

Objective: Deploy the controls, solutions, etc. identified to address risks and priorities.

Target Audience: Assigned IT resources.

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

POLICY CREATION

Objective: Build out additional policies, plans, etc.

Target Audience: IT / cyber lead and key team members.

Policies, Plans, etc.:

- Vendor Management Program
- Business Continuity Plan
- Disaster Recovery Plan
- Incident Response Plan
- Written Information Security Policy (WISP)
- Standards and Procedures
- Monitoring Objectives and Metrics

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC

QUESTIONS?

THANK YOU!

EXPEDIENT
TECHNOLOGY SOLUTIONS, LLC