TIP SHEET:

HOW TO RUN AN EFFECTIVE CYBERSECURITY PROGRAM

> *"How a security program is planned, executed, and governed is likely as important as how much money is devoted to cybersecurity."*
> – DELOITTE INSIGHTS, 2020

Whether you have an emerging cybersecurity program or a mature operation, there is always room to be more effective and efficient. Follow these steps to help optimize your organization's security plan.

1 KNOW WHAT YOU'RE TRYING TO PROTECT

Inventory Your Data & Assets

Data is hazardous material! Start with a comprehensive inventory, including:

- What sensitive data your organization stores
- Where the data is stored
- Who has access (include employees and third parties)

To simplify, it can be helpful to classify data into categories based on regulatory requirements and security risks.

2 UNDERSTAND YOUR OBLIGATIONS

Create a Statement of Applicable Laws, Regulations, and Obligations

A qualified cyber attorney should evaluate your organization's regulatory and contractual obligations with respect to cybersecurity and produce a written statement, which should be reviewed and updated annually. This assessment should include:

- Industry
- Geographic areas of service
- Type and volume of information stored
- Key existing contracts
- Insurance coverage
- Other relevant factors recommended by counsel

Know Your Oversight Responsibilities

Your minimum responsibilities are often defined by law, regulatory guidance, or industry standards. Assign a qualified team member to:

- Research and document your organization's responsibilities
- Ensure that the oversight processes are aligned with requirements

3 MONITOR YOUR RISK

Obtain a Risk Assessment Report

Organizations should have a cybersecurity risk assessment report produced by a third party, with a one-page summary suitable for an annual presentation to your leadership team.

- Be sure the assessment is aligned with all applicable laws, regulations, standards, and contractual obligations
- Consider using a common risk assessment framework such as the NIST 800-30 standard
- Leadership teams can use this report to accept and prioritize risk reduction activities to help create a risk management plan

Perform a Cybersecurity Controls Assessment

A controls assessment typically evaluates your organization's cybersecurity program, compares it to your cybersecurity goals, and helps define a prioritized plan to increase your cyber maturity over time.

- The assessment should be based on a widely accepted framework, such as the NIST Cybersecurity Framework
- Be sure to align with all applicable laws, regulations, standards, and contractual obligations
- Get a third-party assessment with a one-page summary suitable for an annual presentation to the Board

Conduct Technical Testing

Select annual security assessments based on your organization's needs. These should include:

- Penetration testing and vulnerability scanning of organization-maintained resources
- Configuration reviews for any cloud assets containing high-risk data
- Appropriate testing of other key applications, devices and IT resources

Track and Analyze Cybersecurity Incidents

Keep track of cybersecurity incidents, analyze root causes, and provide reports and metrics to your leadership team. This enables your organization to learn from incidents and identify effective measures for reducing the risk of future issues.

4 MANAGE YOUR RISK

Assign Roles and Responsibilities

Ultimately, your people design, build, and implement your cybersecurity program. Ensure that you have an experienced cybersecurity professional leading your program, and budget for appropriate staffing at all levels. Outsource as needed to ensure that you have qualified and trained personnel responsible for each component.

Build Your Cybersecurity Program

Every organization should have a formal, written cybersecurity program which is designed to comply with relevant laws, regulations, and other obligations. The program should be reviewed and updated at least annually.

Choose and use a Cybersecurity Controls Framework

Use a reputable cybersecurity controls framework such as the NIST Cybersecurity Framework or ISO 27001 as the foundation for your cybersecurity program and customize it as needed.

Develop Your Risk Management Plan

Create, implement, and maintain a plan for prioritizing and addressing cybersecurity risks. Update this plan as often as practical, and proactively include supplier risks.

Engage in Training and Promote Awareness

Routinely communicate cybersecurity policies, procedures, and threat updates to all stakeholders, including IT staff, security team members, legal counsel, general employees, and the leadership team. Provide regular training via on-demand training platforms, live webinars, and/or awareness campaigns.

Fund your Cybersecurity Program

No cybersecurity program can address every risk. Prioritize investments in cybersecurity to address the most concerning risks. This may include allocating budget for human resources, equipment, services, and more.

Get Cyber Insurance

Select cyber insurance coverage based on the anticipated residual risks to ensure that appropriate risks are transferred. Coverage should be aligned with your leadership team's risk appetite. Incorporate any required technologies or practices into your cybersecurity and incident response programs.

LMG SECURITY

145 W FRONT STREET
MISSOULA, MONTANA 59802
www.LMGsecurity.com

WE ARE HERE TO HELP

Please contact us any time you have a question or need additional support.
Phone: 406-830-3165 | Toll-Free: 1-855-LMG-8855 | E-mail: info@LMGsecurity.com

REFERRING A CLIENT

To refer a client to LMG Security, please email info@LMGsecurity.com