LP3

# Service Offerings

June 29, 2019

This document includes data that shall not be disclosed outside the recipient organization listed on the cover page and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. The data subject to this restriction are contained on all pages of this technical proposal.

# Table of Contents

## Purpose

This document describes a sampling of the available LP3 services for government and business clients. Additional services are available. Any of these listed services can be tailored to meet the needs of a specific client. This is an overview only and the content of these services may be modified at any time.

## Virtual CISO (V-CISO) Services

Cyber security is a major concern for businesses across all industries. The need for specialized security experts to help plan for the future and manage daily operations has become more important than ever. Recruiting, hiring and maintaining a cyber security team or senior cyber executive can be a time consuming, expensive, and frustrating task

LP3 offers a V-CISO role designed for organizations that need someone to help with roadmap planning, implementation, and maintenance of the information security program but cannot afford, or do not need a full-time CISO. LP3 provides an enterprise-scale subject matter expert on a part time basis at a fraction of the cost.

With this program, all of LP3's security services are immediately available on an as-needed basis. In addition to helping with your information security initiatives, our team is always available to provide security expertise and guidance. Many small and medium sized businesses are adopting this virtual cyber executive model; it is easy to see why this is one of the best ways to assure expert security guidance and executive security leadership for your organization.

- Security Point-of-Contact for all cyber security issues
- Direct phone support during normal business hours
- Attend scheduled executive and board meetings
- Provide bi-annual Security Awareness Training Services
- Review existing Vulnerability Management monitoring reports
- Assist with data classification guidance
- Provide guidance on Data Loss Prevention (DLP) implementation approaches
- Cyber security compliance initiatives (NYS DFS, NIST 800-171, GDPR, SOX, etc.)
- Cyber security program design and roadmap
- Privacy program recommendations
- Vendor Contracts and Risk Management program review
- Identity and Access Management security posture analysis
- Cyber Security Architecture Roadmap
- Cyber Security Policy drafts and reviews
- Bring your own device (BYOD) security strategies
- Answering Security Questionnaires for your customers
- Cyber Security Risk Reviews
- Cyber Security Audit Remediation recommendations
- Cyber Security Incident Response
- Cyber Security Data Breach Management

## Baseline Security Assessments

Business are increasingly dependent on third party Managed Service Providers (MSP) relationships to fulfill critical business infrastructure roles while allowing the business to focus on your core competency. These relationships introduce the requirement for the managed service providers to demonstrate that they maintain a strong security posture and protect sensitive data. Regulatory pressures such as HIPAA, NYSDFS. DFARS, NIST SP 53 & 171, GLBA, NCUA, PCI, as well as IT security policies drive these requirements. If you don't comply, your competition might. Worse yet, if you don't have an effective security posture, your business may be compromised, breached, or disrupted by attackers.

If your organization is constantly fielding requests from your customers regarding data security posture, LP3 can help. We offer solutions to help your business comply with security requirements levied by the DoD, State, or Prime Contractor. LP3 acts as an objective external assessor helping you navigate through various requirements and can provide externally facing reports suitable for distribution to prospects, partners, and customers.

Understanding rules and regulations and then applying them to your business is a costly and time-consuming task. Many compliance regulations and best practices require internal self-assessments to achieve consistent compliance. The difficulty associated with managing this task is a lack of available and experienced cyber resources to carry out and maintain the proper compliance and policy documentation, as well as technical solutions, needed to achieve and maintain a strong security posture.

**LP3 will help by providing:**

- Help client to choose the right security framework for your industry
- Complete Assessment of Citations/Controls of Compliance/Security Framework
- Provide Draft policies and procedures in-line with the security framework
- Deliver Overall Security Plan or System Security Plan (SSP)
- Deliver Executive Summary Report on Compliance
- Deliver Gap Analysis report or Plan of Action and Milestones (POA&M)

## External Vulnerability Assessment and Penetration Testing

The external vulnerability assessment and penetration test is conducted from the Internet. It attempts to exploit critical vulnerabilities that could be exploited by an adversary to remotely compromise client networks. The penetration test consists of identification of specific vulnerabilities followed by common exploitation methodologies to gain access. The concept is to clearly demonstrate critical issues to aid the client in rapid correction of these vulnerabilities that could affect business continuity and company reputation.

Penetration testing is different from vulnerability scanning. A vulnerability scan is used to identify, rank, and report vulnerabilities while a penetration test is used to exploit vulnerabilities or otherwise defeat the security controls and features of a system. Once a penetration tester has compromised an information system, the tester will use that access to move beyond the initial system in order to determine the adequacy of the organization's security processes and controls. This provides a better analysis of the business risk and can be used to make better informed cyber security investment decisions.

**Comprehensive perimeter network penetration scanning includes:**

- Publicly Registered IP address space will be scanned.
- All internet facing web applications and services: these applications will be subject to extensive analysis and probing including multiple false input attempts, input buffer scanning (i.e. heap/stack overflow), site mining, cross-site scripting, SQL injection, and other common attacks.
- Any remote access solution will be evaluated for authentication and authorization issues in addition to known SSL VPN and IPSec VPN vulnerabilities.
- SMTP (email) gateways will be assessed for common configuration mistakes such as 'open relay' and forwarding as well as vulnerability and penetration risks.
- All wireless access points (WAPs) and wireless networks will be assessed for isolation and unauthorized access.

LP3 employs commercial, open source, as well as custom tools and techniques to circumvent network access controls. LP3 professionals rely on proprietary scanning practices and procedures as well as available security tools to assess the security posture of client external networks to a security compromise. All LP3 consultants, engaged in these assessments, receive formal training in network security vulnerability and penetration assessments and possess significant field experience. LP3 professionals will conduct all assessments utilizing “safe and sound” techniques to minimize business disruption. All security assessment activities will be coordinated and planned with the direct involvement with client IT management and staff. All Assessment and Analysis performed by LP3 conforms to industry best practices and standard Cyber Security Frameworks (SANS Institute, the InfoSec Institute, and National Institute of Standards & Technology (NIST)) during this vulnerability and penetration assessment.

## Internal Vulnerability Assessment

The vulnerability assessment is a fully credentialed scan of internal servers, workstations, and network management devices to identify critical issues impacting internal cyber security such as configuration management, patching, and overall cyber resiliency.

that require remediation.

**Scope includes:**

- Comprehensive vulnerability analysis of the internal network space and all network hosts and devices.
- Evaluation of each ‘zone’ or network segment such as a DMZ, VLANs, and VPN environments.
- Vulnerability assessment of discovered hosts and identified applications including intranet websites
- On-premise or cloud hosted internal hosts

**Scanning includes:**

- Discovery scanning of all networks
- Port Scanning of all devices discovered on networks
- Vulnerability Assessment Scanning
- Operating System Patch compliance
- Third-Party application Compliance (Firefox, Chrome, Java, Adobe)

## Security Awareness Assessment, Testing & Training

Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks. Old-school security awareness training doesn’t hack it anymore. Lack of security awareness by your employees can be a huge risk and vulnerability, exposing an organization to compromises. Companies can implement extensive, costly, multi-layered cybersecurity defenses, but with a click of a button, these defensive layers can be circumvented and rendered useless. Knowing the “Security Awareness” level of the organization, identifying weaknesses, and mitigating weaknesses through training is key to managing this risk. Reducing the Phish-prone percentage of your employees through awareness testing and training is likely the most cost-effective network protection measure you can take. Our proven process provides the following services and deliverables:

**Baseline Testing**

We provide baseline testing to assess the Phish-prone percentage of your users through various simulated phishing spear-phishing, and vishing attacks.

**Train Your Users**

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

**Test Your Users**

Best-in-class, fully automated simulated phishing, spear-phishing, and vishing attacks, thousands of templates with unlimited usage, and community phishing templates.

**Analyze Results**

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show security awareness improvement and ROI!

## Configuration Management Assessment

One of the most important aspects of cyber security compliance and resilience is knowing what you need to secure. Many organizations do not know how many IT assets they have and where they are. Some do not know how they are all connected. Gathering this information and including all workstation, server, mobile, and peripheral devices is critical. In addition, cloud and business associate services should be under configuration management as well.

**LP3 can help by:**

- Conduct technical scanning and inventory assessments to validate CM information is accurate
- Draft a Configuration Management Plan to maintain strong CM over time under governance and change control
- Establish technical controls to validate security posture of all devices connecting to the network such as forcing laptops to execute 2-factor authentication and then take patches and update AV signatures before accessing sensitive company information

## Policy and Procedure Development

Policies are the foundation for most cyber security frameworks. They are the first step to achieve cyber resilience documenting the initial cyber requirements for people, process, and technology implementations throughout an organization. Each cyber framework, such as NIST or CIS, requires policies. For example, policies may include mobile device use for company information.

Implementing policies often requires procedures tailored to your individual organization. Procedures are detailed step by step instructions in how to comply with a particular policy. An example procedure is termination of an employee or contractor. The procedure should clearly identify how to remove that individual's access from all applicable company systems, including external service providers, and the timeline required for accomplishing these tasks.

**LP3 can help by:**

- Provide initial draft policies and procedures associated with the appropriate framework for rapid compliance
- Work with client to develop detailed policies and procedures tailored to your unique business environment
- Provide online cyber security portal to maintain policies and track staff member sign-off

## Host Security Profile Management

Operating systems and many commercial security tools have thousands of configuration options to manage workstation and server security profiles. Managing security configuration and service level agreements internally and across multiple service providers is complex and challenging. Some of this work is done by external service providers however the business is still responsible for those configurations. In addition, as businesses grow and change, maintaining configuration control is critical to establish and maintain compliance as well as keep a solid security posture over time.

**LP3 can help by:**

- Assisting with product selection business cases and requirements mapping for security systems and products to help businesses make informed purchasing decisions for cyber security products and services
- Provide subject matter experts for installing, configuring, and operating commercial products enabling the business to focus on operations while LP3 secures the network

## Log Analysis and Alerting

Many business IT staffs are overwhelmed with the huge volume of cyber security data generated by the workstations and servers in the business. Especially when configured to meet NIST or CIS framework standards, there could be hundreds of gigabytes or even multiple terabytes of data generated per day in some enterprise networks. Analyzing this volume of data and providing effective alerts on possible malicious activity is a unique cyber security operations skill that many businesses do not have in house. LP3 can bring cyber SMEs with enterprise-scale expertise to reduce that data down to a manageable volume while minimizing false positives but not dropping critical alerting events. An example of this activity is that LP3 will configure your perimeter firewalls to alert on unusual outbound traffic. Most organizations do not do this egress filtering, but this technique can quickly identify malicious activity enabling the IT staff to work smarter on the most critical issues.

**LP3 can help by:**

- Conduct an assessment on current host logging configurations for compliance with frameworks
- Develop a strategy to maximize critical alerting while minimizing noisy alerts
- Develop draft Standard Operating Procedures (SOPs) helping your staff work effectively and efficiently
- Conduct off-site log analysis and alerting as a service
- Configure on-site systems, such as Splunk, ARCSight, RSA Archer, to optimize alerting
- Collaborate with IT staff to efficiently prioritize cyber security actions, alerting, and environment updates
- Deploy enterprise-scale deception technology with zero-false positives to immediately identify compromised hosts, identify insider threats, alert on data exposed on the Internet, and enable reduction of manual log review labor

## Cyber Product Selection and Analysis of Alternatives

There are a wide variety of products available with overlapping claims of solving cyber security challenges in networked environments. Some of these products are fantastic and will help your organization quickly and effectively. Other products may duplicate capability that you already invested in. Some products are duplicative but may fill a critical compliance or cyber security posture gaps. Some open source products may look very inexpensive, but the support cost may be significantly higher than using a supported commercial product. Knowing which product to choose, and which license type is best, requires subject matter expertise across multiple product lines. Some cloud and MSP services may duplicate on-premise products and services. An example of this service is helping an organization decide between LogRhythm, Splunk, ArcSight, or RSA Archer. LP3 can help with the tradeoff analysis and assist with deployment and operations. Most businesses are not experts in security products and some external assistance is needed.

**LP3 can help by:**

- Assisting with product selection and Analysis of Alternatives to help businesses make informed purchasing decisions for cyber security products and services
- Analysis of licensing alternatives to control cost
- Planning and deployment of SEIM tool
- Configuration and operation of SEIM tool

## SOC Operations

Security Operations Centers (SOCs) are critical to cyber resilience. Many firms struggle to staff a SOC with qualified cyber security engineers. With high demand, positions are hard to fill. Not having expertise on duty during a critical time can negatively impact business operations by missing compromise activity or responding improperly.

**LP3 can help by:**

- SOC staff augmentation

- Standard Operating Procedure development for consistent response actions
- SOC outsource SLA development and contract review
- Robotic Process Automation (RPA) reducing SOC staffing level while increasing capability
- SOC staff incident handling training
- SOC tabletop scenarios

## Forensics

Cyber forensics is the analysis of compromised devices post-event. In most cases, the purpose is to analyze who, what, when, where, how, and why the attacker compromised the device. These questions are challenging to answer with limited data available. Also, expertise for particular device types may not be available in the organization.

**LP3 can help by:**

- Providing key forensic expertise for specific platforms
- Deliver quick results on how the attacker exploited the system for prompt remediation
- Deliver quality reports with high fidelity information for after action follow up and prosecution
- Support prosecution efforts with expert testimony

## Network Engineering and Performance Analysis

Enterprise scale networks are increasingly complex with multiple layers of transport technology, various levels of performance, and limited visibility. Some organizations are unable to map critical business functions to communications links and minimum performance levels to maintain operations.

**LP3 can help by:**

- Providing mapping and route verification services
- Conducting WAN performance analysis and tuning
- Conducting cross-domain system performance analysis and tuning
- Execute application performance testing verifying functionality at various levels of network latency, jitter, packet loss, and bandwidth availability
- Deliver Software Defined Networking (SDN) to end points significantly improving performance with multi-path communications transport services
- Deliver enterprise DNS Spoofing protection to reduce risk of compromise from redirection attacks

## Enterprise Anti-virus

Enterprise anti-virus and malicious code tools are critical to maintaining host security especially on workstations where users can inadvertently download malicious software.

**LP3 can help by:**

- Providing enterprise AV services
- Coordinating enterprise AV service contracts and SLAs with vendors
- Validating AV performance and alerting configurations
- Conducting technical penetration tests verifying successful and unsuccessful detections
- Assessing percentage of devices under AV protection across the enterprise

## Enterprise SPAM Filtering

Enterprise anti-spam filtering is required to reduce the volume of unauthorized, unexpected, and possibly malicious email directed to organizational email accounts. Effective spam filtering reduces the risk of compromise via phishing.

**LP3 can help by:**

- Providing enterprise AV service Analysis of Alternatives
- Conduct planning and implementation to install and activate a SPAM filtering solution

## Mobile Device Management (MDM)

Mobile devices may contain organizationally sensitive information and this data needs to be controlled to provide authorized access but also maintain an effective data security posture. Mobile devices could be lost or stolen possibly resulting in unauthorized access or data breach.

**LP3 can help by:**

- Providing enterprise MDM service Analysis of Alternatives – internal or outsourcing
- Conduct planning and implementation to install and activate an effective MDM solution
- Operate the MDM solution

## IoT Security and Enterprise Integration

Internet of Things (IoT) integration requires additional security engineering expertise to ensure the IoT system and communications methods are properly secured to maintain effective visibility and control of the IoT devices and management infrastructure. Some IoT devices cannot be configured in a secure manner and require external secure networking solutions to protect them. Some outsourced IoT approaches do not match the level of enterprise security or compliance required to maintain effective business operations.

**LP3 can help by:**

- Deliver business case analysis documentation to clarify pros and cons of various approaches leveraging IoT for business growth
- Providing enterprise IoT security engineering services
- Conduct planning and implementation to install and activate an IoT solution for expanding business operations
- Operate and maintain the business IoT environment, products, and management solution

## SOC 2 Compliance and Support

SOC 2 applies to SaaS companies, as well as any company that stores customer information in the cloud. Before 2014, cloud vendors had to meet SOC 1 (SSAE 16) compliance. Now, any company storing customer data in the cloud must meet SOC 2 compliance requirements in order to minimize risk and exposure to that data.

**LP3 can help by:**

- Streamlining policies, processes, and practices to operate quickly and effectively while reducing cost
- Configure continuous monitoring for unusual system activity, authorized and unauthorized configuration changes, and user activity
- Configure monitoring for alerting on unknown and unexpected activity in the environment
- Build anomaly alert action Standard Operating Procedures for unauthorized exposure or modification of data, controls, or configurations, file transfer activities, privileged filesystem, account, or login access
- Audit trail configuration to provide information on who modified what and when relating to modification, addition, or removal of key system components, unauthorized modifications of data and configurations, and breadth of attack impact and possible source
- Configure host-based monitoring for the forensic visibility to see where an attack originated, where it traveled to, what other parts of the system are impacted, the nature of impact (DDoS, IP theft, ransomware, etc.), and what the attackers next move might be

# HIPAA/HITECH Compliance and Medical Environment Security

HIPAA/HITECH requires strong protections on Electronic Health Information (EHI) including extending that protection to business associates. This law provides for strong penalties including fines and jail time for executives failing to properly protect this sensitive information. However, many medical environments offer wireless remote access to this data, operate equipment with obsolete operating systems, and have limited protections in place resulting in frequent compromises and breaches.

**LP3 can help by:**

- Analyzing HIPAA/HITECH compliance posture and providing a Plan of Action and Milestones (POA&M) to remediate findings on a prioritized basis—the items most like to impact business operations or finances
- Conduct external penetration testing and internal vulnerability analysis to provide higher fidelity information on the specific challenges on each network segment
- Deploy network isolation and protection solutions to take vulnerable medical devices off the network making them invisible to attackers while still providing authorized access
- Conduct wireless vulnerability testing and configure devices for secure access only
- Conduct security analysis and recommend remediation on medical devices in preparation for deployment in hostile Internet connected environments

# Summary

Cyber Security and compliance to industry and government standards could mean the difference between success and failure. It is no longer a nicety but mandatory for business continuity and resiliency. Having a Chief Information Security Officer to lead and coordinate security process, procedure and operations is imperative to a strong Cyber Posture.

LP3 provides a variety of cyber security services and products to meet government and business needs. The services can be tailored to the specific needs of the client. LP3 is also vendor independent and provides reliable trusted advice to help clients make well-informed decisions on cyber security and IT roadmap investments.

Lastly, the cost of a compromise or breach can be in the millions of dollars. With a clear ROI, LP3 delivers cost effective solutions to prevent and minimize the impact of these disruptive events helping to achieve cyber resilience. From a long-term value perspective, LP3 guidance can help your organization leverage cyber technologies to improve cyber resilience and expand mission and business operations sharing information with more people in more locations faster than ever before. Change is accelerating and LP3 is your trusted partner to not only cope with rapid change but embrace it for mission and business value.