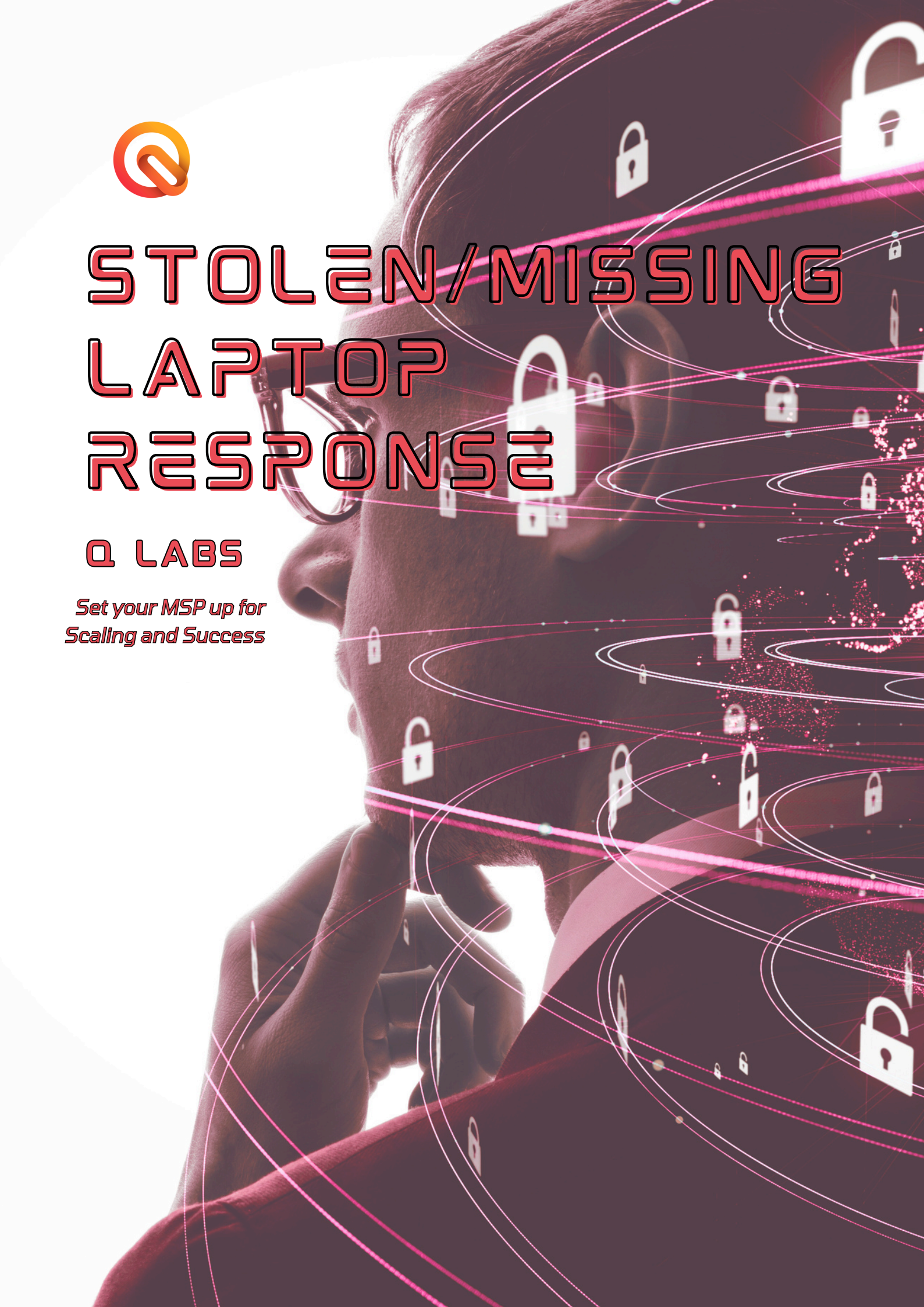

STOLEN/MISSING LAPTOP RESPONSE

Q LABS

Set your MSP up for Scaling and Success

INTRODUCTION

THE MSP SECURITY CHALLENGE

Every MSP knows the panic that strikes when a client calls about a missing laptop. Data breach risks. Regulatory compliance issues. Frantic clients demanding immediate action.

Without a standardized response plan, these incidents create chaos, increase your liability, and damage client confidence.

Our three-tiered Stolen/Missing Laptop Response SOP transforms this emergency from a crisis into a streamlined process that showcases your MSP's security expertise.

LEVEL 1: BASIC RESPONSE PROTOCOL

FOR MSPS IMPLEMENTING THEIR FIRST SOPS

01 INITIAL TICKET CREATION

1. Create new ticket with priority: URGENT
2. Use ticket template below:

Subject: URGENT - Lost/Stolen Device Report - [Company Name]

Incident Details:

- Date/Time Reported: [DateTime]
- Reported By: [Name]
- Contact Number: [Phone]
- Company: [Company Name]
- Device Name: [Hostname]
- Asset Tag (if any): [Tag]
- Last Known Location: [Location]
- Date/Time Last Seen: [DateTime]
- Suspected Lost or Stolen?: [Lost/Stolen]
- Police Report Filed?: [Yes/No]
- Police Report Number: [If applicable]

Actions Taken:

☐ BitLocker Lock Attempted
☐ Site Contact Notified
☐ Security Measures Implemented
☐ Documentation Complete

BitLocker Recovery Key: [Key]

LEVEL 1: BASIC RESPONSE PROTOCOL

FOR MSPS IMPLEMENTING THEIR FIRST SOPS

02 IMMEDIATE ACTIONS

1. Technical Response

- Attempt to connect to device remotely
- If device is online:
  - Execute "Lock endpoint with BitLocker" component
  - Force device reboot
- Document BitLocker recovery key in ticket

.2. Communication

- Send basic notification email to site contact

3. Documentation

- Update ticket with all actions taken
- Attach all communication records

LEVEL 1: BASIC RESPONSE PROTOCOL

FOR MSPS IMPLEMENTING THEIR FIRST SOPS

02 IMMEDIATE ACTIONS

Subject: URGENT: Lost/Stolen Device Notification - [Company Name]

Dear [Contact Name],

We have received a report of a lost/stolen device from your organization. We are taking immediate security measures to protect company data.

Device Details:

- Device Name: [Hostname]
- Last Known Location: [Location]
- Date/Time Last Seen: [DateTime]

Actions Taken:

- Remote security measures implemented
- Device encryption enforced

Recommended Actions:

1. File a police report if theft is suspected
2. Document the incident for insurance purposes
3. Contact us with any additional information

Please reply to confirm receipt of this notification.

Best regards,
[Your Name]
[MSP Name]

LEVEL 2: ENHANCED RESPONSE PROTOCOL

FOR MSPS WITH BASIC PROCEDURES LOOKING TO IMPROVE

01 INITIAL TICKET CREATION

1. Create high-priority incident ticket with enhanced template:

Subject: URGENT - Lost/Stolen Device Incident - [Company Name] - [DateTime]

INCIDENT DETAILS

Primary Information:

- Incident Date/Time: [DateTime]
- Report Date/Time: [DateTime]
- Reported By: [Name]
- Contact Information: [Phone & Email]
- Company: [Company Name]
- Department: [Department]

Device Information:

- Device Name: [Hostname]
- Serial Number: [SN]
- Asset Tag: [Tag]
- Device Type: [Laptop/Tablet]
- Operating System: [OS]
- Last Known IP: [IP]
- Last Connected: [DateTime]
- Last Backup Status: [DateTime]
- Installed Software: [Key Applications]

Location Information:

- Last Known Location: [Location]
- Date/Time Last Seen: [DateTime]
- Circumstances: [Brief Description]
- Suspected Lost or Stolen?: [Lost/Stolen]

Security Status:

☐ BitLocker Active
☐ GPS Tracking Enabled
☐ Cloud Backup Current
☐ VPN Access
☐ Admin Rights

LEVEL 2: ENHANCED RESPONSE PROTOCOL

FOR MSPS WITH BASIC PROCEDURES LOOKING TO IMPROVE

01 INITIAL TICKET CREATION

1. Create high-priority incident ticket with enhanced template:

Subject: URGENT - Lost/Stolen Device Incident - [Company Name] - [DateTime]

Action Checklist:
☐ BitLocker Lock Attempted
☐ User Accounts Disabled
☐ Active Sessions Terminated
☐ GPS Tracking Initiated
☐ Site Contact Notified
☐ Manager Notified
☐ Security Measures Documented

Timeline of Actions:
[DateTime] - Incident Reported
[DateTime] - Ticket Created
[Add additional actions with timestamps]

BitLocker Recovery Key: [Key]
Network Access Credentials: [If applicable]

LEVEL 2: ENHANCED RESPONSE PROTOCOL

FOR MSPS WITH BASIC PROCEDURES LOOKING TO IMPROVE

02 COMMUNICATION TEMPLATES

1. Initial Site Contact Notification

Subject: URGENT: Security Incident - Lost/Stolen Device - [Company Name]

Dear [Contact Name],

This email serves as formal notification of a lost/stolen device incident affecting your organization. We have initiated our security response protocol and are taking immediate action to protect company data.

Incident Details:

- Device: [Device Name/Type]
- Last Known Location: [Location]
- Date/Time of Last Known Usage: [DateTime]
- Affected User: [User Name]

Actions Already Taken:

1. Remote security measures implemented
2. Device encryption enforced
3. User accounts secured
4. Remote access disabled

Required Actions:

1. Please acknowledge receipt of this notification
2. File a police report if theft is suspected (template attached)
3. Document the incident for insurance purposes (template attached)
4. Complete the attached incident form for our records

LEVEL 2: ENHANCED RESPONSE PROTOCOL

FOR MSPS WITH BASIC PROCEDURES LOOKING TO IMPROVE

02 COMMUNICATION TEMPLATES

1. Initial Site Contact Notification

Subject: URGENT: Security Incident - Lost/Stolen Device - [Company Name]

Next Steps:

1. We will provide hourly updates until all security measures are confirmed
2. A detailed incident report will be provided within 24 hours
3. We will schedule a brief meeting to discuss any data exposure risks

Please contact us immediately if you have any questions or receive any information about the device.

Attachments:

- Police Report Template
- Insurance Claim Template
- Incident Documentation Form

Best regards,
[Your Name]
[MSP Name]
[Contact Information]

LEVEL 3: ENTERPRISE-GRADE RESPONSE PROTOCOL

GOLD STANDARD FOR MSPS

01 ENHANCED COMMUNICATION TEMPLATES

1. Initial Site Contact Notification

Subject: SECURITY INCIDENT ALERT - Lost/Stolen Device - [Company Name] - [Severity Level]

INCIDENT NOTIFICATION
Status: Active Response Required
Severity: [Level 1-4]
Incident ID: [Ticket Number]

PRIMARY DETAILS

- Client: [Company Name]
- Incident Type: Lost/Stolen Device
- Time Reported: [DateTime]
- Current Status: [Status]

DEVICE INFORMATION
[Detailed device information]

CURRENT ACTIONS

- Security Protocol: Initiated
- Response Team: Activated
- War Room Status: [If Applicable]

IMMEDIATE RESPONSE REQUIREMENTS
Technical Team:
☐ Execute security lockdown protocol
☐ Initialize tracking procedures
☐ Begin data exposure assessment

LEVEL 3: ENTERPRISE-GRADE RESPONSE PROTOCOL

GOLD STANDARD FOR MSPS

01 ENHANCED COMMUNICATION TEMPLATES

1. Initial Site Contact Notification

Subject: SECURITY INCIDENT ALERT - Lost/Stolen Device - [Company Name] - [Severity Level]

Management Team:
☐ Client relationship management
☐ Regulatory compliance assessment
☐ Insurance/legal notification review

Communications Team:
☐ Prepare client updates
☐ Draft regulatory notifications
☐ Coordinate with PR if needed

NEXT STEPS

1. Join war room: [Link]
2. Acknowledge receipt
3. Begin assigned tasks
4. Report status hourly

Updates will follow according to incident response protocol.

[Signature Block]

LEVEL 3: ENTERPRISE-GRADE RESPONSE PROTOCOL

GOLD STANDARD FOR MSPS

01 ENHANCED COMMUNICATION TEMPLATES

2. Client Executive Brief

Subject: Executive Brief: Security Incident [Incident ID] - [Company Name]

Dear [Executive Name],

This brief provides a comprehensive overview of the security incident affecting your organization.

EXECUTIVE SUMMARY

- Incident Type: Lost/Stolen Device
- Impact Level: [Level]
- Current Status: [Status]
- Business Risk: [Assessment]

KEY POINTS

- [3-4 bullet points of critical information]

ACTIONS TAKEN

Technical:

- [List of technical measures]

Administrative:

- [List of administrative actions]

Legal/Compliance:

- [List of legal/compliance actions]

LEVEL 3: ENTERPRISE-GRADE RESPONSE PROTOCOL

GOLD STANDARD FOR MSPS

01 ENHANCED COMMUNICATION TEMPLATES

2. Client Executive Brief

Subject: Executive Brief: Security Incident [Incident ID] - [Company Name]

RISK ASSESSMENT
Data Exposure: [Assessment]
Regulatory Impact: [Assessment]
Business Impact: [Assessment]

RECOMMENDATIONS

1. [Primary recommendation]
2. [Secondary recommendation]
3. [Additional steps]

NEXT STEPS

- [Immediate next steps]
- [Timeline for resolution]
- [Required client actions]

We have assigned [Name] as your dedicated incident manager. They can be reached 24/7 at [Contact Information].

A detailed technical report is attached for your IT team's review.

Best regards,
[Your Name]
[Title]
[MSP Name]

THE MSP DIFFERENCE MAKER

THIS SOP DOESN'T JUST PROTECT YOUR CLIENTS' DATA—IT TRANSFORMS SECURITY INCIDENTS INTO OPPORTUNITIES TO DEMONSTRATE YOUR VALUE.

WHAT YOU'LL RECEIVE

- ✅ The Stolen/Missing Laptop Response SOP with 3 maturity levels
- ✅ The full-resolution Device Security Incident Flowchart
- ✅ Editable templates for all communication examples
- ✅ Implementation checklists to get started immediately

Don't let operational chaos be your MSP's villain. With these five critical SOPs, you'll be equipped with the secret weapons you need to scale efficiently, serve clients consistently, and build an MSP that runs like a well-oiled machine.

Your clients don't just need IT support—they need IT management. These SOPs are how you deliver on that promise.

MORE ABOUT Q LABS

READY FOR YOUR NEXT MISSION BRIEFING? CONTACT Q LABS TODAY TO RECEIVE YOUR FREE SOP TEMPLATE BUNDLE.

Note: For MSPs looking to take their automation to the next level, Q Labs offers premium access to our Cleared Access program with advanced automation scripts and personalized implementation guidance. Ask us how during your strategy session.

Clearance Details:

- Access Level: Immediate
- Cost: $0.00 per endpoint
- Classification: MSP Eyes Only

Get your clearance now:

REQUEST ACCESS

This message will not self-destruct, but do act quickly.

Q LABS

Contact Us

www.qlabs.dev

(504) 262-1234