CYBERATTACK Readiness Kit

The first hour after a cyberattack is your critical advantage. Here's the playbook your company needs before, during, and after a cyberattack.

LeapFrog®

Extraordinary IT and Cybersecurity Services

Cyberattack Landscape Overview

LEAPFROG

Understanding today's risk environment and the importance of preparedness.

- Average breach cost: **$4.88M**
- Average breach lifecycle: **258 days**
- Organizations with tested Incident Response plans save **$1.49M per breach**
- Only **55%** of companies have documented plans
- Only **30-35%** regularly test those plans
- **68%** of breaches involve human error
- **Ransomware remains a dominant threat vector**

Did you know: A cybercriminal will stay in your IT environment, observing and planning an attack for an average of **200 days**.

Early detection paired with a well-prepared, highly responsive first hour dramatically reduces business impact and remains one of the strongest predictors of successful recovery.

Cyberattack Readiness Checklist

LEAPFROG

Assess your organization's preparedness across four critical areas.

Planning & Governance

- ☐ Incident response plan is documented and reviewed annually
- ☐ Leadership roles and decision-makers are clearly defined
- ☐ Critical business systems and processes have been prioritized

Detection & Reporting

- ☐ Employees know how to report suspicious activity
- ☐ Security monitoring is in place to identify potential threats
- ☐ Incident reporting and escalation procedures are documented

Response & Communication

- ☐ Key response contacts are documented and accessible
- ☐ Cyber insurance, legal, and response partners are identified
- ☐ Alternative communication methods are available during an outage

Recovery & Testing

- ☐ Recovery procedures are documented and backups are regularly tested
- ☐ Response exercises or tabletop simulations are conducted regularly
- ☐ Readiness is reviewed as business operations and technology evolve

Readiness Snapshot
10-12 checks = Advanced Readiness
6-9 checks = Foundational Readiness
1-5 checks = Improvement Opportunities

ARE We Under Attack?

LEAPFROG

Common warning signs

- Files encrypted or renamed
- Lock screen demanding payment
- Sudden inability to access shared drives or applications
- Unexpected password resets
- Emails sent you didn't write
- Vendor payment changes or unusual financial requests
- Suspicious links or attachments
- Requests for credentials or MFA codes
- Emails impersonating executives or vendors
- Login alerts from unfamiliar locations
- MFA prompts you didn't initiate
- Unauthorized changes to accounts or settings
- Unusual data downloads
- Unauthorized access attempts
- Privileged account misuse

If you suspect an attack, do these four things immediately:

1. Disconnect affected devices from the network, leaving power on if possible. Only unplug Ethernet cables and disable Wi-Fi.

2. Stop all data movement. Avoid restoring, deleting, or modifying files until the incident is assessed.

3. Preserve evidence. Capture screenshots of error messages, suspicious emails, login alerts, or unusual activity.

4. Notify your Executive contact by phone call or in person.

We ARE Under Attack

LEAPFROG

Time is Critical

Notify your contacts by phone. (Attacker could be monitoring your emails and other online platforms)

1. **Internal Response Team:** IT/Security Lead, Executive Leadership, Legal Counsel
2. **External Incident Response Team:** Leapfrog Services **at 404-974-RISK (7475)**
3. **Insurance**
4. **Law Enforcement:** FBI Field Office and/or Local Police
5. **Regulatory & Compliance Contacts**
   - State Attorney General: Required if personal data is exposed
   - Industry Regulators: FTC, HIPAA, PCI-DSS, financial regulators, etc., depending on your business
   - CISA/US-CERT
   - Internet Crime Complaint Center (IC3)
6. **Communication & PR:** Internal Comms Lead
7. **Affected Third Parties:** Vendors, Partners, Customers

What to know before you call Leapfrog: Details of incident • Systems and data affected • Who has access • Backup Information
404-974-RISK (7475)

Response Team Directory

These are the people you call.

Complete this call tree to clarify roles during an incident.

Executive Contact: First point of contact for staff, coordinates with all parties involved, and can authorize major decisions.
Name: _____
Phone: _____

IT Lead / Technical Contact: Coordinates with the incident response team, gathers logs, preserves evidence, and manages containment steps.
Name: _____
Phone: _____

Legal Counsel: Advises on regulatory requirements, breach notification obligations, and risk exposure.
Name: _____
Phone: _____

Finance / Insurance: Handles cyber insurance claims, financial impact assessments, and vendor payment reviews.
Name: _____
Phone: _____

Communications / PR: Manages internal and external messaging, including staff updates and customer notifications.
Name: _____
Phone: _____

HR Coordinates employee communication, access changes, and any personnel-related investigations.
Name: _____
Phone: _____

Leapfrog + Seedpod Cyber
Stronger together

This partnership helps our clients strengthen their cybersecurity posture and align their IT protections with cyber insurance requirements from day one. Leapfrog underwent a rigorous vetting process, allowing our clients to gain a clearer view of their cyber risk, identify coverage or compliance gaps, and access guidance designed to help your policy perform when it matters most.

Benefits include:

- A complimentary cyber insurance eligibility review
- Industry-specific risk insights
- Validation of key security requirements
- Support closing insurance gaps
- Preferred cyber insurance pricing – often at a savings of 30% or more

And, if something does go wrong, our clients can be confident that not only will your policy pay out, but that we will lead the remediation directly - giving you a quicker recovery, reduced downtime, and a claims process that works.

Extraordinary IT and Cybersecurity Services

Recovery is just the beginning. From incident response to long-term protection, Leapfrog provides a seamless path to a carefully curated cybersecurity and IT solutions designed to reduce risk, support compliance, and strengthen business resilience.

We are a security-first managed IT service provider offering:

- Infrastructure Strategy, Roadmapping, and Management
- Cybersecurity & CyberRisk Beyond IT program
  - Cyber Risk assessments
  - Cyber Retainer packages
- vCIO and vCSO services
- Cloud Services
- Support Services
- Application Services
- Governance and Compliance Guidance & More

If you think you have been attacked, call Leapfrog Services:

404-974-RISK (7475)

For additional inquiries: Leapfrogservices.com

LEAPFROG®

Extraordinary IT and Cybersecurity Services