LBMC INFORMATION SECURITY

INFORMATION SECURITY INCIDENT RESPONSE & FORENSICS SERVICES

When responding to a security incident, there should be three primary goals:

- Minimize the Impact
- Restore the Affected Environment to Full Working Order
- Communicate with Relevant Parties as Appropriate

The ability for today's organizations to quickly and effectively respond to an information security incident has never been more crucial. A prompt and proper response to network and data attacks can prevent unneeded expense, avoid over-extending internal resources, and provide the essential information needed to make critical decisions on how to move forward.

THE ISSUES — STATISTICS RELATED TO DATA BREACHES AND CYBERSECURITY

U.S. COMPANIES **PAY** **$7,350,000** ON AVERAGE PER BREACH IN FINES, REMEDIATION COSTS, AND LOSS OF CUSTOMERS.

(PONEMON INSTITUTE'S SIXTH ANNUAL BENCHMARK STUDY ON PRIVACY & SECURITY OF HEALTHCARE DATA)

89% of studied healthcare organizations have experienced a data breach that involved patient data being stolen or lost over the past two years.

(Ponemon Institute's Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data)

87% of companies experienced at least one incident in the past year.

(Sans 2017 Incident Report Survey)

CONTACT US TODAY

PHONE (844) 526-2732

EMAIL info@LBMCInformationSecurity.com

ONLINE LBMCInformationSecurity.com

LBMC INFORMATION SECURITY

SERVICES — WHY LBMC?

WHEN IT COMES TO ADDRESSING INCIDENT RESPONSE, LBMC INFORMATION SECURITY LEVERAGES EXTENSIVE SECURITY AND DIGITAL FORENSICS EXPERTISE WHILE SEEKING TO MINIMIZE THE OVERALL IMPACT THROUGH THE FOLLOWING SERVICES:

1. Incident Response

LBMC Information Security's incident response methodology leverages the NIST-800-61 Computer Security Incident Handling Guide to determine answers to critical questions such as:

WHEN— We determine when the incident initially occurred to define the timeframe of exposure. It is not uncommon to find that the intruders have been on networks for months before detected.

WHERE— We determine the point of initial compromise, and document all locations of the compromise to properly contain and eradicate the threat.

WHAT—We determine the extent of the compromise to outline next steps.

HOW— We determine the root cause of the incident to provide the needed details for proper remediation.

2. Incident Response Plans

Incident Response Plan = A documented plan/procedure for how the incident will be handled.

While the contents may vary from organization to organization, most consist of standard operating procedures, processes, and communication plans.

3. Incident Response Programs and Training

LBMC Information Security also works with organizations to elevate their incident response plans into proactive incident response programs. We design and deliver custom incident response tabletop exercises, which can pay dividends with faster response times, better communications, and lower costs when an incident does occur.

4. Forensic Analysis

LBMC Information Security's certified forensic analysts follow strict evidence handling procedures and employ a forensics analysis methodology that has been built on more than 10 years of experience.

5. Penetration Testing

Penetration testing will reveal vulnerabilities that an attacker could use to compromise your security. Some of the ways we determine these vulnerabilities are through:

Social Engineering
This process helps expose practices that create vulnerabilities and helps determine the vigilance and awareness of your personnel.

Web-Application Testing
This two-pronged approach provides you with a clear picture of any security weaknesses that exist in your applications, as well as the likelihood of the exploit.

External Penetration Testing Services
This assessment determines the security posture of your external (Internet facing) network infrastructure and provides recommendations to improve the existing security measures in place.

Internal Network Penetration Testing Services
Internal penetration testing constitutes an analysis of the network and systems from the point of view of an attacker who has already gained access to the internal network.

Wireless Network Security Testing
We evaluate the security of your wireless networks, including penetration tests and architecture design reviews, to attempt to access sensitive information and/or leverage a wireless connection to gain access to your private network environment.

6. Our Other Security and Compliance Services

- Risk Assessments / Current State Assessments
- Security Program Development
- Managed IDS / IPS Monitoring
- Security Information and Event Management (SIEM)
- CMS Information Security
- FISMA/NIST
- HIPAA
- HITRUST
- PCI
- System and Organization Control (SOC) Assessments
- SOX/COSO/COBIT

OUR EXPERIENCE — TESTED AND TRUSTED

As GIAC certified incident handlers, we have been called on in response to all types of security incidents caused by all of these threats over the years, including:

Financial Fraud **Nation States** **Insider Threats** **Hacktivists**

Awarded as a Top Ten Cybersecurity Provider

20+ 20+ years of information technology experience

5/8 5/8 of the Largest U.S. For-Profit Health Systems are Our Clients

We can help with your sensitive incident response needs. Our professionals are ready to begin assessing needs, so contact us today for a discreet consultation!

CONTACT US TODAY

PHONE
(844) 526-2732

EMAIL
info@LBMCInformationSecurity.com

ONLINE
LBMCInformationSecurity.com