



# IPkey.com

Business Service  
Management & Monitoring

(505) 243-1010  
(866) 330-1010

## Confidentiality, Integrity & the Inside Threat

Today, the two most important assets of any organization are the people who make it work, and the information they use to do so. In addition to sensitive internal data such as HR files, client data is likely to be found all over your network. Email, documents and spreadsheets commonly exist in insecure locations and are often confidential, preliminary drafts.

This is the 'low hanging fruit' that invites new insider threats. The current economic climate is prompting layoffs and reduced hours at many firms. Combined with the economic desperation that many families are facing, this is the 'perfect storm' for insider threats. A surprising number of employees admit to copying company files to a personal USB key for 'insurance' in a future adversarial situation. What is interesting is that they do not see this act alone as unethical, even though it is a violation of policy and indeed theft.

Two bad things can happen to your data. First, it can be disclosed to the wrong people. Second, it can be altered. If this data

relates to employees or clients, two bad things can happen to you. A lawsuit from the 'injured' party and unwelcome interest from regulatory or compliance agencies.

Problems with data confidentiality and integrity may not hurt your organization as immediately as network outages, but they can be even more damaging in the long run. IPkey can help you assess and understand where and how Data Leaks occur. Our experts will then assist with remediation strategies that address the immediate vulnerabilities, while crafting a long-term organizational strategy to change the way we look at data. We have years of experience; not just with technology, but how to successfully effect change in organizations like yours. (Yes, like yours...)

### 12 tough questions every executive, officer or partner should ask IT:

1. Do we have a *written* employee "Computer and Internet Use Policy?"
2. Are *all* external network access points protected by correctly configured security gateways, VPNs or other devices?
3. Do *all* PCs have *all* the latest Microsoft security patches?
4. Are *all* computers scanning for viruses with the *latest* definitions?
5. How are we preventing employees copying data using personal USB devices?
6. How do we know what sites employees are surfing on the web?
7. Are home and remote users creating a security loophole?
8. What are users downloading and installing from the Internet, and worse, what company information is being uploaded?
9. How is productivity affected when our Internet access is down?
10. Are we compliant with federal, state & industry regulations such as PCI?
11. Where is our Disaster Recovery Plan and has it been tested?
12. How is all of this currently documented and managed?

### Top 10 Threats to your IT Services

1. Phishing
2. Spyware
3. Viruses
4. OS Vulnerabilities
5. Hardware Failures
6. Bad Backups
7. Power problems
8. Employees
9. Hackers
10. IS Contractors

*"Almost every PC on our network had unauthorized software downloaded from the net. Spyware, keystroke loggers. You name it, we had it. The users didn't have a clue, and truthfully, neither did we." [Manager ISD]*

*"Before we used IPKey's Monitoring Service, I couldn't take a real vacation. Now I know any problem will be identified and dealt with quickly." [IT Director]*



### 7 Winning Strategies to Boost Productivity and Cut Costs

*"The key strategy in 2009 for our clients' success is smart innovation. The right technology in the right place can reduce recurring costs while meeting growing IT demand."*

1. **Minimize** revenue lost caused by service outages by real-time monitoring of critical infrastructure.
2. **Save** by using SaaS or Managed Service Providers where possible.
3. **Consolidate** gateway security services and slash annual support & maintenance fees.
4. **Virtualize** servers, gateways & networks to reduce management time and maintenance fees.
5. **Reduce** non-business use of computers and Internet to boost productivity & control Internet bandwidth costs.
6. **Verify** vendor SLA performance with availability & performance monitoring.
7. **Manage** IT efficiently by having accurate, current reporting of metrics you can really use.

We can bring a wealth of 'best practices' to the table and help you decide what will work within your organization. We can take any of our well-proven 'templates' and quickly modify it to your specific needs. Start saving today!

Learn more at [ipkey.com](http://ipkey.com) Productivity section

>>> [ipkey.com](http://ipkey.com) (505) 243-1010  
>>> [info@ipkey.com](mailto:info@ipkey.com) (866) 330-1010



**IPkey.com**

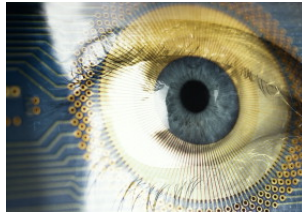
Business Service  
Management & Monitoring

(505) 243-1010  
(866) 330-1010

## Business Continuity & Monitoring

Almost every organization today depends on information technology. Any significant interruption or degradation of IT services is at best very costly, and at worst, crippling to the organization. Year after year, this dependency grows. Ensuring the reliable delivery of IT services to the enterprise has become more critical as IT failures become common and more costly. Interruptions or degradations of these services can occur for many reasons, but the most common are:

1. Employee web activity
2. Phishing & spyware
3. IT Upgrades & changes
4. Unsecured PC/Server
5. System & circuit failures



What these have in common is that while problematic, their symptoms commonly go undetected until major and obvious damage to organizational function has occurred. However, with early detection, many of these issues could have been resolved for a fraction of the cost before the damage cascaded out of control.

This is why after an IT meltdown every organization asks the question, "How can this be prevented?" The answer is monitoring. While root causes can be addressed, there will always be unforeseen events that need timely attention. Once you understand Monitoring, anything less feels like driving a truck blindfolded. You'll likely run out of gas if you don't crash first.

Many firms attempt some form of monitoring internally, but our experience shows that many pitfalls can sideline even the best effort. Lack of time, skills, staffing, budget, priority are common reasons.

With independent external monitoring, you can avoid the challenges and enjoy the benefits immediately. And save money. Take off the blindfold and contact us today!

### Are you (or have you ever been) a Spammer?

Probably, especially if your firm has ever been black-listed. Like it or not, the odds are that at least one PC at your firm has been infected with malware that then used your network to send spam. Indeed, if it can be shown that your spam infected someone else, you might have to pay damages.

*Tip: the only way to be sure is to monitor outbound email traffic.*

*Monitoring has cut our down-time by 85% because any failure of our network is immediately routed to whoever is responsible for repair. It's saved us far more than it costs. It's a no-brainer."*



**IPkey.com**

Is a division of Meridian Group, a New Mexico based corporation founded in 1988. Meridian has been providing organizations with IT solutions for 20 years.

## Business Service Management & Monitoring

	Availability & Performance Monitoring	Security & Vulnerability Monitoring	Professional & Managed Services
<b>1. Evaluation</b>			
Vulnerability Scanning & Assessment		Yes	Yes
Security Policy & Procedure Review			Yes
Security & Access Log File Review			Yes
<b>2. Remediation</b>			
Update Policies & Procedures			Yes
Prepare Remediation Plan			Yes
Correct serious problems			Yes
<b>3. Monitoring &amp; Reporting</b>			
Availability	Yes		
Performance & Capacity	Yes		
Power / Environmental	Yes		
Asset (Detection/Removal)	Yes		
Netflow: Switch, Router	Yes	Yes	
Host / Server	Yes	Yes	
Application (SQL, Exch, VM, etc)	Yes	Yes	
VoIP	Yes	Yes	Yes
Productivity (Web)		Yes	Yes
Security Event & Information		Yes	Yes
Business Service Management	Yes	Yes	Yes
<b>4. Managed Services</b>			
Gateway/UTM Perimeter & Zone	Yes	Yes	Yes
Secure Email (Spam Filtering)	Yes	Yes	Yes
End Point Security	Yes	Yes	Yes
Intrusion Detection & Prevention		Yes	Yes
Secure Remote Access	Yes	Yes	Yes
Web Application Firewall		Yes	Yes
Data Leak Prevention (DLP)		Yes	Yes
VPN (IPSec & SSLVPN)	Yes	Yes	Yes
Web Content Filtering		Yes	Yes
WAN Optimization	Yes		Yes
Application Control		Yes	Yes
<b>5. Business Continuity</b>			
Managed Online Backup	Yes	Yes	Yes
Disaster Recovery Planning			Yes

*"We have so many security-management consoles, we can't keep up with all the information. We have firewalls that haven't been updated in months, and reams of security logs we haven't sifted through. I really couldn't tell you whether we've been hacked or not." [IS Manager]*



In August 2000 Meridian Group was honored by CIO Magazine for outstanding Customer Relationship Management.