

**Patches** are designed to fix problems with, or correct weaknesses present in software code. At times, they can also improve usability or performance. Even some of the best written software need patching. However, if not done in a planned, organized manner, patches can introduce more problems than they fix.

In order to avoid this from happening, ICG's patch management service offering is a tailored solution, in which we review, schedule and deploy specific patches to individual systems at a specified time.

## ICG's Patch Management Solution Cycle

1. **Detect** - Identify available patches as soon as they are available.
2. **Assess** - Define which of those are applicable to your environment.
3. **Acquire** - Download applicable patches for testing.
4. **Patch testing** - Because of the unique environments in ICG's customers, sometimes manufacturer testing is not enough. ICG tests deployment on a subset of machines to determine any obvious conflicts with applications before deploying throughout an organization.
5. **Deployment** - After the testing phase has been successful, ICG pushes out patches behind the scenes to your live environment.
6. **Maintenance** - Many patches are released on a monthly basis. It is important that new patches are constantly assessed, which starts the patch management cycle again.

## Consequences of No Patch Management

- A significant drop in employee productivity as a result of computer downtime. This can be caused by a failure in a workstation, an application or a server. End-users are not able to work when their workstations or applications are down. In addition, IT resources are used to diagnose, repair and restart affected components.
- Loss of business from partners or customers due to a decline in credibility or a drop in confidence in your company's operations and/or security.
- Remediation time to fix compromised computer systems. Workstation rebuilds are costly in terms of time and salaries. In addition the rebuild is only as good as its backup.
- Potential loss or corruption of user data. Data can be compromised by virus attacks or from attempts to repair the system after the attack.

## The ROI for Automated Patch Management

Assumptions from The National Institute of Standards and Technology (NIST):

- One-half of unpatched computers will become infected
- 10 out of 20 patches released will be for vulnerabilities exploitable by a virus.

For a company with 100 computers:

- Each infected computer costs 8 hours of downtime: 4 for IT to rebuild it and 4 in lost end user productivity
- Hourly rate of \$65 /hour for IT staff and employee salary.
- Computers will be infected half of the time there is a vulnerability, so 10 times a year.

Costs for recovering from outbreaks:

$$\begin{aligned} \text{Annual Cost} &= W * T * I * R \\ \mathbf{\$160,000} &= 50 * 8\text{hrs/infection} * 10 \text{ infections} * \$65/\text{hr} \end{aligned}$$

W = The number of workstation (1/2x 100=50)

T = Time fixing systems or lost in productivity (8 hours/infection)

I = Times machine is infected (10)

R = Hourly rate of IT technician/employee (\$65/hr)

## Conclusion

ICG's Patch Management solution can provide immediate benefits for your company and its users. Patch Management leads to less downtime, happier users, and significant cost savings to your organization.



7235 Corporate Center Drive, Bay A, Miami, Florida 33126

(305) 594-0848 • (888) 809-4685 • Fax (305) 594-0724

www.icgi.com | icg@icgi.com