THE VALUE OF DOING THINGS RIGHT

Part 2 of 2

By Mitchell R. Sowards
THE VALUE OF DOING THINGS RIGHT

INTRODUCTION

In Part 1 of this whitepaper, we explored how we intuitively can recognize when “doing things right” clearly benefits us compared to an alternative that delivers a putatively similar product or service in a “less good” way.

For example, at my local gym for many, many years and through multiple owners the exercise equipment was not secured to the floor as warning labels clearly directed. The most recent owner surprised me by finally “going the extra mile” to properly secure the equipment to the floor. I now feel certain that I am at less risk of injury or death due to improperly maintained equipment.

We further explored how in the realm of Information Technology (I.T.) services, there can be a stark difference between firms that do things right and firms that don’t. If you are paying an I.T. services firm a monthly fee, you are expecting them to do more than just fix things that break: you are expecting them to be faithfully performing all of the proactive network management tasks that should ensure that your systems are secure, reliable, and optimized – all the time not just occasionally. They should be doing things like monitoring and testing backups, keeping antimalware software functioning and up to date, making sure systems are cleansed of any malware, applying service packs and patches to operating systems and critical applications, and (often ignored completely) maintaining faithful records of their efforts.

And we reviewed some of the ways that ENTRUST strives to “do things right” compared to our competitors.

You may now agree that you appreciate all the ways in which ENTRUST is more faithful than competitors about performing our responsibilities and intuitively believe that you should have a better computing experience than otherwise because of it.

But how does this translate into “value” for our customers? Below is an approach to putting a dollar value on “doing things right”. First, let us explore the “Cost of Downtime” then we will explore the concept of a “Proactive Score”.

UNDERSTANDING THE COST OF DOWNTIME

Many businesses today depend to a greater or lesser degree on their information technology in order to fulfill their company mission. So, when I.T. systems are down the organization loses productivity, revenue, morale, or some combination of all three. It is possible to calculate the estimated cost of downtime to an organization using a relatively simple formula. One formula for calculating the cost of downtime is as follows:

\[
\text{Company Revenue / Work Hours in a Year} \times \text{Productivity Loss (expressed as a percentage)} = \text{Hourly Cost of Downtime}
\]

So as an example, for an organization with $36M revenue per year and running 3 daily shifts (6240 work hours in a year) and assuming that you take a 50% productivity hit
when critical systems are down, the hourly cost of downtime is $2884.62. Average American firms experience “uptime” of 99% which sounds good. But for the sample organization that would represent 62.4 hours of unscheduled downtime (1% downtime) every year! The total cost to the organization over the course of a year (if they are an “average American company”) would be an astounding $180,000!

Proper 24x7x365 monitoring and care can eliminate many such outages (perhaps down to 6 hours of downtime per year for “best in class” companies achieving 99.9% uptime) and can reduce the recovery time when inevitable problems occur. With proper monitoring, the cause of unexpected outages is more quickly isolated and thus more quickly resolved. Proper monitoring and prompt response can save the sample organization $162,000 per year by reducing downtime from 1% to .1%.

EXPLORE FOR YOURSELF: Visit the ENTRUST website http://www.ntrusts.com/ and click on the Annual Downtime Calculator tool right in the middle of the screen. You can insert revenue and productivity values matching your own organization and calculate for yourself how much downtime is costing you today. There is also an Hourly Cost calculator if you are unable to estimate your current levels of downtime.

UNDERSTANDING THE ENTRUST PROACTIVE SCORE

As shown, the cost of downtime is a relatively straightforward calculation. But an equally important aspect of “doing things right” is performing proper proactive care. ENTRUST uses the concept of a “Proactive Score” to measure ourselves against a “perfect” state for computers under our care.

A computer in a “perfect” state would be:

1. **Updates**: A computer that is 100% up-to-date with all critical operating system service packs and patches
2. **AntiMalware installed**: A computer that has properly functioning antimalware software installed
3. **AntiMalware definitions**: A computer that has 100% up-to-date antimalware definitions
4. **AntiMalware scans**: A computer that was fully scanned for malware within the last 24 hours
5. **Disk Optimization**: A computer that has negligible disk fragmentation
6. **Tool Status**: A computer that has fully functioning monitoring and remote access software installed

Wouldn’t it be great if every single computer at your organization was in this perfect state all the time?
As with most things, our experience is that perfection is unachievable. So, it is necessary to define some states short of perfect.

ENTRUST uses a scale like this for each of the above factors

- **“IDEAL”** – any given factor is very close to perfect. For example, disk fragmentation below 10% or AntiMalware definitions less than 1 week old.
- **“ACCEPTABLE”** – any given factor is less than Ideal but not at any level of concern. For example, disk fragmentation above 9% but less than 15% or antimalware definitions less than 2 weeks old.
- **“ACTION REQUIRED”** – any factor that has fallen into a state below Acceptable
- **“UNACCEPTABLE”** – any factor that has fallen into a state significantly below the Acceptable standard

Once every computer has been graded according to the above scale for every one of the defined factors, it is possible to assign an overall “score” to any given customer and, indeed, to ENRUST as a whole.

The number of factors either Ideal or Acceptable / The total number of factors possible = Proactive Score (expressed as a percentage)

So, for example, assume an organization with 100 computers and the same 6 factors mentioned above. There would be a total of 600 elements that must be measured.

Assume also that 576 of those elements were Ideal or Acceptable at a given point in time (and only 24 elements were in the Action Required or Unacceptable state). This customer would receive a Proactive Score of 96%. (96% of all possible elements were in “good shape” at the time the snapshot was taken). And if we average the scores for all ENRUST customers, we get an overall indicator of how good a job ENRUST is doing caring for our customers’ systems.

So, now how do we assign some dollars to that Proactive Score? This is actually very difficult. But one piece of information we have available to us is the cost of malware. Please examine the below table.
So, this table shows that an organization’s typical risk exposure to the cost of malware is about .68% of revenue (Cost of malware divided by the size of the worldwide economy = risk exposure.). So the same $36M sample company used in the cost of downtime illustration would expect to have an exposure to malware costs of $244,800 per year.

A company that is “doing things right” should be able to reduce that exposure better than companies doing a poorer job.

Now, ENTRUST does not regularly have insight into the practices of our competitors. But occasionally we do get an opportunity when “taking over” a customer from a competitor (or from a completely non-managed environment). And we have taken those opportunities to assess those new customers against the ENTRUST standard Proactive Scoring system. Here is a summary of what we have found:

<table>
<thead>
<tr>
<th>Economic Statistics</th>
<th>Dollar Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of Worldwide Economy</td>
<td>$71.83 trillion dollars</td>
</tr>
<tr>
<td>(2012, source CIA World Factbook)</td>
<td></td>
</tr>
<tr>
<td>Cost of malware and data breaches in 2014</td>
<td>$491 billion dollars</td>
</tr>
<tr>
<td>(source, study by IDC and Nat’l Univ of Singapore, Mar 2014)</td>
<td></td>
</tr>
<tr>
<td>Typical Risk Exposure</td>
<td>.68%</td>
</tr>
</tbody>
</table>

So, this table shows that an organization’s typical risk exposure to the cost of malware is about .68% of revenue (Cost of malware divided by the size of the worldwide economy = risk exposure.). So the same $36M sample company used in the cost of downtime illustration would expect to have an exposure to malware costs of $244,800 per year.

A company that is “doing things right” should be able to reduce that exposure better than companies doing a poorer job.

Now, ENTRUST does not regularly have insight into the practices of our competitors. But occasionally we do get an opportunity when “taking over” a customer from a competitor (or from a completely non-managed environment). And we have taken those opportunities to assess those new customers against the ENTRUST standard Proactive Scoring system. Here is a summary of what we have found:
NOTE: An “unmanaged” network does not mean a network that is wholly unprotected or defenseless! A firm may deploy a firewall and/or antimalware software and may setup updates to “automatically install” and then essentially leave those tools in a “set it and forget it” state most of the time. That is our definition of an unmanaged network. “Poor”, “better”, and “best” competitors simply represent our measurement of the state of some networks for which we have assumed responsibility from a competitor.

You can see that ENTRUST’s typical Proactive Score is 24% higher than an unmanaged network, 22% higher than a network managed poorly by a competitor, 18% higher than a “better” competitor, and even 11% higher than the best competitor we have had a chance to measure. So let’s apply those values against our sample $36M company and just the one element of malware exposure.

If we assume the sample company was at risk each year for the average malware cost of $244,800, then using the values from the above table we can compute the ENTRUST advantage from “doing things right”.

<table>
<thead>
<tr>
<th>Sample Company Revenue</th>
<th>$36,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware/Security Breach Exposure</td>
<td>0.68%</td>
</tr>
<tr>
<td>Dollar Cost of Malware/Security Exposure</td>
<td>$244,800</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ENTRUST Advantage over Various Competitors</th>
<th>Monthly ENTRUST Advantage</th>
<th>Annual ENTRUST Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTRUST Advantage over Unmanaged</td>
<td>$4,896.00</td>
<td>$58,752</td>
</tr>
<tr>
<td>ENTRUST Advantage of Poor Management</td>
<td>$4,488.00</td>
<td>$53,856</td>
</tr>
<tr>
<td>ENTRUST Advantage over Better Mgmt</td>
<td>$3,672.00</td>
<td>$44,064</td>
</tr>
<tr>
<td>ENTRUST Advantage over Best Competitor</td>
<td>$2,244.00</td>
<td>$26,928</td>
</tr>
</tbody>
</table>

Remember that the dollar values shown in the table include only the benefit of ENTRUST management for malware exposure. Improved productivity is not counted.

If you combine the benefit of increased uptime from 99% to 99.9% with the benefit of improved proactive care for the sample $36M/yr. company, if currently operating in an “unmanaged” and purely “reactive” mode, you find that “doing things right” could potentially result in:

Cost savings of $220,752 per year
So, assuming that ENTRUST and “some other competitor” are charging roughly the same price, clearly there is a very significant dollar value to doing business with a company like ENTRUST that “does things right”. Even compared to a “best” competitor “doing things right” represents almost $27,000 of savings for proactive care alone and only if the competitor charges the same price as ENTRUST.

**TWO MORE THINGS:** Normally we close with “One More Thing” but this month we have two final messages:

1. Remember that this whitepaper addressed only the dollar value of increased uptime and reduced malware risk. A future sequel may endeavor to put a dollar value on improved performance derived from better management. Until then, please feel free to explore our website for other useful information.
2. Remember also that “doing things right” does not mean “doing things perfect”. ENTRUST cannot claim to always be perfect at caring for machines, preventing issues, or resolving issues. But we can promise that we always strive to better – better than the competition and better than we were “yesterday”.

Learn more at: [www.entrust.us.com](http://www.entrust.us.com)

Contact us at: [info@entrust.us.com](mailto:info@entrust.us.com)

Call us at: 866-863-4738