SPC®

TECHNOLOGY CASE STUDY

Total cost of ownership:
SPC upgraded a 5 year- old unit that had 11 server instances @ $125 per server per month or $1375 a month to manage them. We replaced it with upgraded technology for $10,000 that reduced them to go to 6 server instances @ $125 per server per month or $750 a month. The server was already past its life expectancy so who knows how long it would have lasted before it needed to be replaced but let's look at a 3-year example.

Old Technology: $1375 x12 = $16,500 per year x 3 years = $49,500

New Technology: $750 x12 = $10,000 + ($9000 per year x 3 years) = $37,000 for a total savings of **$12,500!** Not including 2 more years of server life.

Preventing unnecessary breaches:
A client, let's call them Sleepy Bank. They have a network of 20 workstations in two branches, an Exchange server, a Core server and a separate dedicated server that runs their website, all connected via broadband. The whole thing is a relatively small network, and no one in the company was Cybersecurity IT trained but one person was wearing an administrator hat. Their business was focused on providing bank services to their local customer database.
Last year, Sleepy bank found out that their webserver was compromised. Suddenly all kinds of much higher traffic was going to countries they did not do any business with. Turned out their server was hosting an illegal music download service. We went over and had a look, and sure enough the logs showed what was going on. Turns out that one of the workstations was infected with nasty malware after the user clicked on a phishing email, and from there the hackers penetrated the whole network. Some of the workstations and all servers were compromised. The bad guys completely owned the network. So here was what was needed to disinfect the network, and these are only the headlines:
Select, order, configure and install a good quality firewall – 10 hrs
Build a new webserver from scratch, load with their backups, and bring it near-line -20 hrs
Scanning workstations and servers with several anti-malware tools -25 hrs
Wipe and rebuild Windows on all workstations to make sure no rootkits were left – 15 hrs
Install high-quality anti-malware software on all servers and workstations – 10 hrs
Bring new webserver online and debug initial problems – 10 hrs
Debug various things that broke during rebuild, bring printers back online, install drivers, 20 hrs

The whole thing took 110 billable hour
s (and then some non-billable!) to completely repair all the damage. The normal rates of $90 we charged made this cost $9,900 for just that one network breach.
But now add the cost of downtime. Their main source of income generating webserver was off-line for a whole day, at a cost of about $6,600 of lost revenue.
Their employees each lost at least one working day of time over that week, due to this incident, so that is 20 man-days at an average of $120 per day, for a total productivity loss of $2,400.

So the Direct loss of productivity and revenue was $18,900 consisting of:
Repair cost by outside consultants: $9,900
Lost revenues: $6,600
Lost production time of 20 employees for one day: $2,400

Banks Reputation:
Let's assume the real possibility that an organization faces a 50% chance that an outside hacker will compromise one of your users' passwords causing a security breach. This is the probability of the negative event. Ransomware has exploded on the scene. Fully 98 percent of the organizations surveyed by Ponemon experienced a virus or malware-based network intrusion, and 35 percent said they had experienced 50 malware attempts within a span of just one month, or more than one intrusion per day.
The total cost of the incident for Small and Medium Enterprise is estimated to be an average $150,000 based on recent data. Note, this is a conservative number, the total cost can be much higher.
Therefore: Current annualized loss expectancy without SAT = (.5)($150,000) = $75,000