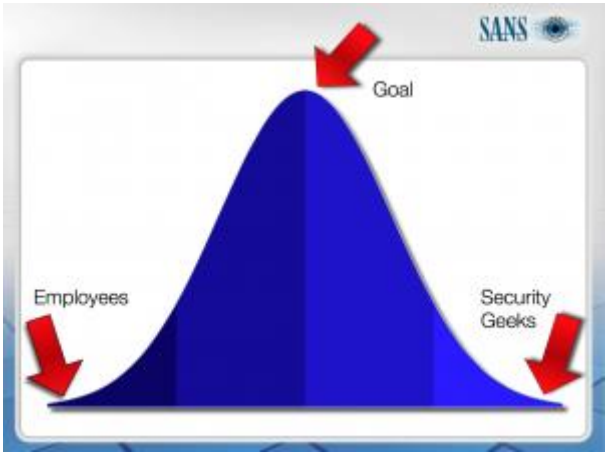
The Return on Investment (ROI) of Security Awareness Training

Now that cybercrime is in its fifth generation, prevent a security nightmare from happening on your watch.

With effective security awareness training, you now can train employees to better manage the urgent IT security problems of social engineering, spear phishing and ransomware attacks.



Today, reducing the Phish-prone percentage of your employees through awareness training is likely the most cost-effective network protection measure you can take. Two common goals of security awareness training are *risk reduction* and *compliance*. Risk reduction is the most important one, and has by far the biggest Security ROI. But what does it mean to reduce risk, and what is good enough? Remember, no technology nor any solution can eliminate risk, we can only reduce it. To be secure means you have an acceptable level of risk related to the threats you are facing. The SANS diagram above shows the optimum budget sweet spot in security awareness training.

The SANS 'Securing The Human' blog put it this way: *"The X axis represents the amount of effort you put in securing end users. The more time, resources and effort you invest the more security aware they are. On the far left is where most employees are today, totally unaware and insecure. This is not because they are stupid, this is because no one has taken the time to train them. On the far right is the security community, highly trained and aware. The Y axis measures your organization's return on investment. There is a sweet spot where you get the greatest return. Invest too little effort and your employees are still low hanging fruit (where most organizations are today). Invest too much and you are entering overkill. For some reason some people expect security awareness programs to turn end users into security experts. This is ridiculous. The goal is 'good enough'. The challenge with security awareness is determining what that 'good enough' is, where you get the greatest ROI. That is different for every organization."*

Definition of ROI:

The comparison between any expected improvement and the cost required to achieve that improvement. In security, this is not measured as a concrete gain, but as we said above, as a reduction in risk. The ROI for Security Awareness Training (SAT) can be broken down in three main components, which you can use all together or independently depending on your current requirements:

Development Cost.

How many man-hours are/would be needed to do SAT in-house?

Direct loss of productivity and revenue.

Employee downtime and IT staff man-hours to disinfect workstations and/or restoring from backups in case of data theft/Loss or ransomware encryption, and website e-commerce downtime caused by a security incident. Revenue loss per minute, per hour, or per day can be significant.

Loss of reputation.

How would your CEO feel reading about a data breach on the front page of his/her morning newspaper? Just think about the direct and indirect cost of having to deal with a security incident: customers, suppliers, and stakeholders. Difficult to quantify but significant.

ROI Methods:

Payback is by far the most common method, and that is the one we will use here. More advanced organizations might want to do a Net Present Value (NPV) calculation but we will not cover that here. So, let's have a look at the three areas listed above and start with the first one

Development Cost

How many in-house man-hours does it take to first research, then write, design and deliver a consistent security awareness program that includes sending regular simulated phishing attacks to all employees, with tracking and reporting of 'pass/fail' per employee for an organization with 200 staff? Well, experience shows that takes at least 5 hours a week for someone who knows what they are doing.

Total man-hours per year required to create/ deliver each month (12mos. x 20 man-hours)	= 240 man-hours
240 man-hours @ $100 per hr. (Sal. & Benefits)	= $24,000
Annual 200-seat subscription cost (Example)	= $3,000
Managed Services for 12 Months	= $1,600
Total Cost Savings:	**= $19,400**

Direct loss of productivity and revenue.

Most non-IT executives have little experience with the amount of time it takes to disinfect a workstation, or worse, a whole network or encrypted file server. However, once you have been hit with an attack, you never want to experience that again. To illustrate this, let me tell you a story which will illustrate what direct damages to expect:

A Real Life Example

In an earlier company I had a client, let's call them Acme, Inc. They have a small network of 20 workstations, an Exchange server, a SQL 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 IT trained, one person was wearing a (very) part time administrator hat. Their business was focused on providing a subscription to their specialized designer customer database.

Last year, Acme 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 all workstations and servers with several anti-malware tools, we rootkits -25 hrs
- Wipe and rebuild Windows on all workstations to make sure no rootkits were left – 15 hrs
- Install and configure 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 this rebuild, bring printers back online, install drivers, etc – 20 hrs
- The whole thing took 110 billable hours (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.

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: $2,400

And all that because one employee clicked on a phishing link and got infected with the Zeus malware. You can now calculate the cost of doing the whole disinfection with in-house IT staff as well, and the number might be a bit lower, but not by much.

Loss of reputation.

Here is a payback example calculation for a general security incident causing lost reputation. The one problem here is the fixed idea: *"Oh, that will not happen to us."* Well, it doesn't, until it does. Small and medium enterprise has a target on its back, and eastern European cyber criminals are not discriminating. Everyone is at risk. They don't care if you have 20 users or 2,000. They just see an IP address with a vulnerability they can exploit.

Let's assume the real possibility that your organization faces a 50% chance that an outside hacker will compromise one of your users' passwords in the coming year, causing a security breach. This is the probability of the negative event. The malware problem is getting worse. 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.

If your organization does suffer a successful data breach, 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

Your organization is considering a Security Awareness Training (SAT) program to help reduce the risk of social engineering, spear phishing, ransomware attacks or a full-fledged cyberheist. Test results show that our SAT program will reduce the chance of an employee falling for a phishing attack climbs up into the 98%+ range over time, but again we will use a conservative estimate of 80% here. So the annualized loss expectancy goes from 50% down to 20% due to the training.

Therefore:

Annualized loss expectancy with SAT implemented = (.2)($150,000) = $30,000

The $150,000 cost of the negative event, if it occurs, did not change. The probability of it occurring did!!

To find expected savings, just take the difference: $75,000 – $30,000 = $45,000

On average, your organization will save $45,000 per year if it implements the SAT program.

This expected savings must be compared against the cost of a managed training program to determine ROI. The managed program for 200 employees is $4,600, so your ROI is positive in the extreme! Many of our customers tell us that this is by far the best bang they got for their security budget dollars.

Contact us today about a complete security awareness program for your organization