White Paper

The Business Case for Security Penetration Testing

Let's start with a simple example. Penetration testing is similar to a health physical. You may not know if anything is wrong until you go to the doctor's office and have him examine you. You hope the doctor doesn't find anything wrong, but that's why you go and get a check-up. If there is something wrong with you and you need extensive tests or procedures done, you will have just realised the ROI on your health insurance. If you get a clean bill of health you may wonder why you carry health insurance, but peace of mind outweighs your concerns about money. Carrying health insurance is an easy cost to justify. Security spending in the form of a penetration test is a little more difficult to justify, but it can be done.

In a tight spending market, CIOs are only going to spend money on something that can demonstrate a return on investment, which includes demonstrating the tangibles in the form of a Payback Period (breakeven point), Net Present Value (NPV), and the Internal Rate of Return (IRR). The intangibles, such as the loss of reputation from a well-publicised security breach, can be difficult to calculate. The intangibles are just as critical as the tangibles; however, a balance of hard numbers and soft numbers needs to be achieved in order to demonstrate a comprehensive ROI.

Demonstrating Return on Investment (ROI) is critical to the success of selling a security product or service, and that includes selling the need for a penetration test. Security professionals and security departments within larger organisations are realising that demonstrating ROI on security is sometimes a complicated and confusing process. You can't go to the decision makers and say, "We need to spend x number of dollars on penetration testing or someone is going to hack us".

You need to demonstrate a business case justification for the expenditure, and that expenditure needs to contribute to the bottom line: profitability. Companies should not spend money without proof of benefit. That benefit needs to be in the form of increased revenue, greater cost savings or significant productivity gains. Executive management will expect you to quantify and qualify the "what and why" for penetration testing and any other security related initiative.

Ounce of prevention

Generally speaking, security measures have been viewed as a necessary evil to prevent unknown disastrous events from occurring. As organisations become more educated and aware of their responsibilities in securing the environment, due to legislation or well publicised events, they are also becoming savvier in their decision-making processes. As organisations begin to get serious about security and start actually budgeting for IT

security products and services they are demanding tried and true methods for evaluating and justifying the expenditure.

Internal security management and staff are struggling with the same issues that external security vendors are struggling with. How do you demonstrate security ROI? It matters not whether you are attempting to justify expenditure for an upgraded firewall solution, IDS (Intrusion Detection System), additional staff, consulting services, or a penetration test. The issue is the same.

If you look only at the costs, there is no revenue attached to the IT side of the organisation. Most of us are familiar with the acronym TCO (Total Cost of Ownership). Companies have been focused on lowering TCO in regard to infrastructure initiatives. While cost control is important, understanding business value is far more important. The business value of IT initiatives are beginning to be understood in terms of user productivity, revenue per employee, business cost reduction, cycle time improvements and risk reduction.

Security is viewed similarly to IT and is associated with risk management. Risk management is a process whose goal is to provide the best possible protection for information systems and the storage, processing and transmission of information assets at the lowest possible cost consistent with the value of the asset.

How can a process such as risk management provide a return on investment? Risk management can be associated with business value. If the value of the information asset is high, risk management needs are high. If the value of the information asset is low, risk management needs are low. The security professional needs to understand information asset valuation methods.

The problem is not just simply a matter of coming up with formulas, methods, and models. The problem is that until you can directly correlate the security product or service (e.g. penetration testing) with business value, you cannot demonstrate a return on the investment. CIOs want to see hard numbers. In these hard times, the fear, uncertainty, and doubt are no longer a good enough excuse for implementing security measures. The new attitude is ***"Show me the money".***

What is ROI?

Return on Investment (ROI) over-simplified means that if you spend $100K on something, you want to know that in a certain period of time the money you spent is going to return something to you. You want to know how long that is going to take and what the percentage of return is. There are financial terms that need to be understood in order to perform an ROI calculation.

Return on Investment (ROI) is the ratio of the net gain from a proposed project, divided by its total costs. Payback Period is the time frame it takes for the project to yield a positive cumulative cash flow. Net Present Value (NPV) is a measure of the net benefit of a project, in today's dollar terms.

Internal Rate of Return (IRR) is the discount rate necessary to drive the NPV to zero; the value another investment would need to generate in order to be equivalent to the cash flows of the investment being considered. The usual ROI calculations are not readily applied to security initiatives, such as penetration test. Technically speaking, there is no return on investment for a preventative method other than to claim that "an ounce of prevention is worth a pound of cure." However, if you align the penetration test with a compliance programme or revenue-generating project that requires it, the test can be seen as a necessary step in order to meet the goals of the wider project.

What's the purpose of a penetration test?

The purpose of a conducting a security penetration test is to discover and expose vulnerabilities in an organisation's security systems. In calculating the ROI, you have to compare the security investment to the potential damage prevented. You will need to have a good understanding of the company's information assets and how those assets relate to business value.

You must be prepared to spend time understanding the business side of the organisation and walk executives through the valuation of information assets as they relate to business value. You must further be prepared to compare the cost of the loss of that asset with the cost of preventing the loss.

The results of a penetration test are the knowledge of potential risk, vulnerabilities or threats to ***Information Assets (IA)*** and the information needed to mitigate those risks.

For organisations who have already been through the process of valuing their IA, it is a much simpler matter to point to a particular asset (such as a customer database), discuss in financial terms what that asset is worth, and then help management think about the impact of the loss of that database.

Consequently, it is extremely beneficial to discuss with the decision makers in financial terms (ROI, Payback/Breakeven, NPV, and IRR) what the business value of the database is.

For instance, if your organisation has made a large investment in converting a legacy mainframe system to an ERP system (e.g. SAP, Oracle, PeopleSoft), they have already done the ROI calculations, estimated the Payback period, and hopefully understand the

Net Present Value/Internal Rate of Return for that implementation. If the database is compromised and goes offline, what happens to the payback period?

Specialist ‘cyber liability’ insurance is beginning to emerge in some countries. In order to qualify for the insurance, an organisation has to comply with particular security processes and have certain safeguards in place.

At some point it is expected that this type of insurance will become more mainstream. In the meantime, it is important for security professionals to understand how Business views and justifies expenditure. It is just as important for the security professional to teach business to think in terms of information asset valuation and correlate that to the financial risk to the company.

Example Business Benefits

• Provides both general and specific information about risks and controls

• Assists in creating a strong security culture

• Improves the effectiveness and consistency of existing controls

• Can stimulate the adoption of additional cost-effective controls

• Helps reduce the number and extent of information security breaches

Overall cost of a company's worst incident in the last year

Direct Costs of a Security Incident	Overall	Large Businesses (10,000+ employees)
Loss of assets, regulatory fines etc.	e.g. DPA £5k max fine for a conviction in the Magistrates Court and unlimited fines for convictions in the Crown Court	e.g. DPA £5k max fine for a conviction in the Magistrates Court and unlimited fines for convictions in the Crown Court

Indirect Costs of a Security Incident	Overall	Large Businesses
Business Disruption	£6,000 - £12,000 over 1- 2 days	£50,000 - £150,000 over 1- 2 days
Time spent responding to incident	£600 - £1,200 2- 4 man- days	£1,75- - £3,500 5 - 10 man- days
Direct cash spent responding to incident	£1,000 - £2,000	£3,500 - £5,000
Direct financial loss (e.g. loss of assets, fines etc.)	£500 - £1,000	£3,500 - £5,000
Damage to Reputation	£100 - £400	£5,000 - £10,000
Total cost of worst incident	£8,000 - £17,000	£65,000 - £130,000

Source: From DTI & PwC Information Security Breaches Survey 2010

Example technical benefits

Features	Benefits
Perimeter security management	Enables access control of local networks
Network intrusion prevention	Removal of attack opportunities
Limits access to servers	Promotes business resilience
Decreases downtime resulting from attacks	Reduces maintenance and network operation costs

Hope that helps. If you have any questions don’t hesitate to contact us at 0800 978 8139 or send us an enquiry via our contact form.