UNDERSTANING HOW TO CALCULATE THE ROI FOR CONDUCTING SECURITY PENETRATION TESTING

To successfully secure buy-in from stakeholders on any security project, you'll need to not only demonstrate the need but the Return on Investment (ROI). This can be challenging for any security professional.

Let's Start with a Simple Example

Penetration testing is like 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 even carry health insurance, but peace of mind will outweigh any concerns about the money spent on verification. 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.

Below are retention techniques you can use in your staff awareness programme that will ensure content is not just learned but helps instil a culture.

Intangible Business Benefits

Showing ROI is critical to "selling the need for a penetration test" to your organisation. But risk management professionals are realising that demonstrating ROI is a complicated and confusing process at best. You can't go to the decision makers and say, "We need to spend X on penetration testing, or someone is going to breach our systems".

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 cyber risk management related initiative.

The problem is that intangibles, such as the loss of reputation from a publicised security breach, can be difficult to calculate. These intangibles are just as critical as the tangibles and therefore a balance of hard numbers and soft numbers needs to be achieved in order to demonstrate a practical and meaningful ROI for security penetration testing.

Since the objective of conducting security penetration testing is to identify (and remediate) system security vulnerabilities which if exploited would result in a breach, let's start with commonly known and accepted losses associated with a typical data breach. Data breaches impacting UK organisations in the past year inflicted losses of up to *£185,000 to them on average. This number is comprised of the average of associated legal, technical, regulatory and costs incurred due to loss of brand equity, customers, and employee productivity.

Prevention is Understood but ROI Needs to be Shown

Cyber security measures such as conducting routine security penetration testing are now commonly understood as standard controls to prevent breaches. As organisations become more educated and aware of their responsibilities in securing their systems, due to best practices established in legislation, regulation and standards, they are also becoming savvier in their decision-making processes. As organisations begin to get serious about security and start budgeting for cyber security controls, they are demanding tried and true methods for evaluating and justifying the expenditure.

Internal security management and staff struggle with the same issues that external security vendors are struggling with. How do you demonstrate ROI? It doesn't matter if 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). Businesses have been focused on lowering TCO regarding infrastructure initiatives. Whilst cost control is important, understanding business value is far more important. The business value of IT initiatives is beginning to be understood in terms of user productivity, revenue per employee, business cost reduction, cycle time improvements and risk reduction.

Cyber 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. Fear, uncertainty, and doubt are no longer a good enough excuse for implementing security measures. The Board's expectation is "Show me the money".

What is ROI?

ROI is a common metric used to calculate the expected return on an investment (spend). Before any significant investment is made businesses calculate the expected return on that investment

to justify that spend. It provides an answer to: "What do we gain by making this investment? While many formulas exist to help calculate the rate of return on investments accurately, ROI is lauded and still widely used due to its simplicity and broad usage as a quick-and-dirty method. The basic formula for ROI is:

$$\frac{\text{Gain from Investment - Cost of Investment}}{\text{Cost of Investment}}$$

As a simple example, Company A wants to calculate the ROI on conducting a security penetration test on their systems. They invest £25,000 on the cost of a test, and in doing so significantly reduced the risk of a breach with associated breach costs commonly acknowledged at £185,000.00 per breach.

$$\frac{\text{£185,000 - £25,000}}{\text{£25,000}} = 638\%$$

Company A's ROI on the penetration test then is 638% (or £160,000.00)

What's the Purpose of a Penetration Test?

The purpose of conducting a security penetration test is to discover and expose vulnerabilities in an organisation's security systems in order to prevent a breach. In calculating the ROI then, you must compare the cost of the test to the potential damage prevented (gain from conducting the test). To do so you obviously 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 businesses 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. This data should come directly from your information security risk treatment plan with asset values and associated loss calculations established by the business stakeholders.

Benefits from conduct security penetration testing are commonly understood to include:

- Identifying security vulnerabilities conductive to a breach for remediation
- Validation of security key performance indicators against risk objectives
- Verification of the effectiveness of existing security controls in scope
- Enhancing the security profile and culture of the business
- Increases business system resiliency
- Reduces system downtime
- Reducing the risk of a breach

Difficulties in Calculating Testing ROI?

It is true that ROI as a metric can be utilised to gauge the profitability of almost anything, but its universal applicability is also the reason why it tends to be difficult to use properly. While the ROI formula itself may be simple, the real problem comes from people not understanding how to arrive at the correct definition for 'cost' and/or 'gain', or the variability involved.

For instance, conducting security penetration testing does not prevent a breach. Good cyber risk management practice entails implementing security controls in people, process and technology. At best then, conducting security penetration testing and remediating the vulnerabilities identified, reduces the risk of a breach associated with technology.

Determining Financial Gain

It's important to put testing into perspective when calculating its ROI. It is essentially an investment made to address the effectiveness of 1/3 of your overall cyber security objectives. The purpose of conducting a security penetration test is solely to verify the security integrity of your systems and not the security controls you have implemented into your people and processes in order to prevent a breach.

Consequently, when determining a financial gain on your investment this needs to be carefully considered. The average cost of a cyber breach is £185,000.00 in the U.K. – perhaps a more realistic amount to use as a potential gain on the investment is 1/3 of this figure or £75,000.00.

To use our previous example, Company A calculates the ROI on conducting a security penetration test on their systems at a cost of £25,000 and in doing so uses an expected gain on investment set at one-third the average cost of a breach of £185,000.00 (or £61,700.00):

$$\frac{£61{,}700 - £25{,}000}{£25{,}000} = 146\%$$

Company A's ROI on the penetration test then is now 146% (or £75,000.00)
Another nuance with calculating ROI is that there should always be a timeframe involved. For

instance, a business trying to decide on purchasing a new firewall with an ROI of 200% or a penetration test with an ROI of 100%. Right off the bat, the new firewall seems like the no brainer, but is it true if the ROI is calculated over the product life of 5 years for the firewall as opposed to the test's ROI calculated over 1 year? Therefore, ROI does its job well as a base for evaluating investments, but it is essential to supplement it further with measurements over a time period.

Annualised ROI

The Risk Crew ROI Calculator includes an Investment Time input to hurdle this weakness by using something called the annualised ROI, which is a rate normally more meaningful for comparison. When comparing the results of two calculations computed with the calculator, oftentimes, the annualised ROI figure is more useful than the ROI figure; the firewall versus test comparison above is a good example of why.

In real life, the investment risk and other situations are not reflected in the ROI rate, so even though higher annualised ROI is preferred, it is not uncommon to see lower ROI investments are favoured for their lower risk or other favourable conditions.

The Bottom Line

Let's face it. Calculating testing ROI is not always straightforward. But with careful considerations to all the associated variables the classic ROI calculation method can be very effective in identifying an expected return to the business for the costs of conducting security penetration testing. The more you work with the model, the more effective it becomes.

Endnotes:
*Hiscox, "Hiscox Cyber Readiness Report 2019", April 2019,
https: //www.hiscox.co.uk/cyberreadiness

Let our experts help you stay ahead of the CYBER THREAT LANDSCAPE.

Shelter from the Storm

Contact us for more information

5 Maltings Place
169 Tower Bridge Road
London SE1 3JB
United Kingdom

information@riskcrew.com
+44 (0) 20 3653 1234
riskcrew.com