Security Training – Why It Benefits Your Organization and How to Make Your Case to Management

Author:

Nick Murison
Senior Security Consultant
Foundstone Professional Services
Introduction

A major challenge within Information Security – and IT in general – is the pace at which technologies, threats and attacks develop. A few years ago, WEP was considered a perfectly adequate security mechanism for wireless networks by some. Today, networks protected with WEP are compromised within minutes. In a corporate environment, relying on outdated information about threats and vulnerabilities can lead to companies being blindsided by attackers. Conversely, the technologies available to protect critical assets are constantly evolving, to provide a higher level of assurance and protection against attackers. Making sure your company is prepared for these changes does not just require investment in technology and processes, but also in people.

The current economic climate makes it tempting for many companies to cut their training budgets, and limit the amount of long term investment that is made in its staff. We believe a better idea is to take advantage of the added downtime of employees to provide them with the skills that can accelerate the organization’s success.

This whitepaper explores the reasons why you should invest in Information Security training, and how to present a case to company management.

How Your Organization Benefits From Training its Employees

Having highly skilled employees who are given the potential to grow their expertise is a great benefit to any organization. An organization’s success can often be directly attributed to the skills and expertise of its individual employees, and these benefits should not be overlooked.

Many companies spend a great deal of money on third party consultants to cover essential business tasks within the organization. Such tasks could include periodic network vulnerability scans, developing security policies, or many others. Being able to provide these types of services internally in the organization could be a great benefit, and the cost of sending employees to the requisite training may prove to be decidedly cheaper in the long run.

Of course, there are times when outside consultants and vendors are always required, such as when external audits are required for compliance reasons, but garnering internal expertise can be very valuable to the
organization. Identifying and mitigating security weaknesses in your systems, instead of having an external auditor identify them during a compliance audit, can save your organization from haphazardly creating a fix to meet minimal compliance requirements.

As an example, consider Foundstone’s Building Secure Software course. This course provides developers and system architects the requisite knowledge to secure their Software Development Lifecycle. The class teaches students about many of the common vulnerabilities, and provides both tactical and strategic guidance on how to avoid developing insecure software. Topics include common weaknesses, remediation for common weaknesses, and how to introduce security into the Software Development Lifecycle through techniques such as Threat Modeling.

Without the expertise learned through Building Secure Software, companies will often find themselves in an endless spiral of developing insecure solutions, and having to spend a vast amount of resources on re-engineering the software when insecurities are discovered later on. With the knowledge that employees gain from attending Building Secure Software, a company can strategically build security in as part of its Software Development Lifecycle and avoid major vulnerabilities. This will save a lot of time, effort, and money when the company undergoes third party security audits of the software.

In addition to the actual knowledge acquired during the course, a company should also consider the value added by networking with other students attending the class who may have experiences to share, as well as the continued contact with the course instructor after the class is finished. Foundstone instructors make a point to keep in touch with their students from previous classes, and are open to answering questions weeks, months, or years after the class is over. As an example, Foundstone now invites students to join the Foundstone Training Alumni group on LinkedIn to enable easy access to the instructors from past classes.

Another aspect that management should consider is job satisfaction. Management may be worried that investing in training for employees will be wasted if it provides the individual with a stepping stone to pursue career opportunities outside the company. On the contrary, research by organizations such as the American Society for Training and Development and the Council on Competitiveness indicate a correlation between

---

1 If you’ve attended a Foundstone class in the past and wish to be added to the group, e-mail training@foundstone.com with details of which class you attended.

investment in training, employee happiness and profits. Although it is tempting to cut back costs on items that do not directly provide a profit, such as training, investing more in training has shown to provide employees with a better sense of worth, and consequently higher productivity.

Identifying how the short term investment (paying for the class) will yield a significant long term Return on Investment (less reliance on third parties) should prove attractive to any organization.

**How Employees Benefit From Training**

As stated in the introduction, technology moves fast. It is both in the interest of a company, and the individual employee to stay on top of trends. For a company, it is an essential business strategy to stay on top of any threats to its assets. For the individual employee, knowledge development should not stop when one leaves High School or College; continued training benefits both your organization and your own career.

The individual can enjoy benefits beyond just the knowledge they learn from the course; job security, pay raises, and promotions may all be benefits of obtaining and applying new knowledge. A temptation for management may be to think that such knowledge is easy to acquire through potentially cheaper mediums, such as technical books or online training services. Although these are cheaper options, they do not provide all the same benefits. Interfacing with the instructor and other students, experiencing hands-on labs and exercises, and building relationships that can later be employed when further expertise is needed are important aspects to “real-world” class environments that cannot be replicated easily through reading a book.

An IT professional’s role within their organization almost always includes specialization. A Microsoft .NET developer is a far more valuable asset to an organization if they’ve undergone specialized training in Microsoft .NET, and can produce code that leverages the underlying framework. Acquiring specialized skills does not just help the organization develop intelligent solutions, but also helps the individual in their career development.

Based on the above, it makes sense for organizations to keep their employees up to date on the latest technologies, and to provide appropriate specialization training for each employee. It also makes sense to the individual employee.
How to Convince Management to Send You to Training

For many, having a company pay for their training seems like a no-brainer. A company who pays for employees to be trained reaps the benefits of the employees’ knowledge. However, management have many aspects they need to consider, and when budgets are tight, training is often overlooked. It is therefore important to be able to communicate the Return on Investment that your company can achieve by paying for employee training costs.

Making a convincing argument for attending a technical training class can require a fair amount of planning, and should be structured to present the benefits to the company, as opposed to the individual employee.

Start by finding the class you wish to attend. There are many different technical training classes out there, provided by many different companies. You should identify a class that matches with your current role within the company. For example, there is little point in trying to convince management they should send you to a Foundstone’s “Ultimate Hacking: Wireless” class if you’re a developer. Instead, classes that relate to your current development language will make much more sense (e.g. Foundstone’s “Writing Secure Code: ASP.NET (C#)” class). Of course, if you’re transitioning into a new role in the company, it makes perfect sense to attend a class that will give you a solid grounding in your new field.

Once you have identified the class you wish to attend, try to get an understanding for what will be covered by the class. This will help you present to management what benefits they can expect to reap. Many companies will provide class outlines for your review before you register; Foundstone’s website contains detailed course descriptions and even a syllabus for each of their classes\(^3\). Printing these out and presenting them to management will give them a better understanding of what they’re being asked to pay for.

If you’ve been fortunate enough to have been sent to training classes by your employer already, think about what Return on Investment this previous training provided to your organization. Showcasing these benefits when making your case for additional training will help management recognize how investing in training benefits them. This should provide additional incentives to management for maintaining employees’ continuing education.

At the end of the day, training costs your organization money, and the cost will be a main concern for management. Preparing a budget that includes travel, training fees and meals to present to management will not only show them how much the training will cost them, but will also show them how committed you are to improving your ability to help serve the organization.

Included below is a sample e-mail you could use to present your case to your manager. Obviously, you will want to customize it to your particular situation (company and individual names are fictional):

To: manager@acme.com
From: joe@acme.com
Subject: Request for approval for external Information Security Training

Dear Manager,

I would like to request approval to attend Foundstone’s “Ultimate Web Hacking” training course. As a member of the Information Security Team with responsibilities for auditing the security of our externally facing web sites, I believe the specialized knowledge about web application testing contained in the course will be very valuable to Acme, Inc.

As you may remember, several of us from the IS Team attended Foundstone’s “Ultimate Hacking: Expert” class last year. Based on what we learned from this class, we were able to create a new security audit methodology for our internally and externally facing servers. Implementing this new methodology revealed several critical weaknesses in our overall security posture, which we were able to identify and address during our regular audits. I believe the “Ultimate Web Hacking” class will provide us with similar benefits.

You may also remember the costs our organization incurred last fiscal year when undergoing a web application security assessment as part of our requirement to be compliant with the PCI Data Security Standard. The issues identified during the audit resulted in a remediation effort that cost us both time and money. I believe this class will provide us with the expertise to identify and mitigate similar vulnerabilities as part of our internal Software Development Lifecycle. Catching these issues early will save us both money and reputational damage.

For more information about what the course includes, please see the attached course description (also available from http://www.foundstone.com/us/education-coursesdescription-ultimate-web.asp).
The course costs $2995USD, and takes place in Washington, DC. Currently, flights from our location to DC cost $450. Hotels in DC will cost approximately $200 per night. Based on this, I have prepared the following budget:

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course cost</td>
<td>$2995.00</td>
</tr>
<tr>
<td>Flights</td>
<td>$450.00</td>
</tr>
<tr>
<td>Hotel stay (4 nights)</td>
<td>$800.00</td>
</tr>
<tr>
<td>Meals (max $50 per day)</td>
<td>$200.00</td>
</tr>
</tbody>
</table>

---------

Total $4885.00

========

I hope you will consider my request, and recognize the clear benefit that the specialized skills will bring to Acme, Inc’s ongoing effort to improve our security posture.

Many Thanks,
Joe Vilella

Conclusions

Do not underestimate the importance of training in the ongoing drive to improve your organization. When arguing your case to management, make sure you choose an appropriate training class, and that the Return on Investment makes sense to your organization.
About the author

Nick Murison serves as a Professional Services Consultant at Foundstone. He focuses on assessment services, identifying weaknesses in clients’ security postures, and providing strategic advice on how to resolve such issues. Mainly concentrating on web application security assessments, Nick also provides expertise for other technology assessments and penetration tests. In addition to his technical assessment skills, Nick is also involved in assessing organizations’ policies for compliance with regulatory requirements and industry best practices. Nick is also a lead instructor for Foundstone’s Building Secure Software and Ultimate Web Hacking classes.

About Foundstone Professional Services

Foundstone® Professional Services, a division of McAfee. Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company’s professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.