

White Paper

Calculating Return on Investment (ROI) of Devfense For Web Application Security

Table of Contents

| | |
|--|----|
| Calculating Return on Investment (ROI) of Devfense For Web Application Security | |
| Part 1: The ROI of Devfense For Web Application Security | 4 |
| Introduction | 5 |
| A Chronology of Data Breaches | 6 |
| The Security Challenge | 7 |
| Part 2: The Challenge of Measuring ROI For Web Security | 8 |
| Introduction | 9 |
| The Meaning of Numbers | 10 |
| Calculating Web Security ROI & Peace of Mind | 11 |
| Part 3: Data Security Breach Costs | 12 |
| Introduction | 13 |
| Actual Costs of Data Security Breach Incidents | 14 |
| Third Party Cost Estimates from the IT, Insurance and Security Research Industries | 15 |
| Part 4: Risk of a Security Breach | 16 |
| Introduction | 17 |
| Quantifying Risk | 18 |
| Part 5: The Value of Trust | 19 |
| Introduction | 20 |
| Added Value from Web Security | 21 |
| Part 6: The ROI of Devfense For Web Application Security | 22 |

| | |
|--|--------------|
| Introduction | 23 |
| Devfense Features | 24 |
| Devfense ROI | 25 |
| A. Devfense ROI From Reduced IT Costs | 26/27 |
| B. Devfense ROI From Security Breach Cost Avoidance | 28 |
| C. Devfense ROI from Maintaining Online Revenue | 29 |
| D. Devfense ROI From Increased Online Revenue | 30 |
| Conclusion | 31 |
| Works Cited | 32/33 |
| About Pacific Coast Information Systems Ltd. | 34 |
| About Boonbox | 34 |

Part 1

An Overview of Web Application Security Needs

Introduction

“There is no security on this earth. Only opportunity.”

– General Douglas MacArthur

Corporations worldwide have taken advantage of web applications to improve all aspects of their business, from production and administration to sales and marketing.

But the growth of business use of the Internet and associated online infrastructure have made web applications extremely tempting targets for hackers and organized crime. Malicious attackers recognize that companies have limited expertise in developing effective web application security or have neglected addressing associated web application security issues.

Organizations are facing increasing pressure to address web application security to avoid costly security breaches and maintain competitive advantage. But in order to address these issues, organizations must be able to justify the investment through calculating Return On Investment (ROI).

This white paper aims to provide overviews and analysis of the following web application security issues:

1. The need for web application security.
2. The challenge of calculating ROI for web application
3. Recent security breach costs
4. Risk of a security breach
5. Quantifying trust
6. The ROI of Devfense for web application security

This white paper serves as a reference for organizations interested in addressing web application security and for managers who wish to create an ROI analysis for web application security solutions they may be considering, such as Boonbox's Devfense boxed service.

A Chronology of Data Breaches

Website applications are the most vulnerable entry point for security threats today, compared with the network and server layers. Roughly 90 per cent of all IT security attacks are against the web application layer, say Gartner research analysts (Application Development Trends, "Application Security Comes Under Attack").

Web applications are extremely vulnerable, reports Forrester Senior Analyst Michael Gavin. "The entire point of HTTP is to allow two sides to communicate, so if there isn't any application-specific security put into place, there's nothing to stop you from injecting SQL into a Web-based form that's looking for information to go query a database," Gavin notes (Application Development Trends).

The Identity Theft Resource Center reports that of 446 media-reported breaches in 2007, nearly 128 million records were stolen by hackers (ITRC 2007 Data Breach Stats). It is suspected by industry analysts that an extremely large number of security breaches remain unpublicized either due to business' concern about loss of reputation, legal liabilities, or because the breach remains undetected.

Privacy Rights Clearinghouse reports the total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005 is nearly 231 million, a number roughly equivalent to 80 per cent of the entire population of the USA (Privacy Rights Clearinghouse "A Chronology of Data Breaches").

Using cross site scripting, SQL injection, malicious code execution and other tactics, criminals are able to gain access to data on websites and web applications, which can lead them to private information on other databases as well. Hackers are often able to penetrate these applications completely undetected, extracting personal information on thousands or potentially millions of individuals. They are in turn able to use this information to commit identity theft, commit fraud, or sell it to other criminals who will use it for their own ends.

The Security Challenge

Catastrophic security breaches involving the records of millions of people have galvanized the public, political leaders and law enforcement to call for stronger security involving private information. Indeed, dozens of regulatory regimes exist, such as PCI DSS, PIPEDA and FIFFA. Other regulations include SOX for financial fraud protection, the GLB Act (finance regulations), and HIPPA (healthcare regulations). These compliance mandates have been enacted either as best practices or mandatory requirements.

Businesses that continue to neglect web application security not only risk huge losses in the form of legal costs, crisis management costs and rapid after-the-fact security tool deployment. They may also face heavy fines from regulation enforcers, including (but not limited to) local and federal governments, credit card companies and regulatory auditors.

Part 2

The Challenge of Measuring ROI for Web Security

Introduction

Web application security measures are available to businesses wishing to secure their web application layer.

The challenge for CFOs and other executives wishing to invest in such solutions is the unique absence of universally agreed-on industry standards and metrics from web security vendors in calculating typical ROI. This poses a significant difficulty for CFOs and CTOs, as investments in web application security cannot be immune from the best-practices requirement for organizations that must calculate ROI for other kinds of investments.

Following is an overview of the challenges that some IT and security experts believe complicate attempts to calculate ROI for web application security.

The Meaning of Numbers

Renowned security expert Bruce Schneier notes these challenges in a recent interview ("ROI Figures Are Meaningless" ZDNet):

"If you ever see one of those ROI models, what they do is measure the cost of an attack and then multiply by the probability of an attack to give you how much money you should spend. This fails when you have very, very rare and very, very expensive events because you are effectively multiplying zero by infinity.

"If the chance of you being attacked is one in a million and I change it to one in two million ... I have halved the amount of money you should spend... Maybe your reputation is worth US\$20 million, or maybe it is only worth US\$10 million, or maybe it is worth US\$40 million. Suddenly I can completely perturb your budget -- because the numbers are so big and so small that minor changes ... make huge changes to the product."

Industry analysts Greg McLean and Jason Brown seem to have discovered an elegant solution for executives trying to calculate a traditional ROI ("Determining the ROI in IT security" CA Magazine): don't do it that way.

According to McLean and Brown, investing in IT security is like investing in insurance. It's an essential business requirement, yet the ROI is more about peace of mind than paying for improved functionality. The cost is customizable for the needs of individual businesses – indeed, it can be adapted for each individual CEO's level of comfort.

"Security should not be planned around providing a return on your investment dollar in terms of a payback in the administration of the process. It should be planned around providing a level of comfort to senior management that intruders are being kept out of the network, errors and omissions are being kept to an acceptable level of risk, and security will act as an enabler for electronic business, not an inhibitor."

But this still doesn't really provide a satisfactory answer for executives who have to quantify an ROI based on real numbers in order to budget for a web application security product. They at least need to know how much a web application security breach might cost their business, even if those costs and the odds of a breach happening may vary even from quarter to quarter.

Calculating Web Security ROI & Peace of Mind

One way to approach that requirement of hard numbers is to look at the cost of previous security breaches, risk management data provided by insurance companies that work at arm's length from IT vendors and the sales conversion rate increases of websites that consumers believe have been made secure.

In the sixth part of this white paper, "Calculating the ROI of Devfense", we will attempt to analyze the ROI of a web application security solution using more traditional calculations.

But given the kinds of variables involved in an ROI assessment on IT security, we advise one to also consider the specific conditions unique to their organizations that may affect those "hard numbers". As well, we would advise them to ponder a more intangible benefit such as peace of mind.

Peace of mind is a phrase often used in the insurance industry. People who take out insurance do so knowing that the odds of ever needing to make a claim on that insurance may be low. Still, the financial implications of one's house or business suddenly being destroyed in a fire or an earthquake, or of death or disability, can be catastrophic for the uninsured. Hence, investing for peace of mind is seen today as best practice for most, if not all, organizations.

As a web security breach may pose severe and sudden financial consequences far more serious than the loss of a single house or business in a disaster, organizations invest in web application security for peace of mind. Even before we have employed a more formal ROI calculation in this white paper, it is important for organizations to recognize that this peace of mind is important. It allows organization to carry on with their day to day business despite innumerable threats from hackers lurking on the Internet. Indeed, this factor alone may be enough of an incentive to go ahead with a significant investment in web application security.

Part 3

Data Security Breach Costs

Introduction

The first part of calculating an ROI for investing in web application security is to look at actual incidents of security breaches and the consequences to the companies affected. This anecdotal approach is more effective than calculating ROI based on what Schneier describes as “very, very rare and very, very expensive events” that may provide inaccurate results.

In the next section, we will examine the cost of large, well-publicized data breaches at TJX and Designer Shoe Warehouse. We will also show more general metrics of data breach costs as determined by third-party research from IT industry analysts, insurance brokers and law enforcement.

Actual Costs of Data Security Breach Incidents

The following examples of data breach incidents that received widespread media attention may illustrate the potential costs associated with a data security breach.

TJX Security Breach

TJX Companies Incorporated announced on January 17, 2007, that it was the victim of an unauthorized computer security breach. By the end of March 2007, the number of affected customers whose credit card information had been hacked reached 45.7 million (Wired Blog Network, "Data Breach Will Cost TJX \$1.7B, Security Firm Estimates").

Wired Blog Network reported on March 30, 2007, that industry analysts expected the breach to cost TJX \$1.7 billion. The estimate was based on assumptions including \$1.14 billion for customer remediation and an average cost per client record of \$37.

Note that Forrester Research puts the average cost of a data breach at \$90 to \$305 per record (Information Week, "Security Breaches Cost \$90 To \$305 Per Lost Record").

Designer Shoe Warehouse Security Breach

A computer security breach at Designer Shoe Warehouses in March 2005 led to 1.5 million customers with credit cards being exposed to fraud from ID thieves. The company claimed losses related to the breach ranging from \$6.5 million to \$9.5 million (Los Angeles Times, "DSW Settles Data Theft Case").

A settlement of a customer class-action suit mandated a comprehensive security program and DSW agreed to have its systems audited by independent experts every other year for 20 years.

The two incidents above, involving TJX and DSW, vary widely in scale. Comprehensive cost estimates for security breaches in more recent cases like the Hannaford supermarket chain data breach that exposed 4.2 million customers to data fraud are not available at this time.

The costs of data breaches are ongoing, including legal bills and payment for crisis management measures. Ultimately, costs may range into the hundreds of millions of dollars for some companies.

Third Party Cost Estimates from the IT, Insurance and Security Research Industries

Third-party security breach cost estimates from groups like the insurance industry and IT security think tank analysts can also be helpful in calculating the ROI of a web application security solution.

Darwin Professional Underwriters is an insurance company that has collated statistics about the cost of security breaches based on data provided by the Ponemon Institute, a research institute dedicated to advancing responsible information and privacy management practices.

Darwin's Tech//404 Data Loss Cost Calculator indicates the cost of an "average" sized data breach (as calculated by Ponemon) involving 99,000 records would cost between \$9 million and \$14 million. This includes the cost of the internal investigation, notification and after-the-breach compliance with regulatory measures.

IT analysts at Forrester Research indicate that the average security breach can cost a company between \$90 and \$305 per lost record. The research firm surveyed 28 companies that had some type of data breach (Information Week, "Security Breaches Cost \$90 To \$305 Per Lost Record").

The 2007 CSI Computer Crime and Security Survey also provides a "hard-numbers" analysis of the costs of a web security breach. The average annual loss reported in the survey shot up to \$350,424 from \$168,000 the previous year. Not since 2004 have average losses been this high.

Part 4

Risk of a Security Breach

Introduction

Executives seeking to protect their web applications with a solution such as a web audit tool will be interested in knowing the likely risks of a security breach to calculate ROI. As previously pointed out, figures on risk are difficult to calculate, in part because the actual number of data breaches is likely to far outweigh the number of known breaches. However, there are some reports from security specialists, law enforcement and IT industry analysts that provide some clues to the risk factor.

Quantifying Risk

In order to calculate ROI for web application security, it is necessary to look at the chances of data breach risk. The full number of attempted data breaches cannot be known, as a significant number of breaches are presumed to have gone undetected. This makes risk assessment challenging. However, the data below provide some measure of the risks.

The 2007 CSI report provides the following clues as to the risk organizations face that might be included in an ROI analysis. Highlights include:

- When asked generally whether they'd suffered a security incident, 46 percent of respondents said yes.
- Financial fraud overtook virus attacks as the source of the greatest financial losses. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place. If separate categories concerned with the loss of customer and proprietary data are lumped together, however, then that combined category would be the second-worst cause of financial loss. Another significant cause of loss was system penetration by outsiders.
- Almost one-fifth (18 percent) of those respondents who suffered one or more kinds of security incident further said they'd suffered a "targeted attack."

The 2005 FBI Computer Crime Survey augments these figures, reporting that nearly 9 out of 10 organizations experience computer security incidents a year; 20% report experiencing 20 or more attacks.

A 2004 report from Forrester Research cited that over 70% of the value of Fortune 500 companies was attributed solely to their information assets.

The statistics cited above point to an extremely high level of risk for companies facing catastrophic security breaches. Coupled with the dollar cost of security breaches measured in the previous section, web application security risks appear to be ruinously expensive for small businesses and even potentially disastrous for larger organizations.

Part 5

The Value of Trust

Introduction

As noted in previous parts of this white paper on Calculating Return on Investment (ROI) for Web Application Security, a traditional ROI analysis may not provide an accurate and holistic figure that a company should spend on web application security.

Executives must first look to the actual cost of publicized security breaches. Second, they should assess the results of security surveys and risk assessments by IT security analysts, insurance companies and law enforcement agencies.

The third requirement is to calculate a “peace of mind” premium akin to amounts businesses pay for the essential service of insurance.

Organizations should also consider added value from opportunities for competitive advantage enabled by being proactive about web application security. This can be seen in the higher web traffic conversion rates for sales and donations that organizations are able to realize when publicizing web application security efforts with products such as trust seals.

Added Value From Web Security

Companies that are proactive and are able to demonstrate commitment to web application security may benefit from additional online revenue through increased sales or donations.

Companies embed "trust seals" on their websites indicating the web application meets security compliance regulations. Consumers using these sites reportedly tend to feel more confident about engaging in e-commerce on them.

Vendor-supplied data from a range of trust seal suppliers indicates that sales conversion rates typically go up an average of 14 per cent after the seals are embedded, according to IT analyst Dave Taylor (Ask Dave Taylor, "Can Hacker Safe, Truste, BBB, And Trust Guard Seals Actually Improve My Sales"). Indeed, the addition of multiple trust seals on a single page may increase conversion rates by several percentage points.

Clearly, consumers will be more easily persuaded to do business using web applications that are seen to be secure.

This comes with a caveat, however: trust seals have been criticized for giving the appearance of security while still leaving users vulnerable to attacks from hackers and ID thieves (The Register, "McAfee 'Hacker Safe' cert sheds more cred"). Web application hosts will have a very short window of opportunity to prove that their trust seals actually indicate security compliance before consumer non-confidence in trust seals becomes widespread.

Businesses that use trust seals and other methods to advertise their web application security compliance need to do more than being seen to be secure; they must make actual efforts to make their web application secure.

To generate added value, companies must be able to demonstrate to their web application users that they have taken provisions to ensure security. The reputation of an organization hit by a security breach from a supposedly secure site would be challenged. This would correspond to a likely decline in web traffic and use and a reduction in conversion rates by at least the amount previously generated with a "secure" trust seal or similar measure.

Assuming this handled well, companies considering an investment in a web application security tool ought to include the potential benefit of increased sales and profits in their ROI calculation. An example of this calculation will be seen in the final part of this white paper, as we calculate the ROI of the Devfense web application security solution.

Part 6

The ROI of Devfense For Web Application Security

Introduction

In previous parts of this white paper, we have looked at considerations for calculating ROI for web security applications generally. We have looked at the scope of the web security issue, the challenge of using valid numbers in making the ROI calculation, potential costs of a web application security breach, the risks involved, the security benefit of peace of mind, added value of web traffic conversions from trust seals and cost savings in an IT department from using a web security solution.

Now we will look at the specific calculation of benefits and ROI for Devfense, a boxed service web application security solution from Boonbox, a division of Pacific Coast Information Systems Ltd. (PCIS).

Devfense Features

Devfense is a web application security solution offered by Boonbox, a division of PCIS Ltd. We will soon look at how an organization might calculate ROI for Devfense as an example of ROI for web application security generally.

First, let us look at the specific web application security benefits of the Devfense solution.

Devfense boxed service combines best-in-class technology with superior IT security expertise to help organizations achieve improved web application security.

Devfense boxed service identifies known security vulnerabilities on web applications and services. Recommending fix recommendations based on priority, Devfense enables organizations to achieve security and regulatory compliance.

Devfense specific features include:

- Addresses known security vulnerabilities including cross site scripting and SQL injection
- Security coverage for Web 2.0 technologies, including support of Flash, JavaScript, AJAX, JSON and web services
- Maintains an audit trail of security and compliance efforts.
- Provides assessment of compliance to industry regulations (forty compliance regulations are supported) including PIPEDA, GLBA, PCI DSS, HIPPA and SOX

Devfense alleviates the organization's in-house IT staff who may not have the combined expertise of infrastructure, web development, and security expertise. Thus, in addition to the ROI from added value to the website and web security breach avoidance, Devfense allows organizations to receive significant IT cost savings.

Devfense ROI

The Devfense ROI for web application security can be calculated in four ways***:

- A. Devfense ROI From Reduced IT Costs
- B. Devfense ROI From Security Breach Cost Avoidance
- C. Devfense ROI From Increased Web Traffic Conversion
- D. Devfense ROI from Maintaining Secure Web Traffic

*** Note on Devfense Boxed Service Pricing

The ROI of Devfense is calculated in the following sections using a simplified single pricing model for convenience and consistency. In this model, a one-time first purchase of Devfense boxed service is priced at \$4,800, and further quarterly purchases of the boxed service are \$1,200 each.

However, it should be emphasized that Devfense boxed service pricing scales in accordance with an organization's web security needs. Devfense boxed service is an extremely adaptable solution.

For instance, some organizations with large or multiple web applications may require more extensive web application security scanning. Some organizations may require more frequent web assessments. Others may require extensive IT consulting.

Therefore, the price to purchase Devfense will depend on the specific web application security needs of each client. The Devfense boxed service pricing quoted in this white paper should be used only as a guideline.

A. Devfense ROI From Reduced IT Costs

Devfense can reduce IT costs considerably.

Industry analysts suggest that it could take a team of IT security specialists working year-round at a cost of about \$250,000 to manually check for web application code vulnerabilities according to a single set of security compliance regulations. This figure assumes only the cost of salaries for the IT security specialists. Other fixed and variable IT costs will vary widely from organization to organization.

Using traditional methods, we could calculate a simple ROI for Devfense on an annual basis with this single variable of IT cost.

Our calculation assumes an initial investment of approximately \$8,600 for first annual deployment of the Devfense boxed service solution. This also assumes that initial boxed service discovers vulnerabilities. It is reasonable to assume that any unprotected website is vulnerable, given previously-mentioned risk assessments (Part 4: Risk of a Security Breach). Fixing these vulnerabilities could provide immediate ROI.

Based on these simple variables, here is one ROI for Devfense for reduced IT department costs:

$\$250,000$ (manual cost) divided by $\$8,600$ for one year of Devfense boxed service = $\$29$ (value for each dollar spent)

For every dollar spent only on the initial deployment of Devfense, the company receives $\$29$ of value.

Should the client continue using Devfense and requirements remain stable in subsequent years, the ROI is even more impressive:

$\$250,000$ (manual cost) divided by $\$4,800$ for initial Devfense deployment = $\$52$ (value for each dollar spent).

Put another way, Devfense pays for itself in terms of saved IT salaries after a week to 10 days. Clearly, this web application security solution can be extremely cost-effective.

B. Devfense ROI From Security Breach Cost Avoidance

Devfense can also help organizations avoid the astronomical costs of a security breach.

As mentioned earlier, Darwin Professional Underwriters has calculated a single average breach can result in the loss of 99,000 records. A corporate security breach could cost an organization between \$9 million and \$14 million in legal bills, crisis management measures and after-the-fact security improvements.

Let's assume again an initial annual investment of \$4,800 for Devfense boxed service. Let us further assume that vulnerabilities are discovered. These vulnerabilities, left unchecked, could have resulted in a security breach.

Fixing the vulnerabilities would provide immediate ROI as per these calculations:

Conservative ROI calculation:

\$9 million (security breach loss) divided by \$5,000 (initial Devfense deployment) = \$1,800

High-end ROI calculation:

\$14 million (security breach loss) divided by \$5,000 (initial Devfense deployment) = \$2,800.

Thus, for every dollar spent only on the initial Devfense deployment, the company receives between \$1,800 and \$2,800 of value.

Many small-to-medium businesses would be crippled or bankrupted by the financial liabilities of a much smaller security breach.

This ROI of Devfense, as with IT security products generally, could be calculated akin to a disaster insurance premium rather than a strict dollar-for-function analysis. However, the calculation above provides a guideline for calculating ROI for the Devfense web security solutions ROI, which may also apply more generally.

C. Devfense ROI from Maintaining Online Revenue

Another way to calculate ROI from added value of web traffic conversions is to look at the potential loss of revenue from web traffic reduction. Let us assume again that an organization raises \$1 million in sales or donations annually online.

This same organization raises its online revenue from just 5 per cent of the website's 1 million visitors, in accordance with the industry average for conversion rates of online retailers (The Paypal Blog, "Conversion: The Art of Turning Browsers Into Buyers").

The average conversion provides the company with \$20 in revenue from each of its 50,000 converted clients or donors.

Let us assume that a security breach on the organization's website is discovered and reported widely in the mass media. The organization takes immediate steps to plug the vulnerability in its web application.

However, the immediate media coverage scares away 70 per cent of website visitors who have heard about the breach for at least one year (the time it takes for the company to undertake damage control measures, security fixes, etc). This is in line with a 2006 IBM survey result that showed 70 percent of online shoppers will buy from a trusted Web site ("IBM Survey: Consumers Think Cybercrime Now Three Times More Likely Than Physical Crime").

Again, the value of revenue generated from this organization's online presence was \$1 million. If just 70 per cent a year's online revenue is taken away as a result of the breach, the organization will lose \$700,000.

Assuming the average contribution of \$20 per converted visitor remains constant despite the security breach, the organization now makes just \$300,000 per year, or \$822 per day from its online presence. It is now losing \$1,918 per day in online revenue after the security breach.

A relatively small investment of \$8,600 for an annual investment for a Devfense deployment could prevent that loss. In fact, Devfense would pay for itself by ensuring web traffic remains secure and available for just five days.

D. Devfense ROI From Increased Online Revenue

Devfense generates ROI through the opportunity to generate improved online revenue. When an organization publicizes the steps it has taken to ensure users' security through deployment of Devfense, it may profit from improved web traffic conversion rates. Put simply, Devfense can increase sales.

Let's assume the validity of the vendor-supplied data that shows sales conversion rates typically go up an average of 14 per cent after users are made aware that resources have been spent to make the website as secure as possible (Dave Taylor).

In addition, let's assume a medium-sized company does \$1 million in sales every year through its website.

Finally, let us assume an initial investment of \$8,600 for an annual investment for Devfense.

Deploying Devfense and publicizing this on the website through a trust seal could provide the following rough ROI calculation:

\$1 million (sales) multiplied by 14 per cent (increased conversion rate) = \$140,000

\$140,000 divided by \$8,600 = \$16

Thus, for every dollar spent in the first year on Devfense, the company receives \$16 of value in increased conversion.

We can also see the ROI per day for this company from extra conversions of website visitors is \$384. Assuming online revenue accumulates roughly evenly throughout the year, Devfense would pay for itself after just 23 days. This organization would have improved security and generated a long-term online revenue boost for a solution that could be paid for just from the increased revenue in less than one month.

Should the client continue with quarterly scans in subsequent years at \$4,800 per year, the ROI could be even more impressive:

\$1 million (sales) multiplied by 14 per cent (increased conversion rate) = \$140,000 million

\$140,000 (increased sales) divided by \$4,800 (quarterly deployment of Devfense boxed service)
= \$29

Thus, for every dollar spent in the subsequent years on Devfense, the company receives \$29 of value in increased sales conversion.

The ROI per day for this company from extra conversions of website visitors remains as \$384. But with the lower price in the second year, assuming online revenue accumulates roughly evenly throughout the year, Devfense would pay for itself after just 12.5 days.

In this example, this organization would have improved security and generated a long-term online revenue boost. The solution could be paid for, just from the increased revenue, in less than two weeks. The potential for a very cost-effective return on investment from deployment of Devfense is quite clear.

Conclusion

The rough ROI calculations in the preceding section may be useful for a general understanding of the financial implications of investing in Devfense.

As we have seen, a web application security solution such as Devfense can provide tangible ROI from multiple sources, such as from boosting online revenue, ensuring the constant flow of current online revenue, avoidance of extremely costly data breaches and conservation of scarce resources in the IT department.

The reader of this report is advised to take a more holistic view of the potential costs and benefits of investing in a web security solution. Whether the ROI from Devfense is \$250,000, \$700,000, 9 million or \$14 million, or a combination of several numbers, there are a host of other variables executives must consider that are applicable to their individual operation.

Indeed, the added benefit of peace of mind may outweigh the financial considerations when executives can claim with confidence to external auditors and regulatory bodies that reasonable steps have been taken to ensure effective web application security.

Deployment of Devfense boxed service for web application security provides cost-effective ROI that is measurable using a range of metrics. It lowers IT costs, helps prevent the high cost of a security breach, assists organizations in maintaining sources of online revenue and can boost online revenue conversion rates. Devfense boxed service is a cost-effective solution for organizations to improve web application security.

Works Cited

Linda L Briggs. "Application Security Comes Under Attack". Application Development Trends. 6 January 2006. <http://www.adtmag.com/article.aspx?id=18708>

ITRC. "2007 Data Breach Stats". Identity Theft Resource Centre. 26 February 2008. <http://idtheftmostwanted.org/ITRC%20Breach%20Stats%20Report%202007.pdf>

"A Chronology Of Data Breaches". Privacy Rights Clearinghouse. July 15, 2008. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Munir Kodatia and Chris Duckett. "Security Expert: ROI Figures Are Meaningless". ZNet Australia. 18 February 2008. <http://www.zdnetasia.com/news/security/0,39044215,62037905,00.htm>

Greg McLean and Jason Brown. "Determining the ROI in IT Security". CA Magazine. April 2003. http://www.camagazine.com/index.cfm?ci_id=14138&la_id=1

Ryan Singel. "Data Breach Will Cost TJX \$1.7B, Security Firm Estimates". Wired Blog Network. 30 March, 2007. http://blog.wired.com/27bstroke6/2007/03/data_breach_wil.html

Sharon Gaudin. "Security Breaches Cost \$90 To \$305 Per Lost Record". Information Week. 11 April, 2007. <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199000222>

"DSW Settles Data Theft Case". Los Angeles Times. 2 December, 2005. <http://articles.latimes.com/2005/dec/02/business/fi-dsw2>

Tech//404® Data Loss Cost Calculator. Darwin Professional Underwriters. <http://www.tech-404.com/calculator.html>

Robert Richardson. "CSI Computer Crime and Security Survey". Computer Security Institute. 2007.

Frank Abagnale et al. "2005 FBI Computer Crime Survey". Federal Bureau of Investigation. 2005. www.fbi.gov/publications/ccs2005.pdf

Drew Bartkiewicz. "Like A Virus". Insurance Journal. 7 November 2005. <http://www.insurancejournal.com/magazines/west/2005/11/07/features/62359.htm>

Dave Taylor. "Can Hacker Safe, Truste, BBB, And Trust Guard Seals Actually Improve My Sales". Ask Dave Taylor. http://www.askdaveataylor.com/hackersafe_truste_bbb_trust_guard_seals_improve_sales.html

Dan Goodin. "McAfee 'Hacker Safe' cert sheds more cred". The Register. 29 April 2008.
http://www.theregister.co.uk/2008/04/29/mcafee_hacker_safe_sites_vulnerable/

"Conversion: The Art of Turning Browsers Into Buyers". The PayPal Blog. 9 October 2008.
<https://www.thepaypalblog.com/2007/10/>

"IBM Survey: Consumers Think Cybercrime Now Three Times More Likely Than Physical Crime". [IBM Press Room](http://www-03.ibm.com/press/us/en/pressrelease/19154.wss). 25 January 2006. <http://www-03.ibm.com/press/us/en/pressrelease/19154.wss>

About

Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS provides technical assessment & services, business analysis, and IT project management. More information about PCIS can be found at www.pcis.com

Boonbox

Boonbox, a division of PCIS, was created in 2007. Boonbox specializes in productivity solutions that deliver immediate results in support of business challenges like security compliance, password protection and data backup issues. More information about Boonbox can be found at www.boonbox.net