How to Quantify the Costs and Benefits of Web Security

An Osterman Research White Paper

Published July 2011

SPONSORED BY

EdgeWave™
Executive Summary

Most organizations should expect that eventually they will be the victim of malware infiltration or a direct attack by hackers. These incursions can be the result of:

- Careless behavior by users who visit inappropriate Web sites or click on links in spam emails.
- Users visiting legitimate Web sites that have been hacked and that now serve as a source of malware.
- Highly targeted phishing (spearphishing) attempts that successfully install malware like keystroke loggers onto corporate computers.
- Malware that is delivered through short URLs in Twitter posts, or direct attacks by hackers intent on stealing funds and/or data.

Osterman Research has found that most organizations have been the victim of malware incursions through simple Web surfing, while more than two in five have had malware introduced through email. Moreover, the recent attacks against high profile targets like Citigroup and Sony underscore the enormous and growing risk that organizations face from malware, phishing attempts and direct attacks.

KEY TAKEAWAYS

Clearly, every organization must be protected with a solution that can detect, prevent and remediate malware incursions and hacker attacks. However, many financial and other decision makers are not as proactive as they should be and often will not approve the investments that must be made to protect an organization until after a successful incursion has been made into their network. Consequently, IT decision makers need to be able to justify investments into Web security technologies using solid return-on-investment (ROI) analysis. Specifically, this analysis should include:

- A conservative, believable estimate of the potential costs of various types of malware incursions and hacker attacks.
- A reasonable estimate of the likelihood that these attacks will occur.
- Analysis of the long term costs of various Web security solutions.
- A calculation of the ROI that each solution will provide over the long term.

ABOUT THIS WHITE PAPER

This white paper provides a framework for evaluating the ROI of Web security using real-world estimates of the costs of various types of Web-based threats. It also provides some high-level recommendations for decision makers as they consider how to justify the expenditures for Web security solutions. Finally, a brief overview of EdgeWave, a leading vendor of Web security solutions and a sponsor of this white paper, is provided at the end of this document.
Web Threats are Running Rampant

THREATS COME FROM A NUMBER OF SOURCES
Most organizations have experienced some sort of malware infiltration through a variety of sources, as shown in the following figure from an Osterman Research survey conducted during 2010.

The occurrence of malware infiltration has become significantly worse over the past several years. For example, in a 2007 survey conducted by Osterman Research, we found that malware had infiltrated through email in only 25% of organizations surveyed, while only 22% had experienced malware infiltration through the Web – decidedly fewer than in the more recent survey noted above. McAfee reported that their identification of new malware increased from roughly 16,000 new samples per day in 2007 to 29,000 in 2008 to 46,000 per day in 2009 to 60,000 in 2010 – an increase of 275% in just three years. EdgeWave shows similar results in their analysis – on June 24, 2011, for example, the company reported that it had detected 28,570 new bots on that day alone.

There are a large and growing number of platforms and venues from which malware and spam can enter an organization:
• **Botnets**
  There have been a number of successful hacking and phishing attacks against high-profile targets. For example, Citigroup, the International Monetary Fund, the US Senate, Sony, Northrup Grumman, Lockheed Martin and RSA have all been recent victims of attacks. The consequence has been the exposure of millions of records that will result not only in the disclosure of personal and sensitive information, but also lawsuits and other expensive remedial actions.

• **User mistakes**
  Users will sometimes install malware or compromised code on their systems, most often inadvertently. This occurs when they install ActiveX controls, download codecs or various applications that are intended to address some perceived need (such as capability that IT does not support or that a user needs when working from home), or when they respond to scareware and fake anti-virus (Rogue AV or Fake AV) software. Rogue AV is a particularly dangerous type of malware, largely because it preys on users who are attempting to do the right thing – to protect their computers from threats. Even users who are reasonably experienced can be fooled by a well-crafted Rogue AV message.

• **Various types of Web site threats**
  There are a number of ways for malware to enter an organization through Web surfing or the use of Web-based applications. For example, **cross-component attacks** occur when two innocuous pieces of malware code appear on the same Web page. Separately, they are harmless and difficult to detect; however, when they appear simultaneously on a single page, they can infect a user’s machine with malware. With **Cross Site Request Forgery** (CSRF) attacks, innocent-looking Web sites generate requests to different sites. CSRF attacks have exploited vulnerabilities in Twitter, enabling site owners to acquire the Twitter profiles of their visitors. As Web 2.0 applications often leverage XML, XPath, JavaScript and JSON, Adobe Flash and other rich Internet applications, those applications are frequently vulnerable to injection attacks using these environments – these technologies are often used to evade anti-virus defenses, motivating attackers to leverage them. **Cross-site scripting attacks** embed tags in URLs – when users click on these links, malicious Javascript code will be executed on their machines. **SQL injection attacks** occur when SQL commands and meta-characters are inserted into input fields on a Web site, the goal of which is to execute back-end SQL code.

• **Smartphones**
  The growth and importance of smartphones is being exploited by criminals. For example, ING customers in Poland have been hit with a man-in-the-middle attack (a variant of Zeus) that will install malware designed to intercept passcodes sent to Blackberry and Symbian devices via SMS as part of a two-factor authentication scheme. The first malware that targets the Google Android OS was discovered in August 2010. McAfee reported a 46% increase in mobile-focused malware during 2010 compared to the year before.

• **Compromised search engine queries**
  Compromised search engine queries are another method for criminals to distribute malware. This form of attack relies on users making typographical errors when typing search queries, resulting in the presentation of malware-laden sites during Web queries. Search engine poisoning is particularly effective for timely and popular search terms, such as the latest
celebrity gossip. Websense reported that searching for breaking trends and current news represented a higher risk (22.4%) than searching for objectionable content (21.8%).

- **Drive-by downloads**
  Related to the blended threat is a “drive-by” download that occurs when a user visits a Web site and has malware automatically downloaded to his or her computer. In some cases, a user will visit a Web site and see a popup window – upon clicking the “OK” button in the popup, a Java applet, an ActiveX control, etc. will be installed on the user’s computer without their consent.

- **Direct hacker attacks**
  Direct hacker attacks can include a variety of exploits, including hackers attacking a known vulnerability in a Web browser, or exploiting an older version of a browser or ActiveX control.

- **Compromised, legitimate Web sites**
  Many legitimate Web sites have been hacked and have served up malware to unsuspecting visitors. Kaspersky found that one in every 3,000 Web sites served up some sort of malware in 2010, while the Online Trust Alliance reported that in excess of 10 billion advertising impressions in 2010 contained malware, with a dramatic increased noted during the last quarter of 2010.

**Web Security Needs to be a Top Priority**

Web threats are becoming much more serious as criminals increasingly exploit holes in corporate Web defenses, and as users employ a growing array of Web-based tools. These threats are becoming so costly that many organizations are at risk of being put out of business through direct financial losses or the loss of data that carries with it enormous remediation and other costs. For example, many organizations have been hit with keystroke loggers, such as Zeus, that allow criminals to transfer funds out of corporate financial accounts to “mules” that are often located in the same country as the victim. These funds are then wired to recipients in Eastern Europe or elsewhere. There have been numerous cases of this type of theft, resulting in significant financial losses as in the following examples:

- Hillary Machinery lost $800,000 and its bank was able to recover only $600,000
- The Catholic Diocese of Des Moines, Iowa lost $600,000
- Patco lost $588,000
- Western Beaver County School District lost $700,000
- Experi-Metal, Inc. lost $560,000
- Village View Escrow lost $465,000
- An unidentified construction company in California lost $447,000
- Choice Escrow lost $440,000
- The Government of Bullitt County, Kentucky lost $415,000
- The Town of Poughkeepsie, New York lost $378,000
- An unidentified solid waste management company in New York lost $150,000
- An unidentified law firm in South Carolina lost $78,421
- Slack Auto Parts lost $75,000
However, direct loss of funds is not the only serious consequence of malware: the 2011 Data Breach Investigations Report found that malware was responsible for nearly 80% of lost data in 2010 and was a factor in roughly one-half of the cases in which data was lost. Data lost can include a wide variety of valuable content, including trade secrets, financial data, marketing plans, server passwords and other sensitive and confidential information.

LESS QUANTIFIABLE CONSEQUENCES
While the direct loss of funds and sensitive information are very serious consequences arising from malware, there can also be serious – albeit sometimes less quantifiable ramifications – from malware. These include the erosion of trust that a company has (or had) with its business partners or customers, as well as the loss of future business opportunities or revenue from customers who fear their data is not as safe with a malware-victimized company as it once was. Further, the filing of legal actions arising from major – and sometimes minor – data breaches and financial losses are almost a foregone conclusion.

How Do You Calculate the ROI for Web Security?

WHAT ARE THE FINANCIAL CONSEQUENCES OF AN ATTACK?
The financial consequences of a Web attack or malware incursion can vary widely, ranging from simply “annoying” issues like the need for IT to reimage machines or install additional anti-malware capabilities; to truly devastating consequences, such as the direct loss of funds as shown in the examples above.

For purposes of analyzing various types of Web security problems, we have chosen three example attacks/incursions that could impact any organization that allows its users to access the Web:

• **Example 1: Major attack**
  In this attack, malware or a direct hacker incursion results in the actual loss of funds totaling $750,000. Alternatively, we could also assume that 30,000 records were stolen as a result of a malware or hacker attack; requiring direct, out-of-pocket remediation expenditures of $25 per record.

• **Example 2: Serious attack**
  This attack is also serious, resulting in the direct loss of $100,000 in funds, but the victim’s bank from which the funds were stolen is able to recover $50,000 of these funds. Alternatively, we could also assume that 2,000 records were stolen as a result of a malware or hacker attack, requiring direct, out-of-pocket remediation expenditures of $25 per record.

• **Example 3: “Minor” attack**
  In this example, no funds or data are stolen, but a malware attack requires the reimaging of 300 desktop computers, resulting in 200 person-hours of IT staff time and 80 person-hours of help desk time to resolve. Further, the reimaging means that the 300 affected employees are without access to their computers for six hours during the remediation process.
WHAT DOES WEB SECURITY REALLY COST?
The total cost of ownership for a Web security solution can vary widely based on a number of factors, including the initial acquisition cost of the hardware, software or service; the cost of IT labor required to manage the system on an ongoing basis; software licensing and maintenance costs; the cost of any hardware that is required to run the software; the ability to re-use existing hardware and other factors. Moreover, the differences in the cost between various solutions will vary based on the features and functions offered in the solution. It is important to evaluate both the Total Cost of Ownership (TCO) and the Total Cost of Acquisition (TCA) for Web security systems, since these can have significant impacts on ROI. We define these terms as follows:

• **TCO**
The total cost of the hardware, software, services and labor required to acquire, configure, deploy and manage the solution over its lifespan. For purposes of this white paper, we are assuming a four-year lifespan for a Web security solution.

• **TCA**
The total cost of the hardware, software, services and labor required to acquire, configure and deploy the solution. A key element of TCA is including the cost of hardware and software that can be re-used for the Web security solution.

For purposes of comparison in this section, we will examine the approximate four-year costs for Web security in a 750-seat organization. Our goal is to present a rough estimate of the costs for the purpose of analyzing the return-on-investment (ROI). The costs of specific Web security solutions will vary from this example, producing higher or lower ROI calculations:

Because on-premises Web security capabilities have widely differing costs, we chose to use a rough average of the four-year costs for providing these capabilities using an amalgam of various on-premises solutions. The figures below include both vendor pricing and Osterman Research data on IT labor costs for managing Web security systems. Using this data, the approximate costs of an on-premises Web security solution are:

- Initial software licensing cost: $20,000
- Initial hardware cost: $10,000
- Software maintenance cost over four years: $10,800
- IT labor cost for initial setup: $7,000
- Annual IT labor cost for maintenance: $15,000

Based on these assumptions, the four-year TCO of an on-premises Web security solution is $107,800. Please keep in mind, however, that the cost of a Web security solution can vary widely based on its features and functions, whether it is offered as a SaaS or on-premise solution, the number of employees served over the lifecycle of the system and other parameters.

HOW LIKELY IS YOUR ORGANIZATION TO BE ATTACKED?
The likelihood of a successful malware or hacker attack can vary widely depending on a number of factors, including the training that employees have received about how to respond to phishing attempts, training on good Web surfing practices, the Web security technologies that
have been deployed, the proactivity of IT staff in monitoring the network, the value of the data assets accessible through the network, and the size of the organization, among other factors. For purposes of this analysis, we have assumed the likelihood of an attack of each type as follows:

- Major attack: 3% during the next 12 months
- Serious attack: 5% during the next 12 months
- Minor attack: 60% during the next 12 months

Again, it is important to keep in mind that these figures might be more or less conservative depending on the wide range of factors noted above. However, we believe that these figures are actually quite conservative and that many organizations face a much higher probability of incurring these types of attacks.

**CALCULATING THE COST OF ATTACKS**

In calculating the actual cost of each of these types of attacks, we have used a quantitative business analysis approach to determine their cost to a victimized organization. This approach simply multiplies the potential loss from an attack by the likelihood of its occurrence. While this approach will not accurately determine the cost of the next attack, it will accurately estimate the cost of these attacks over time. Using this approach, we can determine that the cost of the three types of attacks noted above will be as follows:

- **Major attack**
  Loss of $750,000 x 3% likelihood per year = $22,500 per year

- **Serious attack**
  Net loss of $50,000 x 5% likelihood per year = $2,500 per year

- **Minor attack**
  Cost of $74,200 ($11,200 + $63,000) x 60% likelihood per year = $44,520

  Assumes:
  
  - 280 hours of IT/help desk staff time at $40 per hour = $11,200
  - 300 non-IT employees x 6 hours of downtime at $35 per hour = $63,000

Based on these assumptions and estimates, the total cost of malware and hacker attacks will be $69,520 per year, or $278,080 over four years.

**DETERMINING THE ROI OF WEB SECURITY**

The ROI of a Web security solution is calculated using the following formula. The “return” in this analysis is simply the avoidance of the financial and other losses arising from various types of malware and hacker attacks:

\[
\frac{\text{Return} - \text{Investment}}{\text{Investment}} = \text{ROI}
\]
What this tells us is that an organization can afford a Web security solution that costs as much as its potential loss minus the actual cost of acquiring and managing the solution. Spending exactly this much would yield an ROI of zero, while spending anything less would result in a positive ROI.

Using the example above, the Web security solution would yield a four-year ROI of 158%:

\[
\frac{278,080 - 107,800}{107,800} = 158\%
\]

As noted, we believe that these calculations are relatively conservative and represent the low end of both the potential cost of malware/hacker attacks and the ROI that can be achieved from deploying a Web security solution. However, these figures are made even more conservative by the fact that the typical malware or hacker attack often results in additional costs not noted here, such as extra IT and help desk staff time, the use of external consultants and outside forensics firms, work by internal or external legal counsel, other legal expenses, opportunity costs from delayed IT initiatives, and the like.

**VIEWING THE BENEFITS ANOTHER WAY**

Although the ROI approach to justifying the deployment of Web security is certainly a valid one, a better approach may be to view Web security as something more akin to life insurance. While the decision to purchase life insurance can certainly be justified based on ROI considerations, the purchase decision is normally made simply to avoid the economic consequences of a catastrophic loss.

An example of justifying Web security to avoid potentially business-ending consequences can be found in the experience of Choice Escrow, the company noted earlier that lost $440,000 to a Zeus botnet infiltration. Immediately after the loss was discovered by senior management, the company was able to come up with $300,000 in emergency funds to help cover the losses. However, management had to lay off two employees directly as a result of the attack and had to obtain a small business loan to replace the lost funds. While Choice survived the attack, many weaker companies in a similar position might not have.

The bottom line is that while ROI is a sound and reasonable method for justifying the deployment of a Web security solution, the life insurance approach may represent a better justification argument for some organizations.

**Taking the Next Steps**

Moving forward, decision makers should undertake four basic steps in determining how best to justify the expenditures required to deploy a Web security solution:

- First, it is critical to examine the financial and other benefits of using the Web and Web 2.0 applications. For example, allowing users to surf the Web permits them to do research, make travel plans, learn about industry conferences, monitor competitors, improve marketing reach, work from home more efficiently, and perform a wide range of tasks that
would be more difficult or more expensive using alternative methods. Because of the rapidity with which these tasks can be completed using the Web, the economic advantages of allowing it typically justify allowing employees to access it.

Similarly, Web 2.0 applications like Twitter, Facebook, YouTube and other tools can provide significant benefits to individual employees and the company as a whole. While there may be justification for limiting access to certain tools or features within these applications, giving employees access to at least some of these tools and their features is normally warranted.

• Next, it is important to determine the risks associated with permitting access to the Web and Web 2.0 tools. These risks include the greater likelihood of successful malware infiltration from activities like simple Web surfing or employees clicking on the short URLs contained in Twitter posts, the greater likelihood of a blended threat (a spam message that contains a link to a malware-laden site) introducing malware into a network, or the greater likelihood of a phishing attack that is able to install a keystroke logger on a senior manager’s computer. It is critical to evaluate both the short term and long term risks associated with use of the Web and Web-based tools.

• Next, decision makers must justify the deployment of Web security using some sort of objective criteria. This might include a detailed ROI analysis, as shown above, that includes the costs of specific solutions under consideration and management’s best assessment of the likelihood of various risks and their associated costs. Alternatively, the analysis might simply focus on the prevention of a major attack that would have a high likelihood of putting the organization out of business. This analysis should evaluate the ROI and other benefits of a) doing little or nothing about the problem, b) implementing draconian controls to block virtually all use of the Web and Web 2.0 tools, and c) managing Web and Web 2.0 use through appropriate policies and Web security technologies. Osterman Research believes that in almost every case Option C will yield the greatest combination of ROI, employee productivity and corporate revenue generation.

• Finally, it is important to evaluate Web security solutions based on a) their effectiveness in blocking Web-based threats, as well as b) their overall TCO and TCA. With regard to the latter, the TCA can vary widely based on a number of factors, including software licensing and vendor maintenance costs. As noted earlier, TCA can also be heavily influenced by the ability to re-use existing hardware that may be left over from a server upgrade – using this hardware for a Web security deployment can dramatically reduced the TCA and boost the long-term ROI of the solution.

Summary

Web threats are serious and becoming more so, and carry with them the risk of financial, data and other types of losses. These losses can vary based on a number of factors, but the likelihood of the typical organization being infiltrated with malware or directly attacked in any given year is well over 50%.
To prevent these types of malware infiltrations and Web attacks, organizations of all sizes should deploy Web security capabilities. While management may not want to make the sometimes significant investments in these capabilities, a strong ROI case using reasonable risk and cost estimates can be made to help IT staff and others to justify these expenditures.

Sponsor of This White Paper

EdgeWave (OTCBB/OTCQB: EWVE) develops and markets on demand, on-premises, and hybrid Secure Content Management (SCM) solutions to the mid-enterprise and service provider markets. The EdgeWave portfolio of web, email and data protection technologies delivers comprehensive secure content management with unrivalled ease of deployment and the lowest TCO on the market. The company’s award winning iPrism Web Security and Email Security products are complemented by email archiving and data loss protection, and can be delivered as hosted, on-premises, and hybrid services. With 6,500 customers and over 200 partners worldwide, EdgeWave strives to deliver simple, high performance solutions that offer excellent value.

Based in San Diego, California, EdgeWave markets its solutions through a network of value added resellers, ISPs and MSPs, distributors, system integrators, OEM partners and directly to end users.
How to Quantify the Costs and Benefits of Web Security

© 2011 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader’s compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, “Laws”) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

4 http://www.pcworld.com/businesscenter/article/220223/advanced_zeus_trojan_hits_polish_ing_customers.html
5 Websense 2010 Threat Report
6 http://www.bbc.co.uk/news/technology-12539993
9 http://www.reuters.com/article/2010/01/11/us-usa-zeus-idUSTRE60A5R020110111
12 http://www.post-gazette.com/pg/09195/983738-57.stm
15 http://www.technologyreview.com/computing/23488/?a=f
16 http://www.bankinfosecurity.com/articles.php?art_id=3159&opg=1
18 http://www.computerworld.com/s/article/9153598/Poughkeepsie_N.Y._slams_bank_for_378000_online_theft
19 http://www.suite101.com/content/protect-yourself-against-banking-crimeware-a156086
22 http://gocsi.com/public/dbir