Quantifying the Impact of Network-Based Attacks
A short guide to assessing the value of next-generation firewalls

The Impact of Attacks on Your Bottom Line

Network security is critical. But how do you quantify the value? How do you justify investing in network security products like next-generation firewalls, intrusion prevention systems and unified threat management appliances?

This document will give you some guidelines on how to assess the impact of network-based attacks on your organization. We will look at:

- Different types of network-based attacks
- How those attacks can affect your bottom line
- Methods of quantifying the impact of those attacks

We can’t give you a simple “impact of attacks” calculator. Every organization is faced with different threats, and the cost of attacks depends on many factors. But we can provide sources of industry studies and suggest techniques for creating your own economic model. We can provide sources of industry studies and suggest techniques for creating your own economic model.
Types of Network-Based Attacks

There are hundreds of network-based attacks that can damage an organization. These include:

- Viruses, Trojans, worms and other malware that can shut down servers and workstations or steal data.
- Advanced persistent threats designed to penetrate networks and exfiltrate intellectual property and confidential information.
- Distributed denial-of-service (DDOS) and flooding attacks that can overwhelm servers and shut down web sites.

How Network-Based Attacks Can Affect Your Bottom Line

It is useful to divide network-based attacks into two categories based on the type of harm they cause: data breaches and loss of service.

Data breaches

Data breaches are attacks that result in confidential information being captured and exfiltrated out of the organization so that it falls into the hands of criminals or competitors.

The damages caused by data breaches include:

- Lost business, as measured by reduced revenue, abnormal customer churn and increased customer acquisition costs.
- Detection and technical remediation costs, for identifying and blocking attacks, assessing damage and putting corrective measures in place.
- Notification costs, for communicating facts about the breach to potential victims and protecting victims from harm — for example, giving them memberships in credit monitoring services.
- Legal and regulatory costs, from fines and lawsuits.
- Loss of competitiveness, from intellectual property such as engineering designs and business plans falling into the hands of competitors.

Loss of service

Loss-of-service attacks result in computer systems — workstations as well as web, application or database servers — being disabled or degraded. Financial effects include:

- Lost business, when customers cannot check inventory, place orders or otherwise interact with the organization.
Lost productivity, when business processes are interrupted or employees cannot do their jobs because workstations or servers are unavailable.

Remediation, where IT and support staff lose time diagnosing problems, coaching employees, restarting services and re-imaging PCs.

**Quantifying the Impact of Attacks — Surveys**

To quantify the impact of network-based attacks, industry surveys and studies are a good place to start. Here we will look briefly at two that address the cost of data breaches.

**The Ponemon Institute Cost of a Data Breach Survey**

The most extensive recent survey of the cost of data breaches was performed by the Ponemon Institute in late 2011 and published in March 2012. The institute conducted in-depth interviews with 49 U.S. companies in 14 industries that had experienced the loss or theft of customers’ personal data. Some of the key findings are shown in Table 1.

<table>
<thead>
<tr>
<th></th>
<th>Cost per breach</th>
<th>Cost per record</th>
<th>Typical expenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost Business</td>
<td>$3,007,015</td>
<td>$106</td>
<td>Abnormal customer turnover, increased customer acquisition activities, reputation losses, diminished goodwill</td>
</tr>
<tr>
<td>Post data breach</td>
<td>$1,505,049</td>
<td>$53</td>
<td>Help desk, inbound communications, remediation, legal expenditures, product discounts, identity protection services</td>
</tr>
<tr>
<td>Notification</td>
<td>$561,495</td>
<td>$20</td>
<td>Creation of contact databases, determination of regulatory requirements, outside experts, postal expenditures</td>
</tr>
<tr>
<td>Detection and escalation</td>
<td>$428,330</td>
<td>$15</td>
<td>Forensics, assessment and audit, crisis team management, communications to executive management</td>
</tr>
<tr>
<td>Total (rounded)</td>
<td>$5.5 million</td>
<td>$194</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Figures from the Ponemon Institute 2011 Cost of a Data Breach Survey

The per-record figures allow you to scale these costs up and down based on the number of records of protected personal data in your organization.

The study also includes other figures that can be very helpful in adjusting costs to different situations. The study includes figures for the 14 industries (for example, the reported cost per record is highest for the communications, pharmaceutical and financial industries and lowest for public sector, hospitality and media) and adjustments based on factors such as whether the organization has a CISO and whether the data was lost or stolen due to mistakes by a third party.
However, the study has limitations. The sample was limited in size and geography, and it excluded breaches of over 100,000 records (on the grounds that they would distort the averages). Also, it did not try to measure the effect of losing intellectual property.


**The NetDiligence® Cyber Liability & Data Breach Insurance Claims Study**

In October 2012, NetDiligence published a study of 137 events between 2009 and 2011 that resulted in insurance companies making payouts on cyber liability claims. Some of the findings are shown in Table 2.

<table>
<thead>
<tr>
<th>Cost per breach</th>
<th>Typical expenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal settlement</td>
<td>$2,100,000</td>
</tr>
<tr>
<td>Legal defense</td>
<td>$582,000</td>
</tr>
<tr>
<td>Credit monitoring</td>
<td>$345,000</td>
</tr>
<tr>
<td>Forensics</td>
<td>$341,000</td>
</tr>
<tr>
<td>Notification</td>
<td>$180,000</td>
</tr>
<tr>
<td>Legal counsel</td>
<td>$66,000</td>
</tr>
<tr>
<td>Call center</td>
<td>$50,000</td>
</tr>
<tr>
<td></td>
<td>(but one exceeded $1 million)</td>
</tr>
<tr>
<td>Total (rounded)</td>
<td>$3.7 million</td>
</tr>
</tbody>
</table>

Table 2: Figures from the NetDiligence Cyber Liability & Data Breach Insurance Claims Study

These figures differ from the Ponemon study in part because the sample is different (incidents where an insurance payout was made). However, while this study does not attempt to quantify the costs of lost business, the other estimates are in the same ballpark.

Estimates for Your Organization

Back-of-the-Envelope Calculations
Perhaps industry surveys provide enough “ballpark” data to justify your investment in network security technologies. If not, the next step is to estimate a few key variables based on data for your own organization.

For example, you may have figures for or be able to estimate:

- The revenue loss for every hour your web site is down because of a DDoS attack.
- The productivity loss for every hour a key business process is down because of malware disabling the server.
- The hourly rate for help desk personnel to diagnose malware infections on PCs and for the support group to re-image infected PCs.
- The cost per record for notifying customers or employees in the event of a data breach and providing credit monitoring services to them for a year.

You can then use these hourly or per-record estimates to make back-of-the-envelope calculations based on the number of hours you expect to reduce downtime or the number of records that your organization might lose from a security breach.

‘War game’ simulations
Some organizations have created valuable estimates by conducting “war game” simulations. These involve gathering a cross-section of company staff from IT, marketing, HR, legal and other functions, and running through an attack scenario — say, a denial-of-service attack or a breach of customer information. These exercises not only help quantify costs, but often turn up unexpected effects — for example, contractual obligations or the regulatory impact of data breaches.

Data from peer organizations
It fairly easy to find in the press examples of all of the types of attacks detailed here, often with discussions of the costs. Information can also be found from colleagues, industry associations and other sources.

For example, one survey showed that the cost of DDoS attacks exceeded $10,000 per hour for travel, telecom and financial industry web sites and over $100,000 per hour for large retail web sites. ¹

Detailed business case — an ANSI model


The document is aimed at organizations that manage protected health information and contains details that are specific to healthcare, HIPAA and other health-related legislation.

However, it includes valuable material that can be modified and adapted for other environments.

For example, the following five-step process is outlined in the document:

1. Conduct risk assessment
2. Determine security-readiness score
3. Assess the relevance of a cost
4. Determine the impact
5. Calculate the total cost of a breach

It also includes a hypothetical scenario of a breach with an extremely detailed cost calculation based on reputation repercussions, remediation costs, lost productivity, communications and public relations costs, and legal and regulatory costs. This document is available at: [http://webstore.ansi.org/phi/](http://webstore.ansi.org/phi/).

Recap: Putting the Pieces Together

Depending on how much detail you need, there are many ways to go about quantifying the impact of network-based attacks and, therefore, the potential value of next-generation firewalls and other network security products.

The first step is to understand exactly how data breaches and loss-of-service attacks can affect costs and revenue.

Then, if a broad-brush estimate is enough, you may be able to find the justification you need in industry surveys such as the Ponemon Institute Cost of a Data Breach Survey and the NetDiligence Cyber Liability & Data Breach Insurance Claims Study.

If you need detail that is more specific to your organization, you can create back-of-the-envelope calculations, run “war game” simulations and find data about peer organizations.

Or you can create a highly detailed model, perhaps based on a template like the one provided in ANSI’s “The Financial Impact of Breached Protected Health Information.”

---

See Chapters 7 and 8.