WHITE PAPER

ixia

An Executive Business Case for Network Security

915-3531-01 Rev. A, April 2015

Table of Contents

Executive Summary

Did you know that improving network security is an easy way to protect and increase shareholder value while mitigating corporate risk? This is a true statement. Implementing network security resilience is one of the few things that you can do that will:

- Protect company brand value
- Decrease operational costs
- Preserve your company valuation
- Decrease the possibility and potential costs of a security breach
- Decrease executives' risk of personal liability (not covered under the corporate insurance)

This whitepaper will discuss several fundamental approaches to network security investments and then show you the benefits of choosing a resilient architecture approach. Key conclusions reached in this document include the following:

Did you know that improving network security is an easy way to protect and increase shareholder value while simplifying your life?

- You can reduce the $12.7M average annual costs for security breaches by up to 73%. Annual estimated costs are based the Ponemon Institute $5.85M per breach (in the USA) and the annual probability of experiencing a security breach.
- A representative example of a $1.8M resilient security investment can result in a net present value (NPV) of $11.8M with a payback period of 6.4 months. Even with an overly conservative approach that neglects any company value for a secure network, the payback period is less than one year.
- The rate of return on a representative resilient security investment is 49%
- Resilient security investments can prevent a reduction in company book value by up to 10% of the company's annual sales revenue
- You can reduce part of your OPEX costs, specifically corporate network mean time to repair (MTTR) intervals, by up to 80%
- Testing of security products can result in security vendor discounts up to 30%, although the real value is in having the correct vendor information up front to prevent costly decisions
- You can eliminate potential priority 1 network faults, resulting in average savings of $280K (per potential fault)

These conclusions are reached through the combination of a basic security architecture, visibility architecture, and security resilience components. When combined with a life-cycle approach to securing your network, these three components maximize network security benefits while minimizing costs and risk potentials. Very few company investment options that you consider will achieve as fast a payback as a properly designed network security architecture. Conduct your own financial analysis and see for yourself.

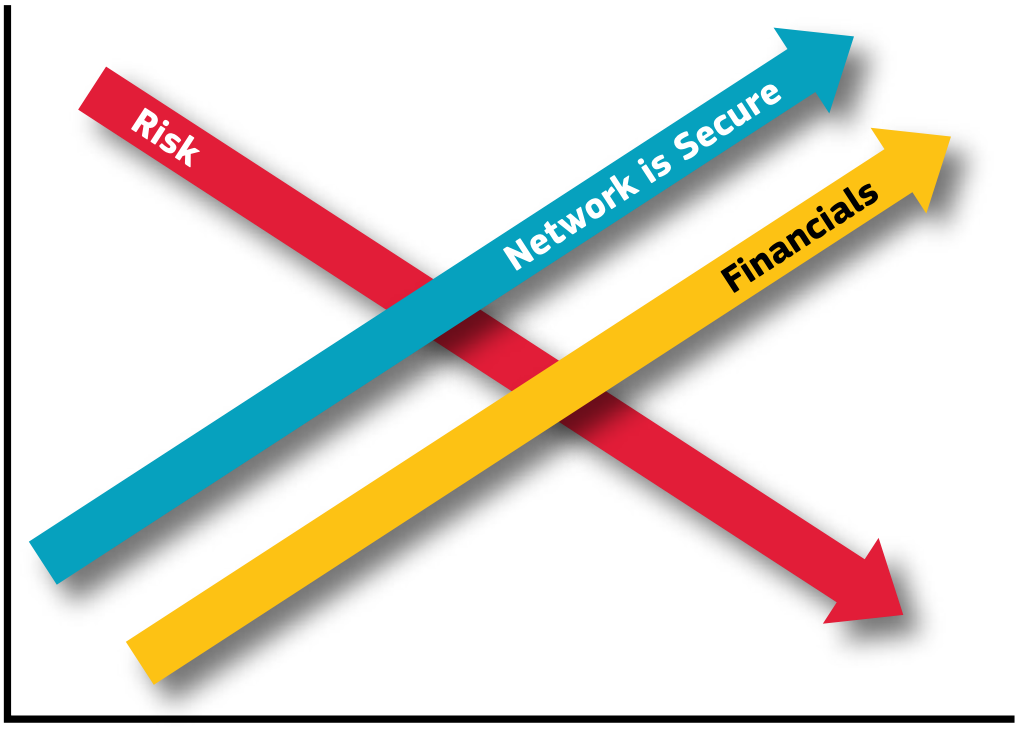
The Great Debate

Network security for today's enterprise is an important topic. Everyone knows this – from the network engineer to the Chief Executive Officer (CEO). But, is network security just as important as generating revenue, controlling costs, and protecting shareholder value? Could it be more important, since public acknowledgement of security breaches has been proven to negatively affect all three items dramatically? This is where the debate (and problem) starts to take place.

The C-suite (particularly the CEO and CFO) are typically measured on three main key performance indicator (KPI) categories:

- Financials (revenue generation, cost reduction, profit, and cash flow)
- Growth potential (customer acquisition, retention, and satisfaction)
- Other (regulatory compliance, productivity improvement, quality, network security, etc.)

Some don't believe that network security should fit into the "Other" category, while some do. If it's not part of the KPI's, it often doesn't get the attention it warrants. And so this debate has contributed to the network security debacle we have now, due to the haphazard belief in its strategic priority. In fact, we are nearing a crisis, as demonstrated by the escalating number and severity of annual network security breaches for enterprises and carriers.



The True Economics of Network Security

There is a simple way to end much of the debate – assign financial value to network security initiatives to create a solid financial benefit for the capital investment and operational expenses, as well as opportunity costs for inaction. This will allow it to be judged upon its merits and contribution. However, the fundamental assumption is that the analysis be complete and accurate – simply using convenient data won't provide the requisite accuracy.

Once a financial analysis is performed, the discussion can be ended quickly. A typical analysis, as will be shown, demonstrates that spending on a resilient security architecture is actually an investment, not a cost.

A typical analysis, as will be shown, demonstrates that spending on a resilient security architecture is actually an investment, not a cost.

To accomplish this, a financial analysis can be constructed as follows:

- Create a cost/benefit analysis specific to your company
- Create an NPV business case around that cost/benefit analysis

A solid financial analysis should include anticipated network attack and breach costs along with the typical security product capital expenditures and ongoing operations costs. Breach costs include: remediation, fines, and potential lawsuits regarding the release of customer and employee personally identifiable information (PII), personal and corporate liability, intellectual property loss, and brand damage.

In this paper, we will create a generic example to illustrate this financial analysis (including the creation of an NPV) based upon public Ponemon Institute research and Ixia-conducted research. The analysis will lean heavily upon Ixia's book, Convincing Your CFO Why Network Security is Important[1], and interested parties should refer to that book for a full detailed analysis and context behind the data points summarized here.

As an additional note, for better accuracy in your financial analysis, you'll probably want to address individual variances specific to your business within your financial analysis. Some primary examples of individual variances that you may want (or need) to address include the following:

- Size of your business
- Geographic location(s)
- Industry sector
- Use of international operations
- Use of cloud services

Different Approaches to Network Security Investment

The first key understanding to acknowledge when conducting a security investment analysis is that there is risk everywhere.

The first key understanding to acknowledge when conducting a security investment analysis is that there is risk everywhere.

For the C-suite, a breach of the corporate network could translate to concerns of "breach of fiduciary responsibility" and whether the SEC and FTC might decide that they, the C-suite, did not provide adequate and reasonable "fail-safes" to avoid the exposure of PII. Issues with the SEC and FTC could even lead to issues with creditors, putting the company in more peril. Neither the CEO nor CFO will enjoy the next board meeting after showing 'material weakness' via breach or audit, as this is a liability issue that can directly impact the company's viability. A solid security and visibility architecture investment will give the CFO and CEO more confidence when reporting to the board of directors about company security and data integrity.

While most companies will not make the nightly news for security breaches, they are generally accountable to the SEC, FTC, and various other federal, international, local, and state agencies. The FTC and other agencies have the power to levy fines and judgments that can be used in legal proceedings against individuals and businesses as well. This can become especially important if you discover that your corporate security breach insurance policy doesn't always protect the C-suite personnel. This can leave executives vulnerable to personal litigation by injured parties.

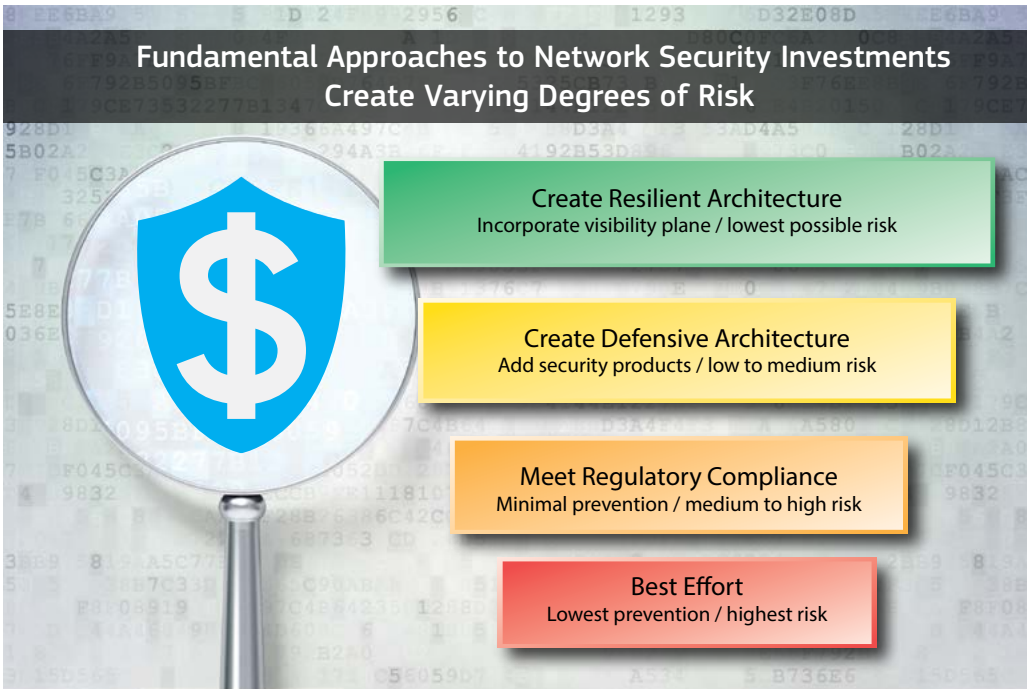
1 http://info.ixiacom.com/2015-Q2-CFO-ebook-sign-up.html

This leads to another set of key points:

- Remediation costs for a breach can become very expensive and could put the company out of business
- Brand damage can affect stockholder sentiment for the business, causing stock price fluctuation, negative changes to company valuation, SEC investigations, and regulatory compliance investigations
- Brand damage doesn't just affect a company, but individuals as well

To counter the threats, there are essentially four fundamental approaches to network security investments that can offer varying degrees of risk levels:

- **Create a resilient architecture:** includes breach recognition and prevention by incorporating a visibility plane to create the lowest possible risk
- **Create a defensive architecture:** focus is on adding security products, which creates a low to medium risk
- **Meet regulatory compliance:** delivers minimal prevention and creates a medium to high risk
- **Best effort:** delivers the lowest prevention and creates the highest risk



Resilient Architecture Approach

The goal of the resilient architecture approach is to quickly stop all threats (attacks and breaches) and to recover from those attacks as fast as possible. This approach combines the defensive architecture approach components of the next section (firewalls, intrusion prevention systems, security processes, etc.) with a visibility architecture (taps, packet brokers, and monitoring tools) and security resilience components (load testing, effectiveness testing, cyber range training, etc.). The goal of stopping all threats may not always be achievable, but this approach should typically result in fewer breaches and less severe breaches (if they do happen). To be effective, the resilient architecture approach relies on an integrated visibility and security architecture. You can't just purchase a few individual products and hope it stops everything.

The goal of the resilient architecture approach is to quickly stop all threats (attacks and breaches) and to recover from those attacks as fast as possible.

In financial liability terms, this approach should typically result in a 60% to 80% cost reduction for every security breach, depending upon several factors of course, and it presents the lowest risk option that is possible. If the architecture has been designed correctly, then you should be able to minimize revenue losses and the risk of encountering significant fines (if any). This is because the fee structure for fines typically depends upon the number of records exposed and the due-diligence displayed in trying to make sure that the network is secure.

A second component to the resilient architecture is to actively test your production network. This is sometimes called "Red-Teaming" and involves penetration testing and cyber war game exercises. These activities assume that a breach can happen and allows you to test how your network and personnel will respond to various threats. The benefits of Red-Teaming and cyber range training include the development of better detection capabilities, practical experience with actual threat response techniques, and the development of capabilities to minimize what a hacker can accomplish during a breach (i.e., prevent/limit loss of intellectual property, data records, etc.).

You need an emphasis on network visibility in the resilient approach to make sure that you see all of the damage and fix it correctly.

Defensive Architecture Approach

For the next option, the defensive security architecture approach should involve a formal security architecture plan. This includes products (firewalls, IPS, SIEMs, threat prevention, forensic recorders, and other devices) and processes. The primary focus here is on adding security products to lower the risks of a breach. However, one of the key points should also be to make sure you have documented policies. The documented policies will go a long way in showing due diligence to try to protect network security, which can lessen, or even eliminate, potential fines and bad press. Unfortunately, this seems to be where many security architectures stop, leaving those businesses susceptible to advanced vulnerabilities (both external and internal) and creating a situation where the mean time to recovery takes longer than it could, and should.

While the defensive security architecture approach is good, it's not as good as the resilient approach. This is mainly because of the lack of focus on making sure that the security architecture can "bounce back" as fast as possible due to network testing and network visibility. You want the system to recover as fast as possible so as to limit the scope of an attack or breach, thereby limiting your current and future financial losses, liability, and embarrassment. You need an emphasis on network visibility in the resilient approach to make sure that you see all of the damage and fix it correctly. Any malware that is missed can be a future ticking time bomb.

Regulatory Compliance Approach

The "meet regulatory compliance" approach is the next rung down. This is often an approach by business leaders who don't fully understand the risks of a breach. By simply focusing on meeting regulatory compliance requirements for network security, minimal real security threat prevention has been accomplished and the risk to your network remains very high. Business leaders may provide sporadic funding for network security because they need to, but otherwise, they probably aren't committed to network security.

In this approach, you've possibly deployed point solutions for firewalls and intrusion prevention systems (IPS) to counter malware and typical denial of service (DoS) threats. However, lack of a coherent plan will usually mean that you have security holes that most hackers will be able to break through. That being said, while the results for the "meet regulatory compliance" approach will obviously be less spectacular than a prevention approach, it can still have the following benefits:

- Results in lower additional costs to the company for breach remediation when compared to the "best effort" approach. You should see some limitation of the costs associated with a breach, but you can probably expect to incur 70% to 80% of the cost of a breach.
- Typically provides a faster MTTR over the best effort approach
- Has the potential of reduced fines (depending upon the level of due diligence)

Best Effort Approach

The best effort approach is self-explanatory. This approach has the propensity to result in the high risks discussed previously (large-scale loss of revenue, reputation damage, company fines, personal liability, and other personal impacts like loss of job). If the company approach to security is to do nothing (or almost nothing), then the task is simplified – there's no need to perform a financial analysis.

The best effort approach has the propensity to result in the high risks discussed previously (large-scale loss of revenue, reputation damage, company fines, personal liability, and other personal impacts like loss of job).

Demonstrating the Financial Business Case for Network Security

This section provides an example financial analysis that can be used to demonstrate the net present value of a resilient network security architecture investment.

Your financial analysis should have the following items from your cost/benefit analysis:

- Technology purchase costs (CAPEX) – equipment, training, installation, etc.
- Technology maintenance costs (OPEX) – personnel, annual license costs, etc.
- Return on investment (ROI) – expected savings, revenue savings/protection, etc.
- Other – quantify other costs and benefits

This example uses an NPV analysis performed on a traditional Fortune 1000 enterprise. A greenfield environment for a company with annual revenues of $800M was assumed for the analysis. An NPV calculator and several ROI calculators were used for the analysis. The basic ROI calculation uses the following equation: ROI = net benefits / total cost. For this analysis, we'll use ROI as synonymous with the financial benefits as we are using an NPV analysis as the basis of our business case.

An NPV analysis includes an ROI calculation plus the time value of money. A typical NPV formula (for 3 years) is as follows:

$$NPV = [(B0 - C0)] + [(B1 - C1) / (1+r)] + [(B2 - C2) / (1+r)2] + [(B3 - C3) / (1+r)3]$$

where B = benefits, C = costs, and r = discount rate (i.e., the interest rate). The time period has already been accounted for with the superscripts. The USA Office of Management and Budget (OMB) recommends a nominal discount rate of 2.7% for a project duration of 3 years.

Example Analysis – Fortune 1000 Enterprise

Basic Assumptions

- Number of company employees = 13,000
- Number of company remote offices = 30
- Number of data centers = 1
- International operations = yes
- Annual company revenue = $800

The Ponemon Institute further states that the average annual cost of cyber crime in the United States can be estimated as $12.7M and the average time to find the breach was 170 days.

Security Breach Cost Estimate

The estimated cost per breach for this study is $5.85M which comes from the Ponemon 2014 Cost of a Breach Study: Global Analysis[2] report. The Ponemon Institute further states that the average annual cost of cyber crime in the United States can be estimated as $12.7M (according to their 2014 Global Report on the Cost of Cyber Crime[3]) and the average time to find the breach was 170 days. For the purposes of this analysis, the actual probability of a breach is assumed to be 60% (according to the 2014 Neustar report[4]) but this will vary depending upon various factors like size of company, use of a cloud network, etc. (See Appendix 1 for more details)

In the study below, the average time to find a breach is assumed to be reduced from a 170-day average to approximately 20 days, although the 20-day figure is extremely conservative. This estimate is based upon the deployment of an Ixia visibility architecture and the use of security resilience testing products, like the Ixia BreakingPoint product.

Security Breach Benefit Summary

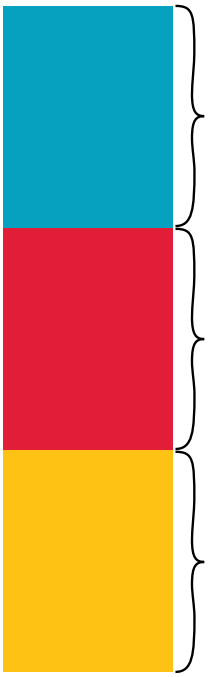
For a Fortune 1000 enterprise, there are three basic categories of benefit:

- Basic (defensive) security architecture contributions
- Visibility architecture contributions
- Resilient security approach contributions

For this example, here is the breakdown of the financial benefit for those three categories based upon the Ponemon and Ixia research:

2 http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/
3 http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/
4 http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

Financial Benefit Contributions of a Resilient Security Approach



Security Resilience Benefits

Security Resilience = $5.311M
Reduced potential legal (33%) = $796K
Reduced lost business (33%) = $587K
Cyber range training = $635K
Vendor price reductions = $308K
Testing productivity = $8K
P1 service error elimination = $280K
Upgrade testing = $31K
Other benefit (33%) = $2,666K

Visibility Architecture Benefits

Visibility Architecture = $6.502M
Reduced MTTR = $699K
Reduced potential legal (67%) = $1,617K
Reduced lost business (67%) = $1,191K
Visibility (general) = $329K
Other benefit (33%) = $2,666K

Basic Security Architecture Benefits

Basic Security Architecture = $6.413M
Strong security posture = $1,270K
Incident plan = $1,143K
Business continuity plan = $762K
Have CISO = $572K
Other benefit (33%) = $2,666K

Details for Basic Security Architecture Benefits and Potential Breach Cost Reductions

The cost of basic security architecture components for this example is estimated to be $1.469M and is based upon the purchase of the following types of equipment:

- Firewalls: traditional and next generation
- Intrusion prevention systems
- Security information and event management (SIEM)
- Threat prevention equipment
- Honey pots
- Sniffers
- Network performance monitors
- Forensic recorders
- Data loss prevention equipment
- Application performance monitors
- Dashboards

Cost details per component are provided in Appendix 2.

The following chart shows a summary of breach-related cost reductions based upon the Ponemon and Ixia research using the average annual security breach cost of $12.7M cited previously. The resilient security architecture investment results in a 73% reduction in the average cost of $12.7M for a savings of $9.271M.

The resilient security architecture investment results in a 73% reduction in the average cost of $12.7M for a savings of $9.271M.

Benefit	Amt	Qty	Init	Yr1	Yr2	Yr3
Reduced cost for breach	73.0%	$ -	$ -	$9.271M	$9.271M	$9.271M
Strong security posture	10.0%	$1.27M	$ -	$1.27M	$1.27M	$1.27M
Incident response plan	9.0%	$1.143M	$ -	$1.143M	$1.143M	$1.143M
Business continuity plan	6.0%	$ 762K	$ -	$ 762K	$ 762K	$ 762K
CISO managing security	4.5%	$ 571.5K	$ -	$ 571.5K	$ 571.5K	$ 571.5K
Reduced MTTR & analysis (see table note)	5.5%	$ 698.5K	$ -	$ 698.5K	$ 698.5K	$ 698.5K
Reduced potential of fines/legal costs (see table note)	19.0%	$2.413M	$ -	$2.413M	$2.413M	$2.413M
Reduced lost business (see table note)	14.0%	$1.778M	$ -	$1.778M	$1.778M	$1.778M
Red flagging and cyber training (see table note)	5.0%	$ 635K	$ -	$ 635K	$ 635K	$ 635K

Table 1: Security Architecture Benefit Summary for This Example (see Appendix 1 for details)

Table note: Benefits are due to the implementation of a visibility architecture and security resilience components

Post initial use testing for routine security scans is assumed to be a conservative 100 personnel hours per year. This equates to a productivity savings of $8K per year plus another $8K during the pre-deployment phase.

Details for Visibility Architecture Investment Benefit Summary (Non-Breach Related Benefits)

Cost of initial purchase is $252,0005 with recurring costs (per year) of $106,144*

Ixia Visibility Architecture benefits (for 3 years) = NPV of $320,364*

- Annual savings (per year) = $328,990*
- ROI over 3 years = 64%*

* Note: values come from Ixia customer research

Details for Security Resilience Benefits (Non-Breach Related Benefits)

Ixia BreakingPoint cost = $20K (for virtual edition)

Typical cyber range cost = $30K (for virtual environment)

BreakingPoint NPV contribution for 3 years = $680K

- Evaluate true product effectiveness of security components (IPS, firewalls, etc.) = 30% reduction in component effectiveness for firewall, next-gen firewall, IPS, and threat prevention. Negotiated an actual 22% reduction in total price of those components, which resulted in a direct $308K savings to CAPEX costs. However, the additional CAPEX and OPEX savings from not investing in the wrong equipment, or less-effective equipment, is probably substantial, even though it can't be quantified here.
- Post initial use testing for routine security scans is assumed to be a conservative 100 personnel hours per year. This equates to a productivity savings of $8K per year plus another $8K during the pre-deployment phase.

5 See Appendix 2 for a breakdown of costs.

- Vulnerability testing (reduced chance of a breach by configuration testing)
  - Initial deployment – On average, Ixia engagements find that 25% of customers have a potential priority 1 network service error (P1) breach waiting to happen. The cost of downtime is assumed to be 50 minutes at a generic cost of $5.6K per minute which results in $280K. It is assumed that a P1 error was found in this analysis.
  - Upgrade testing – On average, Ixia engagements reveal a 10% chance that customers have introduced a P1 error during the upgrade process through a configuration error. This equates to about a $28K savings per year. This does not include Zero-Day security vulnerabilities from the upgrade patches themselves that may be found later.

Other Security Architecture Benefits

A proper security architecture allows the company to maintain full market value (as part of company valuation process). This is worth approximately 1% of company value for a large enterprise (although it could be worth more depending upon whether the company has been breached before) and can be as much as 10% for a smaller business.

We will assume 1% of the $800M revenue for this example, which is a one-time book value benefit of $8M. This benefit is split evenly across all three of the benefit components (i.e. basic security architecture, visibility architecture, and security resilience). Note, even if this benefit is neglected within this study, the payback period for the investment would be less than one year.

On average, Ixia engagements find that 25% of customers have a potential priority 1 network service error (P1) breach waiting to happen.

Detailed Results

Category	Initial	Year 1	Year 2	Year 3
Basic Security Architecture Costs	$1,501,480	$19,840	$19,840	$19,840
Equipment Purchase (Disc.)	$1,469,000	-	-	-
Personnel	$32,480	$19,840	$19,840	$19,840
Visibility Architecture Costs	$259,440	$107,384	$107,384	$107,384
Equipment Purchase	$252,000	$106,144	$106,144	$106,144
Personnel	$7,440	$1,240	$1,240	$1,240
Security Resilience Costs	$20,000	$50,000	$50,000	$50,000
Resiliency Testing	$20,000	$20,000	$20,000	$20,000
Cyber Range Training	-	$30,000	$30,000	$30,000
Estimated Security Breach Costs	-	$7,620,000	$7,620,000	$7,620,000
Total Costs	**$1,780,920**	**$7,797,224**	**$7,797,224**	**$7,797,224**
Security Architecture Benefits	$8,288,000	$9,307,000	$9,307,000	$9,307,000
Reduced Cost for Breach	-	$9,271,000	$9,271,000	$9,271,000
Arch Resilience Testing	$288,000	$36,000	$36,000	$36,000
Potential Book Value Gain	$8,000,000	-	-	-
Other	-	-	-	-
Visibility Architecture Benefits	-	$328,990	$328,990	$328,990
Total Benefits (Present Value)	**$8,288,000**	**$9,635,990**	**$9,635,990**	**$9,635,990**
Interest Rate	2.70%			
Number of years	3			
Cumulative PV	$37,195,970			
NPV	$11,786,721			
Rate of Return	49.28%			
Payback Period (Months)	6.4			
Payback Period (Months, Ultra-Conservative)	11.6			

Table 2: Security Architecture Component Benefit Summary Chart

Table Notes:

1. This study assumes an enterprise with 13,000 employees, 30+ offices, international operations and approximately $800M in annual revenues.
2. The annual cost of a breach value of $12.7M comes from the 2014 Ponemon study. Actual breach costs may be larger or smaller. Frequency of breaches depends upon many factors.
3. Analysis based upon input assumptions. Actual figures will vary based upon the level of security and visibility architecture components actually deployed and the practices and procedures for governance put into place.
4. A 60% probability of a breach is assumed based on the 2014 Neustar study but actual probabilities are based upon unique variances, as previously noted in the paper.
5. An ultra-conservative payback is provided that eliminates any book value benefit of a security architecture investment.

Conclusion

Whether network security should be a formal KPI is now being rendered inconsequential. Network security is something that must be addressed at an executive level. No organization is naturally immune from this affliction. The real problem is what do you do about network security and when do you do it? How your company handles a security attack, and especially a breach, will determine the amount of financial loss inflicted and even whether your company can stay in business after such an attack.

Based upon the costs and benefits collected (both tangible and intangible) for a security architecture investment, a generic business case using a net present value calculator was created. The financial analysis shows that a minimal investment of $1.78M yielded an NPV of $11.8M over three years. Alternatively, the annual cost for a cyber crime in the United States could have resulted in a $12.7M cost to the company. By actually investing in security improvements, this example shows that the company not only reduced the costs of a breach, but also reduced the chances of a breach and improved company value by $11.8M. As an added bonus, the payback period for this investment is only 6.4 months. Even if the book value benefit for a network security investment is eliminated, the payback period for this investment is less than one year.

Network security is something that must be addressed at an executive level.

This example was for a large (Fortune 1000) business and should be representative of a company with 10,000+ employees and over 30+ remote sites. The same strategies are applicable to smaller companies though and are probably even more important. Not investing wisely in security and visibility affects your ability to recognize and mitigate security attacks and can destroy large portions of your profits. For smaller companies, a single breach can actually jeopardize the existence of that business.

In addition to the positive NPV, there are several key takeaways. First, by combining a visibility architecture with your security architecture, you can quantify and use that value as part of your analysis. The visibility architecture has an inherent value. In this case, it was approximately $329K in annual net value. The visibility architecture also contributed to a

It is very important to explore the costs and benefits associated with security architecture investments and the ramifications of each component.

reduction in the cost of a security breach. This was illustrated in terms of a faster diagnosis for breach analysis and mean time to recovery. Ixia customers have experienced up to 80% reductions in their MTTR by deploying a visibility architecture. The actual value of the MTTR will depend upon the level and depth of visibility components deployed in the network.

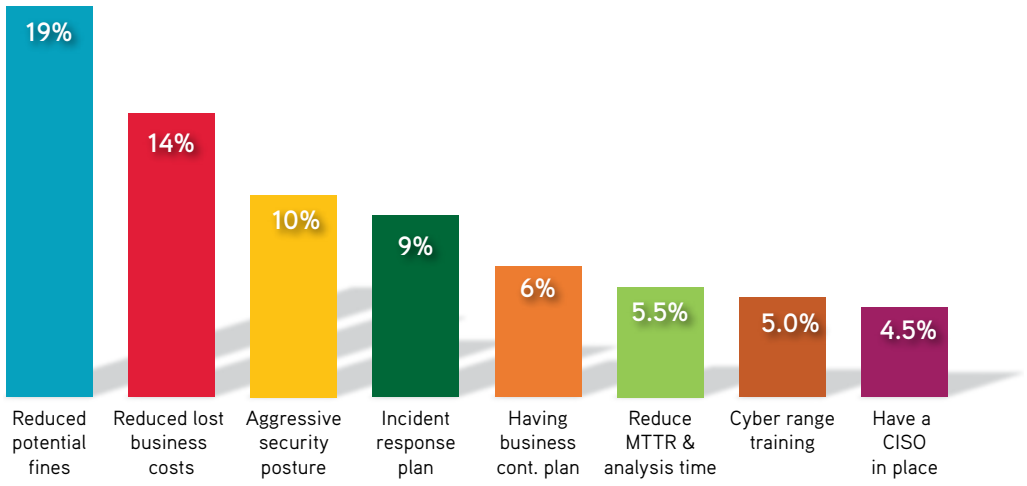
In addition to the positive impacts of integrating a visibility architecture with the security architecture, there are additional financial impacts that can be realized due to adoption of a security resilience approach. This generated an NPV of approximately $680K over the 3 year life cycle.

Another way of looking at these first two points is that your business could potentially realize the following savings, based upon your visibility and security architecture deployments, and whether you take a purely defensive security approach or combine it with security resilience. Security resilience benefits can be briefly summarized as follows:

- Reduce your CAPEX for security purchases:
  - Some equipment costs can potentially be reduced up by 20-30% by using documented, independent performance analysis testing results
- Reduce your OPEX for network security deployments:
  - You can potentially reduce the MTTR of initial breaches and breach remediation by up to 80% by integrating a visibility architecture with your security resilience design
  - Resilience testing can reduce the chance of Priority 1 defects by 25%

Finally, as the following chart shows, security improvements can not only reduce your breach chances, but reduce the actual costs of a breach that you would otherwise incur. This reduction can be as much as 73%.

Reduce the cost of a breach by 73%



The next step is for you to conduct your own analysis specific to your company and security architecture to discover the net present value of a network security investment. Just because you invest $100M to $200M annually on security doesn't mean you'll be secure. You need to make the correct investments.

Appendix 1 – The Costs and Benefits of Network Security

This analysis will focus on the resilient security approach. It is very important to explore the costs and benefits associated with security architecture investments and the ramifications of each component. Data for this analysis comes primarily from public Ponemon research as well as Ixia conducted research. We provide only a quick review of the cost and benefit items here. Details can be found in the reference: Convincing Your CFO Why Network Security is Important[6].

As we dive into breach costs, typical individual cost elements for an enterprise are summarized as follows:

- Breach investigation
- Loss of revenue
- Reputation damage
- Fines
- Purchase of identity protection service for compromised customers
- Fraud liability for compromised accounts
- Breach insurance costs (current and future)
- Loss of company IP
- Extortion costs to ransom IP back
- Hidden breach costs
- Specific business cost impacts, i.e. multipliers or additional costs of doing business (size of your business, geographic location, industry sector, international operations, use of cloud services, and vertical market impacts)

It is very important to explore the costs and benefits associated with security architecture investments and the ramifications of each component.

6 http://info.ixiacom.com/2015-Q2-CFO-ebook-sign-up.html

According to the 2014 Ponemon Institute 2014 Cost of a Breach Study: Global Analysis[7] report, the average cost of a data breach increased in 2013 to be 15% larger than in 2012, with an average of $3.5M per breach worldwide. The USA had the total highest average cost for a breach, which was reported to be $5.85M.

Other useful data included in the report is as follows:

- The worldwide average cost per lost record was $145
- The average cost per lost record for the USA, which was the highest, was $201 per record; Germany had the second-highest costs at $195 per record.
- India had the least-costly breaches at $51 per record and Brazil was the second-lowest at $70 per record
- India had the most breaches due to system glitches, while the UK and Brazil suffered the most breaches due to human error
- The main threats appear to be malicious code and then sustained probes
- 38% of companies have a security structure to protect their IT infrastructure and 45% have a strategy to protect their information assets

In regards to breach investigations, the FTC states that the average time to remediation is 45 days, which includes investigation as well as implementation of network fixes. Remediation costs can run up to 10% to 15% of annual company revenues, depending upon the size and scope of the breach.

When analyzing revenue loss, there are two components – short- and long-term. Short-term revenue loss results from the duration of the attack and/or breach. Examples of this include the loss of ecommerce revenue during a DDoS attack, loss of physical equipment that must be replaced, and loss of productivity. One estimate from a 2011 Cost of Data Center Outages: Sponsored by Emerson Network Power study[8] puts the estimated ecommerce financial losses of a typical DDoS attack at $5,600 USD per minute while the data center is down. However, top e-commerce sites like Amazon.com could lose as much as $1M per minute.

Another data point from a creditcard.com survey[9] suggests approximately 45% of consumers will "definitely not" or "probably not" shop at breached retailers. So, there is a quantifiable long-term customer confidence issue once a breach is reported. Breaches often result in company reputation damage. You can typically quantify reputation damage through corporate stock price decreases and market share reductions.

Within the United States, the FTC will oversee general enterprise security breaches and enforce federal laws. While fines vary, an estimate of $200 per record can be used as a general figure. The SEC can also become involved in corporate breach investigations. Failure to report the information to the SEC can create financial concerns for the business including de-listment from stock exchanges and fines levied by the SEC.

7 http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/
8 http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white papers/data-center-costs_24659-r02-11.pdf
9 http://www.creditcards.com/credit-card-news/shopping-after-breach.php

The following chart provides a summary of cost approximations for a typical financial analysis.

Cost Sources per Breach	Generic Cost Figure for This Analysis
Breach investigation	$500 per hour for 8 hours for 20 days
Breach remediation	Average MTTR to fix problems = 45 days
Loss of revenue	$5.6K per minute for average of 54 minutes for short term losses $141 per record stolen for long-term losses
Reputation damage	~15% drop in stock price short term ~8% drop in stock price for 1 year
Fines	Assume $200 per record for the FTC Assume $100-150 per record for HIPAA Assume $500K for state where incorporated
Purchase of identity protection and notification service for compromised customers	$20 per record (reporting & identity protection)
Fraud liability for compromised accounts	$0 (assume non-PCI regulated company)
Cyber insurance policy costs	$20K per million
Loss of company IP	$6.3M per large company breach
Extortion costs to ransom IP back	$300 per infected computer
Hidden breach costs	300 hours per year, assume 5 year duration
Specific business-dependent costs	Unknown (varies)

Table 3: Security Breach Cost Component Summary Chart

The reason for including a visibility architecture is that you can't accurately respond to security attacks and breaches if you can't see and detect them in the first place.

The second part of the cost/benefit analysis is to accurately document the benefits that your project will create for the business. The assumption in this financial analysis is that a proper security architecture will also include a visibility architecture, so those benefits will be documented below as well. The reason for including a visibility architecture is that you can't accurately respond to security attacks and breaches if you can't see and detect them in the first place. A visibility architecture is critical to the assumption, especially as over 2/3 of breaches are not discovered by the victimized business themselves. According to the 2014 Trustwave Global Security Report[10], most victimized companies are informed by customers, partners, or government authorities that they have been breached. More details about visibility architectures and their benefits can be found at www.ixiacom.com/solutions/visibility-architecture and also in the Ixia eBook How to Secure Your Network Throughout Its Life Cycle[11].

Benefits will obviously be more specific to your company, rather than general in nature. However, some generalizations can be made. In the following business case information, we have used real-world data collected from interviews with Ixia customers or documented sources.

Typical benefits for investing in network security include the following:

10 https://www2.trustwave.com/GSR2014.html?utm_source=redirect&utm_medium=web&utm_campaign=GSR2014

11 http://info.ixiacom.com/Secure_Network_Through_Lifecycle_Website_Download.html

- Limited financial and IP exposure during an attack
- Ability to demonstrate due diligence for FTC investigations and regulatory compliance
- Vettable policies and procedures that will limit C-suite liability (both financial and criminal)
- Cost savings from visibility architectures due to faster threat detection, improved root cause analysis, faster MTTR, and network optimization
- Equipment vendor evaluations and SLA validations that can improve network security and lower your architecture costs at the same time
- Protection of company valuation

While breaches may not be completely prevented, the equipment and methodology can be used to thwart the effectiveness of a breach and limit the financial and IP exposure during an attack. Research from the 2014 Ponemon Institute "Cost of a Breach Study: Global Analysis" study shows that companies that had an aggressive security posture had a 10% cost reduction per record for the breaches that did incur. The study also found that if the same company had a CISO to coordinate network security functions, then the cost of a breach could be reduced by another $6.59 per record, or about another 4.5%.

Also according to the Ponemon 2014 Cost of a Breach Study, approximately 57% of the cost of a breach in the United States is due to lost business. This is approximately $3.3 million out of the average $5.85 million of the cost for a breach and is due to abnormal customer churn, reputation loss, and diminished goodwill. Ixia believes that the scope of this category can be reduced 25% due to achieving a faster MTTR with the introduction of a visibility architecture, greater network visibility, a reduced number of days required to see abnormalities (i.e., attacks), proper resiliency testing, and the use of other technology like application and threat intelligence. By multiplying 25% times the 57% stated above, this results in an additional reduction of a breach cost by up to 14% per record per breach.

Ongoing personnel training will also produce tangible results to mitigate breaches. It's one thing to talk about incident response, it's another to actually practice recognizing and responding to simulated real-world threats. This type of training naturally makes security personnel better at correctly identifying threats and better (faster) at responding to threats. Ixia research has found that training, such as cyber range training and red flag training can reduce financial costs (due to a faster MTTR and reduced network downtime) by up to 5% per breach.

By documenting your security architecture, following regulatory guidelines (FTC, HIPAA, foreign standards, etc.), and documenting mitigation plans (as suggested in the Ixia eBook How to Secure Your Network Throughout Its Life Cycle[12]), you will be able to severely limit, if not eliminate, any chance of regulatory fines or incarceration. These governing agencies are primarily assessing punitive damages based upon negligence and fraud. The fact that you have been breached doesn't mean you will be fined. It's the lack of making a serious attempt to prevent a breach that is the problem. By creating and documenting your architecture and plans, you will almost always be able to demonstrate due diligence for FTC investigations and regulatory compliance.

This means that you can actually prevent the $1M average fine that was documented in the previous cost section, meaning that you can remove most, if not all, of this line item from your financial analysis for this activity. In addition, while consumers can still sue you for the breach of their personal information, you will also have a strong legal argument in court to severely limit any court judgments against your company by showing due diligence. Unfortunately, there will always be a risk here as some court settlements may be influenced more by emotion rather than facts. In addition, if it can be proven that the data was used for unlawful purposes by the attacker, then there is always the possibility of real damages to the affected parties which naturally figures into legal judgments. At the same time, this is a definite reason to have some sort of cyber insurance policy that can offset this risk.

By documenting your security architecture, following regulatory guidelines (FTC, HIPAA, foreign standards, etc.), and documenting mitigation plans, you will be able to severely limit, if not eliminate, any chance of regulatory fines or incarceration.

According to the Ponemon 2014 Cost of a Breach Study, approximately 27% of the cost of a breach in the United States is due to post data breach activities. This is approximately $1.6 million out of the average $5.85 million of the cost for a breach and is due to helpdesk activities, investigation, remediation, legal fees, identity protection services, and regulatory interventions. Ixia believes that the scope of this category can be reduced up to 75% by using proper policies, procedures, and investigation tools that will limit the chance of significant fines and legal costs. The activities just stated will go a long way to demonstrate due diligence to protect PII. By multiplying 75% times the 25% (reducing the 27% stated above slightly to provide a fudge factor), this results in the further reduction of breach costs by up to 19% per record per breach.

These policies and procedures should also be linked to your business continuity plans. If your network, or part of the network is compromised, then you need to have a plan for this. The 2014 Ponemon report showed that by coordinating your network security processes and procedures with business continuity management resulted in a reduced cost per record of $9. For the USA, this equates to another 6% reduction in the cost of a breach. The study also showed that having an incident plan in place could reduce the cost of a breach by another 9%.

A visibility architecture will add additional cost savings to your organizations. While these costs aren't directly attributable to security improvements, by implementing a visibility architecture to augment the security architecture, you will get "pull through" cost savings that are quantifiable and can become considerable in financial terms. The main areas of this additional costs savings are due to a monitoring faster mean time to diagnosis and MTTR, along with network optimization.

Many customers experience an improvement in root cause analysis times. Ixia's experience from our customers has shown that an up to 80% reduction in MTTR is definitely possible. What used to take them 5 days can be reduced to 1 day or less. The faster MTTR can help reduce the cost of a breach by up to 5.5% per record per breach.

12 http://info.ixiacom.com/Secure_Network_Through_Lifecycle_Website_Download.html

Another way to save costs and demonstrate a return on investment in your security architecture is to evaluate prospective vendor equipment and any proposed service level agreements (SLAs) before you buy them. One of the key secrets to network security is not to focus on buying more equipment, but to buy the right kind of equipment that works like it should in your particular network. Vendor data sheets often have inaccuracies or generalizations, which means that the equipment will not work as specified in your network for various reasons (the architecture is different, data sheet specs are often from lab environments and not the real world, etc.). Testing results can be used to negotiate product discounts anywhere from 10% to 30%.

One of the key secrets to network security is not to focus on buying more equipment, but to buy the right kind of equipment that works like it should in your particular network.

Use of third-party test gear to evaluate the security effectiveness, performance under load, and the product vulnerabilities of your devices (firewalls, next-gen firewalls, IPS, load balancer, data loss prevention, storage solution, etc.) can be very effective. Network testing has been used to perform such tests for customers and found that this evaluation process can make customer networks up to 10 times more effective against DDoS attacks by helping security architects optimize their network configurations and choice of DDoS suppression equipment.

Network security investments won't necessarily add to the valuation of a business but lack of investments can definitely detract from the company value. Ixia believes that this range of value is approximately 1 to 10% of annual company revenue. The smaller the company, the more important the value that network security brings. This is due to several factors:

- Less annual revenue to absorb the short term and long term costs of a breach
- Less ability on the part of a small company to counteract the negative effects of a security breach to the company brand, i.e. companies with stronger brands can fend off the public relations concerns better
- Smaller businesses typically have fewer (and therefore more business critical) customers. If the smaller business is hacked and this leads to the hacking of a larger businesses that is one of their customers, the breach could open up the smaller business to lots of expensive lawsuits and damage the ability of the smaller company to get future contracts.

A proper security architecture allows the company to maintain full market value (as part of a company's valuation process) because the following items can be so significantly mitigated:

- Stock price reductions after a breach is disclosed – Could be devalued by 8% or more for a year
- Brand value – Can drop between 17 to 31% according to the Ponemon Institute report (2011 Reputation Impact of a Data Breach[13])
- Customer churn – Contributes to 57% of breach losses for lost business (due to abnormal customer churn, reputation loss and diminished goodwill) per the 2014 Ponemon Cost of a Breach Study[14]
- Intellectual property loss – Loss of competitive edge as other companies get your hard earned technology for free
- Loss of business focus – Financial and human resources (including executive attention) are diverted to focusing on repairing reputation damage, regulatory investigations, and litigation instead of running the business

13 http://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf
14 http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

This company book value is approximated at 1% of company annual revenues for a large enterprise (although it could be worth more depending upon whether the company has been breached before) and can be as much as 10% for a smaller business. We will assume 1% of the $800M revenue for the example in this study, which is a one-time book value benefit of $8M.

The following chart provides a summary of cost approximations for this section.

Benefit Sources	Generic Benefit Figure for This Analysis
Aggressive security posture (Source = 1)	10% cost reduction per record per breach
Having a CISO (Source = 1)	4.5% cost reduction per record per breach
Business continuity management (Source = 1)	6% cost reduction per record per breach
Incident response plan (Source = 1)	9% cost reduction per record per breach
Reduced MTTR and analysis time (Source = 2)	5.5% cost reduction per record per breach
Reduced potential of significant fines (Source = 2)	19% cost reduction per record per breach
Reduced lost business costs (Source = 2)	14% cost reduction per record per breach
Cyber range training (Source = 2)	5% cost reduction per record per breach
Security system testing (Source = 2)	10% to 30% decrease in certain security tool costs 25% chance that a P1 failure is avoided
Increased company book value (Source = 2)	1% to 10% of annual company revenue

Table 4: Security Architecture Component Benefit Summary Chart

Table notes:

Source 1 = 2014 Ponemon Institute "Cost of a Breach Study: Global Analysis"

Source 2 = Ixia independent research

Appendix 2 – Financial Example Details

The following items were used in the net present value analysis:

Visibility Equipment Cost Estimate Summary = $252K (discounted)

Equipment type	Quantity	Cost per Item	Total Cost
In-line tap	2	$20K	$40K
Out-of-band tap	40	$800	$32K
Network packet broker (core)	1	$90K	$90K
Network packet broker (remote)	5	$18K	$90K
Total costs			$252K

Table 5: Visibility Architecture Component Cost Estimate

Security Equipment Cost Estimate Summary = $1.469M (discounted)

Equipment type	Qty	Cost per Item	Total Cost
Traditional firewall	4	$50K	$200K
Next-gen firewall	4	$75K	$300K
IPS	4	$50K	$200K
IDS	0	$50K	$0
SIEM	1	$100K	$100K
Threat prevention	4	$75K	$300K
Honey pot	1	$10K	$10K
Sniffers	4	$1K	$4K
Network performance monitor	4	$75K	$300K
Forensic recorder	1	$100K	$100K
Data loss prevention	1	$75K	$75K
Application performance monitor	1	$75K	$75K
Dashboards	1	$50K	$50K
Installation/professional services	1	$10K	$10K
Total costs			$1,749,000
Discounted total costs (see table note)			$1,469,000

Table 6: Security Architecture Component Cost Estimate for a Single Data Center

Table note: 20% discount applied to firewalls, IPS, threat prevention, network performance monitors, and application performance monitors based upon product effectiveness testing.

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127

915-3531-01 Rev. A, April 2015