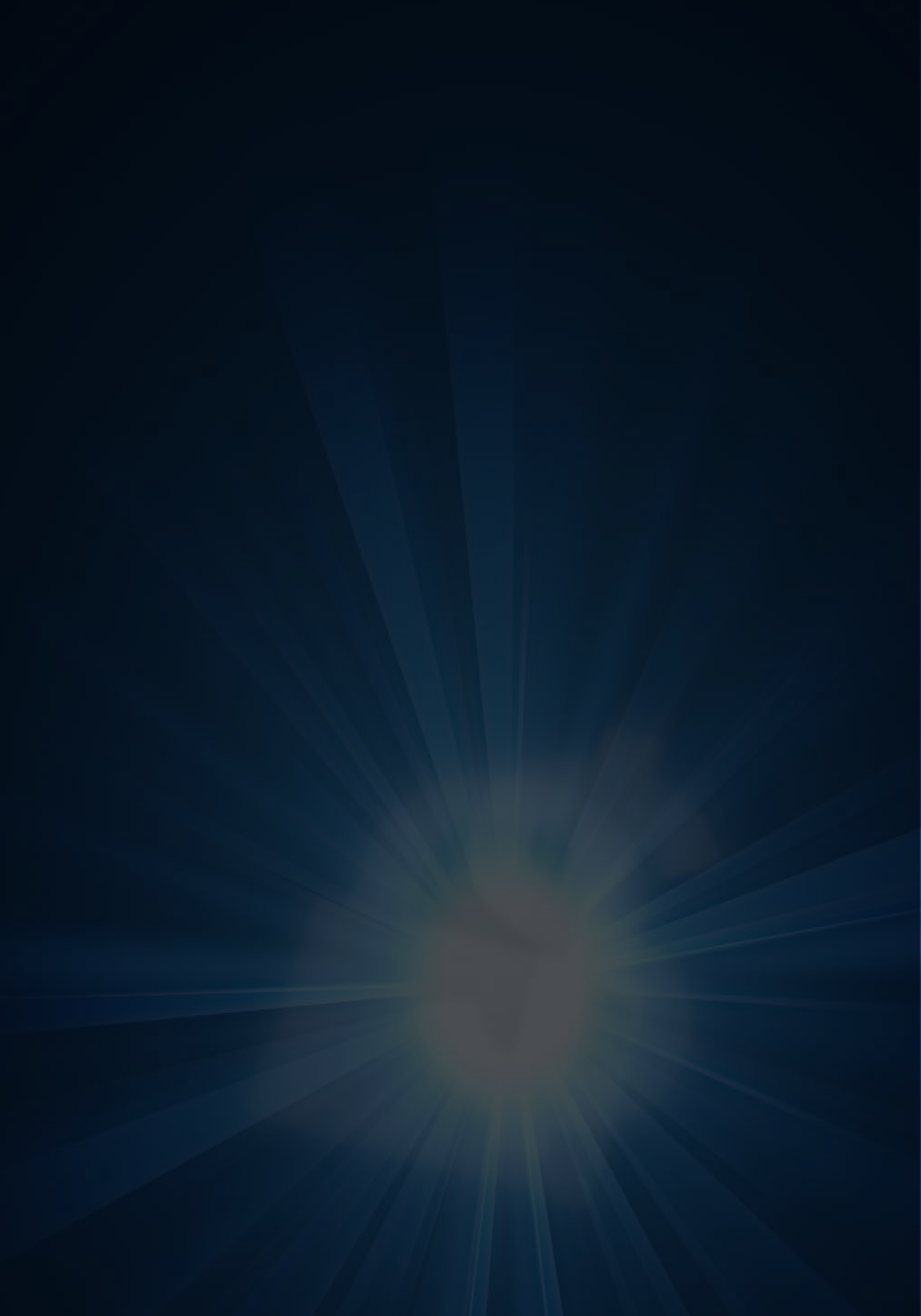
Convincing Your CFO That Network Security Is An Investment

by Keith Bromley | First Edition

ixia



The information herein is furnished for informational use only, is subject to change by Ixia without notice, and should not be construed as a commitment by Ixia. Ixia assumes no responsibility or liability for any errors or inaccuracies contained in this publication.

Note: Additional research material provided by Tim O'Neill.

Contents

Executive Summary 6

Chapter 1: How You Handle Security Attacks and Breaches Will Dictate Your Company's Liability and Viability 7

Chapter 2: Different Approaches to Network Security Investment 13

- Resilient Architecture Approach 15
- Defensive Architecture Approach 16
- Regulatory Compliance Approach 16
- Best Effort Approach 17

Chapter 3: Cost Summary for Breaches 19

- Breach Investigation and Remediation 23
- Loss of Revenue 25
- Reputation Damage 26
- Fines and Reporting 29
- Breach Notification and Identity Monitoring 33
- Fraud Liability 34
- Insurance Costs 35
- Intellectual Property Loss 36
- Extortion Costs 37
- Hidden Breach Costs 37
- Specific Business-Dependent Costs 38
- Cost Summary Chart 41

Chapter 4: Benefits & ROI for Investing in Security 43
Limited Financial and IP Exposure during an Attack 45
Due Diligence for FTC investigations and regulatory compliance 46
Vettable Policies and Procedures 48
Faster Threat Detection and Root Cause Analysis due to Increased Visibility 49
Additional Visibility Architecture Cost Savings 52
Evaluate Vendor Equipment Before you Deploy It 53
Protecting Company Valuation 55
Benefit Summary Chart 58
Chapter 5: Demonstrating the Financial Business Case for Network Security 59
Example Analysis – Fortune 1000 Enterprise 61
Chapter 6: Conclusion 71

Executive Summary

Network security for today's enterprise is an important concern. Everyone knows this – from the network engineer to the Chief Executive Officer (CEO). At the same time, the enterprise C-suite has a myriad of other concerns that they need to address daily. It's one thing to make an investment, it's another to make the correct investment. Indiscriminately throwing money at a problem rarely creates a solution, you need to make wise investments.

So, how can you get their attention, especially your Chief Financial Officer's (CFO) attention, secure the budget you need, and keep your network as secure as possible? This book discusses the fundamental approaches to network security investments and how you can start a discussion with executives on this topic.

Specifically, there are three fundamental areas examined within this book:

- An understanding of U.S. Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), and criminal implications to a business related to network security
- The typical costs and benefits associated with security architecture investments, along with the ramifications of each one
- A net present value (NPV) analysis for a representative business

The last section is designed to give you the real-world answers you need to provide an example financial analysis that can be used to demonstrate the net present value of a network security investment to a CFO. In the end, this is what your CFO wants to see – a solid financial benefit for the capital investment.

Chapter 1:

How You Handle Security Attacks and Breaches Will Dictate Your Company's Liability and Viability

Security attacks on enterprise networks have now become a way of life. There are a multitude of publications that can support this:

- Verizon 2014 Data Breach Investigations Report[1]
- Ponemon Institute 2014 Cost of Data Breach Study: Global Analysis[2]
- Symantec Internet Security Threat Report 2014[3]
- 2014 Trustwave Global Security Report[4]
- Ponemon 2014 Data Breach: The Cloud Multiplier Effect report[5]
- Online Trust Alliance 2014 Data Protection & Breach Readiness Guide[6]
- 2014 The Danger Deepens - Neustar Annual DDoS Attacks and Impact Report[7]

As the reports show, attacks are imminent for an enterprise. No organization is naturally immune – we all know this. At the same time, 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.

So, how do you convince the C-suite that the network security problems need to be fixed now and, more importantly, that you have the correct solution for your business? This document will show in general what you need to know and do to get their attention, and keep it.

One note, there are business differentials that come into play that may not be accounted for, or may not be applicable to your line of business, which makes the business case presented here somewhat general in nature. You'll

[1] http://www.verizonenterprise.com/DBIR/2014/

[2] http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

[3] http://www.symantec.com/security_response/publications/threatreport.jsp

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

[5] http://www.infosecurity-magazine.com/news/ponemon-cloud-apps-can-triple-data/

[6] https://otalliance.org/resources/2014-data-protection-breach-readiness-guide-overview

[7] http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

need to address those individual variances on a case-by-case basis. At the same time, the business case presented here should provide a very good starting point for any business analysis.

For this discussion, we will build a financial analysis based upon the following four-step approach as follows:

1. Determine who your exact audience is and what their key concerns are
2. Understand what your company's approach is to security
3. Perform a cost/benefit analysis specific to your company
4. Build a financial, net present value (NPV) business case around that cost/benefit analysis

Some examples of individual variances that you may also want (or need) to address in your specific business case include the following:

- Size of the business
- Geographic location
- Industry sector (which can have significant variances)
- International operations (have additional disclosure and liability costs)
- Use of cloud services (this increases the likelihood of a breach by 3 times)
- Unique variances for healthcare entities
- Unique variances for retail and ecommerce entities
- Unique variances for utilities, defense contractors, and core public infrastructure
- Unique variances for network security vendors, consultants, and government agencies

In general, the first thing you need to do is to find/target a champion within your C-suite. You need to know who you're trying to convince and what keeps them up at night. In the end, it may simply come down to some sort of financial analysis (e.g., NPV > $$), but you'll already know that by doing your research up front. If something more than financials are involved, then you'll definitely need to know what pain points can be solved by your proposal and make sure that you and your champion can articulate those benefits and any opportunity costs for inaction.

It is also important to understand the worldwide political climate. A fundamental shift is taking place for various geopolitical entities across the world. One trend is that individual privacy has become an important topic. European governments have been leading an effort to tighten up information spying and the release of personally identifiable information (PII) for European citizens. North America is moving in a parallel direction, although at a much slower pace. The driver for North America is less about political fallout for breaches of PII and more about the economic losses to the individuals. This has spilled over into increased pressure for the Federal

Trade Commission to begin assessing fines (potentially large fines) to corporations that don't adequately protect the financial information and PII of their customers and employees. Those customers expect a degree of privacy and if corporations don't protect that information voluntarily, then the public is demanding that there needs to be punitive action as retribution.

The Securities and Exchange Commission is also investigating whether they need to provide more oversight and regulations regarding the breach of PII. For the C-suite, this would translate to concerns of "breach of fiduciary responsibility" and whether the SEC might decide that they, the C-suite, did not provide adequate and reasonable "fail-safes" to avoid the exposure of PII. While most companies will not make the nightly news for security breaches, they are generally accountable to the SEC. This means that the CFO will not enjoy the next Board meeting after showing 'material weakness' via breach or audit, as this is an indemnity and a liability issue that can directly impact the company's viability.

In another new trend, the public retribution referred to previously doesn't just roll downhill anymore, meaning the CEO can't just fire a couple people in IT and the matter is resolved. As an example for the United States, the criminal justice system (FBI and police) along with civil authorities and organizations (like the FTC and Payment Card Industry) can become involved in security breach investigations. Once they become involved, the matter becomes public. If incidences aren't reported correctly, then criminal charges can be filed against the C-suite along with personal civil liabilities. In fact, there are laws currently (2014/15) being discussed in the United States Congress that, if passed, will make it far easier for the FBI to investigate and criminally indict business leaders for security breaches exposing PII.

In addition to personal liability, the corporation as an entity will be held liable as well, usually with fines from the FTC, SEC, state governments, and/or Payment Card Industry (PCI) along with civil lawsuits. This leads to brand damage to the corporation that can follow corporations long after the breach is repaired.

These privacy and liability trends lead to a 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, it can affect the reputation of the C-suite and board of directors

These key points are becoming pain points for the C-suite that you should address in your solution proposal. It is also important to note that there are other improvements from network security investments. These include internal efficiencies, increased employee productivity, and increased company book value. Most of these soft figures are difficult to quantify and won't be addressed in this discussion, but they might be applicable to your analysis.

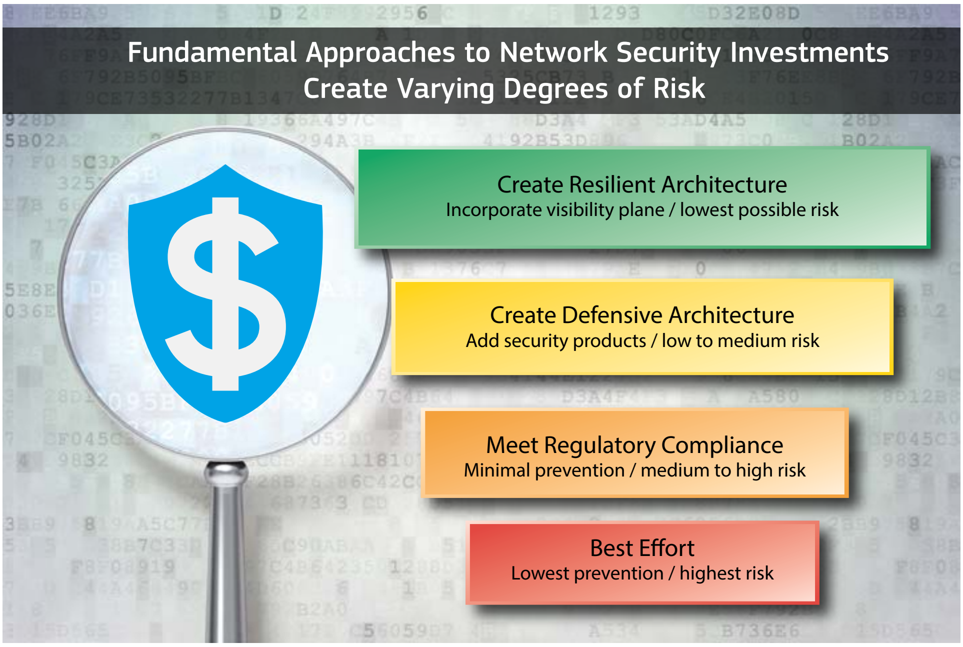
Chapter 2:

Different Approaches to Network Security Investment

The second aspect of your business case is to clearly understand what your company's philosophical approach is towards network security. This will allow you to grasp instantly how difficult your business case task will be.

There are four fundamental approaches to network security investments that offer varying degrees of risk:

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


Fundamental Approaches to Network Security Investments Create Varying Degrees of Risk

Create Resilient Architecture
Incorporate visibility plane / lowest possible risk

Create Defensive Architecture
Add security products / low to medium risk

Meet Regulatory Compliance
Minimal prevention / medium to high risk

Best Effort
Lowest prevention / 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 components with a visibility architecture 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).

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 the network is secure.

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. In addition, you'll need to routinely assess the network to see how it's performing and audit your security logs and equipment for any evidence of break-ins or malfunctions.

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.).

Defensive Architecture Approach

For the next option, the defensive security architecture approach should involve a formal security architecture plan. This includes products and processes. The primary focus here is often 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.

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 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 probably deployed point solutions for firewalls and intrusion prevention systems (IPS) to counter malware and typical denial of service (DoS) threats. Lack of a coherent plan though will usually mean that you have security holes that most hackers will be able to break through. That being said, the results for the "meet regulatory compliance" approach will obviously be less spectacular than a prevention approach, but 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 mean time to repair (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 your task is simplified. There's no need to perform a financial analysis, unless you think your champion really wants (and has the ability) to change that philosophy.

Fundamental Approaches to Network Security

Approach	Best Effort	Regulatory Compliance	Defensive	Resilient
Basic Security (FW, IDS, Sniffer)	●	●	●	●
Simple Monitoring (SPAN, crash cart)	●	●	●	●
Meet Regulatory Compliance (logging, policy)		●	●	●
Application Monitoring			●	●
Advanced Security (NGFW, SIEM, IPS)			●	●
Security Procedures in Place			●	●
Out-of-Band Monitoring (tap, NPB, tools)			●	●
Virtual Data Center Monitoring (virtual tap, NPB, tools)			●	●
In-Line Monitoring (bypass tap, NPB)				●
Resiliency Testing				●
Cyber Range Training				●
Advanced Processes (Network Security Life Cycle)				●

Chapter 3:

Cost Summary for Breaches

The third thing you need to do is to perform a cost/benefit analysis. To convince to your C-suite, it is very important to explore the costs and benefits associated with security architecture investments and the ramifications of each component.

There are resources available to help you analyze your business for breach costs. Some of these are as follows:

- Symantec Cost of a Breach calculator[8]– provides a basic cost summary but doesn't include a lot details
- 2014 Ponemon Institute "Cost of a Breach Study: Global Analysis"[9]
- Zurich American Insurance Corporation, Tim Stapleton, 2012, "Data Breach Cost – Risks, costs and mitigation strategies for data breaches"[10]

According to the 2014 Ponemon Institute "Cost of a Breach Study: Global Analysis" report, the average cost of a data breach increased in 2013 to be 15% larger than in 2012, with an average of $3.5 M per breach worldwide. The USA had the total highest average cost for a breach, which was reported to be $5.85M. The report includes additional important figures – such as the worldwide average cost per lost record was $145. The average cost per record for the USA, which was the highest, was $201 per record. Germany had the second-highest cost at $195 per record.

Other useful data included in the report is as follows:

- Companies that had an aggressive security posture had approximately a 10% cost reduction per record for breaches they incurred
- 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
- Having a CISO reduced the cost of a breach by $6 per record (or 4.5%)

[8] http://www.databreachcalculator.com/GetStarted.aspx

[9] http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

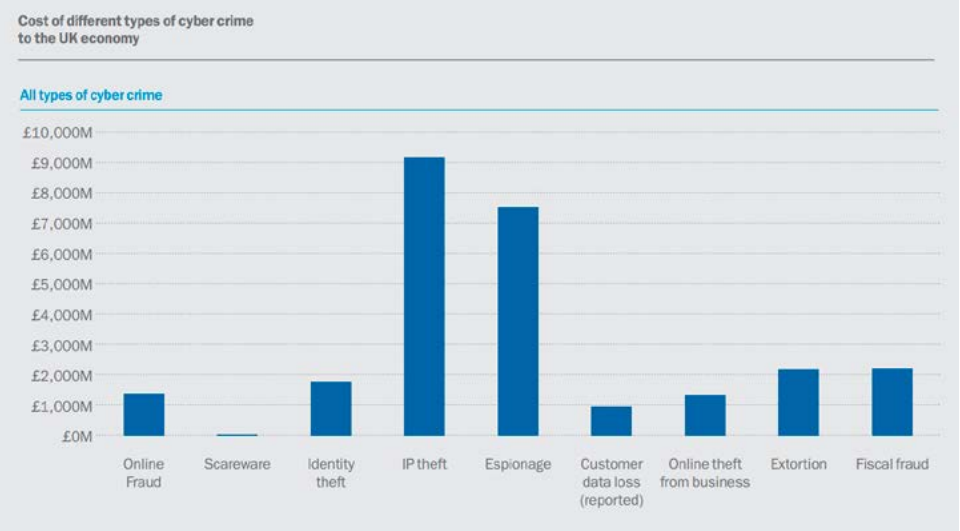
[10] http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/data breach costs wp part 1 (risks, costs and mitigation strategies).pdf

- Having business continuity management reduced the cost per record by $9 (or approximately 6%)
- Companies that had an incident response plan in place could save approximately 9%
- 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

The two main cost figures presented above, average breach cost and breach cost per record, can be used to approximate the cost of a breach to your business. However, these are very broad figures that can add up to huge numbers when applied to specific companies. When presenting the data to your executive management team, the team may not accept these average industry figures. Therefore, you may want to itemize your cost approximations so that you can provide better data transparency during your financial analysis.

In regards to the type of data stolen and costs associated with each threat category, a report titled "The Cost of Cyber Crime,"[11] written by The Detica Limited Research group and the United Kingdom Cabinet Office, showed that the average annual cost of cyber crime for the UK is £27 billion. The largest components are intellectual property (IP) theft and espionage, which contribute £9.2 and 7.5 billion, respectively. The chart below comes from the report and shows the different breakdowns. This chart may be useful as some executives aren't aware of the size of IP and espionage threats that exist. Those executives tend to just think it's mainly DoS attacks affecting ecommerce, website defacement, or credit card data loss.

[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf



Source: 2011 Cost of Cyber Crime Report, by The Detica Limited Research group and the United Kingdom Cabinet Office

The typical individual cost elements of a breach for an enterprise is 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)

Let's investigate each category further. As a general note, the figures and facts used to document individual items below will primarily focus on USA figures as these should be the most costly, and will be based upon the 2014 Ponemon report data (where applicable).

Breach Investigation and Remediation

Once a breach is suspected or detected, it will need to be investigated. If possible, it is typically recommended to use an external consultant to help perform any forensic analysis of the breach. There are a couple of reasons for this. First, the consultant should be an expert on the subject and can help you determine and remediate (if not already done) the exact threat vector used and the scope of the breach. Second, use of a third party will be helpful in the future, with external audits and lawsuits, to show that you were demonstrating due diligence to identify the breach details and conduct remediation in a timely fashion, i.e., remove any hint of negligence or incompetence that can be used in future legal, criminal, or civil proceedings.

Note: this is a very important activity. If you can't prove the exact number of records stolen, then external agencies (such as the FTC) will assume that all records have been compromised and will levy fines based upon that larger number. Each email, phone number, etc. can count as a separate record. The cost of an average fine is estimated to be $200 per each record, so not understanding the exact number of records exposed could become very costly, very quickly.

One interesting note from the Ponemon report was the definite need for breach investigation, especially before you announce. You obviously need to report a breach (according to applicable laws) when it happens, but the study results suggested that you investigate the breach and ramifications in depth before announcing it so that you can be very clear in what you say to regulating authorities and the public. You don't want to understate, overstate, or have to restate the scope and size of the breach. The 2010 Ponemon report on breach costs found that announcing it without knowing all of the impacts can cost about $268 per record, versus $174 per record if you take the appropriate investigation time before announcing the event. As stated before though, make sure you adhere to applicable laws or you can face other severe impacts like larger fines and potentially larger lawsuits.

According to the document "Data Breach Cost – Risks, costs and mitigation strategies for data breaches,"[12] the costs for an external consultant to perform forensic analysis of breaches can range $200 to $2,000 per hour. For this study, we will assume $500 per hour, 8 hours a day, for 20 days to conduct the analysis. If you chose to use internal resources for this activity, then use your own loaded labor rate for the appropriate role in your analysis. As a note, the FTC states that the average time to remediation is 45 days, which includes investigation as well as implementation of network fixes. Remediation costs often run up to 10% to15% of annual company revenues.

[12] http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/data breach costs wp part 1 (risks, costs and mitigation strategies).pdf

Loss of Revenue

When determining 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[13] 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 study by the Ponemon Institute and Radware (Cyber Security on the Offense: A Study of IT Security Experts from November 2012) found that the average cost of downtime is $22K per minute and the average downtime following an attack was 54 minutes, although longer attacks of up to 24 hours are not uncommon. Common targets of these attacks are retail, travel, and financial businesses.

A 2013 Avaya study[14] of mid to large companies further found that 82% of companies surveyed experienced downtime due to IT personnel making errors while making changes to the core network. Of those respondents, 80% experienced revenue loss from that self-inflicted downtime with the average company losing $140,003 per incident. The Financial sector suffered more with respondents stating average losses of $540,358 per incident. For the purposes of this study, we will use the more conservative estimate of $5.6K for the cost per minute of a security incident that shuts the network down.

Long-term revenue loss results from customer concern and customer churn. As an example, once a retailer announces that they have had a breach, customers are typically less willing to shop at that retailer for a while, maybe a long while. It often depends upon the length of time and scale of the security breach.

[13] http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white papers/data-center-costs_24659-r02-11.pdf

[14] http://www.avaya.com/usa/about-avaya/newsroom/news-releases/2014/pr-140305/

In the case of the 2013 Target Corporation (NYSE: TGT) breach, the total cost reported so far by the company is $148 million[15]. This does not include fines by regulatory entities. The cost is offset by a $38 million payout from a cyber insurance policy for a net loss of $110 million. While this loss isn't a huge direct impact to a corporation the size of Target (with annual revenues of $72.576 billion for 2013), it did create a serious public relations issue that the company is still recovering from.

Consumer confidence can be a potentially large problem. In the Ponemon 2014 cost of a breach report, the typical cost of a breach is estimated at $201 per record. This figure includes approximately $141 per record of loss due to a decreased stock price and customer churn, and can be used as a generic long-term loss figure for a financial analysis.

Another data point from a creditcard.com survey[16] 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.

Reputation Damage

Breaches often result in company reputation damage. You can typically quantify reputation damage through corporate stock price decreases and market share reductions due to loss of customer loyalty.

If we examine the Target Corporation further, their stock (NYSE: TGT) had dropped 8.5% since the breach occurred for most of 2014, assuming an average stock price of $61. Target, which has historically been a solid performer on the stock market, took about a 17.4% stock price drop within the first 3 months after the reported breach in 2013. The stock price in mid-November 2013 (November 15) was approximately $66.89 per share and dropped down to approximately $55.07 per share in February 2014 (February 5), rebounded some, and then dropped again in late May. The stock price rebounded after that to approximately $61 (where it bobbed

[15] http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/

[16] http://www.creditcards.com/credit-card-news/shopping-after-breach.php

around for most of the year) in early November (November 3, 2014). This was an approximate 8.5% drop-off of the November 2013 stock price.

At the same time, the S&P 500 was running at about the same price as the Target stock in November 2013 but was now up 9.14% from that price a year later. Using the November 15, 2014 date, this is a net rebound of approximately 9%. However, the Target stock price impact averaged across most of the year was an 8.5% drop. This means that the Target stock price 1 year later was essentially 17.5% (8.5% + 9%) below where it could, and should, have been (assuming all other things being equal). The ensuing widespread bull market surge in mid to late November 2014 propelled Target's stock over the $75 mark by the end of 2014. So, one year out, the stock price had fully recovered and had then significantly surpassed its previous price in November of 2013. The question of the long-term effects still remains. As law suits against Target continue, what will be the cost to the brand?

In a separate example, JPMorgan Chase (NYSE: JPM) announced in August 2014 that they had suffered a breach in July of 2014. PII for 76 million households and 7 million small businesses was exposed. However, the company stated that the reported information only consisted of names, email addresses, phone numbers, and addresses of account holders. Social security numbers, login credentials, and other high value information wasn't compromised. Therefore, other than a couple of dips in the stock price in August and October of 2014, there was very little other impact to the JPM stock.

For the Home Depot (NYSE: HD) breach announced on September 2, 2014, 56 million customer credit and debit card accounts and 53 million customer email addresses were stolen. The Home Depot opening stock price on September 2, 2014 was $93 per share. It closed at $89 per share on September 3, which is about a 4% drop. The stock continued to lag over the course of several days and then rebounded. It took another big dip on October 15, along with the whole market. By mid-November, the stock price had risen to $97 per share, which was an approximate 4% gain to match the DOW (DJIND) and S&P 500.

Thus, the Home Depot and Target stock price increases were probably a reflection of the general bull market sentiment and there may still be a consumer confidence problem due to the breaches. However, investors also appear to show little long-term concern for security breaches.

So, the conclusions to be drawn here for a large-scale breach (assuming all things being equal) would be the following:

- The initial ramification is a possible drop of approximately 15% in the stock price short term
- Long-term impact is a possible 8% drop on average for up to 1 year
- Full recovery is possible approximately 1 full year later

A broader examination would be required to achieve more accuracy, especially as there are other factors in play:

- Apparent consumer fatigue due to all of the recent security breaches
- Question of how much the political elections in the USA affected stock market trading in a positive direction
- There is not enough data yet to properly examine the Home Depot long-term stock impacts

- Sony stock prices need to be examined in the wake of their December 2014 breach
- A need for more investigation into the even longer-term impacts to a company's reputation due to massive breaches (i.e. what's the impact over 2 plus years)

Fines and Reporting

Due to the potential consumer damage from exposed PII and the sheer abundance of security breaches being reported, regulatory agencies are becoming increasingly involved in corporate security breaches, primarily due to privacy issues. This includes both private and public agencies. Most of the agencies will be public (state, federal, and/or international) but private agencies like the PCI exist as well. The main legal argument for government bodies to intervene in these activities relates to consumer privacy and the use of unfair and/or deceptive acts by businesses to not protect that data.

Within the United States there are multiple applicable laws and groups overseeing information privacy that have the ability levy fines. A good summary of the applicable laws is available in a report by Perkins Coie[17]. A short list of the laws is provided here:

- 47 State Data Breach Laws
- USA Patriot Act
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability & Accountability Act (HIPAA)
- Health Information Technology for Economic & Clinical Health Act (HITECH)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Federal Information Security Management Act (FISMA)
- California Data Breach Protection Act (SB 1386)
- Payment Card Industry Data Security Standard (PCI-DSS)

[17] http://www.perkinscoie.com/privacy_security

There are multiple international laws as well. A couple of the more common ones are:

- EU Data Protection Directive 95/46/EC (which most of Europe has adopted)
- Australia Privacy Act of 1988
- Australia Privacy Amendment (Enhancing Privacy Protection) Act 2012

Within the United States, the FTC will oversee general enterprise security breaches and enforce federal laws such as the Gramm-Leach-Bliley Act of 1999, Sarbanes-Oxley Act, Fair Credit Reporting act, and the Children's Online Privacy Protection Act. The Gramm-Leach-Bliley Act mandates that businesses protect the privacy of PII through administrative, technical, and physical safeguards. The FTC can levy fines and mandate federal oversight/ involvement in breach remediation activities. While fines vary, an estimate of $200 per record can be used as a general figure.

In regards to GLBA, the FTC is the primary enforcement agency but the law allows eight different federal agencies and every state to enforce the privacy and safeguards contained within it. This law has several dimensions to it. Fines up to $100K per violation can be levied against businesses. Fines up to $10K can be levied against business owners and officers per violation.

The SEC can become involved in corporate breach investigations as well and issued some basic guidelines on October 13, 2011 (summarized below) on what should be disclosed:

- Remediation costs
- Increased cyber security protection costs
- Lost revenues
- Litigation
- Reputational damage
- Description of relevant insurance coverage

Information should be filed on Form 6-K or Form 8-K. Failure to report the information can create financial concerns for the business including de-listment from stock exchanges and fines levied by the SEC. The SEC is currently considering further oversight regarding security breaches so the financial impact could become even greater if new regulations are adopted.

Other laws like HIPAA are governed by separate agencies. For instance, HIPAA is governed by the Health and Human Services Agency while the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, and the Telecommunications Act are governed by the Federal Communications Commission. Additional Federal rules can be used to govern reporting and levy punitive actions for companies doing business within the United States. An additional law is the US Executive Order 13636, which governs security practices and reporting for businesses involved with aspects of the US critical infrastructure.

Individual states and US territories have also enacted legislation to levy fines against companies that were breached due to negligence. Forty-six states and territories have laws on the books to enforce penalties for the breach of PII. As an example, California can impose their own penalties (up to $500K per incident) for breaches under the California Unfair Competition Law. Massachusetts is another active state in protecting consumer information.

For state fines, civil penalties up to $500K are possible for failures to safeguard personal data, properly dispose of such data, and to provide adequate privacy protections. If reckless or negligent activities are suspected, then criminal penalties with severe fines including up to three years of imprisonment is possible.

Other countries have also enacted laws to levy fines that will need to be accounted for. For instance, the European Union has enacted the EU Data Protection Directive of 1995, which affects the collection, processing, transfer, and export of EU-citizen information.

Specific fines by government agencies can be somewhat subjective. For instance, FTC fines can be as much as $10M, although the average settlement figure is around $1M. However, the aggregate cost is typically based upon a per-record cost for the number of records exposed. If the exact number of records cannot be determined, then (as mentioned previously) agencies like the FTC will typically assume that all records have been breached and levy a fine based upon that assumption.

Specific industry regulations apply as well. As an example, financial entities may be subject to Red Flag rules. Red Flag rule enforcement began for all businesses on November 1, 2009. This mandates that businesses that extend credit or payment terms must look for indicators of telltale signs for identity theft. Fines can range up to $3.5K per violation (each record breached can be counted as a violation) along with court costs. The FTC is the oversight agency for this compliance requirement.

The PCI is an independent organization that polices the use of credit cards and credit card data. The organization has defined its own standard, the PCI-DSS and all members must adhere to those rules. If not, the violating member can be fined. PCI-DSS fines can range between $5K to $100K per month and up to $500K per merchant. The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 require the confidentiality and security of medical information. HIPAA and HITECH fines can range from $100 per violation to a maximum of $1.5M. Up to 10 years of imprisonment is also possible in cases of negligence and fraud.

Reporting is another key requirement of almost all of the laws. Breaches must be reported and follow mandatory state, federal and international laws (SEC, FTC, HHS, EU), as well as private agencies (PCI). The triggers for reporting vary depending upon the laws.

Breach Notification and Identity Monitoring

Once a breach is incurred, two additional activities are typically required. The first is to notify all affected parties that their information has been compromised. The second activity, which may be optional depending upon specific country legal requirements, is to purchase some type of identity protection (and possibly a credit monitoring) service for all affected parties.

According to the “Data Breach Cost – Risks, costs and mitigation strategies for data breaches” report, the average cost to notify 3rd parties about a breach is between $0.50 to 5.00 per record. As another data point, a recent example with IBM records that were lost by a transportation company (called Ex Log) resulted in actual costs of $6M to notify HP’s 500,000 current and former employees about the breach of PII. This equates to a cost of about $12 per record. For this study, we’ll assume a cost of $5 per record that includes research and notification costs.

In regards to the purchase of identity protection and monitoring services for compromised customers, a typical annual retail service can cost $120 to $300 per record. This assumes a full credit monitoring service offering. You can probably safely assume a 50% cost reduction for a bulk service purchase. Another data point suggests that credit and identity monitoring services are available for between $10 to $30 per user, per year. For the purposes of this study, we’ll assume a more limited service (between $10 to $30 cost per record) and assume an average cost of $20 per record.

It should be noted that a McAfee report from 2013, The Economic Impact of Cybercrime and Cyber Espionage[18] shows that a Cambridge University survey on phishing estimated that the net cost of identity theft for an

[18] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

individual victim is $572. This cost may, or may not, be passed on to the business through lawsuits but for our purposes, we'll use the previously cited figure of $20 per record.

Fraud Liability

In the case of a breach of PII, businesses may be held liable for any fraudulent activity that results. This is more applicable to companies handling credit card information, social security information and healthcare information. Typical costs involve lawsuits and legal fees. According to the "Data Breach Cost – Risks, costs and mitigation strategies for data breaches" report, the average legal fees for specialized counsel is approximately $500K with average settlement costs of $1M per law suit. However, exact settlements vary depending upon whether extended costs to the consumer can be proved from identity theft. Between 10 to 40 times the cost of the actual loss to a consumer can be won in a lawsuit. So a $100K consumer loss could result in a $1M to $4M court settlement.

Additional lawsuits can come from banks or other financial entities that might experience losses due to the PII breach. The reissue of credit cards can cost banks between $12 to $22 per card, so large breaches like Target and Home Depot can be expensive. According to a Wall Street Journal article[19] dated February 18, 2014, “The Consumer Bankers Association, a retail-banking trade group, estimates the cost of card replacements for its members to have reached $172 million, up from an initial finding of $153 million. The association says its member banks have replaced about 17.2 million cards at a cost per card of $10 to $15 per card with the average loss to banks amounting to $331 per debit card and $530 per credit card.” Several factors were part of that cost including the actual cost to print a new card, mailing of the cards, and additional customer service help needed.

For the purposes of this study, we will assume that the financial institutions will absorb the complete costs for credit card fraud and credit card replacements. This is not true for non-PCI-compliant companies as they will probably end up being sued by the financial institutions to recoup those costs (plus labor costs to the banks for all activities around the crisis). However, this study also covers breaches that don’t include credit card losses so we’ll exclude the item from our analysis.

Insurance Costs

One way that organizations are trying to protect themselves is to purchase cyber insurance, that is, insurance that specifically covers loss due to some sort of IP-based security breach or a physical breach/loss of equipment (e.g. laptop with critical business data). This type of investment is growing in popularity because of the increased threat and costs of breaches and that most Commercial General Liability policies don’t cover breach costs. Therefore, cyber insurance can be a decent business tool to offset some of the costs of a breach.

There are now at least 25 insurance companies offering cyber insurance. These premiums range from $10K to $35K for every $1M in coverage. The assumptions made for this study is that the average premium cost is $20K per million and the average policy size is $10M. This equates to an annual cost of $200K per year. On the positive side, once a breach is incurred, the $10M will become a financial benefit to mitigate your costs.

[19] http://www.wsj.com/articles/SB10001424052702304675504579391080333769014

Something else to keep in mind is that once you do incur a breach, you can expect that your cyber insurance premium costs for all future policies will increase, possibly significantly.

Intellectual Property Loss

Typical security breaches nowadays are motivated by financial drivers rather than the hacktivism activities that dominated in the past. Hacktivism was more focused on embarrassing the business or government rather than trying to steal/inflict monetary losses. It is now much more common that you will experience the loss of company intellectual property, which can result in the loss of competitive advantage, slower time to market, and customer churn (due to general and targeted account poaching). As an example, a PricewaterhouseCoopers study, Managing Cyber Risks in an Interconnected World[20], surveyed several industries and found that aerospace and defense respondents reported a 97% increase in hard intellectual property theft.

IP can be considered as follows: personally identifiable customer contact data and employee data, trade secrets, merger and acquisition data, business plans, etc. According to a US Department of Commerce report from March 2012, "Intellectual Property and the U.S. Economy: Industries in Focus,"[21] IP theft costs US companies between $200 to $250 billion annually.

To determine what IP theft could cost your business, there are two methods you could use. The first method is to estimate the value of your company's intellectual property. There are standard financial methodologies to do this and companies that are considering mergers and acquisitions commonly conduct this type of analysis. A second approach would be to use a generic approximation. This runs the risk of overvaluing or under-valuing your IP, but it at least gives you a starting point to work from. The 2012 Ponemon Institute's Annual Cost of Cyber Crime Study estimates the annual cost of cybercrime per company to be $8.9M. A study by NetDiligence for 2009 to 2011 came up with a figure of $3.7M per company. By splitting the

[20] http://www.pwc.com/gsiss2015

[21] http://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf

difference, you could use an estimate of $6.3M per company. We'll use this estimate in our analysis.

Extortion Costs

In the last few years, malware variants have emerged that try to extort money from individual victims. Ransomware is a general term for this type of malware that encrypts your computer and locks you out of it. Once infected, you then have to pay a ransom to get the code to unlock your computer. While this type of attack has been around since the 1980's, a new version (family) was recently released in September 2013 called CryptoLocker.

The basic process is that the victim opens up a harmless-looking attachment, which then initiates an executable file to launch a Trojan that works in the background to install a registry key and then runs an encryption program on the victim's hard drive to encrypt their files and lock the owner out.

According to "The Real Cost of Ransomware"[22] by Ian Barker, "A single gang using the Reveton Trojan[23] managed to infect more than 30,000 computers in Finland alone and over 5 million worldwide. Reveton currently charges $300, or 100 euros in Europe, to unlock the system. That amounts to a potential profit of some $800 million from this one attack."

Hidden Breach Costs

In addition to the obvious costs of a breach, there are other lesser-known breach costs that affect the business. Typical examples of this include the following:

- External public relations (PR) firm to overcome consumer-confidence problems
- Crisis management team
- Comprehensive written information security programs

[22] http://betanews.com/2013/10/23/the-real-cost-of-ransomware/
[23] http://www.f-secure.com/v-descs/trojan_w32_reveton.shtml

Breached companies will typically want to overcome any customer confidence problems using an external PR team. These teams can cost $50K or more per month.

Comprehensive written information security programs are a new trend that regulatory bodies are forcing upon businesses as part of fine settlements. These are essentially long-term (multiple year) audits to verify that the business implements and maintains the required changes to protect customer and employee PII.

This audit process often requires dedicated staff (legal, IT network, IT server, and management) to perform the audits and document the project status. This typically involves 10 to 30 people and therefore adds a cost overhead component. A typical rule of thumb can be assumed as 100 to 500 business hours per year for several years (depending upon the FTC's concerns). However, in the case of RockYou, which the FTC determined in 2012 violated the online privacy of children by not protecting their PII under the Children's Online Privacy Protection Act (COPPA), the FTC fined the business $250K and mandated that RockYou must submit to security audits every other year for 20 years.

Specific Business-Dependent Costs

Up to this point, we have covered general costs associated with a breach. There are definite business-specific costs that you should consider as well. Some of the major considerations are listed here.

Size of the business. This appears to be the number one differentiator. Larger organizations will be targeted more than smaller ones. This conclusion is substantiated by the 2011 report "The Cost of Cyber Crime" from Detica Limited Research and the United Kingdom Cabinet Office. Therefore, Fortune® 1000 companies should prepare to be attacked more often.

Geographic location. Different geographies not only experience more or less cybercrime, but the breakdown of threat category types (IP theft, espionage, credit card fraud, hacktivism, etc.) can be different as well.

Has your company experienced a breach before? Cyber criminals love to retarget companies they have previously attacked. Motivations stem from a personal issue with that company, an ongoing desire to protect the public and make companies invest in network security, to a simple desire to see if the hacker can do it again. In addition, other cyber criminals will attack those companies to show that they are just as good a hacker as the first one. One recent example is Sony. Their PlayStation product was hacked in 2011 and again in December of 2014.

Industry sectors can have significant variances. Chemicals, electronic & electrical equipment, pharmaceuticals & biotech, and software & computer services are typically targeted for IP theft whereas aerospace & defense, financial services, and mining companies are typically more common targets of espionage. According to a study from Neustar in April 2013, "Hope is Not a Strategy: 2012 Annual DDoS Attack and Impact Survey: A Year-to-Year Analysis,"[24] 39% of the surveyed retailers admitted to having been attacked in 2012. For ecommerce businesses, 41% were attacked, along with 44% of financial services organizations. By contrast, the Neustar survey stated that only 35% of companies in general admitted to a distributive attack. So, your industry sector can definitely play a role in the probability of an attack, and the type of attack. Throughout 2013, the number of companies admitting an attack was up to 60%, according to the 2014 Neustar report[25].

International businesses have additional disclosure and liability costs. International operations will have a definite financial impact due to higher overhead costs like notification of breaches to oversight entities and affected individuals, country-specific liabilities, additional regulatory disclosure to government agencies, legal fees to defend the business, potentially decreased lawsuit and liability protections, potentially higher brand damage due to cultural impacts, etc.

[24] http://www.neustar.biz/enterprise/docs/whitepapers/ddos-protection/2012-ddos-attacks-report.pdf

[25] http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

Use of cloud services increases the likelihood of a breach by 3 times. This is documented in the Ponemon Institute research report[26], which illustrates the hidden dangers of cloud services.

Healthcare entities have specific privacy regulations like HIPAA (for the USA as well as other worldwide governments) that come into play. If violations occur, fines can be levied.

Retail and ecommerce entities also have specific requirements placed upon them by the Payment Card Industry to follow the PCI-DSS standard. Fines can be levied here as well.

Utilities, defense contractors and core public infrastructure have additional federal and state security regulations placed upon them. Not just through laws but through executive orders as well.

Network security vendors, consultants, and certain government agencies can have additional reputation impacts that affect their brand if they are breached. If your business fits into this area, then you should estimate the value of your company intellectual property accordingly.

[26] http://go.netskope.com/rs/netskope/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf

Cost Summary Chart

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

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)

Chapter 4:

Benefits & ROI for Investing in Security

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 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. More details about visibility architectures and their benefits can be found at www.ixiacom.com/solutions/visibility-architecture[27] and also in the Ixia eBook How to Secure Your Network Throughout Its Life Cycle[28].

Typical benefits for investing in network security include the following:

- 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
- Protect company valuation

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 customers or documented sources.

[27] http://www.ixiacom.com/solutions/visibility-architecture

[28] http://info.ixiacom.com/Secure_Network_Through_Lifecycle_Website_Download.html

Limited Financial and IP Exposure during an Attack

The use of network security equipment and techniques does work. 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% per record (using the average cost per record of $145 from the Ponemon report). Therefore, the average cost of a breach can be reduced 14.5%, or $26 per record in the USA if you use that figure for your financial analysis.

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 the reduction of a breach 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 (i.e., 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.

Due Diligence for FTC investigations and regulatory compliance

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[29]), 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.

[29] http://info.ixiacom.com/Secure_Network_Through_Lifecycle_Website_Download.html

By already having your architecture and policies documented, you will also save overhead administrative costs to collect the information as part of a “fire drill” once the breach is incurred. The cost/savings for this type of activity are very much company specific. That being said, we’ll look back to the Ponemon report for an estimation.

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 reduction of a breach by up to 19% per record per breach.

Vettable Policies and Procedures

As mentioned previously, the company and officers can be held liable for fraud and negligence if proper actions are not taken. This includes responsibilities for actions of the employees if the company environment fosters a company attitude of disregard for PII. However, once you have documented policies and procedures, the liability for the company and C-suite are significantly limited and they usually can't be held liable for the malicious actions of individuals. Think of someone like a disgruntled employee, or Edward Snowden, leaking confidential information to a public website. If your policies are well documented, the criminal and punitive damages can be shifted from the C-suite to the insider responsible for the breach.

In addition, if you have well-documented policies and procedures, then your IT staff can view them when needed, especially during an attack. This will allow them to more quickly document an attack and follow published guidelines on what to do, even if the what to do is to "immediately contact your supervisor."

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%.

Faster Threat Detection and Root Cause Analysis due to Increased Visibility

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.

As an example, Ixia had a customer whose network was dropping packets and the SPAN ports on existing switches were completely full. The customer implemented a visibility architecture centered around a new packet broker. The packet broker solution cost about $100K. Once implemented, the customer saved over $800K and experienced a higher level of quality of experience. In terms of cost savings, this is what the customer experienced:

- $320K due to a 50% reduction in the need for additional IDS & analysis tools to support the network
- $215K due to the elimination of redundant sensors
- $300K due to less rack space needed at each PoP, which reduced the installation, power and HVAC costs for the purchase

A different customer had a long MTTR. Over 50% of the traffic was duplicated and unnecessary and they had exhausted the number of available SPAN and tap ports. Once they implemented their visibility architecture, this customer experienced the following benefits:

- The MTTR for network problems decreased from days to hours
- IT was now able to implement proactive network scans to eliminate anomalies before they became problems
- Increased security tool efficiency due to the removal of duplicated traffic, which doubled the amount of real traffic that could be processed and reduced monitoring tool errors

- The monitoring probe resource contention issue was eliminated due to SPAN/tap port sharing

In a third customer example, this customer saw the following benefits when they implemented a visibility architecture using a network packet broker and a few taps:

- A faster MTTR was experience that resulted in reduced outages. A few minutes of outage on the e-commerce portal used to result in thousands of dollars lost per minute.
- The IT staff was no longer gated by an executive change board to insert diagnostic tools into the network, i.e. the tools were already connected through the packet broker so the customer could start resolving problems as soon as they were recognized
- Fewer monitoring tools (which means less cost) were needed due to tool port optimization, packet filtering and packet de-duplication

A fourth customer had experienced many of the same problems. This included lack of timely network access that was causing their MTTR to exceed SLAs, which was resulting in service penalties. In addition, they were experiencing high costs due to having to deploy lots of monitoring tools to cover all network links. Finally, root cause analysis could take days. The customer experienced the following benefits from their visibility architecture:

- $200K cost savings resulting from a 4 to 1 reduction in purchasing performance monitoring appliances
- $140K cost savings because proposed data collectors were no longer needed
- An 80% reduction in troubleshooting time was identified
- $50K savings from reduced/eliminated SLA penalties due to a faster MTTR
- Improved customer satisfaction from a faster incident response time and closure of trouble tickets

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. This is also documented in the next section on Additional Visibility Architecture Cost Savings. The faster MTTR can help reduce the cost of a breach by up to 5.5% per record per breach.

Additional Visibility Architecture Cost Savings

In general, adding a visibility architecture will improve the transparency and ease of access to information. Besides the cost savings due to faster threat detection and root cause analysis (mentioned previously), the automation of network packet brokers can provide additional benefits in the area of near real-time responsiveness for out-of-band monitoring solutions. This allows the packet broker to provide a faster response that can further improve MTTR capabilities.

Another optional benefit of a visibility architecture is application intelligence. Application intelligence can provide application filtering, faster threat detection, and geo-location information for faster indication of who, what, and where. Here is a quick summary of features and benefits:

- Helps monitoring tools work better by enabling engineers to filter unwanted traffic (Pandora, NetFlix, Amazon Prime, etc.) by application signatures and geo-location. The relevant information is then sent to a NetFlow collector. This can reduce unwanted data up to 80% on the NetFlow engine and translates to a faster MTTR but also means that IT could buy lower cost tools that don't need to process as much information (particularly irrelevant information). For example, this could reduce the need for a rack mounted chassis and allow IT to use a laptop with Wireshark (depending upon your requirements) instead.
- Application intelligence allows you to see unknown/suspicious applications faster for threat detection, sort of like an early warning system for suspicious activities. This can help reduce the amount of intellectual property lost during a breach by allowing you to discover the breach faster and stop the attack faster. For instance, Sony could have used this capability to see that files were being transferred off of their network long before they did. This could have translated to a savings of millions of dollars.

- Application intelligence can also provide a quick view of applications running on the network. This data can be used for better bandwidth management and trend analysis. This is extremely important to help monitor application bandwidth explosions that can slow down the network or potentially even cause it to crash.
- Geo-location information delivers a faster indication of device impacts and user trend behavior (who, what, where). This can also help assist in identifying rogue security threats.

Evaluate Vendor Equipment Before you Deploy It

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. These validations have been shown to improve network security (which lowers your chance of a breach) and to actually lower your purchase costs as well.

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.). An Ixia customer had a real-world experience with this situation where they had a purchase of a server load balancer already planned. The customer tested the device and found that they had to change it out because the actual throughput of the device did not match data sheet specifications.

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. Ixia equipment has been used to perform such tests for customers and found that, in several instances, this evaluation process can make customer networks up to 10 times more effective against DDoS attacks. This comes about by helping security architects optimize their network configurations (and choice of DDoS suppression equipment) so that the DDoS suppression capability can be up to 10 times faster.

In one specific example, a customer tested its firewall latency and found that it was 30% lower than what was specified on the product data sheet. The customer collected the irrefutable test data and went back to the firewall vendor to demand a 30% price reduction. They secured the price reduction and saved approximately $15K.

In a third example, a customer wanted to test their DDoS defenses and found a critical flaw in their design. There was a router configuration error that could have resulted in a Priority 1 service outage. This flaw was estimated to have corresponded to a 50% increased possibility of a breach from that threat vector with the probability of 50 minutes of downtime to discover and fix the error. At a generic cost of $5.6K per minute (quoted earlier from the Emerson Network Power study), the corrected design potentially saved the customer $280K. Ixia has found that 20 to 25% of businesses typically have a Priority 1 programming flaw in their networks that can be identified by the BreakingPoint product.

A final area of improvement is the ability to use these test solutions to validate and eliminate at least 100 man-hours in post-purchase configuration, troubleshooting, and fine tuning. Basically, you can test configurations ahead of time to come with a final, optimized security architecture to prevent costly live network problems. Using a loaded labor rate of $80 per hour for IT staff, this results in a minimum soft dollar productivity savings of $8K. Potential productivity losses from regular employees was excluded but would contribute as part of the $5.6K cost per minute of unplanned outages.

Protecting Company Valuation

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 business 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 van be so significantly mitigated:

- **Stock price reductions after a breach is disclosed –** Could be devalued by 8% or more for a year
  - Based upon Ixia research, the company stock value could drop by 8% over the course of a year.
  - A 2007 Ponemon Institute survey (The Business Impact of Data Breach[30]) shows that 32% of businesses reported a decline in share value

[30] http://www.scottandscottllp.com/main/business_impact_of_data_breach.aspx

- **Brand value –** Can drop between 17 to 31% according to the Ponemon Institute
  - A Ponemon report (2011 Reputation Impact of a Data Breach[31]) interviewing executives shows that a company's brand value drops between 17 to 31%. A company's brand value can range between 10 to 500% of annual revenues.
  - The report shows that the average brand value loss was between $184M to $332M.
  - It also stated that brand value losses can take more than a year to recover according to respondents.
  - According to the Ponemon report, 53% of executives thought the impact to brand was "moderate" while 23% thought it was "significant."
  - The survey respondents estimated that a data breach (which was widely reported by the media involving the loss of more than 100,000 confidential employee records) would likely result in an average 12% decrease in brand value. The loss or theft of a small number of sensitive files containing trade secrets, new product designs or source code would likely lower brand worth by about 18%.

Customer churn – Contributes to more than half of breach losses for a company

- A 2014 creditcard.com survey[32] suggests approximately 45% of consumers will "definitely not" or "probably not" shop at breached retailers.
- The 2007 Ponemon Business Impact of Data Breach survey shows that 74% of businesses reported definite losses of customers after a breach.

[31] http://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

[32] http://www.creditcards.com/credit-card-news/shopping-after-breach.php

  - The 2014 Ponemon Cost of a Breach Study[33] indicated that lost business (due to abnormal customer churn, reputation loss and diminished goodwill) accounts for an average of approximately 57% of the cost for a breach.

- **Intellectual property loss –** Loss of competitive edge as other companies acquire business technology for free.
  - A 2011 Detica Research Cost of Cybercrime report[34] estimates that IP theft costs British companies £9.2 billion annually.
  - A 2014 McAfee report[35] states that cyber theft results in the loss of $445 billion annually. An important finding[36] is that most governments and businesses are underestimating losses.

- 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

So, a proper network security architecture, or lack thereof, can have a significant impact to a company's current and future valuation. This is especially true as large corporations evaluate their network security practices and those of their contractors.

[33] http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

[34] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

[35] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[36] http://www.politico.com/story/2014/06/cybercrime-yearly-costs-107601.html

Benefit Summary Chart

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 value (Source = 2)	1% to 10% of annual company revenue

Table notes:

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

Source 2 = Ixia independent research

Chapter 5:

Demonstrating the Financial Business Case for Network Security

This last section provides an example financial analysis that can be used to demonstrate the net present value (NPV) of a network security investment to a CFO. Many business cases have failed because IT managers have tried to use a cost justification approach. In the end, an investment analysis is what a CFO really wants to see. This is a fundamental mindset change to understand. The C-suite is looking at how to grow the company so their focus is on making solid financial investments. One note here is that financial figures (costs and particularly benefits) can always be over-valued or under-valued. The key to credibility is to document your assumptions. Should someone disagree with an assumption, you can always defend it or change it to agree with them and then re-run your NPV analysis.

Part of any investment analysis has to include costs, but the other element is the projected revenue. By using a cost basis model, IT managers often kill their project before they ever begin a presentation. By using a net present value model, you'll be able to present the information a CFO wants to see, in the format they want to see it. This makes it very quick and easy for them to understand the trade-offs.

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

We've chosen to perform an NPV analysis on a traditional Fortune 1000 enterprise. An NPV calculator and several ROI calculators were used for the analysis. The basic assumptions are documented within this section so that you can perform a similar analysis for your company.

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, which is why it is more attractive to the CFO. 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. The time period has already been accounted for with the superscripts. The discount rate is the cost of capital (i.e., the interest rate you would pay). The USA Office of Management and Budget (OMB) recommends the following nominal discount rates:

Duration	3 years	5 years	7 years	10 years
Discount rate	2.7%	3.3%	3.7%	4.2%

The financial benefits will need to be determined for your specific company. Guidelines were provided in the previous chapter. Basic costs include the security architecture and visibility architecture solution costs – this includes technology purchase costs (CAPEX) for equipment, training, installation, etc. as well as technology maintenance costs (OPEX) for personnel, annual license costs, etc.

Example Analysis – Fortune 1000 Enterprise

- Number of employees = 13,000
- Number of remote offices = 30
- Number of data centers = 1
- International operations = yes
- Company annual revenue = $800M
- Company value = $800M

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 report[37]. 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[38]) 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) but this will vary depending upon various factors like size of company, use of a cloud network, etc. The average time to find a breach is assumed to be reduced from 170 days to 20 days (although the 20-day figure is extremely conservative) based upon the deployment of an Ixia visibility architecture and the use of security resilience testing (e.g., Ixia BreakingPoint product).

A cost of a breach calculator has been created by Symantec and Ponemon and is available at http://www.databreachcalculator.com/ to help if you want to try to customize the cost of a breach. However, please note that the calculator also reduces the actual cost of a breach based upon a few benefits as well – meaning this may not give you an accurate cost-only figure depending upon how you answer the calculator's questions.

Security Breach Benefit Summary

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

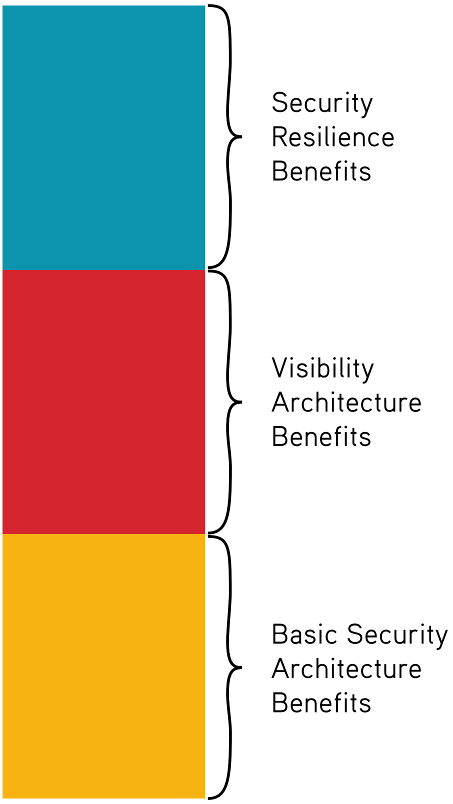
- Basic (defensive) security architecture contributions
- Visibility architecture contributions
- Resilient security approach contributions

For this example, here is the breakdown of contributions based upon the Ponemon and Ixia research:

[37] http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

[38] http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

Financial Benefit Contributions of a Resilient Security Approach


Security Resilience Benefits
Visibility Architecture Benefits
Basic Security Architecture 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 = $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 = $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 later.

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

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

- Annual savings (per year) = $328,990*
- Cost of initial purchase = $252,000
- Recurring costs (per year) = $106,144*
- ROI over 3 years = 64%*

* Note: values come from the Ixia visibility ROI calculator

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

Details For Basic Security Architecture Benefits and Potential Breach Cost Reductions

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.

Security Architecture Benefits

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

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 $308K savings for security equipment costs.
- 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.

- 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 $31K 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 (as previously discussed in the "Protecting Company Valuation" section).

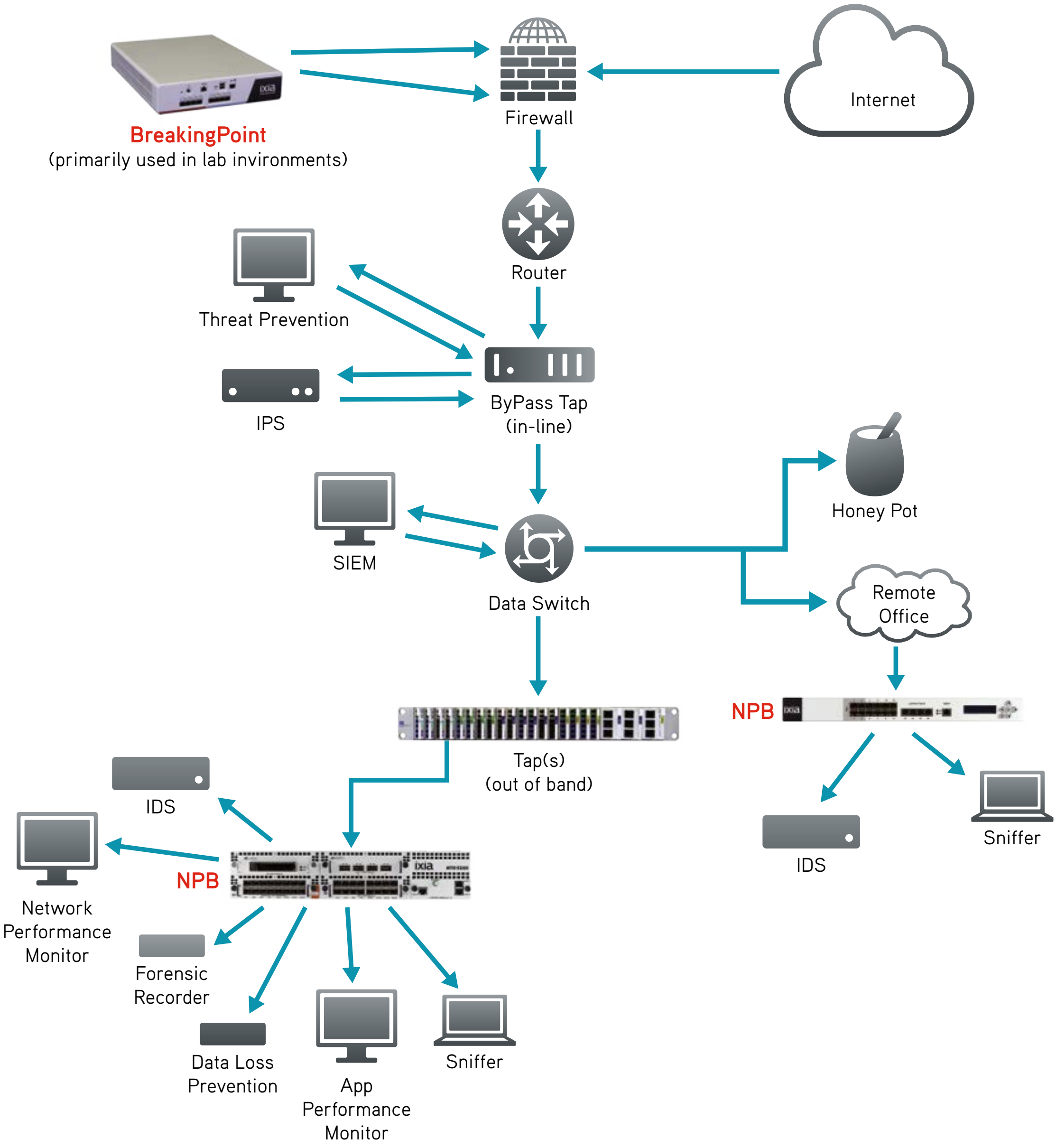
We will assume 1% of the $800M, which is a one-time benefit of $8M. This benefit is split evenly across all three of the benefit componenets (i.e., basic security architecture, visibility architecture, and security resilience. Note, even if this benefit is neglected within this study, the payback for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

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

Reference Architecture for NPV Analysis



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 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.

Chapter 6: Conclusion

Understanding the financial aspects of security investments is very important, especially the opportunity cost for inaction. It needs to be understood that this is a strategic investment, not just another cost decision. 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. A greenfield environment for a company with annual revenues of $800M was assumed for the analysis.

The financial analysis presented here shows that security isn't just a cost. A minimal investment of $1.78M yielded an NPV of $11.8M over three years. Alternatively, the annual cost for a breach 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. A part of this investment included a conservative company value gain (based upon the security architecture) of 1% of the annual revenue, or $8M. As an added bonus, the payback period for this investment is only 6.4 months. Even if the book value benefit for security is eliminated, the payback period is less than one year.

This example was for a large (Fortune 1000) business and should be representative of a company with 10,000+ employees and 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 three 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 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.

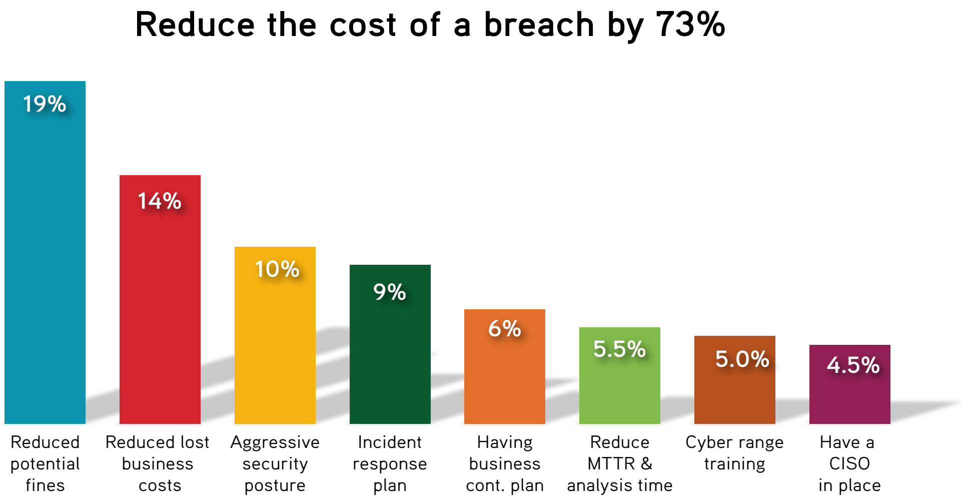
Another way of looking at these first two points is that your business could potentially realize the following savings, based upon your visibility and security architecture deployments and whether you take a purely defensive security approach or combine it with security resilience. Security resilience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

A third key point illustrated within this paper (and the NPV analysis) is that the architecture investments discussed can yield quantifiable reductions in the costs of a breach. This can be especially true if a life-cycle approach is adopted because it allows you to validate that you are following the steps needed to minimize your security risk and financial exposure. A life-cycle approach can also help make you organize your security architecture and plans so that you reduce revenue losses, reduce potential fines, increase responsiveness to issues, and decrease remediation times and costs. The Ixia eBook How to Secure Your Network Through Its Life Cycle[39] can give you a plethora of tips and strategies to help you protect your enterprise.

[39] http://info.ixiacom.com/Secure_Network_Through_Lifecycle_Website_Download.html

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%.



The next step is for you to conduct your own analysis specific to your company and security architecture to demonstrate the NPV of a network security investment to your CFO. In the end, this is what a CFO wants to see – a solid financial benefit for the capital 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.

The Most Trusted Names in Networking Trust Ixia

Enterprises worldwide rely on Ixia test and visibility solutions to validate and improve the performance of devices, networks, services, and applications.

The demands on the network are constant and your security must have resilience to maintain its effectiveness as it comes under attack, is challenged to maintain visibility to traffic and events across the network, or just needs an operational change to deploy the latest threat updates. Ixia's portfolio of security solutions allow enterprises to:

- Optimize security device investments such as IPS, Firewall, NGFW or DDoS Mitigation by helping you select the best technology with the right performance and deploying it in the network most effectively with network visibility and optimal load balancing.
- Minimize downtime and improve operational change control for security upgrades by validating security updates and changes and providing the inline deployment tools to ensure that these changes are not disruptive to network operations.
- Train and prepare for realistic cyber security exercises with systems that can create the real-world application loads and attack traffic required for a cyber range and also provide the visibility required to stream high volumes of events to security tools to monitor the exercises.

For more information go to www.ixiacom.com

ixia

26601 W. Agoura Road
Calabasas, CA 91302 USA
Tel +1.818.871.1800
www.ixiacom.com

April 2015 – 915-3529-01 Rev. A