Quantifying Security Incidents

Annual loss expected (ALE) versus annual loss realized (ALR)

White Paper

Introduction

Measuring the success and value of an information security organization is a perennial challenge. To help address that challenge, Cisco has developed a process to consistently capture and quantify losses from security incidents and compare them against an established industry benchmark.

We use annual loss realized (ALR) metrics for our board and C-level reports of security effectiveness. These metrics support decision-making in individual business units regarding security investments and bring visibility to the business impact of security incidents.

This paper outlines the method and how the data is used.

Christian Willard, Business Analyst
Kaveriappa Muddiyada, Business Manager
Sean Stack, Manager of Operations

Table of Contents

Overview

Corporate boards of directors and C-level executives are increasingly concerned about cybersecurity. They want to know the risks that their companies face, their security preparedness, and the effectiveness of those preparations and defenses. Teams tasked with security who report to C-suites and boards require accurate metrics that are accessible and relevant to nonspecialist audiences.

One metric has proved valuable as a board-level measure of the overall effectiveness of an organization's cybersecurity effort: the comparison of annual loss expected (ALE) with annual loss realized (ALR), expressed in monetary terms. This measurement helps an organization understand the extent of its losses from security incidents and the trend against an industry benchmark

ALE

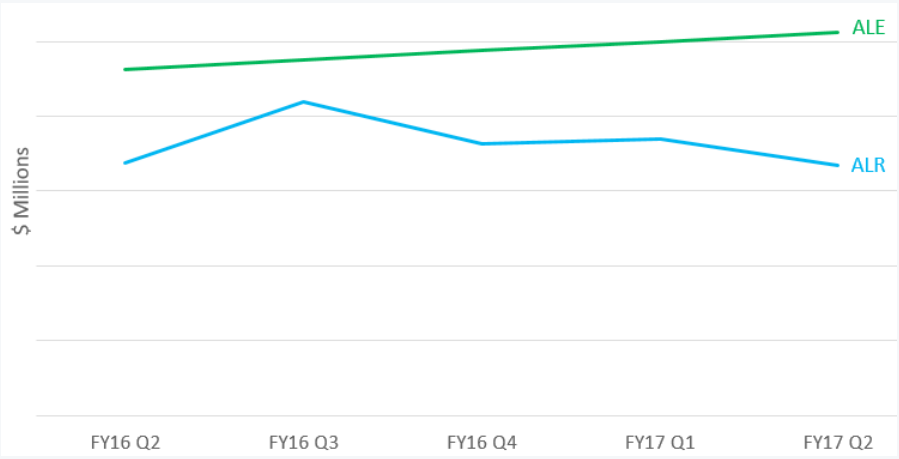
ALE is an indicator of an organization's expected losses from security incidents. It is influenced by the organization's size, its geographical scope, the nature of its business, and its security posture. Cisco has used the "Cost of Cyber Crime Study" from the Ponemon Institute to derive the ALE benchmark for itself.

ALR

ALR captures the actual impact and cost of handling security incidents. It enables us to look across types of incidents and individual Cisco functions and make specific recommendations that will reduce our losses from security incidents. To get an accurate comparison against an industry benchmark, the costs in the ALR calculations should cover the same categories of costs included in the ALE calculations. To compute the ALR value, data is gathered from various teams across Cisco.

Figure 1 shows a mockup of a report. Cisco reviews the ALE versus ALR metric every quarter and delivers a detailed readout to the chief of information security officer (CISO) and senior leadership of the teams involved in handling security incidents at Cisco. This metric provides insights to decision-makers about Cisco's security posture. The costs in ALR also provide insights for those determining security investments for the company.

Figure 1: example chart for trend of ALR vs ALE (mock data)



Methodology

We first establish an appropriate benchmark ALE for Cisco, and then develop the methodology for creating a consistent, repeatable process to calculate the ALR. The process enables Cisco to consistently report ALE versus ALR to executives on a quarterly basis. To achieve this, the following is required:

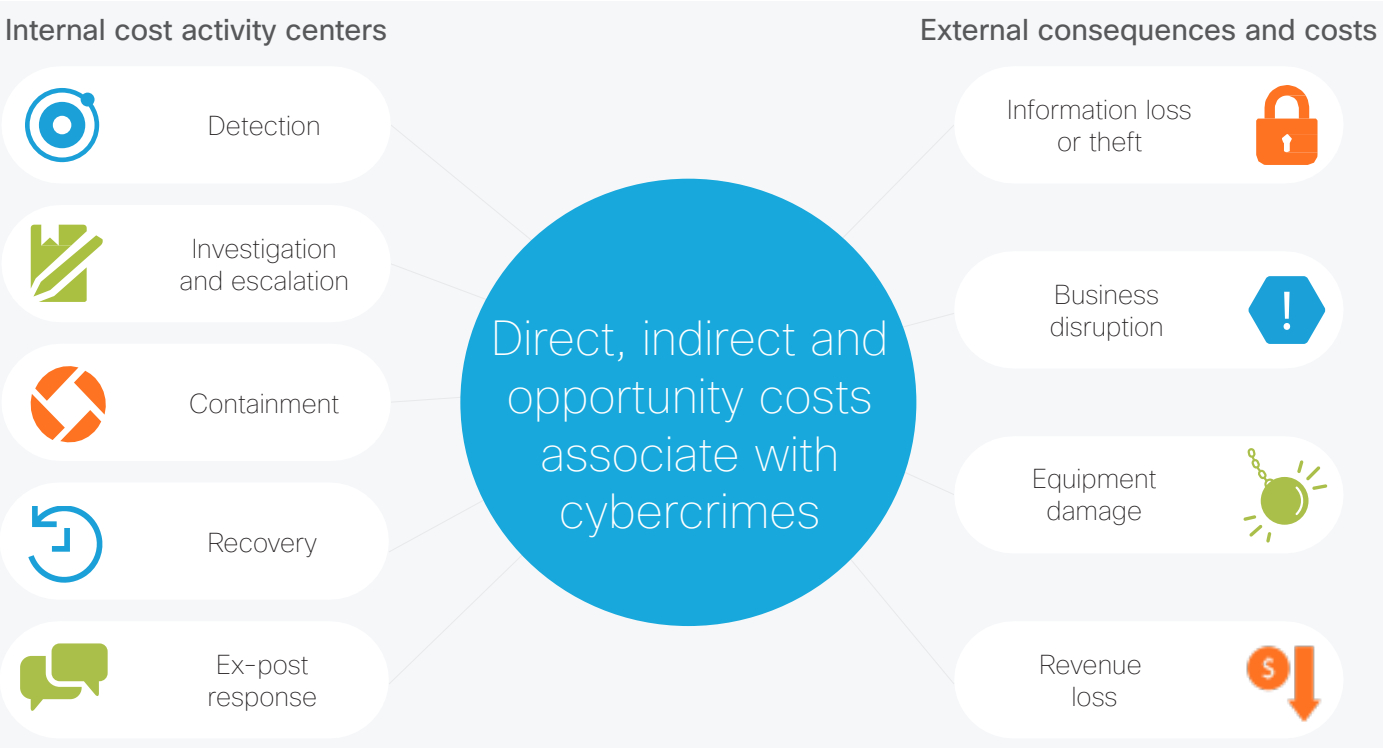
- An appropriate ALE benchmark for Cisco
- Equivalent components for Cisco's ALR
- Validation of the data sources for ALR
- Processes and tools to capture and communicate the ALR metrics in a clear, consistent, and repeatable fashion

Establishing the ALE Benchmark

The industry report "Cost of Cyber Crime Study" was used to derive the ALE measurement. The Ponemon Institute gathers data from more than 200 companies in seven countries. The report breaks down the data according to company size and security posture. Because of the scale of Cisco's operations around the world, we decided to use the per capita cost for large organizations in the study. The ALE baseline is reset every two years, following Ponemon's biannual update cycle.

ALE captures the costs incurred when organizations respond to cybercrime incidents. These costs include the costs to detect, recover, investigate, and manage the incident response. Figure 2 shows the components of the cost framework in the Ponemon Institute study.

Figure 2: Components of ALE per Ponemon



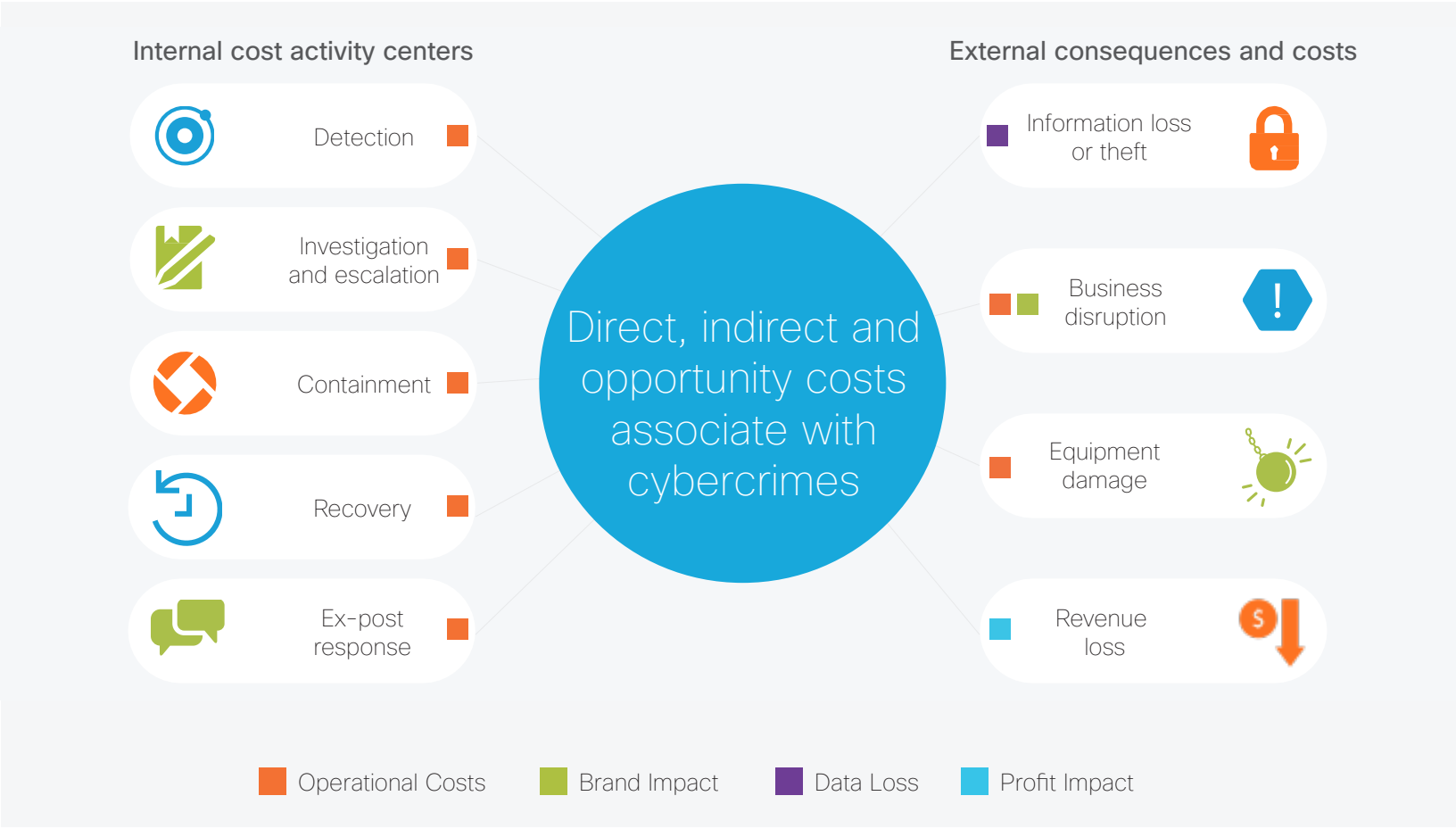
Delivering ALR

The next step was to develop a methodology to calculate the ALR for Cisco. To meet the objective of comparing Cisco against the industry benchmark, all the cost components from the ALE were included.

- Operational costs: Incident-handling costs derived from all primary and secondary incident management teams across Cisco. Incident response activities include detection, investigation, containment, recovery, and productivity loss.
- Data loss: The value of data lost in a security incident. This includes the value of our intellectual property.
- Brand impact: The effect on Cisco's brand based on the degradation of a service provided to customers and any impact to the valuation directly attributed to a security incident.
- Profit impact: The impact on Cisco profits from a security incident that directly affected sales or penalties and discounts.

Figure 3 shows the cost components from the Ponemon Institute study and how the equivalent cost components from handling security incidents across Cisco were captured. We followed the data lifecycle structure as defined by the cross-industry standard process for data mining. The four broad cost categories that matched the industry benchmark are denoted by colored squares in Figure 3.

Figure 3: Mapping equivalent cost components



Building Business Partnerships

The purpose of producing the ALR is to quantify the financial impact of information security incidents across the company. Various Cisco teams that handle incident detection and response (ID&R) functions collaborated to understand the available data of security incidents. The Computer Security Incident Response Team (CSIRT) is Cisco's cyber investigation and forensics team. CSIRT, along with the Data Protection and Privacy (DP&P) team within the Security and Trust Organization, handles the bulk of the ID&R functions. In addition, Cisco IT protects intellectual property from internal threats through the Intelligent Context and Content Aware Monitoring service. The nature of the data required to compute the ALR is sensitive. The partnership of these teams to establish objectives and create a mechanism to gather data each quarter was key to understanding the nuances of security incidents and to capturing all the relevant costs.

Data Gathering

Building the ALR required data from the teams identified in the previous section. The quarterly incident data provides a breakdown of security incidents by US-CERT category. This data also has many attributes critical to computing the ALR. Subject matter experts (SMEs) were engaged to analyze the data received from the aforementioned teams. Most of the structured data sets had an established format.

Meetings were conducted with SMEs for incidents that required a follow-up to understand their context and to gather all the relevant data required to compute their cost. In addition to incident information, data was required from financial systems. This included the costs related to human resources, hardware, and software for the various teams involved in managing security incidents. SMEs were engaged to allocate these costs into various incident categories.

Some data came in free-text forms, especially for significant security incidents that required attention and follow-up across the company. The data set was unstructured and was therefore transformed into a format that could be used in this model. Common attributes that were consistently captured included the type of incident, the value of loss, and the loss category.

Data Preparation

The ALR requires data gathering from various sources in a spectrum that ranges greatly from a structured to an unstructured format. The various data sets needed to be transformed into information that was suitable for our purpose.

In addition, some aspects of the data, such as incomplete records, errors, and outliers, could cause inaccuracies during the modeling phase.

- Incomplete records could be an issue because missing data attributes make it impossible to move data into bins (for example, moving data into either security incident categories or fiscal quarters).
- Errors could be problematic because incorrect data attributes will cause data to move into the wrong bins.
- Outliers, especially extreme ones, could also be an issue in creating standardized security incident costs or analyzing trends over time.

A formal process was defined to gather data from various sources. The majority of the data was in structured formats, and the process to transform it was automated to fit our needs. Unstructured data requires some manual formatting and transformation before it is run through the model. Although efforts were made to automate the process, the complexity of calculating the costs of unique, high-impact incidents also required some percentage of the data to be manipulated manually.

Data Understanding

The function of developing an ALR model is to aggregate all the data gathered in the previous phases to generate meaningful outcomes. Building the model can be done in a number of ways because of the myriad of analytic solutions that exist today. Each organization should choose the one that best fits its own needs, but as a general guideline, it is best to find a solution that is easy to update, accurate, and cost-effective. This model is designed to parse data for the ALR into the four cost categories we identified earlier (operational costs, data loss, brand impact, and profit impact).

For operational costs, establishing a baseline to standardize security incident costing by category is one of the most important calculations the model will perform. The calculation starts with historical data for both incident counts and operational costs. Attributes from a five-quarter period to establish standard costs were included. The baseline is normalized for variations and outliers in the data as we move along the timeline. A too-long timeline will include data that may no longer be relevant because incident detection and response techniques change over time.

Table 1 presents an example of calculating the standard cost for Category 3 (CAT 3) malicious code incidents. This cost will be applied to CAT 3 incidents every time the model is updated with security incident counts for a reporting time period (monthly, quarterly, annually) in the future.

Table 1. Example of a standard cost calculation

	Five Quarter Total	Standardized Incident Cost
Number of security incidents	5,000	
Labor cost	$2,500,000	$500
Tools (hardware and software)	$500,000	$100
PC remediation		$500
Cat 3 Cost		$1100

The majority of operational costs are incurred by the incident management teams. Collaborating with SMEs from these teams and gathering their insights on classifying resources by various incident categories was crucial in ensuring an accurate baseline cost. The productivity loss from security incidents under the operational costs category was recorded. The majority of the productivity cost was from disruptions to employees' ability to perform regular daily functions when impacted by a security incident.

The cost of data loss incidents varied considerably depending on the nature of the data that was impacted. Determining the cost of intellectual property data loss incidents required additional modeling on its own. Work with SMEs in the DP&P team helped to establish a standard cost to record when there is intellectual property loss. Return on investment (ROI) information of various Cisco products in various stages of the product lifecycle was the building block for this model. The ROI for a wide range of Cisco products gave us the data we needed to establish a standard cost for each intellectual property data loss incident.

Brand impact costs stem from the disruption of services to customers. An example of this would be a distributed denial-of-service incident against a service that Cisco provides to customers. Service outages cause business disruption to the customers and can cause additional damage if customers are using a service as a part of a bundled product. Published research was used to establish the impact of various durations of downtime with associated estimates of brand impact costs.

In the event of an interruption to the service that Cisco provides because of a security incident, various teams collaborate to understand the impact. Costs are then recorded to reflect the severity of service degradation based on the downtime duration (see Table 2).

Table 2. Brand impact from downtime

Length of Downtime in minutes	Min	Mean	Max	Brand Impact
Substantial	277	442		$5,274, 273
Moderate	$2,500,000		$500	$468,309
Minor	$500,000		$100	$20,929

Source: IBM, 2013

Profit impact is recorded when security incidents directly result in income statement loss to Cisco. To derive the revenue or expense loss, these incidents require additional data collection and analysis with the teams handling the incident.

Major incidents can have a noticeably higher financial impact. These rare incidents are handled independently of the normal ALR model. Although the information security team is the primary handler of the majority of security incidents at Cisco, these high-impact incidents require a wide effort across the company to resolve. Each incident is unique and tends to have high visibility within certain parts of the company. Costs are typically recorded for these incidents in more than one of the cost categories. The follow-up on these types of incidents will typically span multiple fiscal quarters. We record relevant costs in the quarters when the loss is incurred, not when the incident occurred.

Cisco's ALE versus ALR analysis is reported every quarter. Data collection streams are well defined with all the teams involved in managing security incidents. Each data set is transformed into an established format. The model is designed to accept this structured data as inputs, and therefore the vast majority of the analysis is automated. The format of the data received for high-impact incidents cannot be defined because each incident is unique, and there is no set input structure. The teams involved and the type of incident dictate the data collection process for these incidents. This unique data feed must be transformed manually. Having a manual data-load step in the model provides the flexibility to handle the diverse nature of these incidents.

Potential Uses

We use ALR metrics for board and C-level reports of security effectiveness, for decision-making support regarding security investments in individual business units, and for bringing visibility to the business impact of security incidents. The cost structure established for various types of incidents and the historical data support leaders' investment decisions and the cost analysis of specific incidents. Data is used to drive targeted action.

Use Case 1

As mentioned earlier, major security incidents that have a material business impact require more consideration when their costs are being determined. We perform a deeper dive into these incidents to ensure we cover all aspects of the impact. In some instances the quantification of these major incidents drives change in the organization. For example, malicious code (aka CAT 3) incidents represent about 85 percent of the security incidents handled by the Cisco CSIRT. When the Gamarue malware infection led to an uptick in CAT 3 incidents in the enterprise network, it was determined that 99 percent of the infections were spreading through auto-run USBs. CSIRT recommended three steps to counter the spread of this malware. They were unable to secure agreement from the business unit because of the associated cost and the effort needed to implement the technical controls. CSIRT then used ALR data to calculate the costs associated with these malware infections as well as potential future losses. With this quantitative expression of business impact, senior leadership immediately saw the benefit of implementing the controls and approved the three-step recommendation.

Use Case 2

With the inclusion of additional data sets, ALR can be further dissected for internal use. The human resources team manages hierarchical business unit data that can be merged with ALR data to reveal the impact of security incidents in each department. After the data is merged, visualizations can be created to portray the impact of the security incidents. This exercise enables limited security educational resources to be more effective because it targets the areas in an organization that represent the most pressing need for them. For example, if CAT 4 security incidents are more prevalent in the engineering department, educating engineers on how to properly use system access would help lower the number of improper-usage incidents in that part of the organization.

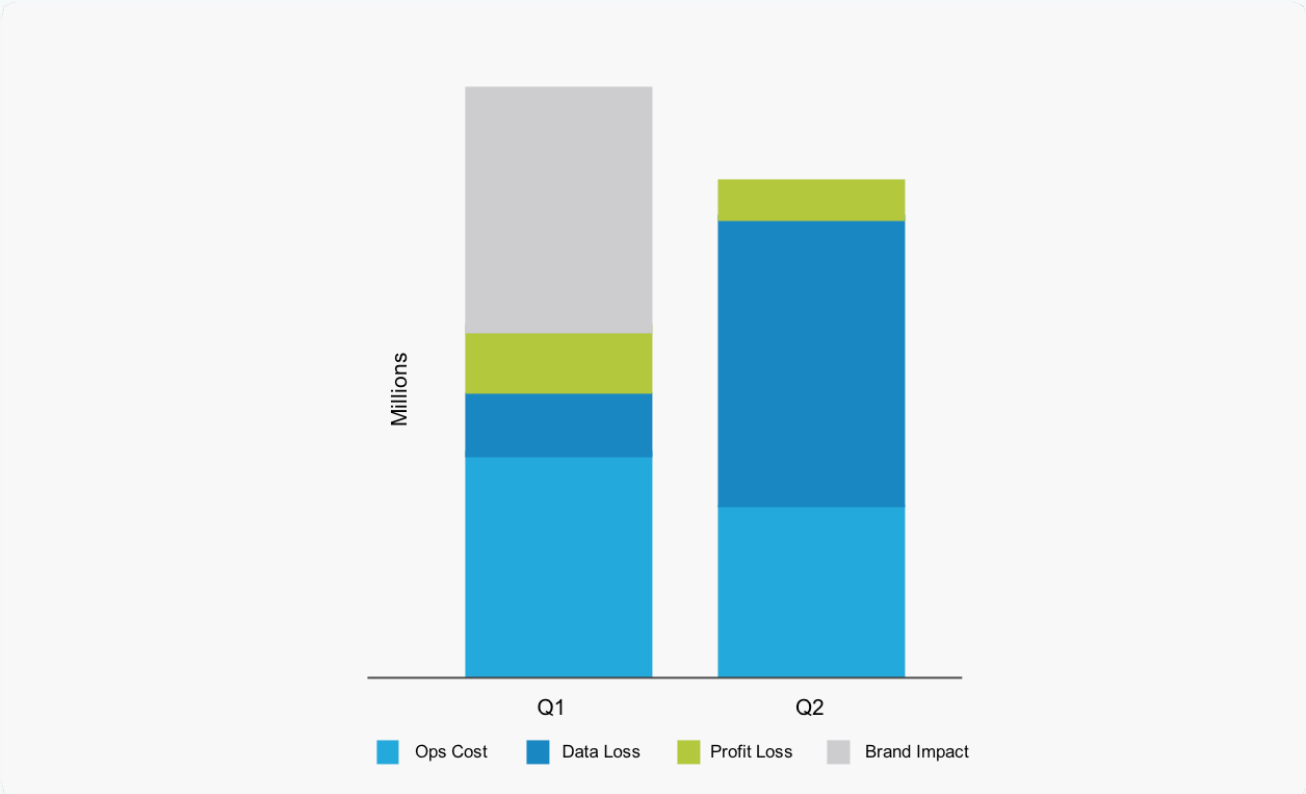
Use Case 3

Another data set that can help focus limited educational resources can be obtained with an internal phishing campaign. Cisco works with an external organization to create phishing emails on a quarterly basis as a preventive measure. After each phishing campaign, the data is disseminated by business unit, once again using the HR organizational hierarchy data. Users who click a link in the fake email are promptly directed to a website for immediate training on how to recognize a CAT 5 incident. This is a proactive measure that Cisco deploys so that, when the inevitable phishing email is received, the employee will be better able to recognize the signs that it is a phish. In addition, we can merge the internal phishing campaign data with actual CAT 5 phishing incidents to judge the effectiveness of the internal phishing campaign and the education that follows it. This can be done by performing various statistical correlation analyses.

Usage Summary

The output of the model gives us the ability to consistently capture ALR as the cost of security incidents at Cisco. With the established ALE, we can compare Cisco against the industry benchmark. Flexibility in the model provides the ability to slice and dice the data in multiple ways to generate the appropriate reports for executive briefings. For example, the ALR is broken down by cost categories, CERT incident categories, and functions within Cisco. We can also provide more detail in each of these breakdowns and address various questions that arise when the information is analyzed or presented to stakeholders. The consistency of the methodology enables us to monitor the effectiveness and the trends of the security controls in place.

Figure 4: Example breakdown of ALR by cost category (mock data)



Conclusion

At the end of every fiscal quarter, the Cisco information security group works with internal clients, stakeholders, and subject matter experts to gather security incident data and determine its total impact on the business.

The analysis is presented to the CISO and other business leaders. In addition to the overview and the breakdown of costs by various categories, a deep dive into all the unique and high-impact security incidents in the period are included. This forum also provides an opportunity for senior leaders to discuss trends and upcoming changes in processes and tools. In the rare event of a high-impact incident, this data is shared beyond the information security team. The cost breakdown and analysis are disseminated across the company to help staff understand the impact of these types of incidents. ALR data is used in cost-benefit analyses for various security initiatives. The cost of security incidents is also used in investment prioritization.

The ALE versus ALR project has established a method to quantify the losses incurred from security incidents. The collaboration of various teams at Cisco will be the foundation in establishing a methodology to quantify existing risk and risk mitigation using the factor analysis of information risk (FAIR) methodology. Collaboration with the SMEs who own the controls and tools provides ready access to the inputs needed for this extended model. In addition, the cost components established in the ALE versus ALR project will be used to derive the loss-magnitude components of the model.

The ALR method provides a consistent and repeatable process to quantify different aspects of information security across Cisco. The data informs information security decisions and demonstrates the value of those investments to executive management in financial terms.

"The ALR/ALE process helps us benchmark our security program versus our peer group, while giving us a metric to demonstrate our effectiveness to senior management."

Steve Martino
CISO, SVP, Information Security, Cisco

"It wasn't until we applied the ALR incident costing to the Gamarue malware scenario that we were able to receive the buy-in we needed from the organization to implement a solution to stop the spread of the virus."

Michael Scheck
Director, Cisco CSIRT

References

1. Ponemon Institute. "2014 Global Report on the Cost of Cyber Crime." Ponemon Institute. "2016 Cost of Cyber Crime Study & the Risk of Business Innovation."
2. Leaper, Nicole. "A Visual Guide to CRISP-DM Methodology."
3. "Advanced Machine and Deep Learning Helps Digitization of IT."
4. US-CERT. "Federal Incident Reporting Guidelines."
5. "The Economics of IT Risk and Reputation."
6. The FAIR Institute

About the Cisco Security and Trust Organization

Cybersecurity is a rapidly growing boardroom issue. Highly visible data breaches and service disruptions have left companies and governments exposed and have left many more worried about the risks. Short-term revenue loss is unfortunate, but long-term reputational damage can destroy a business.

Secure digitization provides the critical foundation that organizations require to protect themselves, earn the trust of their customers, move faster, add greater value, and grow.

The Cisco Security and Trust Organization (S&TO) underscores Cisco's commitment to address two of the most critical issues that are top of mind for boardrooms and world leaders alike. Ensuring pervasive security across our business—protecting Cisco, our customers, data, and privacy—is mission critical. We take the best of what we do to secure our enterprise and share it with our customers to enable their success. We work to embed holistic security and trust into the Internet of Things and make sure that security is a leading enabler of country digitization acceleration, while helping to shape international standards, regulations, and trends.