Making the Business Case for Threat Intelligence
Table of Contents

Executive Summary .......................................................... 3
Defining the Need ............................................................. 4
Aligning Needs and Business Objectives ............................... 6
Formulating a Plan ............................................................ 10
Business Case Example Scenario .......................................... 13
In this white paper, we examine what we consider to be three necessary steps when making a business case for threat intelligence for your organization. Companies must define what they need and why they need it, align security needs and business objectives, and finally, create an actual plan. We then offer two example scenarios of how businesses can put these steps together and created a solid justification for threat intelligence.
Creating a security budget can be challenging for even experienced security professionals. In many cases, the practitioners who see the day-to-day value of threat intelligence – cyber threat analysts, security analysts, and others – are not the stakeholders who control the budget. In fact, a recent PricewaterhouseCoopers survey found that 49 percent of boards view cybersecurity as only an IT risk, and not an overall corporate risk.¹

Before building your business case, it is critical to define “threat intelligence” and determine if your organization needs it, and if so, how it will be used. Our view, which is shared by many security industry experts, ² is that there’s a big difference between “threat intelligence” and “data.” Our definition states that to turn data or information into threat intelligence, the final product must meet at least three criteria:

1. **Relevance** – The information must relate to, or at least potentially relate to, your enterprise, industry, networks, and/or objectives

2. **Actionable** – It must be specific enough to prompt some response, change, action or decision, or to dictate an explicit and informed decision not to act

3. **Value** – Even if relevant and actionable, if the data (and the action) does not contribute to any useful business outcome, there is no value

When threat activity, known actors, historical tactics, or attack information can be combined with vulnerabilities, activity data, or other particulars present in your network and environment, then the information becomes relevant, actionable intelligence.


The Need for Threat Intelligence

There are two key factors driving the need for, and value of, information from outside of the corporate network. They are based on the belief that actual intelligence (as defined above) is derived from correlating information from outside of the corporate perimeter or span of control with things from inside of the perimeter.

The first driver is the explosion of risk types in both complexity and number. Besides well-known risk types such as phishing, domain name spoofing, distributed denial of service (DDoS) attacks, and SQL injections, security teams must now combat cyber risks that touch on physical security, state and federal regulations, and both protection of, and compliance around, customer data. Understanding your exposure to these types of threats, whether and how often your company and industry are targeted, and the potential impact of those activities is key to determining whether you actually have a need for threat intelligence. If so, these factors will be key to making the business case and budget justification for a threat intelligence program.

The second driver is the expanded attack surface. Threat actors continue to use older channels, such as Internet Relay Chat (IRC) and Usenet, along with the web and other channels such as social media to plan attacks, trade data, and organize resources. The number and type of sources continue to expand, and the volume of content being produced across those sources has increased literally by orders of magnitude.

Effectively monitoring across the web, social media, and underground channels, as well as staying abreast of current threat activity is a daunting task for any security team. The volumes of data, and the time required to sift through it all, becomes cost-prohibitive. The problem is even greater for organizations with a global presence, requiring both data collection and analysis in multiple languages.

Due to these factors, it is nearly impossible for many in-house security teams to effectively collect, sort through, and process information sourced outside the perimeter, making it a necessity to procure third-party services and tools to help keep the organization safe. Security experts will need to be able to translate the need for resources into management’s language, and explain the expected outcomes in terms of value to the business, in order to obtain the budget needed to equip the company network to mitigate threats.

Remember, data alone is not intelligence; threat intelligence can best be defined as information that is relevant to the organization, has business value, and it is actionable. As the threat landscape has expanded, more and more organizations have found the need for, and can benefit from, threat intelligence. Key drivers of this expanding need include the explosive growth in risk types and the volume of content and sources to be covered.

3: http://searchnetworking.techtarget.com/definition/Usenet
Now that we’ve defined threat intelligence and how to determine if your organization needs it, we will discuss how to align your security needs and business objectives.

In a typical management structure, the two forces behind business decisions are often governing bodies or fiduciary duties. Most chief information officers (CIOs) or chief financial officers (CFOs) don’t want to spend money unless there is documented proof that something will have a real impact to the business, which often makes it difficult to quantify investments in solutions to address security threats. Although at a high level the forces behind the security team’s decisions merge with those of management, at a more detailed level, security professionals are driven by protecting the organization and its assets, causing them to speak a different language than management.

In a recent PricewaterhouseCoopers study, many senior executives and boards said they found it hard to link security technology to the related tactical risks it is supposed to help mitigate. In order to successfully argue the need for a threat intelligence capability, security professionals must map their objectives to management’s objectives.

The following business objectives are always a good place to start: reducing cost or risk, generating or retaining revenue, utilizing assets, and meeting regulatory requirements.

Reducing Cost or Risk

Breaches, intellectual property loss, and service disruptions all incur costs. In some cases, those costs can be quite significant. To date, estimates of the hard-dollar cost of major breaches like Home Depot and Target have run into the tens of millions of dollars or more.

Some costs are obvious, such as direct operational fees for legal and forensic services, consultants, and customer care. There can also be costs that are harder to directly measure but are no less real, including loss of brand equity and reputation damage. If risk is viewed simplistically as the impact of an event times its likelihood, then intelligence activities that can reduce the likelihood and/or impact of those events, or quantify their risk-reduction value, have a clear business justification. This has been supported in research showing that using threat intelligence can save companies millions of dollars.

In addition to the potential savings through risk reduction, a well-equipped and carefully scoped threat intelligence capability can reduce the actual cost to run a security and intelligence function. For example, providing staff with collection, prioritization, and analysis tools that make them more efficient will enable them maximize the value of the tools that make up most of a typical threat intelligence budget.

Generating Revenue

Security professionals are typically focused on protecting the organization, so they may not see themselves as playing a role in retaining or increasing revenue. However, the risk of revenue loss from customer defections or cancellations after a breach, as well as the potential loss of business not yet won, needs to be factored in when building a justification for a threat intelligence budget.

For instance, as noted above, data breaches not only incur monetary costs, but they also impact reputation and customer perception. They can even have a direct impact on real-world operations, such as interrupting or impeding online sales or production and distribution of inventory.

Investing in threat intelligence can also contribute directly to revenue capture. In a real world example, two government contractors were bidding on a major project in a remote and dangerous area. One firm, a Cyveillance client, included in their proposal a description of their use of online monitoring and real-time threat intelligence as a major discriminator in their approach to security (and therefore risk) for the project. In this situation, the threat intelligence function gave the Cyveillance client a leg-up against its competition, allowing the company to win the proposal.

Even though revenue is not typically a security team’s primary mission, a chance to contribute to revenue should never be overlooked as a way to win friends and influence budget holders.

**Utilization of Assets**

A third avenue to align threat intelligence (and the budget for it) to management’s interests is to view it as a way to increase utilization of assets or resources that have already been budgeted or bought. If you can tie your activities or budget request to increased employee productivity, efficiency, or effectiveness with assets already in hand, this is a “pure business” rationale that may play well with budget holders.
For example, we routinely see customers who have made significant (six- or seven-figure) investments in buying, configuring, and running a Security Incident and Event Management (SIEM) platform or other similar tool. Despite this investment, many find themselves overwhelmed with data flows and lack of clear rules for prioritization, as well as suffering from a talent shortage and “alert fatigue.” If these customers made a modest investment in additional data feeds, lookup services, or APIs, they could increase the productivity of existing staff or increase the effectiveness of assets already paid for, which can provide an avenue for business justification of specific tactical purchases.

Increasing Compliance

Another common justification for a threat intelligence program is to examine how the process can address regulatory or industry compliance requirements. For example, in 2013 the Federal Financial Institutions Examination Council (FFIEC) issued clarifying guidance on financial firms’ responsibilities around both use and monitoring of social media.

In the insurance industry, agents and contractors selling Securities and Exchange Commission (SEC)-registered products, such as mutual funds or annuities, must abide by strict rules regarding marketing language and advertising. Violations of these rules do not just put the agent or salesperson at risk, but the corporate broker-dealer under whom they operate may be subject to fines of thousands of dollars per violation. In the pharmaceutical industry, producers are in some cases required to monitor for online sale of highly-controlled or so-called “restricted distribution” drugs.

Especially in tightly regulated industries such as these, there may well be a clear argument that effective online monitoring or externally-sourced intelligence can lead to increased compliance, lower risk of fines, and/or potentially less time spent dealing with regulators and audits.

The security professional’s objective or desired initiative will ultimately drive the data, tools, and activities within the security or intelligence organization. By understanding the larger organization’s business objectives, security professionals can gain insight into justifying investments in threat intelligence capabilities, and formulate a budget request that management will understand and value. Now we will show you what you need to make a real plan.
We’ve explained the importance of using threat intelligence and how to justify your security needs by equating them with a business objective, now it’s time to get to the nitty gritty: creating an actual plan. Let’s take the principles we’ve discussed and use them to formulate a plan and a budget request.

**Step 1: Envision the End State**
Picture the finished product of your threat intelligence plan – the security operations center, the analysts, the tools, and the activities that will be required. Then work backwards and list out the actual needs to fulfill that vision.

**Step 2: T.E.S.T. for Readiness – Gap analysis**
A dollar figure will be associated with your vision. Before coming up with actual numbers, put together a gap analysis to find out what must be procured to fulfill the Tools, Expertise, Skills, and Time (T.E.S.T.) framework.
**Tools:** The hardware, software, physical space, workstations, and platforms that are required to complete the vision. It’s a catch-all for the physical “stuff” needed to bring the envisioned future state into reality.

**Expertise and Skills:** Both expertise and skills are knowledge-based needs, but they have subtle differences. In our definition, expertise is based on knowledge, experience, and wisdom. It is often the purview of specialists, consultants, and experts, and procured on a limited or short term basis. Skills are the learned abilities required for on-going operations. These can often be developed with existing staff through learning programs such as certifications or trainings. Take inventory of what skills need to be procured, learned, hired, or deployed to determine specific costs to obtain those things as needed to complete the vision.

**Time:** This comprises two related, but subtly distinct elements. The first and more obvious element is the time available from existing resources; does your organization have the human bandwidth available on staff to build the desired capability? If not, then additional short-term or permanent headcount may be required.

Secondly, independent of the available bandwidth, there is sometimes a concrete business benefit derived from speed. Revisiting the scenario in the last section, having an already established intelligence capability in place can differentiate one bid from another, providing a huge potential revenue upside to accelerating the project. This is what ultimately allowed the company using Cyveillance’s feeds to win the major contract. Other drivers that could justify acceleration include the availability of expiring funding such as a grant, or the timing of a major event such as the World Cup or Olympics, which greatly increase the importance or value of standing up a capability faster.
Step 3: Speak Business

In most organizations, the budget holders are not security people, they are business people. The links between the threat intelligence capability and clear business objectives, activities, and results, provide a clear direction for how to couch budget requests in the business language and outcomes that appeal to management.

For example, we have seen several clients struggle with budget justifications because they appear to incur very large first year costs. However, upon review, once they differentiated long-term start-up costs for their threat centers from smaller operational costs, they were able to capitalize much of the up-front expenditure. This dramatically reduced the first-year hit to the department’s operating budget.

While this might seem like accounting administrivia (or even incomprehensible gibberish) to many security professionals, accounting for a six- or seven-figure project correctly can make a critical difference in the project’s acceptance. Knowing how to properly treat the costs and work with finance can be the difference between a proposal that is dead-on-arrival and one that is given serious consideration.

Step 4: Reporting

Finally, it is important to create reporting that will be useful for management, not just the security team. Nominal metrics are operational – lists of alerts, documents tagged, or items investigated. While these numbers are interesting to you, they do not tell management how the organization’s business objectives are, or are not, being met. Meaningful reporting will tie into the drivers for the threat intelligence initiative, as well as a business outcome, such as policies that are changed, employee actions taken, or legal processes initiated as a result of the activities reflected in those nominal activity metrics.

To make the case for procuring threat intelligence, align security needs with the organization’s business objections by envisioning the desired security outcome, using the T.E.S.T. method to determine readiness, translating security objectives into business objectives and language.

We will provide two example scenarios that show you exactly how to create a threat intelligence business case.
Up to this point, we’ve explained why threat intelligence is essential for your security plan, how to map your security needs to business objectives, and how to formulate a plan. The next and final step of making a business case for threat intelligence is to put all of that knowledge together. In this section, we will review two example business case scenarios; one for information security and the other for physical security.

**Information Security Case: Preventing Counterfeits**

Your security team must protect your organization from intentional or inadvertent exposure of sensitive product intellectual property data online. While this is self-explanatory to a security team, tying it back to a business objective may not be as clear.

In this case, the business objective is to prevent knockoffs from diverting revenue from the organization. If plans, blueprints, specifications, or other technical data leak before the physical product is available, it could speed up how quickly knockoff products are released. Thus, any intelligence capability that could help prevent, monitor for, or respond to and remediate such losses of sensitive data could be justified on the basis of protecting that “knockoff free” revenue window.

Here is what a budget justification model might look like for any technology, tool, or resource that can reduce the risk of a “jump start” to the counterfeiting process.
Based on this model that only one product is released per year, it is clear that any capability with the potential to prevent or delay the counterfeiting process by even a few days or weeks may well be worth a modest expenditure. If the company were to release more items more often, this case can be multiplied many-fold.

**Physical Security Case: Preventing Business Disruption**

Let’s apply the same principles to the physical security for a brick-and-mortar retailer. In addition to employee and customer safety, which are security priorities in their own right, there are business drivers that can help justify the costs of a threat intelligence capability. For example, any disruption or protest activity at company retail locations can temporarily stop sales and prevent access to the property, thereby directly impacting revenue. Such events also incur public relations costs, consume management time, and generally create a distraction for everyone involved. Disruptions can also create a negative customer experience that will reduce store traffic and sales long after the event itself has passed.

Many of these types of disruptions are organized, discussed, or planned online via forums, social media, and activist web sites, so intelligence collected from these sources may provide early indications and warnings that allow the prevention or mitigation of such planned activity.
Below is a sample budget justification model for procuring a tool, capability, or service that allows for efficient, cost-effective gathering of relevant, actionable intelligence from social media, blogs, websites, and forums. This uses real numbers based on a retail chain that was recently involved in a highly-controversial set of court cases and political discussions.

**ASSUMPTIONS**

<table>
<thead>
<tr>
<th>ASSUMPTION</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of retail stores</td>
<td>600</td>
</tr>
<tr>
<td>Company revenue</td>
<td>$3,000,000,000</td>
</tr>
<tr>
<td>Average per-store sales annually</td>
<td>$5,000,000</td>
</tr>
<tr>
<td>Average per-hour, per-store sales (open 9-5 M-Sat)</td>
<td>$2,003</td>
</tr>
<tr>
<td>Percent of locations impacted by a coordinated disruption event</td>
<td>3%</td>
</tr>
<tr>
<td>Length of a typical disruption event in hours</td>
<td>2</td>
</tr>
</tbody>
</table>

**CALCULATIONS**

<table>
<thead>
<tr>
<th>CALCULATION</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monthly revenue upon launch</td>
<td>18</td>
</tr>
<tr>
<td>Monthly revenue lost to knockoffs</td>
<td>$72,115</td>
</tr>
<tr>
<td>Value of “no counterfeits” window</td>
<td>$30,000</td>
</tr>
<tr>
<td>Value of each week counterfeiting is accelerated or delayed</td>
<td>$102,115</td>
</tr>
</tbody>
</table>

This model does not factor in the impact of any future sales lost after the event due to negative customer experience or bad press. It addresses only the value of store traffic prevented during the course of the event itself.

If a threat intelligence capability or tool can help provide the early indications and warnings that might allow an organization to prevent potential threats, whether physical or online, then there is clearly a justification for some expenditure for such a capability that provides this protection. When you make the business case for threat intelligence, establishing regular, meaningful executive-level reporting is critical to garner ongoing support for the expense.
The first and most important step when putting together a business case for threat intelligence is to define your need for it and how it will be used at your organization. Once that’s complete, find a way to map your security objectives to your management’s overall business strategy. If you can show the budget holders how a threat intelligence capability will benefit not just you, but the organization as a whole, then you will have a much easier time having your request approved. Lastly, you need to create a plan that includes how threat intelligence will fill gaps within your current capability, as well as regular, meaningful executive-level reporting to garner ongoing support for the expense.
While your network may be secure, do you have visibility beyond the perimeter? Security is no longer about what you can see. What you can’t see is where the true threats hide.

Cyveillance offers an easy-to-use platform that enables security professionals the ability to see beyond the perimeter. Our solutions identify cyber and physical threats and risks across the globe, allowing you to mitigate and eliminate them before they disrupt your business.

We go beyond data to provide the threat intelligence that you need to achieve your organization’s business goals. Contact us today to learn more and get a free trial.


A study by Verizon has shown that the targets of 85 percent attacks are small businesses with less than 1,000 employees. Verizon, “2012 Data Breach Investigations Report.” http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-etok_en_xg.pdf
Cyveillance is the leading provider of cyber threat intelligence, enabling organizations to protect their information, infrastructure, and employees from physical and online threats found outside the network perimeter. Founded in 1997, Cyveillance delivers an intelligence-led approach to security through continuous, comprehensive monitoring of millions of online data sources, along with sophisticated technical and human analysis. The Cyveillance Cyber Threat Center, a cloud-based platform, combines web search, social media monitoring, underground channel information, and global intelligence with investigative tools and databases of threat actors, domain names and IP data, phishing activity, and malware. Cyveillance serves the Global 2000 and the majority of the Fortune 50 – as well as global leaders in finance, technology, and energy – along with data partners and resellers. For more information, visit www.cyveillance.com.

Cyveillance is a wholly-owned subsidiary of QinetiQ, a FTSE250 company which uses its domain knowledge to provide technical support and know-how to customers in the global aerospace, defense and security markets. For more information, visit www.qinetiq.com.