Using the Predict, Prevent, Detect, Respond Framework to Communicate Your Security Program Strategy

Published: 18 April 2016

Analyst(s): Perry Carpenter

CISOs need a clean and consistent way to categorize their communication efforts in easy-to-understand, outcome-focused terms. The predict, prevent, detect, respond framework can serve as a method for bringing clarity to strategic CISO communications.

Key Challenges

- CISOs often experience difficulties when communicating security strategies or initiatives to differentiated audiences, such as other executives, boards of directors, third-party companies or even their own staff.
- High-level information security communications can be inherently challenging, due to the sheer number of moving parts and variety of interested parties.
- Security leaders tend to unintentionally create confusion or dissent, due to cluttered messaging and by going into inappropriate levels of detail for most audiences.

Recommendations

- Adopt the predict, prevent, detect, respond framework to declutter and enforce precision in your security communications.
- Reinforce your messaging by adding icons and other branding methodology to drive instant recognition, understanding and recall.
- Review Gartner’s use-case examples to see how these concepts may be used for different audiences.

Table of Contents

Introduction............................................................................................................................................ 2
Introduction

Chief information security officers (CISOs) often struggle with communicating their vision, strategy and progress effectively and succinctly across the organization. Adopting a simple and consistent framework can help give definition and structure to what may otherwise seem to be a number of disjointed projects and initiatives. This research outlines the use of the predict, prevent, detect, respond (PPDR) framework as a method for bringing clarity to strategic CISO communications (including, but not limited to, budget proposals, initiative descriptions, vision documents and program overviews).
Analysis

The Context of Communication

Organizational cultures vary wildly from company to company. As such, finding appropriate methods to communicate and resonate with the overall corporate narrative and mission is not a one-size-fits-all endeavor. Gartner’s growing body of research and toolkits for security executives contain multiple models for the prudent security leader who is seeking the most appropriate way of communicating effectively. See:

- "Use a Structured Approach to Communicate Your Security Strategy"
- "Articulating the Business Value of Information Security"
- "How to Build an Effective Cybersecurity and Technology Risk Presentation for Your Board of Directors"
- "Board-Ready Slides for Cybersecurity and Technology Risk: Sample Narrative — First-Time Presentation"
- "Board-Ready Slides for Cybersecurity and Technology Risk: Sample Narrative — Funding Request"

Using the PPDR Model as a Go-To Framework for Communicating Strategy

The predict, prevent, detect, respond model is in use within Gartner research to describe a robust security technology strategy (see "Designing an Adaptive Security Architecture for Protection From Advanced Attacks"). The model resonates extremely well across both executive and technical audiences for two primary reasons:

- It is a short and easy-to-remember way of encapsulating critical security functions.
- It reminds audiences that there is much more to security than just prevention.

Because the model resonates so well, Gartner has found it to be an effective model for communicating broadly — in ways not related merely to technology strategy. This research discusses a few of those areas and offers some resources for CISOs to further adopt the model for their own security communications.

Describing the PPDR Elements

- **Predict**: Predictive capabilities enable the security organization to learn from external events via external monitoring of the hacker underground. It can then proactively anticipate new attack types against the current state of systems and information that it is protecting, and proactively prioritize and address exposures. This intelligence is then used to feed back into the preventive and detective capabilities, thus closing the loop on the entire process.

- **Prevent**: Preventive strategies include policies, products and processes that are put in place to prevent a successful attack. The key goal of this category is to raise the bar for attackers by
reducing their surface area for attack, and blocking them and their attack methods before they impact the enterprise.

- **Detect**: Detective capabilities are designed to find attacks that have evaded the preventive category. The key goal of this category is to reduce the dwell time of threats and, thus, the potential damage they can cause. Detection capabilities are critical because the enterprise must assume that it is already compromised.

- **Respond**: Responsive functions are required to investigate and remediate issues discovered by detective activities (or by outside services). They provide forensic analysis and root cause analysis, and recommend new preventive measures to avoid future incidents.

Figure 1. The PPDR Model

Benefits of the Model in Your Communication Strategy

One of the reasons security leaders struggle with effective communication is that they tend to communicate at inappropriate levels of depth for their intended audiences. For instance, many CISOs completely overwhelm their boards of directors (BODs) with technical content rather than having a compelling narrative that invites constructive discussion. Similarly, they approach other executive stakeholders with too much detail, too little context and no unifying idea. For more information on BOD resources, see "Article Top View: The Comprehensive Guide to Presenting Risk and Information Security to Your Board of Directors."

With this in mind, here are a few immediate benefits of broadly adopting the PPDR model:
It provides the unifying idea.

It helps create instant understanding and recognition (branding).

It reduces complexity and enforces greater simplicity.

It provides natural hooks/buckets for answering the what and why questions related to security technologies, processes and directions.

Marketing and Branding for Security Programs

Marketing has many principles that can be beneficial for security leaders in communicating ideas in ways that can influence the audience, and be readily understood and easily remembered. A few they relate to working with the PPDR model are:

- **Make it visual**: Visual cues provide a psychological hook on which you can hang ideas.
- **Make it short**: Too much detail is difficult to remember and tends to cause people to focus on the details rather than the big picture.
- **Make it relatable**: For people to care, they need to understand why something matters.

The following sections will provide details and examples of how security leaders can use these marketing and communication principles.

Make It Visual

Visual cues provide a psychological hook for your ideas, allowing the audience to immediately attach ideas, feelings and even groups of concepts to the image. This means that a single small image can allow you to convey a great amount of context and meaning in a way that is consumable at a glance. As such, you should use visual cues (such as icons) whenever possible and appropriate. In your security strategy, it is possible to use an icon to represent each of the PPDR elements. This has the benefit of enhancing recognition and creates a virtual brand for the principle.

Figure 2 illustrates examples of icons that may be used in presentations and documents for branding each of the PPDR elements. It is important to understand that your choice of icon/image should take into account aspects of acceptability or resonance within your corporate culture. Our recommendation is to choose one icon — and use it consistently — when you are referring to/referencing each of these capabilities. We show multiple icons so you can get a feel for the different ways that an organization may choose to represent the capability.
Make It Short: Embrace a "Less Is More" Mindset in Your Communication

In developing communications, it is important to remember that too much detail tends to breed distraction and dissent. Nitty-gritty-level details are easier to dissect and challenge than a compelling story, and virtually everyone you are trying to communicate with is overly burdened with multiple priorities. It is for this reason that we suggest being as succinct as possible, without being brisk. While you may be tempted to include great levels of justification and key data points about why something is important, keep it to a bare minimum — and offer to follow-up with people who desire greater detail. A good strategy is to keep your core story upfront and have an appendix at the end of your presentation or document that contains more information for those interested. For more on this topic, see "Five Tips for Security and Risk Leaders When Communicating With Business Stakeholders."

Make It Relatable: Tell the Story

As mentioned above, nitty-gritty details are easier to dissect and challenge than a compelling story. Therefore, prudent leaders have learned to package their content in compelling narratives that focus on benefits, drawing parallels and demonstrating wanted outcomes.

Storytelling is a very effective mechanism to get your points across, and it provides a basis for engaging the audience. The narrative need not be complicated; in fact, simple stories tend to
resonate more effectively than overly complex stories. The narrative should be concise and simple, and connect business goals to risks and program objectives.

The three goals for business storytelling are:

- **Inform and educate**: For example, while moving to the cloud for all new business objectives, you may wish to communicate that there are new risks that come with such a paradigm shift.
- **Influence a decision**: For example, maybe the time has come to move IT risk and security out of IT to address segregation of duties and risks.
- **Change behavior**: For example, the enterprise may be subject to high levels of risk resulting from staff signing up for consumer-grade cloud services.

A few tips to consider when creating your narrative:

- Stories need to have a beginning, a middle and an end. This may seem obvious, but many of the presentations Gartner analysts review miss this basic concept.
- It is more important to be interesting than it is to be complete. Data can persuade people, but it doesn't inspire them to act; to do that, you need to wrap your vision in a story that fires the imagination and stirs the soul. If you engage the audience, they will ask questions, and you can provide the data to back up the story.
- Emotion is important. Think about how you want the audience to feel. People remember how they feel more than the details of what you told them. If you start with the feeling you wish to trigger, the narrative will be that much more powerful.
- Use communication experts (e.g., from your marketing and communications departments) to help craft your story lines and graphics.
- Road-test your presentation. Present a draft to one or more business (that is, nontechnical) colleagues to get their view on how understandable your narrative is, and to help you "translate" your messages into appropriate business language.

Note: Gartner plans to publish more research on storytelling for security leaders in 2016.

**Examples for Consideration**

This last section provides a few examples. It is important to note that these examples are not an end unto themselves, but should always be woven into the greater framework.

In planning and reporting functions, consider creating a matrix that covers each of your security processes and technologies, and categorizes them by primary, secondary and tertiary functions. This can be used to help identify strengths and gaps in your overall security coverage. Historically, security programs have focused on building up an arsenal of preventative technologies. As such, when you first inventory your technologies and processes according to the PPDR framework, it is extremely likely that you’ll notice a clear preference for technologies with preventative capabilities as their primary function.
As you consider the need to evaluate efforts across the PPDR focus areas, this matrix can serve as a powerful visual tool to use in project requests for tools and processes that will help address gaps. Additionally, it can be beneficial to add the context of specific business applications, processes and infrastructure areas. Table 1 is a sample matrix that captures all of this information at a high level.

Table 1. Example Capabilities Matrix for Security Processes and Technologies

<table>
<thead>
<tr>
<th></th>
<th>Predict</th>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS/IPS</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
<td>Currently providing coverage of ____. Known limitations with _____.</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>S</td>
<td>P</td>
<td></td>
<td></td>
<td>Currently in monitor-only mode with the majority of the organization. Blocking capabilities only being used for _______ scenarios.</td>
</tr>
<tr>
<td>Threat Intel Feeds</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td>Currently evaluating feeds that relate to our company brand and industry-level threats/trends.</td>
</tr>
<tr>
<td>SIEM</td>
<td></td>
<td>P</td>
<td></td>
<td></td>
<td>Good coverage across the network.</td>
</tr>
<tr>
<td>Employee Monitoring System</td>
<td>S</td>
<td>P</td>
<td>T</td>
<td></td>
<td>Initial deployment with the sales, marketing and customer service teams. Currently detecting and blocking ____ behaviors, and automatically opening investigation tickets for suspicious activities.</td>
</tr>
</tbody>
</table>

P = Primary capability by design; S = Secondary capability — provides some value in this area; T = Tertiary capability — provides extremely limited, targeted value in this area.

Source: Gartner (April 2016)

As with all data, there are many ways to present your findings. The above examples are useful because they are clear about the actual technologies and their capabilities; however, this level of detail is not appropriate for all audiences (as has been discussed). Therefore, it is prudent to develop ways of conveying the critical story in a high-level, easy-to-consume manner. Figures 3 and 4 show examples of a higher-level method.
### Figure 3. High-Level PPDR Capability Assessment

<table>
<thead>
<tr>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
<th>Predict</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Yellow</td>
<td>Green</td>
<td>Red</td>
</tr>
</tbody>
</table>

*Insert a one- or two-sentence strategic insight/comment here.*

1. None or needs attention
2. Good
3. Best in class

Source: Gartner (April 2016)

### Figure 4. Example Individual Capability Strength and Needs

**Our Capabilities:**
- Strong capabilities in ________.
- Solid practice of ________.
- Best-in-class ________.

**Our Needs:**
- Improve our technologies for rapid detection of evolving threats.
- Additional head count for "hunters/killers" to proactively search out threats.

Source: Gartner (April 2016)
As stated above, these examples are not to be seen as an end unto themselves. Rather, they are components in an overarching story, and should be used at appropriate times and tailored to appropriate audiences. The simple mnemonic nature of the PPDR framework, combined with both visual and story convenience mechanisms, will serve security leaders well as they seek to communicate with greater effectiveness.

What About Communicating Nontechnology Areas of Security?

Many of the examples above are demonstrating the value of PPDR in communicating technology-related capabilities; however, PPDR is not limited to technology-related communications. This framework can also be used when referring to, for example, security culture/awareness, governance and policy. For instance, in Figure 1, you’ll notice the reference to "continuous monitoring and analytics." In a nontechnical way, that can be referred to as governance.

Additionally, consider the effectiveness of each of the following as they relate to each of the PPDR elements. Figure 5 is an example of how to use the PPDR model in conducting security culture planning. This could also be used in a matrix format to help evaluate the specific components of an overarching culture management strategy to map each component against PPDR and potentially identify areas where additional focus is needed.

Figure 5. Using the PPDR Framework to Help in Security Culture Planning

Source: Gartner (April 2016)
Conclusion

PPDR is one of a number of tools and methods that are available to security leaders. This research has outlined the use of the PPDR framework as a tool for communicating security strategy in a simple manner, while still enforcing comprehensiveness and consistency.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How to Build an Effective Cybersecurity and Technology Risk Presentation for Your Board of Directors"

"Article Top View: The Comprehensive Guide to Presenting Risk and Information Security to Your Board of Directors"

"Effective Communications: Lead Through Storytelling"

"Five Tips for Security and Risk Leaders When Communicating With Business Stakeholders"

"Articulating the Business Value of Information Security"

"Security Management Strategy Planning Best Practices"

"Use a Structured Approach to Communicate Your Security Strategy"

"What Does an Information Security Strategic Plan Contain?"

Evidence


GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations, visit http://www.gartner.com/technology/about.jsp