[[copy edited by Kezia Endsley]]

TE color code: GREEN check out OK; YELLOW needs attention; RED is an error that needs fixing

Editors: The authors use “consumer” to refer to the people who read and use the reports and dashboards, and “producer” to refer to the people to create them. I’m not a fan of this usage because both terms imply aspects of each and also there relationship that don’t hold. I think it would be simpler and more direct to use “reader” or “viewer” for the first and “analyst” for the second. I’ve been going with your suggestion in the chapters (reader/viewer/analyst). Kezia

AR: understood.

Also, I am not comfortable with the use of abbreviations like “OSSIM” and “IPS” that are not spelled out. I’ve inserted a few of these. Of course, an alternative is to have a separate appendix for definitions. Either way works, but I don’t think it is respectful to the reader to expect them to know all of these, even if 99% of readers know 99% of abbreviations.

AR: agreed. fixed. Thx.

Chapter 10: Designing Effective Security Dashboards

[AU: Some of the figures in this chapter require eps versions to accompany the readable PDF I have. Please send eps versions for the PDF figures in this chapter. And though I don’t see any code listings in the chapter, there was a download accompanying, so if there are any code changes or if you add some, please resubmit the code download after AR. Thanks, Kevin (PjE)]

AR: done. Thx.

Perfection is achieved, not when there is nothing more to add, but when there is nothing left to take away.

Antoine de Saint-Exupéry, Airman's Odyssey

Just when you thought it was safe to leave the comfort of your analytics lab to grab another caffeinated beverage you find yourself in a conversation with one of the security managers and are asked the inevitable and dreaded question, “Can you help us build a security dashboard?” If that sentence did not cause even a flicker of your own fight-or-flight response, you may not truly understand the difficulty of designing succinct, meaningful displays of quantitative information in order to drive some type of action. This chapter presents techniques and advice that will enable you to design dashboards to help measure, monitor, and mobilize every layer of security in your organization.

[AU: Nice opening paragraph. Thanks, Kevin (PjE)]

What Is a Dashboard, Anyway?

It’s nigh impossible to discuss the subject of dashboards without quoting the definition of *dashboard* coined by the “Godfather” of dashboards, Stephen Few:

A dashboard is a visual display of the most important information needed to achieve one or more objectives that has been consolidated in a single computer screen [or printed page] so it can be monitored at a glance.

—Stephen Few, *Information Dashboard Design*

We’ve added “or printed page” since organizations are still quite fond of paper and there are special design considerations when including printed output.

We can make Few’s definition a bit more real by phrasing it another way: A dashboard provides a single screen/page opportunity to provide the most critical/relevant information in the most concise and effective ways possible to enable the viewer to quickly understand the elements being described and, if necessary, make the most appropriate decision(s).

If you present data that is irrelevant, your dashboard will not be used. If you have too many or too complex encodings, your dashboard will be ignored. If it’s ugly . . . well, at least you won’t be asked to make dashboards anymore! Dashboard creation truly is a daunting endeavor. To fully grasp the nuances of what a dashboard *is* we’ll start by chipping away at the marble block of what a dashboard *is not* to reveal the underlying true nature.

A Dashboard Is Not an Automobile

The term *dashboard* originally referred to a board in a horse-drawn carriage that helped prevent mud from splashing on occupants. When the automobile was invented, the term morphed into something that we all recognize today as the crucial set of performance indicators available to drivers. It was this familiarity (almost everyone knows what an automobile dashboard is) that caused the computer industry to associate the term with the summary displays in executive information systems.

The automobile dashboard has the elements it does because they make sense in context. Gauges react to the point-in-time changes we make when accelerating or decelerating; we get an accurate—but not necessarily precise—understanding of fuel supply and battery condition; and, we know how far we’ve gone—all at a quick glance. Somewhere along the way, designers of executive information systems forgot the concept of “makes sense in context” and brought these (and other) real-world elements into the digital world.

Gauges, dials, thermometers, stoplights, and other skeuomorphic elements consume valuable space and rarely communicate information better than other visual elements, but they *can* hold useful information, including:

* Current value of key measure(s)
* Comparison to target measure(s)
* A range of possible values of the measure(s) with a qualitative association

Consider Splunk’s dashboard example for “Notable Events by Security Domain” gauges in Figure 10-1. The gauges are *huge* and the information displayed in each—47, 81, 8, 2, 31, 30— is repeated in the top-level labels, making them also redundant. It’s also hard to mentally correlate the gauge needle position to any type of urgency, since each one has a giant red arrow above it but not all needles being in the red zone on the gauge.

Figure 10-1: Sample Splunk dashboard [793725 c10f001.png]

[AU: What should readers be getting out of this figure. What do you want them to see here? Indicate that before moving on to the next example because I don’t think it’s fully clear yet. Also indicate that you do not think this is the most successful presentation of this information. Help the readers to “read” each figure before moving on. Thanks, Kevin (PjE)]

AR: not sure why I left out the explanation to begin with. Thx. Done.

If you apply the knowledge gained from Chapter 6, you can combine a few basic plots to make what’s known as a *bullet graph* and replace the skeuomorphic gauges (see Figure 10-2), although you have to invent some of the comparative measures and guess at the quantitative scale since the original did not encode those well (or at all). This new view makes it much easier to see where you are exceeding event thresholds in various areas than you could in the figure using the gauges.

[AU: Addition okay? I finished the comparison to draw it back to the other figure. Thanks, Kevin (PjE)]

AR: aye. Rly good addition.

Figure 10-2: Bullet graph makeover [793725c10f02.png]

type="general"

Bullet Graph Basics

The bullet graph is a fairly new chart type, especially when compared to more traditional visualizations, such as bar charts and line graphs. It was invented in 2005 by Stephen Few as a way to incorporate the positive attributes of gauges into a more utilitarian graphic. As such, there is a bit of a learning curve both in creating them (encoding) and understanding (decoding) them.

As seen in Figure 10-3, there are five core components of a bullet graph:

* A bar that encodes the *performance measure* of the actual item you are measuring and trying to communicate the value of
* The overall *scale* of measures
* At least one marker with a *comparison measure*
* Background shades or colors that represent qualitative ranges for values
* A label for the bullet graph

[AU: I moved the figure slug to after the reference in the text to the figure. Thanks, Kevin (PJE)]

AR: cool. Thx.

Figure 10-3: Elements of a bullet graph [793725 c10f003.eps]

The sixth component shown in Figure 10-3—the actual value of the number of events per second being processed by the security information and event management (SIEM) system on the right side—is optional, but useful if your viewers need more precision.

Although these examples are sized a bit larger for the purposes of explanation, bullet graphs resize/shrink quite well without losing their ability to communicate effectively and efficiently.

[AU: Addition below okay? You are referring back to Figure 10-1, right? Thanks, Kevin (PjE)]

AR: yep. Good. Thx.

The value change is also important to display, but the giant red, upward-pointing arrows in Figure 10-1 do not help to tell an accurate story. You can augment the bullet graph with paired sparklines—“data-intense, design-simple, word-sized graphics” (from Tufte and Graves-Morris, 1983, which you can find in the references in Appendix B of this book)—of each 24-hour measure to provide a quick picture of what happened in the various event streams. See Figure 10-4.

[AU: Above, should that be Tufte and Graves-Morris above or is just Tufte correct? Thanks, Kevin (PjE)]

AR: my bad. Yes. Graves-Morris never gets the spotlight. Corrected. Thx.

Figure 10-4: Sparklines [793725 c10f004.png]

The file ch10/R/bullet.R on the book’s web site ([www.wiley.com/go/datadrivensecurity](http://www.wiley.com/go/datadrivensecurity)) shows how to create bullet graphs in R, but you can easily create basic bullet graphs in Google Charts by building a simple URL such as (enter the following as one, contiguous line in your browser or look at the example in ch10/docs/bullet.html):

http://chart.apis.google.com/chart?cht=bhs&chs=250x30&chd=t:93

&chm=r,DDDDDD,0,0.0,0.57|r,999999,0,0.57,0.85|r,888888,0,0.85,

1.0|r,FF0000,0,0.85,0.86&chco=000000&chbh=15

You can even use of Excel to make enhanced visualization elements. The source for the sparklines used in Figure 10-4 can be found in ch10/docs/ch10-sparklines.xlsx, and Excel offers both sparkline and “sparkbar” chart options with many options for customization.

Ironically, Splunk has a rich visualization library that includes bullet graphs and sparklines, so if you’re building your dashboards in that tool, ditch the gauges and switch to the more informative options.

There was nothing in the code zip archive for “enhanced dashboard elements” in Excel, R, or Google Charts. //Author, Please make sure what you say is going to be in the download is there, and give the readers specific folders to go to and filenames to look at so they know exactly where to look. Thanks, Kevin (PjE)

AR: done. Thx.

A Dashboard Is Not a Report

IT and information security professionals tend to be very detail-oriented people. They are the type of people who get excited at the “show your work” directive on school assignments and love to dig into the details to show folks how they arrived at their conclusions. It’s absolutely necessary to have multiple levels of detail behind the dashboards you create to enable verification/validation and to support drilling into specific areas as needed. However, the top-level view should be designed solely to give the viewer situational awareness of the desired task. Just because the onboard diagnostic system in an automobile *can* tell you the value of the “Bank 2, Sensor 3: Oxygen sensor voltage, Short term fuel trim” does not mean that we need another gauge in our cars that displays this value while we’re driving. The “check engine” light is enough for us to know that something requires more deliberate attention and detailed examination.

Do not take this caution to mean that you shouldn’t use text, lists, and tables in a dashboard. Those elements are valid to include where you need precision, provided they support quick perception, comprehension, and a call to action. If you wanted to communicate number of events per second being processed by the SIEM from Figure 10-3 with just straight text, there are multiple possibilities to choose from, as shown in Figure 10-5, including plain text or colored text (if highlighting the value as “interesting”) or even a simple textual table. If you really just need to drive action with out presenting underlying detail, the simple “Variance +43%” statement should be enough to motivate someone to find out why the system is suddenly seeing 43% more events than usual.

Figure 10-5: Encoding measures with text [793725 c10f005.eps]

[AU: Again, why don’t you briefly explain what the readers are looking at, and what you want them to take away from these different presentations. Thanks, Kevin (PJE)]

AR: done. Thx.

As indicated in Chapter 6, it’s usually best to display a graphic instead of large amounts of tabular data. Numbers and text always require attention whereas shapes and colors can draw attention preattentively. Just be ready to call up specific values or provide a data table if there is a call to action that requires a detailed review before making a decision. This can be easily done online, since most dashboard-creation tools provide some sort of drill-down capability. For printed or non-interactive dashboards, you can provide a standalone, supplemental report or a link to an online resource that supports further investigation.

type="general"

When Dashboards Fail

Dashboards establish a partnership between the viewers and producers. Viewers need to trust that the summarized views they are interpreting represent a good-faith attempt on the part of the producers to provide the most accurate data in the most effective way possible. Similarly, producers must have some assurance that the “messenger won’t be shot” for providing honest, accurate information.

This seems obvious, but how many times have you been in a dashboard review meeting where you cringed at some measure being reported as acceptable when you *knew* that there was cause for concern (especially as it relates to the status of highly visible projects). This is a situation even the most elegantly crafted dashboard cannot resolve. Chapter 6 presented the concept of “truth” as it relates to data, and it’s vital that a dashboard always display truthful measures if an organization is serious about managing operations with them.

Dashboards also fail when they regularly miscommunicate or over-communicate the performance measures. It’s a far easier task to make a lazy guess and put a green stoplight in a PowerPoint document than it is to admit you don’t have enough real data to back the analysis and quantification of an important measure. Similarly, if the viewers always review the supporting material for every performance measure, they probably don’t trust the producers and should trade their dashboards in for reports.

[[Author: “take a swag at something”? Do you mean take a swing? I don’t recognize this saying as it is... Kezia]] //Authors, Will that be too slangy? Just write “to make a guess” instead? Thanks, Kevin (PjE)

AR: remove techno-slang ☺ thx.

A Dashboard Is Not a Moving Van

Boxes are great for shipping items, but they are detrimental to the effective display of information on a dashboard, as seen in Figure 10-6.

Figure 10-6: Sample “boxy” dashboard [793725 c10f006.png]

[AU: We’ll need a version of this that is not a jpg. A tif or png would be best. Thanks, Kevin (PJE)]

AR: done. Thx.

Most of the elements contained in those boxes are themselves boxes, making the extra framing redundant. Excessive framing is often an issue with online dashboards. This is because many interfaces tend to align items in singular cells in a fixed grid and provide options for “on-the-fly” modification.

Figure 10-7 shows a transformation of Figure 10-6 using Microsoft Excel. You start by removing superfluous markings, borders, and annotations. We also take the opportunity to change the encoding of some of the measures to enhance the readability.

Figure 10-7: Dashboard makeover [793725 c10f007.eps]

Whitespace now frames each element and there is a more cohesive feel to the entire dashboard. We’ve removed the map, since a color-coded table is a better choice for the type of information displayed. We’ve also replaced the “funnel” with a normalized, grouped bullet graph. We significantly reduced the “chartjunk” and used a more subdued but deliberate color. You can find an Excel version of most of the components for this example in ch10/docs/ch10-overhaul.xlsx, which should be a good starting point for your own dashboard makeovers.

There are still some core issues with this dashboard. The individual elements seem haphazardly chosen and put together with almost no opportunity for logical groupings. The foremost issue is that there are no indicators of what is good or bad (we had to fabricate thresholds for the bullet graphs in order to use them). Without those indicators, a dashboard like this more appropriately belongs in the “report” category, although it falls short of those requirements as well.

type="general"

Dashboard Excel-lence

We chose to model the dashboard in Figure 10-7 in Excel, as this will likely be the only tool available to most readers. Books dedicated to dashboards often provide examples of perfect dashboards that require specialized tools or post-processing by hand in applications like Adobe Illustrator to generate. With a *little* extra effort, it *is* possible to make well-designed charts, graphs, and dashboards in Excel.

It’s important to note that the single-cell, fixed-grid is not your only option. Figure 10-8 shows sample layout combinations. These layouts can layer on top of a virtual landscape grid to provide more room for larger or more prominent chart types or to allow for logical groupings of elements that naturally fit together. You must take your output medium into consideration when planning your dashboard elements and layout. Your dashboard may look wonderful on the 27-inch “retina” display where you designed it, but it may be unintelligible on a standard resolution, 15-inch laptop screen. There may also be times when a vertical (portrait) layout works better with your data, so you should not box yourself into a corner by having only one layout system handy.

Be sure to follow the advice on eye movements in Chapter 6 and reserve the upper-left area for the most critical information that needs attention by your viewers.

[[Author: This figure shows a bunch of empty boxes--is that correct? Kezia]] //Author, The CE is right. The PDF we have of Figure 10-8 doesn’t show us anything. Please resend a new version with your author review. Thanks, Kevin (PJE)

AR: Removed it. Originally wanted to show different grid systems (hence my ask a few weeks ago to see if your graphics ppl cld make some magic happen here).

A Dashboard Is Not an Art Show

Given the graphical nature of dashboards, it’s easy to fall into the trap of making them look like pieces of modern (or fringe) art when they are far more akin to architectural/industrial diagrams that require more controlled, deliberate, and constrained design. To put it simply: Just because you *can* do something in the context of a dashboard does not mean you *should*. Take Figure 10-9 (from http://www.securitywizardry.com/radar.htm), for example.

Figure 10-9: Example of a monitoring dashboard from Security Wizardry [793725 c10f009.png]

[[Author/Kevin: Is this figure big enough to be legible? It looks pretty tiny on my screen. Kezia]] //Author, Can you give us this figure in higher resolution? I doubt this will be legible at all in print. Thanks, Kevin (PJE)

AR: Switched it around to an even more egregious example.

This is an example of a situational awareness dashboard from Security Wizardry. It uses the “modern” light-on-black design with quite a diversity of colors and tries to pull in data from multiple sources. It’s “glitzy” but it is not informative.

The system dashboard in Figure 10-10 pushes the artistic envelope even further with considerable use of various 3D charts. If you can overlook the redundancy between the “Recently Completed Scans” and “Current Threat Level” panels (even with the discrepancy between where the gauge reports the value versus the marked, segmented bar), you are faced with having to spend real mental cycles processing 3D shapes for “Current License Usage” and “Total Vulnerabilities Last 12 Months” when a simple numeric value would have sufficed. The pyramid in the “Vulnerability Severities” forces you to perform even more cognitive processing to decode and inverts the usual “most critical on top” rule that is usually associated with triangular charts. In other words, you spend far more time deciphering and decoding these panels than understanding what information they are trying to convey and reacting to those messages.

Figure 10-10: 3-D dashboard [793725 c10f010.png]

[AU: Quickly reflect on why Figure 10-10 isn’t an effective dashboard. Again, let the reader have a way to read the figure. Thanks, Kevin (PjE)]

AR: done. Thx.

To be effective, dashboards must be pleasant to view, so there must *some* amount of artistic choice going into the creation. However, it’s necessary to design within constraints. It’s similar to the difference between free verse poetry and more formal types⎯such as a haiku or a Shakespearean sonnet⎯where constraints provide context for creativity without muting it in any way. Likewise, there are some design guidelines that can help channel your creative side when building dashboards.

Limit Chart Types

When encoding information into a chart, stick with the ones that are easiest for viewers to decode. Some good choices are:

* Bar graphs/bullet graphs
* Dot plots/scatterplots
* Line graphs/sparklines
* Boxplots
* Spatial maps/heatmaps/treemaps

[[Author: heat maps and sparklines were not covered by name in chapter 6. Also, bullet graphs were introduced in this chapter. Might just be best to delete that reference to chapter 6 above. Kezia]] //Author, The CE has a point there. Not all those are covered explicitly in Ch. 6. Thanks, Kevin (PJE)

AR: agreed. Removed reference.

Limit the diversity of chart types used in any single dashboard and ensure that the chart you’ve chosen is the most appropriate one for the type of information you are encoding. Tools such as Chart Chooser (http://labs.juiceanalytics.com/chartchooser/index.html) by Juice Analytics and Chart Suggestions (http://extremepresentation.typepad.com/files/choosing-a-good-chart-09.pdf) can help refresh your memory if that book isn’t handy and you are unsure which chart to use.

Remember Space Constraints

You have one page or screen. That’s it. Choose the best encoding element for the medium you are using. This may mean re-thinking the types of elements you choose if you learn your viewers prefer viewing information on their phones or mini-tablet-sized screens.

You should also be wary of cramming elements into that single screen and use whitespace whenever possible to group and separate elements. If the information density of the dashboard is too high to enable the use of whitespace, subtle placement of very light lines and borders can facilitate the same grouping and separation.

Take Care with Colors

Choose a focused color palette and stick with it throughout the dashboard. Color has a strong ability to tie elements together, even when they are separated onscreen. Your viewers may draw erroneous correlations if your dashboard lacks color consistency. Take a look back at Figure 10-7. We deliberately used consistent colors for categorical measures⎯(High, Medium, Low) and (Incidents, Intel, Exposures)⎯to logically tie elements with similar attributes together even though they were not physically grouped together.

Remember the lessons of Chapter 6 and also consider that your digital creations may find their way to black-and-white laser printers more often than you would like to admit. The charts in the dashboard in Figure 10-7 lose much of their meaning when they become black and white (Figure 10-11). In this case, we knew our graphics were destined for a four-color press. Make sure *your* creations can withstand such a transformation without completely losing their meaning.

Figure 10-11: De-saturated dashboard [793725 c10f011.pdf]

Use Fonts Wisely

\*\*\*Layout: the word *color* below should be in a second color, not black\*\*\*

Stick to a single font if at all possible. Choose serif (such as Palatino or Times New Roman) or sans-serif (such as Verdana or Arial) and be consistent where and how you apply the font. If you look to more modern or esoteric font choices, be sure to select one that scales consistently, supports variable width text, and has fixed-width numbers. Finally, use **bold**, *italics,* and **color** sparingly with fonts to highlight only the most important qualitative elements.

type="general"

No One Dashboard to Rule Them All

Dashboard Evolution

From their first physical incarnations, dashboards have been living, evolving organisms. For example, the dashboard on the Ford Model T—produced in 1908—contained a single element: an *ammeter* (an instrument used to measure the electric current) that helped show the health of ignition system. It was one of the only components that could not be visually inspected without a specialized instrument. To know the status of gas reserves, you just checked the dipstick. To see whether the car was overheating, you just looked for the signs of smoke and steam coming out of the engine compartment!

Drivers who were concerned about violating the speed limit (8 mph city/20 mph highway at that time) *could* purchase an optional speedometer, which eventually joined the ammeter as standard equipment years later. It was also possible to replace the radiator cap with a *motometer*, a very fancy and expensive temperature gauge that was more ornamental than operational (perhaps a sign of things to come in modern dashboards?). As drivers became more dependent on the automobile, other elements were added to the dashboard out of both need and convenience.

Dashboards in many modern vehicles retain most of the same elements as the updated Model T instrument panel, but some require new and customized elements to, say, monitor the performance of their electric, natural gas, or hybrid systems. Similarly, vehicles that can switch between two-wheel and four-wheel drive require a special indicator letting the driver know which mode they are operating in.

An Iterative Process

This same process of evolution and customization should occur in the digital realm where each dashboard must be tailored to:

* The specific process(es) being monitored
* The viewers of the information
* The display medium
* The data available for encoding
* The expected update frequency

For example, when creating a dashboard for the chief information security office (CISO), it’s unlikely your that executive will care about the number of events per second being processed by the SIEM. However, this is a performance measure that the Security Operations Manager may be keenly interested in, especially when if there have been performance issues with the SIEM.

[[Author: Will your readers know what the CISO is above without explaining or spelling out this first time? Also, the last half of that sentence was very confusing--who was *she*, for one? I assumed you meant your viewer here?? Please check my edits for accuracy. Thanks, Kezia]]

AR: re-worked it and made sure to define SIEM waaay earlier.

Indeed, if SIEM issues are emerging, you should consider adding salient performance measures to the interactive, daily or weekly operations dashboard until the situation is resolved. Once stable, the measure can be replaced with other important items requiring evaluation and response. Thoughtful, regular updates to dashboard’s core content will help keep it fresh and—more importantly—reviewed and processed by your viewers.*If a dashboard developed 2 years ago has never changed a single element, chances are good that your organization is not using dashboards effectively.*

The only way to know what truly belongs on a dashboard is to have regular dialogue with the various viewers/process owners to understand what *they* care about and inform them as to *what data is available*. Ask them to identify what they view as the model for the processes or objectives they find most important. Ask them how they mentally assess the efficacy of those models now and then ask them what data would help support a more quantitative view of this model. This will help you make the dashboard a success while also identifying and resolving gaps in your ability to provide situational awareness for a given process.

Communicating and Managing “Security” Through Dashboards

There is an inherent “call to action” nature to dashboards, with each element being either quantitative (has a value) or categorical (a list of items). Most of us have a great deal of readily available quantitative data related to information security ranging from lost assets, to security incidents, to SIEM events-per-second, to firewall/IPS operational data. In order for this data to be useful in the context of a dashboard, these quantitative measures must be able to answer two questions:

* What’s going on?
* So what?

For the categorical measures, you are usually identifying a set of elements that provide

* **useful information**—such as “which incident handlers are primary for the day?”;
* **require the most attention**—such as “which Payment Card Industry Data Security Standard (PCI DSS) controls are slipping?”, or
* **need follow up**—such as “what are the top expedited firewall port open requests?”.

[[Author: Will readers know what PCI controls are without explaining above? Kezia]]

AR: most likely, but I’ve heeded the guidance to define the acronyms

Let’s take a look at these measures through some examples.

Lending a Hand to Handlers

The incident response team has asked for help in creating an incident response dashboard and—among other items—would like a view of “bad port” activity. You decide, without probing any further, that the problem is the number of denied firewall transactions for a port for the month-to-date, so you whip up the graphic shown in Figure 10-12.

Figure 10-12: Top port denies [793725 c10f012.eps]

Although the chart answers *a* “what’s going on?” question, it may not fully answer *the* “what’s going on?” question for the incident response team. It definitely lacks an answer to the “so what?” question. It’s back to the drawing board and back to the incident response team to see if you can glean more about what they are looking for and whether you have the data to support it.

Through your investigation, you learn that the team really wants a view of the top five ports with *anomalous* activity. This is quite a different measure than just a raw port count and requires answering both questions⎯“what’s going on” and “so what?”⎯ in order to provide the view they are looking for.

In general, “what’s going on?” will be a count of some kind (it’s a quantitative value, after all). For the anomalous port measure, what will you count? Session attempts and/or bytes transferred? What time frame will you count over? The past hour, intra-day to now, or the past week/month? Will you focus on denies and accepts or just denies (which will shape the answers to some of the previous questions)?

After further consultation with the team, you agree that “what’s going on” is answered by counting denied attempts over the past 24 hours. But…so what? This measure alone has little value. It requires context or comparison to be useful and comparisons are trickier than you might expect at first glance. For the port activity, for example, do you compare the measure against:

* The same port’s position in SANS trending port list (<https://isc.sans.edu/trends.html>) for that time period (that is, the same measure but from a different source)?

[[Author: Will your readers know what SANS is above without explaining or spelling out this first time? Kezia]]

AR: in this case, yes. No one *ever* refers to what the acronym stands for and I suspect including it would cause more confusion than elucidation. I added a URL for context;

* The same value against the same 24-hour period (that is, the same day of the week) at one or more points in the past?
* The same value against a different 24-hour period (that is, a different day of the week)?
* The same value as it relates to daily activity across the previous week or month?

If you choose to compare the port activity against the same value for the same day the previous week (in this case, percentage change from previous week), you get a much different view/list (Figure 10-13).

Figure 10-13: Top anomalous ports [793725 c10f013.eps]

Knowing there was a 2,000+ percent change in volume for this port is definitely more actionable that a raw session count. That’s a significant change that should trigger an investigation into *why.* For example, you might examine which nodes were involved in the communication, check to see if external Information Sharing and Analysis Centers (ISACs) identified malicious activity on this port. Although it’s not perfect, it’s a good starting place for this new dashboard element. As the team uses this data and as you perform additional exploratory data analyses using the other comparative conditions, you may find that one or more of the other measures works better for the team.

[[Author: Will your readers know what ISACs are above without explaining or spelling out this first time? Kezia]]

AR: modified it

Raising Dashboard Awareness

Your dashboard prowess is garnering quite a bit of attention with your latest request coming from the CISO. She wants a new measure added to the CISO dashboard that shows how well the new security awareness initiatives are working. You can’t say “no” to the CISO, but this request lies far outside your comfort zone of bytes, sessions, and IP addresses. How are you going to measure the effectiveness of an awareness program?

Consider the advice offered on the website of the SANS “Securing the Human” project(http://www.securingthehuman.org/resources/metrics). There, you will find some seemingly “easy” measures such as “percent completion of annual security awareness training,” but t these you should quickly dismiss.. That example may be good for a compliance dashboard, but it’s not what the CISO is looking for. Instead, there are some good candidates that you can hone in on:

* Tracking the number of people who fall victim to a phishing attack
* Tracking the number of people who detect and report a phishing attack
* Tracking the results from a comprehensive security awareness survey

You might offer these to your CISO to see which one(s) meet her objectives. After your discussion, she chooses to go the security awareness survey route. For you, this means working with the appropriate internal groups to regularly set up the survey, select the recipients, distribute the survey, and collect, analyze, and publish the results. However, dealing with the mechanics of the survey is the easy part.

This dashboard request is going a bit more smoothly than the last one, but still poses some challenges. Which part of the organization is going to get the survey and when will they receive it? How frequently will you run the survey? What supplemental data will be required if the CISO asks for more information?

Although it may seem intuitive to decide who will receive the survey, you actually need to step back and define whom you want to describe with the survey. In statistics, this is known as defining the *population* from which you want to sample. For example, if you want to measure all employees, you should survey a random sample of employees. If you limit these surveys to one or two departments, you could be introducing bias and might not be able to apply these results to all employees. You may also want to think about how and if this survey will be repeated. If you know the survey will be repeated and you want the results to be comparable (conducting a *benchmark study*), you need to focus on standardizing the questions and the long-term goals. Conducting a survey like this has some challenges and pitfalls, but with a little preparation you can get some interesting and informative data from surveys.

After significant collaboration, you decide to focus on new hires as the population, so the samples are defined as the monthly new hires as the survey recipients. Most of these individuals are completely unfamiliar with the security awareness program. There is a full multi-month training program that interleaves security awareness messages throughout this introduction period. By waiting 3 months after the hire date, you can see how much each new hire class retains. You can also get a feel for how tweaks to the awareness program impact new groups.

You get only one measure for the CISO dashboard, so let’s opt for the summary effectiveness metric recommended by SANS (the calculation is documented in their survey materials). See Table 10-1.

Table 10-1: Security Program Effectiveness Measures

|  |  |
| --- | --- |
| Security Awareness Risk Level | Description |
| Low (25-39) | Users are aware of good security principles and threats, have been properly trained, and comply with all organizational security standards and policies. |
| Elevated (40-60) | Users have already been trained on organizational security standards and policies; they are aware of threats, but may not follow good security principles and controls. |
| Moderate (61-81) | Users are aware of threats and know they should follow good security principles and controls, but need training on organizational security standards and policies. They also may not know how to identify or report a security event. |
| Significant (82-96) | Users are not aware of good security principles or threats nor are they aware of or compliant with organizational security standards and policies. |
| High (97-120) | Users are not aware of threats and disregard known security standards and policies or do not comply. They engage in activities or practices that are easily attacked and exploited. |

Source: http://www.securingthehuman.org/resources/metrics

The benefit of the SANS approach is that you get standardized questions and a defined and open source method for computing the metric. This should provide a good measure for the CISO and you can refer to the individual responses to the survey questions when you’re asked for more details. This new process also tracks the number of new hires per survey, the primary “handlers” responsible for the new hires during their introductory period, and the date the survey was held along with the survey results. None of this detail should or will make it to the dashboard chart, but may be invaluable when seeking to make changes based upon the dashboard element.

As this new process runs, data is accumulated and the awareness performance measure becomes populated. As you can see in Figure 10-14, the measure begins to trend in the wrong direction but never gets to the point where it needs immediate action; instead it seems to level off. Rather than bombard the CISO with colored bands, this method uses subtle, colored level markers that delineate when an individual month measure moves into a different zone. It also shows, at a glance, how well the awareness program is performing.

Figure 10-14: Security awareness risk [793725 c10f014.eps]

The CISO becomes curious and asks someone to look at the supplementary data you collected to see what happened in June and July. It turns out that there is usually a single “handler” for the new hires and she was out on maternity leave in June and July, leaving a substitute to take her place. The new individual was not as familiar with the security elements of the new hire program and did not follow up in the same ways the primary handler typically does. Because of this knowledge, the CISO was able to ensure that all potential handlers were familiar with the elements of the security awareness program.

This measure will no doubt change yearly. Once there is a comfort level that the awareness program is reaching new employees, you might want to consider running the survey against other areas of the organization or switch to one or both of the phishing measures to get a different view of program effectiveness.

The Devil (and Incident Response Delays) Is in the Details

Just as you are about to dive into a new data set, you get an instant message from the incident response manager stating that her dashboard is “broken.” Since you take a great deal of pride in your professional work, you head down to her office to see what the problem is and (hopefully) find a quick resolution.

It seems that she received a call from one of the application teams complaining about how long it took to resolve an incident last week. She was surprised, given that there were no indications on the weekly dashboard that anything was amiss. The performance measure showed that Tier 4 incidents (the level of the incident that was flagged by the application team) were handled within the standard one-day timeframe. You immediately suspect what’s causing the issue and you head to the data to validate your assumptions. Sure enough, the culprit lies in the name of the performance measure itself: “*Mean* Time to Incident Resolution.”

The *mean* is often used as a singular, descriptive statistic for a data set and it *can* be used as a quick comparative measure of performance (such as batting average in baseball), but it isn’t perfect. Consider the resolution times (in days) for the incidents on the “broken” dashboard:

0.50 1.10 1.10 1.10 0.10 0.30 0.20

0.10 0.60 0.10 0.10 0.10 0.60 7.00

The mean works out to be 0.9286, which falls within normal parameters. Now, look at the last value (7.00). This incident took substantially longer than normal, but did not generate a call to action on the dashboard. There are a few ways to fix this. If there is room, you could add a new performance measure that lists all incidents that fall within a certain percentage outside of an expected range. However, the incident manager really likes the single line encoding you’ve provided for the measure:

MTT Incident Resolution: 0.93

You need to come up with a way to programmatically identify problematic conditions and fit the encoding in the same space without losing any detail. The ultimate solution comes from three data analysis and visualization allies: the five number summary from Chapter 3, boxplots from Chapter 6, and sparklines (introduced in this chapter).

As a refresher, the five number summary consists of:

* The minimum (smallest observation)
* The lower quartile or first quartile
* The median (middle value)
* The upper quartile or third quartile
* The maximum (largest observation)

These values are important for encoding many types of performance measures and can be used to succinctly summarize data without losing as much detail as you currently do with the mean alone. A boxplot provides a visual representation of these values that you can augment with a line for the performance measure threshold, as shown in Figure 10-15.

Figure 10-15: Boxplot sparkline [793725 c10f015.eps]

The incident manager now has an at-a-glance view that encodes valuable details without sacrificing space. If necessary, the boxplot can be color-coded to more overtly call attention to measures outside normal parameters. The mean value can be displayed next to the boxplot if that measure still provides value.

Projecting “Security”

The word “security” is in quotes here and in the section title because the definition of security is up to individual interpretation. A penetration tester might think of security in a completely different way than a CISO, just as an application developer will likely have a different view of it than a firewall engineer. From a big picture perspective, these interpretations are complementary because they are all parts of a whole. Each activity is necessary to ensure the protection of an organization’s information assets.

Perhaps one of the least “security-like” elements that readily lends itself to a dashboard is the venerable project or task “status view.” This could involve tracking projects for remediation of internal audit issues or monitoring full-scale, enterprise-wide security programs. Security, IT, and business executives need some way to get a quick overview of all these moving parts so they know where resources and attention should potentially be redirected. It might not be sexy, but there would be little happening in “security” without this governance layer.

If you become known as the “dashboard person” in your organization, you must face the inevitable request to build a set of measures to track program, project, and remediation status. These initiatives will have their own set of detailed measures and reports, which project and program managers will gladly provide. The challenge lies in how to communicate the status of 35-50 (or more) measures at a glance as one component of an executive-level dashboard.

The first step is to identify the components that your viewers want to track. For our make-believe organization, the components will be:

* Internal audit issues remediation items
* Enterprise-wide security program initiatives
* Customer audit-remediation process (these are the items your customers are requesting that your organization remediate)
* PCI DSS compliance controls remediation progress

From your discussions with the CISO you know that you are constrained to one quadrant of the executive dashboard and that the items of most importance to her are PCI controls and customer audits. You’ve verified that the data for the performance measures are readily available and accurate and you set off to meet this challenge head on.

The prioritization and list of measures provided by the CISO gives you logical groupings for the measures you need to encode. For each group, you must decide how to prioritize the elements within the group. Given that all of these elements will themselves be grouped together, the individual encoding for each measure you choose should be common across all four groups. Finding a way to satisfy all these constraints will create a seamless message for the “Security Program, Project & Remediation Status” dashboard component.

[[Author: something is amiss above? “will tie create??” Kezia]]

AR: indeed. Fixed. Thx.

After reviewing the data, you settle on four sections and draw a rough sketch showing how you want to present the information. This sketch eventually turns into the wireframe concept, as shown in Figure 10-16 (the phrases “Lorem ipsum” are placeholders for real text labels).

Figure 10-16: Dashboard wireframe [793725 c10f016.eps]

This will become a common process for your dashboard development:

1. Stakeholder/viewer identifies a need.

2. You work to understand the need and determine if you have the data to support the dashboard or dashboard element.

3. You sketch a set of rough concepts for the dashboard, and then wireframe and model the ones that seem to work best.

4. You choose a final model and find the most efficient process to encode the measures in support of the frequency requirements.

[[Author: Lists that follow a sequential order should be numbered, hence my edits above. Kezia]]

AR: aye. Thx. As you have no doubt noticed, I seem to live in a “bullet” world vs numbered bullets.

For encoding each list of items, the proper order becomes apparent after examining the project and program artifacts:

* The PCI program has been laid out according to the 12 requirements.
* The customer audits make the most sense in reverse date order (so the ones that should be closing soon are at the top).
* The enterprise-wide security program initiatives are displayed in the order they appear in the budget documents.
* The internal audit items are ordered like the customer audits.

This ordering is part of the dashboard contract with the CISO and other viewers. Once established, the expectation will be that it does not change without informing involved parties.

Given that projects track completion to 100 percent, bars are good choices for the overall encoding. However, shorter does not necessarily mean “bad” in this case. You could use a variation on a bullet graph to provide more details, but that level of encoding is not necessary for this scenario. The viewers can always head to the supporting data (which includes detailed Gantt charts, project risks, and status history) for more detail. A subtle color highlight for the projects or program elements that are truly in danger of missing their dates is all that is needed to identify areas of concern, projects or elements that may need help from senior management to get back on track. Management will need to dig into the details of each wayward issue, so make sure the project and program managers have armed the CISO with all the necessary details.

[AU: Below, what’s the filename of the template so readers can find it easily? Also, I’ve added the Wiley website address there, okay? Thanks, Kevin (PjE)]

The finished product can be seen in Figure 10-17, and the Excel template can be found in ch10/docs/ch10-project-security.xlsx on the book’s website (www.wiley.com/go/datadrivensecurity).

[AU: The following seemed like a good tip to call out to readers attention, so I’ve set it off that way. Change okay? Thanks, Kevin (PJE)]

AR: fixed. Thx.

type="tip"

Excel’s built-in ability to make sparkline-like “data bars” can drastically reduce the time it takes to produce an effective dashboard component. These elements implement user-defined rules to apply color and size from cell values.

Figure 10-17: Project and program status dashboard [793725 c10f017.eps]

Summary

Designing, building, and delivering dashboards is not for the casual practitioner. It takes skill, practice, and a great deal of trial and error to create minimal, optimal encodings for critical measures and present them in a logical and visually appealing manner.

This chapter presented core dashboard concepts through both real-world scenarios and critiques/makeovers of actual dashboards found in the wild. You also learned about innovative encodings (such as bullet graphs and sparklines) along with design techniques that you can replicate in Excel and R using materials provided on the companion website.

Recommended Reading

[AU: Please include a short explanation of the recommended reading below to match the format we’ve settled upon for this section. We’ll have just the title and author here, followed by a short explanation. Then in the References appendix, you’ll include the full bibliographic info. Thanks, Kevin (PjE)]

AR: done thx.

The following are some recommended readings that can further your understanding on some of the topics we touch on in this chapter. For full information on these recommendations and for the sources we cite in the chapter, please see Appendix C.

***Information Dashboard Design: The Effective Visual Communication of Data* by Stephen Few—**If you can only acquire one other resource for designing dashboards, pick this one. It provides detail on every level of element creation with numerous examples.

***Security Metrics: Replacing Fear, Uncertainty, and Doubt* by Andrew Jaquith**— Dashboards are about displaying the most important information and driving action. Jaquith’s book is your gateway drug into finding the right **security** information to present and how best to present it.

***The Visual Display of Quantitative Information* by Edward R. Tufte, and P. R. Graves-Morris**— This book is required reading for anyone who wishes to fully understand how information should be presented. While not a “dashboards” book, it emphasizes how best to *communicate* with visualizations with numerous examples.

[AU: For the above source, I was unable to confirm the coauthor. Please confirm that. Thanks, Kevin (PjE)]

AR: looked right in my copy of the book ☺

***Design, Evaluation, and Analysis of Questionnaires for Survey Research* by Willem E. Saris and Irmtraud N. Gallhofer**— This book will help you see that designing surveys is no trivial task. Even researchers in fields that are reliant upon surveys have trouble building ones that are effective at getting to the information that they truly want captured. If you dare to delve into this area for your security program, you’ll absolutely need this book as a guide.

***Modern Analysis of Customer Surveys: with Applications Using R* by Ron Kenett and Silvia Salini—** If you’re still adamant on using surveys, you’ll need to know how to analyze them. This text will provide you with the proper statistical foundations along with a good set of reusable R code that should make you more confident in presenting your results.