Chapter 10: Designing Effective Security Dashboards

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 and complexity of designing succinct, meaningful displays of quantitative information in order to drive some type of action. This chapter will present techniques and advice that will enable you to design dashboards to help measure, monitor and mobilize every layer of security in your organization.

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 planning for 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 consumer 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 was usurped and the original hardware was hacked into something that we all recognize today as the crucial set of performance indicators available to a driver during a road trip. It was this familiarity (almost everyone knows what an automobile dashboard is) that caused the computer industry to associate the term to the summary displays in executive information systems.

The dashboard in an automobile has the various elements it does because the make sense for the context. Gauges react to the point-in-time changes we make by 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 for the 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:

Figure 10.1 Sample Splunk Dashboard [793725c10f01.jpg]

If we apply the knowledge gained from Chapter 6, we can combine a few basic plots to make what’s known as a bullet graph to replace the skeuomorphic gauges (Figure 10.2), though we 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 we are exceeding event thresholds in various areas.

Figure 10.2 Bullet Graph Makeover [793725c10f02.jpg]

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. They were 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.

Figure 10.3 Elements Of a Bullet Graph [793725c10f03.eps]

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

The sixth component—the actual value of the SIEM events per second on the right hand side in Figure 10.3—is optional, but useful if your consumers would benefit from the precision.

While our examples here 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.

The value change is also important to display, but the giant red, upward pointing arrows do not help to tell an accurate story. We can augment the bullet graph with paired sparklines—“data-intense, design-simple, word-sized graphics” (*Tufte*)—of each 24-hour measure to provide a quick picture of what happened in the various event streams.

Figure 10.4 Sparklines [793725c10f04.jpg]

Examples of how to create these enhanced dashboard elements in Excel, R and with Google Charts are provided on the book’s web site. 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.

A Dashboard Is Not A Report

IT and information security professionals tend to be very detail oriented. We are the type of people who got excited at the “show your work” directive on school assignments and love to dig into the details to show folks how we arrived at whatever conclusions we have come to. It’s absolutely necessary to have multiple levels of detail behind the dashboards we 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 consumer situational awareness for 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 car 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 text, lists and tables should not be used in a dashboard. Those elements are valid to include where precision is necessary, provided they support quick perception, comprehension and a call to action. If we wanted to communicate the SIEM events per second from Figure 10.3 with just straight text, there are multiple possibilities to choose from as shown in Figure 10.5.

Figure 10.5 Encoding Measures With Text [793725c10f05.pdf]

As we indicated in Chapter 6, it’s usually best to display a graphic versus large amounts of tabular data since numbers and text always require attention whereas shapes and colors can draw attention preattentively; just be ready to call up specific values or provide the 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="note"

When Dashboards Fail

Dashboards establish a partnership relationship between the consumers and producers. Consumers 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 be 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 take a swag at something 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 consumers always review the supporting material for every performance measure then it’s likely the they do not trust the producers enough and should trade their dashboards in for reports.

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 [793725c10f06.jpg]

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 given how many interfaces tend to align items to singular cells in a fixed grid and provide options for “on-the-fly” modification.

We can take Figure 10.6 and do a quick transformation using Microsoft Excel, starting by removing superfluous markings, borders and annotations. We’ll also take the opportunity to change the encoding of some of the measures to enhance the readability.

Figure 10.7 Dashboard Makeover [793725c10f07.jpg]

The 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 and replaced the “funnel” with a normalized, grouped bullet graph. We significantly reduced the “chart junk” and used a more subdued but deliberate color. 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 falls more into the “report” category, though it falls short of those requirements as well.

type="note"

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 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 that 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” laptop screen. There may also be times when a more vertical (portrait) layout works better with the data you need to present, so you should not box yourself into a corner by only having one layout system handy.

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

Figure 10.8 Variations On a Grid System [793725c10f08.pdf]

A Dashboard Is Not An Art Show

Given the graphical nature of a dashboard, 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, for example:

Figure 10.9 Sample Executive Dashboard From AlienVault [793725c10f09.png]

This is an example of a management-level dashboard in AlienVault’s OSSIM. It does a great job showcasing various esoteric chart types available to OSSIM users but does little to provide a quick overview of the security posture of the fictional organization it represents.

Figure 10.10 3-D Dashboard [793725c10f10.png]

The system dashboard in Figure 10.10 pushes the artistic envelope even further with considerable use of various 3D charts.

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 haiku or a Shakesperian 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 consumers to decode. Some good choices (most of which were covered in Chapter 6) are:

* Bar graphs/Bullet Graphs
* Dot plots/Scatter Plots
* Line Graphs/Sparklines
* Box Plots
* Spatial/Heat/Tree Maps

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 our book isn’t handy and you are unsure which chart to use.

Remember space constraints

You have one page/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 for the encoding if you learn your consumers prefer viewing information on their phone 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 be used to 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 on screen. Your consumers 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.

Figure 10.11 De-saturated Dashboard [793725c10f11.pdf]

Remember the lessons of Chapter 6 and also consider that your digital creations may find their way to a black and white laser printer more often than you would like to admit and fail to communicate properly. The colors in the dashboard in Figure 10.7 lose much of their meaning when they become de-saturated by a black and white printer (Figure 10.11). In our case, we knew our graphics were destined for a four-color press and also needed to setup this example. Make sure *your* creations can withstand such a transformation without completely losing their meaning.

Use fonts wisely

Stick to a single font if at all possible. Choose either serif (e.g. Palatino or Times New Roman) or sans-serif (e.g. 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 back in 1908—contained a single element: an ammeter (an instrument used to measure the electric current) that helped show the health of ignition system: one of the only components that could not be inspected visually without a specialized instrument. To know the status of gas reserves, one just checked the dipstick. To see if the car is overheating, one just looked for the signs of smoke and steam coming out of the engine compartment!

Drivers who were concerned about violating the speed limit (8mph city/20mph 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 for ornamental than operational (perhaps a sign of things to come in modern dashboards?). As we 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 consumers of the information
* The display medium
* The data available for encoding
* The expected update frequency

For example, when creating a dashboard for the CISO, it is unlikely she will want to or needs to consume/evaluate/respond to the events per second metric of the enterprise SIEM. However, this is a performance measure that the Security Operations Manager may be keenly interested in, especially if there are signs of issues with SIEM performance.

Indeed, if SIEM issues have begun to emerge, you should consider adding salient performance measures to the interactive, daily or weekly operations dashboard until the situation is verified to be resolved. Once stable, the measure can be replaced with other important items requiring evaluation and response. Thoughtful, regular updates to dashboard core content will help keep it fresh and—more importantly—reviewed and processed by your consumers**. If a dashboard developed two 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 dialog with the various consumers/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 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 (i.e. has a value) or categorical (e.g. 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, we are usually identifying a set of elements that provide useful information (e.g. which incident handlers are primary for the day), require the most attention (e.g. which PCI controls are slipping) or follow up (e.g. what are the top expedited firewall port open requests).

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

Lending A Hand To Handlers

The incident response team has asked for help creating an incident response dashboard and—among other items—would like a view of “bad port activity”. You decide, without probing any further, that “what’s going on” is the number of denied firewall transactions for a port for the month-to-date and whip up the following graphic (Figure 10.12):

Figure 10.12 Top Port Denies [793725c10f12.pdf]

While 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 and definitely lacks an answer to the “so what?” question; so 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 if you have the data to support it.

Through your investigation, you learn that the team really wants a view of top five ports with *anomalous* activity. This is quite a different measure than just a raw port count and requires answering both “what’s going on” *and* “so what?” 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 twenty-four 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 do you compare the measure against:

* The same port’s position in SANS trending port list for that time period? (i.e. same measure but from a different source)
* The same value against the same twenty-four hour period (i.e. same day of the week) at one or more points in the past?
* The same value against a different twenty-four hour period (i.e. a different day of the week)
* The same value as it relates to daily activity across the previous week or month?

If we choose to compare it against the same value for the same day the previous week (in this case, percentage change from previous week), we do get a much different view/list (Figure 10.13):

Figure 10.13 Top Anomalous Ports [793725c10f13.pdf]

Knowing there was a 2000+% 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 (e.g. examine which nodes were involved in the communication, check to see if external ISACs identified malicious on this port, etc.). While 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 work better for the team.

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?

After some research (http://www.securingthehuman.org/resources/metrics) you find there are some seemingly “easy” measures that you quickly dismiss, such as *“% completion of annual security awareness training*”. That one may be good for a compliance dashboard, but it’s not what the CISO is looking for. There are some good candidates that you 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

and choose to bring to the CISO to see which one(s) may meet her objective. After your discussion, she chooses to go the security awareness survey route. For you, this means working with the appropriate internal groups to regularly setup 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 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?

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

After significant collaboration, you decide to focus on new hires as the population and 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 and elements of the security program and there is a full multi-month training program that interleaves security awareness messages throughout this introduction period. By waiting three months after hire date, you will be able to see how much each new hire class retains and also get a feel for how tweaks to the awareness program impact new groups.

You only get one measure for the CISO dashboard, so you opt for the summary effectiveness metric recommended by SANS (the calculation is documented in their survey materials):

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. |

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

The benefit to the SANS approach is that we get standardized questions and a defined and open metric computation method. This should provide a good measure for the CISO and you can refer to the individual responses to the survey questions when asked for more details. You also opt to track 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 begins to become populated. As seen in Figure 10.14, the measure begins to trend in the wrong direction but never gets into a zone requiring immediate action, then seems to level off again. Rather than bombard the CISO with colored bands, subtle, colored level markers are used to delineate when an individual month measure moves into a different zone and provide an at-a-glance understanding of how well the awareness program is performing.

Figure 10.14 Security Awareness Risk [793725c10f14.pdf]

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 for 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 did. 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 may 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 saying 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 resolution time frame. You immediately suspect what might be 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 (e.g. “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. But, 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 problem conditions and fit the encoding in the same space without losing the 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.

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 are with the mean alone. A boxplot provides a visual representation of these values that we can augment with a line for the performance measure threshold as seen in Figure 10.15:

Figure 10.15 Boxplot Sparkline [793725c10f15.pdf]

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

Projecting “Security”

We wrapped security in quotes here and in the section title because the definition of “security” lies in the interpretation of the individual. A penetration tester may 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 very complementary as they are all parts of a whole and each activity is necessary to ensure the protection of information assets in an organization.

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 be 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 may not be sexy, but there would be little happening in “security” without this governance layer.

If you do become known as the “dashboard person” in your organization, you must face the inevitable request to build a set of measures for to track program, project and remediation status. These initiatives will have their own set of detailed measures and reports that 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 consumers wish to track. For our make-believe organization, this 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 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 and customer audits. You’ve verified the data for the performance measures are readily available/accurate and 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 and—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. Fitting into all these constraints will tie create a seamless message for the “Security Program, Project & Remediation Status” dashboard component.

After reviewing the data, you settle on four sections and draw up a rough sketch for how you want to present the information that eventually turns into the wireframe concept shown in Figure 10.16.

Figure 10.16 Dashboard Wireframe [793725c10f16.eps]

This will become a common process for your dashboard development:

* Stakeholder/consumer identifies a need
* You work to understand the need and if you have data to support the dashboard or dashboard element
* You sketch out a set of rough concepts for the dashboard, then wireframe and model the ones that seem to work best
* You choose a final model and find the most efficient process to encode the measures in support of the frequency requirements

For encoding each list of items, the order manifests pretty clearly 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 consumers. Once established, the expectation will be that it does not change without being informed.

Given that projects track completion to 100%, bars are good choices for the overall encoding, but shorter does not necessarily mean “bad” in this case. We could use a variation on a bullet graph to provide more details, but that level of encoding is not necessary at for this scenario and the consumers can always head to the supporting data (which include 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 that may need help from senior management to get back on track. They’ll 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. The finished product can be seen in Figure 10.17 and the Excel template can be found on the book’s web site. 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 use user-defined rules to apply color and size from cell values.

Figure 10.17 Project And Program Status Dashboard [793725c10f17.pdf]

In Summary

The task of 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.

Core dashboard concepts were presented through both real world scenarios and critiques/makeovers of actual dashboards found in the wild. Innovative encodings (i.e. bullet graphs, sparklines) were presented along with design techniques that can be replicated in Excel and R using materials provided on the companion web site.

Recommended Reading

Few, Stephen. *Information dashboard design*. O'Reilly, 2006.

Jaquith, Andrew. *Security metrics: replacing fear, uncertainty, and doubt*. Upper Saddle River: Addison-Wesley, 2007

Tufte, Edward R., and P. R. Graves-Morris. *The visual display of quantitative information*. Vol. 2. Cheshire, CT: Graphics press, 1983

Saris, Willem E., and Irmtraud N. Gallhofer. *Design, evaluation, and analysis of questionnaires for survey research*. Vol. 548. John Wiley & Sons, 2007

Kenett, Ron, and Silvia Salini. *Modern analysis of customer surveys: with applications using R*. Vol. 117. Wiley, 2011