Realtime publishers

Data Protection and Compliance in Complex Environments

The CSO Executive Series

Data Protection Reporting and Follow Up

sponsored by

CREDANT®
We Protect What Matters

Kevin Beaver

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Data Protection Reporting and Follow Up

Once you've found, classified, and established the necessary controls for your critical data, the next step is to ensure everything is working as it should. Can you truly evaluate the effectiveness of your controls? The answer to this questions along with how you should go about reporting and follow up are contained in this final piece.

Establishing Metrics

You cannot build your reputation as an information security leader based on what you're going to do. Instead, you have to show that your initiatives are contributing to the business *today*. Implementing a system of security metrics to measure what's actually taking place is key. But where do you start?

It's easy for people to proclaim that you need good metrics before you can be successful managing information risks, but what exactly does that mean? It goes back to the popular business phrase "What gets measured gets done." Security metrics are nothing more than standards of measurement that provide insight into how the security function is performing; for instance, consider the following:

- The number of data breaches prevented during the loss or theft of a mobile device due to well-designed endpoint security controls
- The decrease of critical and high-ranked vulnerabilities found in quarterly vulnerability assessments compared with your original baseline assessment
- The number of malware infections successfully blocked at the network perimeter, server, and desktop
- The pass rate of employee security awareness testing

Metrics that you know are easily measured will provide insight into important areas and uncover the need for additional metrics you haven't yet thought about.

Don't Feel Like You Need Metrics?

Michael Coles once said "If it ain't broke, you haven't looked hard enough." This applies nicely to security metrics. If, based on what you're measuring, everything seems to be falling into place with no gaps and no need for improvement, it may be time to tweak your metrics or reassess how you're gathering information. Quite often, information security "success" leads to contentment. I've seen many people responsible for information security believe that all they've done to a certain point is all that's needed and they do absolutely nothing else to stay ahead. You have to always be in search of ways to improve things. Establishing and refining your metrics over time is the best way to go about achieving continued success.

Next, you have to determine how your metrics relate to data—specifically, data protection and compliance; for instance, consider the following:

- Do the numbers we've gathered cover all the areas of intellectual property, customer records, and other sensitive data?
- What compliance gaps and/or security risks are not being addressed with our existing metrics?
- Once we have a handle on the most sensitive data, what level of protective measures do we want to implement for the next level of data classification?

Finally, for the sake of benchmarking and comparison, you might want to gather data from friends and colleagues who work in the security space. Doing so could help you answer the question that will undoubtedly come up: How do we compare to similar-sized businesses?

Reporting on Data Protection Metrics

Metrics will show you what you're doing well and highlight areas that need improvement. You can then use that information to demonstrate the business tie-ins of data protection and compliance. However, your metrics are only as good as the quality of your reporting.

It's All in Your Deliverables

If you fail to produce information reports with actionable items, a large part of your efforts to achieve a reasonable level of data protection and compliance will have been for nothing. Make it a priority to bring things full circle by providing real actionable items. It's the only way you'll be able to maintain support for the information security function, and it's the only way you'll be able to plug the holes you find and effect change in the areas of data protection and compliance.

You and other stakeholders will have to rely on these metrics to not only demonstrate compliance but also make higher-level business decisions such as:

- How much money/resources should be spent on security?
- Are we really reducing our exposure?
- What business systems do we need to focus our money and efforts on?
- Can we make changes in policies and processes and make effective changes?
- How will continued improvements be measured?

Too Much of a Good Thing

There's a fine line between reporting on the positive aspects of your security metrics and inundating your peers with information they don't need. One of the key aspects of getting buy-in of other stakeholders is to keep them in the loop and show how your efforts are providing value to the business. You just don't want to do it too often or use any sort of fear or pressure tactics to get your points across. Providing high-level metrics data once per quarter or every 6 months during executive leadership meetings or board retreats may be sufficient. If you find that people are interested in the data you're gathering, keep them posted by sending out periodic reports from the data protection and compliance tools you're using.

Always consider your audience before compiling your security metrics data. Odds are your technical audience will be interested in the minutiae of how their systems are working. However, your executive peers and other non-technical managers might want just the basics. If you're going to get people on your side and keep them on your side, you have to be able to speak on their level and in their terms.

Follow Up

Metrics will guide you and tell you when you need to change before you actually have to, but you cannot stop there. In the context of data protection and compliance, you have to rely on metrics to not only achieve a reasonable state of security and compliance but also maintain that state long term.

Managing Risk

Outside of the political and cultural factors of your business, you and the key stakeholders have a choice in managing information risks. You can choose to address data protection and compliance at different points in time:

- Before a data breach occurs
- In the midst of a data breach
- After a data breach has come and gone
- Never

Data protection and compliance metrics can help you determine the best preventative controls as well as help you decide when is the best time to step in and take action.

As time goes on, you might find yourself in a situation of information overload. You've built out your security metrics to a point where you're getting good information, but it could take on a life of its own and eventually become unmanageable. An effective process for preventing this situation is recertification, whereby you refine the scope of the systems you monitor and the specific data sets that fall into your oversight.

One of the most important aspects of recertification—as well as data protection and compliance in general—is to get everyone on board with your initiatives. From the data entry clerk to the CEO, if you communicate your goals and messages effectively, you can eventually build a team of people who are on your side eager to get you the data you need to succeed. Proven ways to get your message out can be incorporated into everyday business for little to no cost:

- Video sessions during new employee orientation
- Periodic formal classroom training and/or lunch-and-learns
- Ongoing display of posters around the office
- Computer screen savers and banner pages on your intranet Web site
- Trinkets that employees will use while at their desks

Most importantly, as you venture through the data management life cycle, remember what Chuck Yeager once said: "You don't concentrate on risks. You concentrate on results. No risk is too great to prevent the necessary job from getting done." It's this mindset that will help you wade through the confusion, gain the visibility and control you need, and, most importantly, ensure that your data protection and compliance initiatives work toward the greater good of the business.