EDPACS
THE STATE OF INFORMATION SECURITY LAW: A FOCUS ON THE KEY LEGAL TRENDS
Thomas J. Smedinghoff

Taylor & Francis
Taylor & Francis Group

EDPACS

The EDP Audit, Control, and Security Newsletter

ISSN: 0736-6981 (Print) 1936-1009 (Online) Journal homepage: http://www.tandfonline.com/loi/uedp20

Why Risk Assessments Fail

Barak Engel

To cite this article: Barak Engel (2017) Why Risk Assessments Fail, EDPACS, 56:4, 1-6, DOI: 10.1080/07366981.2017.1362227

To link to this article: https://doi.org/10.1080/07366981.2017.1362227

Published online: 28 Nov 2017.

EDPACS THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

2017 VOL. 56, NO. 4

WHY RISK ASSESSMENTS FAIL

BARAK ENGEL

Abstract. In this article, we will examine in a light-hearted tone the chief reason why, in many organizations, risk assessments tend to be ineffective at driving actual, meaningful change, beyond fulfilling compliance requirements. While acknowledging the importance of identifying technical and operational risk areas, we focus on the lack of an appropriate, contextual business driver oriented discussion in a typical assessment, and how critical that missing communication can be to influencing important decision makers.

We spent 3 months going through a detailed analysis of the security posture of the company, and then writing the report. Six weeks later, the risk assessment is finally ready. It's an impressive document: at 97 pages long, it provides a comprehensive review of every attack vector that could be used to compromise the company's information systems, categorizing and prioritizing the threats, and providing guidance for corrective action. Everything is summarized neatly in a table that includes a description of the risk, the priority, and the suggested remediation.

Somehow, though, while we feel good about producing such a valuable and well-considered document, it seems like nobody actually wants to read it, let alone fix anything. The internal audit people are certainly happy, but beyond another round of fixes to system vulnerabilities, all the report seems to be good for is to satisfy compliance requirements. And senior management? They congratulate us, as always, and pay lip service to how important this exercise is before moving on to business as usual. Are we missing something?

The above scenario takes place, depressingly, like clockwork in countless organizations every year. If you have ever performed a risk assessment, then it's highly probable that you have run into some variation of it. There is certainly recognition that managing risk is important for any company (or agency), and that security has a role to play. But truth be told, that recognition seems to … well, peter off … the higher one goes inside the bigger technical and audit organizations.

Taylor & Francis
Taylor & Francis Group

Try going outside of those two and, let's face it, people look at you funny.

Something is clearly missing. Why? What is it? What's going on? And more importantly, how do we transform this process into something more practical and less frustrating?

HIDDEN ASSUMPTIONS

In order to address this problem, we first have to understand its underlying causes. For that, I will turn to one of my favorite cause célèbres in the general field of information security, which is those hidden assumptions.

What do I mean by that?

Ask yourself this: what is the purpose of a risk assessment? What are we actually trying to achieve when we undertake this fairly arduous task, year in and year out?

Clearly, we want to identify risk. After all, the path we're embarking on is called "risk assessment."

Easy.

Except that now I want to ask you another question: what kind of risks are we looking for? Risks to what, exactly?

That's easy, too. Right? In fact, when I ask this question, even of people with many years of risk evaluations under their belt, I usually get a variation of the following answer:

"Technology-driven risk to sensitive data."

And to that, my friends, I say Poppycock.

With a capital P.

Let's first examine what that answer means, and more importantly, what it implies.

In the simplest of translations, it means that we are searching for attack vectors that could compromise business systems. It's right there in the entire formulation of risk assessments, and in all the education about the process.

Attack vectors representing threats.

To systems.

Except that this implies a lot of things that it might not have been intended to imply. For example, attack vectors are typically things we consider in the context of nasty people using various (and often technical) means to do something to an electronic resource of some kind to get it to behave in an unexpected way.

If you have information of interest to *EDPACS*, contact Dan Swanson (dswanson_2008@yahoo.ca). *EDPACS* (Print ISSN 0736-6981/Online ISSN 1936-1009) is published monthly by Taylor & Francis Group, LLC., 530 Walnut Street, Suite 850, Philadelphia, PA 19106. Subscription rates: US$427/£259/€343. Printed in USA. Copyright 2017. *EDPACS* is a registered trademark owned by Taylor & Francis Group, LLC. All rights reserved. No part of this newsletter may be reproduced in any form — by microfilm, xerography, or otherwise — or incorporated into any information retrieval system without the written permission of the copyright owner. Requests to publish material or to incorporate material into computerized databases or any other electronic form, or for other than individual or internal distribution, should be addressed to Editorial Services, 530 Walnut Street, Suite 850, Philadelphia, PA 19106. All rights, including translation into other languages, reserved by the publisher in the U.S., Great Britain, Mexico, and all countries participating in the International Copyright Convention and the Pan American Copyright Convention. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients may be granted by Taylor & Francis, provided that $20.00 per article photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISSN 0736-6981/06/$20.00 + $0.00. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged. Product or corporate names may be trademarks or registered trademarks, and are only used for identification and explanation, without intent to infringe. POSTMASTER: Send address change to *EDPACS*, Taylor & Francis Group, LLC., 530 Walnut Street, Suite 850, Philadelphia, PA 19106.

Another term for this, incidentally, is hacking, and while it's not explicitly stated, most people's minds turn automatically to hacking when they think of information security risk.

Why, it's easy to think about. There's a system with important stuff contained within, and if somebody were to leak that stuff out it might discomfit the business.

As my daughter would say, like duh.

Do not get me wrong, there's certainly a lot of value in this kind of conversation. But do you notice what's missing?

THE BUSINESS OF RISK

Put yourself in your chief executive's shoes. Do you think they care about all this technology stuff, beyond a general acceptance that it's a practical necessary? Of course not. It's a thing they delegate to their chief information officer (CIO). They have much better stuff to do, like care about how well the business is doing in terms of sales and market share and the stock price and the competition.

The chief financial officer (CFO)? Depending on the size of the company involved, their focus may be more broad or less so, but overall they care about things like cash flows. They rely on technology, sure, but a good CFO knows exactly what's going on when and where in terms of the things under their purview, and trust me, unless they have an unusually expansive understanding of risk, no matter how good you are at evaluating it, they will not give you access to the company's electronic banking systems to evaluate. They just will not.

They will never trust you that way.

Heck, those are typically run by the bank anyway.

What about the chief operating officer (COO)? Surely, they would care about operational metrics, and availability and reliability and all that jazz. That's directly impacted by technology, so they must care. Right?

Wrong. First of all, even if they are not the chief revenue officer in disguise (a recent but increasingly popular development of the role of COO), the operational metrics they care about tend to be business ones, and the technology ones they care about are typically only as they pertain to business performance. It is often shocking just how few systems truly qualify as mission-critical, regardless of how important their business owners may believe them to be.

So now you have the three top executives in the organization who are, for the most part and to put it mildly, politely disinterested in your risk assessment. They simply do not feel that it applies, let alone appeals, to them. The last thing any of them wants to do is waste time sitting in a room with you hearing you talk about how they need to spend more money to protect technology assets because you were so clever in finding all these ways to compromise systems.

That gorgeous 97-page report?

Oy.

UPGRADING OUR GAME

Is it any wonder that risk assessments are typically understood in technical-operational terms, and have highly limited visibility to very specific parts of the organization? In fact, in so many companies, risk assessments ultimately devolve into a sort-of hybrid penetration test/vulnerability assessment, a highly technical exercise that is utterly divorced from business reality.

That may be fun but it's not going to drive much change beyond that rather limited scope.

Assuming that we would indeed prefer that our efforts have more impact let us, then, redefine things a bit, shall we?

First, we will start by acknowledging the significant value of this common form of risk assessment. It can be a great tool in the arsenal of any security, compliance, and internal audit team, and it is also (and I find myself grumbling as I write this) indeed often a compliance milestone that must be fulfilled.

With that said, it's time to try something else as well.

Something we can add to our assessments.

We will call it a business risk evaluation.

And no, it's not just an executive summary.

What we will do here is focus on business drivers, not technology ones. You could call it "technology-driven risk to the business" instead of to sensitive data.

To start with, ignore systems. Forget them. Think of the organization and its purpose, in the context of its business cycle. Is the company in aggressive growth mode? Then a major risk to the business would be anything that could hamper that growth. For example, constraints on scalability that result from too much legacy code can be a serious problem. Note that too much legacy code is a technical security risk as well. But it may not apply as much for a consumer business that is trying to handle an economic downturn. For that company, the biggest risk might be anything that could negatively impact its brand as it attempts to distinguish itself from its competitors—say, a data leak of consumer PII (Personally Identifiable Information).

See how it all ties nicely into what we normally like to think about as a risk assessment?

But now we have made it contextual and relevant to the business cycle, as opposed to being stranded on the technology island.

Note something else as well. You can perform your regular analysis and emerge with all the attack vectors in the world, but when the time comes to present your findings, you need to consider another constituency: the business managers.

And for them, you will not need detailed graphs or lists of prioritized system vulnerabilities.

PHYSICIAN, HEAL THYSELF

In fact, as long as the risk is truly relevant to the business, then it should be extremely easy to articulate and communicate in a short narrative.

I urge you to try.

Next time you perform one, once you are done with all that exciting analysis, take one extra step.

Open a new document.

Spend a couple of paragraphs explaining what you are doing. Talk about risks to the business.

Come up with a few—and only a few!—categories of risk that you would like to discuss. Keep them both high-level and specific to your company or organization. For example, you could have a "Cloud Operations" category, which will be used to encapsulate every and all things related to, well, operating the company's cloud systems. More exciting would be a category such as, if contextually appropriate, "International Expansion Strategy," where you would probably discuss things like the impact of cyber-sovereignty laws.

Then write **one page per category**. That's it. No more than one. If you can do it in a half-page, all the better. You can divide it into multiple sections—for example, it could have an introduction containing a brief description of the risk category, a discussion of existing organizational remediative factors, and a summary of the issues involved. You may want to add a one-statement assessment of, say, brand and legal risk.

And that's it. That's all you need to do.

Can you see yourself doing that?

Because I guarantee that your chances of this sort of document being read by the folks who run the business will be significantly enhanced.

And as a result, your chances of being heard next time you see something that really, truly could jeopardize the company's survival, you may be able to have that conversation early enough to actually matter.

Considered this way, one no longer has to wonder why the results of risk assessments often end up as dusty archives, a digital version of horror genre's creepy old hospital. It's mainly because they are not written in a manner that is contextually (and, uh, volumetrically) digestible to the primary business decision makers, such as the CEO, CFO, and COO. These reports are just too cumbersome and too technical to gain any traction. Communicate appropriately at the right levels, and not only will you be more likely to gain a sympathetic ear, but by going through this exercise, you may find that you actually learn something new about the business itself.

And that sounds like a fairly worthy goal.

EXAMPLES? WE DON'T NEED NO STINKIN' EXAMPLES

If you have not seen the Bogart western that this header references, *The Treasure of the Sierra Madre*, I highly recommend you look it up. Alas, it would seem that an example may serve us well, so I would like to end with one.

This comes directly from an actual evaluation I wrote a few years back, slightly modified so as to be cleansed of identifying detail. This entry was used to **secure funding for a secure coding training program for third parties—**which, if you have ever worked in security, may strike you as downright astonishing.

But it worked. Not by itself, of course; this built on having established the right kind of relationship with the right decision makers, so that they were open to this sort of suggestion. But you can (I hope) see the power of eliminating all the jargon and just explaining things in simple terms, and sticking to business instead of technical risk.

Here we go:

As part of our response to evolving market needs, we recently implemented a third party developer program to support customers who wish to outsource the development of their sites on our platform to third parties. This program allows outside parties to work within our pre-production environment directly on behalf of customers, and specifically, to implement live sites for them (which is a function of our professional services team at present).

While these developers do not have access to platform code, they can still introduce bugs into a site since they can write code that interacts with user input (e.g., forms), and the bugs may end up allowing an attacker to compromise a site as well as the entire platform.

Unfortunately, we do not have direct control over third party developers, or insight into their coding practices, code quality, and so on.

At the present time, we have only certified one development house as a qualified third party allowed to work in our environment, and the overall risk to our ability to run our platform is still small. It will, however, increase as the number of these external development houses grow, and we will continue to evaluate and evolve the program in response to market demand.

To further reduce the risk involved in allowing external developers working within our platform, it is strongly recommended that we develop a standard approach toward certifying any third party developer that will work in our environment for basic secure coding skills.

Barak Engel *is the author of "Why CISOs Fail—the Missing Link in Security Management and How to Fix It," available from Amazon and CRC Press. He can be reached at* barak.engel@gmail.com