Join the Discussion Connect

Architecting Adequacy: When Good Enough Really Is

By Benjamin Tomhave – ISSA member, Northern Virginia (NOVA), USA Chapter

It is incumbent upon the security architect to achieve a legally defensible position that appropriately balances between "too little" and "too much" in architecting solutions that are "good enough."

Abstract

The notion that "good enough" can be adequate is much maligned, and for good reason. When implemented poorly, a "good enough" mind set can increase the liability burden for an organization. However, by the same token it is foolish to continually invest in technology improvements that have little real or measurable value. It is incumbent upon the security architect to achieve a *legally defensible* position that appropriately balances between "too little" and "too much" in architecting solutions that are "good enough."

There seems to be a common misconception in the security industry, often promulgated by vendors, that security architecture means always implementing everything possible in the endless game of staying ahead of the "bad guys." Perhaps this misconception is also driven by the prominent "breaker" contingent within the security community who are constantly finding holes in the armor through which attacks can be perpetrated. Pile on the various actors in the risk management drama and things get complicated (and ugly) right quick.

The simple fact is that security is not, nor will it ever be, a zero-sum game. There is no "war" to "win," and it is instructive to take this point to heart. It is time to quit positing security as a "challenge" or "competition" and instead start structuring it in more business-oriented terms, looking at ways to provide reasonable protection to the business while enabling it to operate more efficiently and effectively. Security architecture today is less about picking a specific tool than it is about a blended responsibility for helping manage the people, processes, and technologies that go into protecting the homelands of our respective organizations.

Survivability

I first encountered the concept of "survivability" (or "survivable network systems"[1] [2]) through reading Chris Hoff's blog[3] and hearing him speak at conferences. The idea, in a nutshell, is that we should be focusing on building resilient (or "elastic"[4]) organizations that work to achieve an optimal level of defensibility and recoverability. That is to say, rather than laboring under the false belief that you can stop everything, it is instead imperative to understand that bad things will happen. It is not a matter of if, but a matter of when. As such, building defenses that are purely geared toward stopping bad things from happening are destined for failure, and are increasingly likely to represent a stance that has a greater liability burden. Let's look at these key concepts in more detail.

Recoverability

As defensibility tends to draw most of our collective attention, let's first look at *recoverability*. The goal of recoverability is to allow the business to continue operating under degraded conditions and to resume normal business operations as quickly as is reasonable without leaving the door open to repeating the same failure(s) that resulted in the incident. In traditional language, we are essentially talking about business continuity planning and disaster-recovery plans. The objective is clear: identify what is important and then model threats against those things to build contingency plans, because, again, the assumption should always be that some-

1 R.J. Ellison, et al, "Survivable Network Systems: An Emerging Discipline," CMU/SEI (May 1999), http://www.cert.org/research/97tr013.pdf.

2 R.J. Ellison, et al, "Survivable Network System Analysis: A Case Study," Carnegie Mellon University (undated), http://www.cert.org/archive/pdf/network-analysis.pdf.

3 Rational Survivability, http://www.rationalsurvivability.com/blog.

4 Benjamin Tomhave, "Elasticity: Will your organization bend or break?," *ISSA Journal* (September 2009).

thing bad will happen some day. If it never does, fine, but the chances of that being true are slim to none (in fact, according to Symantec's 2010 "State of Enterprise Security" report, 100% of respondents had experienced "cyber losses"[5]). The key is demonstrating reasonable forethought in planning for a dark day.

Recoverability has significant ties with architecture. How compartmentalized are data and systems within your organization? Can there be more compartmentalization? Also, what other controls are in place that would hasten recovery and lessen the impact of a breach? Are there business continuity and disaster recovery policies, processes, and procedures in place? Have they been tested? Do you have the right people onboard, and are they sufficiently trained to respond while under duress in the middle of an incident? Do you have support and interest from the right stakeholders, including business leaders, HR, legal, IT, operations, development, etc.?

Consider, for example, the breach of Heartland Payment Systems and its believed attack vector being through non-PCI systems.[6] Clearly there is a case to be made here that their environment may not have been adequately compartmentalized, allowing a system in a lower security zone to become compromised and leveraged into compromising a system in a higher security zone. Their recoverability from such a string of incidents was in theory lessened in part because the compromises were able to spread between zones when they should have been limited to just one zone. One could also talk here about logging, monitoring, and detection across the entire environment, and how it played into (or did not play into) minimizing the severity of the compromise and the rapidity of recovery.

Remember, then, that it is not a question of if, but when, you will have a security incident. If you do not have regular backups in place for data important to the business, then you are setting yourself up for failure. If you do not have alternative locations and communication plans in place addressing natural disasters and epidemics, then you are setting yourself up for failure. If you do not have personnel employed or on retainer to assist with forensics and incident response, then you are setting yourself up for failure. If you do not have current network diagrams and a thorough, documented understanding of systems, applications, networks, and data flows, then you are setting yourself up for failure. Logging and monitoring are also key components of recoverability. If you lack extensive logs of what is happening with your applications and systems, then your options for recovery will be severely limited and you are setting yourself up for failure. How can you prevent the same bad thing from happening again if you don't know what happened in the first place?

5 Symantec, "State of Enterprise Security," *Symantec* (February 2010), available online at http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf.

6 Bill Brenner, "Heartland CEO on Data Breach: QSAs Let Us Down," *CSO Online* (August 2009), available at http://www.csoonline.com/article/499527/Heartland_CEO_on_Data_Breach_QSAs_Let_Us_Down.

Defensibility

Historically, when thinking about defensibility, we have usually correlated the concept with something like Defense in Depth (DiD). DiD talks about setting up layered controls within an environment so that if one control fails, then others will compensate and contain or stop the resultant incident. However, if you consider that exposing services to the outside world effectively dissolves much of DiD, then you will quickly understand that DiD is really only effective when you are not letting anything through your perimeter. In the modern era, organizations are intentionally letting the world walk through their virtual doors, oftentimes relying on antiquated approaches, weak authentication schemes, and minimal additional protection (e.g. see Gunnar Peterson's excellent article on the continued use of passwords[7]). DiD strategies need to evolve accordingly to become more agile and resilient.

The legacy flaw in logic here is thinking about defensibility in just technical terms. Defensibility is not really about the tools you use to defend yourself – or, at least, it should not be. Instead, it should be about legal protection for your organization.[8] Defensibility in the legal community is about establishing a position against which arguments (or accusations), such as negligence, liability, or criminal wrongdoing, can be countered from sound footing. That is, when your organization has a breach, it can come to the table and demonstrate that it has in fact taken reasonable measures to implement a reasonable standard of care. Taking again the case of Heartland, it appears that they falsely believed that compliance with PCI DSS was an adequately defensible position,[9] only to learn later that protecting only one part of the business does not a complete protection scheme make.

Using this perspective of legal defensibility changes the game a bit, or at least it should for the techies in the crowd. On the surface, it may seem like it is regressing to a stance of focusing on "best practices" (a.k.a. "mediocrity"[10]), which to a point would be true, but beyond that it asks the question: Did you do all that was reasonable in protecting your corporate assets? A subjective question to which would come a subjective answer, but it is an important point to carry forward.

The Heartland incident is again instructive in this perspective of legal defensibility and sufficiency. Heartland CEO Carr went so far as to say, "The audits done by our QSAs (Qualified Security Assessors) were of no value whatsoever. To the extent that they were telling us we were secure beforehand, that we were PCI compliant, was a major problem." That is, merely being compliant with PCI DSS was not, and is

7 Gunnar Peterson, "Identifying Opportunities for Improvement in Security Architecture," *1 Raindrop Blog* (February 2009), available online at http://1raindrop.typepad.com/1_raindrop/2010/02/identifying-opportunities-for-improvement-in-security-architecture.html.

8 Please note, the author is *not a lawyer*, nor does he play one on TV. He is not providing legal advice.

9 Bill Brenner, "Heartland CEO on Data Breach: QSAs Let Us Down," *CSO Online* (August 2009), available at http://www.csoonline.com/article/499527/Heartland_CEO_on_Data_Breach_QSAs_Let_Us_Down.

10 See http://www.dilbert.com/strips/comic/2008-09-03.

ISSA Discount:

Save an additional $100 off

already discounted Early Bird Rates. Enter IssA2010 in the discount code area to save **30%** on CEIC registration.

CPE Credits - 110+ Learning Sessions - EnCE® Certification Exam - Networking - Exhibit Hall

Sample Learning Topics

- Mobile Device Acquisitions
- Windows® 7 Investigations
- Forensic Tracking of USB Devices
- Anti-Forensics
- Corporate and Government Cybersecurity
- Cloud Computing

CEIC®
Computer and Enterprise Investigations Conference
2010

Show Sponsor

Guidance® SOFTWARE
The World Leader in Digital Investigations™

Platinum Sponsor

DELL

Register Now at www.ceicconference.com or 626.463.7945

not, sufficient. What did it take to then achieve a more defensible position? Carr goes on to say that they "added additional network segmentation, much more intense monitoring, and added data loss prevention technology," spending $32 million in the first half of 2009, and expecting to continue spending at a high rate.[11] The outcome – and the situation itself – almost certainly would have been different if they had started from a reasonably defensible position.

Defensibility should be one of your top goals in making arguments for implementing changes in your environment. Forget about risk for a minute as the sole focus of your program (don't forget about it permanently, because you will need a risk management program to help demonstrate defensibility) and instead consider that if you cannot make a coherent argument in front of 12 angry men[12] that your organization is doing what is necessary and reasonable to protect company assets, then you need to identify those gaps and start making real changes.

The Sufficiency of "Good Enough"

From this concept of legal defensibility comes a natural and sufficient method for achieving "good enough." It is time to engage your legal department, because this is an important point. How you approach security architecture should be directly tied, not to "best practice" or "risk management" but to what is considered a reasonable standard of care.[13]

What this means, quite simply, is that the role of the security architect now includes having to determine what is reasonably foreseeable as part of the process of architecting defenses that meet a reasonable standard of care. This reasonable standard of care will determine, beyond simply relying on prevailing practice, what is a sufficient defensive posture (read the T. J. Hooper case from 1932[14] to blow your mind on what the courts may consider to be a reasonable standard of care). Going forward, one can assume that a sufficient posture will minimally need to have strong ties to well-established holistic approaches, like ISO/IEC 27001/27002 (in fact, one could argue that comprehensive information risk management plus ISO 27001 certification of an effective ISMS plus an extensive program of audit, testing, metrics, and reporting, may quickly become the best working definition of a legally defensible position).

The point of legal defensibility, then, is this: threats, vulnerabilities, and incidents are an inevitability, so the responsibility of security architecture shifts from being about stopping bad things from happening to doing what is demonstrably adequate in the eyes of stakeholders and the courts. When an incident occurs, organizations are increasingly subject to legal and regulatory scrutiny to evaluate whether or not they did enough to protect their business and investors. The security architect is now responsible for ensuring that the people, processes, and technologies are aligned in a sufficiently defensible and recoverable manner to withstand such scrutiny.

As such, it is constructive to look at contracts, partnerships, stakeholders, and the desired survivability (and success) of the business to architect an approach and solution set that is "good enough" without exposing the enterprise to unnecessary liability. In other words, quit obsessing about information risk exposure and instead focus on optimizing the survivability of the business. In the long-term this approach will dovetail with information risk management as it matures, but until then stick to a fundamental approach that starts with "When we get compromised and sued by our stakeholders, investors, or customers, will we be able to demonstrate that we did enough to protect ourselves from unnecessary harm?" If you can answer that question confidently, with evidence and a demonstrated track record, then you should be satisfied that "good enough" really is just that; good enough.

Concluding thoughts

It is time to move aggressively away from the status quo, particularly with respect to risk and risk management, and instead force the focus of security architecture to be on doing what is adequate to protect the business from the inevitable. Instead of endlessly investing in technology, it is instead time to shift investments to non-technical efforts that optimize recoverability while emphasizing the need to architect soft solutions, such as policies and processes, alongside common-sense training and awareness initiatives.

Formal models, such as for information risk management, can be a useful tool in establishing a legally defensible position, but we need to stop deluding ourselves into thinking that they are the end-all be-all pinnacle solution. Consider, for example, the role of risk management within the ISO/IEC 27001/27002 standard. Yes, it is present, but it is not the single most important attribute. So should risk also not be the single most important component of your defensive strategy.

The goal of security is, and should always have been, how to best enable the enterprise to weather the storms that will come. Losing that focus undermines our ability to benefit the organization. Our focus should be on building survivable systems comprised of people, processes, and technology that seek to minimize legal exposure through the provision of a reasonable standard of care.

About the Author

Benjamin Tomhave, CISSP, is an independent consultant based in Fairfax, VA. He holds a MS in Information Security Management from George Washington University and is a member of committees within the American Bar Association and OWASP NoVA . He may be reached at tomhave@secureconsulting.net.

11 Bill Brenner, "Heartland CEO on Data Breach: QSAs Let Us Down," *CSO Online* (August 2009), available at http://www.csoonline.com/article/499527/Heartland_CEO_on_Data_Breach_QSAs_Let_Us_Down.

12 A reference to the U.S. legal system and pop culture. See http://en.wikipedia.org/wiki/Twelve_Angry_Men for more information.

13 See http://answers.encyclopedia.com/question/legal-definition-reasonable-care-356614.html.

14 See http://itlaw.wikia.com/wiki/T.J._Hooper for more information.