Filling the Gaps

Robert Smith

Filling the Gaps

GIAC GSNA Gold Certification

Author: Robert Smith, Roberts.Smith49@gmail.com
Advisor: Adam Kliarsky
Accepted: August 15, 2016

Abstract

There should be an emphasis on the importance of regular internal and external auditing focusing on the business mentality of "It can't happen to me" and mitigating the risk of complacency. The key areas covered will be cementing assessments and audits as a benefit versus a reactive or troublesome activity. The cost savings from regular auditing against the alternatives such as breaches and poor publicity. The world is full of technical and administrative compliance requirements, understanding where gaps are present is not something to be afraid of, but to readily embrace and act upon those deficiencies. Thinking that you are compliant and knowing you are compliant can make a large difference in business longevity and profitability.

1. Introduction

Many small businesses feel that “No one is going to bother hacking me; I’m just the little guy.” Amongst the number of cyber-attacks and breaches that occurred in 2014 involving card data theft, 90% of them impacted the small business owners (Small Businesses, 2014). In 2015 according to an article from Property Casualty 360, “62% of cyber-breach victims are small to mid-size businesses” (Harman, P. L., 2015). The last of these statistics from The Guardian indicates that “The latest Survey found that nearly three-quarters (74%) of small organizations reported a security breach in the last year” (Smith, 2016). So on average the percentage is greater than 50% or higher concerning a breach to a small business. Meaning “Yes, it can happen to you and how do you know it hasn’t already”?

The harsh truth is that small businesses are the prime targets for cyber-attack and the times of letting the fog of technology keep us from being aware are long past (Harman, 2015). Understanding your business and the systems that support it are the first steps to ensuring that you take appropriate measures to protect your business and its’ customers’ data. Feeling confident in your businesses security standing should be something that pursued with relentless vigor. Otherwise, you may become a statistic as mentioned above. However, in any circumstance, whether confident or unsure, the expertise of a third party should be sought to validate your standing.

While the word “auditor” can cause one to cringe, depending on one’s previous interactions, they should be seen as entities looking to help you find your gaps. Reviewing *A Practical Guide to IT Security*, published by the Information Commissioner's Office (ICO), the first item is assessing the threats and risks to your business (ICO, 2016). Knowing what data is valuable and what it could effect if stolen is an essential step in understanding what risks you should be looking for within your business. Working to identifying business risk is a task that most auditors should be familiar with and the first step in any business or security betterment process. Also, the process can bring to your attention items that you may have taken for granted or assumed were being done. The issue with most findings is there is not a “one size fits all” solution. Having an auditor involved can assist you in coming up with comprehensive recommendations that help you in building a roadmap to closing the gaps in your business systems.

Robert Smith, Roberts.Smith49@gmail.com

The focus should be understanding not where you failed to do something or how someone dropped the ball but more on the process that is allowing these things to happen. People, no matter how good they are, make mistakes. If a repeatable process is not in place, then the mistakes people make could potentially lead to things fall through the cracks and not getting done as expected. In addition to understanding these processes, a focus must also be dedicated to things like your compliance requirements. Currently, the top heavy hitters in the world of compliance are The Health Insurance Portability and Accountability Act (HIPAA) and The Payment Card Industry Data Security Standard (PCI DSS). If the thought of either of these two things brings on waves of panic or shortness of breath, they should. Heavy fines and legal proceedings are the tips of the issues iceberg for companies or practices that neglect these requirements. Hiding from the gaps in your compliance requirements does not lift from your business the burden of failing to meet them. Quite the contrary, it intensifies the actions taken against you and places you in a state of gross negligence. Auditors for these organizations, HHS and PCI QSAs, are more likely to work with you when you have identified shortcomings and their compensating controls rather than pleading ignorance.

Cost is a concern when thinking about involving any third party firm or contractor to conduct an audit. Even more so when that individual is reviewing things like compliance requirements. For instance Catalyze, a provider of HIPAA compliant infrastructure has a post outlining the direct cost for HIPAA Assessments. These costs can range from $15,000 to $45,000, depending on the depth (Good, 2015). That can seem like a lot, but when you figure the cost of a patent record in the United States per HIPAA Journal is averaged at $217, the cost of remediation may be cheaper (2015). So even if you are a small practice, the loss of 100 records starts at $21,700 and does not include legal fees, fines, and other costs if your clients decide to sue.

2. Understanding Where You Are

It is important to understand the current security posture. Making the assumption that you have no way to improve your security posture could be more trouble than the cost of an audit. Being vigilant and understanding the threat landscape involves constantly reassessing processes and technologies. For example, in an article by Ali Raza titled “The Top Five Cybersecurity

Robert Smith, Roberts.Smith49@gmail.com

Vulnerabilities for Businesses" shows that the following are common areas of concern, which can be used as a starting point to evaluate your current security posture:

1. Sensitive Data Exposure

Problem	Solution
- Lack of strong access control lets users access data they shouldn't	- Implement a strong IAM (Identity and access management) program that implements role-based access control - SANS Critical control #4
- Users abuse privilege to steal data or intellectual property unchecked	- Implement a privileged account monitoring solution, such as a SIEM that can monitor privileged user activity and alert on anomalous behavior. Ensure these logs/alerts are being monitored by some security operations center. - SANS Critical Control #6
- Breach of internal systems by external entities exposes sensitive data	- Verify perimeter protection such as firewalls, intrusion detection/prevention, and monitoring of activity is in place.

2. Buffer Overflow

Problem	Solution
- Vulnerabilities in software	- Implement host and network

Robert Smith, Roberts.Smith49@gmail.com

can be exploited by malicious programs to compromise internal systems and data	protection to catch threats on these vulnerabilities and prevent successful exploitation. - SANS Critical Control #4

3. Injection Vulnerabilities

Problem	Solution
- User controlled input in web forms is not validated before being passed to backend systems, resulting in database or OS compromise.	- Implement web application firewalls to identify attacks on user controlled input. - Ensure applications validate user input before sending to backend systems - Use parameterized queries

4. Broken Authentication or Session Management

Problem	Solution
- Data subject to Man-in-the-Middle Attacks - Data decryption if weak encryption utilized	- Implement web application firewalls to identify attacks on user controlled input. - Ensure applications validate user input before sending to backend systems - Use parameterized queries

5. Security Misconfiguration

Problem	Solution

- Human error in setting up a system	- Documented procedures for setting up all company systems - Regular review of system configurations - SANs Critical Control #3 - SANs Critical Control #11
- Default credential utilization	- Documented procedures for setting up network or other types of devices that utilize a set of default credentials - SANs Critical Control #3 - SANs Critical Control #11

Set up some routine 'interview' style questions with stakeholders. Identify policies and procedures in place. Some key issues might include:

- Are policies in place that have the ability to take action against employees that mishandle company data?
- Is there a system for classifying the sensitivity levels of the company's data?
- Are users' permissions restricting them to just information necessary for their daily duties?

The list, in this case, goes on but if the answer was "no" or "not sure" to any of those questions, the reality of the situation is probably setting in. This is not uncommon. Business owners just do not realize they are exposed. Executing due diligence and accepting any shortcomings is one of the first steps to being where you want to be.

3. Charting a Course

So you have decided to move forward with an audit but how do you know what to focus on in your business? The short answer is the things that are the most critical, or have the most impact to the business. Knowing that your payment processes system must be up at all times puts it in a high priority next to the administrative assistance's printer. Knowing that your reporting system, if compromised, would result in heavy losses both financially and in reputation are prime candidates for review. You as the business owner have to decide what is relevant to the business and what is replaceable or "nice to have".

To understand an audit processes at a high-level, refer to the steps in Figure 1 (Price, 2000). There are many steps in the process in which an auditor takes to define your risks and help you to understand the severity of each. In this process, they work with you to determine if your defined controls are acceptable in mitigating any risk and to what degree those risks can potentially affect your business. As a business owner, you assist the auditor by being familiar with your processes and helping them to understand what is critical to your success.

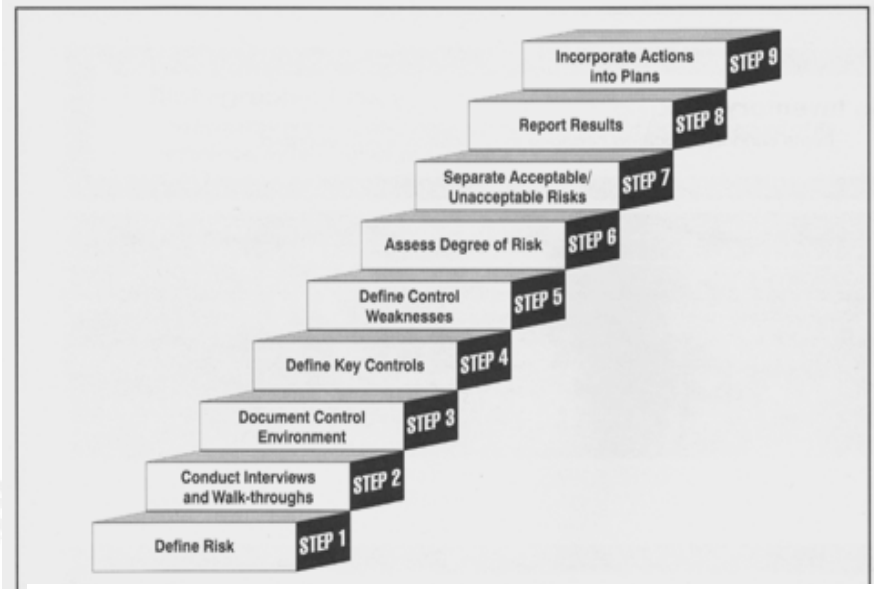

Figure 1. Example of an audit process

An important step is picking your auditor. Auditors can specialize in a wide range of services including accounting, compliance and regulatory requirements, general security reviews and more. Just as employers scrutinize employees, ensure you want to make sure you are thorough in the selection processes. A partnership between auditor and business will require solid and clear communication. The ability of an auditor to clearly articulate findings, remediation, and other issues is essential to the success of the audit and subsequent changes. While researching an auditor, check for reviews or information about their business. Has it recently been opened? Will they give you references, maybe a copy of the resume for the auditor that will be reviewing your systems? In addition to examining the credentials of the auditor and making sure they are a right fit for your company, you will also want to validate their

area(s) of expertise. If you have an auditor that has no experience in working with medical practices, and you are a medical practice, will the results be meaningful and impactful? Make sure, whatever industry you are in, that your auditor has the experience to evaluate your systems effectively. Lastly and most important, once an auditor has been selected – be transparent. These individuals work for you and it's their job to review systems, both business and technical, with an unbiased view. If you do not give them all of the information, then you run the risk of tainting the audit. By being forthcoming and working with your auditor, you set yourself up for positive change and movement towards a higher security standing.

3.1 Audit Process

As mentioned your auditor will go through several steps to complete the risk assessment. The following is provided to give insight into this process and allows for a better understand of your auditors' direction.

The first step for the auditor is to define the business risks. Within this area, the auditor is attempting to determine what is critical and what is not. As the business owner, it is pertinent to provide as much information as possible. The auditor should understand the major process points of the business so they can adequately gauge the risk against them. An example would be the payment processing system not being able to have any downtime due to high volumes of transactions. Outside of the major process the following should be provided as well:

- Data sensitivity levels
- Physical equipment locations
- Policies and procedural documentation

This information will provide the auditor with the whole picture, and better prepare them to perform the assessment.

The next step is to conduct interviews and a walkthrough. The auditor will be asking employees about their tasks and the systems they support. During this time the auditor is looking for adherence to company policy and noting any discrepancies that may arise. Employees should be allowed to answer openly and honestly as not doing so could skew the audit results and dampen the benefit to the business.

Next, they will document the controls present in your environment. The auditor is trying to determine how the systems keep your data in line with the CIA triad; Confidentiality, Integrity, and Availability. If a system is considered critical, then it must meet these three points in some fashion. If the systems are not kept in good working order then they could become unavailable, availability is lost. If a system is backed up, but the backups are corrupted at the time of recovery, then that data has poor integrity. Last in the triad, if information between systems is shared in plain text but is considered confidential, this could leave confidential information exposed. The auditor must make sure these three points are being met with every critical system.

They will then define key controls. Key controls are essentially the items or processes that prevent or detect material issues promptly. Auditors will want to measure these controls and ensure that they are functioning accordingly. In identifying these key controls, especially in an instance where compliance requirements must be met, the data/process owners can effectively manage risk to these systems and auditors can effectively measure risks to the systems.

Once the controls are identified, it is your auditor's job to find, if any, weaknesses in those controls. The instance we can use here is an application that is utilized for filling orders. For the order to be shipped certain things must happen:

- A product must be paid for by the client
- The product must be identified as in stock and found
- The product must be properly adjusted to show the new quantity in the database
- The product must be shipped to the appropriate address

If any of these things are skipped or are incorrect, the process does not complete successfully. Even, for instance, the process does complete, if any of the data is not accurate, then it's integrity has been compromised. Understanding each of the business processes and their controls allows for a better understanding of the risks within the business.

Next, they will assess the degree of risk present. In this step, your auditor is looking to assign a value to the risk, and this is typically either quantitative, monetary or other numerical value or qualitative, typically high/medium/low. For instance, if on average 1 in 100 transactions fail and you process 1000 a month this could be considered a low risk, especially if they can be reprocessed.

Robert Smith, Roberts.Smith49@gmail.com

Then they then attempt to separate the acceptable from the unacceptable risks. In this step, there is a need to define what the business can accept as a risk and what the business cannot accept. The acceptance of risk can also be dependent on the cost of remediation versus the loss caused by the risk. For example, if the business risk causes a loss of $100 in revenue per month but the remediation of that risk is $15,000 what is the ROI there? It would take 150 months or 12.5 years to recoup the cost of remediation. Is it reasonable then to expect the business to accept such a risk? However, if there is a risk that could potentially cost the business $150,000 a year if exploited and $1,200 to remediate, then the business may find that to be an unacceptable risk, then appropriate action would follow.

They will then create a report specific to your business. Once all of the controls and risks have been identified the auditor should furnish a report containing all of the findings. This report will allow the business to prioritize better and address risk based on severity. The auditor should present this report to key stakeholders and executive management when possible as these will be the individuals behind any changes. Once the report is thoroughly reviewed and key risks identified it is time to take action.

Last you will work to incorporate needed actions into a plan. Based on the audit report it is now time to identify key action items and milestones. It makes no sense to attempt to mitigate one hundred risks at a time as this can be overwhelming. The key is to make a top ten list and address these items. It will ensure that you do not become overwhelmed and that progress focuses on the areas critical to the businesses continued operations.

4. Review the Results

You selected the auditor, went through the conferences and discussed their findings. With any of these results, your auditor should be able to speak to each point and convey how they found the information and why it is relevant. If you find that your report is cumbersome or overly populated with technical jargon, you may want to probe deeper into your auditor's methods. Not saying that some technical information is a red flag, but if that information is not meaningful it should not be in the report; once you have reviewed all of the information it is time to make your list for remediation.

Robert Smith, Roberts.Smith49@gmail.com

During this process you should make sure that you understand why the findings are relevant and what risk they pose to your business. Based on these risks you should prioritize the areas that you will focus on first. It does not make sense to worry about the time not being synced on your machines first when you have no formal way to collect logs. In addition to systems for log collection, do you even have a procedure in place for reviewing these logs? Some things are dependent on other systems or policies being in place and must be addressed first. By correctly laying out your plan you can address the items accordingly and more efficiently. Also, you can identify the risks that may be acceptable and remove them from the list.

In this situation, it is easy to turn a molehill into a mountain and get overly stressed about your results. The biggest thing to remember is now you know and nothing within this report, flagged as a risk, was any less of a risk before. These results allow you to make decisions on mitigating these risks through a few avenues. You can choose to avoid the risk by removing the object from the environment entirely. An example of this would be a software version that has a known vulnerability. Update the software to a version that does not have the vulnerability and you have removed the risk, although you may potentially introduce a new one in the process. You can choose to mitigate the risk by implementing controls that lessen the likely hood of the risk realized. You can transfer the risk by moving the activity to a third party. Instead of hosting something like your email internally you can use a cloud solution instead. Hosting will not remove risk entirely, but it puts some of the risks on the Software as a Service (SaaS) provider. Last, you can accept the risk and monitor it. Acceptance is not always the best avenue, seeing as most risks have some form of mitigation or compensating control that could reduce their likelihood of becoming a problem.

In all of this make sure that your list is manageable first and foremost. If you have one hundred risks, break it down into your top ten or twenty list. If you allow your staff to determine what they will work off that list, then they will be drawn to the easy fixes. If you give them a set list, then you remove the opportunity to implement the quick or easy fixes. Once the list is handed off, you can schedule milestones for the tasks and officially start to remediate your findings.

Robert Smith, Roberts.Smith49@gmail.com

4.1 Are You Where You Want to Be?

Now that you have worked through your milestones and scratched some items off of the list are you where you want to be? Nothing about becoming compliant or secure is fast, and the processes can seem cumbersome at times. In the end, the key goal is ensuring that your data and the data of your clients is secure. Once you have identified all significant risks and come to a conclusion that you are now secure, it is always beneficial to have your systems re-assessed to ensure no changes have left any gaps. Regular assessments help to keep your network from lapsing back into a state of disarray and ensures that meeting any compliance or security requirements is an easier endeavor.

The future of your review process should be something that is planned and consistent. In looking at the Model for Improvement, based on the PDSA Cycle, you can understand one method for continuous improvement (Moen, R., & Norman, C., 2009). Essentially you will have a continuous cycle, where you ask the first three questions in the list.

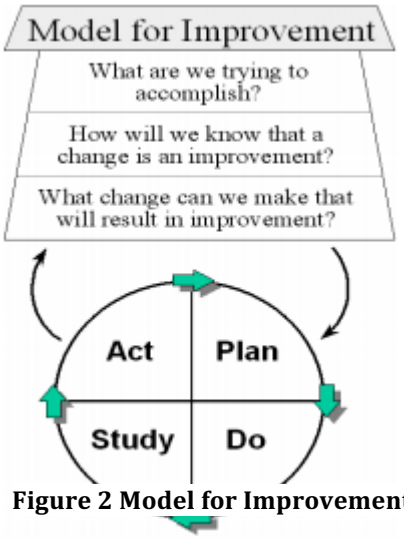

Figure 2 Model for Improvement

1. What are we trying to accomplish?
2. How will we know that change is an improvement?
3. What change can we make that will result in improvement?

From this point, you plan to make the change determining the who, what, where, and when. Then you Do the action by carrying out the plan and start the analysis of what the change has done. You then Study these changes to determine if the findings reflect what you expected and then Act on those findings to move closer to a resolution of the goal you set. This simple method will help you to further your security standing and ensure that you make no changes without thoroughly thinking them through and stay involved every step of the way.

5. Conclusion

Looking back at where you were, you may have thought that being a small business put you in a category that was not for the attention of cyber criminals

but quickly it became apparent that no such safety exists for small businesses. In reality, small businesses are the key targets for cyber criminals. In knowing this, we moved through helping you to ask the right questions and come to terms with where you are in regards to your security standing. We then moved through knowing your priorities and based on those findings picking an auditor that would be beneficial to your business. Once the auditor was selected and the review completed, we discussed some key points to look for in the results and how to turn those items into remediation milestones and effectively use a process like Model for Improvement to assist. While it may seem simple at a glance, these are some key measures to ensuring you fill your gaps and maximize your businesses security standing.

Robert Smith, Roberts.Smith49@gmail.com

References

2015 Cost of Data Breach Study: Global Analysis." May 2015. Web. 28 May 2016.

ICO*. "A Practical Guide to IT Security."* 6 Jan. 2016. Web. 28 May 2016.

Donlon, Rosalie. *"Small, Mid-sized Businesses Hit by 62% of All Cyber Attacks."* 27 May 2015. Web. 28 May 2016.

Good, Travis. *"What Is the Cost of a HIPAA Audit?"* 19 Mar. 2015. Web. 28 May 2016.

Harman, P. L. (2015, October 7). 50% of small businesses have been the target of a cyber attack. Retrieved June 03, 2016, from http://www.propertycasualty360.com/2015/10/07/50-of-small-businesses-have-been-the-target-of-a-c

Moen, R., & Norman, C. (2009). Evolution of the PDCA Cycle. Retrieved June 6, 2016, from http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf

"Ponemon: Data Breach Cost Increases to $154 per Record - HIPAA Journal." 27 May 2015. Web. 28 May 2016.

Price, L. (2000, March). Risk-Assessment Process. Retrieved June 06, 2016, from http://www.clir.org/pubs/reports/pub90/risk.html

Raza, A. (2015, August 29). *The Top Five Cybersecurity Vulnerabilities for Businesses* | Hacked. Retrieved May 28, 2016, from https://hacked.com/top-five-cybersecurity-vulnerabilities-businesses/

"Small Businesses: The Cost of a Data Breach Is Higher Than You Think." 2014. Web. 28 May 2016.

Smith, Mark. *"Huge Rise in Hack Attacks as Cyber-criminals Target Small Businesses."* 08 Feb. 2016. Web. 28 May 2016.

Robert Smith, Roberts.Smith49@gmail.com

Last Updated: October 23rd, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**