Interested in learning more about security?

SANS Institute InfoSec Reading Room

Show Me the Money! From Finding to Fixed to Funded

Corporations both large and small, whether public or private, can always benefit from an information security audit to improve their security posture. This security audit will highlight vulnerabilities and provide prescriptive guidance on how to fix them within a formal report. The ability to motivate organizational teams to complete the necessary work has historically been a challenge. While tracking of these findings using a workflow management tool has its value, most organizations stop at simply tracking the defici...

Show Me the Money! From Finding to Fixed to Funded

GIAC (GSNA) Gold Certification

Author: Robert Mavretich, bmav@rocketmail.com
Advisor: Stephen Northcutt
Accepted: April 18, 2017

Abstract

Corporations both large and small, whether public or private, can always benefit from an information security audit to improve their security posture. This security audit will highlight vulnerabilities and provide prescriptive guidance on how to fix them within a formal report. The ability to motivate organizational teams to complete the necessary work has historically been a challenge. While tracking of these findings using a workflow management tool has its value, most organizations stop at simply tracking the deficiencies, rather than take the necessary steps to remediate them in a timely manner. Thus, vulnerabilities from a decade ago are still causing disruption in our present day hyper-connected world. By applying an economic incentive system to the resolution of those findings, much like a sales division incentive program, a company can create a remediation bounty program. This will assist in motivating non-managerial staff to conceive of innovative ways to apply necessary fixes quickly, and to manage systems that are less susceptible to nefarious actors and their less than honorable intentions.

1. Introduction

While the benefits of audits cannot be overstated, especially in a world as connected as ours, some may have difficulty accepting the results as beneficial. Audit findings as a general category may be viewed as a formal accusation upon those being audited; a critique of the ability to do assigned jobs properly and effectively. Despite that potential viewpoint, any organization can benefit from an information security audit to ensure the implementation of best practices and guidance to effectively fix the highlighted vulnerabilities.

The farther one rises in the ranks of responsibility within an organization, the easier it may become to accept these audit findings as data points that simply represent ways to improve a company product or process. A concise way to manage the process of applying necessary patches or hardening standards and publishing the related metrics, represents a way to give high level executive's visibility to the problems that the organization faces. The data are also useful in advocating for a bonus program for the IT practitioners charged with driving the audit items to closure.

Senior executives are responsible for driving the vision and execution of company goals. As such, these leaders also have access to a powerful financial reward system in the form of at-risk compensation. In years where the execution of a strategy meets or exceeds expectations, the at-risk portion of overall compensation can exceed base compensation, also known as a salary. In years where the corporate strategy does not closely match or exceed the corporate financial forecast, high-level executives' base compensation may still be significant enough to provide for their desired standard of living. Without the benefit of financial at- risk compensation to provide an increase to base salary, individual contributors may not earn enough to provide for their desired standard of living as well as save for their future. If audits can potentially be used to provide a conduit to additional compensation, attitudes towards audits and acceptance levels may improve as a result.

As most corporate pensions or defined benefit programs are sun-setting and being replaced with defined contribution plans, creating an environment where individual contributors can have a positive impact on a portion of their overall compensation can help offset this financial security paradigm shift. For the American worker, "living paycheck-to-paycheck isn't only a lower-income dynamic. It's actually reflected across income levels nationwide" (Saving, spending, and living paycheck-to-paycheck in America, 2015). This struggle (independent of income level) is why compensation programs that reward innovation should be considered. Objectivity is crucial when rewarding employees through an incentive program regardless of company rank. Keeping this is mind will help drive the type(s) of audit(s) used to unlock value through developing incentive programs.

A penetration test is a great example of an objective type of audit. With this type of audit, there is a high degree of objectivity of the findings. The final report of a professionally executed penetration test will include a short description of the vulnerability, a summary or rationale as to why this finding is an issue, the business impact, risk, likelihood of exploit, effort to fix, and the suggested remediation steps to take. By using this information objectivity combined with a metrics program, such as defined in the National Institute of Standards and Technology (NIST) standard 800 – 55, individual contributors can help guide unique metrics that represent a direct connection to a performance-based bonus.

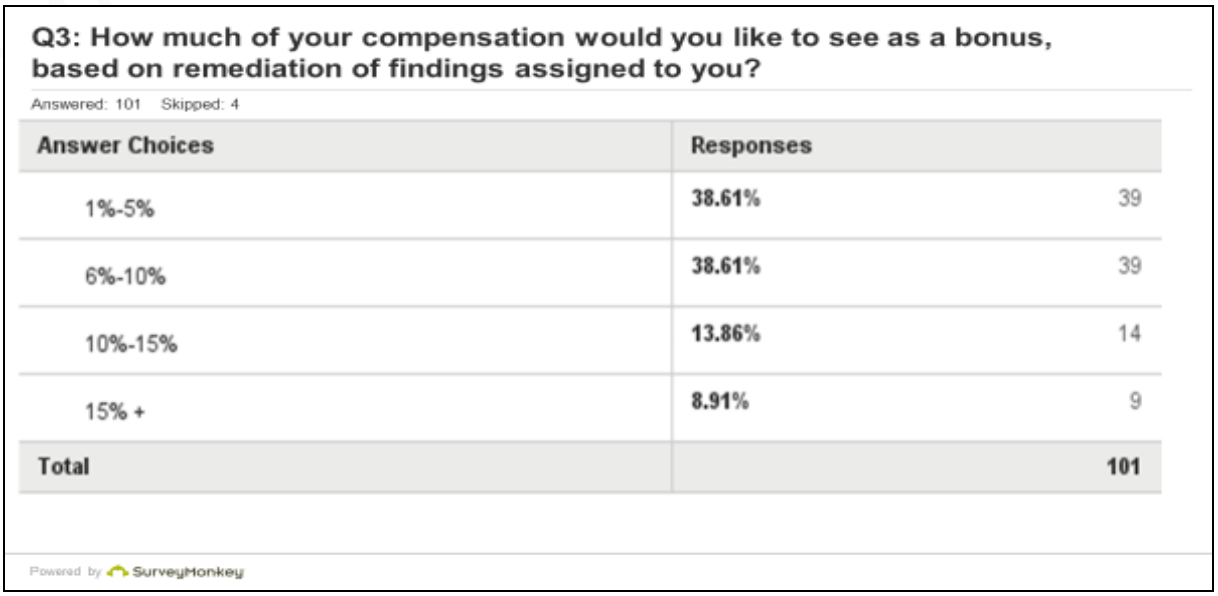
Providing financial incentives to the individual practitioners responsible for the maintenance of critical systems can allow for a positive effect by reducing the overall security risks to the organization. "Distributed Analysis and Work" (Erlin, 2015) is a method of remediation which can create an effective and friendly competition that reduces overall risk, allowing individuals and mid-level leadership to systematically publish overall metrics with the assistance of a Governance, Risk, and Compliance workflow tool (eGRC).

A personal interview with Steve Levinson, Vice President of Risk, Security, and Privacy at Online Business Systems (www.OBSglobal.com), indicates that pay for performance related to remediation of audit findings may be met with resistance - for legitimate business reasons. He explains, "From my experience in performing hundreds

of audits/engagements, loud protests from the application owners/business such as "don't break my application" (qualitative) and timing issues such as holiday freezes and required change control reviews/windows (quantitative) may often occur. These factors can potentially conspire to eliminate an incentive-based program from even being considered" (S. Levinson, personal communication, May 2, 2017).

This interview also revealed that, according to Steve's knowledge, no company has implemented this type of incentive program yet because of at least one of the limiting factors he listed. A follow up conversation indicated his enthusiastic desire to hear about a company implementing a program such as this, so the idea does show potential. Based on the SurveyMonkey responses from the parties owning remediation responsibility (Figure 1), over 70% voted in favor of a modest bonus (up to 10%) based on completed remediation tasks. There was an even split between the respondents for a bonus of 1%-6% and a bonus of 6%-10%, with the remaining 25% indicating a desire for an even larger escalator bonus based on the results assigned to them. One possible way to answer the desire collected from this survey question is to provide a program to tie remediation results to compensation.

Figure 1: Desired Bonus Amount Based on Remediation Tasks



Q3: How much of your compensation would you like to see as a bonus, based on remediation of findings assigned to you?

Answered: 101 Skipped: 4

Answer Choices	Responses	
1%-5%	38.61%	39
6%-10%	38.61%	39
10%-15%	13.86%	14
15% +	8.91%	9
Total		101

Powered by SurveyMonkey

Photo Credit: https://www.surveymonkey.com/r/ZNY37T7

The research indicates that the potential pitfalls for this type of program are clearly not insurmountable from the perspective of those who would be subject to the risk and rewards of the program. Leadership should take this predominant attitude expressed within the survey into account when they are facing audits, and recognize that their most valuable "assets" in the audit process can be the IT practitioners.

The ability to publish historical results from every audit, year after year will help to create a compelling long term dashboard view that senior management can use to track the success of the program. Similarly, participants can use the same dashboard and data points to advocate (with clear metrics) for their bonus over a base salary. Developing a program to reconcile these two diverse opinions and move an organization's security posture forward would create a win-win-win scenario - for the employees, the management, and the entire company.

2. Audit Finding Tracking

Audit findings may come from many different places within organizations such as the internal corporate audit division, an independent third-party security audit assessment, or simple observations by either information security staff or general end user population. Regardless of the size of the organization, these findings may proliferate quickly. Semi-formal tracking of these organizational findings may occur in a simple spreadsheet application at first.

Within a simple spreadsheet, pivot tables can be used to develop graphs that show the status and progress of the remediation of the audit findings. "Among other functions, a pivot table can automatically sort, count, total or give the average of the data stored in one table or spreadsheet, displaying the results in a second table showing the summarized data" (n.d. Pivot table). For Excel wizards, this can be an easy and repeatable way to manage findings and present high-level dashboard graphics to senior leadership in a concise fashion. This would be considered an early step in the overall program development process when companies may not yet see value until an initial baseline of metrics are gathered and presented.

Many large organizations can engage with a holistic Information Technology Service Management (ITSM) tool vendor such as HP or ServiceNow who provide a platform for incident management, change management, and service requests. Even if an organization is not large enough to benefit from a major toolset, there are practical and open-source resources that will allow a determined small or medium-sized organization and committed staff the opportunity to mirror a formal ITSM. A few examples of these open-source resources are Combodo ITOP (http://www.combodo.com/) or the offering from provider CITSMART (http://sourceforge.net/projects/citsmart/).

Erik Blum provides guidance on the adoption of such products: "Before you make a decision which solution to choose, you have to consider that open source projects also get discontinued. Even though source is available for anyone to see, the question is if anyone is ready to pick on a project and continue with development" (Blum, 2015). While the message is certainly one of "buyer beware," an organization can help mitigate this risk by adding value to the open source product in use to ensure continuity or at least define a practical usage lifecycle. This can be accomplished through financial support to the open source program foundation (if one exists) or contribution of code updates.

For the purposes of providing evidence that an audit finding was remediated, leveraging a tracking tool within the ITSM provides the opportunity to produce objective evidence for the closure of the finding. Auditors can then tie back the work that the staff has performed through a formal process with multiple layers of approval and multiple layers of acceptance of the change. Whether using a formal or semi-formal tracking methodology based on the size of the organization, the ability to track changes is a key item, especially if it will tie real "completion compensation" dollars to the remediation of those findings.

Another important part of the process is to be able to tie back the completion of the work and the desired result – no additional vulnerabilities identified of the same should be found going forward. This should not imply, but directly mandate, that if a vulnerability for a Windows Exchange 2013 server exists, and is found on **one** host, that **all** Windows Exchange 2013 hosts be reviewed for possible remediation activity for the identified vulnerability. This ensures that the organization is taking a security- centric-

risk- based approach towards increasing their security posture, rather than attempting to satisfy and auditor with promises yet not taking substantial action to fix.

With the ability of hackers to pivot from one asset to another to gain and maintain their unauthorized access, they only need to find the specific subset of Windows Exchange 2013 servers that did not receive the patch to wreak havoc on a network, its employees, and valuable customers. Remediation on one single asset to show progress to an auditor is not progress, and may give a false sense of security and inaccurately frame risk to those relying on the integrity of the reporting.

2.1 Metrics Development

To be able to represent the overall security posture of an organization, it is necessary to track unique metrics that can assist the organization in prioritizing the available security budget to address the issues highlighted within the audit. If the company is a large web-based, e-retailer company such as Amazon, the risk posture and desired metrics might heavily trend towards mitigation of web vulnerabilities, rather than a laser focus on physical security audit findings (although the physical ones should not be dismissed). If the company is a freight forwarder, the opposite may be true – that spotlight may focus brighter upon the physical security metrics rather than web vulnerabilities.

If companies are to reward information security practitioners based on the run rate of their successes, then those companies must have an effective way to objectively "score" the vulnerabilities that they are tasked with remediation of through these audit findings.

> "The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores." (https://nvd.nist.gov/cvss.cfm)

For the development of a program designed to track these identified vulnerabilities to remediation and tie it to individual practitioners, an organization should start with base

metrics. Base metrics do not materially change. Temporal and environmental factors can change materially over time, and even over a short enough period that they may interfere with an attempt to gain stable metrics.

The audit findings (vulnerabilities) are loaded into the metrics tracking program platform with as much detail as possible. Details include: the date found, the CVSS severity level, guidance on remediation steps and/or references to vendor support sites. The enterprise-defined patching schedule should also be included; the team responsible for the remediation will be given an acceptable timeframe to fix the issue (security focus) and stay within the parameters of their own information security standards (compliance focus). This allows for a successful path of remediation. The Figure 3 graphic described by NIST outlines what is needed to accurately define (Measurement ID): a goal and how to get there (Goal, Measure, Measure Type), who is responsible for the finding (Responsible Parties), and acceptable evidence and collection guideposts (Implementation Evidence, Frequency).

Figure 3: NIST Metrics Example

Field	Data
Measure ID	PenTest_Wireless_1 – WPA in use
Goal	To remediate the finding that pertains to the use of WPA in the environment
Measure	Number of WPA enabled devices in the environment
Measure Type	Numerical
Formula	NA
Target to Reduce	This number should be a high number with practical expectation levels set
Implementation Evidence	Request For Change (RFC) will be provided to prove the number of hosts that have been successfully migrated off of WPA
Frequency	Collection Frequency: Weekly Report Reporting Frequency: Monthly
Responsible Parties	CERT, System Owner/Subject Matter Expert, Chief Information Security Officer
Data Source	Penetration Testing - Q1 20xx

(n.d.) Using the NIST Model Framework to Measure Metrics

3. Compensation Models

One way to reward IT practitioners is to place higher value on the remediation of the higher-rated vulnerabilities. When an organization completes a penetration test and has ten (10) Critical, five (5) High, and ten (10) Low vulnerabilities, it would appear to be easy to see which vulnerabilities will receive the most attention. Should those Critical findings be related to web application vulnerabilities that have been seen in the wild for some time (such as SQL Injection), correcting that vulnerability/finding may carry a higher "bounty" if it is done so in a timely manner (this can be defined differently by internal versus external auditors). While it does not minimize the importance of addressing other findings, the objective score provided by the Common Vulnerability Scoring System can represent a fair and objective reference model upon which to base monetary compensation.

Considering the management of only one set of findings, the compensation would be easily translatable. If the report has identified ten (10) Critical findings, and patching activities resulted in seven (7) vulnerabilities fixed, it equals a 70% success rate (7 ÷ 10 = .70) of adequately eliminating the Critical subset of overall findings. Assuming a $50,000 salary with $5000 "at-risk" additional compensation (10% of salary in this example), the formula below is a guide on compensation. This transparency and simplicity may facilitate acceptance by the very practitioners who will be engaged in this compensation model.

In this scenario, the payout would equal a $3500 bonus ($5000 x .70 = $3500). It is important to note this is above the base salary of $50,000, and acts as a bonus - for a total compensation of $53,500 for the fiscal year. This is represented as a fixed bounty, for a subset of findings that the organization deems to be worthy of a bonus. Organizational considerations such as administrative controls may lessen the perceived risk of the identified vulnerabilities; therefore, the desire to include a subset of Low findings as part of a bonus program may not be possible.

Alternatively, an organization may decide to define the compensation rewards by using the percentage of all remediation activity. This has the benefit of showing a wide range of addressed vulnerabilities no matter the Common Vulnerability Scoring System

score. While this may not address the most critical findings first, it does show progress in the remediation of overall findings, which may result in an increase in overall security posture. A top-down methodology (Critical first) for remediating findings may seem the most logical; however, a bottom up (Low first) may be the most practical in certain organizations.

Within these select organizations, where buy-in from multiple support groups (web, middleware, micro server, workstation) may be difficult or impossible to gain, there may be relatively little friction in getting the Lows and Mediums corrected. The Low and Medium findings may be issues that can be corrected by a single administrator within a single environment – with no other organizational input necessary other than a simple Request for Change (RFC). This has the ancillary benefit of ensuring that today's Medium risk vulnerabilities do not become tomorrow's High or Critical risk vulnerabilities. Seeking the "low-hanging fruit" is not just for attackers.

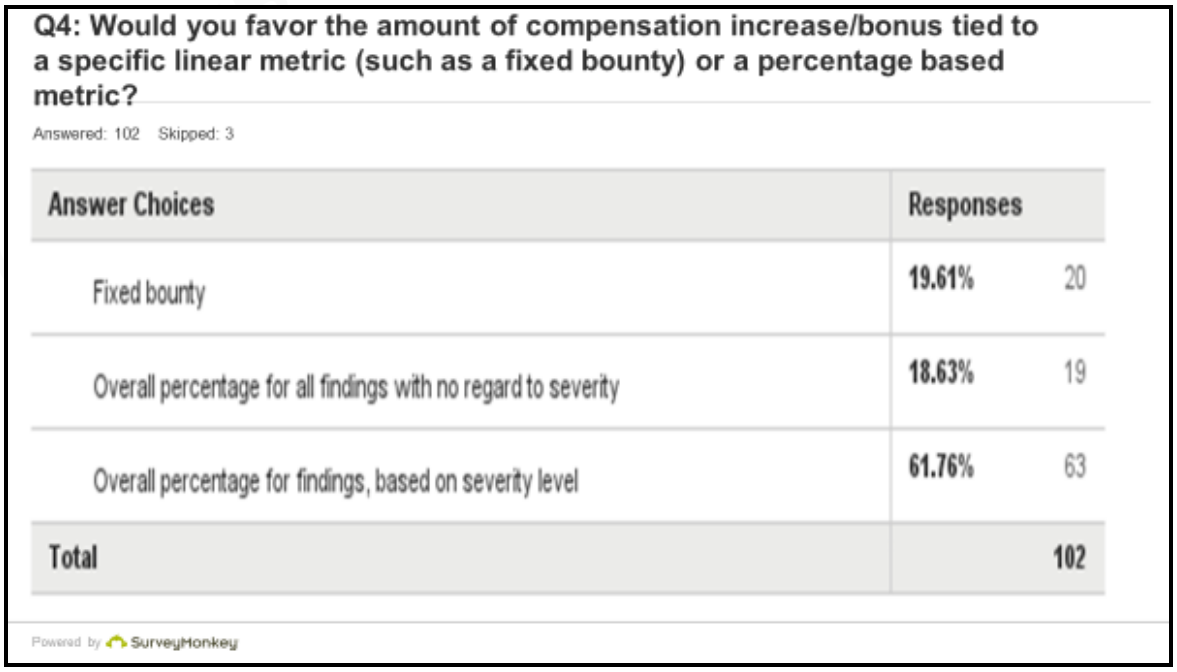
Remediation in a Low to High/Critical fashion may also present an opportunity to mitigate some of the potential future High and/or Critical vulnerabilities if they are on the same platform. For example, eliminating the use of a persistent cookie that is truly not needed will reduce the likelihood that an attacker will have that cookie available to reuse it as a stepping stone for a web application attack. Attackers are frequently finding new ways to combine low risk items together to create a previously undefined, higher aggregated risk exploit. By eliminating as many lower risk findings as possible, evolving higher risk threats can be reduced.

Using a simple fixed compensation table and applying the same completed percentage to the "at-risk" portion of compensation produces the bonus, and shows progress towards total reduction/mitigation of the audit report threats. With a total number of pen test audit findings of 25, remediation of 10 overall (with no regard to severity) would equal a 40% remediation rate (25 ÷ 10 = .40) of all findings. The compensation pool of $5000 is awarded at the 40% success rate of addressing the vulnerabilities ($5000 x .40 = $2000). This is slightly more progressive than awarding a fixed bonus based on a subset of findings, because it accounts for all findings across all risk categories. This helps address the concerns that new exploits are conceived daily, from what may have once been considered a Low or Medium risk finding.

A final method to consider would be tracking the findings with an appropriate severity weight assigned to each one of them. “Weighted average is an average in which each quantity to be averaged is assigned a weight. These weightings determine the relative importance of each quantity on the average.” (n.d., Investopedia). This is where the CVSS score is used as the “weight” as the Critical findings will be weighted higher than the Low findings. The fact that the CVSS is a widely-accepted barometer of the severity of all published vulnerabilities should result in fewer arguments against this as a measurement-weighting metric.

Referencing the multi-part independent SurveyMonkey results, this final method of an overall percentage based on severity level was preferred by greater than half of the surveyed population as seen in Figure 4.

Figure 4: Linear or Weighted Compensation Metrics



Q4: Would you favor the amount of compensation increase/bonus tied to a specific linear metric (such as a fixed bounty) or a percentage based metric?

Answered: 102 Skipped: 3

Answer Choices	Responses	
Fixed bounty	19.61%	20
Overall percentage for all findings with no regard to severity	18.63%	19
Overall percentage for findings, based on severity level	61.76%	63
Total		102

Powered by SurveyMonkey

Photo Credit: https://www.surveymonkey.com/r/ZNY37T7

The best way to operationalize this effort would be to take audit findings and correlate them into repeatable metrics for payouts - a formula to share with the employee and use as a reference. Start with a baseline of all the findings with their CVSS weights in

a fashion referenced by Figure 5 as an example. This helps to guide the employee as to the severity of the issues found in the test, and highlights the "highest value" remediation to pursue.

Figure 5: CVSS Ratings

Cumulative Findings	Finding Type Identifier	CVSS Rating
1	PenTest_External_Network_1	8
2	PenTest_External_Network_2	8
3	PenTest_External_Network_3	8
4	PenTest_Internal_Network_1	4
5	PenTest_Internal_Network_2	4
6	PenTest_Internal_Network_3	4
7	PenTest_Internal_Network_4	3
8	PenTest_Application_1	3
9	PenTest_Application_2	3
10	PenTest_Wireless_1	3

After pulling all the findings from the audit report, adding a CVSS weight to the finding will help in determining not only what the highest value is, but it will also tie a higher payout to the remediation of the findings considered most critical. A SQL Injection vulnerability would correlate to a higher risk and payout than perhaps a lengthy persistence of a session cookie that is in place for legitimate business reasons. This is not to suggest that the cookie cannot be dangerous, but there is a clear threat with SQL Injection that needs to be addressed more expeditiously than the cookie setting.

Once the full list passes through the ITSM tracking tool currently in use, the findings should be condensed into a smaller table for tracking and weighting. Rather than replace the CVSS scores with High, Medium, and Low, it might be valuable to keep the numbers present as a numerical representation aligned with the quantitative nature of the payout formula. If necessary, the widely accepted and industry-popular heat map severity colors of Red (Critical/High), Yellow (Medium) and Green (Low/Informational) can be leveraged as well, shown below in Figure 6.

Figure 6: Total Open Weighted Score

No. of Findings Open	CVSS Rate	Total Weight Rate	
3	8	24	Critical/High
3	4	12	Medium
4	1	4	Low
10		**40**	**Total Open Weight Score**

As the findings are closed, the numbers can adjust for a quarterly or yearly historical reference. The research that is performed to prove a false positive finding can also produce valuable insight for the overall project and subsequent tracking of vulnerabilities going forward. Similarly, the evidence provided to prove the finding addressed/closed should be both a Request for Change (RFC) or service ticket, and should support screen shots proving that the practitioner properly addresses the problem that they need to solve. These detail items should be tracked within the ITSM tool as well, using specific and consistent key words that directly relate to the audit finding. By maintaining this vigilance in process, common items are indexed and found quickly when performing searches within the tool in the future.

Occasionally, even Subject Matter Experts (SME) may not have exposure to the specific situation at hand due to custom development or coding, and may need to research the steps to complete the configuration properly. This necessary research process is of value because it enhances the learning process by forcing the practitioner to exceed their comfort zone. Even the most accomplished practitioners cannot possibly know everything; this is especially true in the current "zero-day" vulnerability environmental state in which the Information Technology industry operates.

This opportunity for training (with the audits as the evidence for the need) should begin an iterative process of addressing and forecasting training needs for all team members. Either the data within the toolset can be referenced for specific training needs (many web application findings may indicate a need for targeted training for developers), or the number and variety of the findings may indicate a larger audience with differing training topic needs. Care should be taken to ensure that some practitioners do not attempt to "game" the system by allowing findings to "age" until their vulnerability scores increase (and potentially increases the bonus weight). Even if the practitioner

needs training to fix what is broken, findings should be updated on a regular cadence to ensure they are acknowledged and being addressed appropriately.

For Critical findings, the practitioner should be expected to update the finding within the eGRC tool frequently to provide updates to management as its impact will likely be felt outside of Information Technology. For findings that are less severe, a longer period may pass between updates but not extend past one month. It is important to show progress as well as show reasons for lack of progress. Vendor assistance (or vendor "training") may be an acceptable reason for lack of progress.

The chart in Figure 7 represents the graph from the end of an agreed upon period, such as year-end: 30 (Total Closed Weighted Score) ÷ 40 (Total Open Weighted Score) = .75 (Weighted Score), or 75% of vulnerabilities remediated.

Figure 7: Total Closed Weighted Score

No. of Findings Closed	CVSS Rate	Total Weight Rate	
2	8	16	High
3	4	12	Medium
2	1	2	Low
		30	**Total Closed Weight Score**

On an at-risk compensation base of $5000, the employee would be eligible for a $3750 increase in pay for that year, as shown by Figure 8.

Figure 8: Total Compensation Awarded – Weighted Score

Total Open Weight Score	Total Closed Weight Score	Overall Completion Weighted Score
40	30	0.75
Total Compensation Pool	**Total % Remediated**	**Total Compensation Awarded**
$5,000.00	0.75	$3,750.00

At year-end, the remaining findings would continue to exist the following year within the tracking tool. The assumption is that through further audits, the finding(s) would occur again if not currently fixed. In addition, they would not count twice or add to the new overall count on the subsequent year's score. This is especially fair if the reason vulnerabilities persisted were due to funding challenges and or vendor hardware/software limitations rather than the individual efforts of the technologist tasked with solving the identified issues.

Regarding findings that technically have no remediation as the vendor no longer supports the product, a judgement call by management of the additional mitigation steps suggested by the practitioner (and subsequently agreed upon and implemented by the system owner) should be manually reviewed with management. This accounts for the fact that there may not be a solution that would render the vulnerability unexploitable (such as a vendor software patch), but does make it extremely difficult to initiate an attack on the currently unsupported platform.

Examples of substantial mitigation tactics may include the following:

Identity and Access Management Mitigation

1. Remove unused accounts
2. Require complex initial passwords and expire after initial logins
3. Set password parameters for end users, expire passwords every 90 days
4. Do not allow sharing of passwords – use an enterprise password vaulting product if many employees must have elevated access to an application

Application Mitigation

1. Ensure all available application patches are applied from the vendor
2. Ensure that this application is continually pen tested for new vulnerabilities that may be/are exploitable

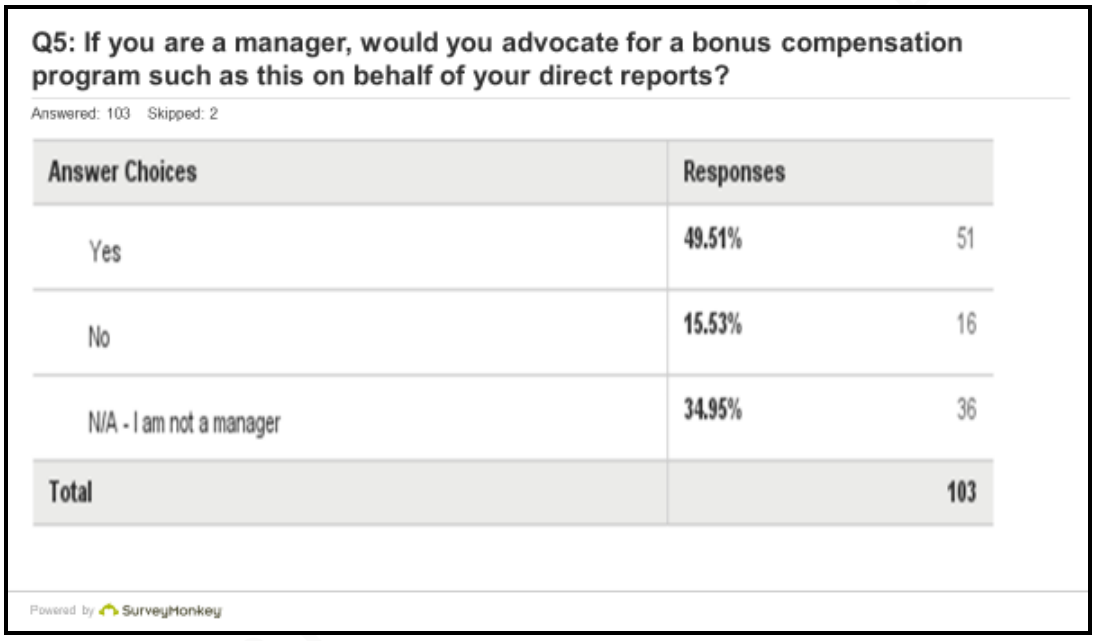
Infrastructure Mitigation Tactics

1. Move application to a secure network segment (important if it is carrying sensitive and/or regulated data) requiring additional authentication/verification
2. Move application behind a Web Application Firewall, with updated rulesets from a vendor that is currently supporting and defending against all known and released vulnerabilities.

By cataloging this type of substantial work within an ITSM workflow management tool, the practitioner can make the case that they have gone beyond a response of "it can't be fixed" and have mitigated the vulnerable application/device to the fullest extent possible. If system owners took the consultative guidance and applied it, then this should signal to management that this was a substantial “win” for the application owner(s) and therefore the practitioner who suggested it. This is exactly the type of action that should be rewarded. Actions such as those listed above clearly demonstrate exceeding expectations despite limitations, to provide a comprehensive mitigation response to the finding in question.

There was a high positive response from the management respondents within the SurveyMonkey conducted towards rewarding these types of effort with bonus compensation for a job well done. When accounting for the non-managerial representatives, and reducing the sample population accordingly, this results in a positive response of over 75% of survey participants, as seen in Figure 9.

Figure 9: Managerial Advocacy for Bonus Compensation



Q5: If you are a manager, would you advocate for a bonus compensation program such as this on behalf of your direct reports?

Answered: 103 Skipped: 2

Answer Choices	Responses	
Yes	49.51%	51
No	15.53%	16
N/A - I am not a manager	34.95%	36
Total		103

Powered by SurveyMonkey

Photo Credit: https://www.surveymonkey.com/r/ZNY37T7

4. Conclusion

Countless companies have been front page news at one time in the various news media outlets suffering negative press because of what may be considered trivial attacks. These attacks may have been less devastating or never succeeded at all if the right defenses existed, or if existing defenses were appropriately hardened. While updating and/or patching software and hardware may be considered part of any Information Technology professional's "business as usual" duties it has unfortunately not been the case.

As malicious actors continue to grow in population and their attacks, methods, and the number of available platforms proliferate, it is time to forge a new path forward to ensure audit finding vulnerabilities are remediated/mitigated quickly and potentially in innovative ways. This requires a strong partnership between the company and its IT staff.

As efforts to stem the tide of these malicious and persistent attackers are undertaken, appealing rewards for a potentially wide range of information technologists can be a difficult proposition. In a capitalist society, additional compensation is likely the most democratic option for an organization. Alignment in this way may result in an increase of managerial support to harden and defend infrastructure and applications, lead to higher public confidence (as the company does not end up in the news for a breach), and enhance cyber security awareness on a regular basis.

An innovative program that challenges a company's IT practitioners to rise to the challenge of staying ahead of nefarious hackers and benefitting from a correlated bonus follows this method defined by the research:

1. Present the concept of the program to applicable employees,
2. Create a baseline of metrics using a recent or upcoming security audit,
3. Based on research performed weight the metrics based on severity,
4. Use a common scale such as the CVSS score and tie the compensation formula to those ratings (a higher severity remediation gets a higher bounty paid),
5. Track the remediation of these weighted metrics on an appropriate schedule for visibility and progress indicators for management and employees to see,
6. Reward employees and socialize their success within the organization

References

Blum, E. (2015, February 1). 6 Best Service Desk Open Source solutions - ITSMDaily.com. Retrieved from http://www.itsmdaily.com/best-service-desk-open-source-solutions/

Citefast*, Citefast automatically formats citations: APA 6th edition, MLA 7th ed. and Chicago 16th ed*. (n.d.). Retrieved July 29, 2014, from http://www.citefast.com/

Crowe, C. (Director). (1996). *Jerry Maguire* [Motion picture]. USA: TriStar Pictures.

Erlin, T. (2015, January 6). Six strategies for reducing vulnerability risk. Retrieved from https://www.tripwire.com/state-of-security/vulnerability-management/six-strategies-for-reducing-vulnerability-risk/

Kendrick, T. (2012). *Results without authority: Controlling a project when the team doesn't report to you, second edition*. New York, NY: American Management Association

Levinson, S. (2017, March 2) Personal interview

Mavretich, R. J. (2017, March 10). *From Finding to Fixed to Funded Survey*. Retrieved from https://www.surveymonkey.com/r/ZNY37T7

n.d. NIST 800-55 Measure 19, Page 72

n.d. CVSS Reference = https://nvd.nist.gov/cvss.cfm

Strunk, W., & White, E. B. (1999). *The elements of style*. Boston: Allyn and Bacon.

Saving, spending and living paycheck-to-paycheck in america. (2015, July 28). Retrieved from http://www.nielsen.com/us/en/insights/news/2015/saving-spending-and-living-paycheck-to-paycheck-in-america.html

Pivot table. (n.d.). In *Wikipedia, the free encyclopedia*. Retrieved April 26, 2016, from https://en.wikipedia.org/wiki/Pivot_table

Last Updated: May 24th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced