

## Confirmation Bias

*Why Your Security Metrics Suck!*

**R**isk Management is essential to a proper security program yet many organizations struggle with implementing risk management. Savid advises companies around the world and are frequently asked what risks really matter. Should we be worried about a zero-day attack? What about all these mobile devices? Many CISOs get caught up in the risk management process and when push comes to shove they end up making a decision based on their gut instinct using the data to rationalize their decision.

This phenomenon actually has a psychological name – Confirmation Bias. Confirmation Bias is the tendency for people to favor information that confirms their preconceptions. Confirmation Bias is the reason why managers and executives will spend 30% of their budget on a project that no one else seems to think is important but gets pushed through anyway.

At Savid, we have been researching confirmation bias for over two years now and have identified a few key areas that most CISOs can tweak to reduce the chance of making gut decisions that more often than not don't succeed. Let's discuss the biggest one: Bad Metrics.



Most security organizations manage risk using metrics that don't matter. The percentage of machines with high risk vulnerabilities, patch latency, or anti-virus metrics are important, don't get us wrong, but they don't help the CSO make decisions because most metrics simply provide data. Properly built metrics will provide the data in addition to answering a question. Let's use an example to explain.

If we have 122 machines with more than 5 high risk vulnerabilities per machine what does that mean to the organization? The answer: who knows? There are many other questions that must be answered first before we can use this data to make a decision, such as were the 122 machines the entire environment or

*Continued on page 2*

## What you can learn from Asset Allocation

**W**e have all seen the graphs, three pies: one marked aggressive, conservative, and moderate. Usually associated with 401K or IRA accounts, these graphs show an allocation of various assets in order to meet a specific return level given a certain amount of acceptable risk. You pick one and the company handles the reallocation and dirty work of making sure you never have more risk than you want.

Is your risk management program structured the same way? It should be.

Most risk management programs involve committee meetings, an excel file with many risks identified by a high, medium, or low, and the committee arguing over which one should be addressed. Besides the confirmation bias problems we discuss in our other article, most risk management programs don't have goals. Think about those 401K accounts, you pick the conservative model because the goal you want is a return of 4% with very low risk. If you had a higher risk tolerance you could have selected the aggressive model which gives an 8% return with a much higher risk.

Your risk management program should be structured in a similar way. All of the risks in that excel file are there to help the organization understand their current risk exposure and how it compares to the risk tolerance for the organization. If there is a gap between the current risk exposure and the risk tolerance of the organization, that is an opportunity to introduce additional risk for additional gain. The problem is most organizations haven't defined their risk tolerance and have defined metrics to determine if they are above or below that risk tolerance.

How do you implement this approach to risk management? It's actually rather simple. Instead of looking at metrics and the individual risks to make decisions, take a step back. First, categorize the metrics into projects they apply to;

*continued on page 2*

### Inside this Issue

**Confirmation Bias** ————— 1  
*Why Your Security Metrics Suck*

**What you can learn from Asset Allocation** ————— 1

**The 2011 Holiday Tech Gift Guide** ————— 3

**Monthly Special** ————— 2

**The CEO Corner** ————— 2  
*Michael Davis shares his thoughts*

**Events** ————— 3

## Confirmation Bias – Why Your Security Metrics Suck

continued from page 1

was I only able to scan 122 out of 3,244? Are the 5 high risk vulnerabilities all unique (meaning I have 610 separate risks) or are they the same problem appearing 122 times? While these questions are important, the ultimate question that is usually never answered is this: Is having 122 machines with more than 5 high risk vulnerabilities above my organization's tolerance for risk?

And that is where confirmation bias jumps in. CISOs, executives, and decision makers might look at the data and start running around concerned that the 122 machines are a massive threat to the organization and we must fix the problem immediately or they might ignore it, and it all depends on the risk tolerance and the risk aversion of the person responsible for making decisions.

So how do you address bad metrics? First, never use a metric that does not have the following properly defined: Name, Category, How to Measure, Purpose/Decision to be made from the metric, baselines, Target Audience, and Reporting Frequency/Period. If you went through all the data your team collects today how many metrics would you keep if you actually assigned a Decision/Purpose to each one? Our research shows that you will end up with less than 15 but will keep some others around when deep diving is needed.

Each metric must have a baseline defined and not just a single baseline but areas. For example, if we take our example above, we should have a defined baseline for the minimum number of machines that must be scanned, the threshold for when this metric indicates an acceptable amount of risk (Green) such as less than 1 high risk per machine, when it is a moderate risk (Yellow) of more than 2 but less than 5 per machine, and an immediate risk when greater than 5 (Red).

While this example isn't a perfect example that you can use in your environment today, it should illustrate the picture we want you to see – Metrics thresholds are not metrics, they are measurements and you cannot manage risk without decisions being linked to each metric.

Once you implement and define metrics appropriately, the chance of Confirmation Bias causing a problem is greatly reduced because the decision parameters are already laid out and decided within the metric itself - the CISO won't have to make a gut decision on whether to address the problem or not, the organization has defined when the problem will be addressed based on the status of the metric.



## What you can learn from Asset Allocation

continued from page 1

if you can map these projects to business goals, even better. Next, for each project, have the owner of the project create a success state and failure state for the project. For example, if our critical apps are available for 98% or more of the time, the project is a success. Lastly, have them review their metrics, and answer a simple question: On a scale of 1 to 5, where 1 is unlikely and 5 is very likely, what is the likelihood the project will meet the success state?

Using qualitative, instead of quantitative, metrics on the likelihood of success is similar to what a mutual fund manager does. If the conservative portfolio you selected has stock, it becomes much riskier and the likelihood of meeting the 4% return has gone down, they will adjust the portfolio to meet the goal.

Risk management isn't about eliminating risk, it is about managing risk to an acceptable level so that the business can innovate and grow. Our guess is, if you start adjusting your audit items based on the likelihood of meeting project outcomes instead of just their risk level you will have more items addressed, less meetings talking about why things need to be done, and will be able to start identifying opportunities where you can take additional risk because the organization is managing their current risk appropriately.

## CEO Corner



The business wants to ride a bike and doesn't know how. The security group has the option to try and prevent them from riding the bike and make them stick with the tricycle, or it can provide some ground rules, a helmet and knee pads, in the form of simple controls, and tell the business they can ride where they like knowing that if the business falls off the bike the chance of them getting hurt is much less.

Whether intentional or not, too many security teams end up preventing the business from doing new projects because they introduce security issues or the business goes around security to get things done. Don't!

Implement effective risk management and let them ride the bike!

## Executive Report

### Beyond Confirmation Bias: Five Ways to Get Rational About Risk



Get your free report today at:  
<http://mcaf.ee/jf9xg>

# The 2011 Holiday Tech Gift Guide!

*Well who better to ask about tech gifts or gadgets than the tech guys themselves? Here at Savid we are always interested in finding the coolest and latest tech gadgets out there. So to help you out this holiday season we have put together our 2011 Holiday Tech Gift Guide to help you with your shopping. Get ready, this will be a quick shopping trip and you will never have to leave your comfy office chair! Our engineers have these items on their shopping list this year and we are sure they will make someone happy on yours.*

The new **Kindle Fire** at a great price for just \$199! There's much to do, view movies, TV shows, magazines, songs, and books. Thousands of apps right at your fingertips view it all on this full color 7" inch screen multi-touch display. Its ultra fast and you even get free cloud storage for your Amazon content, what a great buy. It's sure to be on someone Holiday list.

**Trent IMP500 iFuel Spare Battery Charger** This little gadget is a must have, tired of your battery always losing charge? Well this device can give you the added life your gadget needs, 38hrs of movie time on your iPhone or iPod Touch. It also works on Motorola Droid, HTC Android EVO phones, Kindle DX, Blackberry, and Samsung Galaxy. Not to mention Sony PSP, Amazon Kindle, Nintendo DS lite, DSi and Gameboy with optional adapters. Great price, around \$40

**The Kinect** Do you want to get someone active this holiday season, well then the Kinect is the right gift for giving. This brings gaming to a new level; no controllers needed it works by your body movement and the sound of your voice. It's fun for the whole family and online for \$159.

**Sony Internet TV Blu-ray Disc Player** This device allows you to play Blu-ray, DVD's and CDs. You can also connect to the internet and download Android apps as the device has built in Wi-Fi. The player comes with a remote that has a full QWERTY keyboard. Priced online for \$200.

**Boxee TV** This device finds your favorite TV show and movies and puts them on your TV. But Boxee also allows you to use Apps, and get Social all while setting on your sofa watching TV. There are two ways to get a Boxee buy one or make one. You can purchase a Boxee from the store or make one with their free software using your laptop. Now they even have Boxee for iPad. Boxee device is pricing around \$180.

**Altec Lansing M812 Octiv Air Wireless Speaker System with iPod docking station.** This would make a great gift for any music lover. Simply place your iPod in the docking station and kick back and listen as the system delivers 80 watts of powerful high-fidelity sound and better yet, its clutter free, portable, easy to use, and even comes with a remote. It's priced around \$180 online.

**KeyFolio™ Pro Universal BT Keyboard Case for 10" Tablets** This keyboard was designed for 10" Android based tablets. The keyboard and viewing angles were designed to be ergonomic. The tablet fits securely in the elastic bands and the corners secure your tablet in place. This gift is great for those who prefer to type on an actual keyboard verse touch screen. You can pick the KeyFolio™ up for around \$90.



## Monthly Events

### Dec. 7th at 12:30pm, Zurich Webcast

Michael Davis will be presenting his topic on Intellectual Property Theft on this webcast, don't miss out! Email to follow with further details. Also LIKE us on Facebook for more information on this event and others.

### Complimentary Executive Briefing, by Appointment

Michael Davis will discuss his Security outlook for 2012. In this briefing he will discuss what changes to expect and how organizations approach security strategically, and what information executives need and want to know. This unique briefing can be scheduled for a webinar or in person meeting. For further questions please contact us at 877-307-0444 or info@savidtech.com

### On-Demand Webinar: Top 10 Risk Assessment Best Practices

48% of organizations fail to link risk to budget. Let us show you how to do it right! Learn the newest trends in risk management that must be in your risk assessment process. BONUS: How to properly prioritize remediation. HINT: It isn't always by risk! Watch this anytime at the comfort of your own desk by using this link: <http://mcaf.ee/6ysa9>

### On-Demand Webinar: Top 10 Mobile Application Security Risks

This on-demand webinar teaches you how to strategically approach mobile security, so you can stay one step ahead of attackers. To watch, simply use this link: <http://mcaf.ee/w6opx>

### Holiday Like Us Campaign, The Season For Giving



<http://mcaf.ee/aw86s>



<http://mcaf.ee/wcp5m>

This is our 2nd Annual Holiday Like Us Campaign. The details are simple, for every new Like on Facebook and Follower on Twitter we will GIVE \$1 to the Boy's and Girls Club & you will RECEIVE exclusive content, informational videos, and insight on events and promotions. On December 18th we will announce on Twitter and Facebook one lucky follower that will receive a \$50 Best Buy gift card just in time for the holiday's! For further questions please contact us at 877-307-0444 or info@savidtech.com





savidtechnologies

18470 Thompson Ct. Ste. 2B  
Tinley Park, IL 60477

Comprehensive Knowledge. Delivered.

## Take a Break!

© Original Artist  
Reproduction rights obtainable from  
www.CartoonStock.com



"I think we need to take another look at your risk-management strategy."

### Joke of the Month

"MEETINGS, A practical alternative to work. "

Got a funny joke? Send it to us at [info@savidtech.com](mailto:info@savidtech.com) and we may include it in an upcoming issue.

### Follow Us On

Get exclusive content, informational videos, and details on our upcoming events .



<http://www.facebook.com/savidtech>



<http://twitter.com/savidtech>



<http://www.savidtech.com/blog>

### Monthly Trivia

Be the first to email us the correct answer and win a \$20 Starbucks Gift Card!

Using the numbers and letter as cues, figure out what these sentences refer to.

206 B. in the H.B.  
64 S. on a C.  
50 S. on the U.S.F.  
24 T.Z. on the E.  
24 L. in the G.A.  
435 C. in the H. of R.

Email your answer to: [info@savidtech.com](mailto:info@savidtech.com) and look for the winner listed in next months newsletter  
Congratulations to our last trivia winner.

## Implement Security as a Service

Gain insight on melding process, security and tools.



Get your FREE copy today!  
<http://mcaf.ee/m16eq>