2011 S3 Results

Justin Somaini

www.somaini.net

Table of Contents

Introduction

As a practitioner I spend a great deal of my time focusing on my environment to ensure that we are working closely with the business to mitigate risk. In the process of doing that, I strive to grow my team and individual capabilities. Part of that is building relationships and reading industry materials. Those industry materials, in part, are surveys that we attempt to glean information on how others are handing the same problems we are and/or see the trends we need to be prepared for. Unfortunately, the majority of surveys focus on areas that aren't necessarily beneficial and only focus on the ***threat and not the solutions***.

It is my attempt to create a survey by practitioners for practitioners. As a result, the survey focuses on five key areas (Information Security Function, Governance and Risk Management, Culture and Communication, Metrics and KPI's and Threats and Risks). It should be obvious, but it is not my goal to just "present the data". Instead, I chose to present the data and give my interpretation of it. I feel it's one of the benefits of being in an industry for so long as I can interpret these data points and colorize them with my experience. Agree or disagree with my reading of the results it's the conversation that is most important to me. Feel free to reach out to me directly or post on my blog your thoughts.

Above all else, I'd like to thank each and every one of you who've participated in this survey. It was a much bigger success than I ever anticipated. When I sent out the survey it was truly a one hour response to an ongoing frustration. The participation, questions, suggestions and considerations form everyone around the globe has been fantastic. It's the participation of everyone of the submitters that has made this what it is. I can't wait to do the next one.

Executive Summary

Being the first S3 report it's important to note that there are significant lessons learned as to what to do in the next survey as well as the results themselves. The overall intent of the survey was well served with the responses that were received. In total, over 55% of respondents were CISO level individuals giving a strong view into how security is implemented across our industry. The results showed a strong support of our function in some ways but limiting in others. The limits could very well be our lack of focus in bringing them to see our point of view and communicating appropriately. In addition, the structure of security is maturing but still needs work. The overall concept of "risk" has been slowly getting better; yet, we lack the adoption and maturity of existing models to bring it to fruition. With the threats increasing over the past 6 years it's our maturity within our respective organizations that is needed to ensure we are protected. To mature our functions we need to pause, learn from others, develop a strategy and plan then implement.

Lessons Learned

- Writing this report takes longer than I thought
- Outreach
    - Need to do a better outreach of responders internationally.
    - Send reminder emails to my network to complete survey
- Streamline questions to ensure ease of answering
- Limit questions to 25 or less.
- Drive better structure of the question to be more specific in areas and remove ambiguity
- Include questions and comments from this survey into the next

Key Observations

- Over 82% feel that Culture Change is the most important factor in implementing security
- Over **67% feel their company does not have a culture of security**, even though over 69% have a strategy to change company culture and behavior.
- 86% feel they do not have enough funds or people to accomplish their function
- 67% feel they need skills development of people in their team to get the job done
- Over 1/3 do not have a formal report on risk (security) to their executive team
- Over 53% have not had a conversation with their executives on the appropriate level of security to implement
- Support and knowledge decrease as you go down the organizational hierarchy. However, it's those lower levels that get the least communication and interactions with by security.
    - **62%** do not perform regular town halls
    - 56% do not perform annual employee surveys
    - 55% do not perform monthly companywide communications on security
- **No one** communicates metrics to all employees
- 55% have metrics but those metrics don't explain why things are occurring
- Over 1/3 feel that state sponsored espionage is not an issue compared to other threats.
- **48**% of responders see malware as "significant" threat to their business
- When incidents have occurred, over 60% feel their CEO, CEO's directs and/or board is supportive of Information Security

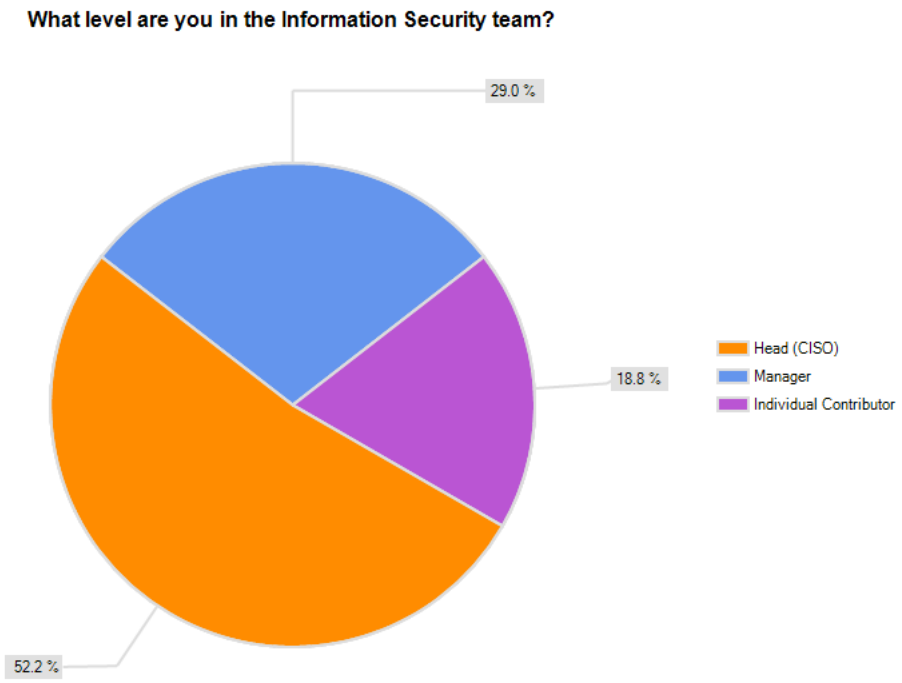
Recommendations

- **Information Security Function**
    - Take time and document up a formal Vision, Mission Statement, Strategy and Roadmap
    - Ensure the roadmap goes out to 2 years.

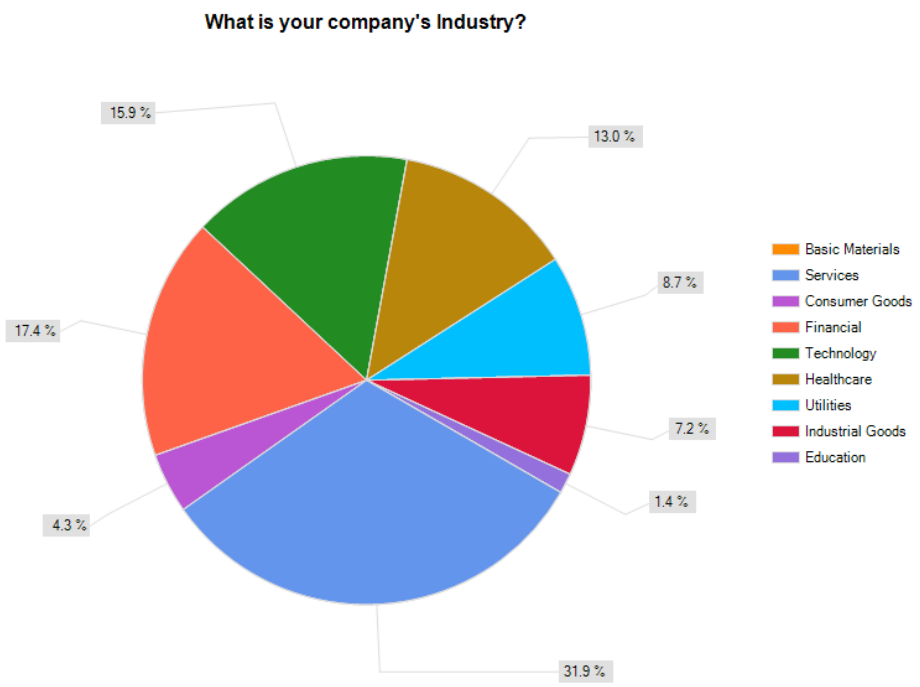
    - Develop a two year internal training program, with HR, to ensure the right skills are being developed internally
- **Governance and Risk Management**
    - Drive a governance model to the BU leaders on a monthly basis to ensure their support and their driving of key initiatives in their organization
    - Drive a quarterly or annual enterprise risk report to the CEO and their directs to ensure their awareness and support.
    - Investigate a threats based model that feeds into a controls framework vs. starting from a controls framework to ensure holistic and complete coverage.
    - Initiate an open conversation with BU leaders, CEO and their directs over what is the appropriate level of security that is needed. Ensure this includes understanding on revenue, brand and operational impact.
    - Take time and investigate existing models of risk such as FAIR, DREAD, ALE, OCTAVE, etc.
- **Culture and Communication**
    - Drive an overall communication plan for all employees that ensures their understanding on the metrics and controls initiatives
    - Implement a telemetry mechanism to understand where your enablers and detractors are in the company. This can be done via an annual survey with appropriate geographical and organizational breakdowns.
    - Drive a communication and education plan to the detractors to both educate them as well as drive their awareness to where it needs to be. As a result, their support should follow.
    - Implement an annual town hall program to facilitate a companywide involvement and understanding on security issues and initiatives.
- **Metrics and KPI's**
    - Start the metrics discussion with your team over the top 5 questions that need to be answered. Use those questions to detail the metrics that are needed to answer them.
    - Consider the questions in relation to how the business operates not how the tools provide data.
    - Ensure the metrics answer "why" not just "what".
- **Threats and Risks**
    - Drive a threat taxonomy discussion with your team over what are the threats that you have data on and what the plan is. This should include incident data as well as tool telemetry.
    - Focus on realized threats that drive an actual loss of revenue, company operational capability or intellectual property. Consider reporting impact in those three categories for business context.

Security and Company Information

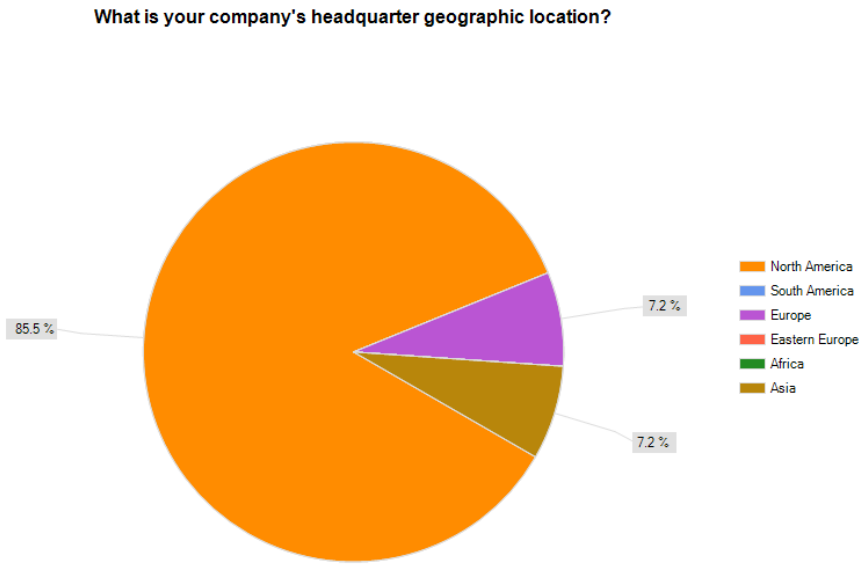
Overall, the response was great considering how it was distributed and notified. The response included a significant majority of CISO's participated out of the overall population. Over half of the responses came from heads of security or CISO's. The results need to be put in context of this fact as the CISO has an overall view of the enterprise security. This is great from a capability of understanding and relaying the risk of the enterprise. However, I find that individuals within the organization have a better understanding and impression on the actual attacks that occur.



A weakness in the industry question was identified midstream where higher education and technology was no appropriately broken out and resulted in slight skewing of the responses. However, the response is pretty clear overall. It does underscore the overall point that a better outreach needs to occur to specific industries. In addition we have over 31% from "Services" and it's that term in which should be better broken out to give a granularity to the responders. Where, holistically, industry should not matter in how security is implemented it will have a significant impact on the culture and hurdles the security organization has in front of it. Those hurdles will change the methodology or implementation of security.

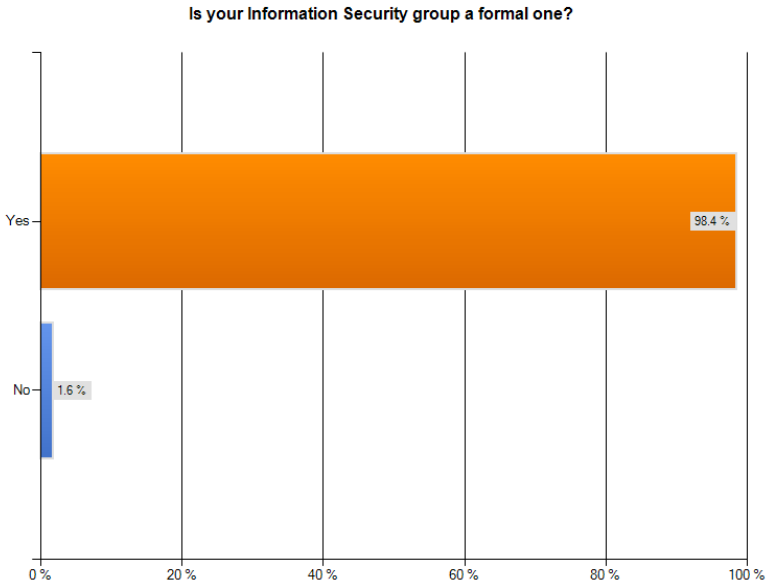


Simply put, it's the cultural differences in how Information Security is seen across the globe that drives a need to include international corporations. The dramatic increase in technology, and resulting security needs, in those countries will drive a maturity curve in the results in the future.

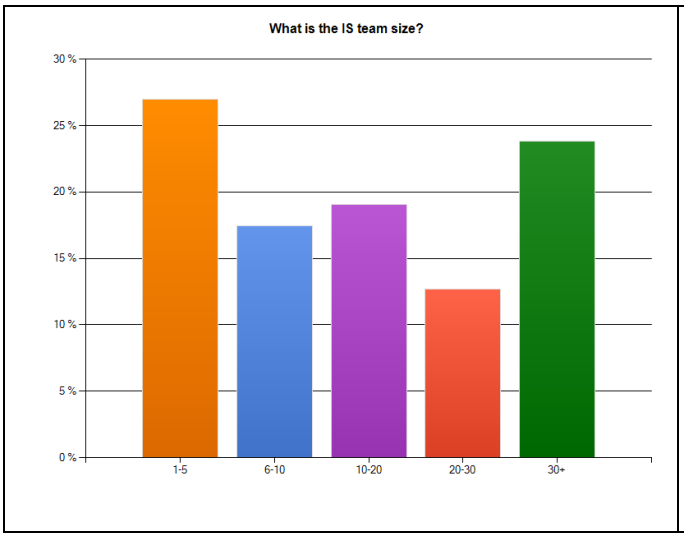


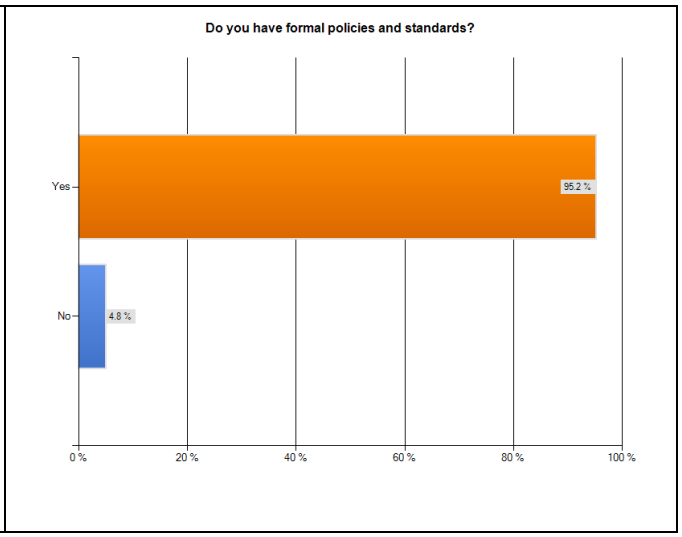
Information Security Function

There are core understandings that we should have across the type of Information Security functions and what they have. Due to the list of respondents we expected to have a formal security group and its subcomponents, however, the details are quite interesting.

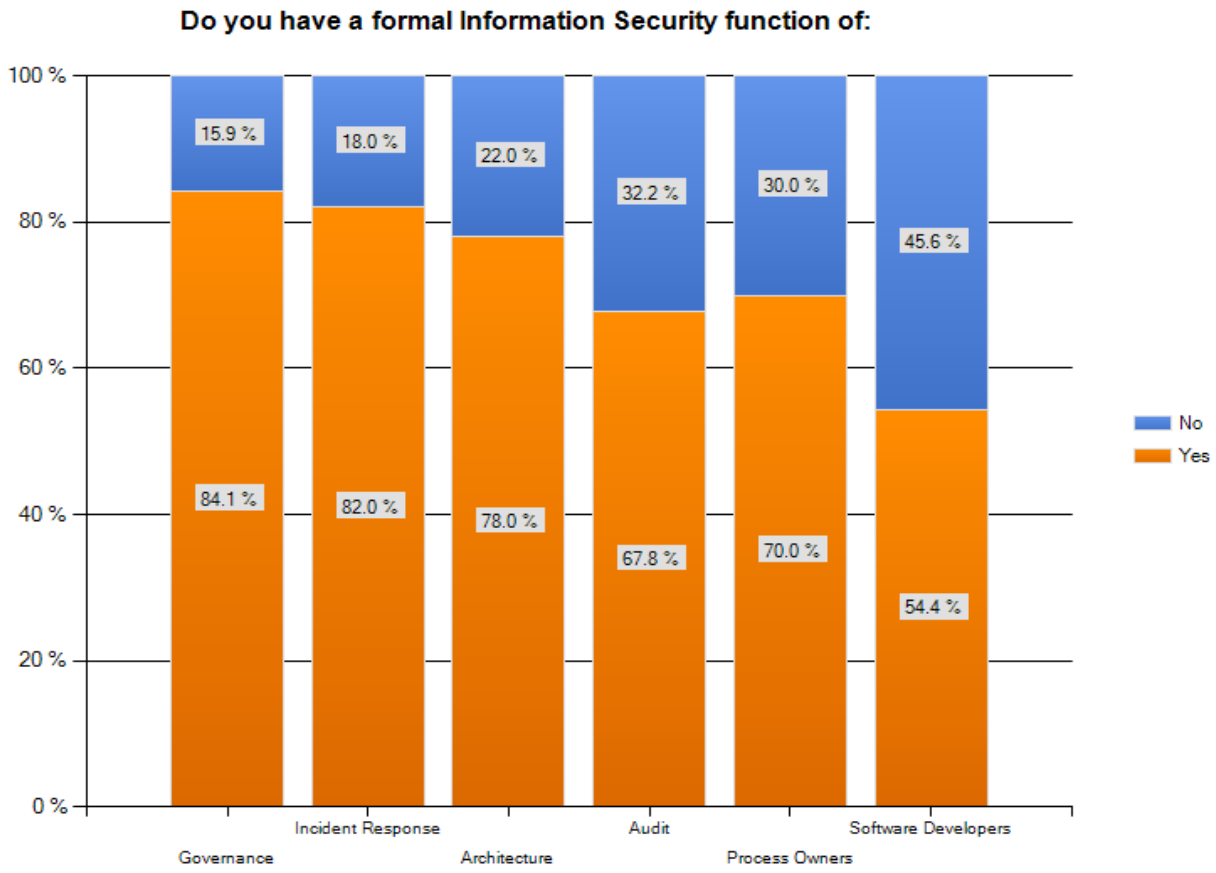


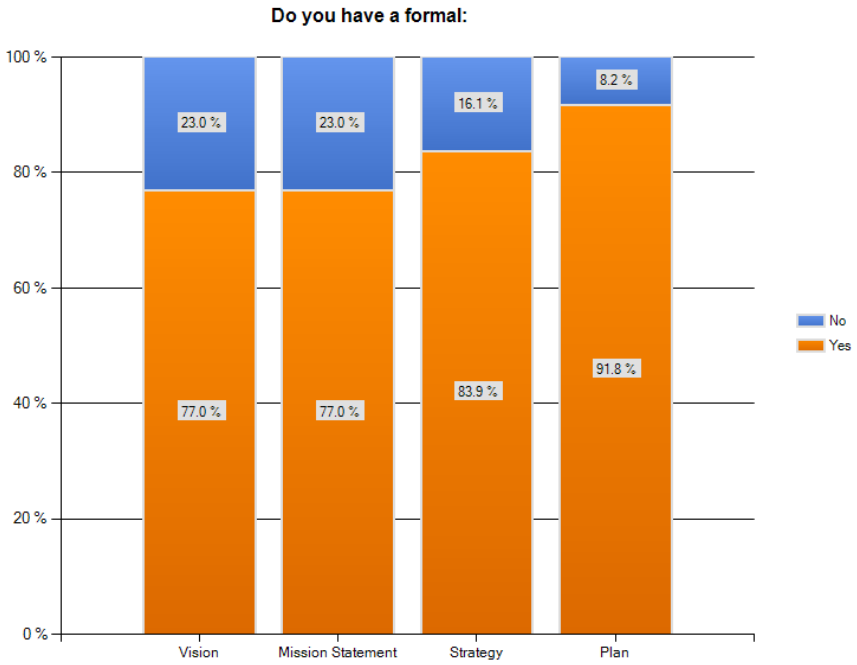
Not surprisingly, there is a good spread of staffing within the various teams. However, this is a lesson learned where the question would be more beneficial to have it relate to total population of the company, systems or some other factor. Another area of expected results is the fact that over 95% have formal policies and standards documented. This can and should be considered a expected practice.



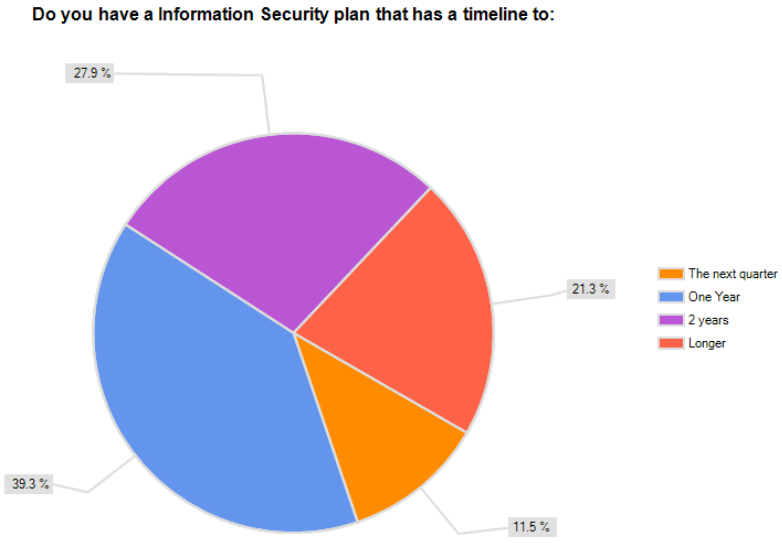


One of the more interesting results was the areas of formal focus for the IS group. Here we have the breakdown where governance is expected it starts to drop off. Two areas that took me back was the over 67% having a Audit function and the 54% having software developers. It was expected that these would be very small percentages if any at all. The real question goes to what type of software development these teams are doing. A couple of considerations are regarding application security and tool development. Application security has been implemented by few organizations, in my opinion, yet the development of common application api's for security could be part of this. Second, the cost cutting factors could result in teams building out their own tools for monitoring, controls, etc. Future questions should delve into this area to understand what these functions are and do.

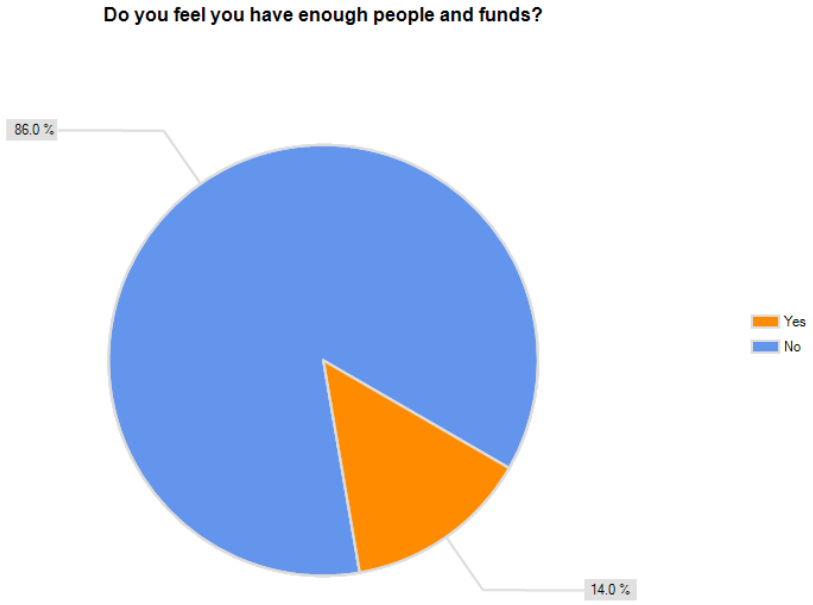


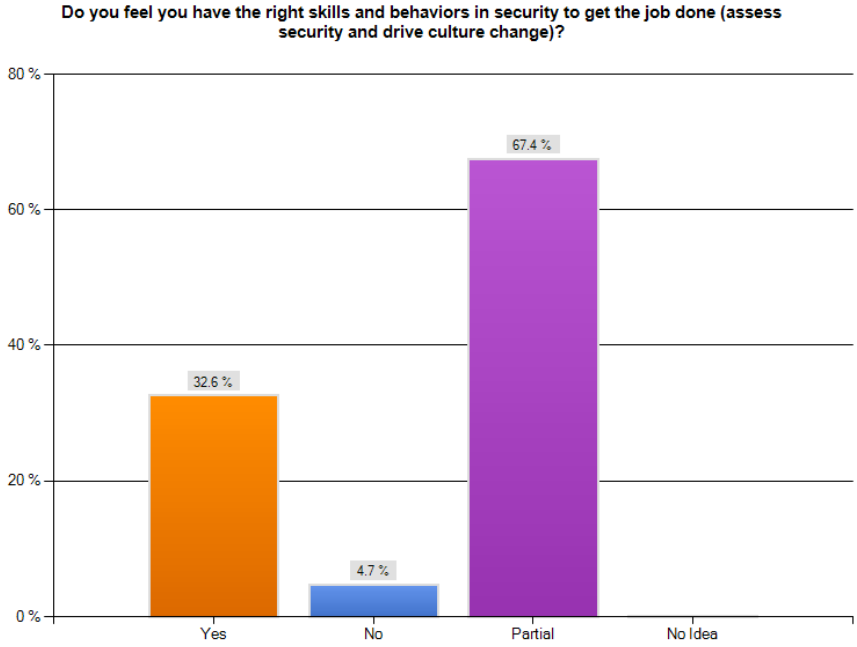


In questions regarding the makeup of the formal documentation we start from a typical vision, or high level, thought to a detailed and tactical nature. It was not surprising that "Plan" had a higher level of performance than "vision". Yet, it's my critical thought that these numbers are inflated as I've seen, in few cases, that any of the formal documentation exists. As we look deeper into the results, the vast majority of organizations have plans that go out one or two years.



One of the largest complaints we all have is lack of resources. Over 86% said they do not have enough people or funds. We do, however, see a partial skills gap between what we need and what we have. Over 67% of respondents say they have only partial skills to get the job done.

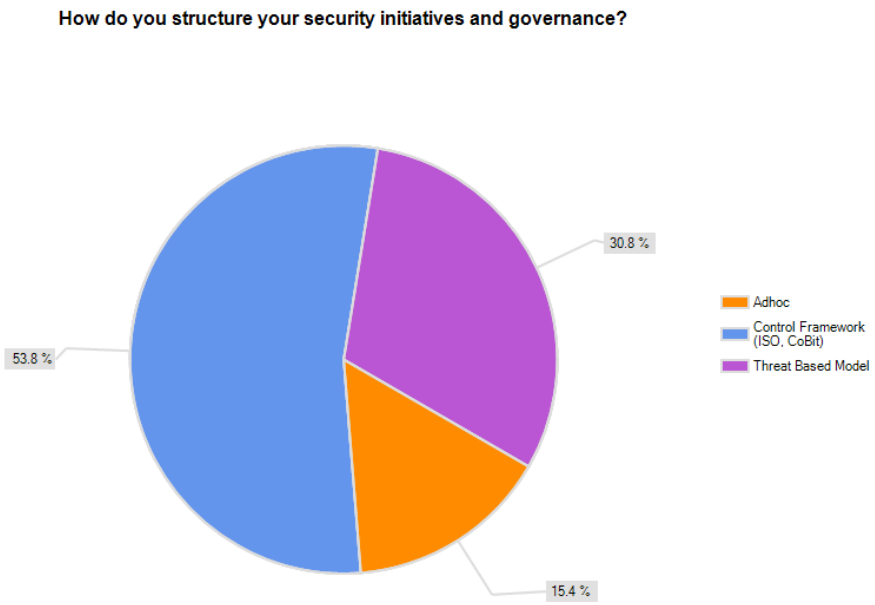




Governance and Risk Management

The subject of Governance and Risk Management have been long discussed throughout the history of Information Security, however, it's true definition and maturity in these areas that I question the most in industry. Where I have strong views on risk management, definitions, etc, I feel it's this maturity in industry that unlocks the potential to truly getting controls in balance to the threats. There is a significant amount of resurveying that needs to be done to drill into the details here, however, it's important to note that it's a conversation much larger than it used to be, regardless of how narrow or wide of focus for individuals.

It's expected to see that the majority of organizations use a control based model to structure their initiatives. I was surprised that a threat based model accounted for over 30%. This model means specific things in my mind and the question could gap from the respondents. Further surveying is needed to drill into particulars.



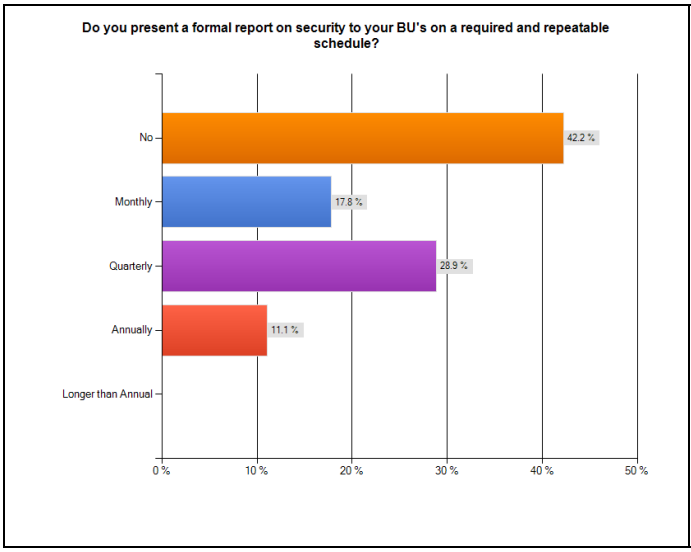
Text Responses

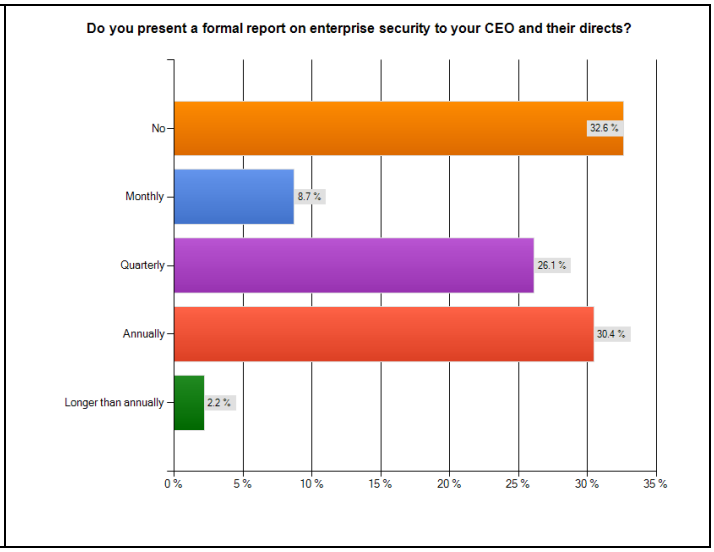
- all the above. start with control framework, work through threat, but modify as needed
- Customer based
- Mix of the above. Trying to move to threat based with a basis in control framework.
- All of the above. Governance is ISO/CoBit. Initiatives are Adhoc or TBM.
- Intelligence driven threat model measuring risk investment tradeoff against control framework

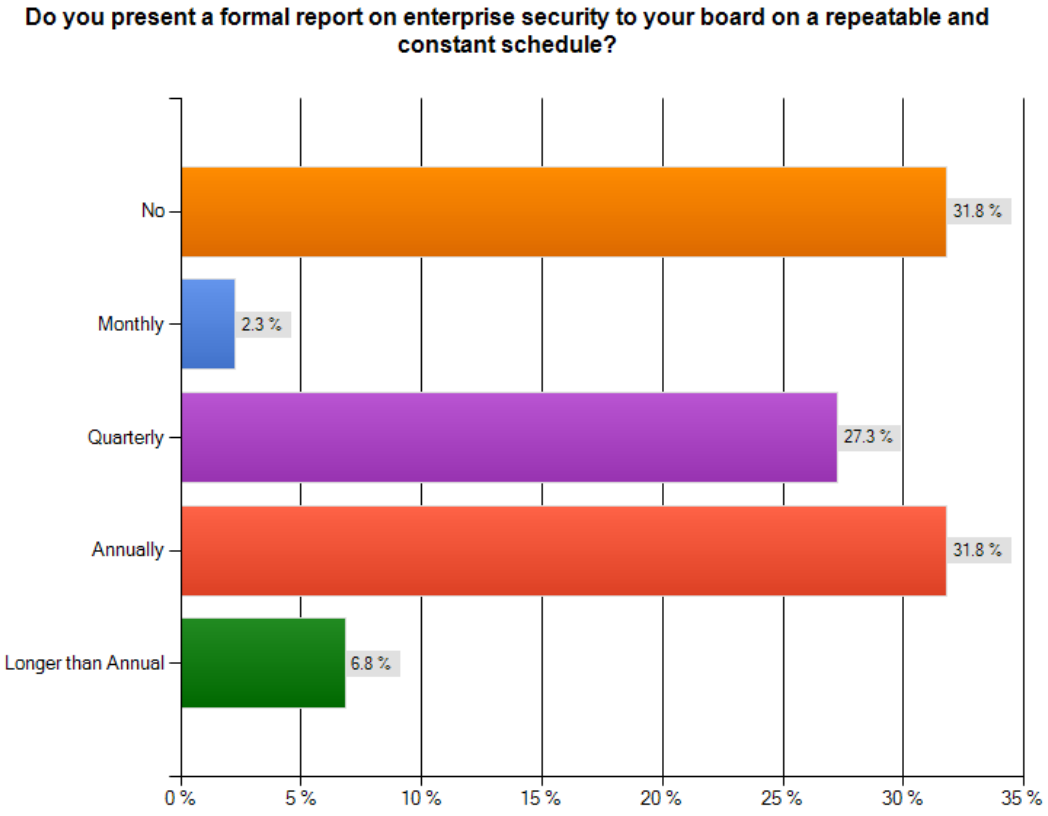
- We use ISO for our overall maturity framework; COBIT for our controls framework, and a long-range (3yr) functional roadmap for site capabilities
- Hybrid of Framework and Threat

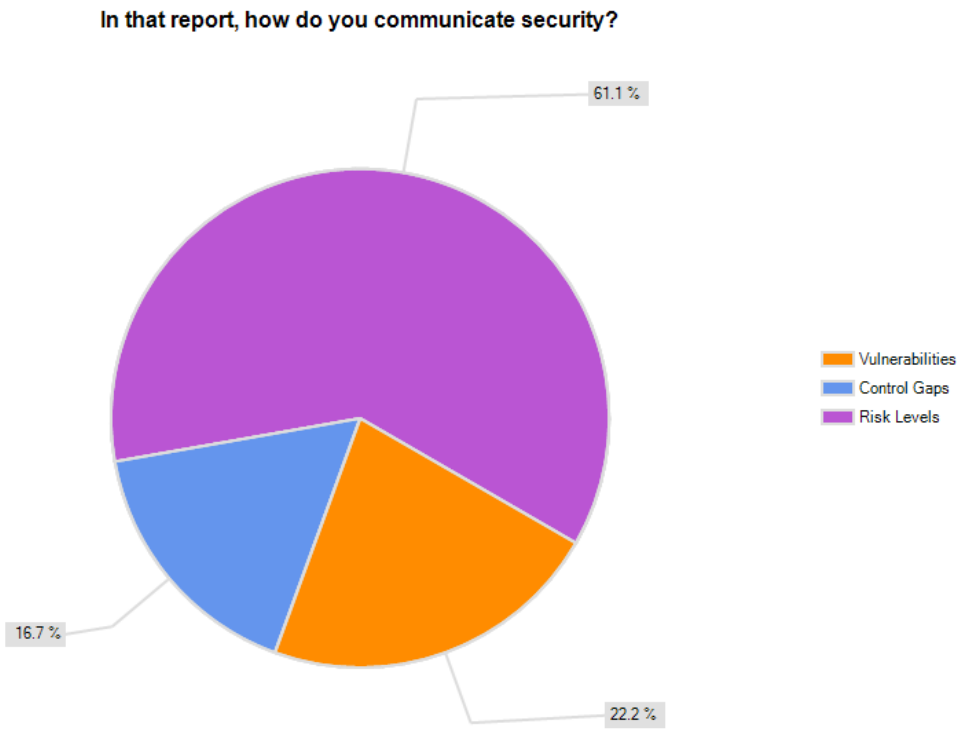
One of the most important things I feel we can do is to drive a risk based conversation into our respective organizations to have a conversation of security. It's only when we change the culture of the company to include one of security that I believe we have the ability to implement controls. To this point, it's important to understand what types of conversations exist. Our conversations, generally, exist between us, CEO, CEO's directs, executives (VP +), managers and company as a whole. Over 40% don't have a formal report on security, risk or not, to business units within their company. Yet, over 30% do report to the CEO and their directs on an annual basis where another 30% don't report to them at all. Over 50% report to the board on a schedule during the year where over 30% don't report at all.

The conversation during those meetings is very interesting where it's over 60% on a "risk conversation". This is important as we look later at the definition of risk. I feel that this is one of the major areas in industry we need to get a maturity on as the way we define "risk" varies greatly. Having said that, regardless of the methodology maturity, "risk" is having some level of judgment on the impact to the company. It's this business understanding that makes the message receptive and executable in actions.





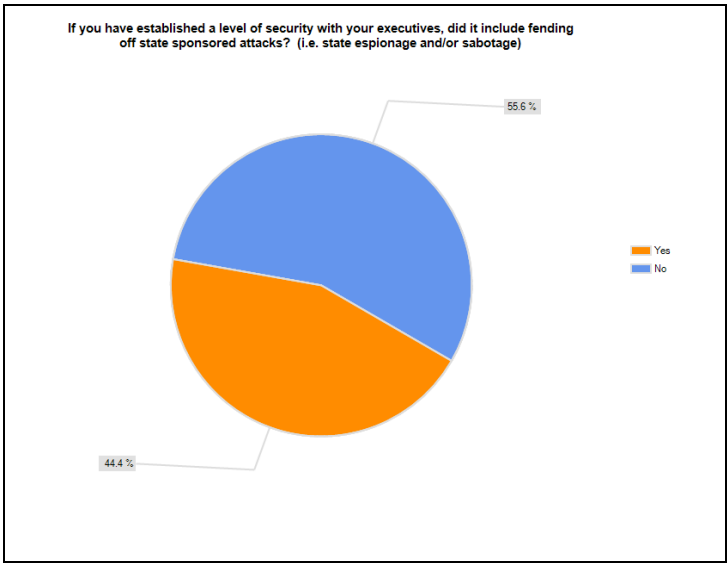

Do you present a formal report on enterprise security to your board on a repeatable and constant schedule?
No
31.8 %
Monthly
2.3 %
Quarterly
27.3 %
Annually
31.8 %
Longer than Annual
6.8 %
0 %
5 %
10 %
15 %
20 %
25 %
30 %
35 %

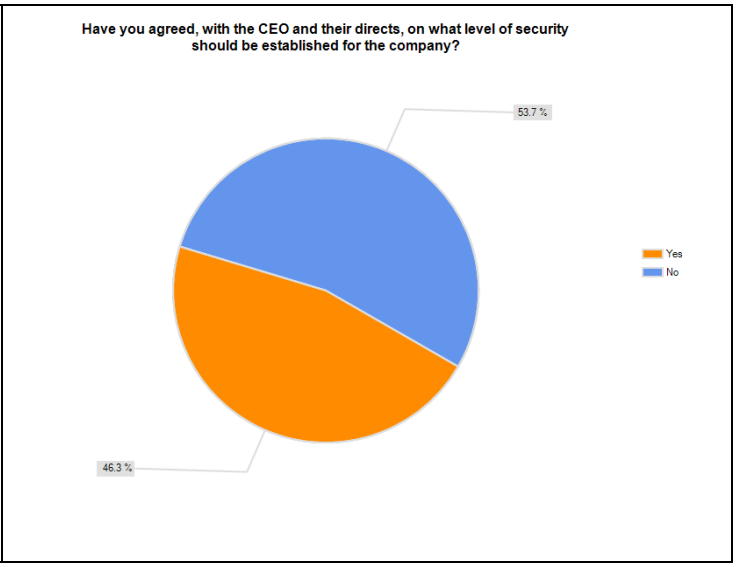


Text Responses

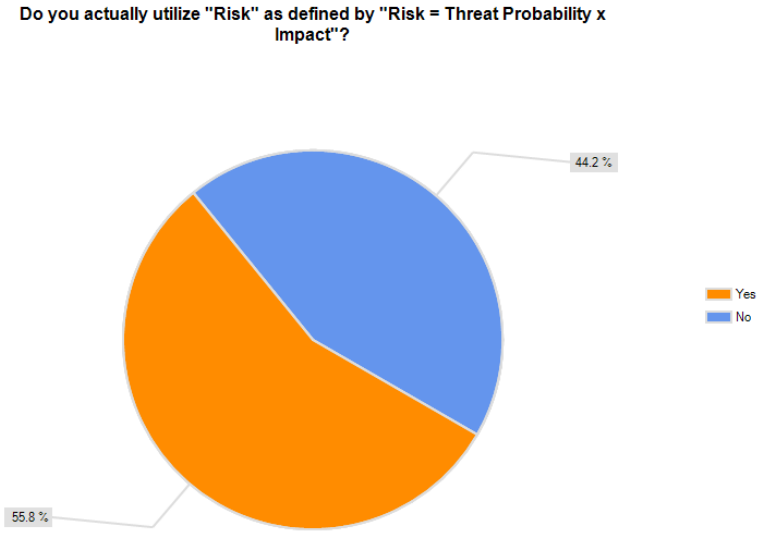
- Very high level report
- ISO CMM maturity level
- Mix of the above
- Security initiatives
- What's moving forward
- All of the above
- Project Metrics
- General maturity, including risk posture
- All of the above

Recently, the media, vendor and industry conversations have surrounded on the subject of "Advance Persistent Threats" (APT) and/or "State Sponsored Attacks". Where my opinion is that these state actions have been going on in the physical world forever and electronic manifestation of them should not be a surprise, it's the response in public that is interesting. There is a feeling, in industry, that our level of security should be one to defend against a nation state espionage or sabotage attack. This is very troubling as that would require a company to implement defenses to the level of intelligence or military organizations. Where it's possible, it's that conversation that is needed within our companies to determine where we want to go. I was not surprised that the conversation came up in over 44% of respondents considering the past two years of media attention. I was, however, surprised that a conversation occurred with the respective CEO on what level of security that should be attained occurred in over 40% of the respondents. I feel that this is a critical understanding that facilitates the implementation of controls and has been lacking in the majority of companies. I see this response as a key indicator in the maturity of our industry.





The definition of "risk" has been, in industry, with the "Risk = Threat Probability times Impact". I have strong disagreements with this definition as I feel it's impossible to ascertain probability. Even other industries have migrated from it to one of estimates and qualitative judgment (Frank Knight 1929 "*Risk, Uncertainty and Profit*"). Over 55% of respondents feel they use this formula to define risk.

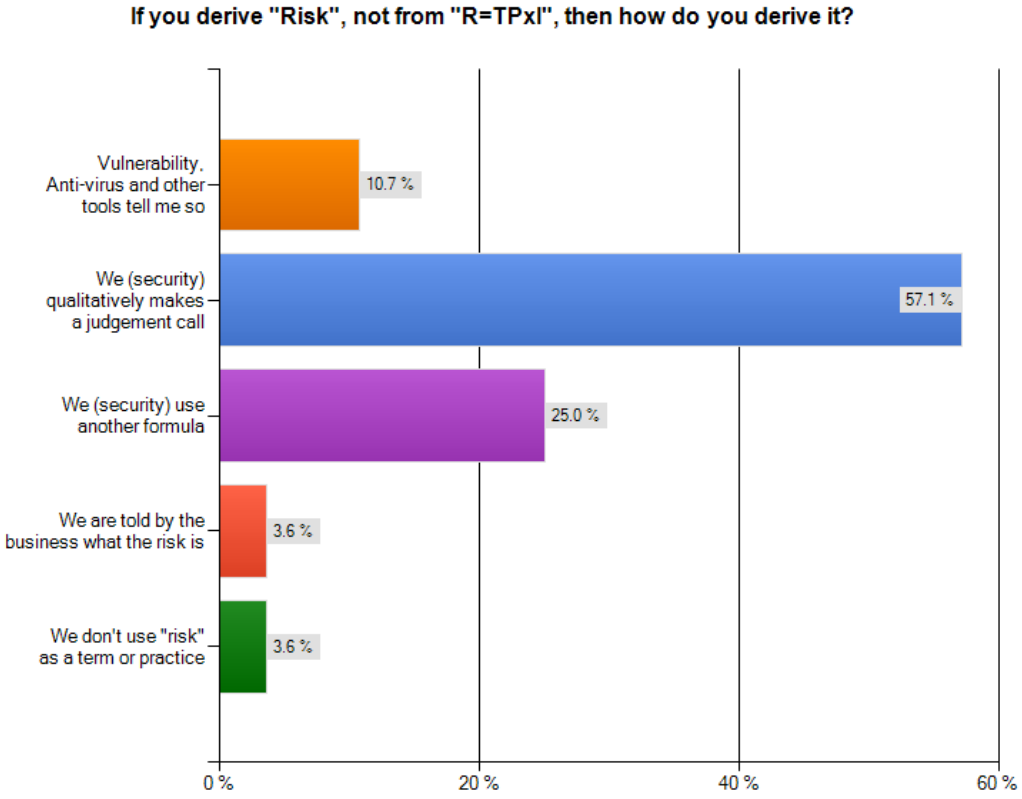


Of the 44% that do not use that formula to derive risk, 57% of them use a qualitative methodology to determine it. 25% use another formula. This is important as a follow up as the details around other methods of deriving risk is critically important to gather. Some of the text respondents show that importance.

Text Question and Response: If you do utilize "R=TPxI", how do you compute "Threat Probability" and "Impact"?

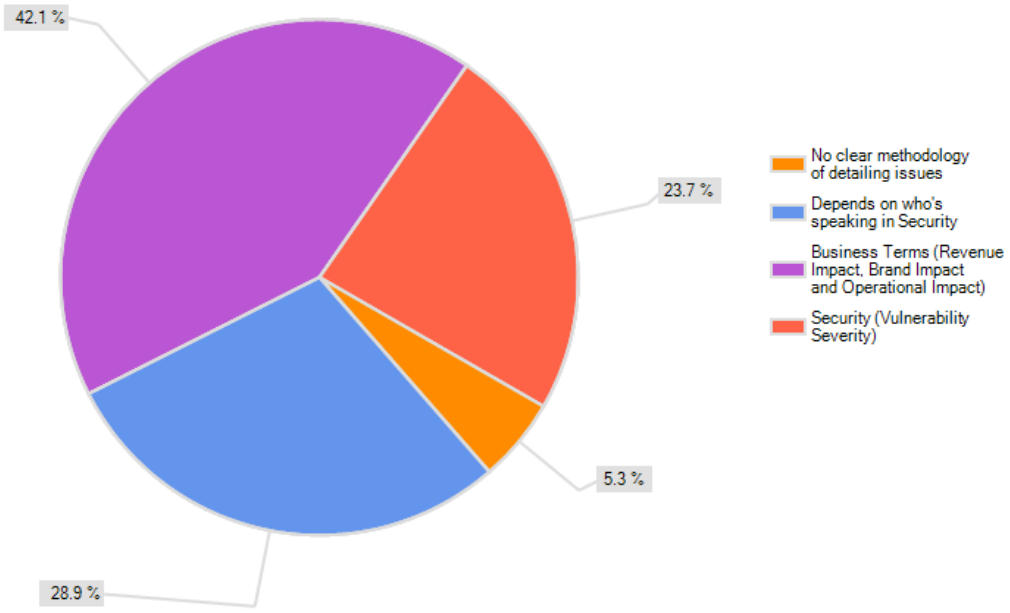
- Utilize CVSSv2 values
- Dread in exception management
- Not formalized
- From a BIA and industry figures when internal numbers cannot be generated.
- FAIR model http://fairwiki.riskmanagementinsight.com/
- Exposure of systems, number of users, known vulnerabilities that exist and their ease of exploiting. Impact includes number of users, dollars going through it How much business we have, what downtime would start to impact the business, whether it is likely to take one system down or many, time to fix. That said it generally isn't a hard number but guestimates.
- Impact is computed by utilizing research on impact of incidents, specifically those reported by our peers. Threat probability is a little more subjective.
- Probability is derived from the perceived complexity of the threat and the required components for the vulnerability to become an exposure. Impact is based upon an average dollar amount calculated from past issues and used as a "best guess".

- Validated threat focused, where TP is already 100%, then prioritized by impact. Actuarial tables on the horizon for TP < 100%
- Risk = Threat Frequency x Probability x Cost Freq = estimated attacks per year (use SIEM to measure) Prob = 1-100% chance of any one attack resulting in a breach (based on known past events & industry events) Cost = $ associated with damages (quantified by legal fees, call centers, lost employee productivity, regulatory fines, stock plummets, and customer losses)
- T*I = Inherent Risk factor in mitigating controls to determine residual risk
- We have a detailed list of factors and scoring to come up with these specific to our business.
- 1 to 5 and 1 to 5 too
- OCTAVE model: Probability = intuition Impact = Financial (real $), reputation, legal penalties, health and safety, productivity.
- With great difficulty, but using categories of impact, rather than actual probabilities.
- Experience and Consultants



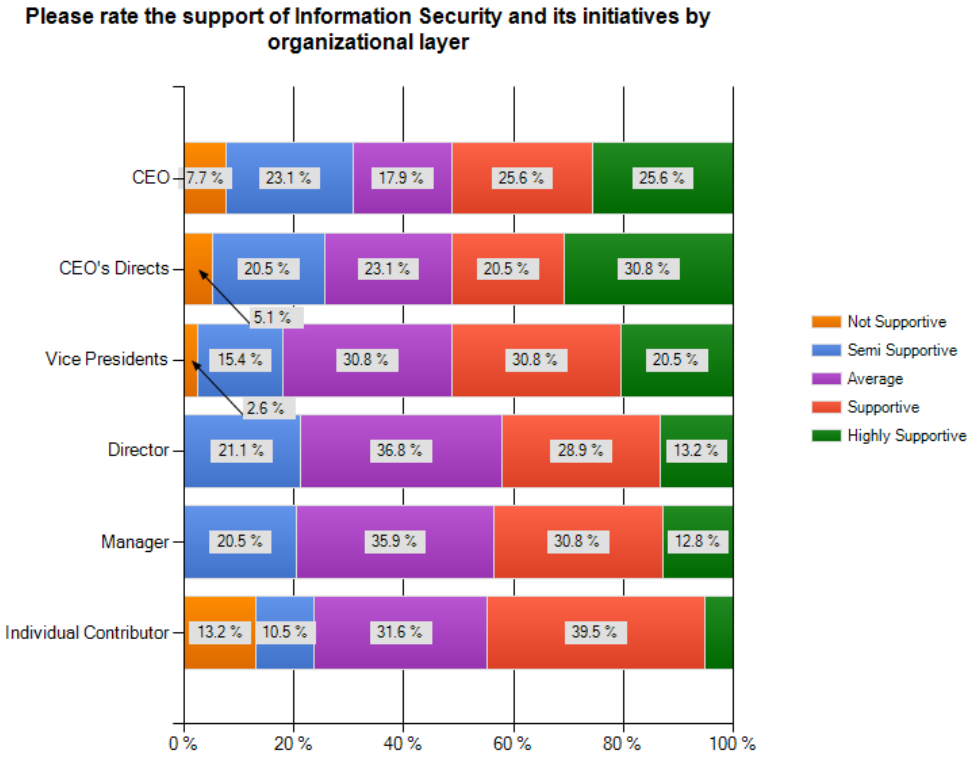
Finally, the risk communication that we make is 42% based on business terms. 23% say risk is communicated in terms of vulnerabilities. Where over 28% say they communicate risk differently depending on who in the security organization does the talking.

Do you communicate out risk in terms of:

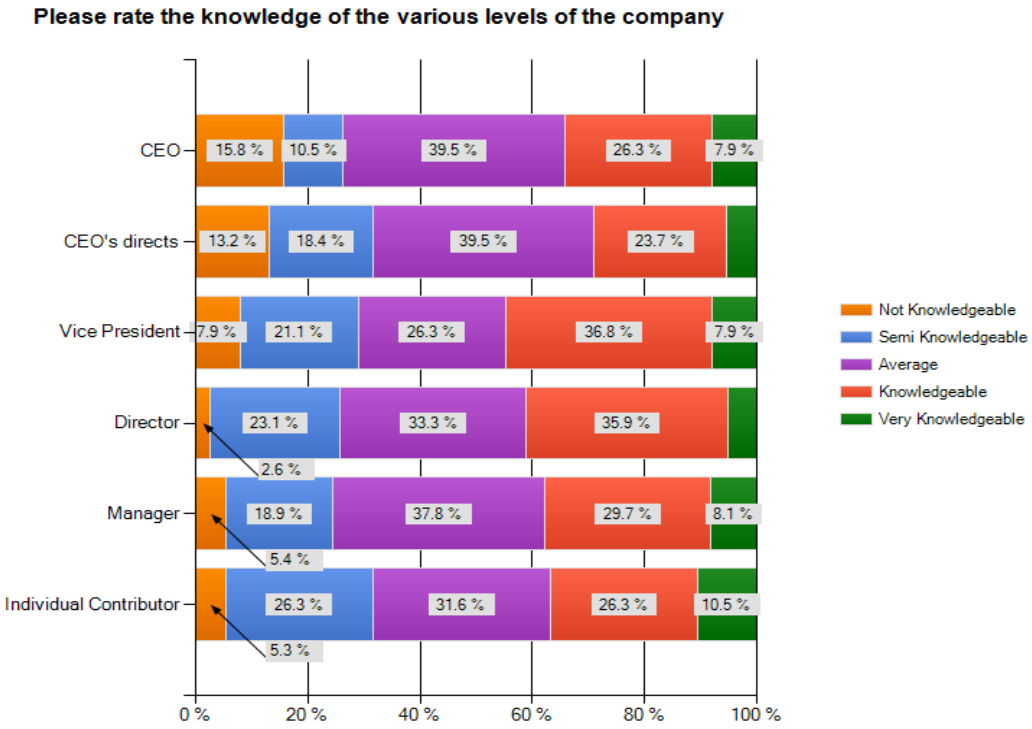


Culture and Communication

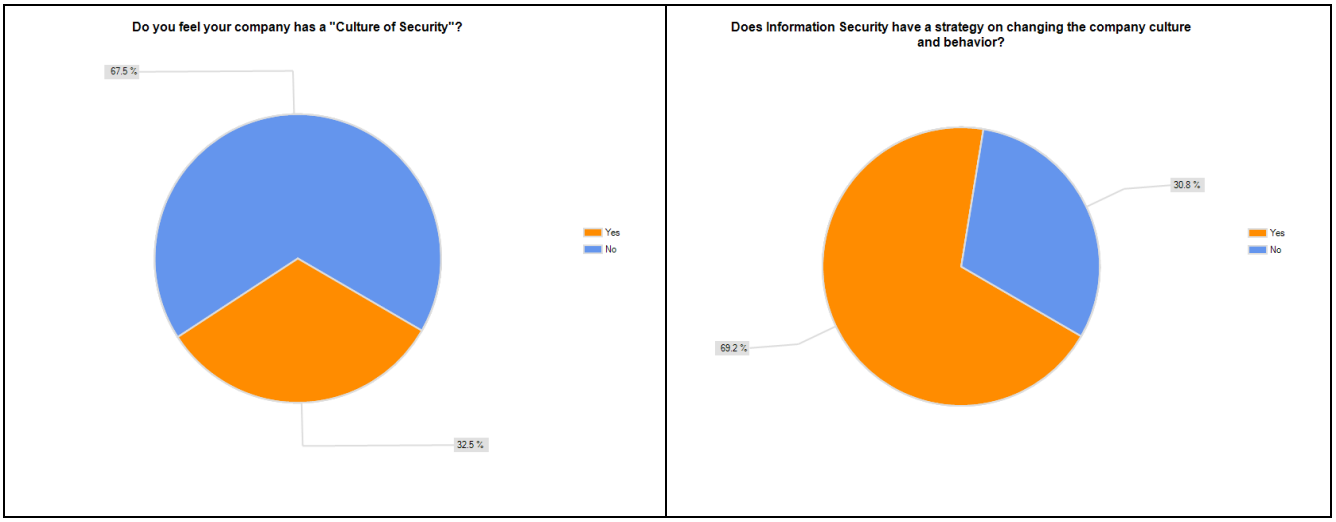
In looking at the overall aspect of driving security into an organization, it's critical that we get the support from the company to implement the controls we need to. To do this we need to look at how we communicate as well as what we communicate. At the various levels it's important to note that there is a feeling of support from the CEO and his/her directs and then starts to decrease as we go lower into the organization.



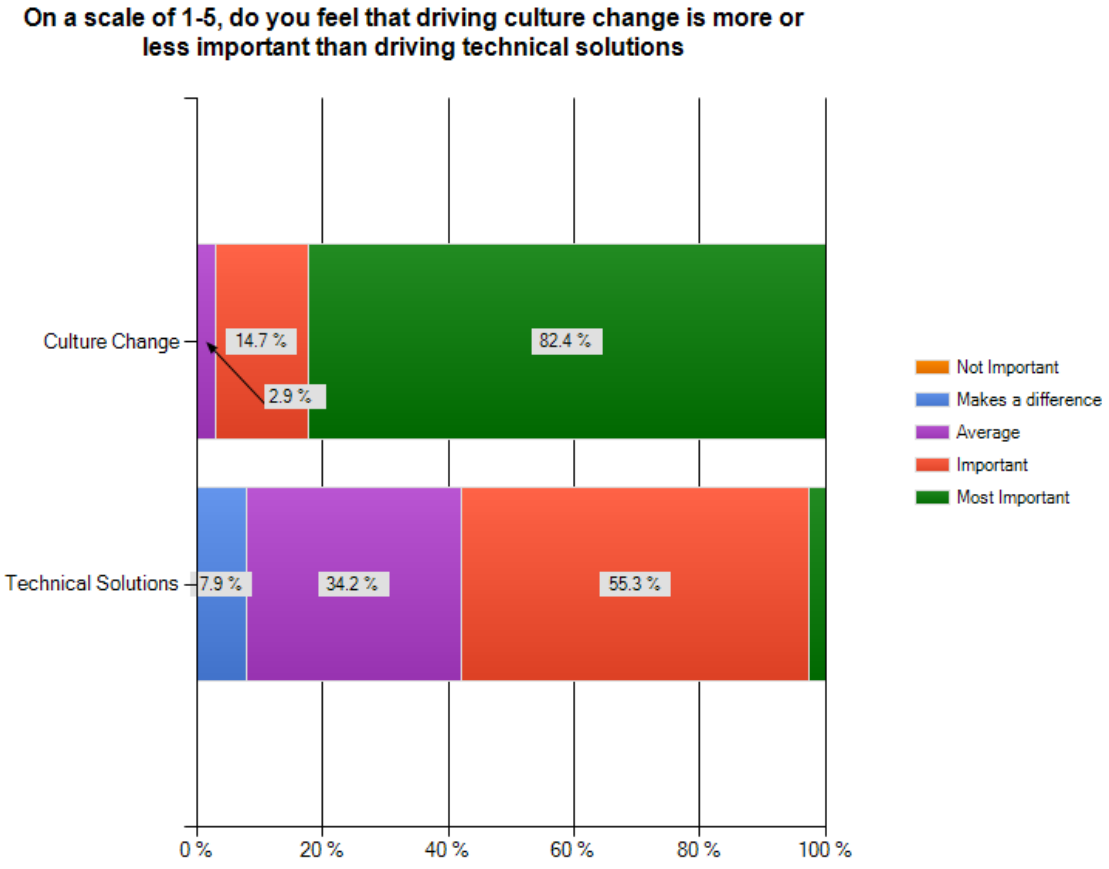
Also important is their knowledge on security. We see a general "average" understanding across the company with no one level really having significant knowledge over the other.



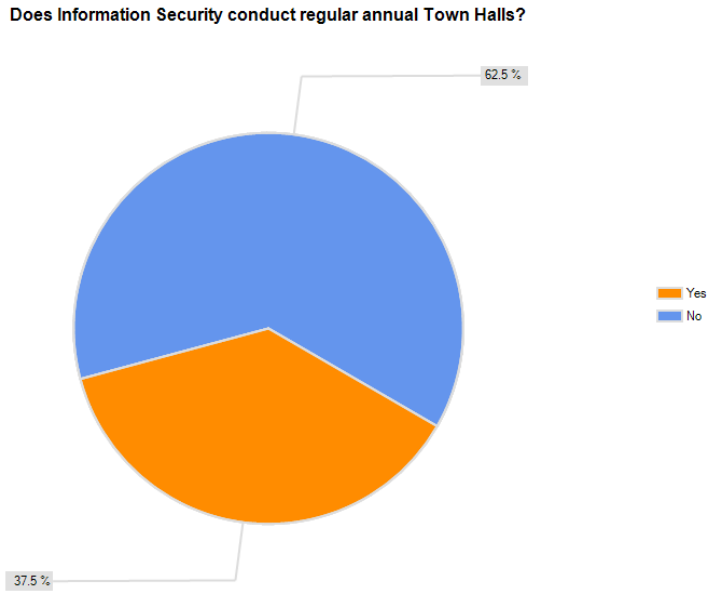
Yet, as we ask the question is if there is a “culture of security” the response is a resounding “no” with over 67%. This begs to ask the question as to “why”. I see we have four key variables, the action of communication, the story that we are communicating, the communication vehicles and the communicator. It’s also critical to note that this is a significant area of importance to companies as over 69% of them have a strategy to change the culture. It’s this failure to drive a conversation to the company that has resulted in the lack of a culture change.



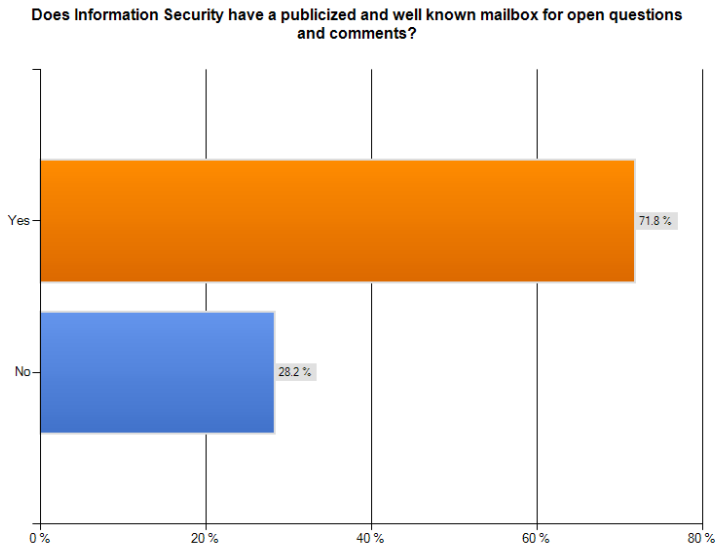
To underscore this, over 82% of respondents feel that culture change is the most important thing when compared to technical solutions. Again, if we feel it's that important, we have strategies to deal with it and we have good CEO-1 support why are we failing? We must look at how we are communicating and who we are communicating to.



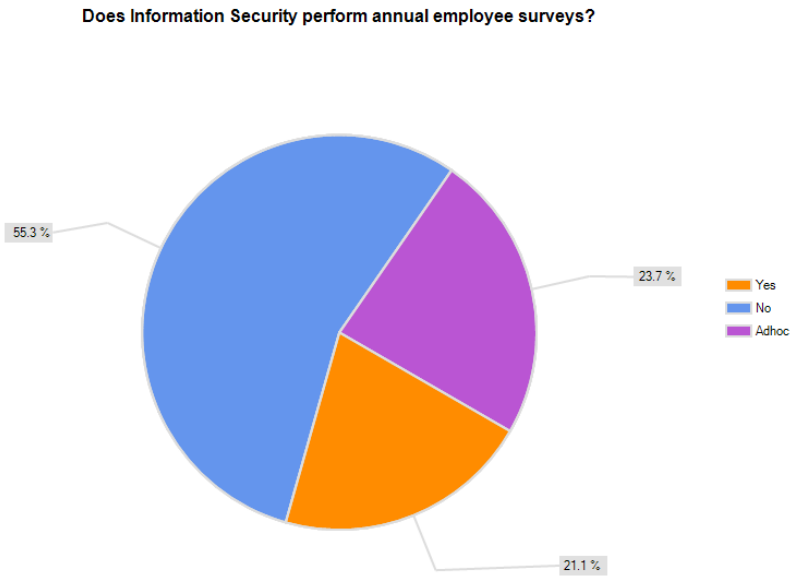
If we feel our CEO and their directs are supportive and the other end of the company is not, then we need to look at how we are trying to solicit their support. One method of doing this is to host town halls to allow for open discussion and education of employees. Over 60% of companies do not have regular town halls.



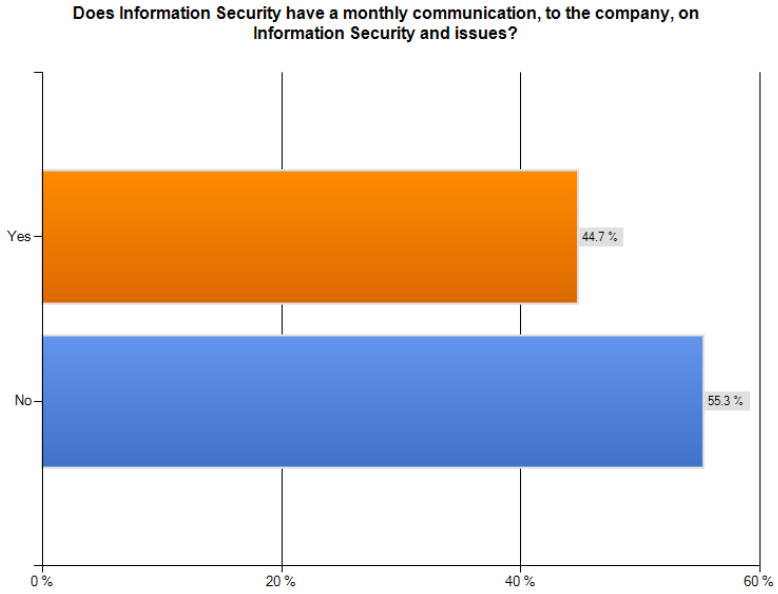
For open communication, over 71% have a mailbox that is there to receive questions and/or issues from the company. Further questions should investigate number and type of messages the mailboxes receive to ascertain effectiveness.



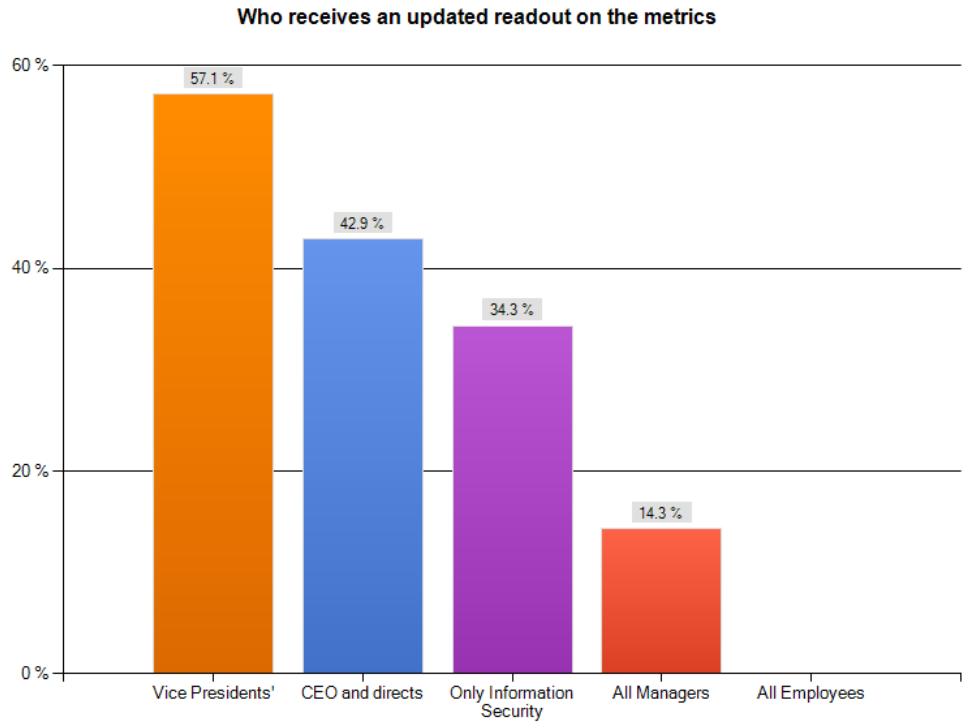
Over 55% of organizations are not performing any company survey's to employees. 23% are doing them adhoc with only 21% doing them annually. These surveys can be a treasure of information as to who's not supportive of the security message and why. It's this level of understanding that is needed to change the culture which appears to be one of the reasons why the cultures don't include it.



On a positive, over 44% are performing monthly communications to employees on security issues. This is a good and common mechanism to reach all employees on what's going on and get their support.



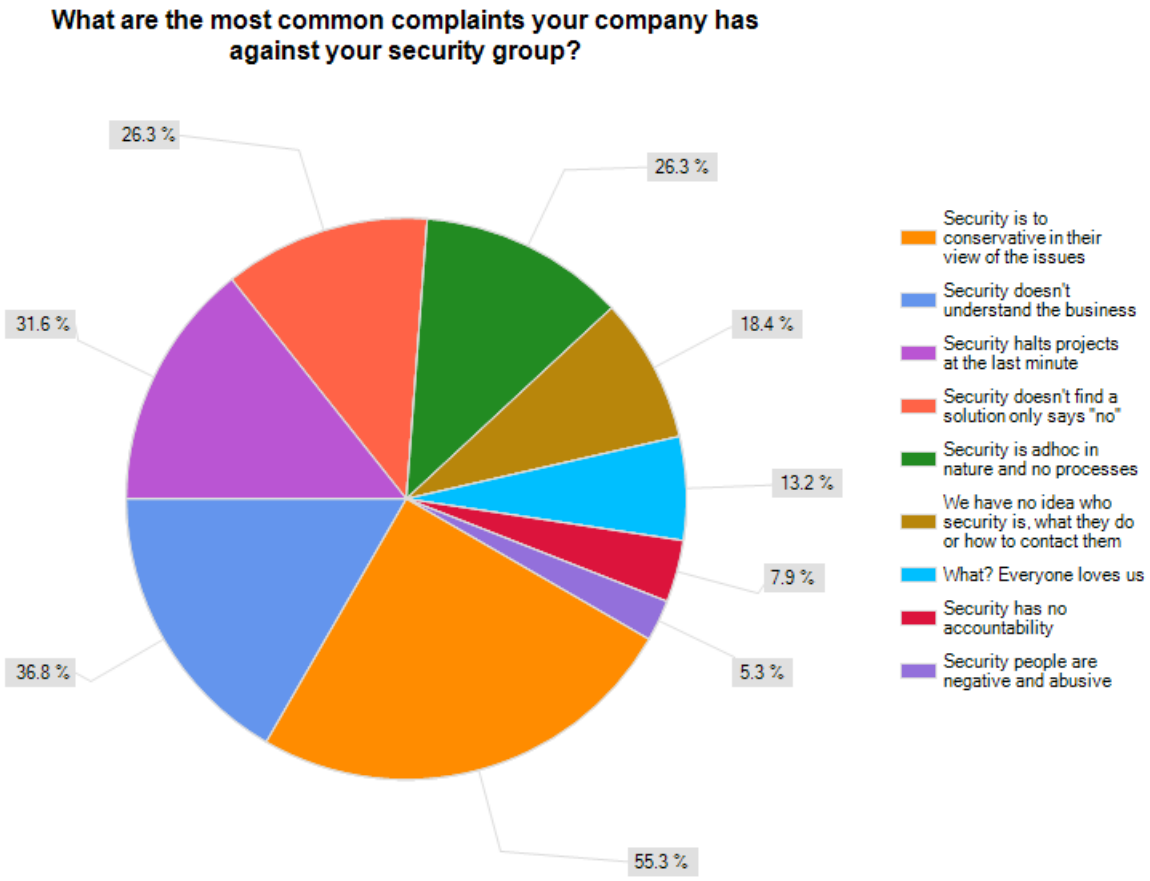
One of the common ways to bring employees into a culture of security is with transparency. To this, we should have a good amount of communication to employees on what's going on. Not shocking, none of the respondents communicate their metrics to all employees. However, almost 58% communicate them to all VP's and 42% to CEO and directs. This is another possible reason as to why executives are supportive and the rest of the company isn't and why our companies do not have a "culture of security".



Text Responses

- CIO
- CTO/CIO and staff and Legal (Privacy)
- Some IT managers and heads get them. Beyond that I'm not sure of the scope
- Technology leadership team

Where it's hard, it's important to understand what the issues are with our organization. Having this level of understanding makes it possible to adjust and/or educate others to a better position. Over 55% feel that "security is "too conservative in our views of the issues". Another 36% feel "security doesn't understand the business" and lastly, 31% feel "security halts projects at the last minute". To these points, having security embedded at the right levels, changing to a risk based conversation on business terms (value, brand and operations) and ensuring business leaders are involved in the decision making process can help. Lastly, it's important to have those business leaders, when the judgment is for less risk, to communicate it to their team. It's this top down support and belief which starts to make it a overall business led effort vs. Information Security.

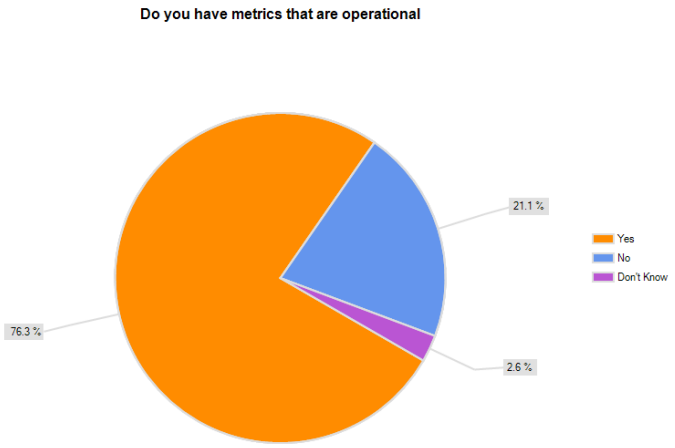


Text Responses

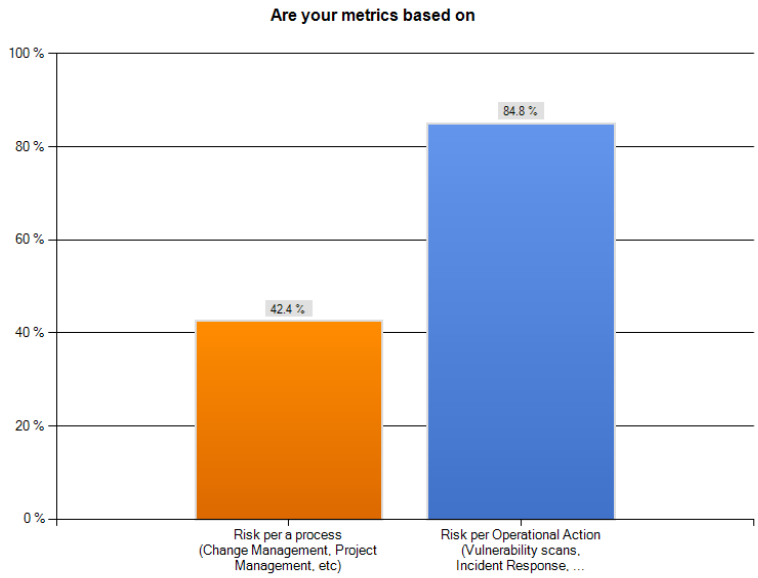
- because we often don't hear about them till the last minute
- Security slows projects, impedes agility
- Minimal complaints. The business is too busy to complain about security.
- We gatekeep some things like LinkedIn, so they don't like us for blocking their access, but we're really just the messenger. Interestingly, usually if given enough time, they come up with some decent security ideas on their own and they realize some of the stupid things and reject them without us speaking up.
- Security is big brother and won't let me do what i want

Metrics and KPI's

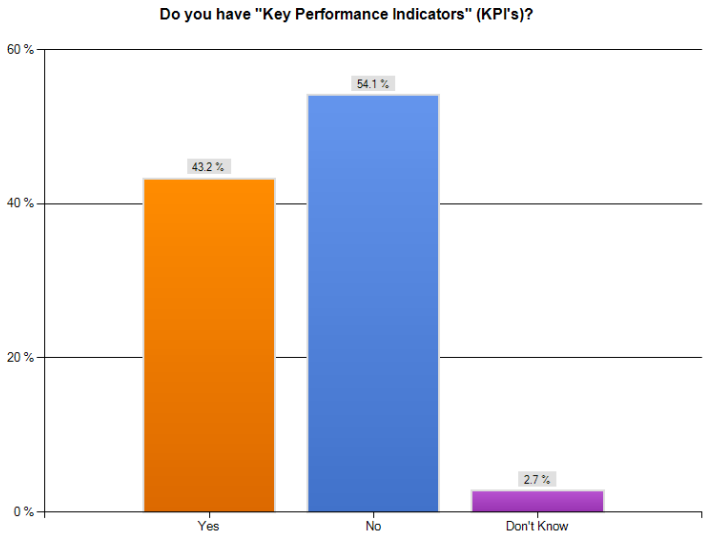
Our entire industry has had significant trouble in defining metrics that actually help us do our job. It's been this lack of ability to get the metrics that has hindered us in being able to mature to a predictive model. Over 76% feel that they have metrics that are operational.



Of those who have metrics, over 84% are based on tools and other means vs. metrics around security within a process. This is interesting as I feel the tools are a used to derive an understanding of risk, yet, the risk needs to be placed within context which is the processes. i.e. "Are we introducing more risk vs. fixing it?" this would be done in change management, project management, etc.



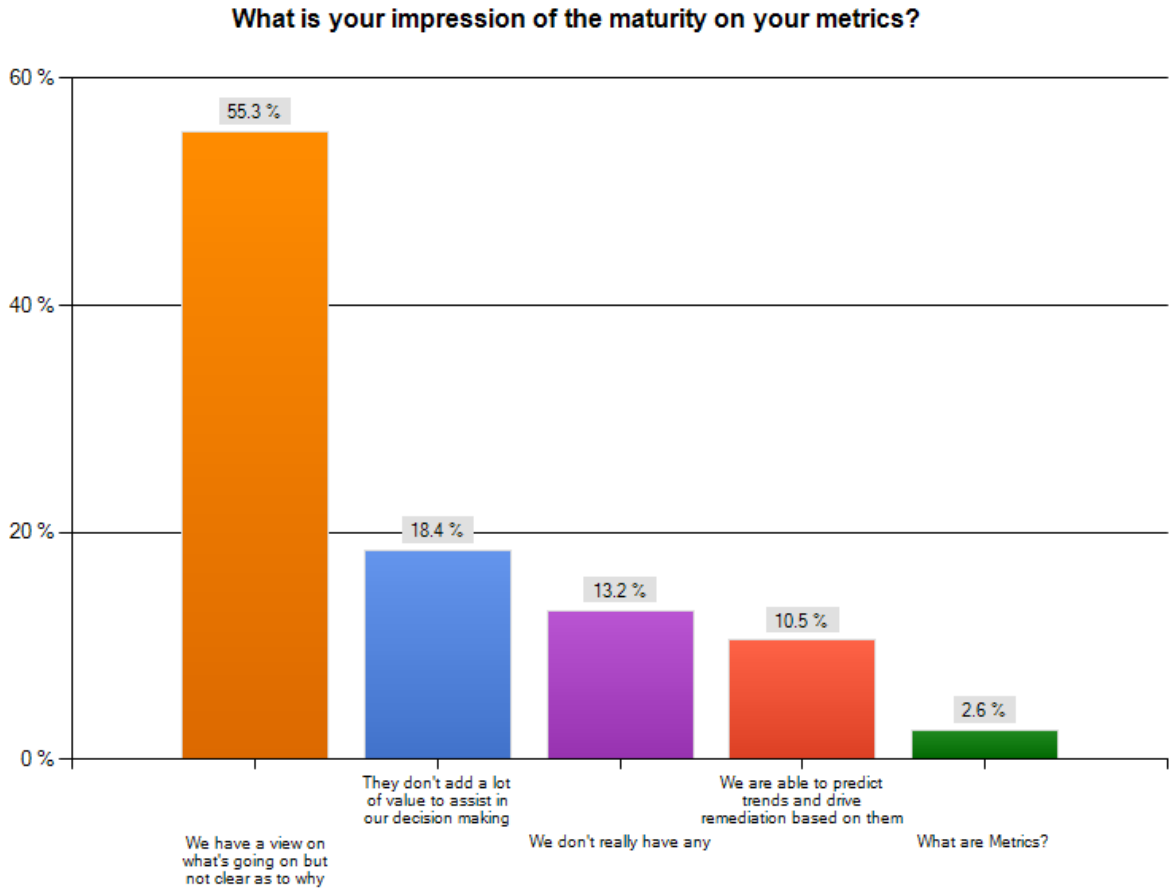
I, personally, have never met anyone who's been able to come up with KPI's, yet, over 43% of people feel that they have. It will be good to get a deeper dive into this in later surveys to understand what this really is made of.



Text Question: What, exactly, are KPI's to you?

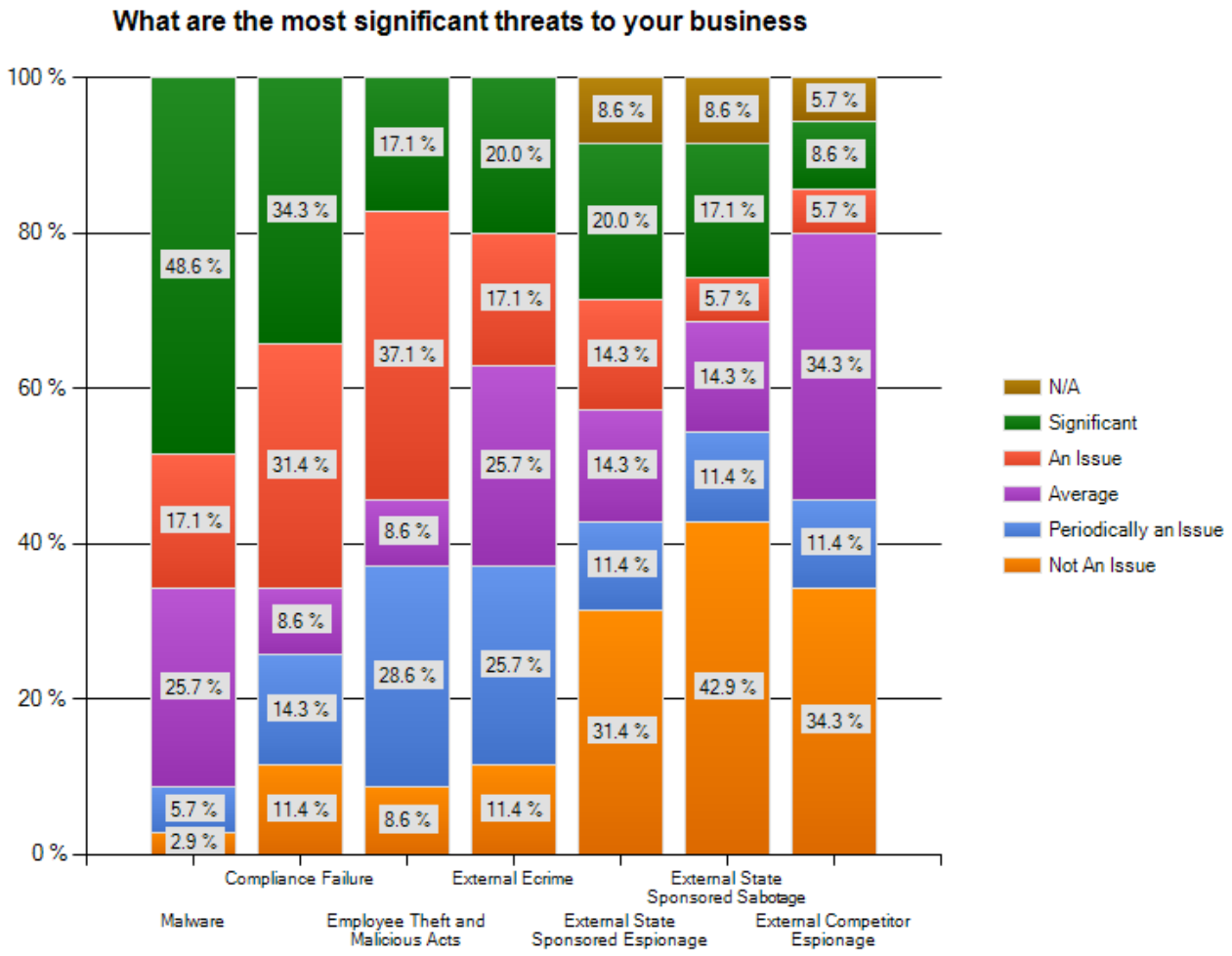
- metrics with value based on business outcomes
- Anything that indicates overall risk posture is trending one way or the other.
- Security indicators that could impact the bottom line
- Indicators of effectiveness of security controls
- YoY TCO Mean time between Security Incidents Mean time to remediate Vulns Number of Security Exceptions, accepted, rejected, closed. KRI - Security engagement vs SDLC engagements and PMO engagements
- Progresses on patch management, anti-virus coverage, ID management, network/firewall alarms and the response, and the relevant metrics.
- Correlation of metrics to tell a story about risk.
- incident metrics, service utilization metrics for our office's services (scanning, consulting, assessments, pentest, architecture)
- We have them, but I wouldn't say they're that good yet. They're more or less in development.
- Metrics, not statistics, with targets than indicate favorable or unfavorable trending of stated objectives.
- A method of holding individuals, organization accountable for delivering on vision, mission, strategy, and specifically the tactical objectives
- My bonus is determine by successfully attaining my KPIs
- As the new CISO here, this is one of my key areas to create in the next 6 mo
- Operational metrics tied to actionable measures, aligned with corporate goals and objectives. I don't have these in place for security yet, but am working towards this.
- Indicators that show the security work and advancement
- Meeting SLA's
- Measure of how well both the infosec team, and company teams generally, are performing their roles with respect to securing the company's resources. For example, we measure, by business vertical, how quickly their corresponding technology development team responds to P1 security vulns.

As expected, the respondents feel, over 55%, that their metrics tell them what's going on but not why. This is a common metrics maturity issue and a very difficult one to migrate from. Almost 20% feel that they don't add any value to their decision making. Only 10% feel their metrics allow them to make predictable decisions.

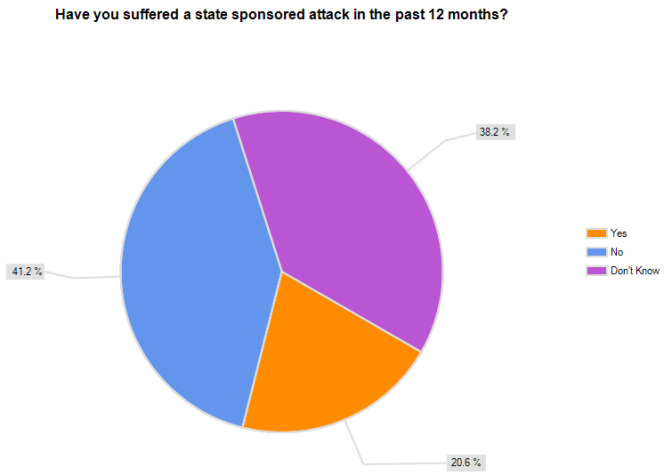


Threats and Risks

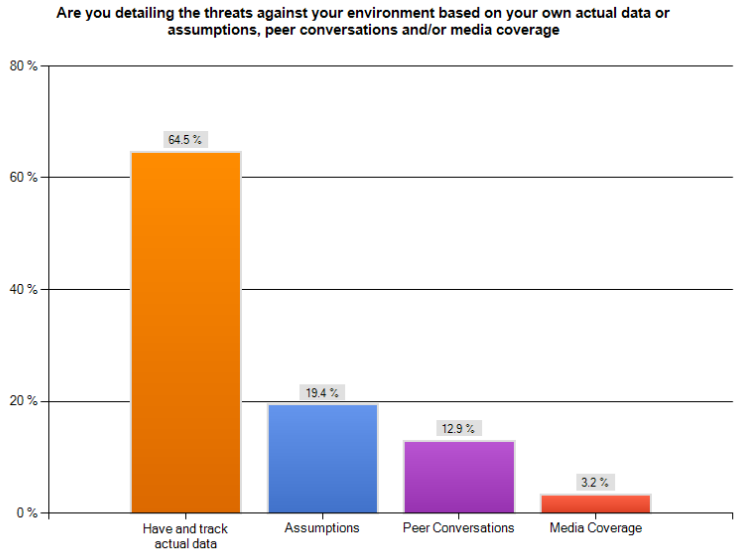
To get a good understanding on what level we need to implement security at it's important to get an understanding on what we feel are the threats. Aside from media attention to state sponsored attacks, it was interesting to note that they were the two least seen issues. State sponsored espionage and sabotage had 31% and 42%, respectively, as not being an issue. Only external competitor espionage ranked as high, with 34%. The two highest ranked threats were malware and compliance failures with 48% and 34%, respectively, at Significant. Where the conversation might be there, they still are not seen as significant threats to our business.



To follow this up in more detail, it was important to note that only 20% of respondents feel they suffered a state sponsored attack.



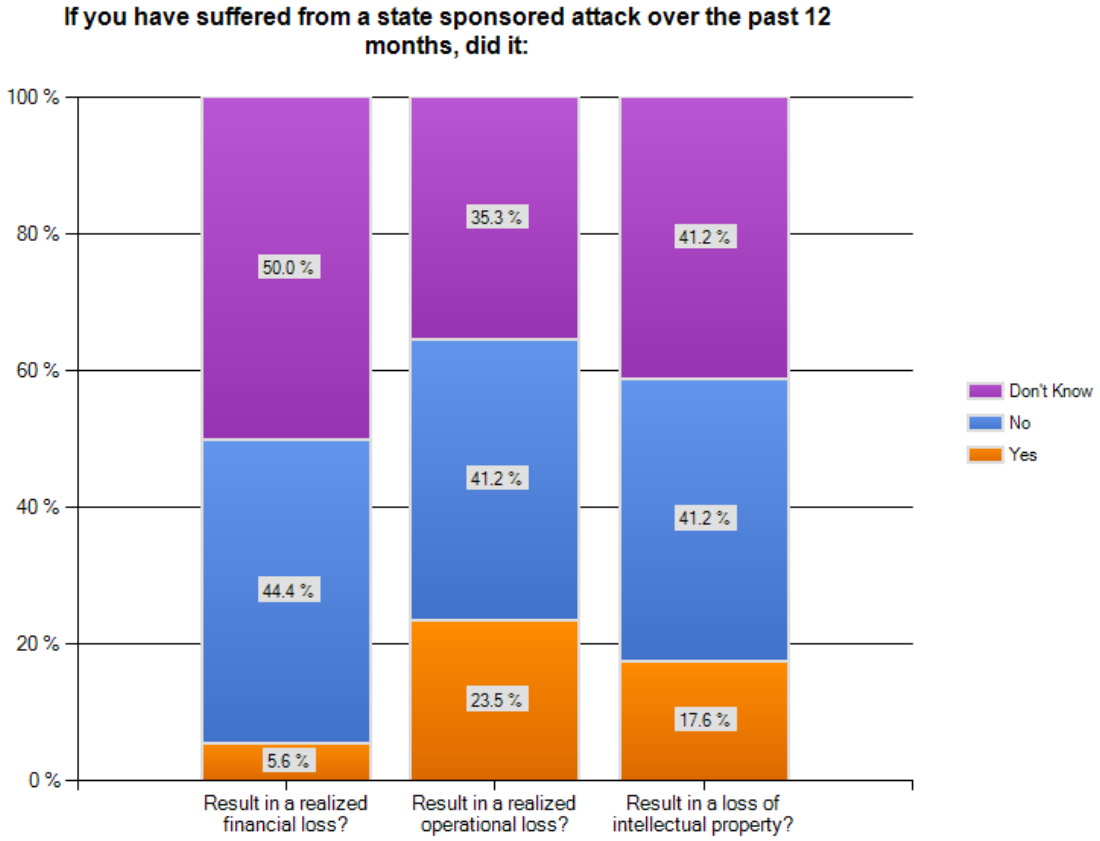
Lastly, it was actual data that most (64%) respondents got the understanding on what the threats are. This is very interesting since state sponsored attacks can't be attributed vs. assumed and 20% feel they have been the victim of them



Text Responses

- many of the above
- All of the above
- A mix, certainly media coverage causes us to get asked by C levels, but we try to keep a well rounded view.

Of those that have suffered from, what they believe, a state sponsored attack, only 17% feel that it resulted in intellectual property. This is a curious point as the main focus of state sponsored attackers, as it's commonly believed, is intellectual property. In either case, if the worst case is 23.5% have a loss of operational capabilities, the realized impact is fairly light.



One of the well known beliefs in security is to have your wish list in the top drawer in the event of an incident. The question that comes up is, when that incident occurs, what is the reality in relation to the support. In a significant positive, over 60% of respondents stated they received support from their CEO, CEO directs and/or board. This is significant as it goes into the face of our historical impression that the CISO's tenure is dependent on whether an incident occurs or not. On the negative, over 33% stated they never met and discussed.