Security Awareness – Many Audiences, Many Messages

By Rob VandenBrink
April 2010

Introduction

The common wisdom is that raising security awareness and influencing behaviors in the area of Information Security is not a dragon that you can slay with a single silver bullet, but is much more akin to the many-headed Hydra of Greek mythology, requiring many simultaneous attacks against each head to make a difference. The problem with this statement of the common wisdom is the same as most other statements that "everyone knows" – the statement is often not backed up with real data, and the multiple attacks are not defined such that the techniques are easy to follow.

This paper tries to explore both of these issues discussing various common job functions, and methods to motivate people in these positions, specifically in areas of Information Security. The raw data for these discussions comes partially from an online survey, posted on the SANS Internet Storm Center (http://isc.sans.org). The survey data was supplemented with interviews of people in these job positions. Additional "tempering" of this data was provided by personal experience.

This paper is targeted towards anyone who needs to raise awareness of security issues in their organization, or their customers' organizations.

Motivators , Job Functions and Industry Sectors

Motivator	Description
Corporate Profit	Impacts on Profit and Loss in the overall corporation
Department Profit	Impacts on Profit and Loss in the Department or Business Unit
Personal Financial Incentives	Personal Financial Incentives include commissions, bonuses and special incentives for education or changes in behavior
Corporate or Department Savings	Direct and Indirect cost savings in the corporation or business unit
Return on Investment	Profit / Loss decisions on a particular project
Uptime of Corporate Systems	Maximizing the uptime of corporate systems and networks
Uptime of Personal Laptop or Workstation	Rather than corporate systems, maximizing the uptime of a personal workstation or laptop
Protection of Intellectual Property	Protection of Images, Designs, Electronic or other assets that incorporate the Intellectual Property of an organization
Protection of Credentials or Passwords	Userids, Passwords, Certificates, keys, tokens and other means of authentication, authorization and access control to electronic or physical systems
Protection from Identity Theft	This is not materially different than the "Privacy issues" question. However, it's a buzzword that resonates differently with non-technical audiences so is included separately. The results for this section are combined with the Privacy section
Other Privacy Issues	Privacy issues incorporate financial, medical or other information that an audience has a reasonable expectation will be protected and private between themselves and their provider in that area.
Regulatory Compliance	Compliance with any regulatory framework - this includes HIPPAA, Sarbanes-Oxly, NERC / FERC, FCC and any other industry specific regulation
Legal Compliance / Avoiding Lawsuits	Compliance with criminal and contract legal requirements
Corporate Policy Compliance	Compliance with policies internal to an organization. These policies frame language for behavior within an organization that combines all of these motivators with corporate norms of behavior and corporate identity.
News Stories Affecting other Companies	Stories affecting other companies and individuals are an often-used, powerful method to influence behavior. They provide a concrete example of what being "that company" can have on an organization's financial standing and credibility in their industry.
Corporate Reputation	The classic contrast between reputation and honor is that "reputation is what others know about you, honor is what you know about yourself". Corporate Reputation is a combination of both of these, as they pertain to many of the motivators in this list.

In the survey (Survey results in Appendix A) these various motivators are evaluated against several Job Functions:

- Senior Management (CEO, CFO)
- Chief Technical Officer
- IT Manager
- Software Developer or IT Business Analyst
- IT Operations or Helpdesk Personnel
- Business Unit Manager
- Accountant
- Salesperson
- Engineer
- Human Resources
- Manufacturing Line Personnel
- Graphic Artist
- Call Center Operator
- Front Desk Reception / Office Manager
- Office Support Staff

The survey also evaluated these motivators across several different industry sectors. The interpretation of these results is not included in this paper, though the uninterpreted survey results are included in Appendix A:

- Medical
- Government (Federal, State or Provincial, Local)
- Financial (Insurance / Banking)
- Law Enforcement
- Emergency Response
- Educational Institutions
- Entertainment
- Food Service
- Transportation or Distribution
- Manufacturing
- Resources and Mining
- Legal
- Retail

Using Motivators to Phrase Your Message

The goal of this paper is to assist the Security Professional in phrasing their messages, with the end goal of positively influencing behavior of people when faced with a security related decision. The key is to understand what motivates your target audience, and phrase your message in those terms. A one size fits all security message will not be received well by most audiences.

For instance, influencing the decisions of an Application Developer, a Salesperson and a Senior Executive will require three completely separate messages. On the other hand, once a "playbook" of messages is built up, overlap often will be seen between target audiences, so content can be re-used. For instance there is a fair amount of overlap in both the motivators and messages when considering Engineering Staff, Graphic Artists and Application Developers.

But now that motivators are defined, how is the message best delivered? This answer again will vary from audience to audience.

If the audience is motivated by regulatory compliance, then the message needs to be phrased that way, but simplified considerably – regulations are complex, and not everyone is an expert! Get the facts right, but the message and the reasons need to be both simplified and shortened.

If the audience is swayed by personal profit, then a survey (phrased in a fun way) with prizes that people will value is a common option. Public recognition of winners is another motivator in this case.

If the motivator is productivity and uptime, then the message is all about the math – but keep the math simple. For instance, even if complex math is used in the day to day calculations of an engineering process or IT function, percentages and averages are about as complex a calculation as should be discussed outside of the department. Keeping the "number count" down to a minimum is also important.

No matter the audience or the motivator that you are leaning on, using a related story is always a good approach. Using a recent – or even a not-so-recent – story that resonates with your target audience will generally play much better than almost any other method. Try to keep the story short and directly applicable.

So what are the Motivators for Common Audiences?

The one motivator that is common to almost every group discussed is access to corporate email. Anything that impacts email impacts everyone, and if corporate email is down, very likely every group (except possibly manufacturing) is either not working, or not working effectively, and really annoyed about it. Email is separate from other corporate systems in this regard. People are often quite happy to not have a personal workstation or to do without other vital corporate systems, as long as email is readily available. As this is applicable to almost every group discussed, it is mentioned here, rather than being repeated for each target audience.

Senior Management (CEO, CFO)

Senior Managers have a lot on their plate, which means that in most cases, details don't play well. Their ideal situation is one that where they can "take in" the message in a short time, get the message, make a decision or delegate, and move on to the next issue.

They are motivated by a myriad of factors, but the ones that are generally at the top of the list are in the "steer the ship" category – things like:

- Shareholder Value is the single largest motivator for most senior managers in public companies, often driven solely by **overall corporate profits** and **corporate savings**. Shareholder Value is a special case for Senior Management. Both profits and savings are a primary goal of most companies, and therefore their senior management team. It's not unusual for both metrics to directly impact the bonus structure for senior management. This is due to the common practice of investors viewing the value of the company based on residual income rather than the value of its assets and business (Mäkeläinen, 1998). While both maximizing profits and savings may not be the only or even the best way to measure shareholder value, in many cases they are the only quantifiable metrics used.
- That being said, the **protection of intellectual property** is now being seen more and more as a quantifiable aspect of shareholder value (Halligan, 2005), and as such is ecoming a powerful motivator for senior managers.
- **Regulatory compliance** is very much front-of-mind for anyone in an executive role, no matter what industry is being considered.
- Very much related to regulatory compliance and legal compliance, **avoidance of lawsuits and fines** is a powerful motivator for Senior Executives. This is especially

true in recent times, as Senior Managers may be personally liable for damages under some regulatory frameworks. ("Sarbanes-Oxley Act", 2002)

- **Corporate reputation** is also a potent motivator. No-one wants their company to be "that company" that's in the news for negative reasons, whether it's a product recall, a security breach or a breach of regulations or legal requirements.
- They are of course also driven by **personal financial incentives**, but at this level these are usually directly tied to Shareholder Value metrics (Profit and Loss)

Because of time factors, the "two minutes is too long" rule applies. Keep the message short, catchy, and directly related to their industry. If they can take the message in as a short story that is related to their situation, that often plays extremely well. If math or graphs are required to convey the message, keep these similarly brief. A single simple graph, or math that uses maximum / minimum / average calculations is about as far down the "math path" as they'll want to tread. Always (always always) recheck any facts or figures presented to Senior Managers. When presenting, especially to senior managers, if any of your facts are found to be in error, the damage to your credibility can be a long-term issue.

Manager / Business Unit Leader

As you would expect, Managers have a lot in common with Senior Managers, but with a narrower scope and smaller scale. So, as would be expected, Managers or Business Unit Leaders have similar motivators:

- **Departmental profits** or **departmental savings** are of course important. Every manager or director is responsible for keeping their department operating inside of its budget, and missing a budget metric is a significant down-check at performance appraisal time.
- **Return on investment** of individual projects that are under their department's purview, or that their department has responsibility for, is a key metric. The departmental outlook is centered on survival year to year on the budgets they are allocated. The return on investment of large projects directly impacts this view, and is a clear "attention getter" for any Department Manager.
- **Project Milestone and completion dates** for projects their group has oversight on. This is important only in departments that are primary on any given project. If a department participates in a project, rather than is responsible for the final deliverables, that Department Manager will tend to place their department's daily interests (which they are measured on) ahead of the project outcomes (which they are not measured on).
- **Regulatory compliance** is an increasingly important motivator for Business Unit Leaders, but since they are not personally liable for breaches as Senior Managers are, this is still often ignored at this level of the organization.
- **Compliance with corporate policies** are important, but are just as often consciously ignored if it is perceived that a large departmental profit can be realized as a result.
- Any other performance metric that they are measured on, or that they feel might reflect on their department or on them personally.

Keep in mind that in many organizations, Department Managers have among the least secure jobs in the company. They will frequently have concerns that may seem disproportionate to the issues being discussed and will want more detail than you might expect.

To that end, it's best to lead with a presentation similar to one you'd present to Senior Managers, but have as much detail as possible available in case questions take things down an unexpected path. This isn't a bad idea for Senior Management presentations as well, but supplemental data will be used much more often at the departmental level.

Human Resources

The Human Resources department has a few unique roles in any security awareness effort. They can assist in conveying the message in any campaign that may be planned – in many companies, they may need to approve a campaign before it can be started. In most organizations, Human Resources owns the corporate policies, so any security related policy must fit their template, and be vetted through them for compliance with privacy and other Human Resources related regulations. Finally, Human Resources is best placed for enforcement in the case of any policy violations. Most policies have that "up to and including termination" clause in them, but what generally happens is that IT calls the department manager of the person who has violated the policy, and then, generally nothing happens. If Human Resources is in the loop, quite often they are legally bound to track policy violations and take action on them.

So how do we influence Human Resources when they are faced with decisions in the information security space? Quite simply, make them a full partner in the process, or better yet, make them the lead in the process, with IT acting as a technical advisor.

In our list of motivators, the ones that resonate most with Human Resources include:

- Human Resources is the custodian and often the owner of the policies of the corporation, so **compliance with corporate policies** is one of their primary mandates.
- **Regulatory compliance** as it applies to **privacy issues** and **legal compliance** are always "front of mind" with Human Resources personnel. As they deal with employees, prospective employees and people external to the organization, care needs to be taken that all Human Resources actions stay well inside compliance on all applicable legislation. All too many people are not only quick to criticize but quick to sue if any Human Resources actions are even close to non-compliance.
- To a lesser extent, **Regulatory Compliance** as it applies to the company's business is also important. This motivator is there partly because Human Resources Directors are normally in the senior management team of any company, but mostly because the Legal Counsel or Legal Department of many organizations is part of, employed by or is an offshoot of the Human Resources group.

IT Manager or Director

On the face of things, IT Managers might be included in the Manager / Business Unit Leader category, but they are not well placed there for several reasons. The most obvious difference is that IT Departments are normally cost centers rather than profit centers. The fact that these costs are then used by all departments, presumably to turn a profit for the organization is often lost on Senior Managers. This places some unique pressures on IT Managers and Departments, which translate into a very different set of motivators:

- **Uptime of corporate systems** is of paramount concern, in many cases to the point that immediate notification of service interruptions and daily reports and statistics are required by IT Managers.
- As a Cost Center, **departmental savings** are important in IT Departments. When considering a project or product, a keen eye is cast on whether it should be pursued at all, especially if proceeding might duplicate an existing tool or permit retiring of an old tool.
- **Return on investment** of Individual Projects is also central in many decisions within IT departments. This is again driven by the fact that IT Departments are cost centers, and so are tied much closer to the expenditure side of the Accounting Department than other groups. In contrast to manufacturing for instance, IT departments generally calculate depreciation on much shorter windows than other groups (2-3 years instead of 7-10 for instance).
- **Limited resources** also play an important factor in IT decisions. There are only so many programmers, Business Analysts, System Administrators and so on that can be applied to the collective project mix within any IT group. This means that opportunity costs are an important aspect of any costing decision. For instance, "if 'Project A' proceeds, how does this affect the schedule of 'Project B', and does that mean we don't have developers available for 'Project C' this quarter" would be a common conversation within any IT group. The project driven, resource constrained nature of IT is then weighed against the ongoing support requirements of existing systems when any new project or action is being considered. Phrasing a security message in a way that a decision action can serve multiple purposes, save resources or be addressed using automation makes good sense when trying to sway an IT manager.
- **Regulatory and legal compliance** is of course critical in IT Departments, but is oddly often ignored until very late in any individual project. While IT ~~is~~ frequently has some responsibility for delivering and auditing for compliance, it's still common to see attempts to "bolt it on" at the end of a project. For instance, applications that

clearly aren't written with security or compliance in mind are often front-ended with an application firewall at the tail end of the project. Messages that involve compliance will generally be well received, but it's important to emphasize that compliance needs to be considered at the beginning of a project, during the design and product selection phases, as opposed to "when there's time for it."

- Many Corporate Policies are authored by the IT Department, and IT is often left with the task of technical auditing and enforcement of these policies. For these reasons, **compliance with corporate policies** is generally considered an important factor in many IT decisions.

These factors combine in the security area, and often result in a set of decision metrics that will very likely sound familiar to the reader:

- Automated, pre-packaged tools are significantly preferred over applications that require significant configuration effort or ongoing support
- Tools that demonstrate Regulatory Compliance are often preferred over tools that focus on a more complete vision of security.
- Tools that can demonstrate a positive impact on uptime or a clear savings are almost always approved in advance of applications that have less quantifiable benefits.
- Because of the service-oriented nature of IT, any tool that can be tied directly to corporate profit or enhanced services will receive preference, especially if it can be financed partially or fully by other groups.

Developer or Business Analyst

Within any IT Department, Developers or Business Analysts are the people trusted to translate a corporate requirement stated in business terms to a technical solution delivered to the user community. They have the most frequent direct contact with other departments, and often have more credibility with core business departments than the IT Director or Manager. They are viewed more as a partner of the Business Unit than as an IT member, and so are perceived to be more at the "profit center" end of the spectrum, as opposed to the traditional IT "cost center" posture. These factors make them an important target audience for any security message.

The job of Business Analyst is less of a job than a series of linked, generally related projects and associated resources. Phrasing security messages in terms of these projects is a powerful way to get the message across. It also means that the message is most effective if both the project management methodology and specific projects are taken into account:

- **Project Dates and Project** Costs involve personal and departmental commitments that are key metrics for Business Analysts. To that end, any security message needs to be injected into the project as early as possible. Coming to a Developer or Business Analyst halfway through a project with a new security project may involve significant rework, impacting both the project costs and schedule. Coming "Late to the Party" with security may simply mean that the security requirement will be ignored, or perhaps treated as a separate project that will need to be approved on its own merits. It's much easier and cheaper to get any security issues into the project plan while initial requirements are being defined, so that these issues and tasks are embedded into the initial schedule and budget estimates and are simply carried with the rest of the project.
- Similarly, Business Analysts and Developers frequently propose new projects, so **Project Acceptance** becomes a metric that they become invested in. Project Acceptance is seen both at the beginning of a project, when the aims, schedule and budget of a project are approved, and also at the end of each phase, when the milestones or final project deliverables are approved. Security solutions that help this process along will be preferred over those that hinder acceptance. For instance, adding too many or awkward security tasks into a business process impact overall acceptance of the process or affected projects. It's much better to have one simple, effective task as opposed to several tasks. For instance, a two factor authentication solution can often be made more attractive if it can be applied to multiple systems, reducing the number of overall passwords that end users see.

- As in any project management role, **uptime of the personal workstation** is critical. Access to the project schedule and email is an absolute requirement for anyone in a project role. Access to the development tools are an absolute requirement for anyone developing actual source code or systems. Interruption to either has a direct impact on the job, the equivalent of locking up the brakes on a loaded semi tractor-trailer, and just as attention getting. Any security message that involves personal workstation uptime should get immediate attention from anyone in this job role.

Helpdesk

The Helpdesk is an important target audience for any security professional – they are the eyes and ears of security, often beating automated tools to the punch if they're onboard with security goals and looking for the right things. There are several motivators that "steer" people in a helpdesk role:

- **Uptime of corporate systems** is of course paramount – this is one of the key metrics that people in this group are measured against. Anything that positively affects uptime without adding significant effort will have the helpdesk onside.
- Minimizing the effort of any security related tasks is also important. People in the Helpdesk role are measured on call volumes and how quickly calls are resolved. Anything that takes away from this effort impacts the metrics that they are evaluated on, and so won't be well received.
- **Compliance with corporate policies** is also important – the Helpdesk is the "eyes and ears" for these efforts as well, so they'll be open to helping with creation, communication or enforcement of these policies. In contrast, Policies imposed on them without involvement will generally be met with resistance.
- **Personal financial incentives** will also be well received, but are a challenge to implement for Helpdesk personnel. From a management perspective, any positive security behavior that might be targeted will simply be viewed as a part of the core job responsibilities. The most common personal financial incentive seen by the helpdesk is overtime, and more overtime simply isn't popular. However, if a personal financial incentive can be tied to a new security metric, it will almost always be well received.

Oddly enough, uptime of the personal workstation is not a key factor for Helpdesk personnel. It appears that (as long as there isn't an IT crisis) if the Helpdesk workstation is down, it's viewed as a welcome break, and fixing it is a nice distraction from resetting passwords and other common Helpdesk tasks.

Engineer

Similar to Business Analysts, Engineers are driven by projects. The main difference is that Engineering projects are firmly on the profit center side of things – they are involved in developing the actual products that the company manufactures or sells. This means that they have a very simple, short list of motivators. They will often view anything (like security for instance) that impacts these motivators negatively as either an adversary or something to be ignored.

Getting engineers to take Security Awareness seriously is an important goal, as this will embed security awareness into the products that the organization offers its customers.

Things that will motivate an engineer are:

- **Protection of Intellectual Property** – at the root of things, it is an Engineer's responsibility to create new thoughts, methods and products. Protection of these is near and dear to their hearts, and any message that speaks to this should get immediate attention
- Engineers are almost always involved in projects, with the project deliverables as their main day-to-day responsibility. Anything that affects a project deliverable will receive similar attention. **Anything that helps to advance a project date or simplifies a task** will be favored over something that impedes a date or complicates their job. This should always be considered when phrasing security concerns with engineers.
- Similarly, **anything that enhances a product or deliverable quality** or features will be favored. This is something that is often overlooked by security professionals. Gaining knowledge of the company product, of course without violating confidentiality requirements, can be a powerful tool. If a suggestion improves security of a company product and provides some advantage over a competitor's product or process, it's a clear win.
- The project-driven nature of the Engineer's job means that **Personal workstation uptime** is paramount. If their station is down, it almost always means that they simply cannot work.

Engineers are almost always given significant autonomy within an organization. They often take this as permission to circumvent policies and rules in order to achieve their goals. Not only that, they will almost always be backed up by management when push comes to shove in this regard. Trying to impose rules on engineers is not like herding cats, it's like herding hostile tigers. It's much better to motivate them by helping them with things they need, rather than trying to impose rules or bounds on their actions.

Graphic Artist

Being project driven, Graphic Artists are similar in motivation to an Engineer or Business Analyst. Unless they are directly involved in project design, they usually have a much smaller power-base.

Graphic Artists are in charge of properly interpreting and delivering key messages to identified target audiences, so in this respect have a similar responsibility as that aspect of a security professional's job. This makes them a good ally to enlist; they can often help in suggesting approaches or assist in creating graphics materials.

They are still, however, part of the user community, and in many cases they'll need to be convinced that one thing or another is an issue based on security concerns. Key motivators for Graphic Artists include:

- Similar to Business Analysts, Developers and Engineers, Graphic Artists are Project Oriented. Anything that affects **project delivery dates** or q**uality of the project deliverables** will be of immediate concern. As Graphic Artists are often independent contractors, these may be of even more concern, as missing on either of these metrics might mean a direct effect on their bottom line.
- If the Graphic Artist is an independent contractor, they may not be dependent on corporate systems at all. However, **Personal workstation downtime** is a powerful motivator, whether they are in-house employees or contractors. If their workstation is down, in many cases they simply cannot work. Not only that, but they often have specialized hardware (monitors, printers and the like), such that they may not be able to use just any other workstation without degradation of their results.
- **Confidentiality of the material currently being worked** on is an important factor for Graphic Artists. As products or advertising campaigns are built, Graphic Artists will have confidential information, either on product capabilities, advertising content or critical business timelines, which they must keep confidential.
- **Confidentiality of the material from past projects** is also important. Even after graphics are delivered, in many cases the material used during creation might have a "Confidential Until" timestamp associated with it, or in some cases might simply be classed as Confidential.

Salespeople

Salespeople are a group unto themselves, and have a completely different set of motivations than anyone else in most organizations. In almost all cases, salespeople are driven by short and medium term sales goals, which often drive personal financial incentives in the form of commission. This makes for some very specific motivators:

- As discussed, **personal financial incentives** in the form of commissions are what drives all other motivators for salespeople – everything is measured by how it affects their personal bottom line.
- **Personal workstation uptime** plays a large part in this. Without a workstation, salespeople cannot work, proposals can't be written, and products can't be costed. If access to email and calendaring is impeded in any way, salespeople will not have access to important client information, and will risk missing customer appointments.
- **Corporate system uptime** can be important, but is not always critical. Salespeople often need access to CRM (Customer Relationship Management) or other central systems in order to access customer contact information, file proposals, enter orders or forecast overall sales volumes. If this is the case, anything that impacts uptime or access to these systems can be important.
- **Corporate reputation** is of course important to everyone on the sales side of any organization. Not only are they selling products, they are often selling the organization as well. If the company is under lawsuit or is seeing bad press for any reason, it almost always immediately impacts product sales.

Phrasing security messages in these terms will gain a receptive ear in sales, and will also gain some cooperation and positive changes in behavior. However security messages to sales organizations need to be a long-term strategy. The short-term nature of the job tends to dictate that people with short-term goals are hired to fill the positions. Also, it's common to see a fair degree of turnover in sales groups. For both of these reasons, security messages to sales groups need to be continuous or on a shorter cycle than for many other groups.

Shop Floor / Manufacturing

Organizations involved in manufacturing will often split their company neatly down the middle, between "office" and "shop". This creates a real problem for security professionals, as in a lot of ways they are now faced with communicating their message to what is now two very different organizations under one corporate banner. The concentration in this paper so far has been on traditional "white collar" job descriptions, but the discussion would not be complete without discussing manufacturing roles.

The main motivators that can be used to influence behavior in the security arena in a shop floor or manufacturing setting include:

- **Compliance with Corporate Policies** works very well to convey the message or influence behaviors. In effect, this makes the security behavior part of the employment agreement. In a union setting, the wording in the corporate policies will need to be extended to any collective agreement that is in place for this to be effective.
- **Corporate reputation** has a surprisingly large impact in almost any message you need to convey in a manufacturing setting. Esprit de corps has a large influence in almost every manufacturing environment that was surveyed or interviewed for this paper. If the people doing the work believe in the company, the quality of the work improves, and security messages are easily discussed in collaborative fashion.
- **Personal financial incentives** have a long tradition in manufacturing settings. Existing Continuous Improvement programs such as Six Sigma can be used or emulated to get the desired results. For instance, rather than dictate a desired behavior, discuss the desired results, and have your audience suggest the best ways to get there. The solutions that are adopted are rewarded with recognition within the company, and a cash award commensurate with the results (often expressed as a percentage of savings or productivity gain).

There are many approaches that don't work in manufacturing environments:

- One-off or limited time security tasks end up being viewed as a "flavor of the month" fad, and will quite rightly be ignored.
- Security tasks that take time away from productive work are also generally ignored. People in production environments are rewarded based on production metrics, and any task that detracts from these metrics will be viewed as a bad idea.
- As in all situations, security tasks and processes must have an obvious perceived value, it must be immediately seen what the benefit to the organization is, or the task or process will be ignored. In manufacturing, it's likely that the task or process

will be ignored in a more “colorful” way, but the end result is the same no matter what the audience.

Support Staff

Quite often when a security message is formulated, the key audiences that have been discussed are not the audiences before us. In some cases, our audience may have different motivators due to their industry, or they may be in a critical department that we have not considered in this paper. It's not a good plan to treat everyone else as the "everyone else department". However, in most cases the motivators below will be in play to one extent or another:

- **Compliance with corporate policies** should almost always be a consideration. Policies are part of what defines the corporate culture, and should almost always be part of the equation.
- **Corporate reputation** should matter to everyone, as the success of the company almost always hinges on this reputation. Corporate reputation also has a large impact on morale, and morale within a company will influence how well people do their jobs (and how compliant they are with their own policies.)
- The survey results (Appendix A) indicate that almost every group has a large interest in **regulatory compliance**. This may or may not be the case, but it should be on everyone's radar, especially if they handle data that is of a personal or financial nature.
- **Personal financial incentives** can be a powerful tool – at one end of the spectrum, stock options based on corporate performance will influence behaviors, but simple contests with small prizes can work amazingly well also.
- **Uptime of personal workstations** and **uptime of corporate systems** are both very powerful motivators. The proverb that "the only thing people hate worse than working is not being able to work" is a very true one. While availability of all systems is never worth mentioning, interruption of service seems to rank somewhere above most natural disasters. Discussing security decisions in terms of preventing interruptions is often very effective.
- Working security compliance into the job requirements can be a powerful tool. If people are evaluated based on their security behaviors, it will certainly pay off.

Things to watch out for:

- One-off or limited time security tasks almost never work. Anything that smacks of "flavor of the week" will generally be immediately dismissed.
- Security tasks must have perceived value. It must be obvious to the people involved how any action will positively affect them, their job or their company in order for it to be taken seriously.

Conclusion

Influencing people to make that right choice in security doesn't seem to be much different than trying to get them to make the right choice in any other matter – people in different roles need different messages to get to the same decision.

The interesting thing about the survey results is the overwhelming emphasis on regulatory compliance. While regulatory compliance is very important to security professionals and many of the audiences typical in most companies, this particular metric seemed to be rated slightly higher than in interview situations with people in the positions being discussed. Aside from this anomaly, the survey and interviews tended to agree on most points.

This paper may seem to describe how to "social engineer" various people in an organization into making decisions that they might not make otherwise. In fact, this is exactly the goal of this paper. Security professionals, either as full time employees in an organization or as consultants, face this challenge daily as part of their core responsibility.

Appendix A: Survey Results - Evaluation of Security Awareness Motivators

This appendix represents the raw data from the “Security Awareness” survey:

Making a Difference in Security Awareness - Different Methods for Different People
In this survey, we're hoping to find different motivators that can be used to influence different people towards greater security awareness, and more importantly, make a positive impact on decisions and behaviors in the security arena. Please indicate below which motivators you have used successfully, or that you have seen used successfully to make such an impact.

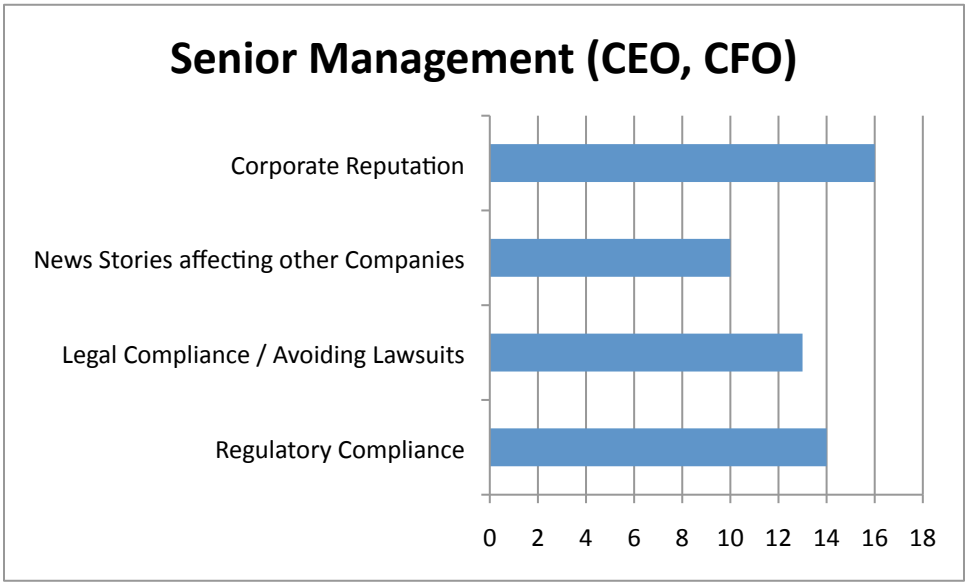
Based on Job Description, how have you personally been able to raise Awareness of Security Issues and motivate change in your organization or in customer organizations? Please indicate in the most successful ones you've seen - multiple picks per row are acceptable, but please don't pick too many, just the "best" ones.

This table represents both the survey questions and the results, expressed in percentages.

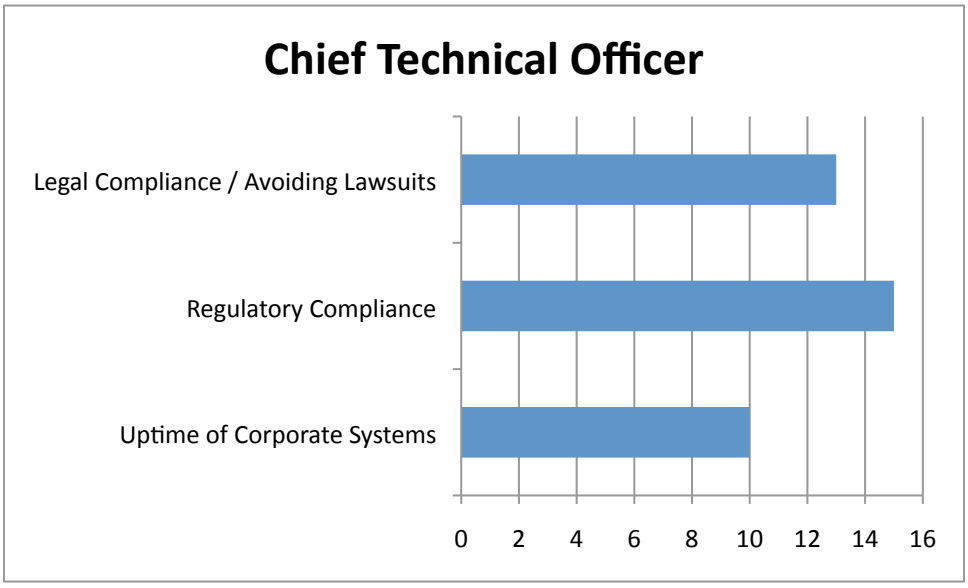
	Corporate Profit	Department Profit	Personal Financial Incentives	Corporate or Department Savings	Return on Investment	Uptime of Corporate Systems	Uptime of Personal Laptop or Workstation	Protection of Intellectual Property	Protection of Credentials or Passwords	Protection from Identity Theft	Other Privacy Issues	Regulatory Compliance	Legal Compliance / Avoiding Lawsuits	Corporate Policy Compliance	News Stories affecting other Companies	Corporate Reputation
Senior Management (CEO, CFO)	2	0	0	4	2	7	1	8	2	6	2	14	13	8	10	16
Chief Technical Officer	0	0	0	5	4	10	5	6	2	7	4	15	13	9	8	6
IT Manager	0	0	0	5	2	17	10	4	7	7	4	12	5	8	5	5
Software Developer or IT Business Analyst	1	2	1	1	3	9	7	10	12	7	3	12	4	7	8	7
IT Operations or Helpdesk Personnel	1	0	0	2	1	14	13	3	11	12	5	7	2	7	9	3
Business Unit Manager	1	7	3	7	3	10	11	3	4	5	1	11	8	11	6	4
Accountant	8	0	1	6	8	4	8	3	6	9	0	14	9	6	8	4
Salesperson	2	0	4	0	1	10	20	2	4	10	5	5	1	7	13	10
Engineer	1	1	1	1	4	12	9	7	8	7	6	10	6	10	7	3
Human Resources	2	1	0	3	1	5	8	3	5	8	6	15	10	16	6	4
Manufacturing Line Personnel	0	0	0	3	0	11	15	0	3	11	7	11	3	7	15	7
Graphic Artist	0	3	0	0	0	6	13	6	6	10	3	13	3	6	20	3
Call Center Operator	0	0	1	0	1	9	17	0	5	11	5	9	7	11	13	3
Front Desk Reception / Office Manager	0	0	1	0	0	7	13	1	4	12	7	12	10	12	12	3
Office Support Staff	0	1	2	1	1	7	14	2	8	11	8	8	7	11	8	1

The graphics that follow represent the survey results. To simplify the results, only motivators that indicate a greater than 10% selection are graphed.

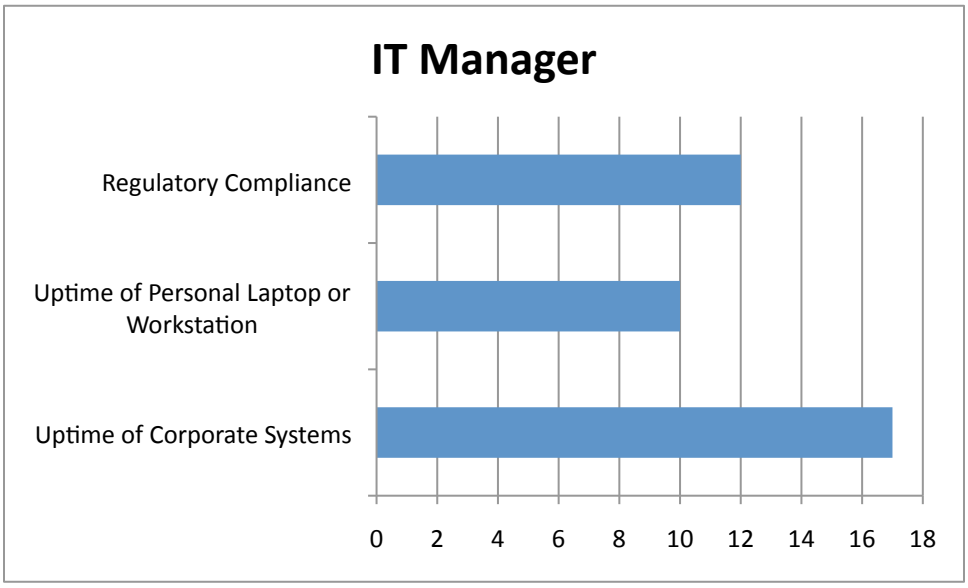
Senior Management (CEO, CFO)



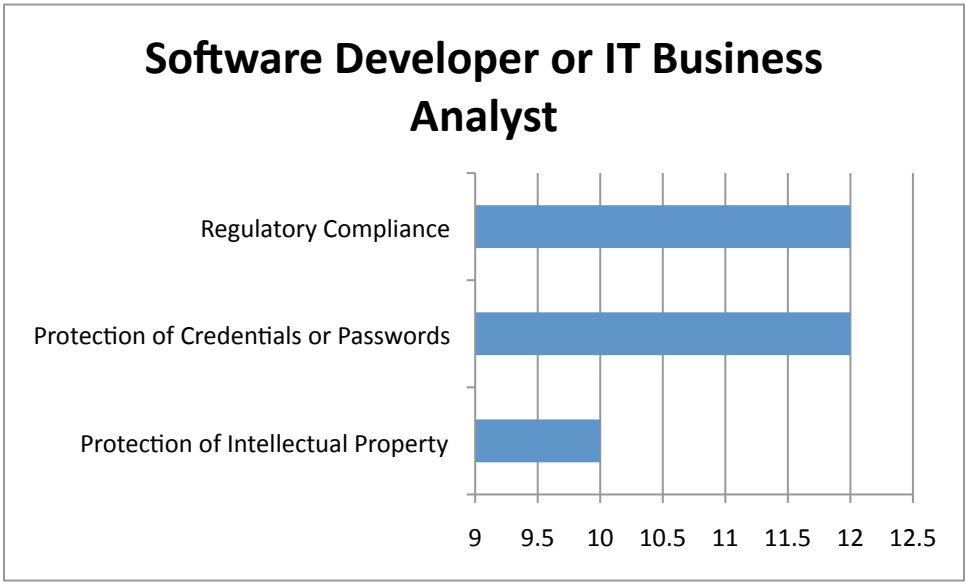
Chief Technical Officer



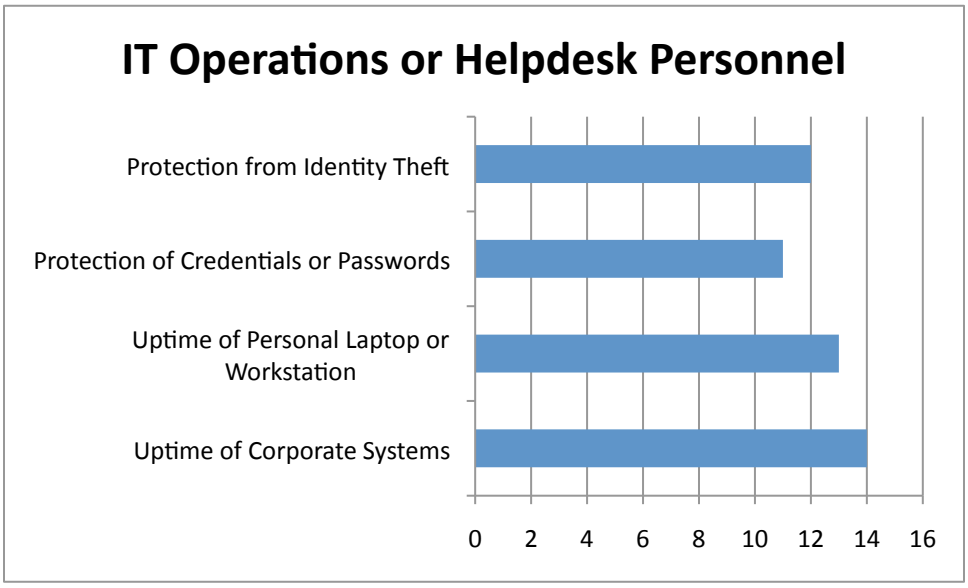
IT Manager / IT Director



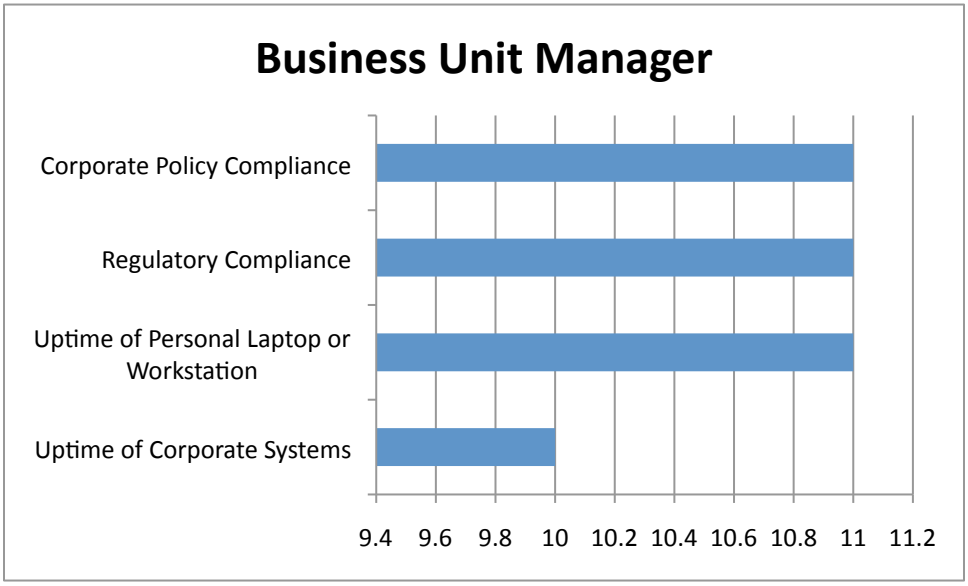
Software Developer or IT Business Analyst



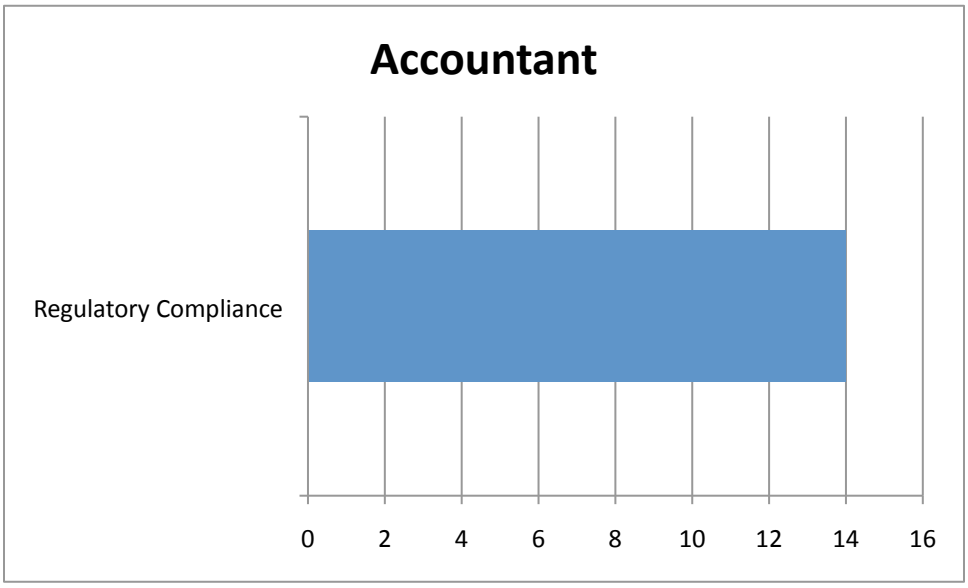
IT Operations or Helpdesk Personnel



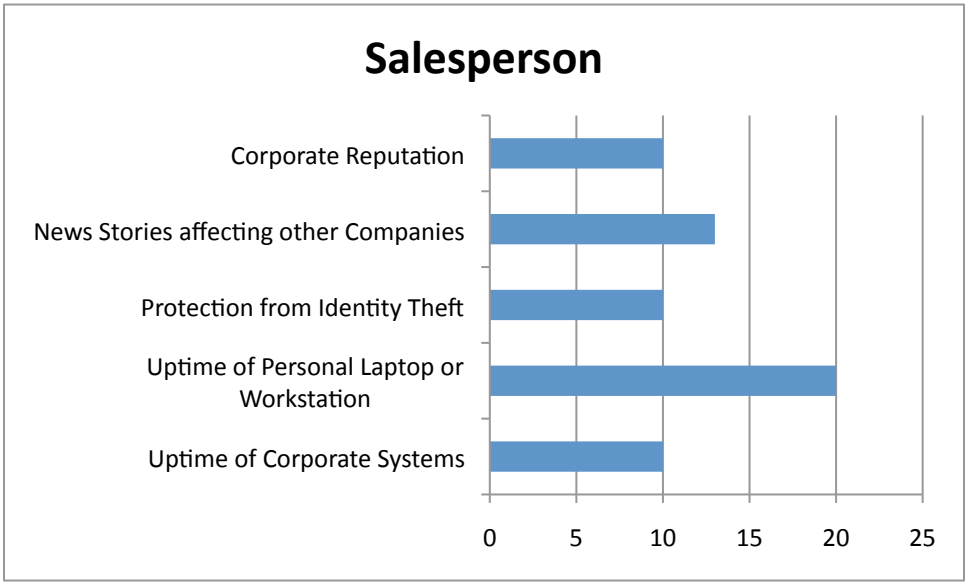
Business Unit Manager



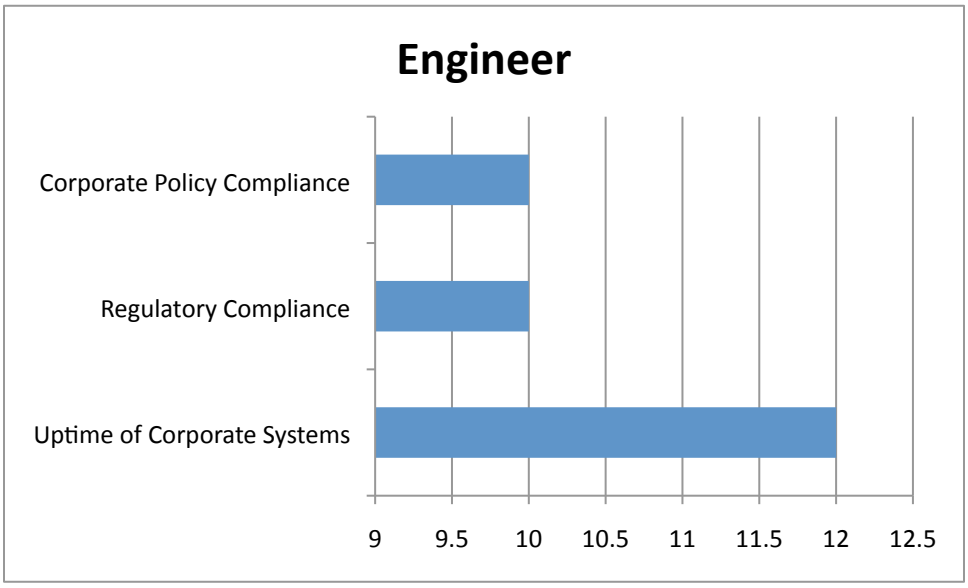
Accountant



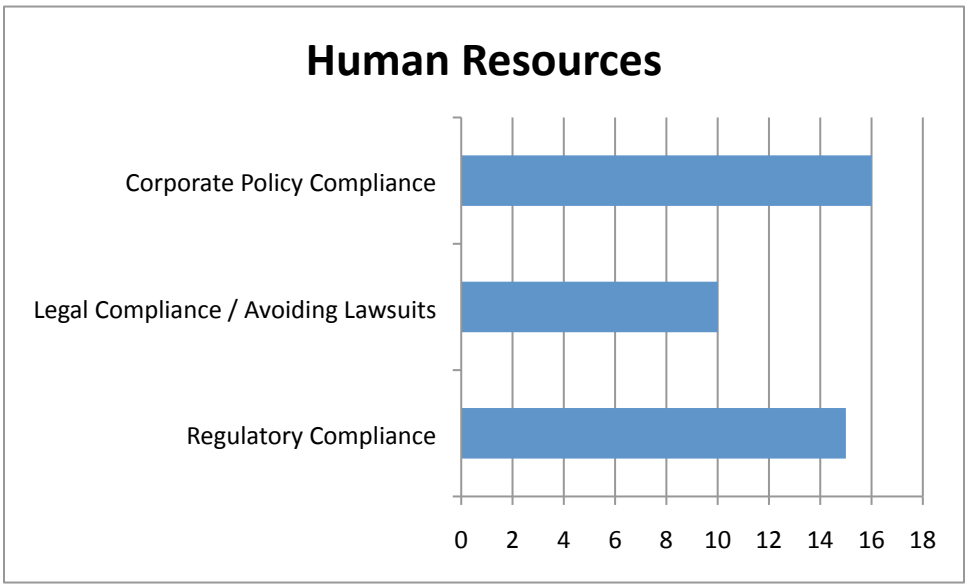
Salesperson



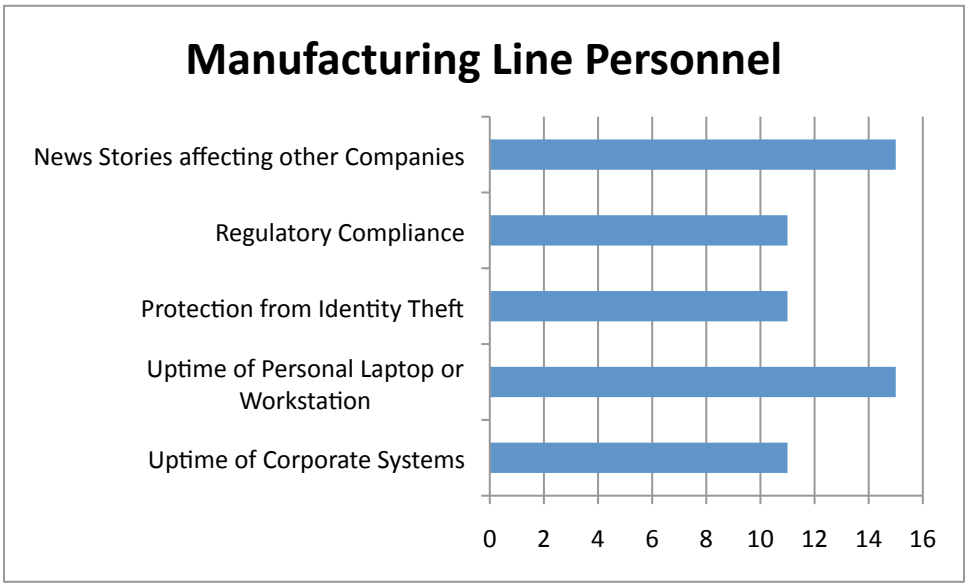
Engineer



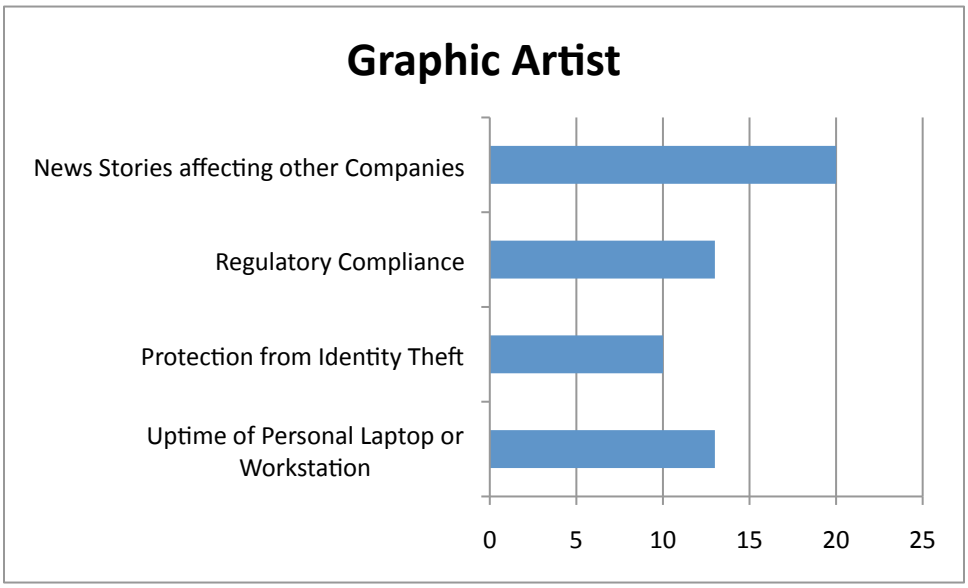
Human Resources



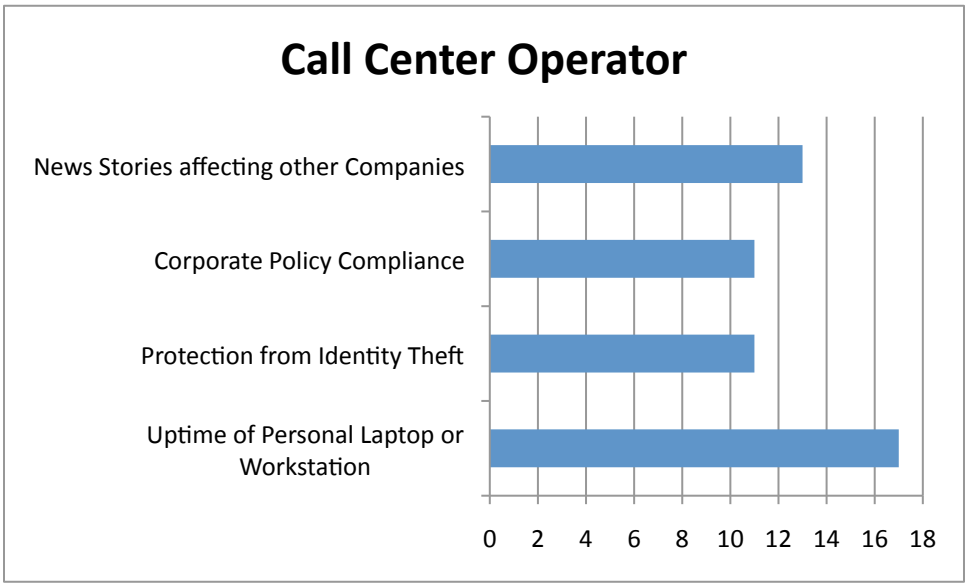
Manufacturing Line Personnel



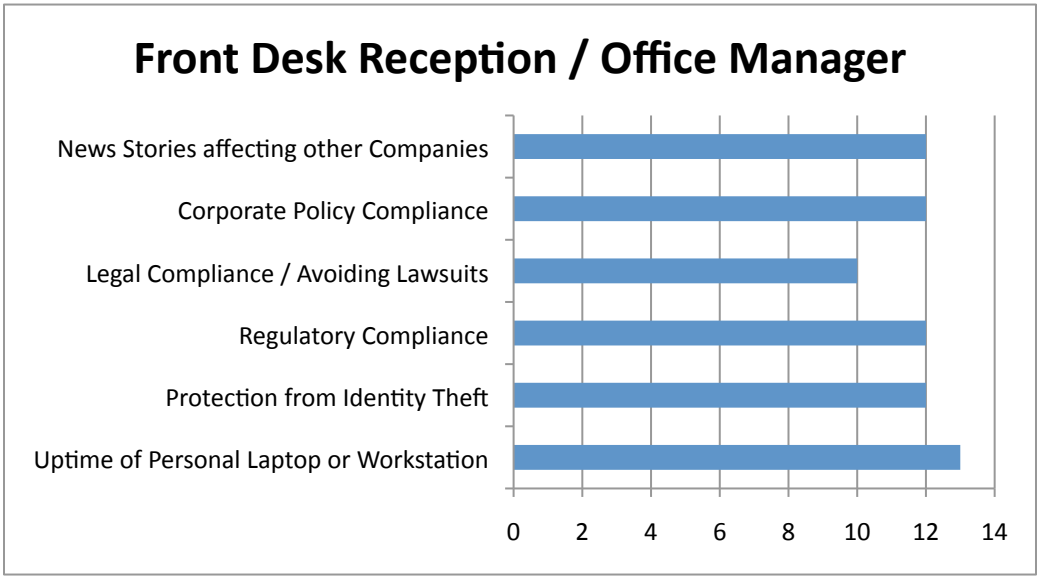
Graphic Artist



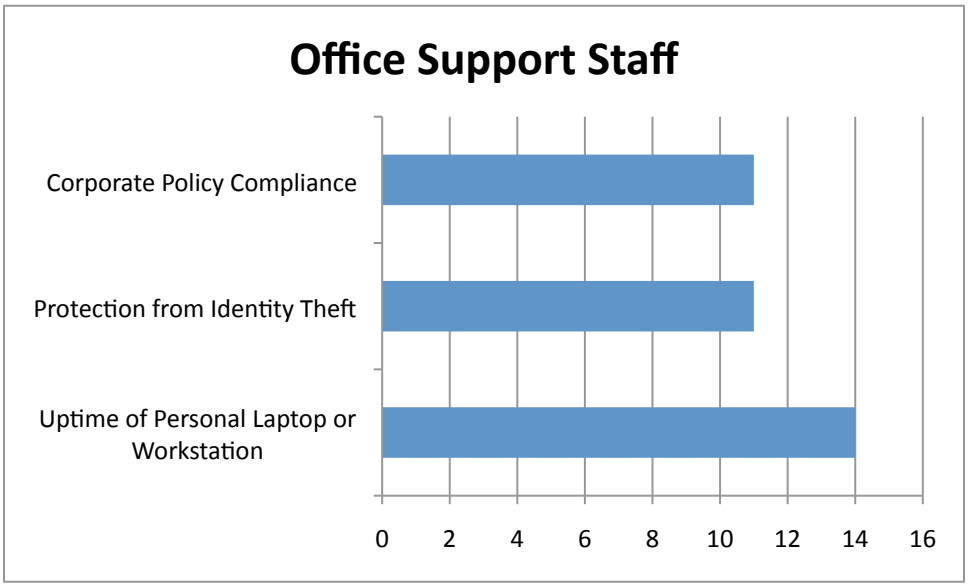
Call Center Operator



Front Desk Reception / Office Manager



Office Support Staff



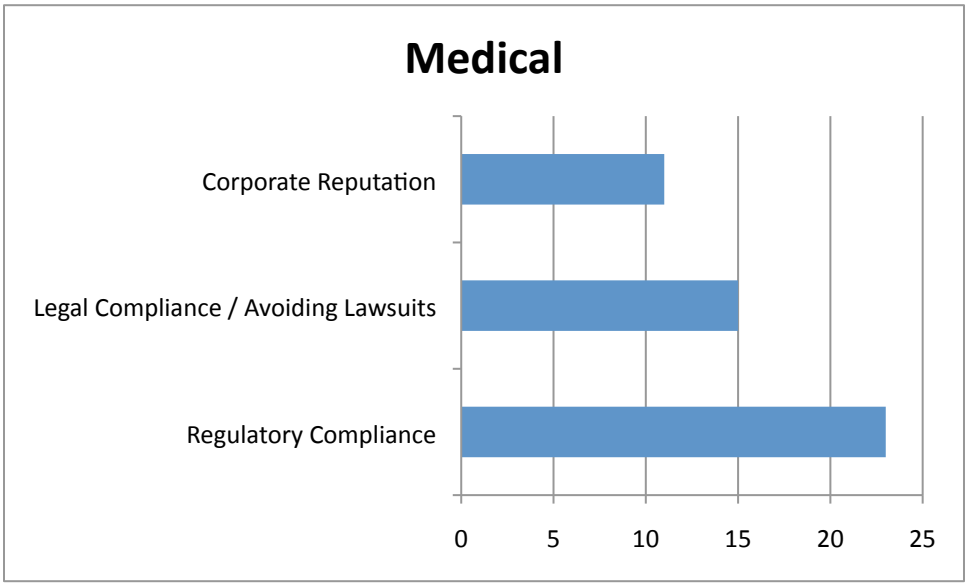
By Industry Sector

Based on Type of Organization, how have you personally been able to raise Awareness of Security Issues and motivate change in your organization in or customer organizations? Please indicate in the most successful ones you've seen - multiple picks per row are acceptable, but please don't pick too many, just the "best" ones.

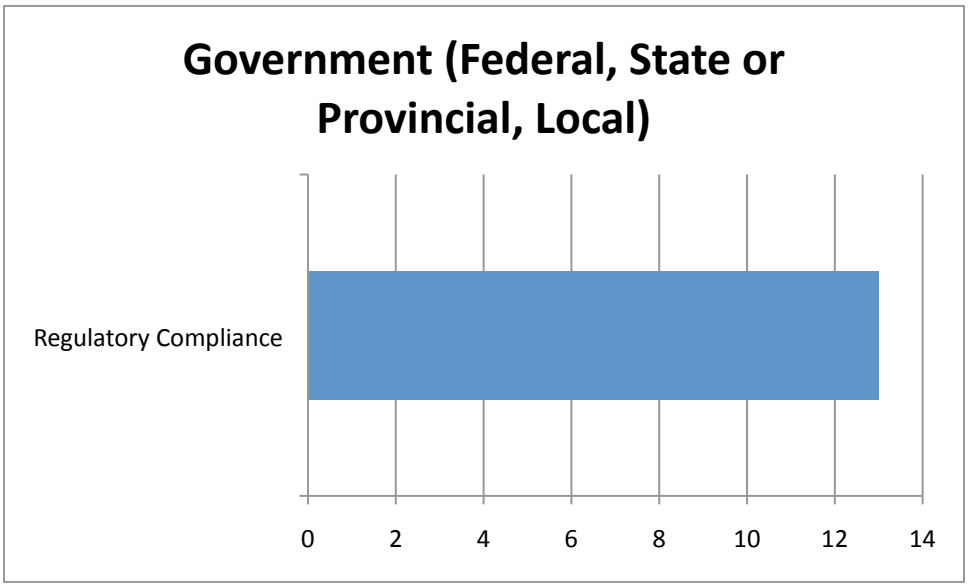
	Corporate Profit	Department Profit	Personal Financial Incentives	Corporate or Department Savings	Return on Investment	Uptime of Corporate Systems	Uptime of Personal Laptop or Workstation	Protection of Intellectual Property	Protection of Credentials or Passwords	Protection from Identity Theft	Other Privacy Issues	Regulatory Compliance	Legal Compliance / Avoiding Lawsuits	Corporate Policy Compliance	News Stories affecting other Companies	Corporate Reputation
Medical	0	0	0	0	1	7	1	0	3	7	9	23	15	7	9	11
Government (Federal, State or Provincial, Local)	4	1	0	3	4	7	5	2	9	7	9	13	7	9	8	8
Financial (Insurance / Banking)	2	0	0	0	0	5	2	4	5	9	8	22	9	9	6	12
Law Enforcement	0	0	0	0	0	0	0	7	7	16	7	16	16	7	7	12
Emergency Response	0	0	0	7	0	15	0	0	7	15	7	15	15	15	0	0
Educational Institutions	0	0	0	0	3	11	9	9	9	10	9	7	6	5	7	9
Entertainment	0	0	0	25	25	0	0	12	12	12	0	0	0	0	0	12
Food Service	0	0	0	16	16	0	0	16	16	16	0	0	16	0	0	0
Transportation or Distribution	0	0	0	0	6	13	6	0	0	13	6	13	13	6	6	13
Manufacturing	2	2	0	5	5	10	10	10	7	7	10	5	7	7	2	5
Resources and Mining	0	0	0	0	0	0	0	0	0	50	0	0	50	0	0	0
Legal	0	0	0	0	0	15	0	7	0	23	7	15	23	0	0	7
Retail	0	4	0	4	0	8	4	0	8	8	0	8	12	12	12	16
Technology	2	1	0	2	4	15	7	15	10	8	4	10	7	2	1	5

The graphics that follow represent the survey results. To simplify the results, only motivators that indicate a greater than 10% selection are graphed.

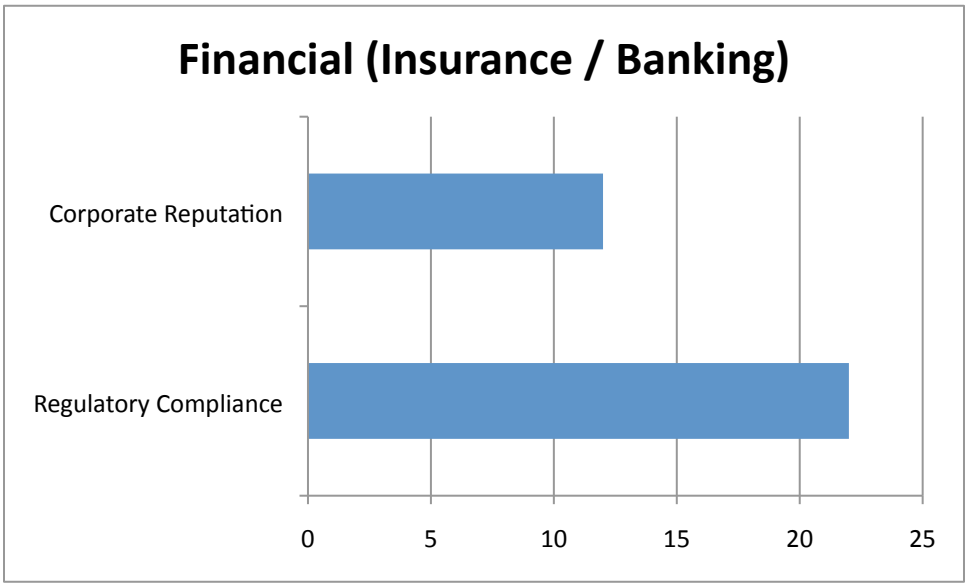
Medical



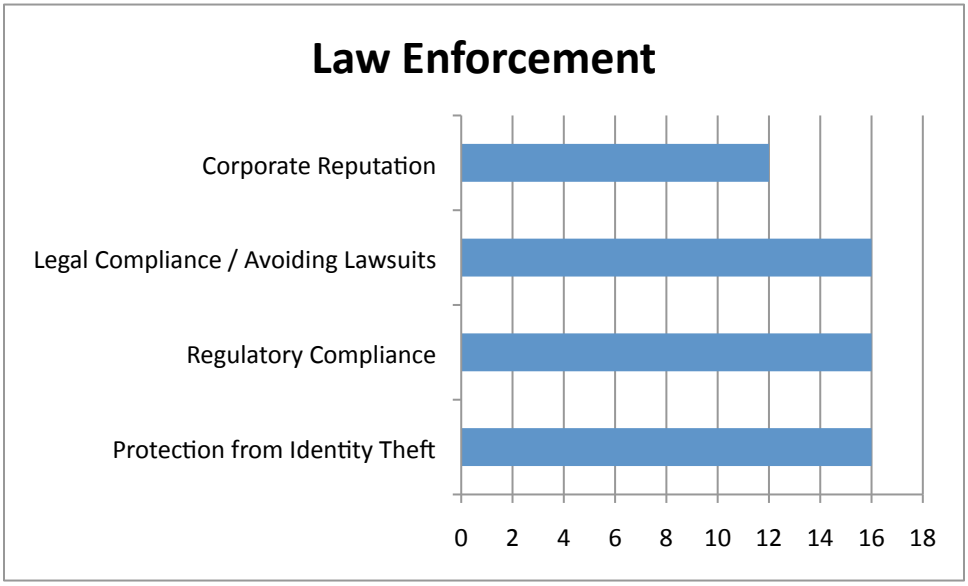
Government (Federal, State or Provincial, Local)



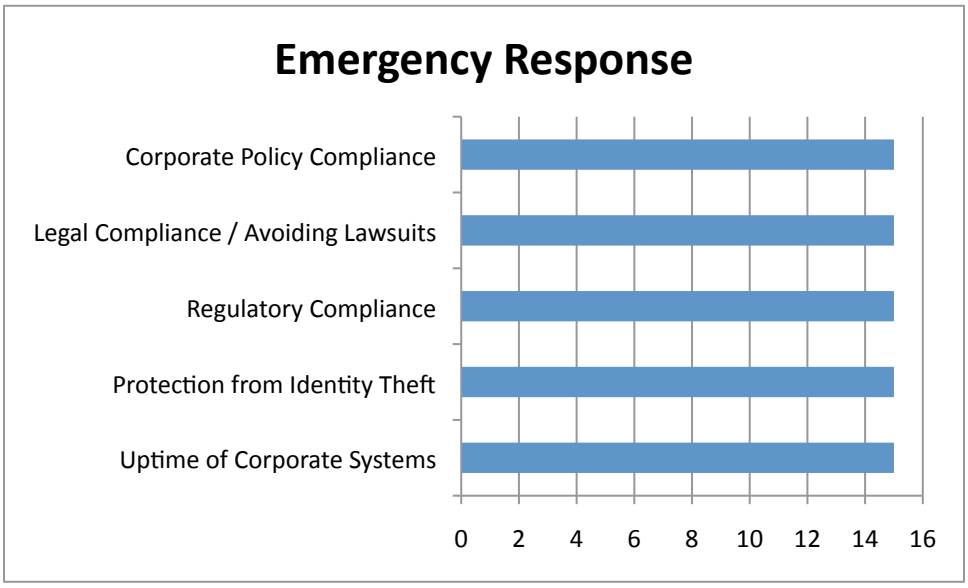
Financial (Insurance / Banking)



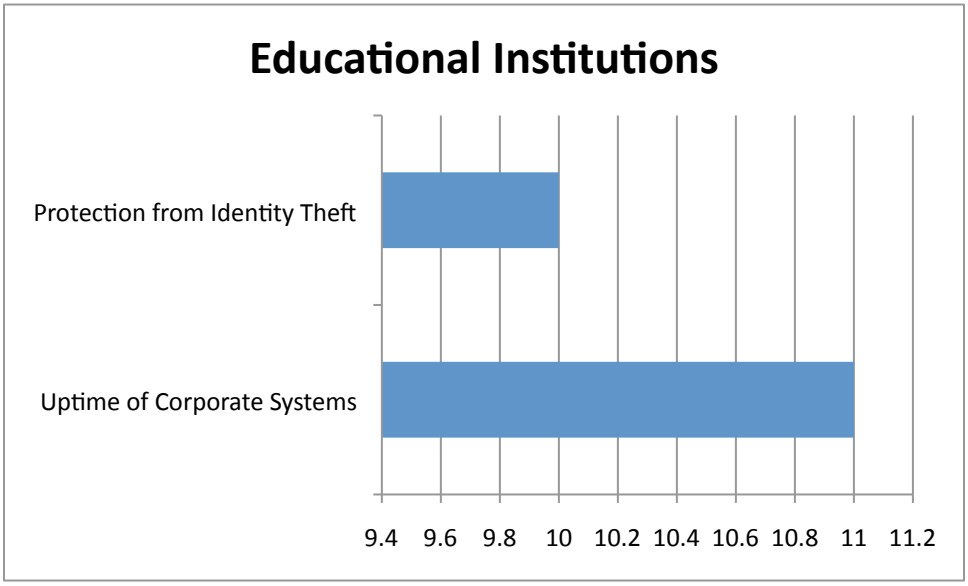
Law Enforcement



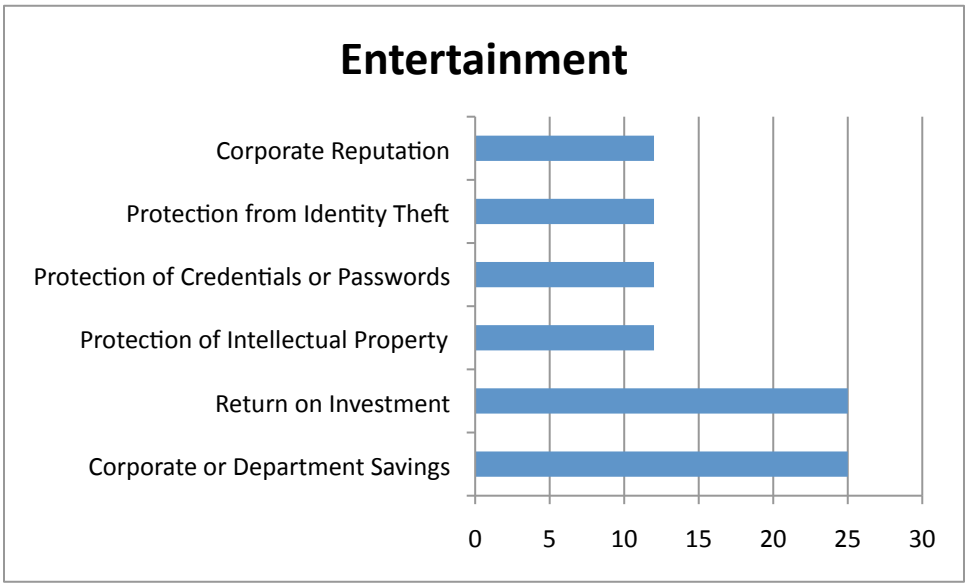
Emergency Response



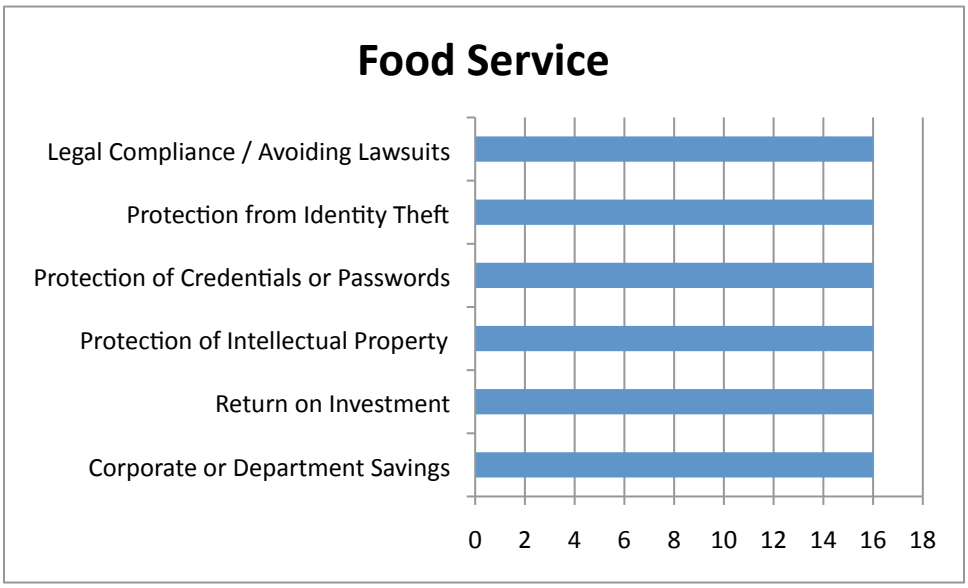
Educational Institutions



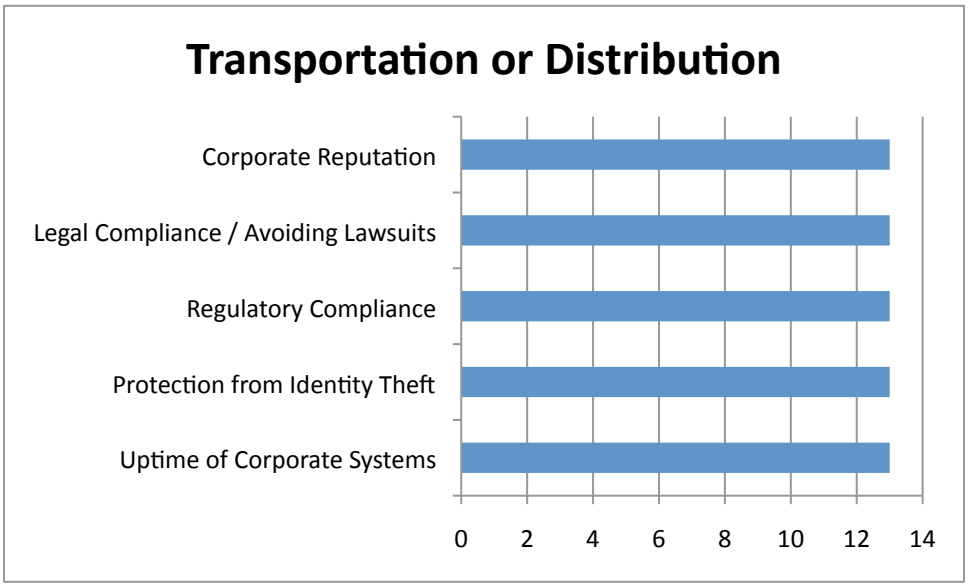
Entertainment



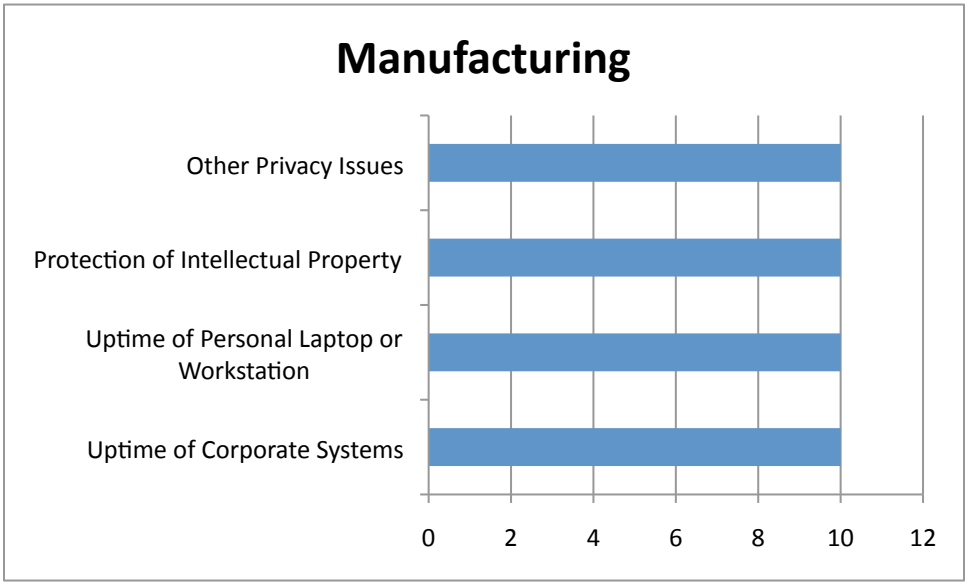
Food Service



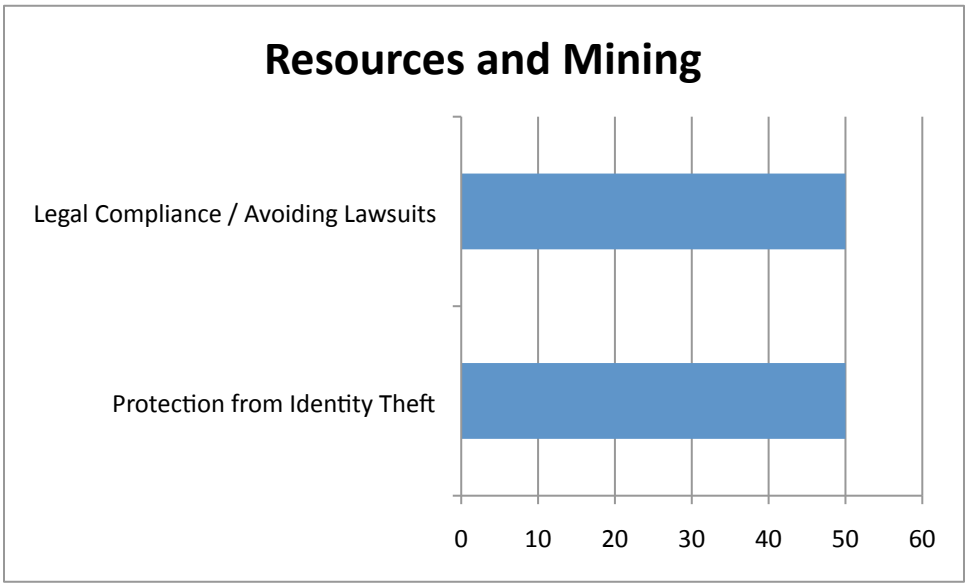
Transportation or Distribution



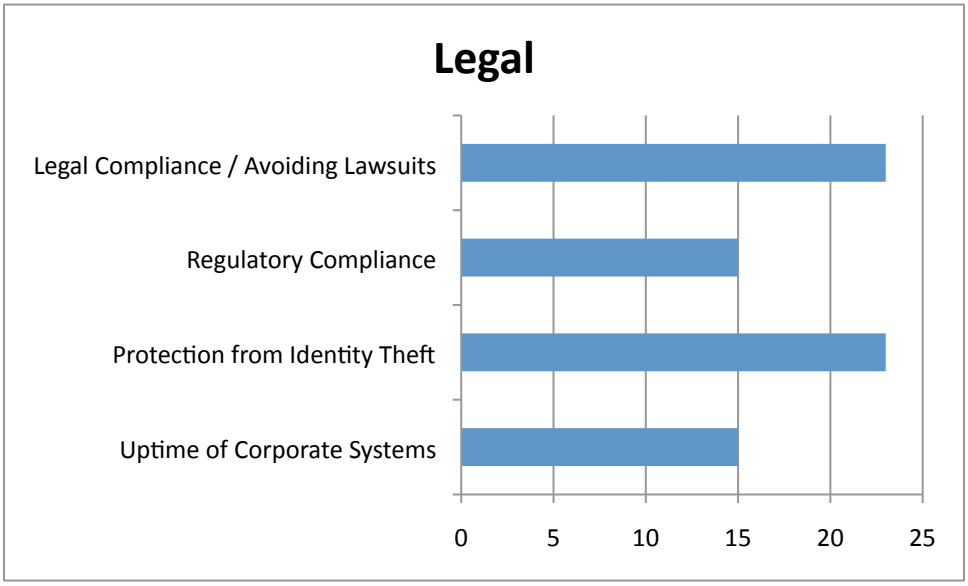
Manufacturing



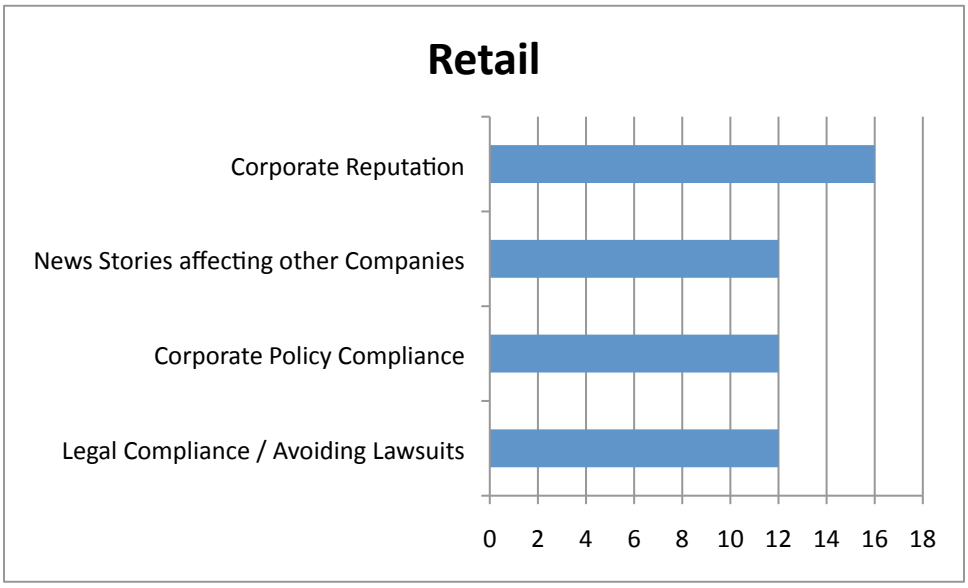
Resources and Mining



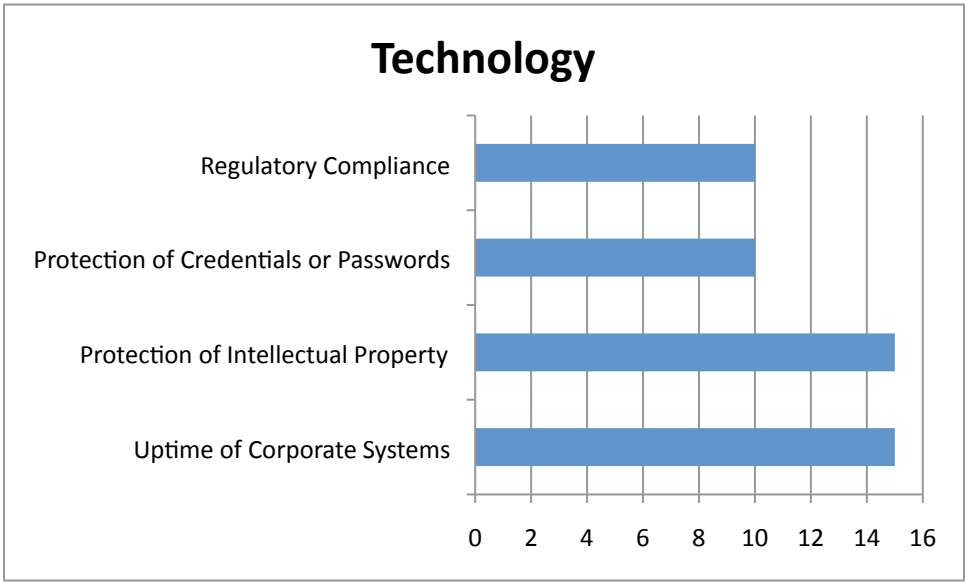
Legal



Retail



Technology



References

Halligan, R.M. (2005). Duty to Identify, Protect Trade Secrets has Arisen: Ssarbanes-Oxley Requires Internal Controls Over How They are Valued.. *The National Law Journal*, *27*(52), 53.

Mäkeläinen, E. (1998, Feburary 9). *"Economic Value Added as a Mmanagement Tool" , Helsinki School of Economics, Finland*. Retrieved from http://www.evanomics.com/evastudy/evastudy.shtml

Sarbanes Oxley Act of 2002. (2002). Retrieved from http://uscode.house.gov/download/pls/15C98.txt