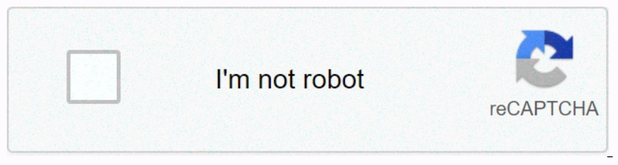

Continue

Internal vs external motivation

A PR audit is an internal process in which business leaders, often in cooperation with a PR firm, review opportunities to communicate and potential threats to the organization's reputation. In carrying out a public relations audit, the entity must take into account both internal factors and possible circumstances beyond the company's control. A PR audit examines both opportunities and potential threats to the company and its image. An analysis of internal opportunities is used to identify strengths and opportunities for promotion that contribute to the development of a proactive strategy. In this step, the company prepares messages and sets media plans to get the word out about brand or product strengths. Free PR opportunities are reviewed in connection with paid marketing strategies. The key is to present a unified, consistent image of your brand. The other half of the internal audit ing is the consideration of fire or product vulnerabilities. It is the weaknesses of your business or potentially controversial issues that may arise. Recognizing these in advance allows for their inclusion in the formulation of a reactive PR strategy, including planned methods and messages of response when competitors, media or the public brings up any of your vulnerabilities. External threats are typically a bigger challenge with public relations because they are harder to predict and out of your control. External threats include any scandals, negative events, societal uproar, boycotts or other outcries from the media or public that could harm your brand. Part of pr audit is to assess as many potential threats or to brainstorm possible scenarios that might affect you. Another component in developing a reactive PR strategy involves planning how to solve unpredictable external threats or events. For example, if an unexpected negative event occurs, it will wait 24 hours to respond or issue an immediate statement. It is also part of the structure strategy to determine which methods, such as press conferences or press releases, should be used to combat negative events. A planned, systematic response to unexpected events generally leads to a more positive impression than an unprepared, impulsive response. Public perception of a company or agency can be significantly affected by external communication, while the job satisfaction of its employees depends in part on internal communication. The creation of an effective message or a communication campaign begins with a study of several factors. In a world where people are being inundated with thousands of messages every day, their primary question is often Why should I care? or what do I get in it for me? Effective communication makes this answer clear to the reader or Ask yourself what information would be most important to you if you were a member of the audience and do your materials provide this information. Highlight the benefits at the beginning of your message or materials before adding less important information. Keeping your communication straightforward increases the likelihood that it will be effective. Target a reading level in sixth to eighth grade for written materials. Avoid using acronyms, regulatory expressions, or jargon. Delete words if an average person you stopped on the street doesn't know their meaning. When preparing writing material, keep sentences short and break up copy with headlines and graphics. A page full of text does not appeal to potential readers. Make information available to customers and employees through a variety of formats. Press releases, text messages and emails can be used to communicate important information, while newsletters may be an appropriate choice for content that is less time sensitive. A website is essential for communication with external audiences, and a well-organized intranet that displays news content and practical resources can be very useful to employees. Built-in video presentations allow you to appeal to visual students and offer new perspectives or details. Holding meetings with employees or the public offers personal interaction that can build credibility and make the audience feel valued. Information your customers need to know needs to be communicated as soon as possible. When your audience learns information from the media instead of directly from your organization, there may be a perception that you intend to hide the information or that you don't really care about your audience. The Centers for Disease Control notes in its crisis communication handbook that two of the most serious mistakes an organization can make when communicating with stakeholders provide information that is too little and too late or comes across as arrogant and doesn't value stakeholders. These thoughts are summed up in an agency slogan: Be first. Get it right. Be trustworthy. Employees and the public are often suspicious of companies and government agencies, but you can build trust by increasing the transparency of your messages. Leaders should be gracious with bad news and be willing to express the regret they feel about difficult circumstances. Sharing the reasoning behind difficult decisions can also build understanding. When you reveal harmful information that you didn't need to reveal, you get a reputation for transparency, says Peter Sandmann, an expert in risk communication and business consultant. People start to notice that when you do something wrong, you say it; It follows that when you don't say it, you haven't done anything wrong. Customers and employees don't just have to hear from you when the news is bad. A monthly newsletter or meetings can keep employees informed about the company's activities, while articles about the company's and opt-in emails keep customers in the loop. Financial risk refers to the risks that companies take when making investments, planning the future and carrying out day-to-day operations. All companies take some risk in making financial decisions. Some of these risks are external, depending on external factors and decisions taken by other organisations and consumers. Other risks are internal and take care of the chance that the strategies and actions chosen by business leaders may have negative effects on operations. Market interest rates are one of the most common types of external factors when it comes to financial risks. Market changes based on consumer interest, supply and demand and new elements such as technology. When the economy accelerates or slows, interest rates for bonds and loans change. These changing rates can make it more expensive for a company to get a loan, or require it to make higher payments on bonds it uses to generate capital. Government regulation is another important factor in all financial planning. Governments create tariffs (or taxes on imports and exports), amend existing tax laws and constantly introduce new financial rules. Some changes are beneficial, e.g. Others can make it more difficult for a company to make profits, such as lowering government bond rates and adding new requirements to tax reports. Credit is halfway between being an external and internal factor. In many ways, business credit is an external risk factor because it depends on what external lenders are willing to borrow and the rates or requirements lenders choose for the business. On the other hand, credit depends on the previous decisions the company has made, which lenders it is approaching, and its current financial position - internal factors. Liquidity is simply how easy it is for a company to turn securities into cash. Cash is the most liquid type of fund, but it also makes the minimum amount. Companies must balance how much cash they have in emergencies with less liquid securities such as bonds or shares. Cash flows refer to the company's daily income and expenses. This is an internal risk factor that depends on what expenses a company chooses to pay and how much revenue is directed towards specific areas of the business. By Shea Laverty The vast amount of data stored in a database makes it a critical point of defence for any company – and a valued target for electronic ne'er-do-wells. While external threats are always a priority in data security, a potentially more dangerous and insidious threat is always present: an attack from within. If you learn the differences between an internal and an external attack, you can better protect your database from attacks from all sides. The basic between an external and internal threat is the identity of the Attacker. A simplified way to see this is to look at attackers versus saboteurs. External threats, or attackers, act from outside the company and must overcome your outside defenses to reach your database. Internal threats, or saboteurs, work in the company and can thus bypass external defenses. As trusted members of the company, they already have far more access than any external threat. The intentions behind a threat to the database are another key issue. External threats are almost always malicious, with data theft, vandalism and disruption of services all possible targets. Internal threats can be just as vicious and may also include extortion or other illegal activities. Internal threats, however, are not always malicious. Sometimes the threat is not a person at all, but poor internal security policies and measures that cause unexpected or accidental database breaches, or reveal weaknesses for external attackers if they violate or circumvent external security measures. External threats are limited to what access they can gain outside the company's data network. They must be able to bypass or disable external defenses before they can even log into the network and access what data is available for non-privileged accounts. Internal threats have different levels of access based on privilege level, but generally have access to basic network resources through legitimate login information. More privileged users may also have direct access to the database and other IT resources, as well as potentially sensitive information. Many external attacks have an internal component that facilitates easier access or performs their own illegal operations. While in some cases this is an actual saboteur, many other internal components of external attacks include Trojans, keyloggers and other malicious software that either creates open channels for intruders or enable them to use legitimate log-in information to gain unauthorized access. Social engineering, or manipulation of personnel to create or expose security vulnerabilities, serves as both an external and internal threat. Social engineers prey on unwitting victims with scams, including calling and pretending to be technical support to get sensitive information or install malicious software and leaving official-looking physical media filled with malware for unsuspecting victims to find. Social engineers can even swap for common courtesy, after oblivious staff in restricted areas and pretend to have lost their validation token or ID card. The only way to really mitigate attacks from social engineers is to strictly educate employees about password confidentiality and security protocols and enforce these protocols. Purely external threats are primarily covered with strong firewall and IPS protection on the web The more difficult task is internal security, security, often require significant policy changes. This includes changing password policies to increase password strength and monitor all database access, especially of users running from abnormal locations such as programs outside the network. Internal security should be geared in a top-down way, with security measures in the case of users of all privileged levels, as saboteurs can come from all levels of the organization. Organization.