ABERDEENGROUP

HOW TO MARKET THE VALUE OF INFORMATION SECURITY SOLUTIONS

WHITE PAPER

HOW TO MARKET THE VALUE OF INFORMATION SECURITY SOLUTIONS

For marketers of information security solutions, getting the message across about your company's products and services can be challenging. You know your solutions are effective at protecting against security compromise, but your efforts don't always pay off quite like you've planned.

This brief is designed to provide insights into how information security buyers think to help you effectively articulate the impact of information security solutions on their company's bottom line while improving your own.

The Value of Information Security

What makes a company secure? It depends largely on who you ask. As you probably well know, security can mean different things to different people—from physical security to virus protection to firewalls and more, there are many facets to keeping a company protected.

And, some would say that different industries require different levels of security and protection. While it is certainly true that a government or financial entity would be likely to do as much as possible to keep their data safe, the impact of a security breach can be proportionally disastrous for a retailer or even a very small business.

Over the past several years, we've heard increasing numbers of news stories about information security breaches at large institutions. Although those incidents were highly publicized, they constitute only a fraction of security incidents that occur every year. When customer data is compromised, it makes headlines; however, smaller incidents can spell disaster for companies of all sizes.

Information security providers have the unfortunate position of being largely underappreciated players in the IT space. People tend only to think of information security when a problem occurs—have you ever heard a news story about how secure a company network was? No, we tend only to hear anything when something goes drastically wrong.

With such high stakes, you'd think companies would place as much value on information security as they are in the newest, shiniest phone or tablet. The absence of a security breach makes a company no more secure than a house without locks on the doors; just because nothing bad has happened so far certainly does not mean it can't or won't happen in the future. It also doesn't mean that a company should neglect to protect itself. The true value of information security is difficult to quantify, but considering all the

Top two factors in risk identification = Likelihood + Impact

SECURITY INCIDENTS

› Verizon's 2014 Data Breach Investigations Report (DBIR) analysis indicated that about 90% of security incidents could be placed in one of these nine categories:

- Point of sale intrusions
- Web app attacks
- Insider and privilege misuse
- Physical theft and loss
- Miscellaneous errors
- Crimeware
- Payment card skimmers
- Denial of service
- Cyber espionage

ways a business can be affected by any number of incidents, that value becomes increasingly clear—and this is where you need to begin to focus your marketing message.

is difficult to quantify, but considering all the ways a business can be affected by any number of incidents, that value becomes increasingly clear—and this is where you need to begin to focus your marketing message.

Identifying Risks and Threats

The two most important things to consider when identifying risks are to estimate the likelihood of a security breach, and to estimate the impact to the business of a security incident does occur. But modern security breaches are still in their infancy, since digital data loss has only been a concern for a few decades.

Understanding the effects of data breach and other security disasters is only one piece of the puzzle. Disasters can strike at any time with little or no warning. Companies need a comprehensive disaster recovery and business continuity plan that covers loss due to human error, software errors, hardware failure, natural disasters, viruses, and crimeware in addition to security breaches by hacking. After all, even a few hours of downtime or a small amount of data loss can be damaging, if not devastating, to most companies.

To cover all their bases, an organization needs to know where they stand in terms of protection against all of these threats. Only after a company has conducted an investigation into the current state of their information security can they begin to determine how to protect themselves against threats. It's crucial for all organizations to have a plan in place that will enable them to continue conducting business, even if some of their critical systems are compromised.

The good news is that the information security industry is maturing in its ability to help companies predict the likelihood of a security incident along with the measures necessary to counteract specific types of threats. Research data like Verizon's DBIR, which provides a fact-based perspective on the impact of security incidents by organization size and industry, enables analysts to better quantify the risk of falling victim to specific types of security incidents along with the associated costs. A key part of your marketing communication strategy should include leveraging this type of analysis to help your buyers find that first piece of the

risk identification puzzle—likelihood of a security incident—by correlating any or all of the nine categories to the solution set you are marketing.

A less-obvious risk is one that the news stories don't often cover—the risk of fines and other legal action. In the United States, many government agencies and other organizations like the FBI, the SEC, the FTC, and the Payment Card Industry (PCI) can levy fines not only on the company itself but also its C suite if found liable for data breach. And, entities affected by security incidents can pursue litigation to recoup costs and repair damages. As a marketer, you can help educate your buyers by sharing any updates or changes to legislation or thought leadership from trusted experts on the real-world impact of these regulations.

Speaking the Same Language

When communicating about information security solutions, you want to be sure you're speaking the same language as your buyer. Using highly technical terminology and jargon won't always help your customer understand the benefits of buying your products and services. And, understanding the company's approach to security before you begin your conversation can help you personalize messaging that addresses specific areas where the company may be at increased risk.

It's also important to differentiate between communicating about threats versus risks. Many security professionals use words like "vulnerability," "threat," and "exploit" interchangeably with the word "risk." But they are not the same. Think about it this way: a

TECHNOBABBLE

› Will this kind of information actually help influence your buyer?

"Cleverly engineered *stealth malware*, known as *rootkits*, is designed to evade detection, persisting on endpoints for prolonged periods of time. And new strains of malware are targeting an area of endpoints that performs critical startup operations, the master *boot record*, which provides attackers with a wide variety of capabilities for penetration, persistence, and control. In both cases, we may already be infected but not even aware."

DEFINITIONS

- A **security incident** refers to any event that attempts to compromise the confidentiality, integrity, or availability of an information asset.
- A **data breach, or data compromise**, refers to a security incident resulting in the confirmed disclosure of an information asset to an unauthorized party.
- The **risk** of a data breach must be described in terms not only of the likelihood that it may occur, but also of the business impact if it actually does occur.

What costs are associated with security compromise?

- Reimbursement for fraudulent charges
- Insurance premium increases
- Lost or stolen device replacement
- Fees to consultants assisting with the forensic investigations and assessments
- Incident response team management
- Fines
- Legal fees
- Training
- Notification costs
- Identity monitoring
- Product discounts
- Remediation costs
- Corporate fines
- Loss of company IP
- Stock price decline
- Loss of reputation
- Revenue loss
- Diminished rate of new customer acquisition or customer retention
- Abnormal turnover

vulnerability is leaving your doors and windows unlocked when you are not at home. An exploit is the method by which a robber breaks into your home: they walk right through that unlocked door, or break a window to gain access. And, the risk is that heirloom jewelry or other personal items are stolen, or family members are placed in harm's way—the after-effects of a break-in if it does occur.

Let's continue the robbery scenario for a moment. If you were selling a home security system to a concerned father, he might tell you, "I need everything you have to keep my family safe." That father is leaving it up to the security company as an expert to handle all the details. He may not need or want to know all the different ways someone could break into his family home—he just wants to be assured that he is purchasing the best possible protection and has engaged an expert to carry out the specifics.

The same is true when it comes to information security and businesses: you're the expert. Offer your customer everything you have to keep their business safe. It's likely there will be details they will want to learn about how your products and services protect against specific types of threats, but the most important thing they will want to know is that they will be protected—not only against specific threats, but also the financial impacts of those threats.

Explaining Costs Associated with Security Compromise

Using tools like the data from the DBIR along with the Aberdeen Group's simple Monte Carlo model1, you can help a prospective customer understand their level of risk, based on a variety of factors. While the costs for security compromise for small and mid-sized organizations are lower than those for large enterprises, the amounts are likely to create setbacks for any company. This is where you can help them fit in the other piece of the risk identification puzzle—impact on their business.

Certain industries are at higher risk for security compromise than others, so when you are working with a prospect, be sure to factor that information into a risk analysis. Communicating the risks to buyers can be impactful when presented in terms of the

Now that you have picked a few tips on how to refine your messaging strategy, check out the latest trends in content strategy.

dollar value based on a variety of scenarios. For example, the DBIR tells us that for the private sector:

- The median cost of a data breach is about $63,000, based on a compromise of 10,000 to 100,000 records
- In the next 12 months, there's a 90% likelihood that a data breach will cost more than $20,000
- In the next 12 months, there's a 10% likelihood that a data breach will cost more than $112,000

That type of quantifiable information can be infinitely more helpful to a potential security solution customer than granular descriptions of the type of threats that could affect them. Communicating the specific costs associated with security compromise can provide your customers with a bigger picture of what they might face in the event they are breached in some way. It's possible they may never have considered the full business impact of a security incident.

The ability to identify and express risk in terms of the likelihood AND impact—as a range of associated costs—will help your prospect comprehend just how dangerous inadequate or nonexistent protection can be over time. When paired with the ways your solution can help defend their data, their revenue, and their reputation, the value of your products and services will stand out to your buyers in a way that they cannot ignore.

Source

[1] *Quantifying the Risk of a Data Breach, Based on Verizon DBIR, Aberdeen Group, 2016*

About Aberdeen Group

Aberdeen Group is the leader in bringing big data and content marketing services together for sales and marketing professionals. Our solutions provide proprietary intelligence on who their ideal target audiences are, what they are interested in now, how to connect with them and what content to share with them. The Aberdeen integrated marketing solution provides our customers with a unique ability to reach the best opportunities.

*Learn more at **aberdeenservices.com**.*