ZECURITY ASCENT

Elevating Your Brand & Reputation CYBERSECURITY

ZecurityAscent
eBooks
First Edition

Table of Contents

What is Your Cybersecurity Brand & Reputation?

Everyone has a brand and a reputation. Everyone. Even information and cybersecurity programs have them. Some are cleverly branded the "department of no", while others are seen as nothing short of role models. And some are simply not seen at all, which is also a bit of a brand...and reputation.

MEASURING FOR SUCCESS

IT departments have long held dear the business need for customer satisfaction. As a result, the best do what they can to measure their success.

Now, as it relates to cybersecurity, what if you take that to the next step, which is to ask the Chief Information Security Officer (CISO) to convey both the brand and the reputation of the overall program. Would he/she be able to say what, exactly, that is... for both? And knowing that it can change daily, is there a program in place to proactively measure the sentiment? Just putting a social media type of scale on it, would it convincingly support 1, 2, or 5 stars?

CREATING YOUR OWN VALUE AND SCORE

As companies across the globe prepare themselves for a potential data breach, it's inevitable that such an incident would have a negative impact on both the brand and, if/when disclosed, reputation.

But what if the cybersecurity program itself was widely considered to be a role model? And what if the public sentiment started out sufficiently high enough that faith in the security team and the company was more or less implied?

In other words, what if the brand and reputation started out at 5 stars and only dipped to 4 for a week while more content was created to again get back to the top? Isn't that better than starting at empty or the bottom?

This is exactly what is at stake. Just how prepared an organization is for a cyber crisis will ultimately come down to what these scores are going in.

BRAND is what the security team has promised to their customers (lines of business) for their service and what that commitment means to them.

REPUTATION goes beyond brand to further include all the external parties as well: journalists, investors, employees, regulators, local communities, etc...

> Lose money for the firm and I will be understanding. Lose a shred of reputation for the firm and I will be ruthless.
>
> **Warren Buffet**

Chapter 1

Mind the Gap [between marketing & security]

Branding and marketing are not the same. As we discussed already, the brand is what the security team has promised to their customers and what that commitment means to them.

Marketing is the vehicle and creative engine that helps get the message out where it can do the most good.

WHERE SECURITY & MARKETING MEET

For most organizations, these two roles are very far removed, save for one of two situations:

Tabletop Exercises: This is the land of make believe, where security invites marketing, among many others, to pretend a large cybersecurity incident has occurred. Done right, it's a great opportunity to reveal, on an ongoing basis, what gaps might exist and work diligently to close them, adopting every new best practice along the way.

The Real World: Now, it's for real. Something bad has happened and the top IT executives are working day and night, helping do all they can to defend both the brand and the reputation. This is where everyone finds out just how well prepared both were going in, how solid the tabletop exercises truly are, and how refined the cyber crisis playbook ultimately was.

> **IT practitioners do not believe that brand protection is their responsibility.** Sixty-six percent of IT respondents do not believe protecting their company's brand is their responsibility. However, 50 percent of these respondents do believe a material cyber security incident or data breach would diminish the brand value of their company.
>
> **Ponemon Institute** | The Impact of Data Breaches on Reputation & Share Value

KEY RECOMMENDATIONS

- **Work Closer:** Marketing and security teams should now be working closer than ever, finding common ground around enhancing and protecting both brand and reputation.
- **Be Cyber Crisis Ready:** Absolutely 100% all in. All stakeholders must be totally confident that a cybersecurity incident will not spiral out of control. The reputation of the cybersecurity program must remain overall positive, before, during, and certainly after an incident.
- **Augment as Needed:** Most organizations don't have marketing leads who know security or security leads who know marketing. And even if they do, a looming crisis is a tough time to expect them to be dedicated to the cause, while also remaining objective listeners to the what the market is saying.

Chapter 2

Actually Avoiding a Cyber Crisis

While for many large organizations it may be considered quite inevitable to encounter a major cybersecurity-related incident, such as a data breach, that doesn't mean that it has to turn into a long term crisis. To illustrate this, let's walk through a fairly typical data breach incident to see how things can unfold...in your favor.

WE'VE BEEN HIT! AND IT'S REALLY BAD!

You have just been contacted by the FBI that they have discovered 2.4 million records on the Dark Web and, well, they have extremely high confidence that it links back to your organization. After a bit of confirmation, you agree that it is, in fact, from one of your systems and a more thorough review is pending.

While this has been rehearsed time and time again through all the quarterly tabletop exercises, things are really starting to sink in. But everyone has their checklist, so off we go.

FORENSICS IS IN. AND IT'S WORSE.

Thankfully you not only have a great forensics team, but they are further backed up by a highly reputable firm that you keep on retainer for situations like this. Both did all their due diligence and have come to the same conclusion: The 2.4 million records was just from one taker. There's evidence that the hole / vulnerability existed for much longer and it must now be assumed that the entire database, roughly 10 times more, is now gone.

IT'S TIME. WE'RE GOING PUBLIC IN 3...2...1

Actually, haphazardly making the obligatory notifications is what most would do. You all, on the other hand, are much more prepared.

As part of your thoroughly rehearsed and detailed playbook, you have quickly assembled a communications package that all stakeholders are as pleased as they possibly can be to get 100% behind. From the top to the bottom, everyone has given the green light.

CEO...check

Public Relations...check

General Counsel...check

Chief Marketing Officer....check

Chief Information Security Officer...check

With the knowledge, belief, and responsibility to do all that is ethically, legally, and purposefully right to now defend the brand and reputation, the collective trigger is pulled and the world is now about to see what you all are made of.

MEDIA CONTACT

Times have indeed changed. It used to be that a single press spokesperson armed with a well crafted press release may have been enough. But then social media happened. Now there are countless bloggers, tweeters, and podcasters. And they are all swimming deep in the media pool. And they have massive influence.

It's time to meet them where they are.

So now all key executives and their delegated representatives are assembled for one final review. The public relations lead (in this case, an outside firm) takes the stage, with the nodding approval of the general counsel. Nothing crazy. Just a quick 15 minute call for one last refresher, making sure everyone's head is the game. Consider it a pep rally if it helps.

Everyone knows exactly what they have to do. By the end of the day every single media influencer on their personalized contact list will have been contacted. Each will ask more questions than the press release divulged and will be pleased that their authentic insider has given them that something extra and of real value, with the particular context that matters most to their readers, viewers, or listeners. Confidence is growing.

Here's just one example. This one is from the perspective of the CISO, who is avoiding the "We reached out to them, but they did not immediately return our calls" situation.

Dear Mike (aka TopSecurityBlogger),

I am the CISO for [insert company name] and just wanted to reach out to you directly, as we are right now connecting with all the top media outlets to let them know the details of a security breach we suffered (press release attached for your convenience).

Given the size and severity, I wanted to be sure you could cut through the noise as well as any of the typical gatekeepers order that you may speak with me directly.

I'm including my direct contact information below (mobile). Obviously please don't share this with anyone else, but rather use it for yourself, as needed/desired. If I don't answer right away and you would rather not leave a voicemail, please go through the two backup contacts that I am also providing. More than likely I am already on another call/meeting, but one of them will surely make fast contact with me to let me know that you reached out. I will then call you back as soon as possible.

Regards,

Bobby CISO: (xxx) xxx-xxxx

Assistants: John (xxx) xxx-xxxx | Jane (xxx) xxx-xxxx

WARNING:

Do NOT do this if you and/or the organization has not fully prepared.

This is a critical crisis phase, full of activity, emotions, and, yes, stress.

Like any crisis, you can choose to fight, freeze, or flee. This is you taking the fight to the streets. Training and preparation is what will make the difference.

THE NEXT DAYS, WEEKS, MONTHS...

The blogosphere and social media are now running wild with all the stories. Everything from LinkedIn to Twitter, to Instagram is commenting with both fury and favor.

The tasks, now, are how to **listen, measure, and engage**. Let's quickly explore each 3.

1. Social Media Listening

Simply looking at what lands on your own personal social media accounts is not what we are talking about here. Neither is going into Google and setting up some saved searches. And we definitely don't encourage you to wallow in the commentary day in and day out, searching for everything you can find.

The media, by and large, is full of opinions, often spilled out by those who seek only to build themselves up by tearing you down.

2. Measuring the Sentiment

Furthermore, real media listening, at scale, takes several things that you will surely be in short supply of. These include: time, tools, and the unbiased discipline to really dig in, discover, and measure the sentiment.

Another way of looking a this is that there are times where you want things to be fuzzy/blurry, as it doesn't warrant much inspection. While at times you will need to be borderline obsessive about just one piece of negative/neutral/positive content. And you will know why when you see it.

3. Hacking YOUR Media

When security professionals speak of hacking, they do so knowing that the term "hacker" started out very much as a good thing. Someone who is a hacker is widely regarded as someone who can expertly solve problems. And that is what we are referring to with that very same spirit here.

So how can you expertly use your skills to positively influence your media presence? And, do so **ethically, responsibly, truthfully, professionally,** and **authentically** to the brand and reputation of each spokesperson?

Copywriting (or ghostwriting) is what most will have to turn to, as it's the best way to meet all the criteria. This includes simply being able to scale.

By expertly filling the vacuum of information that has come to light through all the social media listening, marketing copy must be created for each platform whenever and wherever it makes sense.

Engagement is really required. After all, it doesn't do much good to just have amazing thoughts in your head, in draft sitting on your computer, or held up through a dysfunctional social media approvals process. Engaging with your audience, as well as creating new audiences, it going to take real, daily execution.

Go to Brand24.com and create a free account. Then use that to build a view on just the cybersecurity brand and reputation of your organization. Is the sentiment negative, neutral, or positive? And is close to being right?

Now, without overthinking it too much, ask yourself if you would consider, as an outsider, if your cybersecurity program should be 1, 3, or 5 stars.

ZecurityAscent is not affiliated with Brand24. It's just one of the many tools that we, ourselves, use.

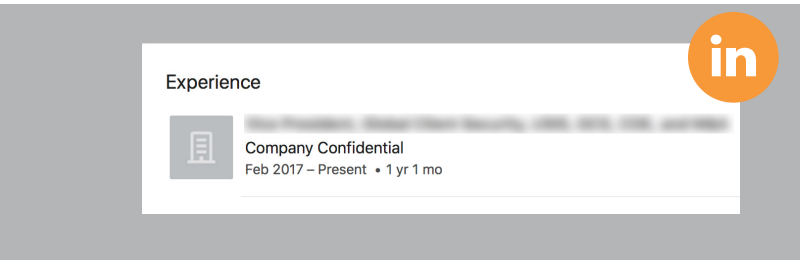
Chapter 3

Recruiting Top Talent

Do the very best IT organizations attract and retain the top cybersecurity professionals? From our experience, the answer to that is undoubtedly yes. But if you are not quite sure, consider what the potential looks like for those organizations who have faced, or are now facing, a cyber crisis.

LEAD OR FALL BY EXAMPLE

The image below is from a top cybersecurity executive who works for a data breach headline-making company. As you can tell, this is very much a sign of a personal brand in crisis. Because while all previous employers are listed, the most current one is clearly being excluded. The pride is gone.



PREPARING FOR THE BEST

When you, yourself, start looking for a new and exciting opportunity, do you go to places like Glassdoor and LinkedIn to see who all is working there, who all left, and what caliber of individuals you would likely be working with?

Of course you do. The great ones always do.

Absent anything else out there, such as impactful content from the IT security organization itself, and especially the security executives, the go/no-go decisions to pursue a position with your team(s) may very well be made on what is perhaps some otherwise really bad data.

But, by creating the right content, that is as authentic as it is valuable to the cybersecurity community at-large, and using that to exponentially enhance your brand/reputation, it's far more likely that the best talent won't have to be found. Instead, they will find you.

> **When you start losing confidence in an organization, all the parts that rely on data become questioned by the individual. Organizations going through digital transformation lose.**
>
> Ponemon Institute | SecurityRoundTable.org
>
> **For Today's Chief Marketers, Cybersecurity Is a Key Campaign**

About the Author

Kevin Peterson is the founder and chief content officer at ZecurityAscent. With 3 decades in security, ranging from the US Air Force to Silicon Valley and up to the Fortune 10 ranks, Kevin is a steady global voice on the value that great security brings to our lives. As an executive blogger, author, speaker, analyst, and copywriter with full cybersecurity proficiency, his ability to understand incident findings and instinctively put them to use for both internal and external brand & reputation needs is the positive force that companies search him out for.

> As if data breach notification costs weren't enough of a financial penalty, businesses that fumble the ball in responding publicly to a data breach can incur additional indirect costs from a loss of brand value in the marketplace. CISOs are making significant investments in people, processes and technology to protect the privacy of their customer data. It's a shame if all that investment was neutralized by a weak, reactive, uncoordinated marketing response.

Patrick Gaul | Executive Director
National Technology Security Coalition

Chapter 4

5 Steps to Your New **Brand** Success

> When ego clouds our judgment and prevents us from seeing the world as it is, then ego becomes destructive. When personal agendas become more important than the team and the overarching mission's success, performance suffers and failure ensues.
>
> **Jocko Willink & Leif Babin**
> Extreme Ownership | How the U.S. Navy Seals Lead and Win

Few would argue that the U.S. Navy Seals don't have an unbelievable brand. Those who must call on them certainly have do doubt of their capabilities and what to expect in their desired outcome. And of course their reputation across all military branches and the outside world is nothing short of legendary.

But they lead and win because they take extreme ownership in all that they do, putting aside their egos in order to work with all internal and external partners as needed. And as quiet and behind the scenes as they are, everyone still knows their brand.

What most seldom consider though is that their brand and reputation is always being fully managed. While they are quiet professionals by design, they move quickly to address anything that might jeopardize their mission. There is simply nothing as important as maintaining their standing as the very best, as the fate of current and future missions depends on it. And you can bet the Department of Defense, through their marketing efforts, invests appropriately in that image.

Now let's look at what 5 steps can be taken by any company to ensure that their cybersecurity teams have a brand that matters as much to their business needs as the elite special operators do to their chains of command.

1 | COMMIT TO YOUR BRAND

Both the IT and marketing teams must commit to enhancing the cybersecurity brand of the organization. And, ideally, do so long before a security incident lands right on their doorstep.

If the consensus brand of the cybersecurity program is currently "the department of no", that needs to get fixed. And it needs to get fixed internally first, if it is going to have any chance of survival externally.

Having all parties aligned around this mission is what will make it successful. It's not enough that security takes it seriously if the marketing resources are not there to help get the message out. Likewise, it does no good for marketing to simply state that they will protect and defend the brand if/when called for, as that need is already there each and every day.

What do you and the business want and need your brand to be? How can both marketing and security work together in making that a reality? And what benefits will be gained once that is achieved?

Only when both are committing to the brand of the cybersecurity program will the full benefits for the business even begin to be realized.

2 | DISCOVER YOUR TRUE BRAND

It's time for some good old-fashioned market research. Much like any survey that IT might roll out to gauge their standing in the business, this one is specifically crafted to the needs of the cybersecurity program.

SURVEYS

Internally, this seeks to discover what the various stakeholders believe the cybersecurity program to be. Will they have your back when a cybersecurity incident happens, or will they rather be stabbing you in the back by quickly running out and declaring on social media that it was really just a matter of time?

Externally, it's about what others in the cybersecurity landscape believe your program to be. For example, if you were to tap into the local Information Systems Security Association (ISSA) chapter and could get an estimated score of your security program from each of their officers, who are all generally very well connected throughout the community, what do you think that would be? Why not get a trusted third party to ask them?

SENTIMENT SCORES

Beyond the brand itself is reputation. Specifically, the way the rest of the world sees your cybersecurity program. This is measured by sentiment. While it's hard to nail down, there are several marketing tools that can help. While they are mostly outside the scope of this document (Brand24 was mentioned), let's just say that in the hands of someone that really knows how to use them and can fully apply the security context to that data, a great deal can be learned.

Just know that an accurate measurement of the cybersecurity sentiment is not magically going to find you. And a few tweets in your feed won't even scratch the surface. It takes tools, applied knowledge, research, and objectivity.

If content is king, context is god

Gary Vaynerchuk

3 | GO CREATE, BUILD CONTENT

A strategy is a great thing to have. But the discipline, resources, and drive to execute is even better—and required. To help keep that alive, a professionally managed **editorial calendar** for your content marketing activities is always recommended. Marketing maintains it, but of course the security team, or at least the security copywriters that know you, will keep it filled with as much relevant content as is needed. And all of the content is attributed directly back to your cybersecurity thought leaders, as it should be.

At a minimum, a positive security/marketing alliance will regularly build great content across 3 key areas:

BLOGS

Blogs exist just about everywhere you look.

Don't want to use the corporate blog (we seldom recommend you do), go create one yourself. Just make sure it stays well secured and regularly updated with fresh content. The best part is that the audience can subscribe to your content, so they always get your new content in their inbox.

LinkedIn can also make for a fairly useful ad-hoc blogging platform, but should not be the primary place to go.

Beyond this, partners and security vendors would no doubt love to see you share on their sites.

SECURITY TALKS

All those local and sometimes far off security conferences you or your team never gets around to going to...**GO!**

And not only go, but reach out to the conference hosts and tell them you have a great presentation for their audience, told by someone who is not a vendor. Most will jump at the chance to at least put you on a panel. This will also get you and your company's name on the web site, which then shows up on later searches.

Speaking at any security event sends, at the very least, a signal that both you and your company are true thought leaders.

SOCIAL MEDIA

Twitter, Facebook, Instagram, LinkedIn, Reddit...the list goes on and on.

Links to blogs, talks, and even just a healthy balanced retweet of something you find interesting is going to generate a historical view of who you are, what you bring to the community, and why your company is damn lucky and smart to have you.

There's increasingly a science to this, especially when seeking to make the most out of each. But again, marketing can really help out here.

And don't be afraid of paid advertisements, especially for recruiting top security talent.

If you find yourself looking for a job, where is perhaps the first place you look these days? LinkedIn? Sure, most likely.

And why is that? There are 3 reasons, actually: **Relevance, Reach,** and **Resonance**. More specifically, you will instinctively start looking at or through your relationships for those leads that are relevant, have a broad reach across your shared landscape, and resonate with others through their own engagement activities as people "like" what they, themselves, are saying.

"Hey, Bob, I know that you are super connected and certainly considered a true thought leader. I read and respond to your stuff often, as I'm sure you have seen. Anyway, I am putting myself on the open job market and wondered if you know of any organization in need of my skills. As always, please let me know if I..." - Suzy

But what if you didn't even have a LinkedIn account to begin with? How will you possibly engage everyone in the time you most need them (hint: you won't)?

THE CYBERSECURITY INFLUENCER

Everyone in cybersecurity knows the name Brian Krebs. And everyone in marketing who has had to deal with a cybersecurity incident or crisis also has. He is the go-to name that will be dropped by the majority whenever anyone asks who the top security-related influencers are.

Brian hits all 3 traits of a great one: relevance, reach, and resonance.

He's not the only one though. There are quite likely dozens that you will want to research, follow, and keep on your target list and engage should anything go wrong. And then there are many more that might pop up after a security breach, as they have suddenly taken a interest in your business and the security posture thereof.

You could go about trying to become an overnight star and get your positive and encouraging messaging out yourself. Or you could engage them in the most appropriate ways so that they would be willing to put their star power to use for you.

Just don't underestimate the amount of work involved in getting them to amplify your message.

> For the visionary marketer, the rise of the social media influencer creates a world of possibilities. It opens up a new channel for brands to connect with consumers more directly, more organically, and at scale.
>
> **Adweek** | 10 Reasons Why Influencer Marketing is the Next Big Thing

5 | DEFEND: LISTEN, EXECUTE

The path to cybersecurity brand resilience is not produced by a public relations spokesperson or outside firm. Neither is it born from hiring new security leadership that merely promises to make changes. It is the product of an ongoing program that delivers real content that matters, as told by those who are truly closest to the facts.

Just as any successful salesperson and their company follows a process, the cybersecurity marketing efforts must also follow through. This means listening to the markets, including all relevant channels and platforms, then executing as early and often as needed. Be it proactive or reactive, it takes more than one social media savvy/driven security professional. This is truly a team sport, complete with coaching and regular exercise.

So with each post or speaking engagement, the goal must always be to keep the process working in your favor. Keep driving and defending until you know you are a 5 star cybersecurity program. Then go teach the rest of the world.

DEFENSE-IN-DEPTH:

This time the top layer of defense is the brand and reputation of the cybersecurity program itself, allowing the business to breath a sigh of relief that the culture is working in everyone's favor.

If/when the worst happens, the best media channels will see that whatever may have failed or been victimized, the cybersecurity team is more than capable of dealing with it and maintaining confidence.

In Conclusion

Just as the first impression is always of the utmost importance, the same can be said about the first one an organization must make when being re-introduced to the world following any major cybersecurity incident. Will a great brand and reputation precede them, or will the media as well as their partners, customers, and other stakeholders have to go digging? And if they don't find anything meaningful or otherwise compelling, who will fill that vacuum? Who, in fact, will tell their story for them?

The rules that once governed corporate marketing, public relations, and risk management have been altered by the rise of social media. Just as security teams have had to wrestle with gigantic shifts in security due to various governance, risk, and compliance standards that are many times at odds with the business and their users, the ways in which both marketing and security executives must now come together to enhance and defend brands and reputations through both legacy and new media brings with them some clear challenges.

There is work to be done, but the map to success is surprisingly quite clear. It's simply about bridging the natural gap that exists between marketing and security. It's about being both a thought leader as well as an organization that can execute. Because while there are countless "strategists" out there laying out what all should be done, building out a cybersecurity marketing team/program that can execute on that plan daily is where the real reward is.

This is what the entire business is after. From the CEO to the boardroom and every long-term investor/stakeholder, the successful business has truly 'cracked the code' on how to sustain the brand and reputation that matters in a cybersecurity incident: that of the cybersecurity program itself. After all, no one rushes back into a restaurant when it's failed the health inspection, at least not without a fair amount of marketing and retargeting efforts. The very same holds true when it comes to information security.

Building out the program before a cyber crisis is perhaps the best way to avoid getting into one in the first place.

Who Are The [cybersecurity] Leaders in Your Neighborhood?

I live in Atlanta and whenever anyone asks me who the local cybersecurity leaders are I can pretty much name them off the top of my head. That goes double for their highly respected security programs.

Their brands are solid, and their reputations precede them. They lead by example and are often as public as they can be. Sadly, nearly all of them could be much more, as they simply don't have the time or supporting marketing programs to take them and their organizations to that now critical next level.

Unfortunately, there are many that no-doubt assume they are on the leaders list and would be genuinely shocked to find out that they are, quite objectively, not. And for a variety of reasons.

But this is what we wish for every company. We wish to see them ***enhance their brand and reputations before a breach, so that they can quickly recover them after one.***

Because from all that we and others have seen and measured, those who do not invest in this area are unlikely to be even remotely prepared in defense of a real cyber crisis.

Kevin Peterson, CISSP
Founder | Chief Content Officer
ZecurityAscent, LLC

Please check out our key cybersecurity marketing resources:

- *ZecurityAscent Web Site*
- *Cybersecurity Brand & Reputation Academy*

as well as our direct social media links below....