The Forgotten Fear Factor

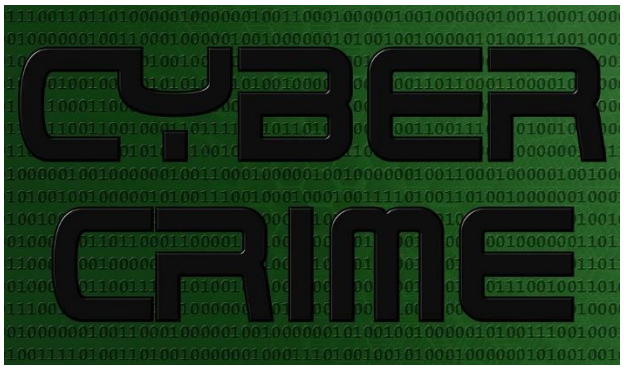
Communicating During a Hack Attack

Ed Barks

www.barkscomm.com

It's not like the impact from an industrial accident or a hurricane. When your business is hit with a cyberattack, you may not learn about it for months. And that's if your tech team is on the ball.

Cybercrime is now a big business. Life was easier when it was just unshaven, smelly guys subsisting on Cheetos and Peanut M&Ms, living in their parents' basements. These days you're in for a business-to-business brawl or, even more dangerous, a sophisticated attack launched by a foreign government.



Today's executives dread cybercrime, with many viewing it as the number one threat to the business. The odds are strong that you are going to be affected at some point, by either an external or internal hack.

You have a plethora of resources at your disposal that cover certain aspects of batting back a hack attack—insurance that covers some of the damages, guidance from federal authorities as to your legal reporting requirements, and an ever-growing population of companies eager to (allegedly) protect you.

The hard truth is, however, few if any of those resources are capable of walking you through what it takes to communicate when hackers worm their way into your systems. This paper examines that essential yet oft-ignored facet—managing the communications component of the crisis, for how you communicate with your stakeholders in the near- and long-term could spell the difference between survival and chronic struggle.

WHEN, NOT IF

Your business is going to experience a cyberattack. It may occur today, tomorrow, or several months from now. Are you a doubter? Try these example on for size:

- A health insurer that loses track of confidential policyholder data.
- A retail outlet that suffers theft of customer credit card records.
- An online small business that is forced to devote massive resources and months to overcoming a nefarious hacker.
- A medical device manufacturer whose products—and more important, patient safety—are compromised.
- The internal threat, in which one of your workers sells access to your data for a few thousand dollars.
- Another internal threat where the hacker gives one of your workers a thumb drive (and a bounty) to inject malware into your system.
- A problem your chief risk officer never saw coming.
- You discover you've been victimized by ransomware, a situation in which black hats put a "time bomb" in your system that activates after your backups are too old to do any good. Do you want the solution? Pay the blackmail to the not-so-nice man.

Do you still have doubts? Don't take my word for it. Ask executives at Anthem, Target, the Democratic National Committee, SmallBizDaily.com, Medtronic, and a plethora of other firms. The above examples are not fantasy. Those businesses and the marketplaces that rely on them paid the price of a hack attack. They suffered these all too real impacts:

> When your business is hit with a cyberattack, you may not learn about it for months. And that's if your tech team is on the ball.

- Shrinking revenues
- Lost customers
- Untold financial pain
- Psychic anguish
- Time and productivity costs
- A tarnished reputation, both for your firm and for your executives' career arcs

Why do you think insurers now offer cyber risk seminars that offer insight into potential cyber threats, how to combat them, and their regulatory ramifications? Yes, there's gold in them thar cyberhills.

An infographic from Cybernetic Global Intelligence outlines what's on the cybersecurity horizon. Things are not getting any easier as hackers become more sophisticated and pursue targets that have yet to harden themselves.

Your business plan likely sets forth the information technology (IT) resources you'll rely on when hackers hit. Some businesses stop there. Big mistake.

Your discovery of and recovery from the attack may be altogether elegant. Your technical team may succeed in fending off or minimizing negative consequences. Regardless, you're going to come under fire from customers, shareholders, industry analysts…perhaps even government regulators.

Yes, you may lose intellectual property, suffer theft of credit card information, and become subject to a slew of governmental oversight hearings. Of equal import, your good reputation—the one you've taken decades to foster—will be in tatters.

COMMUNICATION IS KEY

More and more businesses are developing cybersecurity disaster preparation plans. It's a necessity in this day and age. But if you stop there, you're only fighting part of the battle.

A cyber *communications* plan is also a must. Just as an overall communications plan guides your business to a better public image (you do have a communications plan, don't you?), a cyber communications plan spells out how you will react and the steps you will take when hackers assault your organization.

Fail to devise such a plan and you'll be left scrambling in a panicked and most disorganized manner when catastrophe arises. Make no mistake, this means a written plan, one that all of your workers can reference.

Sadly, relatively little guidance is available about this vital facet of crisis planning, though the tip sheet "Nine Crucial Crisis Communications Tips" can help you set a general framework for your approach to a cyber intrusion.

Plug the term "cybersecurity communications plan" into your favorite search engine and you'll see plenty of advice about privacy, securing credit card information, better

protecting mobile devices, and fending off email incursions. But you have to scour deep to find anything substantive and helpful about communicating with your publics.

WHAT TO DO IN THE MIDST OF YOUR CYBERCRISIS

The biggest cyber threat cited by many chief information officers is their own staffs. Workers who click on phishing links, visit sketchy web sites, or steal data for their own illegal gain scare the bejeebers out of these executives. For a look into the biggest perceived hazards, see "What Will Be the Biggest Security Threat of 2016?" by Kathryn Cave in *IDG Connect*.

This, of course, argues that your communications about cybersecurity need to begin *before* events occur. You must communicate with employees and bring them up to speed on best security practices.

Once the cat is out of the bag, the pace of your communications picks up rapidly. You must be ready with a plan that answers such key questions as:

- How much information can you disclose, both legally and from a business perspective?
- Who is empowered to speak on your business' behalf?
- Who belongs on the team that will craft and continue to refine your message as the crisis unfolds?
- Is there still a way to protect any intellectual property that may have been pilfered?
- What steps can you take to assuage clients and consumers and make them whole if their data has been swiped?

Cyber theft is as much a communications problem as an IT issue. To be sure, you need to include your online security and risk teams as you seek to understand and define your predicament. In most cases, however, these are not the spokespeople you want front and center when explaining things to the world. Jane and John Q. Public don't need a buzzword-laden technical rundown; they need

Preparing for Your Cybercrisis

- ✓ Charge your communications staff with organizing and leading regular simulations surrounding cyber threats.
- ✓ Hold periodic media training workshops for those executives who will be in the press' line of fire. Note that this means more than a "one and done" session. You need ongoing skill sharpening.
- ✓ Do your best to assure that your communications, legal, and public affairs teams play nice together.
- ✓ Establish a relationship with an experienced communications training consultant who can guide you before, during, and after your cyberattack.

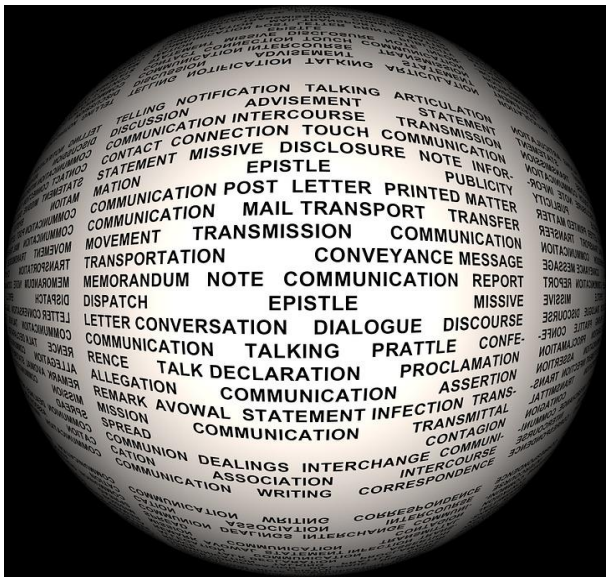
to know how your incident affects them, what you are doing to solve the problem, and what, if anything, they need to do.

In most cases, the bad news and resulting solutions should come right from the top—your CEO. Let's hope that your business is one that plans for the future ahead of time and that you have a strong relationship with an experienced communications training consultant capable of guiding your leadership through an ongoing media training program.

When the crisis strikes, hold that consultant close (you may want to consider a retainer arrangement to see you through the hot and heavy times; this ensures you have ready access to the strategic communications and messaging counsel you're going to need).

PREPARATION STEPS YOU NEED TO HEED

Take the long view. This is admittedly a challenge in the day and age of quarterly results and their expectations serving as the benchmark for success or failure. Prudent investments—both in technology and in communications capacity—are necessary on a sustained basis.



There is plenty of advice available regarding how to bolster your IT department: Hire more skilled workers, buy that shiny new company's anti-hacker services, tighten your company's email filters.

But what of the important question, how can your business ramp up its communications strength? There seems to be far less discussion on this matter, so here are some suggestions to help guide you:

- Charge your communications staff with organizing and leading regular simulations surrounding cyber threats.
- Craft your message in anticipation of an attack. While you won't be able to divine the precise nature of your situation, you can and should set a general template that helps you outline what to say when the time comes.
- Decide which executives will be your public face in which situations. It is normally a good idea to place your CEO front and center, unless he is a lost soul as a communicator.

- Hold periodic media training workshops for those executives who will be in the press' line of fire during any cyber crisis. Note that this means more than a "one and done" session. You need ongoing skill sharpening.
- Do your best to assure in advance that your communications, legal, and public affairs teams play nice together. Anticipate disagreements about how much to say when crisis strikes (the lawyers typically want to say little while communicators argue for more disclosure), and decide on the proper balance for your state of affairs.
- Establish a relationship with an experienced communications training consultant who can guide you through your mess before, during, and after your cyberattack. If you are under contract with a public affairs or public relations agency, make sure they have someone on staff with this specific type of expertise; be aware that many agencies, even the global players, have axed their training departments in recent years and may lack this capability. Unless your contract with them is written to your extreme disadvantage, you have the right to select an independent consultant to work hand-in-hand with you and your agency.

> You're going to come under fire from customers, shareholders, industry analysts…perhaps even government regulators.

- If your issue is liable to incur governmental oversight, arrange a testimony training workshop for your executives who may be called to testify before Congress, state lawmakers, or federal and state regulatory bodies.
- When the attack comes, put that messaging document into action and make it specific to the real-life conditions you now face.
- Insist on periodic reviews of your messaging as the drama unfolds. In some cases—particularly in the early hours of your crisis—this may require hourly or even minute-by-minute adjustments.

Allow me to emphasize that you must take action and prepare *before* your cyber crisis hits. You will be sorely disappointed if you find yourself scrambling when a crisis jolts you into awareness.

STEEL THY SPOKESPEOPLE

"While terrorist attacks dominate headlines, the threat posed by hacking attacks are the major concern of UK industry," reports the *Telegraph* of London, citing the security

consultancy Control Risks ("Hacking Is the Biggest Threat to British Business," December 14, 2015). Things are no different elsewhere across the globe.

Without doubt, your enterprise is jeopardized when cybercriminals strike. It is important to realize that company executives and board members are at risk, too. The *Telegraph* article goes on to say that cyberattacks, "could lead to a shake-up of companies' boardrooms."

Elsewhere in the article, Control Risks CEO Richard Fenning claims that, since most companies "tend to be run by older people," they are less capable of understanding the risks. As our British friends might say, "Rubbish!"

While some younger workers might have a solid grasp on the technology, they are generally on shakier ground when it comes to designing and implementing strategy. This is not a knock on youth; it's simply due to the fact that depth of insight comes with time and experience. Should board members invite younger workers with different skills to share their perspectives? Absolutely, and those viewpoints should be factored in to the decision-making process. Decision-making authority, however, should rest in experienced hands.

Your communications leadership team offers another indispensable viewpoint. You would be wise to grant them a seat at the policymaking table before, during, and after any situation, crisis or otherwise.

YOUR CALL TO CYBER ACTION

The next time you read an article about a cyberattack and think, "That could have been us," it's too late. The hackers may already have infiltrated your system, too. How effectively are you ready to communicate when that ticking time bomb detonates?

Part of your preparation must involve messaging (for more depth on constructing your message, see "Eleven Elements to Mold a Magnetic Message: How to Shape Your Story

for the Press, Policymakers, and the Public"). With your message in hand, game out some possible scenarios and run your crisis team through them. Determine:

- What aspects of our message work?
- What doesn't work?
- What surprised us?
- Who shined in the spotlight?
- Who should never speak for us in public settings?

> You must take action and prepare *before* your cyber crisis hits. You will be sorely disappointed if you find yourself scrambling when a crisis jolts you into awareness.

Your leadership must insist—indeed, mandate—that your designated spokespeople be part of a regular communications training regimen. This does not mean that your consultant needs to lead formal workshops every month. What it does mean is that they should design a program that ensures your executives sharpen their communications edge steadily over time.

Yes, the program should involve periodic refresher workshops under your training consultant's guidance. Additionally, it should include drills that you can implement internally interspersed with recurrent check ins (by the way, if your consultant fails to mention this type of program, it means one of two things: 1) they aren't savvy enough to set up such a program or 2) they want only to sap your budget by insisting on nothing but soup-to-nuts workshops; run away quickly from such charlatans and seek out another expert capable of advancing your learning in a way that benefits you).

THE BOTTOM LINE

The health of your business revolves around your ability to respond to a cyberattack. The safety and well-being of your clients, customers, and members is at stake. Your good reputation hangs in the balance.

A cyberattack is bad enough. A failure to communicate will seal your fate, relegating you and your business to the proverbial "dustbin of history."

ABOUT THE AUTHOR

As a communications training consultant and author, Ed Barks zeroes in on the messages and skills that executives need on a daily basis. As a result, they gain an enhanced reputation, greater confidence, more opportunities for career advancement, and achievement of long-term business goals.

He wrote the book about verbal and nonverbal communications, *The Truth About Public Speaking: The Three Keys to Great Presentations*, and the training guide, *Face the Press with Confidence: The Media Interview Companion*.

Ed contributes to leading industry journals and is the former "Speaking Sense" columnist for the *Washington Business Journal*. He has published numerous additional works such as "A Buyer's Guide to Communications Training Consultants," "How Important Are Nonverbal Signals?" and "Maximize Your Next Media Training: Best Practice Standards."

He is also the author of the research reports *Thrill on the Hill: How to Turn Congressional Testimony into Public Policy Success*, *But Mom Told Me Never to Brag: Overcoming the Thought Leadership Hurdles*, *The Lasting Effects of Media Training: Lifelong Learning or Temporary Phenomenon?* and *Can We Talk Off the Record? Resolving Disagreements, Increasing Understanding Between Reporters and Public Relations Practitioners*.

Ed has taught more than 5000 business leaders, association executives, government officials, athletes, entertainers, and public affairs staff. His clients say he "knows how to elicit peak performance." They call him "a master at connecting with his audience" and "an effective educator," and give his communications training workshops "two thumbs up!"

He has served as President of Barks Communications since its founding in 1997. He also holds several other leadership roles including service on the Board of Governors of the National Press Club and the faculty of the U.S. Chamber of Commerce Institute for Organization Management.

Visit him online at www.barkscomm.com and follow him on Twitter at @EdBarks. He encourages comments, so get in touch at (540) 955-0600 and by e-mail.